Load Balancing IBM Watson Health iConnect Access by Merative

Version 1.4.0
# Table of Contents

1. About this Guide .................................................................................. 3
2. Loadbalancer.org Appliances Supported ............................................. 3
3. Software Versions Supported .............................................................. 3
   3.1. Loadbalancer.org Appliance ............................................................ 3
   3.2. IBM Watson Health iConnect Access by Merative ....................... 3
4. Load Balancing iConnect Access ........................................................ 3
   4.1. Load Balanced Ports ................................................................... 3
   4.2. Deployment Concept .................................................................. 4
   4.3. VIP Requirements ..................................................................... 4
   4.4. Deployment Mode ...................................................................... 4
5. Loadbalancer.org Appliance – the Basics ............................................ 4
   5.1. Virtual Appliance ....................................................................... 4
   5.2. Initial Network Configuration ....................................................... 5
   5.3. Accessing the WebUI .................................................................. 5
       Main Menu Options ..................................................................... 6
   5.4. Appliance Software Update .......................................................... 7
       Determining the Current Software Version .................................. 7
       Checking for Updates using Online Update ................................ 7
       Using Offline Update .................................................................. 8
   5.5. Ports Used by the Appliance .......................................................... 8
   5.6. HA Clustered Pair Configuration ................................................... 9
6. Appliance & iConnect Access Configuration ........................................ 9
   6.1. Appliance Configuration ............................................................... 9
       Configuring VIP1 – ICA_WEB ......................................................... 9
       Configuring VIP2 – ICA_DICOM .................................................... 10
   6.2. iConnect Access Configuration .................................................... 11
       Solve the ARP Problem ................................................................ 11
7. Testing & Verification ......................................................................... 16
   7.1. Checking the Status Using the System Overview ......................... 16
   7.2. Client Connection Tests ............................................................... 16
8. Technical Support .............................................................................. 17
9. Additional Documentation ................................................................... 17
10. Appendix .......................................................................................... 18
   10.1. Configuring HA - Adding a Secondary Appliance ...................... 18
       Non-Replicated Settings ................................................................ 18
       Adding a Secondary Appliance - Create an HA Clustered Pair ....... 19
11. Document Revision History ............................................................... 21
1. About this Guide

This guide details the steps required to configure a load balanced IBM Watson Health iConnect Access by Merative environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any iConnect Access Server configuration changes that are required to enable load balancing.

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

2. Loadbalancer.org Appliances Supported

All our products can be used with IBM Watson Health iConnect Access by Merative. For full specifications of available models please refer to https://www.loadbalancer.org/products. Some features may not be supported in all cloud platforms due to platform specific limitations, please check with Loadbalancer.org support for further details.

3. Software Versions Supported

3.1. Loadbalancer.org Appliance

- V8.3.8 and later

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

3.2. IBM Watson Health iConnect Access by Merative

- All versions

4. Load Balancing iConnect Access

For high availability and scalability, IBM Watson Health recommend that multiple iConnect Access Servers are deployed in a load balanced cluster.

Note: It’s highly recommended that you have a working iConnect Access environment first before implementing the load balancer.

4.1. Load Balanced Ports

The following table shows the ports/services that are load balanced:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>80 &amp; 443</td>
<td>TCP</td>
<td>HTTP &amp; HTTPS</td>
</tr>
<tr>
<td>4444</td>
<td>TCP</td>
<td>DICOM</td>
</tr>
</tbody>
</table>
4.2. Deployment Concept
When iConnect Access is deployed with the load balancer, clients connect to the Virtual Services (VIPs) on the load balancer rather than connecting directly to one of the iConnect Access Servers. These connections are then load balanced across the iConnect Access Servers to distribute the load according to the load balancing algorithm selected.

4.3. VIP Requirements
To provide load balancing and HA for iConnect Access, 2 VIPS are required as depicted in the diagram above, these are:

- VIP1 : ICA_WEB
- VIP2 : ICA_DICOM

4.4. Deployment Mode
The Virtual Services (VIPs) are configured using Layer 4 DR (Direct Return) mode. This mode offers the best possible performance since replies go directly from the iConnect Access Servers to the client, and not via the load balancer. To use this mode, the "ARP Problem" must be solved as explained in Solve the ARP Problem.

