Load Balancing Oracle Application Server

Version 1.5.0

Table of Contents

1. About this Guide

This guide provides a quick reference for setting up Oracle HTTP Server (OHS) load balancing using Loadbalancer.org appliances.

2. Loadbalancer.org Appliances Supported

All our products can be used with OHS. 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

- v8.3.8 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. Oracle HTTP Server

- v12 and later

4. Related Documentation

For additional information, please refer to the Administration Manual and the relevant Quick Start / Configuration Guide.

5. Oracle HTTP Server

Oracle HTTP Server is the web server component for Oracle Fusion Middleware. It provides a listener for Oracle WebLogic Server and the framework for hosting static pages, dynamic pages, and applications over the Web.

6. Load Balanced Ports / Services

By default Oracle HTTP Server listens on TCP port 7777 and HTTPS is disabled.

Port	Protocol
7777	HTTP

🔒 Note	The Virtual Service on the load balancer is configured to listen on port 80 and uses port

7. Appliance Configuration Overview

7.1. Operation Mode

The load balancer is configured using single-arm layer 7 SNAT mode. This mode does not require any mode specific configuration changes to the load balanced Real Servers. HTTP cookie persistence is used to ensure clients connect to the same OHS for the duration of their session.
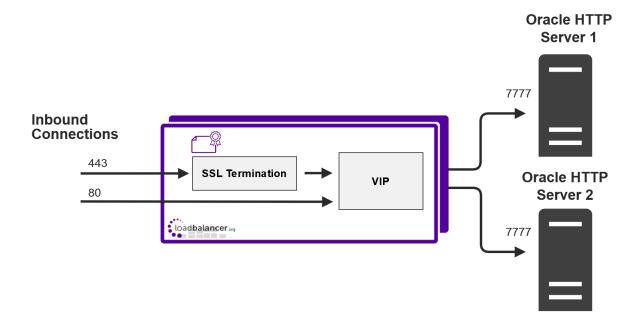
7.2. SSL Termination

SSL Termination is configured on the load balancer. This provides a corresponding HTTPS Virtual Service on port 443. Decrypted traffic is then load balanced and forwarded to the HTTP servers on port 7777.

7.3. OHS Health checks

A HTTP negotiate health-check is used to verify that each Oracle HTTP Server is available.

7.4. Deployment Concept

Once the load balancer is deployed, clients connect to the Virtual Service (VIP) on the load balancer rather than directly to one of the Oracle HTTP Servers.

8. Deploying & Accessing the Appliance

8.1. Deployment

Deploy the Loadbalancer.org appliance as described in the relevant Quick Start / Configuration Guide.

8.2. 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.

> 🔒 **Note** A number of compatibility issues have been found with various versions of Microsoft Internet Explorer and Edge. The WebUI has been tested and verified using both Chrome & Firefox.

1. Using a browser, navigate to the following URL:

   https://<IP-address-configured-during-the-network-setup-wizard>:9443/lbadmin/

   > 🔒 **Note** 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:

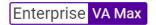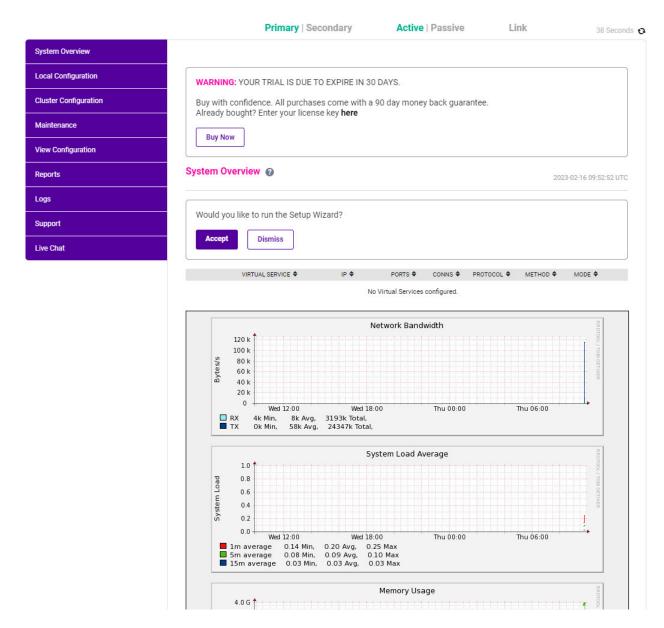   **Username**: loadbalancer
   Password: <configured-during-network-setup-wizard>

   > 🔒 **Note** 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.

