# 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 connect Enterprise Archive & MergePACS Software Versions Supported .................................................. 3
5. Load Balancing connect Enterprise Archive & MergePACS ........................................ 3
   Port Requirements ......................................................................................................... 3
   Deployment Concept ..................................................................................................... 4
   Virtual Service (VIP) Requirements ............................................................................ 5
   Deployment Mode ......................................................................................................... 6
6. Loadbalancer.org Appliance – the Basics .................................................................. 6
   Virtual Appliance .......................................................................................................... 6
   Initial Network Configuration ..................................................................................... 6
   Accessing the WebUI ..................................................................................................... 6
      Main Menu Options ................................................................................................. 8
   HA Clustered Pair Configuration ................................................................................. 9
7. Appliance, connect Enterprise Archive & MergePACS Configuration ......................... 9
   Appliance Configuration .............................................................................................. 9
      Network Configuration ............................................................................................. 9
      Floating IP Configuration (For the connect Enterprise Archive’s Default Gateway) ........................................................................... 9
      Configuring VIP1 – All VNA Services .................................................................... 10
      Configuring VIP2 – All PACS Services .................................................................. 12
   iConnect Enterprise Archive Server Configuration ................................................... 14
   MergePACS Server Configuration .............................................................................. 14
8. Testing & Verification ................................................................................................. 19
   Automatic Failover .................................................................................................... 19
   Manual Failover .......................................................................................................... 19
   Client Connection Tests ............................................................................................ 20
9. Technical Support ........................................................................................................ 20
10. Additional Documentation ......................................................................................... 20
11. Conclusion .................................................................................................................. 20
12. Appendix .................................................................................................................... 21
    Configuring HA - Adding a Secondary Appliance ...................................................... 21
    Non-Replicated Settings ............................................................................................. 21
13. Document Revision History ...................................................................................... 24
1. About this Guide
This guide details the steps required to configure a highly available IBM Watson Heath iConnect Enterprise Archive & MergePACS environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any iConnect Enterprise Archive & MergePACS 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 for load balancing IBM Watson Health iConnect Enterprise Archive & MergePACS. 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 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.

4. IBM Watson Health iConnect Enterprise Archive & MergePACS Software Versions Supported
   - IBM Watson Health iConnect Enterprise Archive – all versions
   - IBM Watson Health MergePACS – all versions

5. Load Balancing iConnect Enterprise Archive & MergePACS
For high availability, IBM Watson Health recommend that a load balancer is used to enable rapid failover to the secondary iConnect Enterprise Cluster / MergePACS 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>System</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>12000</td>
<td>TCP</td>
<td>VNA</td>
<td>DICOM</td>
</tr>
<tr>
<td>12100</td>
<td>TCP</td>
<td>VNA</td>
<td>DICOM Proxy</td>
</tr>
<tr>
<td>12200</td>
<td>TCP</td>
<td>VNA</td>
<td>DICOM Work List</td>
</tr>
<tr>
<td>12300 &amp; 12301</td>
<td>TCP</td>
<td>VNA</td>
<td>VNA Admin</td>
</tr>
<tr>
<td>12950</td>
<td>TCP</td>
<td>VNA</td>
<td>VNA Stream</td>
</tr>
<tr>
<td>12800</td>
<td>TCP</td>
<td>VNA</td>
<td>VNA HL7</td>
</tr>
<tr>
<td>Port</td>
<td>Protocols</td>
<td>System</td>
<td>Use</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
<td>----------</td>
<td>--------------</td>
</tr>
<tr>
<td>104</td>
<td>TCP</td>
<td>PACS</td>
<td>DICOM</td>
</tr>
<tr>
<td>80,8080,443,8443</td>
<td>TCP</td>
<td>PACS</td>
<td>HTTP &amp; HTTPS</td>
</tr>
<tr>
<td>5222</td>
<td>TCP</td>
<td>PACS</td>
<td>Instant Messenger</td>
</tr>
<tr>
<td>1001</td>
<td>TCP</td>
<td>PACS</td>
<td>PACS HL7</td>
</tr>
</tbody>
</table>

**Deployment Concept**

**Connect Enterprise Archive**

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.

**MergePACS**

When MergePACS 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 MergePACS Clusters. Under normal conditions, these connections are then forwarded to the Primary Cluster.
Note | VIP1 (VNA) and VIP2 (PACS) are configured on a single clustered pair of load balancers.

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.

**Virtual Service (VIP) Requirements**

To provide load balancing and HA for iConnect Enterprise Archive & MergePACS, 2 VIPs are required as depicted in the diagrams above, 1 multiport VIP for iConnect Enterprise Archive and 1 multiport VIP for MergePACS:

**iConnect Enterprise Archive**

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

**MergePACS**

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

- Deployment mode: Layer 4 DR (Direct Return) 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

iConnect Enterprise Archive

As mentioned above, the VIP for iConnect Enterprise Archive 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.

MergePACS

As mentioned above, the VIP for MergePACS is configured using Layer 4 DR (Direct Return) mode. This mode offers the best possible performance since replies go directly from the MergePACS Cluster to the client, and not via the load balancer. To use this mode, the "ARP Problem" must be solved on each MergePACS server as explained in iConnect Enterprise Archive Server Configuration.

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 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.

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.

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:
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, simple 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 & MergePACS Configuration

Appliance Configuration

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](image)

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.

Floating IP Configuration (For The iConnect Enterprise Archive’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.

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) 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.

