Load Balancing Insignia Medical Systems

Version 1.1.0
# Table of Contents

1. About this Guide .................................................. 3  
2. Loadbalancer.org Appliances Supported .......................... 3  
3. Loadbalancer.org Software Versions Supported ................. 3  
4. Medical Systems Supported ..................................... 3  
5. Medical Information System Standards & Protocols .............. 3  
   DICOM ........................................................................ 3  
   HL7 .......................................................................... 3  
6. Load Balancing Overview ......................................... 3  
   Basic Concepts .......................................................... 3  
   Load Balancer Deployment .......................................... 4  
   Load Balancing Deployment Modes ................................ 5  
   Our Recommendation .................................................. 5  
   Load Balanced Ports & Services .................................... 5  
   Persistence (Server Affinity) ......................................... 6  
   Server Health Checking .............................................. 6  
7. Loadbalancer.org Appliance – the Basics ...................... 6  
   Virtual Appliance ....................................................... 6  
   Initial Network Configuration ....................................... 7  
   Accessing the WebUI .................................................. 7  
   Main Menu Options .................................................. 8  
   Clustered Pair Configuration ....................................... 9  
8. Appliance and Server Configuration .............................. 9  
   Load Balancing Mode ................................................ 9  
   Health-Check Configuration ....................................... 9  
   Load Balancing DICOM ............................................. 9  
   Setting up the Virtual Service (VIP) ................................. 9  
   Setting up the Real Servers (RIPs) ................................. 10  
   Configuring the load balanced DICOM servers .................. 10  
   Load Balancing HL7 .................................................. 11  
   Setting up the Virtual Service (VIP) ................................. 11  
   Setting up the Real Servers (RIPs) ................................. 11  
   Restart HAProxy ....................................................... 12  
9. Testing & Verification ............................................... 12  
   Using the System Overview ....................................... 12  
   System Logs & Reports ............................................. 13  
10. Technical Support .................................................. 13  
11. Further Documentation ........................................... 13  
12. Conclusion .......................................................... 13  
13. Appendix ............................................................ 14  
   Configuring HA - Adding a Secondary Appliance ............... 14  
   Solving the ARP Problem .......................................... 16  
14. Document Revision History ..................................... 17
1. About this Guide

This guide details the steps required to configure a load balanced Insignia Medical System environment utilizing Loadbalancer.org appliances. It includes details on load balancing DICOM & HL7.

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 Medical Imaging and Information Systems. 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

- V8.4 & later

4. Medical Systems Supported

- Any systems that utilizes medical system standards & protocols such as DICOM and HL7

5. Medical Information System Standards & Protocols

**DICOM**

The Digital Imaging and Communications in Medicine (DICOM) Standard describes the means of formatting, storing and exchanging medical images and image related information to facilitate the connectivity of medical devices and systems. The DICOM Standard endorsed by the National Electrical Manufacturers Association (NEMA) is a result of joint efforts of users and manufacturers of medical imaging and health-care information technology.

Today, virtually all imaging devices (Modalities) that are used in radiology, such as CT, MRI, Ultrasound, RF, and other digital rooms, supports the DICOM standard for the exchange of images and related information.

**HL7**

Health Level Seven (HL7) is an American National Standards Institute accredited Standards Developing Organization (SDO) operating in the health-care arena. Since its inception, HL7 has specified standards for a large number of application areas. HL7 standards cover generic application fields such as patient administration, patient care, order entry, results reporting, document and financial management. In addition to that, HL7 addresses the departmental information system communication needs of clinical specialties like laboratory medicine and diagnostic imaging. HL7 is the language used for communication between health-care IT systems.

6. Load Balancing Overview

**Basic Concepts**

To provide resilience and high availability, multiple Virtual Services (VIPs) are configured for the various protocols and systems. Clients and systems then connect to these VIPs rather than directly to the application servers. Each VIP can be configured in one of the following ways:

- Load balanced mode
Load is distributed across all configured servers/endpoints

- Failover mode

The second server is used only when the first server/endpoint fails

Load Balancer Deployment
The following diagram shows a simplified view of Insignia Medical System in load balancing mode:

The following diagram shows a simplified view of Insignia Medical System in failover mode:

Notes

1. **VIP (Virtual IP)** – This is the IP address presented by the load balancer. Clients and other systems connect to this rather than directly to the back end servers/endpoints.
2. A single load balancer appliance can be used to load balance all services. More that one load balancer appliance may be required depending on throughput and physical network topology.

Load Balancing Deployment Modes

The load balancer supports the following deployment modes:

**Layer 4 DR Mode** – this mode offers the best performance and requires limited physical Real Server changes. The load balanced application must be able to bind to the Real Servers own IP address and the VIP at the same time. This mode requires the "ARP Problem" to be solved as described in Solving the ARP Problem. This mode is transparent, i.e. the Real Servers will see the source IP address of the client.

**Layer 4 NAT Mode** – this mode is also a high performance solution but not as fast as DR mode. It requires the implementation of a two-arm infrastructure with an internal and external subnet to carry out the translation (the same way a firewall works). Also each Real Server must use the load balancer as the default gateway. This mode is transparent, i.e. the Real Servers will see the source IP address of the client.

