Load Balancing Hyland OnBase

Version 1.2.0
# Table of Contents

1. About this Guide ......................................................... 3
2. Loadbalancer.org Appliances Supported ............................ 3
3. Loadbalancer.org Software Versions Supported .................... 3
4. Hyland OnBase Software Versions Supported ........................ 3
5. Load Balancing Hyland OnBase ....................................... 3
   Load Balancer Deployment Mode ...................................... 3
   Persistence (aka Server Affinity) ...................................... 3
   Timeouts ......................................................................... 3
   Virtual Service (VIP) Requirements .................................... 3
   SSL Offloading ............................................................... 3
   Port Requirements .......................................................... 4
   Health Checks ............................................................... 4
6. Deployment Concept ....................................................... 4
7. Loadbalancer.org Appliance – the Basics ......................... 4
   Virtual Appliance .......................................................... 4
   Initial Network Configuration ........................................... 5
   Accessing the WebUI ...................................................... 5
      Main Menu Options ..................................................... 6
   HA Clustered Pair Configuration ....................................... 7
8. Appliance Configuration for Hyland OnBase ....................... 7
   Web Servers ............................................................... 7
      Configuring VIP 1 – HTTP Virtual Service ....................... 7
      Defining the Real Servers (RIPs) .................................... 7
      Configuring SSL Termination ....................................... 8
   Application Servers ....................................................... 9
   Finalizing the Configuration ............................................. 9
9. Testing & Verification ..................................................... 9
   Using System Overview .................................................. 9
10. Technical Support ......................................................... 9
11. Further Documentation ................................................ 10
12. Conclusion ............................................................... 10
13. Appendix ............................................................... 11
   Configuring HA - Adding a Secondary Appliance .................. 11
14. Document Revision History ........................................... 14
1. About this Guide

This guide details the steps required to configure a load balanced Hyland OnBase environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Hyland OnBase 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 for load balancing Hyland OnBase. For full specifications of available models please refer to https://www.loadbalancer.org/products. Some features may not be supported in all cloud platforms due to platform specific limitations, please check with Loadbalancer.org support for further details.

3. Loadbalancer.org Software Versions Supported

- V8.3.8 and later

4. Hyland OnBase Software Versions Supported

- Hyland OnBase – all versions

5. Load Balancing Hyland OnBase

Note: It's highly recommended that you have a working Hyland OnBase environment first before implementing the load balancer.

Load Balancer Deployment Mode

The load balancer is deployed at Layer 7 This enables cookie based persistence to be used.

Persistence (aka Server Affinity)

The load balancer supports several persistence methods. For Hyland OnBase, both IP or HTTP cookie persistence is supported. In this guide, cookie based persistence is used.

Timeouts

For OnBase, the layer 7 client and server timeouts are set to 20 minutes.

Virtual Service (VIP) Requirements

To provide load balancing and HA for Hyland OnBase, the following VIPs are required:

- Web Server VIP
- Application Server VIP

SSL Offloading

SSL offloading is used on the load balancer to enable HTTP cookies to be inserted.
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>HTTP</td>
<td>Web &amp; Application server HTTP traffic</td>
</tr>
<tr>
<td>443</td>
<td>HTTPS</td>
<td>Web &amp; Application server HTTPS traffic</td>
</tr>
</tbody>
</table>

(*) These ports can be changed if required.

Health Checks
By default, a simple ‘Connect to port’ health check is used by the virtual services described in this guide.

If required, a more comprehensive HTTP or HTTPS negotiate check can be configured to provide a more robust check.

6. 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 Configuring HA - Adding a Secondary Appliance for more details on configuring a clustered pair.

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.
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.

