1. About this Guide
This guide details the steps required to configure a load balanced McKesson Radiology and McKesson Cardiology environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any McKesson Radiology and McKesson Cardiology 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 relevant Administration Manual:

- v7 Administration Manual
- v8 Administration Manual

2. Loadbalancer.org Appliances Supported
All our products can be used for load balancing McKesson Radiology and McKesson Cardiology. The complete list of models is shown below:

<table>
<thead>
<tr>
<th>Discontinued Models</th>
<th>Current Models *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise R16</td>
<td>Enterprise R20</td>
</tr>
<tr>
<td>Enterprise VA R16</td>
<td>Enterprise MAX</td>
</tr>
<tr>
<td>Enterprise VA</td>
<td>Enterprise 10G</td>
</tr>
<tr>
<td>Enterprise R320</td>
<td>Enterprise 40G</td>
</tr>
<tr>
<td></td>
<td>Enterprise Ultra</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA R20</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA MAX</td>
</tr>
<tr>
<td></td>
<td>Enterprise AWS **</td>
</tr>
<tr>
<td></td>
<td>Enterprise AZURE **</td>
</tr>
<tr>
<td></td>
<td>Enterprise GCP **</td>
</tr>
</tbody>
</table>

* For full specifications of these models please refer to: [http://www.loadbalancer.org/products/hardware](http://www.loadbalancer.org/products/hardware)
** Some features may not be supported, please check with Loadbalancer.org support

3. Loadbalancer.org Software Versions Supported

- V76.4 and later

4. McKesson Radiology and McKesson Cardiology Software Versions Supported

- McKesson Radiology, McKesson Radiology Manager, McKesson Clinical Reference Viewer, and McKesson Cardiology – all versions
5. McKesson Radiology and McKesson Cardiology

Change Healthcare's suite of radiology and cardiology applications provide a comprehensive set of tools for medical imaging. The whole workflow is covered, from working with modalities and importing images to image viewing and reporting.

McKesson Radiology and McKesson Radiology Manager are a PACS solution based on well known standards such as DICOM. Features include 3D visualisations and tools, analytics and metrics tools, and a flexible deployment model.

McKesson Clinical Reference Viewer is a browser based image viewing application, giving clinicians easy access to medical imaging data through an intuitive interface.

McKesson Cardiology is an application that helps with managing cardiology imaging, data management, reporting, and more.

6. Load Balancing McKesson Radiology and McKesson Cardiology

**Note:** It's highly recommended that you have a working McKesson Radiology and McKesson Cardiology environment first before implementing the load balancer.

**Persistence (aka Server Affinity)**

The virtual service for McKesson Radiology web traffic does not require session affinity at the load balancing layer.

All other virtual services require session affinity, aka persistence. When using the default layer 4 DR deployment mode described in this guide, source IP address persistence is used and different persistence timeout settings are used across the different virtual services. The specific settings are detailed in the ‘Appliance Configuration’ sections 11 and 12.

**Virtual Service (VIP) Requirements**

To provide load balancing and HA for McKesson Radiology and McKesson Cardiology, the following VIPs are required:

- McKesson Radiology (DICOM Traffic)
- McKesson Radiology (Web Traffic)
- McKesson Radiology Manager
- McKesson Clinical Reference Viewer
- McKesson Cardiology

**Port Requirements**

The following table shows the ports that are load balanced:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP/HTTP</td>
<td>Web application traffic for all McKesson products</td>
</tr>
<tr>
<td>Port</td>
<td>Protocol</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>443</td>
<td>TCP/HTTPS</td>
<td>Encrypted web application traffic for all McKesson products</td>
</tr>
<tr>
<td>4000</td>
<td>TCP/DICOM</td>
<td>DICOM import traffic</td>
</tr>
<tr>
<td>5000</td>
<td>TCP/DICOM</td>
<td>DICOM query traffic</td>
</tr>
</tbody>
</table>

**Health Checks**

Standard, built-in health checks are used for all virtual services, with one exception.

If using McKesson Radiology Web Server version 12.0, it is possible to use the same health check that is used for version 12.1, which is a built-in Negotiate check.

McKesson officially advise to perform an additional two health checks on version 12.0 Radiology Web Servers in order for them to be considered to be functioning fully. This is possible to achieve using an external health check script. For assistance in implementing this, please contact solutions@loadbalancer.org.

**7. Deployment Concept**

VIPs = Virtual IP Addresses

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 section 2 in the appendix on page 37 for more details on configuring a clustered pair.