**Layer 4 SNAT Mode** – this mode is also a high performance solution but not as fast as the other layer 4 modes. It does not require any changes to the Real Servers and can be deployed in one-arm or two-arm mode. This mode is ideal for example when you want to load balance both TCP and UDP but you’re unable to use DR mode or NAT mode due to network topology or Real Server related reasons. This mode is non-transparent, i.e. the Real Servers will see the source IP address of the load balancer.

**Layer 7 SNAT Mode** – this mode offers greater flexibility but at lower performance levels. It supports HTTP cookie insertion, RDP cookies, Connection Broker integration and works very well with either Pound or STunnel when SSL termination is required. It does not require any changes to the Real Servers and can be deployed in one-arm or two-arm mode and. HAProxy is a high performance solution, but since it operates as a full proxy, it cannot perform as fast as the layer 4 solutions. This mode is non-transparent, i.e. the Real Servers will see the source IP address of the load balancer.

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.

Note

If you are using Microsoft Windows Real Servers (i.e. the backend servers) make sure that Windows NLB (Network Load Balancing) is **completely disabled** to ensure that this does not interfere with the operation of the load balancer.

Load Balanced Ports & Services

The following tables shows the typical ports/services that are load balanced.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>104</td>
<td>TCP/DICOM</td>
<td>Exchange of images and related information</td>
</tr>
<tr>
<td>2575</td>
<td>TCP/HL7</td>
<td>Communication between health-care IT systems</td>
</tr>
</tbody>
</table>
Persistence (Server Affinity)
Source IP address persistence is used for all protocols. This ensures that a particular client will connect to the same load balanced server/endpoint for the duration of the session.

Server Health Checking
The default health-check used for new VIPs is a TCP port connect. This verifies that the port is open and accepting connections. However, it does not necessarily guarantee that the associated service is fully operational. Also, repeated ongoing connections to the service port may cause multiple log entries reporting incomplete connections or other issues.

More robust service oriented health-checks can be configured for both layer 4 and layer 7 services using the negotiate option. This effectively tests and verifies the running service.

For example, the load balancer can be configured to look for specific content on an HTTP web page on the load balanced Real Server. If the page can be opened and the content can be found, the check will have passed. If not, the check will fail and the server/endpoint will be marked as down.

If the service running is not HTTP based, a custom page could be setup on the load balanced servers that simply indicates service status. The load balancer can then use this for health checking.

The page to check and the content to be verified can easily be configured for layer 4 and layer 7 VIPs using the WebUI. Select the required negotiate option and configure the required settings. For more details on configuring health-checks please refer to Real Server Health Monitoring & Control.

Note: The configuration examples in this guide use a TCP port connect (the default) to check the health of load balanced servers.

7. 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. Appliance authentication is based on Apache .htaccess files. User admin 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, RIPv 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 & RIPv
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
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.

8. Appliance and Server Configuration

Load Balancing Mode
As mentioned in Load Balancing Deployment Modes, Virtual Services can be configured in one of four fundamental ways, i.e. Layer 4 DR mode, Layer 4 NAT mode, Layer 4 SNAT mode or Layer 7 SNAT mode. The following sections illustrate how to configure the Virtual Services using various modes. If a different mode is required for a particular VIP, please refer to one of the other sections that uses that mode for guidance. Please also don’t hesitate to contact our support team: support@loadbalancer.org.

Health-Check Configuration
As mentioned in Server Health Checking, health checks can be configured in several different ways. The sections below all use a TCP port connect on the service port.

Load Balancing DICOM
(Using Layer 4 DR Mode)

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:

   ![Layer 4 - Add a new Virtual Service](image)
3. Enter an appropriate name (Label) for the Virtual Service, e.g. DS_DICOM.

4. Set the Virtual Service IP address field to the required IP address, e.g. 172.26.11.70.

5. Set the Virtual Service Ports field to the required port(s), e.g. 104.

6. Set Protocol to TCP.

7. Set Forwarding Method to Direct Routing.

8. Click Update.

9. Now click Modify next to the newly created Virtual Service.

10. Set Persistent Timeout to 300, i.e. 5 minutes.

11. Set the Check Type to External Script.

12. Set the External script to DICOM-C-ECHO.

13. Set the Check Port to the same port as the VIP, e.g. 104.

14. Click Update.

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 Virtual Service.

2. Enter the following details:

   **Layer 4 Add a new Real Server - DS_DICOM**

<table>
<thead>
<tr>
<th>Label</th>
<th>DS1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>172.26.11.100</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 name (Label) for the first DICOM server, e.g. DS1.

4. Change the Real Server IP Address field to the required IP address, e.g. 172.26.11.100.

5. Click Update.

6. Repeat these steps to add additional server(s).

Configuring the load balanced DICOM servers

1. As mentioned in Load Balancing Deployment Modes, the ARP problem must be solved for all load balanced servers. Please refer to Solving the ARP Problem for more details.
Load Balancing HL7
(Using Layer 7 SNAT Mode)

Setting up the Virtual Service (VIP)

1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Virtual Services and click Add a New Virtual Service.

