LOADBALANCER

DEPLOYMENT GUIDE

Load Balancing Oracle WebLogic Server

Version 1.1.0

Table of Contents

1. About this Guide

This guide details the steps required to configure a load balanced Oracle WebLogic Server environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Oracle WebLogic Server 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 Oracle WebLogic Server. For full specifications of available models please refer to https://www.loadbalancer.org/products/enterprise.

Some features may not be available or fully supported in all cloud platforms due to platform specific limitations. For more details, please refer to the "Main Differences to our Standard (Non-Cloud) Product" section in the appropriate cloud platform Quick Start Guide or check with Loadbalancer.org support.

3. Software Versions Supported

3.1. Loadbalancer.org Appliance

- V8.9.1 and later

> **Note** The screenshots used throughout this document aim to track the latest Loadbalancer.org software version. If you're using an older version, or the very latest, the screenshots presented here may not match your WebUI exactly.

3.2. Oracle WebLogic Server

- WebLogic Server 12cR1 and later

4. Oracle WebLogic Server

Oracle WebLogic Server is an application server designed for developing and deploying Java Enterprise Edition (EE) and Jakarta EE applications. While it can be used as a web server in its own right, it is better suited for hosting dynamic applications. This generally means it will sit behind another web server, e.g. OHS, Apache, Nginx, or IIS.

5. Load Balancing Oracle WebLogic Server

> **Note** It's highly recommended that you have a working Oracle WebLogic Server environment first before implementing the load balancer.

5.1. Persistence (aka Server Affinity)

HTTP cookie persistence is used to ensure that a given client connection sticks to the same web server. This is the default setting for HTTP mode virtual services at layer 7.

5.2. Virtual Service (VIP) Requirements

To provide load balancing and HA for Oracle WebLogic Server, a single VIP is required:

- HTTP

In addition, a TLS/SSL termination service is required to allow clients to connect using HTTPS.

5.3. Port Requirements

The following table shows the ports that are load balanced:

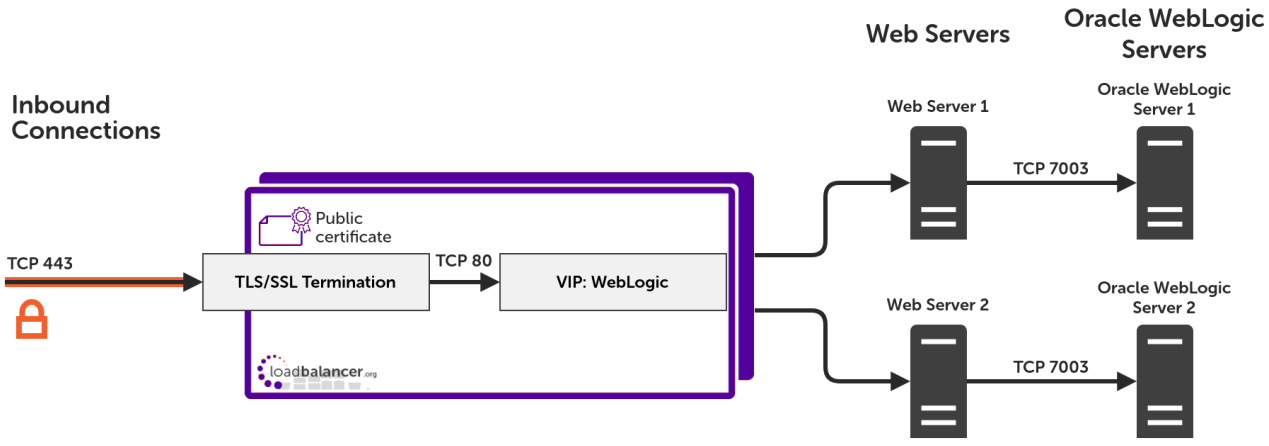
Port	Protocols	Use
80	TCP/HTTP	Client HTTP Traffic
443	TCP/HTTPS	Client HTTP Secure Traffic (Configured for TLS/SSL Termination, Not Strictly Load Balanced)

5.4. TLS/SSL Termination

TLS/SSL connections must be terminated by the load balancer. This allows HTTP header manipulation to take place, which is required in order for Oracle WebLogic Server to be correctly load balanced.

Instructions on how to configure a TLS/SSL termination service are given in the 'Appliance Configuration' section.

6. Deployment Concept



> **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 the section Configuring HA - Adding a Secondary Appliance in the appendix for more details on configuring a clustered pair.

By default, Oracle WebLogic, along with any hosted Java EE / Jakarta EE applications, will not be aware that an inbound client connection used TLS/SSL. This is because all calls to `HttpServletRequest.isSecure()` return "false".