**8. Load Balancer Deployment Methods**

The load balancer can be deployed in 4 fundamental ways: Layer 4 DR mode, Layer 4 NAT mode, Layer 4 SNAT mode and Layer 7 SNAT mode.

For McKesson Radiology and McKesson Cardiology, using layer 4 DR mode is recommended. It is also possible to use a combination of layer 4 NAT mode and layer 7 SNAT mode, however the performance of this set up is not as great as layer 4 DR mode. These modes are described below and are used for the configurations presented in this guide. For configuring using DR mode please refer to the section starting on page 14, and for configuring using a combination of layer 4 NAT mode and layer 7 SNAT mode refer to the section starting on page 22.
Layer 4 DR Mode

One-arm direct routing (DR) mode is a very high performance solution that requires little change to your existing infrastructure.

Note: Kemp, Brocade, Barracuda & A10 Networks call this Direct Server Return and F5 call it N-Path.

- DR mode works by changing the destination MAC address of the incoming packet to match the selected Real Server on the fly which is very fast.
- When the packet reaches the Real Server it expects the Real Server to own the Virtual Services IP address (VIP). This means that you need to ensure that the Real Server (and the load balanced application) respond to both the Real Servers own IP address and the VIP.
- The Real Server should not respond to ARP requests for the VIP. Only the load balancer should do this. Configuring the Real Servers in this way is referred to as Solving the ARP Problem. Please refer to page 32 for more information.
- On average, DR mode is 8 times quicker than NAT for HTTP, 50 times quicker for Terminal Services and much, much faster for streaming media or FTP.
- The load balancer must have an Interface in the same subnet as the Real Servers to ensure layer 2 connectivity required for DR mode to work.
- The VIP can be brought up on the same subnet as the Real Servers, or on a different subnet provided that the load balancer has an interface in that subnet.
- Port translation is not possible in DR mode i.e. having a different RIP port than the VIP port.
- DR mode is transparent, i.e. the Real Server will see the source IP address of the client.

Layer 4 NAT Mode

Layer 4 NAT mode is also a high performance solution, although not as fast as layer 4 DR mode. This is because real
server responses must flow back to the client via the load balancer rather than directly as with DR mode.

- The load balancer translates all requests from the external Virtual Service to the internal Real Servers.

- Normally eth0 is used for the internal network and eth1 is used for the external network although this is not mandatory. If the Real Servers require Internet access, Autonat should be enabled using the WebUI option: Cluster Configuration > Layer 4 – Advanced Configuration, the external interface should be selected.

- NAT mode can be deployed in the following ways:

  2-arm (using 2 Interfaces), 2 subnets (as shown above) - One interface on the load balancer is connected to subnet1 and the second interface and Real Servers are connected to subnet2. The VIP is brought up in subnet1. The default gateway on the Real Servers is set to be an IP address in subnet2 on the load balancer. Clients can be located in subnet1 or any remote subnet provided they can route to the VIP.

  2-arm (using 1 Interface), 2 subnets - same as above except that a single interface on the load balancer is allocated 2 IP addresses, one in each subnet.

  1-arm (using 1 Interface), 1 subnet - Here, the VIP is brought up in the same subnet as the Real Servers. For clients located in remote networks the default gateway on the Real Servers must be set to be an IP address on the load balancer. For clients located on the same subnet, return traffic would normally be sent directly to the client bypassing the load balancer which would break NAT mode. To address this, the routing table on the Real Servers must be modified to force return traffic to go via the load balancer - for more details on 'One-Arm NAT Mode' refer to chapter 6 in the Administration Manual.

- If you want Real Servers to be accessible on their own IP address for non-load balanced services, e.g. SMTP or RDP, you will need to setup individual SNAT and DNAT firewall script rules for each Real Server or add additional VIPs for this - please refer to chapter 6 in the Administration Manual.

- NAT mode is transparent, i.e. the Real Server will see the source IP address of the client.
• Port translation is possible in NAT mode, i.e. VIP:80 --> RIP:8080 is possible.

Layer 7 SNAT Mode
Layer 7 SNAT mode uses a proxy (HAProxy) at the application layer. Inbound requests are terminated on the load balancer, and HAProxy generates a new request to the chosen Real Server. As a result, Layer 7 is a slower technique than DR or NAT mode at Layer 4. Layer 7 is typically chosen when either enhanced options such as SSL termination, cookie based persistence, URL rewriting, header insertion/deletion etc. are required, or when the network topology prohibits the use of the layer 4 methods.

This mode can be deployed in a one-arm or two-arm configuration and does not require any changes to the Real Servers. However, since the load balancer is acting as a full proxy it doesn't have the same raw throughput as the layer 4 methods.

