# Table of Contents

1. About this Guide ................................................................. 3
2. Loadbalancer.org Appliances Supported ........................................ 3
3. Loadbalancer.org Software Versions Supported ............................... 3
4. IBM Watson Health iConnect Enterprise Archive Software Versions Supported ......................................................... 3
5. Load Balancing iConnect Enterprise Archive ................................. 3
   Port Requirements ........................................................................ 3
   Deployment Concept ....................................................................... 3
   Virtual Service (VIP) Requirements ............................................. 4
   Deployment Mode ......................................................................... 4
6. Loadbalancer.org Appliance – the Basics ....................................... 5
   Virtual Appliance ......................................................................... 5
   Initial Network Configuration ...................................................... 5
   Accessing the WebUI ..................................................................... 5
   Main Menu Options ...................................................................... 7
   HA Clustered Pair Configuration .................................................. 7
7. Appliance & iConnect Enterprise Archive Configuration .................. 7
   Appliance Configuration ............................................................. 7
   Network Configuration ............................................................... 7
   Floating IP Configuration (For The Clusters Default Gateway) ......... 8
   Configuring VIP1 – All VNA Services ......................................... 8
   iConnect Enterprise Archive Server Configuration ....................... 10
8. Testing & Verification .................................................................. 10
   Automatic Failover ...................................................................... 11
   Manual Failover ......................................................................... 11
   Client Connection Tests ............................................................. 11
9. Technical Support ....................................................................... 11
10. Additional Documentation ......................................................... 11
11. Conclusion .............................................................................. 11
12. Appendix ............................................................................... 12
   Configuring HA - Adding a Secondary Appliance ......................... 12
13. Document Revision History ....................................................... 15
1. About this Guide

This guide details the steps required to configure a highly available IBM Watson Health 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 IBM Watson Health iConnect Enterprise Archive. 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. Loadbalancer.org Software Versions Supported

- V8.3.8 & later

4. IBM Watson Health iConnect Enterprise Archive Software Versions Supported

- IBM Watson Health iConnect Enterprise Archive – all versions

5. Load Balancing iConnect Enterprise Archive

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

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.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>12000</td>
<td>TCP</td>
<td>DICOM</td>
</tr>
<tr>
<td>12100</td>
<td>TCP</td>
<td>DICOM Proxy</td>
</tr>
<tr>
<td>12200</td>
<td>TCP</td>
<td>DICOM Work List</td>
</tr>
<tr>
<td>12300 &amp; 12301</td>
<td>TCP</td>
<td>VNA Admin</td>
</tr>
<tr>
<td>12950</td>
<td>TCP</td>
<td>VNA Stream</td>
</tr>
<tr>
<td>12800</td>
<td>TCP</td>
<td>VNA HL7</td>
</tr>
</tbody>
</table>

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.
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.

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

### 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

### 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.

6. Loadbalancer.org Appliance – the Basics

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 The Virtual Appliance - Hypervisor Deployment and the ReadMe.txt text file included in the VA download for more detailed information on deploying the VA using various Hypervisors.

Note: For the VA, 4 NICs are included but only eth0 is connected by default at power up. If the other NICs are required, these should be connected using the network configuration screen within the Hypervisor.

Initial Network Configuration
After boot up, follow the instructions on the console to configure the IP address, subnet mask, default gateway, DNS and other network settings.

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

Accessing the WebUI
The WebUI is accessed using a web browser. By default, user authentication is based on local Apache .htaccess files. User administration tasks such as adding users and changing passwords can be performed using the WebUI menu option: Maintenance >Passwords.

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

Note: If required, users can also be authenticated against LDAP, LDAPS, Active Directory or Radius. For more information please refer to External Authentication.

1. Using a browser, access the WebUI using the following URL:

2. Log in to the WebUI:

**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:

![WebUI screenshot](image)

**Note**  
The WebUI for the VA is shown, the hardware and cloud appliances are very similar. The yellow licensing related message is platform & model dependent.
3. You'll be asked if you want to run the Setup Wizard. If you click **Accept** the Layer 7 Virtual Service configuration wizard will start. If you want to configure the appliance manually, simply click **Dismiss**.