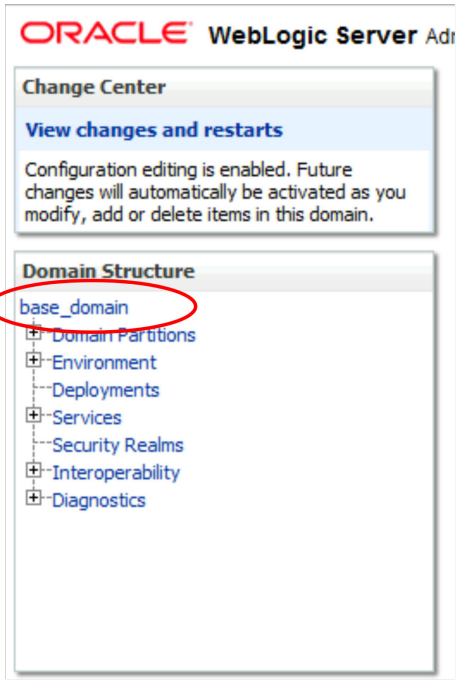
The solution to this issue is to inform the WebLogic server that it is running behind a proxy server. This is done by enabling the ***WebLogic Plugin***. This will, among other things, prompt WebLogic to look for certain HTTP request headers: in particular, a header field named `WL-Proxy-SSL`. The load balancer needs to add this header to client HTTP requests, ensuring that the header is present on connections that are sent to the backend servers.

7. Configuring Oracle WebLogic Server for Load Balancing

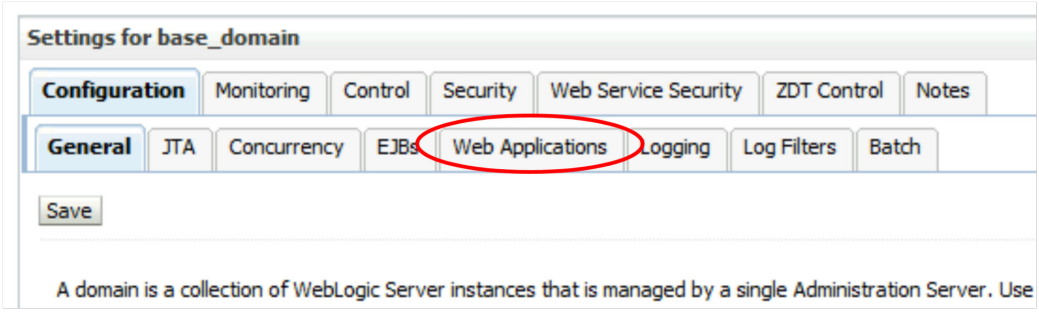
The ***WebLogic Plugin*** must be enabled for WebLogic servers to be correctly load balanced. To do this:

1. Log in to the WebLogic Console (http://<ip_address>:7001/console/) as the `weblogic` user.

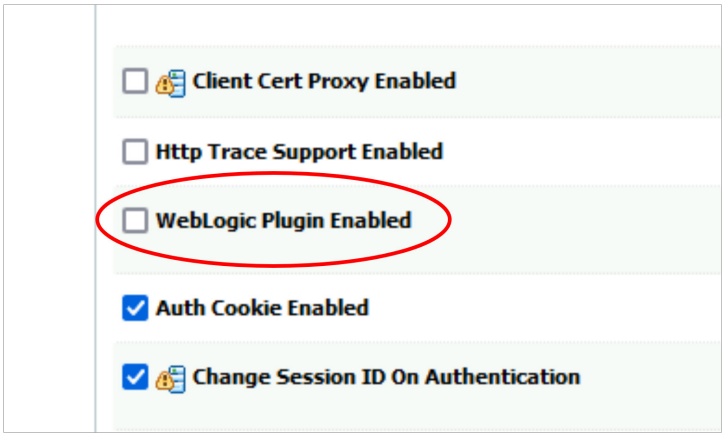
2. On the left hand side of the admin console, select your base domain.



3. In the main console window, select ***Configuration > Web Applications***.



4. Scroll down in the console window and find **WebLogic Plugin Enabled**. Tick the checkbox to enable the WebLogic Plugin at the domain level.



5. Scroll down to the very bottom of the console window and click **Save**. This will apply the setting server-wide and will not require a restart of WebLogic server.

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 servers and other network and administrative 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:

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

   > **Note** You'll receive a warning about the WebUI's SSL 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.