The load balancer proxies the application traffic to the servers so that the source of all traffic becomes the load balancer.

• SNAT mode is a full proxy and therefore load balanced Real Servers do not need to be changed in any way
• Because SNAT mode is a full proxy any server in the cluster can be on any accessible subnet including across the Internet or WAN
• SNAT mode is not transparent by default, i.e. the Real Servers will not see the source IP address of the client, they will see the load balancers own IP address by default, or any other local appliance IP address if preferred (e.g. the VIP address), this can be configured per layer 7 VIP. If required, the clients IP address can be passed through either by enabling TProxy on the load balancer, or for HTTP, using X-forwarded-For headers. Please refer to chapter 6 in the administration manual for more details
• SNAT mode can be deployed using either a 1-arm or 2-arm configuration

Our Recommendation
Where possible we recommend that Layer 4 Direct Routing (DR) mode is used. This mode offers the best possible
performance since replies go directly from the Real Servers to the client, not via the load balancer. It’s also relatively simple to implement. Ultimately, the final choice does depend on your specific requirements and infrastructure.

If DR mode cannot be used, for example if it is not possible to make certain changes to the real servers, or if the real servers are located in remote routed networks, then layer 4 NAT mode with layer 7 SNAT mode is recommended.

9. Configuring McKesson Radiology and McKesson Cardiology for Load Balancing

Layer 4 DR Mode – Solving the ARP Problem
If using layer 4 DR mode, the ‘ARP problem’ must be solved on each real server for DR mode to work. For detailed steps on solving the ARP problem for Windows, please refer to section 1 of the appendix on page 32 for more information.

For a detailed explanation of DR mode and the nature of the ARP problem, please refer to the section that covers layer 4 DR mode on page 7.

Layer 4 NAT Mode – Changing the Real Servers’ Default Gateways
If using layer 4 NAT mode, each back end real server must be configured so that the default gateway is an IP address owned by the load balancer. If using an HA pair of load balancers, this IP address should be a floating IP address so that network communication continues after a load balancer fail over.

For a detailed explanation of NAT mode, please refer to the section that covers layer 4 NAT mode on page 7.
10. Loadbalancer.org Appliance – the Basics

Virtual Appliance Download & Deployment
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 and XEN and has been optimized for each Hypervisor. By default, the VA is allocated 1 CPU, 2GB of RAM and has an 8GB 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 Administration Manual and the ReadMe.txt text file included in the VA download for more detailed information on deploying the VA using various Hypervisors.

Initial Network Configuration
The IP address, subnet mask, default gateway and DNS settings can be configured in several ways as detailed below:

Method 1 - Using the Network Setup Wizard at the console
After boot up, follow the instructions on the console to configure the IP address, subnet mask, default gateway and DNS settings.

Method 2 - Using the WebUI
Using a browser, connect to the WebUI on the default IP address/port: https://192.168.2.21:9443
To set the IP address & subnet mask, use: Local Configuration > Network Interface Configuration
To set the default gateway, use: Local Configuration > Routing
To configure DNS settings, use: Local Configuration > Hostname & DNS
Accessing the Web User Interface (WebUI)
The WebUI can be accessed via HTTPS at the following URL: https://192.168.2.21:9443/lbadmin
* Note the port number → 9443

(replace 192.168.2.21 with the IP address of your load balancer if it’s been changed from the default)

Login using the following credentials:

Username: loadbalancer
Password: loadbalancer

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

Once logged in, the WebUI will be displayed as shown on the following page:
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 slave unit is covered in section 2 of the appendix on page 37.
11. Appliance Configuration for McKesson Radiology and McKesson Cardiology – Using Layer 4 DR Mode

This load balancing method (layer 4 DR mode) is recommended as it offers the best possible performance.

When load balancing McKesson Radiology and McKesson Cardiology, up to five virtual services need to be configured: a virtual service for McKesson Radiology (DICOM traffic), a virtual service for McKesson Radiology (web traffic), a virtual service for McKesson Radiology Manager, a virtual service for McKesson Clinical Reference Viewer, and a virtual service for McKesson Cardiology.

