

Load Balancing Merative iConnect Enterprise Archive

Version 1.4.1



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. Merative iConnect Enterprise Archive	3
4. Load Balancing iConnect Enterprise Archive	3
4.1. Port Requirements	3
4.2. Deployment Concept	4
4.3. Virtual Service (VIP) Requirements	4
4.4. Deployment Mode	5
5. Loadbalancer.org Appliance – the Basics	5
5.1. Virtual Appliance	5
5.2. Initial Network Configuration	5
5.3. Accessing the Appliance WebUI	6
5.3.1. Main Menu Options	7
5.4. Appliance Software Update	8
5.4.1. Online Update	8
5.4.2. Offline Update	8
5.5. Ports Used by the Appliance	9
5.6. HA Clustered Pair Configuration	10
6. Appliance & iConnect Enterprise Archive Configuration	10
6.1. Appliance Configuration	10
6.1.1. Network Configuration	10
6.1.2. Floating IP Configuration (For The Cluster's Default Gateway)	10
6.1.3. Configuring VIP1 – All VNA Services	11
6.2. iConnect Enterprise Archive Server Configuration	13
7. Testing & Verification	13
7.1. Automatic Failover	13
7.2. Manual Failover	13
7.3. Client Connection Tests	14
8. Technical Support	14
9. Additional Documentation	14
10. Appendix	15
10.1. Configuring HA - Adding a Secondary Appliance	15
10.1.1. Non-Replicated Settings	15
10.1.2. Configuring the HA Clustered Pair	16
11. Document Revision History	18

1. About this Guide

This guide details the steps required to configure a highly available Merative iConnect Enterprise Archive environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any iConnect Enterprise Archive configuration changes that are required.

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 Merative iConnect Enterprise Archive. 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. Merative iConnect Enterprise Archive

- All versions

4. Load Balancing iConnect Enterprise Archive

For high availability, Merative recommend that a load balancer is used to enable rapid failover to the secondary iConnect Enterprise Cluster should the Primary Cluster become unavailable.

4.1. Port Requirements

The following table shows the ports used by iConnect Enterprise Archive. The load balancer must be configured to listen on the same ports.

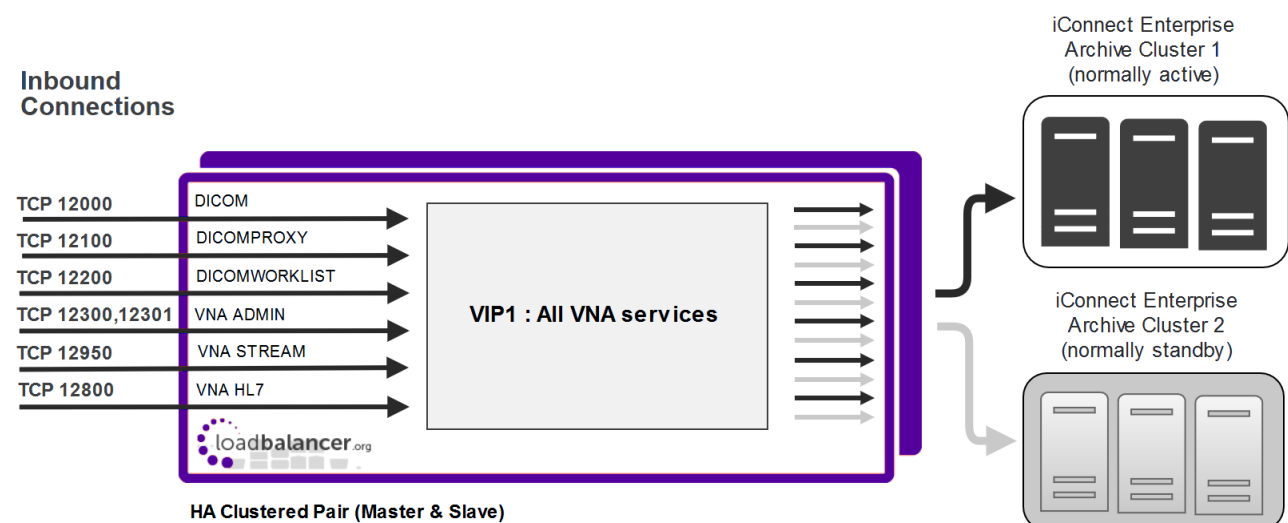
Port	Protocols	Use
12000	TCP	DICOM
12100	TCP	DICOM Proxy



Port	Protocols	Use
12200	TCP	DICOM Work List
12300 & 12301	TCP	VNA Admin
12950	TCP	VNA Stream
12800	TCP	VNA HL7

4.2. Deployment Concept

When iConnect Enterprise Archive is deployed with the load balancer, clients connect to the Virtual Service (VIP) on the load balancer rather than connecting directly to one of the iConnect Enterprise Archive Clusters. Under normal conditions, these connections are then forwarded to the Primary Cluster.