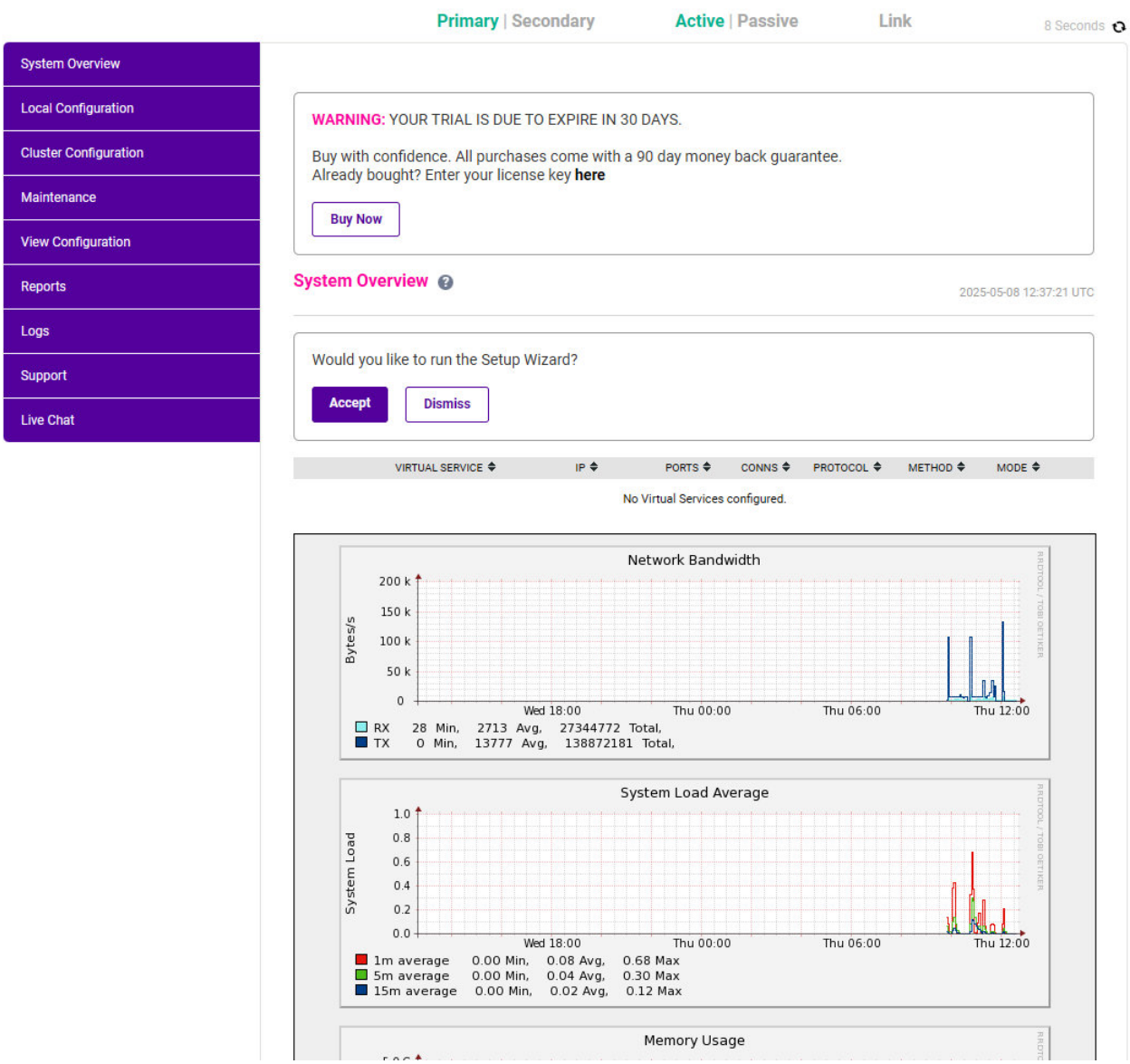
   > **Note** If you need to change the port, IP address or protocol that the WebUI listens on, please refer to Service Socket Addresses.

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.

8.3.1. 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 creating 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

8.4. Appliance Software Update

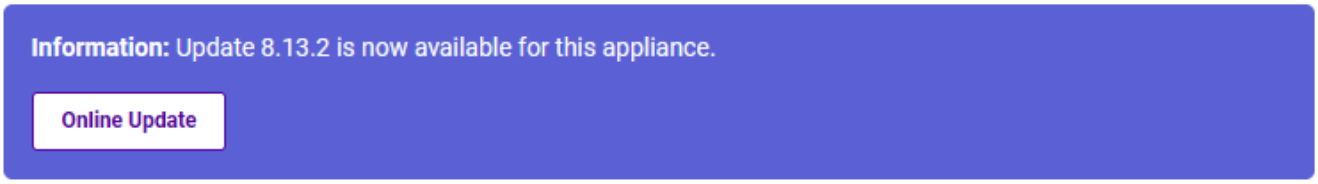
We recommend that the appliance is kept up to date to ensure that you benefit from the latest bug fixes, security updates and feature improvements. Both online and offline update are supported.

> **Note** For full details, please refer to Appliance Software Update in the Administration Manual.

> **Note** Services may need to be restarted/reloaded after the update process completes or in some cases a full appliance restart may be required. We therefore recommend performing the update during a maintenance window.