5. Loadbalancer.org Appliance – the Basics
5.1. 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.
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.

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.

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.

5.2. Initial Network Configuration

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

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

5.3. Accessing the 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.

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

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

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


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

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:

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

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

**Main Menu Options**

- **System Overview** - Displays a graphical summary of all VIPs, RIPs and key appliance statistics
- **Local Configuration** - Configure local host settings such as IP address, DNS, system time etc.
- **Cluster Configuration** - Configure load balanced services such as VIPs & RIPs
**Maintenance** - Perform maintenance tasks such as service restarts and taking backups

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

**Reports** - View various appliance reports & graphs

**Logs** - View various appliance logs

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

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

## 5.4. 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:

```
ENTERPRISE VA Max - v8.9.0
```

### 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 v8.9.0 is the current release. No updates are available

4. If an update is available, you’ll be presented with a list of new features, improvements, bug fixes and security related updates.

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:

   **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.

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.

5.5. 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</td>
</tr>
<tr>
<td>TCP &amp; UDP</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>Protocol</td>
<td>Port</td>
<td>Purpose</td>
</tr>
<tr>
<td>----------</td>
<td>------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>TCP</td>
<td>7778</td>
<td>HAProxy persistence table replication</td>
</tr>
<tr>
<td>TCP</td>
<td>9080</td>
<td>WebUI - HTTP (disabled by default)</td>
</tr>
<tr>
<td>TCP</td>
<td>9081</td>
<td>Nginx fallback page</td>
</tr>
<tr>
<td>TCP</td>
<td>9443</td>
<td>WebUI - HTTPS</td>
</tr>
</tbody>
</table>

5.6. 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.

6. Appliance & iConnect Access Configuration

6.1. Appliance Configuration

Configuring VIP1 – ICA_WEB

a) Setting up the Virtual Service (VIP)

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

2. Enter the following details:

3. Enter an appropriate label (name) for the VIP, e.g. ICA_WEB.

4. Set the Virtual Service IP address field to the required IP address, e.g. 192.168.100.100.

5. Set the Virtual Service Ports field to 80,443.

6. Leave Protocol set to TCP.

7. Leave Forwarding Method set to Direct Routing.

8. Click Update.

9. Now click Modify next to the newly created VIP.
10. Scroll down to the **Health Checks** section.
11. Set the **Check Port** to **443**.
12. Click **Update**.

**b) Setting up the Real Servers (RIPs)**

1. Using the WebUI, navigate to **Cluster Configuration > Layer 4 – Real Servers** and click **Add a new Real Server** next to the newly created ICA_WEB VIP.

2. Enter the following details:

   ![Real Server Configuration](image)

   - **Label**: ICA_WEB1
   - **Real Server IP Address**: 192.168.100.110
   - **Weight**: 100
   - **Minimum Connections**: 0
   - **Maximum Connections**: 0

3. Enter an appropriate label (name) for the RIP, e.g. ICA_WEB1.
4. Change the **Real Server IP Address** field to the required IP address, e.g. **192.168.100.110**.
5. Click **Update**.
6. Repeat these steps to add your other iConnect Access Server(s).

**Configuring VIP2 – ICA_DICOM**

**a) Setting up the Virtual Service (VIP)**

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

2. Enter the following details:

   ![Virtual Service Configuration](image)

   - **Label**: ICA_DICOM
   - **Virtual Service IP Address**: 192.168.100.100
   - **Ports**: 4444
   - **Protocol**: TCP
   - **Forwarding Method**: Direct Routing
3. Enter an appropriate label (name) for the VIP, e.g. ICA_DICOM.

4. Set the Virtual Service IP address field to the required IP address, e.g. 192.168.100.100.

5. Set the Virtual Service Ports field to 4444.

6. Leave Protocol set to TCP.

7. Leave Forwarding Method set to Direct Routing.

8. Click Update.

b) Setting up the Real Servers (RIPs)

1. Using the WebUI, navigate to Cluster Configuration > Layer 4 – Real Servers and click Add a new Real Server next to the newly created ICA_DICOM VIP.