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.

Should the Primary Cluster become unavailable, failover to the Secondary Cluster can be handled in either of the following ways:

- **Automatically** – In this case, health checks are configured at 30 second intervals. Should there be 10 consecutive health check failures, failover to the Secondary Cluster occurs.
- **Manually** – In this case, failover to the Secondary Cluster must be triggered manually using the 'Halt' feature in the load balancer's WebUI. Please refer to [Manual Failover](#) for more details.

Note

The way the Virtual Service's health check is configured determines which of these failover methods is used.

4.3. Virtual Service (VIP) Requirements

A single multi-port VIP is used that listens on all required ports. The VIP is configured as follows:



- Deployment mode: Layer 4 NAT (Network Address Translation) mode
- Listens on a total of 7 ports as described on the table and diagram in [Port Requirements](#)
- The health-check configuration depends on whether automatic or manual failover is required:
 - for **automatic** failover an external script is used, the script checks that **all** 7 ports are available and runs every 30 seconds, if connection to one or more of the ports fails, the health check is deemed to have failed, if there are 10 consecutive health check failures, cluster failover occurs
 - for **manual** failover the health check is set to: **No checks, always On**
- The associated Real Server is configured to be the cluster IP address of the Primary Cluster
- The fallback server is configured to be the cluster IP address of the Secondary Cluster

4.4. Deployment Mode

As mentioned above, the VIP is configured using Layer 4 NAT mode. With this mode, return traffic must pass via the load balancer. To achieve this, the default gateway of each cluster must be set to be the load balancer. For a clustered pair (our recommended configuration), an additional floating IP address must be used for this purpose. This allows the same IP address to be brought up on the Secondary appliance should an appliance failover occur.

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](#).

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.

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 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.