8.4.1. Online Update

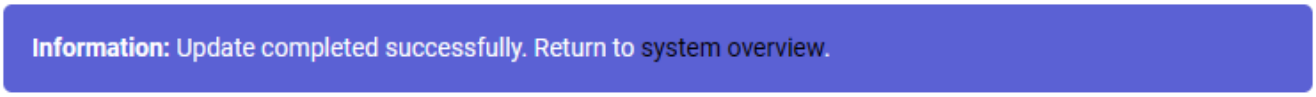
The appliance periodically contacts the Loadbalancer.org update server (**update.loadbalancer.org**) and checks for updates. This is the default behavior and can be disabled if preferred. If an update is found, a notification similar to the example below will be displayed at the top of the WebUI:



Click **Online Update**. A summary of all new features, improvements, bug fixes and security updates included in the update will be displayed. Click **Update** at the bottom of the page to start the update process.

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

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



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

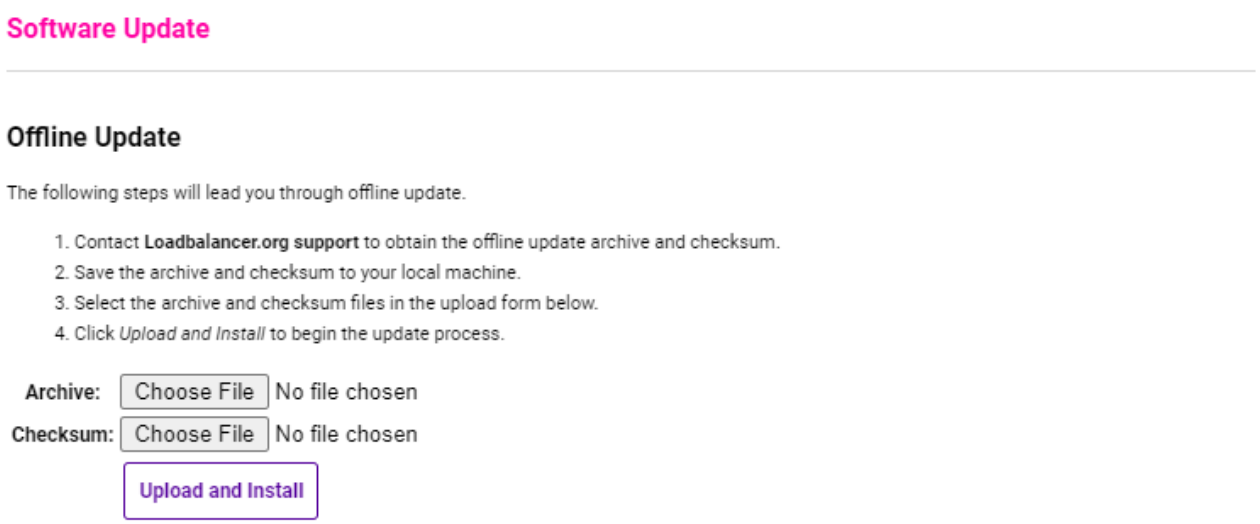
8.4.2. Offline Update

If the appliance does not have access to the Internet, offline update can be used.

To check for the latest version, please refer to our product roadmap page available here. To obtain the latest offline update files contact support@loadbalancer.org.

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:



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:

Protocol	Port	Purpose
TCP	22 *	SSH
TCP & UDP	53 *	DNS / GSLB
TCP & UDP	123	NTP
TCP & UDP	161 *	SNMP
UDP	6694	Heartbeat between Primary & Secondary appliances in HA mode
TCP	7778	HAProxy persistence table replication
TCP	9000 *	Gateway service (Centralized/Portal Management)
TCP	9080 *	WebUI - HTTP (disabled by default)
TCP	9081 *	Nginx fallback page
TCP	9443 *	WebUI - HTTPS
TCP	25565 *	Shuttle service (Centralized/Portal Management)

> **Note** The ports used for SSH, GSLB, SNMP, the WebUI, the fallback page, the gateway service and the shuttle service can be changed if required. For more information, please refer to Service Socket

Addresses.