2. Enter the following details:

![Real Server Configuration](image)

3. Enter an appropriate label (name) for the RIP, e.g. ICA_DICOM1.

4. Change the Real Server IP Address field to the required IP address, e.g. 192.168.100.110.

5. Click Update.

6. Repeat these steps to add your other iConnect Access Server(s).

6.2. iConnect Access Configuration

As mentioned earlier, when using Layer 4 DR mode, the ARP problem must be solved. This involves configuring each iConnect Access Server to be able to receive traffic destined for the VIP and ensuring that each iConnect Access Server does not respond to ARP requests for the VIP address – only the load balancer should do this.

Solve the ARP Problem

Note: The steps below are for IPv4 addresses on Windows 2012 & later. For other versions of Windows & IPv6 configuration steps, please refer to DR Mode Considerations.

Note: The following steps must be performed on all iConnect Access Servers.
**Windows Server 2012 & Later**

Windows Server 2012 and later support Direct Routing (DR) mode through the use of the Microsoft Loopback Adapter that must be installed and configured on each load balanced (Real) Server. The IP address configured on the Loopback Adapter must be the same as the Virtual Service (VIP) address.

> **Note**
> If a Real Server is included in multiple DR mode VIPs, IP addresses for each VIP must be added to the Loopback Adapter.

In addition, steps must be taken to set the strong/weak host behavior on each Real Server. This is used to either prevent or allow interfaces to receive packets destined for a different interface on the same server.

> **Important**
> The following 3 steps must be completed on each Real Server.

**Step 1 of 3: Install the Microsoft Loopback Adapter**

1. Click **Start**, then run `hdwwiz` to start the Hardware Installation Wizard.
2. Once the Wizard has started, click **Next**.
3. Select **Install the hardware that I manually select from a list (Advanced)**, click **Next**.
4. Select **Network adapters**, click **Next**.
5. Select **Microsoft & Microsoft KM-Test Loopback Adapter**, click **Next**.
6. Click **Next** to start the installation, when complete click **Finish**.

**Step 2 of 3: Configure the Loopback Adapter**

1. Open Control Panel and click **Network and Sharing Center**.
2. Click **Change adapter settings**.

3. Right-click the new Loopback Adapter and select **Properties**.

**Note** You can configure IPv4 or IPv6 addresses or both depending on your requirements.

**IPv4 Addresses**

1. Uncheck all items except **Internet Protocol Version 4 (TCP/IPv4)** as shown below:

   ![IPv4 Properties](image)

   2. Ensure that **Internet Protocol Version (TCP/IPV4)** is selected, click **Properties** and configure the IP address to be the same as the Virtual Service address (VIP) with a subnet mask of **255.255.255.255**, e.g. **192.168.2.20/255.255.255.255** as shown below:
192.168.2.20 is an example, make sure you specify the correct VIP address.

3. Click **OK** then click **Close** to save and apply the new settings.

**IPv6 Addresses**

1. Uncheck all items except **Internet Protocol Version 6 (TCP/IPv6)** as shown below:
2. Ensure that **Internet Protocol Version (TCP/IPv6)** is selected, click **Properties** and configure the IP address to be the same as the Virtual Service (VIP) and set the **Subnet Prefix Length** to be the same as your network setting, e.g. **2001:470:1f09:e72::15/64** as shown below:

![Internet Protocol Version 6 (TCP/IPv6) Properties](image)

**Note**

2001:470:1f09:e72::15/64 is an example, make sure you specify the correct VIP address.

3. Click **OK** then click **Close** to save and apply the new settings.

**Step 3 of 3: Configure the strong/weak host behavior**

Either Network Shell (**netsh**) commands or PowerShell cmdlets can be used to set the required strong/weak host behavior.