**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

**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](#).

7. **Appliance & iConnect Enterprise Archive Configuration**

**Appliance Configuration**

**Network Configuration**

When using Layer 4 NAT mode, two Interfaces are required, this can be achieved by using two network adapters, or by creating VLANs on a single adapter. The following configuration uses 2 separate network adapters, one for each subnet.

To configure network settings using eth0 & eth1:

1. Using the WebUI, navigate to: **Local Configuration > Network Interface Configuration**.

   ![IP Address Assignment](image)

   - eth0: 192.168.100.1/24
   - eth1: 192.168.200.1/24

   MTU: 1500 bytes

2. Enter an IP address/mask in the subnet where the iConnect Enterprise Archive Servers are located, e.g. 192.168.100.1/24.
3. Enter an IP address/mask in the subnet where the VIP & clients are located, e.g. **192.168.200.1/24**.

4. Click **Configure Interfaces**.

**Note**

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

**Floating IP Configuration (For The Clusters 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](image)

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**.

**Configuring VIP1 – All VNA Services**

**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](image)

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. Configure health check settings:

For automatic failover:

- Create the following file: `/var/lib/loadbalancer.org/check/IBM-WHI-iConnect-Enterprise-Archive`.
- Set file permissions to 755.
- Edit the file and copy / paste the following script:

```
#!/bin/bash

########################################################
# #
# IBM Watson Health Imaging - iConnect Enterprise Archive #
# (c) Loadbalancer.org 2019 #
# #
# 2019-07-31 - Initial write - Aaron West <support@loadbalancer.org> #
# #
########################################################

## Variables
# Space separated port list to check using a TCP half open check (SYN Scan)
HALF_OPEN_RPT="12800"
# Space separated port list to check using a full 3 way handshake (Connect to port)
FULL_3WAY_RPT="12000 12100 12200 12300 12301 12950"
# $3 represents the real server address as passed by the load balancer
RIP="$3"
# Timeout for checking each port
TIMEOUT="3"
## Shouldn't need to edit below here
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
for i in \${HALF_OPEN_RPT}; do
    timeout ${TIMEOUT} nmap -sS -p \${i} \${RIP} 2>&1 | grep -q 'open'
    ec=$?
    if [ $ec -ne "0" ]; then
        exit $ec
    fi
done
for i in \${FULL_3WAY_RPT}; do
    nc -w ${TIMEOUT} -zvN \${RIP} $i &>/dev/null
    ec=$?
    if [ $ec -ne "0" ]; then
        exit $ec
    fi
done
```
- Save the file.
- In the Health Checks section set the Check Type to External Script.
- Set the External Script drop-down to IBM-WHI-iConnect-Enterprise-Archive (the script just created).
- Click Update.

For manual failover:

- Set the Check Type to No checks, Always On.
11. Set the **Fallback Server IP Address** field to the IP address of the Secondary iConnect Enterprise Archive Cluster.

12. Set the **Fallback Server Port** field to 0 (numerical zero), this ensures that the fallback server (i.e. the Secondary Cluster) can receive connections on all required ports.

13. Enable (check) the **MASQ Fallback** checkbox.

14. Click **Update**.

b) 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 VNA VIP.

2. Enter the following details:

   ![Real Server Configuration Form](image)

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**.

**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.

8. Testing & Verification

   **Note** For additional general guidance please also refer to Testing Load Balanced Services.

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 (seeVirtual Service (VIP) Requirements).
Automatic Failover
Automatic failover occurs after 5 minutes. To trigger a failover, the Primary Cluster must be continuously unavailable for this time.

Manual Failover
To trigger a failover to the Secondary Cluster, the ‘Halt’ option in the System Overview is used:

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

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

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.

9. 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.

10. Additional Documentation

11. Conclusion
Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced IBM Watson Health iConnect Enterprise Archive environments.
12. Appendix

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 should be configured first, 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.

Note

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>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 Configuration</td>
<td>Various settings including Internet Proxy, Management Gateway, Firewall connection tracking table size, NIC offloading, SMTP relay, logging and 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>

To add a Secondary node - i.e. create a highly available 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.

3. Specify the IP address and the loadbalancer user’s password for the Secondary (peer) appliance as shown 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 blue 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](#).
## 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>1.1.0</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>20 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>
</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.