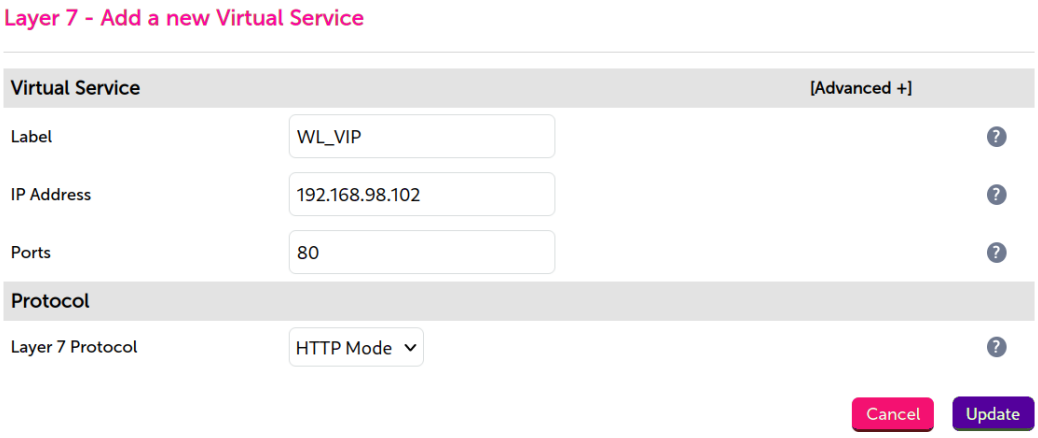
8.6. HA Clustered Pair Configuration

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.

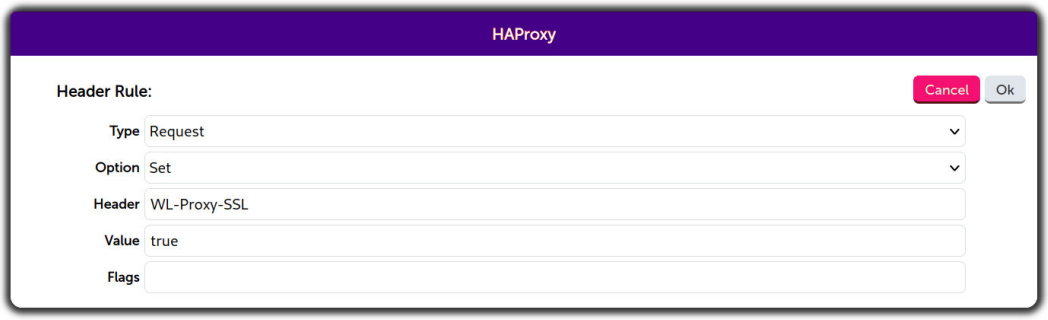
9. Appliance Configuration for Oracle WebLogic Server – Using Layer 7 SNAT Mode

9.1. 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. **WL_VIP**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.98.102**.
4. Set the *Ports* field to **80**.
5. Set the *Layer 7 Protocol* to **HTTP Mode**.
6. Click **Update** to create the virtual service.



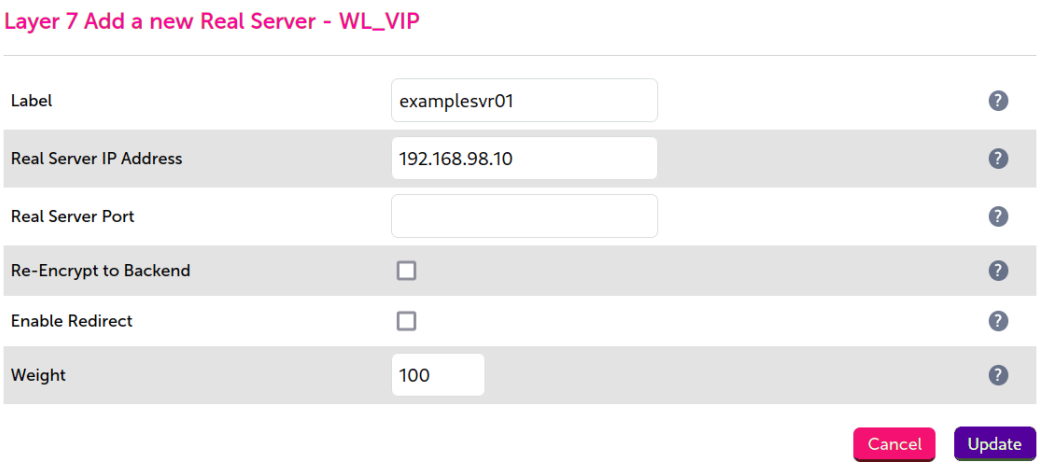
7. Click **Modify** next to the newly created VIP.
8. Under *Header Rules* click **Add Rule**.
9. Set *Type* to **Request**.
10. Set *Option* to **Set**.
11. Set *Header* to **WL-Proxy-SSL**.
12. Set *Value* to **true**.



13. Click **Ok** to add the header rule.
14. Click **Update**.

9.2. 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. **examplesvr01**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.98.10**.
4. Click **Update**.
5. Repeat these steps to add additional servers as required.