5.3. Accessing the Appliance WebUI

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

Note

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

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

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

Note

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

Note

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

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

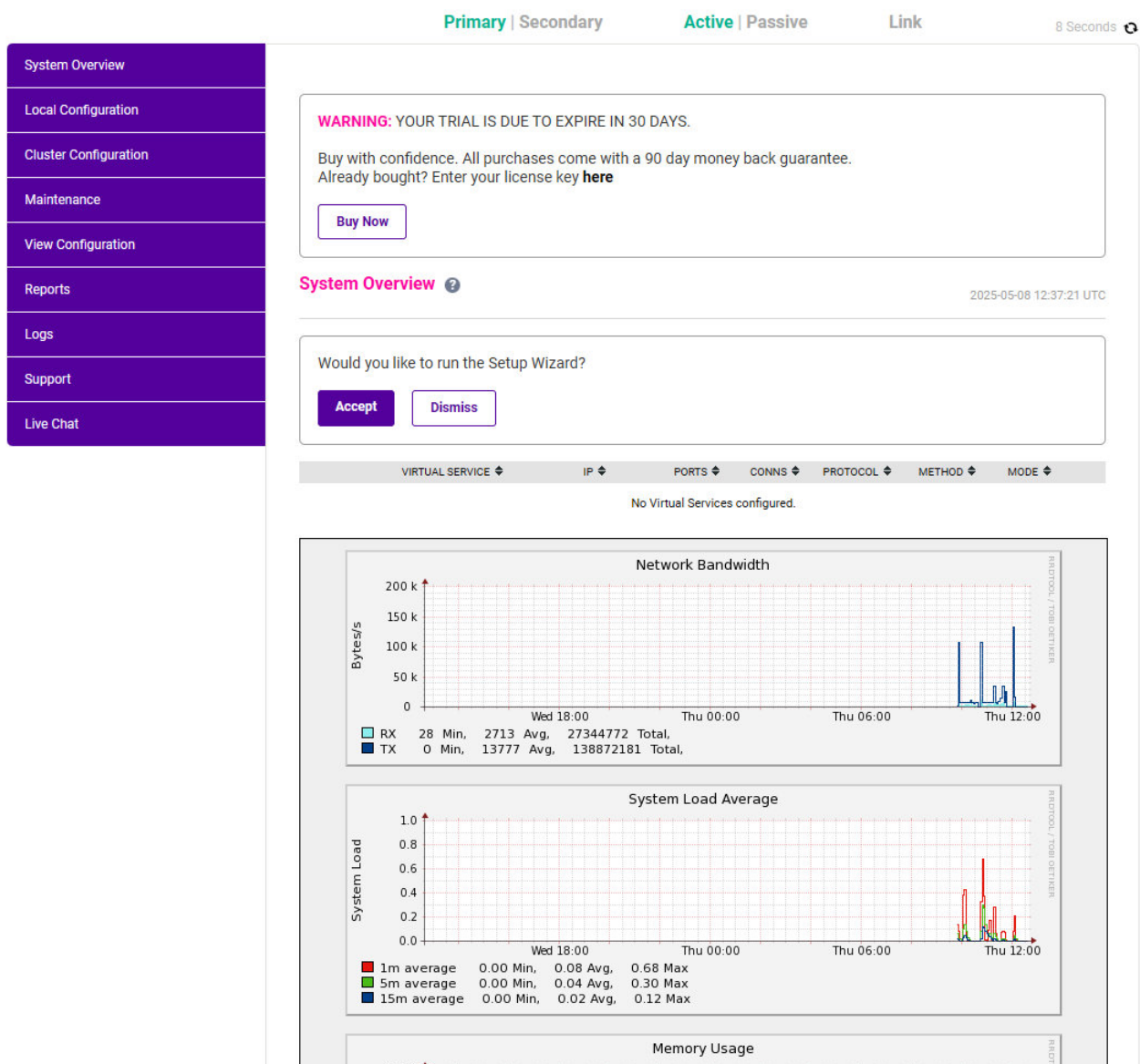
Username: loadbalancer

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

Note

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

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



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.

5.3.1. 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 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

5.4. 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.

5.4.1. 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.

5.4.2. 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.

5.5. 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
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](#)



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 Enterprise Archive Configuration

6.1. Appliance Configuration


6.1.1. Network Configuration


Layer 4 NAT mode 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 [Layer 4 NAT Mode](#).


To configure an additional network interface for a 2-arm configuration:


1. Using the WebUI, navigate to *Local Configuration > Network Interface Configuration*.
2. Scroll to the *IP Address Assignment* section.

IP Address Assignment


eth0
 1 GB/s


eth1
 1 GB/s


eth2


eth3

eth0

192.168.100.1/24

eth1

192.168.200.1/24

MTU bytes

MTU bytes

3. Specify an appropriate IP address for **eth1** in CIDR format as shown above.
4. Click **Configure Interfaces**.

Note

There are no restrictions on which interface is used for each requirement.

6.1.2. Floating IP Configuration (For The Cluster's Default Gateway)

As mentioned in [Deployment Mode](#), when using Layer 4 NAT mode and a clustered pair of load balancers, a floating IP address must be configured on the load balancer for use as the iConnect Enterprise Archive server's default gateway.

1. Using the WebUI, navigate to: *Cluster Configuration > Floating IP's*.

New Floating IP

192.168.100.254




Add Floating IP

2. Enter the IP address you'd like to use as the default gateway. e.g. **192.168.100.254**.
3. Click **Add Floating IP**.

6.1.3. Configuring VIP1 – All VNA Services

a) Configure the External Health Check Script (used for automatic failover)

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

Health Check Details		
Name:	<input type="text" value="Merative-iConnect-EntArchiv"/>	
Type:	<input type="text" value="Virtual Service"/>	
Template:	<input type="text" value="IBM-WHI-iConnect-Enterprise-Archive"/>	

2. Specify an appropriate **Name** for the health check, e.g. **Merative-iConnect-EntArchive**.
3. Set **Type** to **Virtual Service**.
4. Set **Template** to **IBM-WHI-iConnect-Enterprise-Archive**.
5. Click **Update**.

b) 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:

Label	VNA	?
Virtual Service		
IP Address	192.168.200.100	?
Ports	12000,12100,12200,12300,1	?
Protocol		
Protocol	TCP	?
Forwarding		
Forwarding Method	NAT	?
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>

3. Enter an appropriate label (name) for the VIP, e.g. **VNA**.
4. Set the *Virtual Service IP* address field to the required IP address, e.g. **192.168.200.100**.
5. Set the *Virtual Service Ports* field to **12000,12100,12200,12300,12301,12950,12800**.
6. Leave *Protocol* set to **TCP**.
7. Set the *Forwarding Method* to **NAT**.
8. Click **Update**.
9. Now click **Modify** next to the newly created VIP.
10. Scroll to the *Health Checks* section.

For **automatic** failover:

- a. Set *Check Type* to **External Script**.
- b. Set *External Script* to **Merative-iConnect-EntArchive**.

For **manual** failover:

- a. Set the *Check Type* to **No checks, Always On**.

