Load Balancing Mach7 Technologies

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. Mach7 Technologies Software Versions Supported ......................... 3
5. Mach7 Technologies ...................................................................... 3
6. Load Balancing Overview .............................................................. 4
   - Basic Concepts ........................................................................... 4
   - Load Balancer Deployment ....................................................... 4
   - Load Balancing Deployment Modes ......................................... 5
   - Our Recommendation ............................................................. 6
   - Load Balanced Ports & Services .............................................. 6
   - Persistence (Server Affinity) .................................................... 6
   - Server Health Checking ......................................................... 6
7. Loadbalancer.org Appliance – the Basics ......................................... 7
   - Virtual Appliance ...................................................................... 7
   - Initial Network Configuration .................................................. 7
   - Accessing the WebUI .................................................................. 7
     - Main Menu Options ............................................................ 9
   - Clustered Pair Configuration .................................................... 10
8. Appliance & Server Configuration .................................................. 10
   - Load Balancing Mode ............................................................. 10
   - Health Check Configuration .................................................... 10
   - Load Balancing VNA DICOM .................................................. 10
     - Setting up the Virtual Service (VIP) ..................................... 10
     - Setting up the Real Servers (RIPs) ........................................ 11
   - Load Balancing HL7 ............................................................... 11
     - Setting up the Virtual Service (VIP) ..................................... 11
     - Setting up the Real Servers (RIPs) ........................................ 12
   - Load Balancing DMWL (DICOM Modality Worklist) ..................... 13
     - Setting up the Virtual Service (VIP) ..................................... 13
     - Setting up the Real Servers (RIPs) ........................................ 13
     - Restart HAProx ................................................................. 14
9. Testing & Verification .................................................................... 14
   - Using the System Overview ..................................................... 14
   - System Logs & Reports ......................................................... 15
10. Technical Support ......................................................................... 15
11. Further Documentation ............................................................... 15
12. Conclusion ................................................................................... 15
13. Appendix .................................................................................... 16
   - Configuring HA - Adding a Secondary Appliance ..................... 16
     - Non-Replicated Settings ....................................................... 16
14. Document Revision History .......................................................... 19
1. About this Guide

This guide details the steps required to configure a load balanced Mach7 Technologies environment utilizing Loadbalancer.org appliances.

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

Our hardware and virtual products can be used with VMware App Volumes. For full specifications of available models please refer to: https://www.loadbalancer.org/products

3. Loadbalancer.org Software Versions Supported

- V8.4 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. Mach7 Technologies Software Versions Supported

- Mach7 Technologies – all versions

5. Mach7 Technologies

Mach7 Technologies delivers an Enterprise Imaging Platform that unlocks disparate archive silos, consolidates patient data, and simplifies sharing and access. Improve patient care, reach compliance goals, and deliver clinical and operational decision support enterprise wide.

Mach7 Technologies offers the most advanced software solutions to manage your enterprise imaging strategy and become your EMR for clinical media. Mach7 believes that our customers know their healthcare regional needs, services, and patients best. Mach7 has focused on providing a platform that supports our customers and partners in deploying their best-of-breed healthcare ecosystems. Through Mach7 Enterprise Imaging Platform, providers can plug-in any combination of Mach7 and third party clinical applications to deliver optimal patient care.

Mach7 brings clarity to your image management processes and puts you in control of data ownership, access, sharing, and communication. Mach7 enterprise image management solutions unlock disparate archive silos, consolidate patient data and simplify sharing and access across the connected enterprise.

- Consolidate archiving and communication across the enterprise with a single integration point
- Build a comprehensive view of the patient electronic care record
- Image-enable the EMR
- Plug and play best-of-breed specialty visualization and reporting solutions
- Resolve proprietary formats enabling standards-based storage and interoperability
- Engage patients and referring physicians through an image enabled web-based portal
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/backup server is used only when the first server/endpoint fails.

**Load Balancer Deployment**
The following diagram shows a simplified view of Mach7 Technologies VNA DICOM Nodes in load balancing mode:

![Load Balancer Diagram](image)

The following diagram shows a simplified view of Mach7 Technologies HL7 Nodes in load balancing mode:
The following diagram shows a simplified view of Mach7 Technologies DICOM Modality Worklist Nodes in load balancing mode:

Notes

- **VIP (Virtual IP)** – This is IP address presented by the load balancer. Clients and other systems connect to this rather than directly to the back end servers/endpoints.

- 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 Server’s own IP address and the VIP at the same time.
This mode requires the **ARP Problem** to be solved as described [here](#). Layer 4 DR 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 default gateway of each Real Server to be the load balancer and supports both one-arm and two-arm configurations. Layer 4 NAT 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. Layer 4 SNAT 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 also enables content switching and header manipulation rules to be implemented. It does not require any changes to the Real Servers and can be deployed in one-arm or two-arm mode. HAProxy is a high performance solution, but since it operates as a full proxy it cannot perform as fast as the layer 4 solutions. Layer 7 SNAT mode is non-transparent by default, i.e. the Real Servers will see the source IP address of the load balancer. This mode can be made transparent through the use of TProxy.