9.3. Setting Up the TLS/SSL Termination

9.3.1. Uploading the Certificate

The appropriate certificate for the service in question must be uploaded to the load balancer for TLS/SSL termination to work. The process for doing this is as follows:

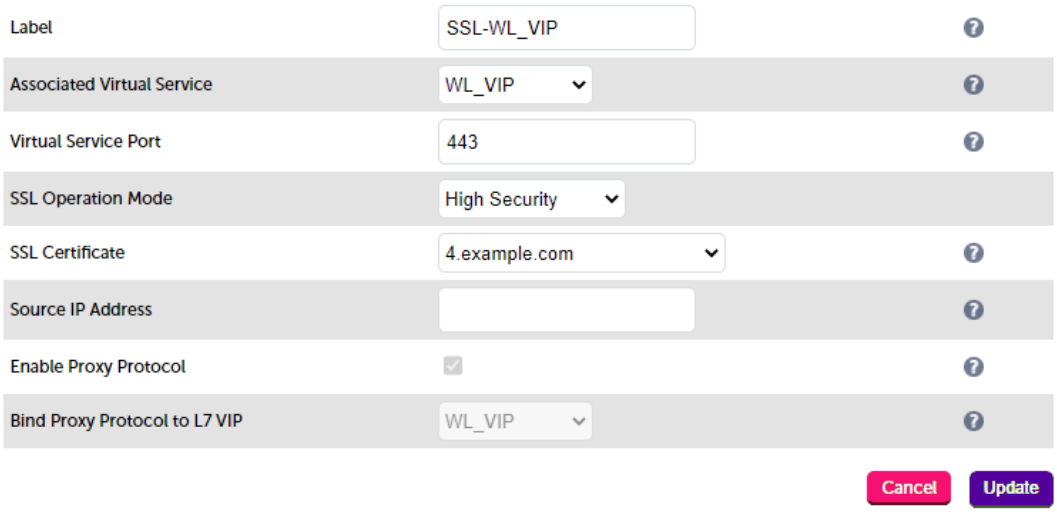
1. Using the web user interface, navigate to *Cluster Configuration > SSL Certificate* and click on **Add a new SSL Certificate**.
2. Press the *Upload prepared PEM/PFX file* radio button.
3. Define the *Label* for the certificate as required. It may make sense to use the domain that the certificate is associated to, e.g. **4.example.com**.

4. Click on **Browse** and select the appropriate PEM or PFX style certificate.
5. If uploading a PFX certificate, enter the certificate's password in the ***PFX File Password*** field.
6. Click **Upload certificate**.

For more information on creating PEM certificate files and converting between certificate formats please refer to Creating a PEM File.

9.3.2. Creating the TLS/SSL Termination

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



2. Using the ***Associated Virtual Service*** drop-down, select the Virtual Service created above, e.g. **WL_VIP**.

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

3. Leave ***Virtual Service Port*** set to **443**.
4. Leave ***SSL Operation Mode*** set to **High Security**.
5. Select the ***SSL Certificate*** uploaded previously, e.g. **4.example.com**.
6. Click **Update**.

9.4. Finalizing the Configuration

To apply the new settings, HAProxy and STunnel must both 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:

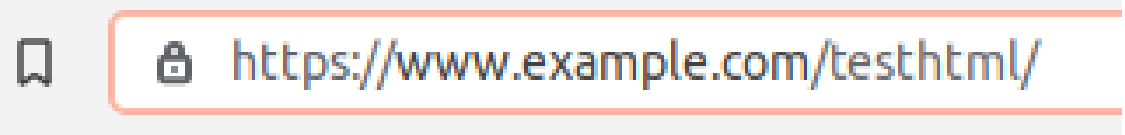
1. Using the WebUI, navigate to: ***Maintenance > Restart Services***.
2. Click **Reload HAProxy**.
3. Click **Reload STunnel**.

10. Testing & Verification

> **Note** For additional guidance on diagnosing and resolving any issues you may have, please also refer to Diagnostics & Troubleshooting.

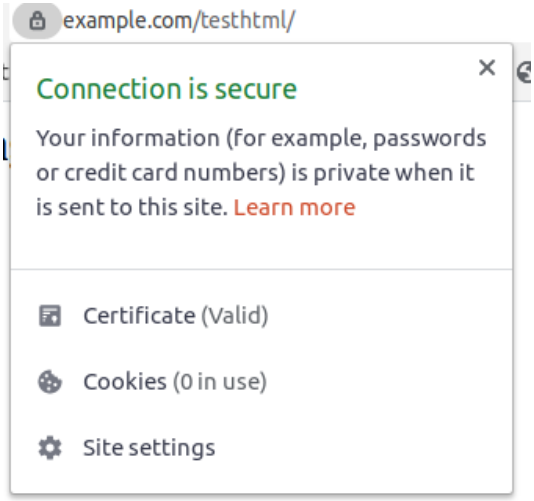
10.1. Using the Load Balanced Service

Use the URL associated to the virtual service to test connecting via a web browser, e.g. https://www.example.com/testhtml