> 🔒 **Note**   The Setup Wizard can only be used to configure Layer 7 services.

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

Support - Create a support download, contact the support team & access useful links

Live Chat - Start a live chat session with one of our Support Engineers

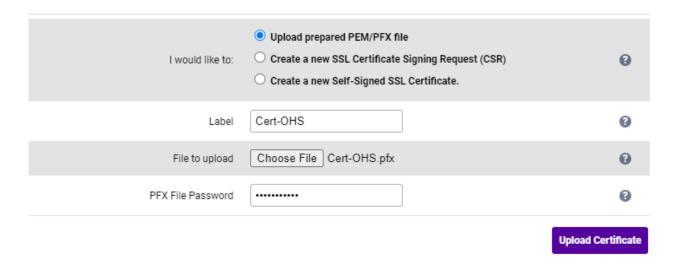# 9. Configuration Steps

9.1. Appliance Configuration

Upload the SSL Certificate

Certificates in either PEM or PFX format can be uploaded.

To upload an SSL certificate:
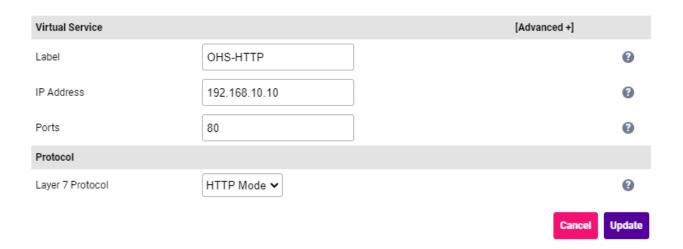
1. Using the WebUI, navigate to *Cluster Configuration > SSL Certificate* and click **Add a new SSL Certificate**.

2. Select the option **Upload prepared PEM/PFX file**.

3. Enter the following details:

I would like to:	⦿ Upload prepared PEM/PFX file ◯ Create a new SSL Certificate Signing Request (CSR) ◯ Create a new Self-Signed SSL Certificate.
Label	Cert-OHS
File to upload	Choose File Cert-OHS.pfx
PFX File Password	••••••••••

Upload Certificate
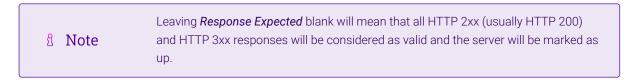
4. Specify an appropriate *Label*, e.g. **Cert-OHS**.

5. Click **Choose File**.

6. Browse to and select the relevant PEM or PFX file.

7. For PFX files specify the password if required.

8. Click **Upload Certificate**.

Configure the Virtual Service (VIP)

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

2. Enter the following details:

Virtual Service		[Advanced +]	
Label	OHS-HTTP		❓
IP Address	192.168.10.10		❓
Ports	80		❓
Protocol			
Layer 7 Protocol	HTTP Mode ⌄		❓

<div align="right">

Cancel　Update

</div>

3. Enter an appropriate label for the VIP, e.g. **OHS-HTTP**.

4. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.10.10**.

5. Set the *Virtual Service Ports* field to **80**.

6. Click **Update**.

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

8. Scroll to the **Health Checks** section and click **[Advanced]**.

    ▪ Set *Health Checks* to **Negotiate HTTP (GET)**.

    ▪ Leave *Request to Send* blank.

    ▪ Leave *Response Expected* blank.

    > 🔓 **Note**　Leaving *Response Expected* blank will mean that all HTTP 2xx (usually HTTP 200) and HTTP 3xx responses will be considered as valid and the server will be marked as up.
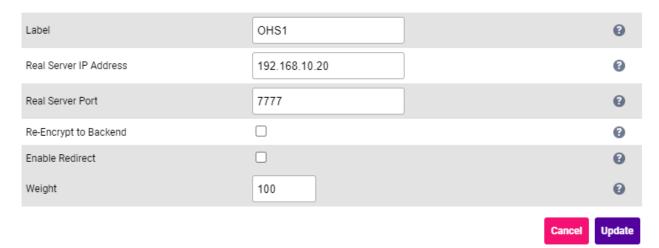
    ▪ Set *Check Port* to **7777**.