Configuring VIP 1 – McKesson Radiology (DICOM Traffic)

**Configuring The Virtual Service (VIP)**

1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Virtual Services* and click on **Add a new Virtual Service**
2. Define the *Label* for the virtual service as required, e.g. **McK-Radiology_DICOM**
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.30**
4. Set the *Ports* field to **4000,5000**
5. Leave the *Protocol* set to **TCP**
6. Leave the *Forwarding Method* set to **Direct Routing**
7. Click **Update** to create the virtual service

![Layer 4 - Add a New Virtual Service](image)

8. Click **Modify** next to the newly created VIP
9. Leave the *Balance Mode* set to **Weighted Least Connection** (this is equivalent to what F5 call the “Observed (member)” load balancing method)
10. Make sure that the *Persistent* checkbox is checked
11. Set the *Persistent Timeout* value to **3600** (the units are seconds)
12. Set the *Health Checks Check Type* to **Connect to port**
13. Set the *Check Port* to **5000**
14. Click **Update**
Defining The Real Servers (RIPs)

1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – Real Servers and click on Add a new Real Server next to the newly created VIP
2. Define the Label for the real server as required, e.g. McK-Radiology_Srv1
3. Set the Real Server IP Address field to the required IP address, e.g. 192.168.85.200
4. Click Update
5. Repeat these steps to add additional real servers as required

### Layer 4 Modify Real Server - McK-Radiology_DICOM / McK-Radiology-Srv1

<table>
<thead>
<tr>
<th>Label</th>
<th>McK-Radiology_Srv1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.85.200</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>

Configuring VIP 2 – McKesson Radiology (Web Traffic)

Configuring The Virtual Service (VIP)

1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – Virtual Services and click on Add a new Virtual Service
2. Define the Label for the virtual service as required, e.g. McK-Radiology_Web
3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.85.31
4. Set the Ports field to 80
5. Leave the Protocol set to TCP
6. Leave the Forwarding Method set to Direct Routing
7. Click Update to create the virtual service
8. Click **Modify** next to the newly created VIP
9. Leave the **Balance Mode** set to **Weighted Least Connection** (this is equivalent to what F5 call the “Observed (member)” load balancing method)
10. Make sure that the **Persistent** checkbox is not checked
11. Configure health checking depending on the version of McKesson Radiology Web Server in use:
   - If using McKesson Radiology Web Server version 12.1 and later:
     - Set **Health Checks Check Type** to **Negotiate**
     - Set the **Check Port** field to **80**
     - Leave the **Protocol** set to **HTTP**
     - Set the **Request to send** field to **/wpp/srvpacs.asp**
     - Set the **Response expected** field to **srvPACS OK**
   - If using McKesson Radiology Web Server version 12.0, it is possible to use the same health check that is used for version 12.1, which is described above.
     McKinsson officially advise to perform an additional two health checks on version 12.0 Radiology Web Servers in order for them to be considered to be functioning fully. This is possible to achieve using an external health check script. For assistance in implementing this, please contact **solutions@loadbalancer.org**
12. Click **Update**

### Defining The Real Servers (RIPs)
1. Using the web user interface, navigate to **Cluster Configuration > Layer 4 – Real Servers** and click on **Add a new Real Server** next to the newly created VIP
2. Define the **Label** for the real server as required, e.g. **McK-Radiology_Srv1**
3. Set the **Real Server IP Address** field to the required IP address, e.g. **192.168.85.200**
4. Click **Update**
5. Repeat these steps to add additional real servers as required
Configuring VIP 3 – McKesson Radiology Manager

Configuring The Virtual Service (VIP)

1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – Virtual Services and click on Add a new Virtual Service
2. Define the Label for the virtual service as required, e.g. McK-RadiologyManager
3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.85.40
4. Set the Ports field to 80
5. Leave the Protocol set to TCP
6. Leave the Forwarding Method set to Direct Routing
7. Click Update to create the virtual service

8. Click Modify next to the newly created VIP
9. Leave the Balance Mode set to Weighted Least Connection (this is equivalent to what F5 call the “Observed (member)” load balancing method)
10. Make sure that the Persistent checkbox is checked
11. Set the Persistent Timeout value to 300 (the units are seconds)
12. Set Health Checks Check Type to Negotiate
13. Set the Check Port field to 80
14. Leave the Protocol set to HTTP
15. Set the Request to send field to icis/index.html
16. Set the Response expected field to OK
17. Click Update

Defining The Real Servers (RIPs)
1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – Real Servers and click on Add a new Real Server next to the newly created VIP
2. Define the Label for the real server as required, e.g. McK-RadiologyMgr_Srv1
3. Set the Real Server IP Address field to the required IP address, e.g. 192.168.85.210
4. Click Update
5. Repeat these steps to add additional real servers as required

```
<table>
<thead>
<tr>
<th>Label</th>
<th>McK-RadiologyMgr_Srv1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.85.210</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>
```