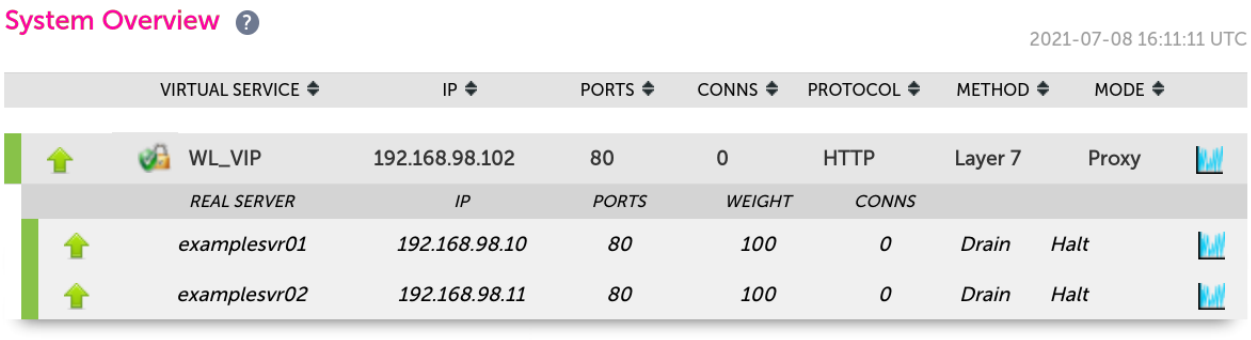
> **Note** It may be necessary to create a host entry for this test to work, if host name resolution using DNS is not possible.

Ensure that the connection is deemed to be "secure" by the browser:



10.2. Using System Overview

The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & RIPs (i.e. the web servers) and shows the state/health of each server as well as the state of the cluster as a whole. The example below shows that both web servers 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 fully configured first, then the Secondary appliance can be added to create an HA pair. Once the HA pair is configured, load balanced services must be configured and modified on the Primary appliance. The Secondary appliance will be automatically kept in sync.

> **Note** For Enterprise Azure, the HA pair should be configured first. For more information, please refer to the Azure Quick Start/Configuration Guide available in the documentation library

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.

13.1.1. 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:

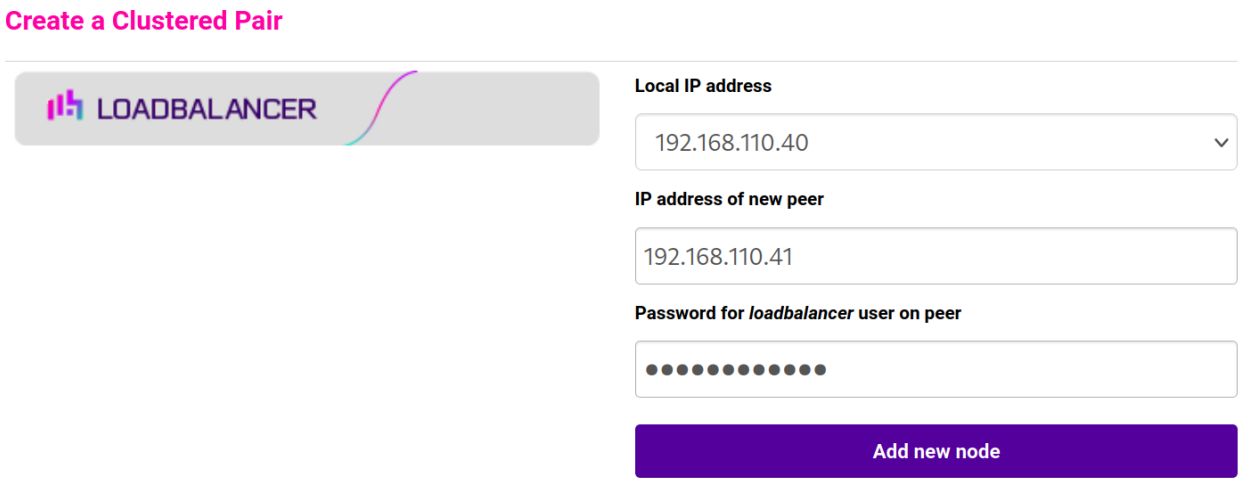
WebUI Main Menu Option	Sub Menu Option	Description
Local Configuration	Hostname & DNS	Hostname and DNS settings
Local Configuration	Network Interface Configuration	Interface IP addresses, bonding configuration and VLANs
Local Configuration	Routing	Default gateways and static routes
Local Configuration	System Date & time	Time and date related settings
Local Configuration	Physical – Advanced Configuration	Various appliance settings
Local Configuration	Portal Management	Portal management settings
Local Configuration	Security	Security settings
Local Configuration	SNMP Configuration	SNMP settings
Local Configuration	Graphing	Graphing settings
Local Configuration	License Key	Appliance licensing
Maintenance	Backup & Restore	Local XML backups
Maintenance	Software Updates	Appliance software updates
Maintenance	Firewall Script	Firewall (iptables) configuration
Maintenance	Firewall Lockdown Wizard	Appliance management lockdown settings

> **Important** Make sure that where any of the above have been configured on the Primary appliance, they're also configured on the Secondary.

