Load Balancing Hitachi Content Platform

Version 1.1.0
1. About this Brief

This brief outlines the steps required to configure a load balanced Hitachi Content Platform environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Hitachi Content Platform 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 Administration Manual.

2. Loadbalancer.org Appliances Supported

All our products can be used with Hitachi Content Platform. 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. Software Versions Supported

3.1. Loadbalancer.org Appliance

- V8.6.1 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.

3.2. Hitachi Content Platform

- All versions

4. Hitachi Content Platform

Hitachi Content Platform is a massively scalable object storage solution with robust security, high performance, and compliance considerations built-in.

5. Load Balancing Hitachi Content Platform

Note: It’s highly recommended that you have a working Hitachi Content Platform environment first before implementing the load balancer.

5.1. Persistence (aka Server Affinity)

Source IP-based persistence is required for all three services related to HCP. This ensures that clients continue to stick to the same server for the duration of their session.
5.2. Virtual Service (VIP) Requirements
To provide load balancing and HA for Hitachi Content Platform, the following VIPs are required:

- Data (for HTTP and HTTPS-based data requests)
- Metadata Query Engine (MQE)
- Namespace Browser (NSB)

5.3. Port Requirements
The following table shows the ports that are load balanced:

<table>
<thead>
<tr>
<th>Ports</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>80, 443</td>
<td>TCP/HTTP(S)</td>
<td>HTTP(S)-based data access</td>
</tr>
<tr>
<td>8888</td>
<td>TCP</td>
<td>Used for access to the Metadata Query Engine</td>
</tr>
<tr>
<td>8000</td>
<td>TCP/HTTPS</td>
<td>HTTPS-based access for the Namespace Browser</td>
</tr>
</tbody>
</table>

5.4. TLS/SSL Termination
It is possible to terminate TLS connections at the load balancer, however this is outside the scope of this document.

For simplicity and best performance, TLS termination should be performed on the real servers.

6. Deployment Concept

VIPs = Virtual IP Addresses

Note: The load balancer can be deployed as a single unit, although Loadbalancer.org recommends a
7. 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 Hitachi Content Platform, using layer 7 SNAT mode is recommended. This mode is described below and is used for the configurations presented in this guide. For configuring using layer 7 SNAT mode please refer to the section Appliance Configuration for Hitachi Content Platform – Using Layer Layer 7 SNAT Mode.

7.1. 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 corresponding request to the chosen Real Server. As a result, Layer 7 is typically not as fast as the Layer 4 methods. 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.

- Because layer 7 SNAT mode is a full proxy, any server in the cluster can be on any accessible subnet including across the Internet or WAN.

- Layer 7 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 balancer’s 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 load balancer can be configured to provide the actual client IP address to the Real Servers in 2 ways. Either by inserting a header that contains the client’s source IP address, or by modifying the Source Address field of the IP packets and replacing the IP address of the load balancer with the IP address of the client. For more information on these methods please refer to Transparency at Layer 7.
Layer 7 SNAT mode can be deployed using either a one-arm or two-arm configuration. For two-arm deployments, `eth0` is normally used for the internal network and `eth1` is used for the external network although this is not mandatory.

- Requires no mode-specific configuration changes to the load balanced Real Servers.
- Port translation is possible with Layer 7 SNAT mode, e.g. VIP:80 → RIP:8080 is supported.
- You should not use the same RIP:PORT combination for layer 7 SNAT mode VIPs and layer 4 SNAT mode VIPs because the required firewall rules conflict.

## 8. Loadbalancer.org Appliance – the Basics

### 8.1. 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.

### 8.2. 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.

### 8.3. Accessing the Appliance WebUI

The WebUI is accessed using a web browser. By default, users are authenticated using Apache authentication. Users can also be authenticated against LDAP, LDAPS, Active Directory or Radius - for more information, please refer to [External Authentication](#).

- **Note** There are certain differences when accessing the WebUI for the cloud appliances. For details, please refer to the relevant Quick Start / Configuration Guide.
1. Using a browser, navigate to the following URL:


You'll receive a warning about the WebUI’s certificate. This is due to the default self signed certificate that is used. If preferred, you can upload your own certificate - for more information, please refer to Appliance Security Features.

2. Log in to the WebUI using the following credentials:

   **Username**: loadbalancer  
   **Password**: <configured-during-network-setup-wizard>

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

Once logged in, the WebUI will be displayed as shown below:
3. You'll be asked if you want to run the Setup Wizard. Click **Dismiss** if you're following a guide or want to configure the appliance manually. Click **Accept** to start the Setup Wizard.