Configuring VIP 4 – McKesson Clinical Reference Viewer

Configuring The Virtual Service (VIP)
1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – Virtual Services and click on Add a new Virtual Service
2. Define the Label for the virtual service as required, e.g. McK-ClinicalRefViewer
3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.85.50
4. Set the Ports field to 80
5. Leave the Protocol set to TCP
6. Leave the Forwarding Method set to Direct Routing
7. Click Update to create the virtual service
8. Click **Modify** next to the newly created VIP

9. Leave the **Balance Mode** set to **Weighted Least Connection** (this is equivalent to what F5 call the “Observed (member)” load balancing method)

10. Make sure that the **Persistent** checkbox is checked

11. Set the **Persistent Timeout** value to **300** (the units are seconds)

12. Set **Health Checks Check Type** to **Negotiate**

13. Set the **Check Port** field to **80**

14. Leave the **Protocol** set to **HTTP**

15. Set the **Request to send** field to **/McKessonEmiCRV/Ping.aspx**

16. Set the **Response expected** field to **OK**

17. Click **Update**

**Defining The Real Servers (RIPs)**

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

2. Define the **Label** for the real server as required, e.g. **McK-ClinRefVwr_Srv1**

3. Set the **Real Server IP Address** field to the required IP address, e.g. **192.168.85.220**

4. Click **Update**

5. Repeat these steps to add additional real servers as required
Configuring VIP 5 – McKesson Cardiology

Configuring The Virtual Service (VIP)

1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – Virtual Services and click on Add a new Virtual Service
2. Define the Label for the virtual service as required, e.g. McK-Cardiology
3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.85.60
4. Set the Ports field to 80,443
5. Leave the Protocol set to TCP
6. Leave the Forwarding Method set to Direct Routing
7. Click Update to create the virtual service
8. Click Modify next to the newly created VIP
9. Leave the Balance Mode set to Weighted Least Connection (this is equivalent to what F5 call the “Observed (member)” load balancing method)
10. Make sure that the Persistent checkbox is checked
11. Set the *Persistent Timeout* value to **14400** (the units are seconds)
12. Set *Health Checks Check Type* to **Negotiate**
13. Set the *Check Port* field to **80**
14. Leave the *Protocol* set to **HTTP**
15. Set the *Request to send* field to **/**
16. Set the *Response expected* field to **OK**

**Defining The Real Servers (RIPs)**

1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Real Servers* and click on **Add a new Real Server** next to the newly created VIP
2. Define the *Label* for the real server as required, e.g. **McK-Cardiology_Srv1**
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.85.230**
4. Click **Update**
5. Repeat these steps to add additional real servers as required
12. Appliance Configuration for McKesson Radiology and McKesson Cardiology – Using Layer 4 NAT Mode and Layer 7 SNAT Mode

This is not the recommended load balancing method, as it does not offer the same level of performance or throughput as layer 4 DR mode. With this method, all reply traffic must go via the load balancer, which can become a bottleneck for performance.

As layer 4 NAT mode is used for load balancing the McKesson Radiology and McKesson Cardiology traffic, the real servers for these services must reside in a separate subnet, to which the load balancer is connected, and must have their default gateway set to be the load balancer. This is required for NAT mode to work.

The outline of this type of deployment is as so:

![Deployment Diagram](image)

When load balancing McKesson Radiology and McKesson Cardiology, up to five virtual services need to be configured: a virtual service for McKesson Radiology (DICOM traffic), a virtual service for McKesson Radiology (web traffic), a virtual service for McKesson Radiology Manager, a virtual service for McKesson Clinical Reference Viewer, and a virtual service for McKesson Cardiology.

**Configuring VIP 1 – McKesson Radiology (DICOM Traffic)**

**Configuring The Virtual Service (VIP)**

1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – Virtual Services and click on Add a new Virtual Service
2. Define the Label for the virtual service as required, e.g. McK-Radiology_DICOM
3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.85.30
4. Set the Ports field to 4000,5000
5. Leave the Protocol set to TCP
6. Leave the Forwarding Method set to NAT
7. Click Update to create the virtual service
8. Click **Modify** next to the newly created VIP

9. Leave the **Balance Mode** set to **Weighted Least Connection** (this is equivalent to what F5 call the “Observed (member)” load balancing method)

10. Make sure that the **Persistent** checkbox is checked

11. Set the **Persistent Timeout** value to **3600** (the units are seconds)

12. Set the **Health Checks Check Type** to **Connect to port**

13. Set the **Check Port** to **5000**

14. Click **Update**

---

**Defining The Real Servers (RIPs)**

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

2. Define the **Label** for the real server as required, e.g. **McK-Radiology_Srv1**

3. Set the **Real Server IP Address** field to the required IP address, e.g. **10.10.0.200**

4. Click **Update**

5. Repeat these steps to add additional real servers as required
Configuring VIP 2 – McKesson Radiology (Web Traffic)

Configuring The Virtual Service (VIP)