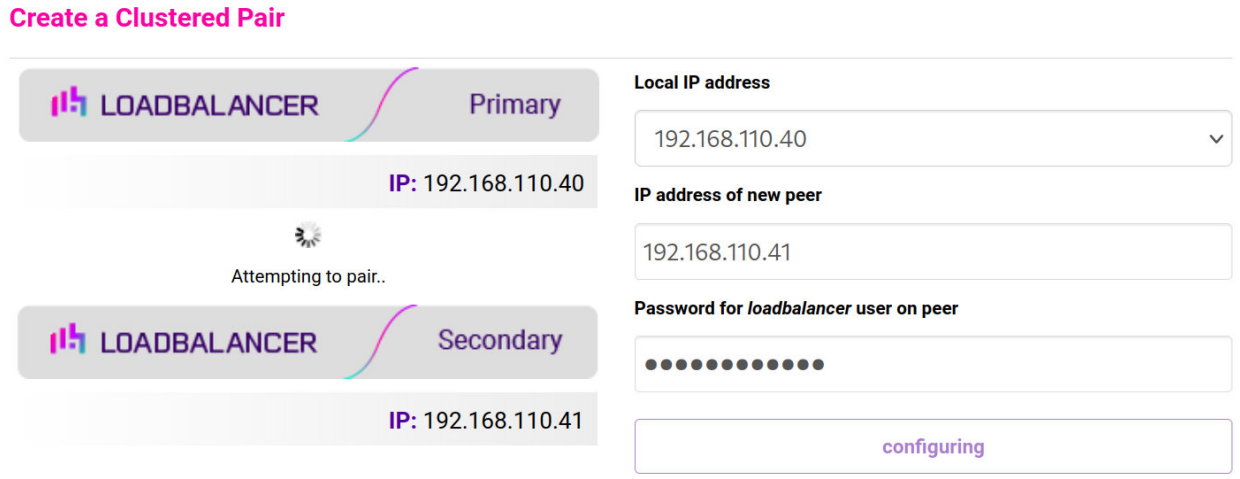
13.1.2. Configuring the HA Clustered Pair

> **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.

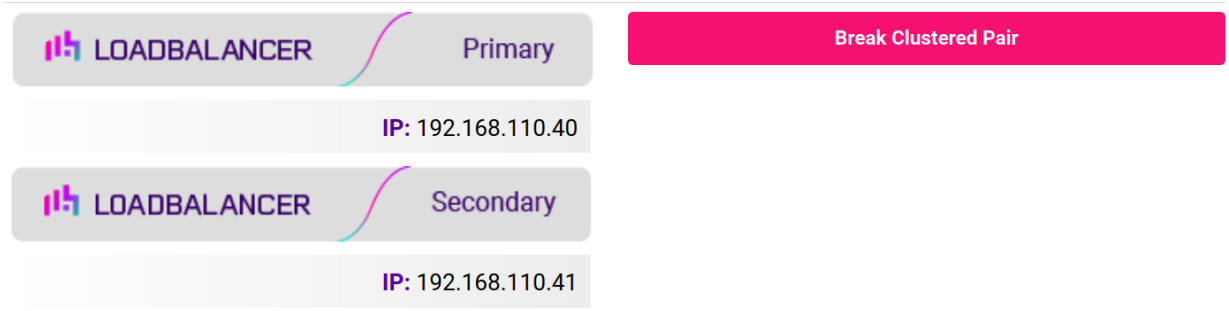
1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI on the Primary appliance, navigate to: *Cluster Configuration > High-Availability Configuration*.



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

Version	Date	Change	Reason for Change	Changed By
1.0.0	9 July 2021	Initial version		DT, AH
1.0.1	13 April 2022	Updated HTTP header manipulation instructions	Changes to the appliance WebUI	AH
1.0.2	26 April 2022	Updated SSL related content to reflect latest software version	New software release	RJC
1.0.3	28 September 2022	Updated layer 7 VIP and RIP creation screenshots	Reflect changes in the web user interface	AH
1.0.4	5 January 2023	Combined software version information into one section Added one level of section numbering Added software update instructions Added table of ports used by the appliance Reworded 'Further Documentation' section Removed references to the colour of certain UI elements	Housekeeping across all documentation	AH
1.0.5	2 February 2023	Updated screenshots	Branding update	AH
1.0.6	7 March 2023	Removed conclusion section	Updates across all documentation	AH
1.1.0	24 March 2023	New document theme Modified diagram colours	Branding update	AH

LOADBALANCER

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

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.