---

**Main Menu Options**

**System Overview** - Displays a graphical summary of all VIPs, RIPv3s 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 & RIPv3s

**Maintenance** - Perform maintenance tasks such as service restarts and taking backups

**View Configuration** - Display the saved appliance configuration settings

**Reports** - View various appliance reports & graphs

**Logs** - View various appliance logs

**Support** - Create a support download, contact the support team & access useful links
8.4. Appliance Software Update

To ensure that the appliance(s) are running the latest software version, we recommend a software update check is performed.

Determining the Current Software Version

The software version is displayed at the bottom of the WebUI as shown in the example below:

Checking for Updates using Online Update

1. Using the WebUI, navigate to: Maintenance > Software Update.
2. Select Online Update.
3. If the latest version is already installed, a message similar to the following will be displayed:

   **Information:** Version v8.9.0 is the current release. No updates are available

4. If an update is available, you'll be presented with a list of new features, improvements, bug fixes and security related updates.
5. Click Online Update to start the update process.

   **Note** Do not navigate away whilst the update is ongoing, this may cause the update to fail.

6. Once complete (the update can take several minutes depending on download speed and upgrade version) the following message will be displayed:

   **Information:** Update completed successfully.

7. If services need to be reloaded/restarted or the appliance needs a full restart, you'll be prompted accordingly.

Using Offline Update

If the load balancer does not have access to the Internet, offline update can be used.
To perform an offline update:

1. Using the WebUI, navigate to: **Maintenance > Software Update**.
2. Select **Offline Update**.
3. The following screen will be displayed:

   **Software Update**

   **Offline Update**

   The following steps will lead you through offline update:

   1. Contact support@loadbalancer.org to obtain the offline update archive and checksum.
   2. Save the archive and checksum to your local machine.
   3. Select the archive and checksum files in the upload form below.
   4. Click Upload and Install to begin the update process.

   Archive:  
   Choose File  
   No file chosen

   Checksum:  
   Choose File  
   No file chosen

   Upload and Install

4. Select the **Archive** and **Checksum** files.
5. Click **Upload and Install**.
6. If services need to be reloaded/restarted or the appliance needs a full restart, you'll be prompted accordingly.

**8.5. Ports Used by the Appliance**

By default, the appliance uses the following TCP & UDP ports:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>22</td>
<td>SSH</td>
</tr>
<tr>
<td>TCP &amp; UDP</td>
<td>53</td>
<td>DNS</td>
</tr>
<tr>
<td>TCP &amp; UDP</td>
<td>123</td>
<td>NTP</td>
</tr>
<tr>
<td>TCP &amp; UDP</td>
<td>161</td>
<td>SNMP</td>
</tr>
<tr>
<td>UDP</td>
<td>6694</td>
<td>Heartbeat between Primary &amp; Secondary appliances in HA mode</td>
</tr>
<tr>
<td>TCP</td>
<td>7778</td>
<td>HAProxy persistence table replication</td>
</tr>
<tr>
<td>TCP</td>
<td>9080</td>
<td>WebUI - HTTP (disabled by default)</td>
</tr>
<tr>
<td>TCP</td>
<td>9081</td>
<td>Nginx fallback page</td>
</tr>
<tr>
<td>TCP</td>
<td>9443</td>
<td>WebUI - HTTPS</td>
</tr>
</tbody>
</table>
8.6. HA Clustered Pair Configuration
Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary unit is covered in the section Configuring HA - Adding a Secondary Appliance of the appendix.

9. Appliance Configuration for Hitachi Content Platform – Using Layer Layer 7 SNAT Mode

9.1. Configuring VIP 1 – Data

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. HCP-Data.
3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.85.150.
4. Set the Ports field to 80,443.
5. Set the Layer 7 Protocol to TCP Mode.
6. Click Update to create the virtual service.

7. Click Modify next to the newly created VIP.
8. Set Health Checks to Negotiate HTTP (GET).
9. Set Request to send to /node_status.
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. *HCP_Node1*.

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 the remaining HCP nodes.

9.2. Configuring VIP 2 – Metadata Query Engine (MQE)

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. *HCP-MQE*.

3. Set the *Virtual Service IP Address* field to the required IP address, e.g. *192.168.85.150*.

4. Set the *Ports* field to *8888*.

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

6. Click *Update* to create the virtual service.
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. **HCP_Node1**.

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 the remaining HCP nodes.