**Our Recommendation**

When load balancing Mach7 Technologies, we recommend that Layer 7 SNAT mode is used. This mode offers high performance with no real server or network changes required since replies go via the same path as the ingress traffic. Using a layer 7 configuration will lose client source IP address transparency. If source IP transparency is required, i.e. if the back end servers *must* see inbound traffic as originating from the client’s true source address, then it is suggested to use either a layer 4 DR or NAT mode configuration. 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 table 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>11112</td>
<td>TCP/DICOM</td>
<td>exchange of images and related information</td>
</tr>
<tr>
<td>6667</td>
<td>TCP/HL7</td>
<td>communication between health-care IT systems</td>
</tr>
<tr>
<td>5104</td>
<td>TCP/DMWL</td>
<td>exchange of patient demographic and related information</td>
</tr>
</tbody>
</table>

**Persistence (Server Affinity)**

Source IP address persistence is used for all virtual services. This ensures that a particular client will connect to the same load balanced server/endpoint for the duration of a session.

**Server Health Checking**
The default health check used for new virtual services is a TCP 'connect to port' check. This verifies that a given port is open and accepting connections. However, it does not necessarily guarantee that the associated service is fully operational. Also, repeated ongoing connections to a service’s 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 then 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 'connect to port' check (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 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:
Note: The WebUI for the VA is shown, the hardware and cloud appliances are very similar. The yellow licensing related message is platform & model dependent.

3. You'll be asked if you want to run the Setup Wizard. If you click Accept the Layer 7 Virtual Service configuration wizard will start. If you want to configure the appliance manually, 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
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 & Server Configuration

Load Balancing Mode

As mentioned in Load Balancing Deployment Modes, Virtual Services can be configured in one of four fundamental ways: Layer 4 DR mode, Layer 4 NAT mode, Layer 4 SNAT mode, and Layer 7 SNAT mode. The following sections illustrate how to configure the Virtual Services using the recommended load balancing mode, Layer 7 SNAT mode. If a different load balancing mode is required for a particular VIP then please don't hesitate to contact our support team at 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 'connect to port' check using the port of the service in question.

Load Balancing VNA DICOM
(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:

3. Enter an appropriate name (Label) for the Virtual Service, e.g. VNA_DICOM.
4. Set the *IP Address* field to the required IP address, e.g. **192.168.0.188**.

5. Set the *Ports* field to the required port(s), e.g. **11112**.

6. Set *Protocol* to **TCP**.

7. Click **Update**.

8. Now click **Modify** next to the newly created Virtual Service.

9. Ensure *Persistence Mode* is set to **Source IP**.

10. Set the *Check Type* to **Connect to port**.

11. 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:

   ![Layer 7 Add a new Real Server - VNA_DICOM

3. Enter an appropriate name (Label) for the first IIS server, e.g. **VNA1**.

4. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.0.41**.

5. Click **Update**.

6. Now repeat for your remaining web nodes (VNA DICOM Nodes).

**Load Balancing HL7**

**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:
3. Enter an appropriate name (Label) for the Virtual Service, e.g. HL7.
4. Set the **IP Address** field to the required IP address, e.g. **192.168.0.189**.
5. Set the **Ports** field to the required port, e.g. **6667**.
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 **Source IP**.
10. Set the **Health Checks** to **Connect to port**.
11. 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. Corepoint1.
4. Change the Real Server IP Address field to the required IP address, e.g. 192.168.86.50.
5. Click Update.
6. Now repeat for your remaining HL7 server(s).

Load Balancing DMWL (DICOM Modality Worklist)

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:
   - Label: DMWL
   - IP Address: 192.168.0.184
   - Ports: 5104
   - Layer 7 Protocol: TCP Mode
3. Enter an appropriate name (Label) for the Virtual Service, e.g. DMWL.
4. Set the IP Address field to the required IP address, e.g. 192.168.0.184.
5. Set the Ports field to the required port, e.g. 5104.
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 Source IP.
10. Set the Health Checks to Connect to port.
11. 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 DMWL server, e.g. MWL1.

4. Change the **Real Server IP Address** field to the required IP address, e.g. 192.168.0.60.

5. Click **Update**.

6. Now repeat for your remaining MWL server(s).

**Restart HAPerx**

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

**Note**

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

**9. Testing & Verification**

**Note**

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

**Using the System Overview**

Verify that all virtual services and their associated real servers are reported as online/healthy (green) as shown below:
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

12. Conclusion
Loadbalancer.org appliances provide a very cost effective and flexible solution for highly available load balanced Mach7 Technologies 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.

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,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Firewall connection tracking table size, NIC offloading, SMTP relay,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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:
Note: If you have already run the firewall lockdown wizard on either appliance, you'll need to ensure that it is temporarily disabled on both appliances whilst performing the pairing process.

1. Deploy a second appliance that will be the Secondary and configure initial network settings.

2. Using the WebUI on the Primary appliance, navigate to: *Cluster Configuration > High-Availability Configuration.*

3. Specify the IP address and the *loadbalancer* user's password for the Secondary (peer) appliance as shown above.

4. Click *Add new node.*

5. The pairing process now commences as shown below:

6. Once complete, the following will be displayed on the Primary appliance:
7. To finalize the configuration, restart heartbeat and any other services as prompted in the blue message box at the top of the screen.

**Note**

Clicking the **Restart Heartbeat** button on the Primary appliance will also automatically restart heartbeat on the Secondary appliance.

**Note**

For more details on configuring HA with 2 appliances, please refer to [Appliance Clustering for HA](#).

**Note**

For details on testing and verifying HA, please refer to [Clustered Pair Diagnostics](#).
## 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>7 October 2020</td>
<td>Initial version</td>
<td></td>
<td>IBG</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.