1. Using the web user interface, navigate to Cluster Configuration > Layer 4 – Virtual Services and click on Add a new Virtual Service
2. Define the Label for the virtual service as required, e.g. McK-Radiology_Web
3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.85.31
4. Set the Ports field to 80
5. Leave the Protocol set to TCP
6. Leave the Forwarding Method set to NAT
7. Click Update to create the virtual service

8. Click Modify next to the newly created VIP
9. Leave the Balance Mode set to Weighted Least Connection (this is equivalent to what F5 call the “Observed (member)” load balancing method)
10. Make sure that the *Persistent* checkbox is not checked

11. Configure health checking depending on the version of McKesson Radiology Web Server in use:
   - If using McKesson Radiology Web Server version 12.1 and later:
     - Set Health Checks Check Type to **Negotiate**
     - Set the Check Port field to **80**
     - Leave the Protocol set to **HTTP**
     - Set the Request to send field to **/wpp/srvpacs.asp**
     - Set the Response expected field to **srvPACS OK**
   - If using McKesson Radiology Web Server version 12.0, it is possible to use the same health check that is used for version 12.1, which is described above. McKesson officially advise to perform an additional two health checks on version 12.0 Radiology Web Servers in order for them to be considered to be functioning fully. This is possible to achieve using an external health check script. For assistance in implementing this, please contact solutions@loadbalancer.org

12. Click **Update**

**Defining The Real Servers (RIPs)**

1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Real Servers* and click on **Add a new Real Server** next to the newly created VIP
2. Define the **Label** for the real server as required, e.g. **McK-Radiology_Srv1**
3. Set the **Real Server IP Address** field to the required IP address, e.g. **10.10.0.200**
4. Click **Update**
5. Repeat these steps to add additional real servers as required
Configuring VIP 3 – McKesson Radiology Manager

Configuring The Virtual Service (VIP)
1. Using the web user interface, navigate to Cluster Configuration > Layer 7 – Virtual Services and click on Add a new Virtual Service
2. Define the Label for the virtual service as required, e.g. McK-RadiologyManager
3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.85.40
4. Set the Ports field to 80
5. Set the Layer 7 Protocol to HTTP Mode
6. Click Update to create the virtual service

```
<table>
<thead>
<tr>
<th>Label</th>
<th>McK-RadiologyManager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>192.168.85.40</td>
</tr>
<tr>
<td>Ports</td>
<td>80</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>HTTP Mode</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

7. Click Modify next to the newly created VIP
8. Leave the Balance Mode set to Weighted Least Connections (this is equivalent to what F5 call the “Observed (member)” load balancing method)
9. Set the Persistence Mode to HTTP Cookie
10. In the Health Checks section click Advanced to show more options
11. Set Health Checks to Negotiate HTTP (GET)
12. Set the Check Port field to 80
13. Set the Request to send field to /cis/index.html
14. Set the Response expected field to OK
15. Click Update

Defining The Real Servers (RIPs)
1. Using the web user interface, navigate to Cluster Configuration > Layer 7 – Real Servers and click on Add a new Real Server next to the newly created VIP
2. Define the Label for the real server as required, e.g. McK-RadiologyMgr_Srv1
3. Set the Real Server IP Address field to the required IP address, e.g. 10.10.0.210
4. Click **Update**

5. Repeat these steps to add additional real servers as required

![Layer 7 Add a New Real Server - MCK-RadiologyManager](image)

**Configuring VIP 4 – McKesson Clinical Reference Viewer**

**Configuring The Virtual Service (VIP)**

1. Using the web user interface, navigate to **Cluster Configuration > Layer 7 – Virtual Services** and click on **Add a new Virtual Service**

2. Define the **Label** for the virtual service as required, e.g. *McK-ClinicalRefViewer*

3. Set the **Virtual Service IP Address** field to the required IP address, e.g. 192.168.85.50

4. Set the **Ports** field to **80**

5. Set the **Layer 7 Protocol** to **HTTP Mode**

6. Click **Update** to create the virtual service

![Layer 7 - Add a New Virtual Service](image)

7. Click **Modify** next to the newly created VIP

8. Leave the **Balance Mode** set to **Weighted Least Connections** (this is equivalent to what F5 call the “Observed (member)” load balancing method)
9. Set the Persistence Mode to **HTTP Cookie**
10. In the **Health Checks** section click **Advanced** to show more options
11. Set Health Checks to **Negotiate HTTP (GET)**
12. Set the **Check Port** field to **80**
13. Set the **Request to send** field to **/McKessonEmiCRV/Ping.aspx**
14. Set the **Response expected** field to **OK**
15. Click **Update**

**Defining The Real Servers (RIPs)**

1. Using the web user interface, navigate to **Cluster Configuration > Layer 7 – Real Servers** and click on **Add a new Real Server** next to the newly created VIP
2. Define the **Label** for the real server as required, e.g. **McK-ClinRefVwr_Srv1**
3. Set the **Real Server IP Address** field to the required IP address, e.g. **10.10.0.220**
4. Click **Update**
5. Repeat these steps to add additional real servers as required