9.3. Configuring VIP 3 – Namespace Browser (NSB)

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 Server**.

2. Define the **Label** for the virtual service as required, e.g. **HCP-NSB**.

3. Set the **Virtual Service IP Address** field to the required IP address, e.g. **192.168.85.150**.

4. Set the **Ports** field to **8888**.

5. Set the **Layer 7 Protocol** to **TCP Mode**.
6. Click **Update** to create the virtual service.

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

8. Set **Health Checks** to **Negotiate HTTPS (GET)**.

9. Set **Request to send** to `/node_status`

10. 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. **HCB_Node1**.

3. Set the **Real Server IP Address** field to the required IP address, e.g. **192.168.85.200**.

4. Set the **Real Server Port** to **443**.

5. Click **Update**.

6. Repeat these steps to add the remaining HCP nodes.
9.4. Finalizing the Configuration

To apply the new settings, HAProxy must be reloaded. This can be done using the button in the "Commit changes" box at the top of the screen or by using the Restart Services menu option:

1. Using the WebUI, navigate to: Maintenance > Restart Services.
2. Click Reload HAProxy.

9.5. Optional Multi-Site Failover

If an HCP deployment is made up of two unique clusters at two sites, with replication taking place across a multi-site link, it is possible to set up a failover mechanism in the event that one HCP deployment should become unavailable.

For each virtual service in turn:

1. Click Modify next to the VIP in question.
2. Under the Fallback Server section, set the IP Address to the VIP address of the HCP service at the other site, e.g. 192.168.1.1.
3. Ensure that the Port field is empty.
4. Click Update.

10. Testing & Verification

Note: For additional guidance on diagnosing and resolving any issues you may have, please also refer to Diagnostics & Troubleshooting.
10.1. Using System Overview

The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & RIPv (i.e. the HCP nodes) 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 services and all HCP nodes are healthy and available to accept connections:

11. 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.

12. Further Documentation

For additional information, please refer to the Administration Manual.
13. Appendix

13.1. 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 is configured first and 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</td>
<td>All network settings including IP address(es), bonding configuration and VLANs</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Routing</td>
<td>Routing configuration including default gateways and static routes</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>System Date &amp; time</td>
<td>All time and date related settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Physical – Advanced Configuration</td>
<td>Various settings including Internet Proxy, Management Gateway, Firewall connection tracking table size, NIC offloading, SMTP relay, logging and Syslog Server</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Security</td>
<td>Appliance security settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>SNMP Configuration</td>
<td>Appliance SNMP settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Graphing</td>
<td>Appliance graphing settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>License Key</td>
<td>Appliance licensing</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Software Updates</td>
<td>Appliance software update management</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Script</td>
<td>Appliance firewall (iptables) configuration</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Lockdown Wizard</td>
<td>Appliance management lockdown settings</td>
</tr>
</tbody>
</table>
Make sure that if these settings/updates have been configured on the Primary appliance, they're also configured on the Secondary appliance.

Adding a Secondary Appliance - Create an HA 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 in the example 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 "Commit changes" 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>14 July 2022</td>
<td>Initial version</td>
<td></td>
<td>AH</td>
</tr>
<tr>
<td>1.0.1</td>
<td>5 January 2023</td>
<td>Combined software version information into one section&lt;br&gt;Added one level of section numbering&lt;br&gt;Added software update instructions&lt;br&gt;Added table of ports used by the appliance&lt;br&gt;Reworded 'Further Documentation' section</td>
<td>Housekeeping across all documentation</td>
<td>AH</td>
</tr>
<tr>
<td>1.0.2</td>
<td>2 February 2023</td>
<td>Updated screenshots</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td>1.0.3</td>
<td>7 March 2023</td>
<td>Added the section 'Finalizing the Configuration' to ensure HAProxy is explicitly reloaded&lt;br&gt;Removed conclusion section</td>
<td>Provided clarity for reloading HAProxy post-configuration&lt;br&gt;Updates across all documentation</td>
<td>AH</td>
</tr>
<tr>
<td>1.1.0</td>
<td>24 March 2023</td>
<td>New document theme&lt;br&gt;Modified diagram colours</td>
<td>Branding update</td>
<td>AH</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.

Visit us: www.loadbalancer.org
Phone us: +44 (0)330 380 1064
Phone us: +1 833 274 2566
Email us: info@loadbalancer.org
Follow us: @loadbalancer.org