2. Enter the following details:

   **Layer 7 - Add a new Virtual Service**

<table>
<thead>
<tr>
<th>Label</th>
<th>HL7</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>172.26.11.71</td>
</tr>
<tr>
<td>Ports</td>
<td>2575</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>TCP Mode</td>
</tr>
<tr>
<td>Manual Configuration</td>
<td></td>
</tr>
</tbody>
</table>

3. Enter an appropriate name (Label) for the Virtual Service, e.g. HL7.
4. Set the Virtual Service IP address field to the required IP address, e.g. 172.26.11.71.
5. Set the Virtual Service Ports field to the required port, e.g. 2575.
6. Set the Layer 7 Protocol to TCP Mode.
7. Click Update.
8. Now click Modify next to the newly created Virtual Service.
9. Ensure Persistence Mode is set to None.
10. Set the Health Checks to External Script.
11. Set the Check script to ping.sh.
12. Set the Fallback Server IP address field to that of the Standby node e.g. 172.26.11.103.
13. Set the Port field to 2575.
14. Click Update.

Setting up the Real Servers (RIPs)

1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Real Servers and click Add a new Real Server next to the newly created Virtual Service.

2. Enter the following details:
3. Enter an appropriate name (Label) for the first HL7 server, e.g. IMS1.
4. Change the Real Server IP Address field to the required IP address, e.g. 172.26.11.101.
5. Set the Real Server Port field to 2575.
6. Click Update.
7. Repeat these steps to add additional server(s).

Restart HAProxy

1. To apply the new settings, restart HAProxy using the WebUI option Maintenance > Restart Services and clicking Restart HAProxy.

Note

If you will be configuring additional layer 7 services, you can restart HAProxy at the end once all layer 7 Virtual Services and Real Servers have been defined.

9. Testing & Verification

Using the System Overview

Verify that all VIPs & associated RIPS are reported as up (green) as shown below:
If certain servers are down, i.e. failing their health check, they will be highlighted red as shown below:

<table>
<thead>
<tr>
<th>REAL SERVER</th>
<th>IP</th>
<th>PORTS</th>
<th>WEIGHT</th>
<th>CONNS</th>
<th>Layer 7</th>
<th>Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>HL7</td>
<td>172.26.11.71</td>
<td>2575</td>
<td>0</td>
<td></td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td>IMSI</td>
<td>172.26.11.101</td>
<td>2575</td>
<td>100</td>
<td>0</td>
<td>Drain</td>
<td>Halt</td>
</tr>
</tbody>
</table>

**System Logs & Reports**

Various system logs & reports can be used to help diagnose problems and help solve appliance issues. Logs can be accessed using the WebUI options: *Logs & Reports*.

**10. Technical Support**

If you have any questions regarding the appliance or would like assistance designing your deployment, please don’t hesitate to contact our support team: support@loadbalancer.org.

**11. Further Documentation**

The Administration Manual contains much more information about configuring and deploying the appliance. It's available here: [https://pdfs.loadbalancer.org/loadbalanceradministrationv8.pdf](https://pdfs.loadbalancer.org/loadbalanceradministrationv8.pdf)

**12. Conclusion**

Loadbalancer.org appliances provide a very cost effective and flexible solution for highly available load balanced Medical Imaging Systems environments.
13. 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.

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.

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

<table>
<thead>
<tr>
<th>WebUI Main Menu Option</th>
<th>Sub Menu Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Configuration</td>
<td>Hostname &amp; DNS</td>
<td>Hostname and DNS settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Network Interface</td>
<td>All network settings including IP address(es), bonding configuration and VLANs</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Routing</td>
<td>Routing configuration including default gateways and static routes</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>System Date &amp; time</td>
<td>All time and date related settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Physical – Advanced 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</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, 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:
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.

**Solving the ARP Problem**

Layer 4 DR mode works by changing the MAC address of the inbound packets to match the Real Server selected by the load balancing algorithm. To enable DR mode to operate:

- Each Real Server must be configured to accept packets destined for both the VIP address and the Real Servers IP address (RIP). This is because in DR mode the destination address of load balanced packets is the VIP address, whilst for other traffic such as health-checks, administration traffic etc. it’s the Real Server’s own IP address (the RIP). The service/process (e.g. IIS, httpd) must respond to both addresses.

- Each Real Server must be configured so that it does not respond to ARP requests for the VIP address – only the load balancer should do this.

Configuring the Real Servers in this way is referred to as **‘Solving the ARP problem’**. The steps required depend on the particular OS being used.

For detailed steps on solving the ARP problem for Linux, Windows and various other operating systems, please refer to **DR Mode Considerations**.
## 14. 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>14 January 2020</td>
<td>Initial document creation</td>
<td></td>
<td>IBG</td>
</tr>
<tr>
<td>1.0.1</td>
<td>1 September 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>1.1.0</td>
<td>1 December 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.