```
<table>
<thead>
<tr>
<th>Label</th>
<th>McK-ClinRefVwr_Srv1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>10.10.0.220</td>
</tr>
<tr>
<td>Real Server Port</td>
<td></td>
</tr>
<tr>
<td>Re-Encrypt to Backend</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>
```

**Configuring VIP 5 – McKesson Cardiology**

**Configuring The Virtual Service (VIP)**

1. Using the web user interface, navigate to **Cluster Configuration > Layer 4 – Virtual Services** and click on **Add a new Virtual Service**
2. Define the **Label** for the virtual service as required, e.g. **McK-Cardiology**
3. Set the **Virtual Service IP Address** field to the required IP address, e.g. **192.168.85.60**
4. Set the **Ports** field to **80,443**
5. Leave the **Protocol** set to **TCP**
6. Leave the **Forwarding Method** set to **NAT**
7. Click **Update** to create the virtual service
8. Click **Modify** next to the newly created VIP

9. Leave the **Balance Mode** set to **Weighted Least Connection** (this is equivalent to what F5 call the “Observed (member)” load balancing method)

10. Make sure that the **Persistent** checkbox is checked

11. Set the **Persistent Timeout** value to **14400** (the units are seconds)

12. Set **Health Checks Check Type** to **Negotiate**

13. Set the **Check Port** field to **80**

14. Leave the **Protocol** set to **HTTP**

15. Set the **Request to send** field to **/**

16. Set the **Response expected** field to **OK**

**Defining The Real Servers (RIPs)**

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

2. Define the **Label** for the real server as required, e.g. **McK-Cardiology_Srv1**

3. Set the **Real Server IP Address** field to the required IP address, e.g. **10.10.0.230**

4. Click **Update**

5. Repeat these steps to add additional real servers as required
Finalizing the Configuration
To apply the new settings, HAProxy must be restarted as follows:

1. Using the WebUI, navigate to: Maintenance > Restart Services and click Restart HAProxy

13. Testing & Verification

Using System Overview
The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & RIPS (i.e. the McKesson servers) and shows the state/health of each server as well as the state of the cluster as a whole. The example below shows that all McKesson servers are healthy and available to accept connections for all five of the virtual services:
14. 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.

15. Further Documentation

16. Conclusion
Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced McKesson Radiology and McKesson Cardiology environments.
17. Appendix

1 - Solving the ARP Problem
When using Layer 4 DR mode, the ARP problem must be solved. This involves configuring each Real Server to be able to receive traffic destined for the VIP, and ensuring that each Real Server does not respond to ARP requests for the VIP address – only the load balancer should do this.

The steps below are for Windows 2012/2016, for other versions of Windows please refer to chapter 6 in the administration manual.

Step 1: 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

![Add Hardware Screen]

6. Click Next to start the installation, when complete click Finish

Step 2: 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. Un-check all items except **Internet Protocol Version 4 (TCP/IPv4)** and **Internet Protocol Version 6 (TCP/IPv6)** as shown below:

![Loopback Properties](image)

Note: Leaving both checked ensures that both IPv4 and IPv6 are supported. Select one if preferred.

**Important:** When configuring the Loopback Adapter to solve the ARP Problem, the following options **must** also be checked (ticked):
- Client for Microsoft Networks
- File & Printer Sharing for Microsoft Networks

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.

8. Now repeat the above process on the other Windows 2012/2016 Real Servers.
**Step 3: Configure the strong/weak host behavior**

Windows Server 2000 and Windows Server 2003 use the weak host model for sending and receiving for all IPv4 interfaces and the strong host model for sending and receiving for all IPv6 interfaces. You cannot configure this behavior. The Next Generation TCP/IP stack in Windows 2008 and later supports strong host sends and receives for both IPv4 and IPv6 by default. To ensure that Windows 2012/2016 is running in the correct mode to be able to respond to the VIP, the following commands must be run on each Real Server:

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
```

