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.

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

- V8.6 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. Oracle WebLogic Server Software Versions Supported

- Oracle WebLogic Server – WebLogic Server 12cR1 and later

5. 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.

6. 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.

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.

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.
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>TCP/HTTP</td>
<td>Client HTTP Traffic</td>
</tr>
<tr>
<td>443</td>
<td>TCP/HTTPS</td>
<td>Client HTTP Secure Traffic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Configured for TLS/SSL Termination, Not Strictly Load Balanced)</td>
</tr>
</tbody>
</table>

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.

7. Deployment Concept

VIPs = Virtual IP Addresses

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.

8. 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.

9. 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.

Note

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
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

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.

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

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.


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.

**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.

---

**Layer 7 Add a new Real Server - WL_VIP**

<table>
<thead>
<tr>
<th>Label</th>
<th>examplesvr01</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.98.10</td>
</tr>
<tr>
<td>Real Server Port</td>
<td></td>
</tr>
<tr>
<td>Re-Encrypt to Backend</td>
<td>☐</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

---

**Setting Up the TLS/SSL Termination**

**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.

Creating the TLS/SSL Termination

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

   ![Virtual Service Configuration Form]

   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.


5. Select the SSL Certificate uploaded previously, e.g. 4.example.com.

6. Click Update.

Finalizing the Configuration

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

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

### 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:

### 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:
12. 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.

13. Further Documentation

14. Conclusion
Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced Oracle WebLogic Server environments.
15. 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, 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>

**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.

![Create a Clustered Pair](image)

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:

![Pairing Process](image)

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**.
## 16. 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>9 July 2021</td>
<td>Initial version</td>
<td></td>
<td>DT, AH</td>
</tr>
<tr>
<td>1.0.1</td>
<td>13 April 2022</td>
<td>Updated HTTP header manipulation instructions</td>
<td>Changes to the appliance WebUI</td>
<td>AH</td>
</tr>
<tr>
<td>1.0.2</td>
<td>26 April 2022</td>
<td>Updated SSL related content to reflect latest software version</td>
<td>New software release</td>
<td>RJC</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.