9. Scroll to the **Other** section and click **[Advanced]**.

    ▪ Enable (check) the *Timeout* check box and set the *Client Timeout* and *Real Server Timeout* to **30m**.

10. Click **Update**.

Define the Real Servers (RIPs)

The Real Servers (i.e. the Oracle HTTP servers) must now be associated with the VIP.
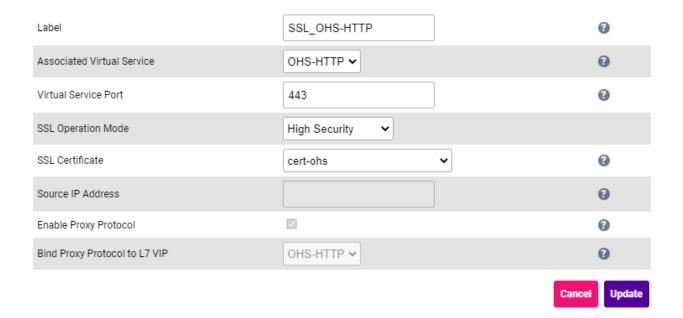
1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a new Real Server** next to the newly created VIP.

2. Enter the following details:

Label	OHS1	
Real Server IP Address	192.168.10.20	
Real Server Port	7777	
Re-Encrypt to Backend	☐	
Enable Redirect	☐	
Weight	100	

Cancel Update

3. Enter an appropriate label for the RIP, e.g. **OHS1**.

4. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.10.20**.

5. Change the *Real Server Port* field to **7777**.

6. Click **Update**.

7. Repeat the above steps to add your other OHS Server(s).

Configure SSL Termination

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

2. Enter the following details:

Label	SSL_OHS-HTTP	
Associated Virtual Service	OHS-HTTP ▾	
Virtual Service Port	443	
SSL Operation Mode	High Security ▾	
SSL Certificate	cert-ohs ▾	
Source IP Address		
Enable Proxy Protocol	☑	
Bind Proxy Protocol to L7 VIP	OHS-HTTP ▾	

Cancel Update

3. Using the *Associated Virtual Service* drop-down, select the Virtual Service created above, e.g. **OHS-HTTP**.

> 🔒 **Note**   Once the VIP is selected, the *Label* field will be auto-populated with **SSL-OHS-HTTP**. This can be changed if preferred.

4. Ensure that the *Virtual Service Port* is set to **443**.

5. Leave *SSL Operation Mode* set to **High Security**.

6. Select the *SSL Certificate* uploaded previously.

7. Click **Update**.

9.2. Oracle HTTP Server Configuration

Follow the steps in the section "Terminating SSL at the Load Balancer" in this Oracle article.

10. Finalizing the Configuration

To apply the new settings, HAProxy and STunnel must be reloaded. This can be done using the buttons 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**.

3. Click **Reload STunnel**.

11. Testing & Verification

Verify that users can can connect to the Virtual Service using both HTTP and HTTPS and can access the load balanced Oracle HTTP Servers.

12. Loadbalancer.org 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.

12.1. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.3.0	5 November 2019	Styling and layout	General styling updates	AH
1.3.1	28 August 2020	New title page Updated Canadian contact details Amended instructions for configuring the persistence timeout	Branding update Change to Canadian contact details Changes to the appliance WebUI	AH
1.4.0	1 September 2022	Converted the document to AsciiDoc Updated links and instructions where necessary	Move to new documentation system Required updates	AH
1.4.1	28 September 2022	Updated layer 7 VIP and RIP creation screenshots	Reflect changes in the web user interface	AH
1.4.2	5 January 2023	Added one level of section numbering	Housekeeping across all documentation	AH
1.4.3	2 February 2023	Updated screenshots	Branding update	AH
1.4.4	8 March 2023	Changed the configuration to utilize SSL termination on the load balancer	Oracle recommended method	RJC
1.4.5	14 March 2023	Improved document structure	Document standardization	RJC
1.5.0	24 March 2023	New document theme Modified diagram colours	Branding update	AH

LOADBALANCER

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.