<table>
<thead>
<tr>
<th>Health Check Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: IBM-WHI-iConnect-Enterprise-Archive</td>
</tr>
<tr>
<td>Type: Virtual Service</td>
</tr>
<tr>
<td>Template: IBM-WHI-iConnect-Enterprise-Archive</td>
</tr>
</tbody>
</table>

2. Specify an appropriate Name for the health check, e.g. IBM-WHI-iConnect-Enterprise-Archive.

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:
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 **IBM-WHI-iConnect-Enterprise-Archive**.

    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:

<table>
<thead>
<tr>
<th>Label</th>
<th>PrimaryCluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.100.110</td>
</tr>
<tr>
<td>Real Server Port</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
<tr>
<td>Minimum Connections</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Connections</td>
<td>0</td>
</tr>
</tbody>
</table>

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**.

**Configuring VIP2 – All PACS 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**.

   - **Name**: IBM-WHI-MergePACS
   - **Type**: Virtual Service
   - **Template**: IBM-WHI-MergePACS

2. Specify an appropriate *Name* for the health check, e.g. **IBM-WHI-MergePACS**.

3. Set *Type* to Virtual Service.

4. Set *Template* to IBM-WHI-MergePACS.

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:
3. Enter an appropriate label (name) for the VIP, e.g. **PACS**.

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 **104,80,8080,443,8443,5222,1001**.

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 to the **Health Checks** section.

    **For automatic failover:**

    a. Set **Check Type** to **External Script**.
    
    b. Set **External Script** to **IBM-WHI-MergePACS**.

    **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** to the IP address of the Secondary MergePACS 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.

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

13. Click **Update**.

c) 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 VIP.
2. Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>PrimaryCluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.100.110</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
<tr>
<td>Minimum Connections</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Connections</td>
<td>0</td>
</tr>
</tbody>
</table>

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 MergePACS Cluster.

5. 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.

### MergePACS Server Configuration

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

**Note**

The following steps must be performed on all MergePACS Servers.

### Windows Server 2012 & Later

Windows Server 2012 and later support Direct Routing (DR) mode through the use of the Microsoft Loopback Adapter. The IP address allocated to the Loopback Adapter must be the same as the Virtual Service (VIP) address. If the Real Server is included in multiple DR mode VIPs, additional IP addresses can be added to the Loopback Adapter that correspond to each VIP. In addition, steps must be taken to set the strong/weak host behavior which is used to either block or allow interfaces to receive packets destined for a different interface on the same server.

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

1. Click **Start**, then run **hdwwiz** to start the Hardware Installation Wizard.

2. When 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**.
4. Uncheck all items except **Internet Protocol Version 4 (TCP/IPv4)** and **Internet Protocol Version 6 (TCP/IPv6)** as shown below:
Note | Leaving both checked ensures that both IPv4 and IPv6 are supported. Select one if preferred.

5. If configuring IPv4 addresses select Internet Protocol Version (TCP/IPv4), click Properties and configure the IP address to be the same as the Virtual Service (VIP) with a subnet mask of 255.255.255.255, e.g. 192.168.2.20/255.255.255.255 as shown below:

6. If configuring IPv6 addresses select Internet Protocol Version (TCP/IPv6), 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:
7. Click **OK** on TCP/IP Properties, then click **Close** on Ethernet Properties to save and apply the new settings.

**Note**

For Windows 2012/2016/2019, it’s not necessary to modify the interface metric on the advanced tab and should be left set to Automatic.

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

To configure the correct strong/weak host behavior for Windows 2012/2016/2019, the following commands must be run on each Real Server:

For IPv4 addresses:

```bash
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:

```bash
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
```

For these commands to work, the LAN connection NIC must be named "net" and the loopback NIC must be named "loopback" as shown below. If you prefer to leave your current NIC names, then the commands above must be modified accordingly. For example, if your network adapters are named "LAN" and "LOOPBACK", the commands required would be:

```bash
netsh interface ipv4 set interface "LAN" weakhostreceive=enabled
netsh interface ipv4 set interface "LOOPBACK" weakhostreceive=enabled
netsh interface ipv4 set interface "LOOPBACK" weakhostsend=enabled
```
For these commands to work, the LAN connection NIC must be named "net" and the loopback NIC must be named "loopback" as shown below. If you prefer to leave your current NIC names, then the commands above must be modified accordingly. For example, if your network adapters are named "LAN" and "LOOPBACK", the commands required would be:

```
netsh interface ipv6 set interface "LAN" 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
```

Note: The names for the NICs are case sensitive, so make sure that the name used for the interface and the name used in the commands match exactly.

- Start PowerShell or use a command window to run the appropriate netsh commands as shown in the example below:

```
netsh interface ipv6 set interface "LAN" 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
```

Note: This shows an IPv6 example, use the IPv4 commands if you’re using IPv4 addresses.

Repeat steps 1 - 3 on all remaining Windows 2012/2016/2019 Real Server(s).

If preferred you can also use the following PowerShell Cmdlets:

The following example configures both IPv4 and IPv6 at the same time:

```
Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled -DadTransmits 0
```

```
Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled
```

To configure just IPv4:

```
Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled
```
To configure just IPv4:

```
Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled -AddressFamily IPv4
```

To configure just IPv6:

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

```
Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled -AddressFamily IPv6
```

8. 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 [Deployment Mode](#)).

**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:

(Screen shots for the VNA VIP are shown, the same concept applies to the PACS VIP)

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 & MergePACS 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.

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>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>

Important

Make sure that if these settings/updates have been configured on the Primary appliance, they’re also configured on the Secondary appliance.

To add a Secondary node - i.e. create a highly available clustered pair:
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 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:
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*.

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>1.1.0</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>1.2.1</td>
<td>11 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>
</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.