11. Scroll to the *Fallback Server* section.
 - a. Set the *IP Address* field to the IP address of the Secondary iConnect Enterprise Archive Cluster.
 - b. Set the *Port* to **0** (numerical zero) , this ensures that the fallback server (i.e. the Secondary Cluster) can receive connections on all required ports.
 - c. Enable (check) the *MASQ Fallback* checkbox.
12. Click **Update**.

c) Setting up the Real Server (RIP)



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

Label	<input type="text" value="PrimaryCluster"/>	?
Real Server IP Address	<input type="text" value="192.168.100.110"/>	?
Real Server Port	<input type="text"/>	?
Weight	<input type="text" value="100"/>	?
Minimum Connections	<input type="text" value="0"/>	?
Maximum Connections	<input type="text" value="0"/>	?

3. Enter an appropriate label (name) for the RIP, e.g. **PrimaryCluster**.
4. Set the *Real Server IP Address* field to the IP address of the Primary iConnect Enterprise Archive Cluster.
5. Leave the *Real Server Port* field blank.
6. Click **Update**.

6.2. iConnect Enterprise Archive Server Configuration

As mentioned in [Deployment Mode](#), when using Layer 4 NAT mode and a clustered pair of load balancers, a floating IP address must be configured for use as the default gateway. Set the default gateway of each iConnect Enterprise Archive to be this IP address.

7. Testing & Verification

Note

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

Under normal circumstances the Primary Cluster handles all connections. Failover to the Secondary Cluster is handled automatically or manually depending on how the VIP is configured (see [Virtual Service \(VIP\) Requirements](#)).



7.1. Automatic Failover

Automatic failover occurs after 5 minutes. To trigger a failover, the Primary Cluster must be continuously unavailable for this time.


7.2. Manual Failover





To trigger a failover to the Secondary Cluster, the 'Halt' option in the System Overview is used:





	REAL SERVER	IP	PORTS	WEIGHT	CONNS		
	PrimaryCluster	192.168.100.110	5.12000,12..	100	0	Drain	Halt 

Once Halted, the VIP & RIP will be shown colored blue, connections will then be forwarded to the fallback server, i.e the Secondary Cluster:

System Overview  2019-05-29 14:42:14 UTC

	VIRTUAL SERVICE	IP	PORTS	CONNS	PROTOCOL	METHOD	MODE	
	VNA	192.168.200.100	5.12000,1..	0	TCP	Layer 4	NAT	
	REAL SERVER	IP	PORTS	WEIGHT	CONNS			
	PrimaryCluster	192.168.100.110	5.12000,12..	halt	0	Online (halt)		

To return to the Primary Cluster, the 'Online' option is used:

	REAL SERVER	IP	PORTS	WEIGHT	CONNS		
	PrimaryCluster	192.168.100.110	5.12000,12..	halt	0	Online (halt)	

7.3. Client Connection Tests

Ensure that clients can connect via the load balancer to the iConnect Enterprise Archive Cluster / MergePACS cluster. You'll probably need to create new DNS records or modify your existing DNS records, replacing the IP addresses of individual servers or the cluster with the IP address of the 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 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.

10.1.1. 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
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

⚠ Important

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


10.1.2. 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

 **LOADBALANCER**

Local IP address

192.168.110.40

IP address of new peer

192.168.110.41


Password for *loadbalancer* user on peer

••••••••••

Add new node

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


Create a Clustered Pair

 **LOADBALANCER**

Primary

IP: 192.168.110.40

Attempting to pair..

 **LOADBALANCER**

Secondary

IP: 192.168.110.41

Local IP address

192.168.110.40

IP address of new peer

192.168.110.41

Password for *loadbalancer* user on peer


••••••••••


configuring

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




High Availability Configuration - primary


 **LOADBALANCER**



Primary

IP: 192.168.110.40

 **LOADBALANCER**



Secondary

IP: 192.168.110.41

Break Clustered Pair

- 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

Version	Date	Change	Reason for Change	Changed By
1.1.0	2 August 2019	Styling and layout	General styling updates	RJC
1.1.1	20 August 2020	New title page Updated Canadian contact details	Branding update Change to Canadian contact details	AH
1.2.0	1 October 2021	Converted the document to AsciiDoc	Move to new documentation system	AH, RJC, ZAC
1.2.1	11 May 2022	Updated external health check related content to reflect latest software version	New software release	RJC
1.3.0	6 September 2022	Renamed document and amended references to the product	Product acquisition	AH
1.3.1	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	Housekeeping across all documentation	AH
1.3.2	2 February 2023	Updated screenshots	Branding update	AH
1.3.3	7 March 2023	Removed conclusion section	Updates across all documentation	AH
1.4.0	24 March 2023	New document theme Modified diagram colours	Branding update	AH
1.4.1	14 August 2025	Removed references to IBM Watson Health	Merative is a separate standalone company	RJC



Visit us: www.loadbalancer.org

Phone us: +44 (0)330 380 1064

Phone us: +1 833 274 2566

Email us: info@loadbalancer.org

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

About Loadbalancer.org

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