The commands in this section assume that the LAN Adapter is named **"net"** and the Loopback Adapter is named **"loopback"** as shown in the example below:

![Network Connections](image)

**Important**

Either adjust the commands to use the names allocated to your LAN and loopback adapters, or rename the adapters before running the commands. Names are case sensitive so make sure that the interface names used in the commands match the adapter names exactly.

**Option 1 - Using Network Shell (netsh) Commands**
To configure the correct strong/weak host behavior run the following commands:

For IPv4 addresses:

```
netsh interface ipv4 set interface "net" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostsend=enabled
```

For IPv6 addresses:

```
netsh interface ipv6 set interface "net" weakhostreceive=enabled
netsh interface ipv6 set interface "loopback" weakhostreceive=enabled
netsh interface ipv6 set interface "loopback" weakhostsend=enabled
netsh interface ipv6 set interface "loopback" dadtransmits=0
```

Option 2 - Using PowerShell Cmdlets

For IPv4 addresses:

```
Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled
-DadTransmits 0 -AddressFamily IPv4
Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled -AddressFamily IPv4
```

For IPv6 Addresses:

```
Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled
-DadTransmits 0 -AddressFamily IPv6
Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled -AddressFamily IPv6
```

7. Testing & Verification

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

7.1. Checking the Status Using the System Overview

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

7.2. Client Connection Tests
Ensure that clients can connect via the load balancer to the iConnect Access Servers. For this, you’ll probably need to create new DNS records or modify your existing DNS records, replacing the IP addresses of individual servers with the IP address of the relevant Virtual Service on the load balancer.

8. 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.

9. Additional Documentation

For additional information, please refer to the Administration Manual.
10. Appendix

10.1. Configuring HA - Adding a Secondary Appliance

Our recommended configuration is to use a clustered HA pair of load balancers to provide a highly available and resilient load balancing solution.

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

Note

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

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

Non-Replicated Settings

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

<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</td>
<td>All network settings including IP address(es), bonding configuration and VLANs</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Routing</td>
<td>Routing configuration including default gateways and static routes</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>System Date &amp; time</td>
<td>All time and date related settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Physical – Advanced</td>
<td>Various settings including Internet Proxy, Management Gateway, Firewall</td>
</tr>
<tr>
<td></td>
<td>Configuration</td>
<td>connection tracking table size, NIC offloading, SMTP relay, logging and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Syslog Server</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Security</td>
<td>Appliance security settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>SNMP Configuration</td>
<td>Appliance SNMP settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Graphing</td>
<td>Appliance graphing settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>License Key</td>
<td>Appliance licensing</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Software Updates</td>
<td>Appliance software update management</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Script</td>
<td>Appliance firewall (iptables) configuration</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Lockdown Wizard</td>
<td>Appliance management lockdown settings</td>
</tr>
</tbody>
</table>
Make sure that if these settings/updates have been configured on the Primary appliance, they're also configured on the Secondary appliance.

Adding a Secondary Appliance - Create an HA Clustered Pair

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

1. Deploy a second appliance that will be the Secondary and configure initial network settings.

2. Using the WebUI on the Primary appliance, navigate to: *Cluster Configuration > High-Availability Configuration*.

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**.
## 11. Document Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Changed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.0</td>
<td>2 August 2019</td>
<td>Styling and layout</td>
<td>General styling updates</td>
<td>RJC</td>
</tr>
<tr>
<td>1.1.1</td>
<td>24 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>1.2.0</td>
<td>1 October 2021</td>
<td>Converted the document to AsciiDoc</td>
<td>Move to new documentation system</td>
<td>AH, RJC, ZAC</td>
</tr>
<tr>
<td>1.3.0</td>
<td>6 September 2022</td>
<td>Renamed document and amended references to the product</td>
<td>Product acquisition by Merative</td>
<td>AH</td>
</tr>
<tr>
<td>1.3.1</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>1.3.2</td>
<td>2 February 2023</td>
<td>Updated screenshots</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td>1.3.3</td>
<td>7 March 2023</td>
<td>Removed conclusion section</td>
<td>Updates across all documentation</td>
<td>AH</td>
</tr>
<tr>
<td>1.4.0</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.