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:
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
8. Appliance Configuration for Hyland OnBase

Web Servers

Configuring VIP 1 – HTTP Virtual Service

Configuring the Virtual Service (VIP)

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

2. Enter an appropriate Label (name) for the VIP, e.g. WebServers.

3. Set the Virtual Service IP address field to the required IP address, e.g. 192.168.10.100.

4. Set the Virtual Service Ports field to 80.

5. Set the Layer 7 Protocol to HTTP Mode.

6. Click Update to create the virtual service.

7. Now click Modify next to the newly created VIP.

8. Under Persistence, click [Advanced] to show more options.

9. Ensure Persistence Mode is set to HTTP Cookie.

10. Set Cookie Max Idle Duration to 60m (60 minutes).

11. Under Other, click [Advanced] to show more options.

12. Enable (check) the Timeout checkbox and set the Client Timeout and Server Timeout to 20m.

13. Click Update.

Defining the Real Servers (RIPs)

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

2. Enter an appropriate Label for the server, e.g. Web1.

3. Change the Real Server IP Address field to the required IP address, e.g. 192.168.10.120.

4. Set the Real Server Port field to 80.

```
Label: Web1
Real Server IP Address: 192.168.10.120
Real Server Port: 80
```

5. Click Update.

6. Repeat these steps to add additional Web servers as required.

**Configuring SSL Termination**

**Upload the Certificate**

*Note* A certificate in either PEM or PFX format can be uploaded to the load balancer.

1. Using the WebUI, navigate to: `Cluster Configuration > SSL Certificates`.

2. Click Add a new SSL Certificate and select Upload prepared PEM/PFX file.

3. Enter a suitable Label for the certificate, e.g. Cert1.

4. Browse to and select the certificate file to upload (PEM or PFX format).

5. Enter the password if applicable.

6. Click Upload Certificate.

**Configure the SSL VIP**

1. Using the WebUI, navigate to: `Cluster Configuration > SSL Termination` and click Add a new Virtual Service.

2. Set the Associated Virtual Service to the appropriate VIP, e.g. WebServers.
3. Leave Virtual Service Port set to 443.


5. Select the required certificate from the SSL Certificate drop-down, e.g. Cert1.

6. Click Update.

Application Servers
Repeat the steps in Web Servers to configure the load balancer for the Application Servers. Change IPs and names as required.

Finalizing the Configuration
To apply the new settings, HAProxy and STunnel must be reloaded:

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

2. Click Reload HAProxy.

3. Click Reload STunnel.

9. 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 Hyland OnBase servers) and shows the state/health of each server as well as the state of the cluster as a whole. This can be used to ensure all servers are up and available.

10. 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
11. Further Documentation


12. Conclusion

Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced Hyland OnBase 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.

**Note**

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

<table>
<thead>
<tr>
<th>WebUI Main Menu Option</th>
<th>Sub Menu Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Configuration</td>
<td>Hostname &amp; DNS</td>
<td>Hostname and DNS settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Network Interface Configuration</td>
<td>All network settings including IP address(es), bonding configuration and VLANs</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Routing</td>
<td>Routing configuration including default gateways and static routes</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>System Date &amp; time</td>
<td>All time and date related settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Physical – Advanced Configuration</td>
<td>Various settings including Internet Proxy, Management Gateway, Firewall connection tracking table size, NIC offloading, SMTP relay, logging and Syslog Server</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Security</td>
<td>Appliance security settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>SNMP Configuration</td>
<td>Appliance SNMP settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Graphing</td>
<td>Appliance graphing settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>License Key</td>
<td>Appliance licensing</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Software Updates</td>
<td>Appliance software update management</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Script</td>
<td>Appliance firewall (iptables) configuration</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Lockdown Wizard</td>
<td>Appliance management lockdown settings</td>
</tr>
</tbody>
</table>

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](#).
## 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>1.1.0</td>
<td>9 September 2019</td>
<td>Styling and layout</td>
<td>General styling updates</td>
<td>AH</td>
</tr>
<tr>
<td>1.1.1</td>
<td>28 August 2020</td>
<td>New title page</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated Canadian contact details</td>
<td>Change to Canadian contact details</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Amended instructions for setting persistence and timeout options</td>
<td>Changes to the appliance WebUI</td>
<td></td>
</tr>
<tr>
<td>1.2.0</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.