For IPv6 addresses:

```
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:

```
netsh interface ipv4 set interface "LAN" weakhostreceive=enabled
netsh interface ipv4 set interface "LOOPBACK" weakhostreceive=enabled
netsh interface ipv4 set interface "LOOPBACK" weakhostsend=enabled
```

```
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
```

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 ipv4 set interface "LAN" weakhostreceive=enabled
netsh interface ipv4 set interface "LOOPBACK" weakhostreceive=enabled
netsh interface ipv4 set interface "LOOPBACK" weakhostsend=enabled
```

```
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.

1. Start Powershell or use a command window to run the appropriate netsh commands as shown in the example below:

   ![Network Connections](image)

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

2. Now repeat these 4 commands on the other Windows 2012/2016 Real Servers

   ![Administrator Windows Powershell](image)

   Note: Solving the ARP problem for other version of Windows is similar. For full details, please refer to the administration manual.
2 – Clustered Pair Configuration – Adding a Slave Unit

If you initially configured just the master unit and now need to add a slave - our recommended procedure, please refer to the relevant section below for more details:

Note: A number of settings are not replicated as part of the master/slave pairing process and therefore must be manually configured on the slave appliance. These are listed below:

- Hostname & DNS settings
- Network settings including IP addresses, bonding configuration and VLANs
- Routing configuration including default gateways and static routes
- Date & time settings
- Physical – Advanced Configuration settings including Internet Proxy IP address & port, Firewall table size, SMTP relay and Syslog server
- SNMP settings
- Graphing settings
- Firewall Script & Firewall Lockdown Script settings
- Software updates

Version 7:

Please refer to Chapter 8 – Appliance Clustering for HA in the v7 Administration Manual.

Version 8:

To add a slave node – i.e. create a highly available clustered pair:

- Deploy a second appliance that will be the slave and configure initial network settings
- Using the WebUI, navigate to: Cluster Configuration > High-Availability Configuration
- Specify the IP address and the loadbalancer users password (the default is 'loadbalancer') for the slave (peer) appliance as shown above
• Click **Add new node**

• The pairing process now commences as shown below:

![Create a Clustered Pair](image)

• Once complete, the following will be displayed:

![High Availability Configuration - Master](image)

• 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 master appliance will also automatically restart heartbeat on the slave appliance.

  **Note:** Please refer to chapter 9 – Appliance Clustering for HA in the *Administration Manual* for more detailed information on configuring HA with 2 appliances.
## 18. Document Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Changed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0</td>
<td>17 July 2018</td>
<td>Initial version</td>
<td></td>
<td>AH</td>
</tr>
<tr>
<td>1.0.1</td>
<td>18 July 2018</td>
<td>Changed document title, and references in the document, from &quot;McKesson Radiology And Cardiology Applications Deployment Guide&quot; to &quot;McKesson Radiology and McKesson Cardiology Deployment Guide&quot;</td>
<td>Required updates</td>
<td>AH</td>
</tr>
<tr>
<td>1.0.2</td>
<td>6 December 2018</td>
<td>Added the new “Company Contact Information” page</td>
<td>Required updates</td>
<td>AH</td>
</tr>
<tr>
<td>1.1.0</td>
<td>7 November 2019</td>
<td>Styling and layout</td>
<td>General styling updates</td>
<td>AH</td>
</tr>
<tr>
<td>1.1.1</td>
<td>27 July 2020</td>
<td>New title page</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated Canadian contact details</td>
<td>Change to Canadian contact details</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added additional instructions for configuring layer 7 health checks</td>
<td>Changes to the appliance WebUI</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.

United Kingdom
Loadbalancer.org Ltd.
Compass House, North Harbour Business Park, Portsmouth, PO6 4PS
UK:+44 (0) 330 380 1064
sales@loadbalancer.org
support@loadbalancer.org

Canada
Loadbalancer.org Appliances Ltd.
300-422 Richards Street, Vancouver, BC, V6B 2Z4, Canada
TEL:+1 866 998 0508
sales@loadbalancer.org
support@loadbalancer.org

United States
Loadbalancer.org, Inc.
4550 Linden Hill Road, Suite 201
Wilmington, DE 19808, USA
TEL: +1 833.274.2566
sales@loadbalancer.org
support@loadbalancer.org

Germany
Loadbalancer.org GmbH
Tengstraße 2780798,
München, Germany
TEL: +49 (0)89 2000 2179
sales@loadbalancer.org
support@loadbalancer.org

© Copyright Loadbalancer.org • www.loadbalancer.org