



Load Balancing Microsoft Sharepoint 2010 / 2013

Version 1.7.1

Table of Contents

1. About this Guide	4
2. Loadbalancer.org Appliances Supported	4
3. Loadbalancer.org Software Versions Supported	4
4. Microsoft Sharepoint Software Versions Supported	4
5. Microsoft Sharepoint	4
Server Roles	4
Installation Options	4
Farm Size & Topology	5
6. Load Balancing Sharepoint	5
Load Balancer Deployment Mode	6
The Basics	6
TCP Ports	6
Persistence (aka Server Affinity)	6
Sharepoint 2010	6
Sharepoint 2013	7
Load Balancer Virtual Service (VIP) Requirements	7
7. Lab Deployment Architecture	7
Lab Environment Notes	8
Planning for High Availability	8
8. Sharepoint Installation & Configuration	9
Installation Considerations	9
Central Administration Website	9
Alternate Access Mappings/Zones	9
Authentication	9
SSL Certificates	9
Service Applications	10
DNS Configuration	10
Lab Environment Installation	10
Site & Zone Structure	10
Installation Steps	10
Accessing Sharepoint	13
9. Loadbalancer.org Appliance – the Basics	13
Virtual Appliance	13
Initial Network Configuration	13
Accessing the WebUI	13
Main Menu Options	15
HA Clustered Pair Configuration	16
10. Appliance Configuration for Sharepoint	16
STEP 1 – Configure Layer 7 Global Settings	16
STEP 2 – Configure the Load Balanced Central Admin Site	16
Create the Virtual Service (VIP)	16
Define the Real Servers (RIPs)	17
STEP 3 – Configure the Load Balanced User Portal Site	18
Create the Virtual Service (VIP)	18
Define the Real Servers (RIPs)	19
STEP 4 – Finalizing the Configuration	19
11. Testing & Verification	19
12. Technical Support	20
13. Further Documentation	20

14. Conclusion	20
15. Appendix	21
Configuring HA - Adding a Secondary Appliance.....	21
Non-Replicated Settings	21
Configuring an HTTP to HTTPS Redirect for the User Portal.....	23
16. Document Revision History	24

1. About this Guide

This guide details the steps required to configure a load balanced Microsoft Sharepoint 2010/2013 environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Microsoft Sharepoint 2010/2013 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 Sharepoint. 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 details.

3. Loadbalancer.org Software Versions Supported

- 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.

4. Microsoft Sharepoint Software Versions Supported

- Microsoft Sharepoint 2010 – all versions
- Microsoft Sharepoint 2013 – all versions

5. Microsoft Sharepoint

Microsoft Sharepoint is Microsoft's enterprise collaboration platform. Sharepoint makes it easier for people to work together. Using Sharepoint, staff can set up web sites to share information with others, manage documents from start to finish, publish reports to help everyone make better decisions and search across a range of internal and external data sources to find answers and information more quickly and effectively.

Server Roles

In Sharepoint 2010 & 2013 there are effectively three server roles – *Web Frontend Servers*, *Application Servers* and *Database Servers*. With Sharepoint 2013, there is flexibility in the architecture because certain underlying components and services can be distributed and shared between servers in the farm depending on server performance, topology requirements, anticipated user load etc.

Installation Options

The Sharepoint installation supports two options as described in the table below:

Option	Description
Standalone	Installs all components on a single machine including SQL Express, but servers cannot be added to a server farm, typically only used for trialling the product or for very small deployments.
Complete	Installs all components (except SQL Express) and allows servers to be added to a farm – this option must always be used in a Farm environment.

Farm Size & Topology

The physical architecture is typically described in two ways: by its size and by its topology. Size, which can be measured in several ways, such as the number of users or the number of documents, is used to categorize a farm as small, medium, or large. Topology uses the idea of tiers or server groups to define a logical arrangement of farm servers. Microsoft uses the following definitions for size and topology:

Farm Size:

Size	Description
Small	A small server farm typically consists of at least two Web servers and a database server.
Medium	A medium server farm typically consists of two or more Web servers, two application servers, and more than one database server.
Large	A large server farm can be the logical result of scaling out a medium farm to meet capacity and performance requirements or by design before a Sharepoint Server solution is implemented.

Farm Topology:

Topology	Description
Single-Tier	In a single-tier deployment, Sharepoint Server and the database server are installed on one computer.
Two-Tier	In a two-tier deployment, Sharepoint Server components and the database are installed on separate servers.
Three-Tier	In a three-tier deployment, the front-end Web servers are on the first tier, the application servers are on the second tier, which is known as the application tier, and the database server is located on the third tier.

For more information on installing and configuring Sharepoint please refer to: <https://technet.microsoft.com/en-us/library/ee667264.aspx>

For more information on building a 3-tier farm, please refer to the following URL: <https://docs.microsoft.com/en-us/sharepoint/administration/configure-sharepoint-server-2013-in-a-three-tier-farm>

6. Load Balancing Sharepoint

Note

It's highly recommended that you have a working Sharepoint environment first before implementing the load balancer.

Load Balancer Deployment Mode

Layer 7 SNAT mode (HAProxy) is recommended for Sharepoint and is used for the configuration presented in this guide. This mode offers high performance and is simple to configure since it requires no additional configuration changes to the load balanced Sharepoint Servers.

Layer 4 DR mode, NAT mode and SNAT mode can also be used if preferred. For DR mode you'll need to solve the ARP problem on each AD FS server - for more information please refer to [DR Mode Considerations](#). For NAT mode the default gateway of the Sharepoint servers must be the load balancer. For layer 4 SNAT mode no additional server configuration changes are required.

The Basics

Load balancing is required for the Front-end Web Servers to provide performance and resilience for users connecting to the Sharepoint farm.

For the middle (application) tier, multiple application servers running the same service applications are load balanced by default and there is no external load balancing requirement.

Sharepoint is based on IIS and associated technologies at the top/middle tier and Microsoft SQL Server for back-end storage. Therefore, load balancing Sharepoint is relatively straight- forward, but to provide a resilient and robust Sharepoint system, it's important to consider Microsoft's various architectural recommendations, best practices and guidelines when designing your Sharepoint Infrastructure.

TCP Ports

Sharepoint uses a range of ports for internal and external farm communication. The ports that need to be load balanced are those used in communications between external users and the Front-End Web Servers as shown in the following table:

TCP Port	Use	Description
80	Web Front-End	Standard HTTP port used for Web Application/Site access
443	Web Front-End	Standard HTTPS port used for Web Application/Site access
8080 ¹	Central Admin	Custom port for Central Administration Website (HTTP)
8443 ²	Central Admin	Custom port for Central Administration Website (HTTPS)

Table Footnotes

1. During the Sharepoint 2010/2013 installation the installer suggests a random HTTP port for the Central Administration website. In the lab environment used for this guide, this was set to port 8080.
2. In the lab environment, the Central Administration website was extended to the Custom Zone and configured for HTTPS on port 8443. System administrators are then able to access the Central Administration website over HTTP and HTTPS.

Persistence (aka Server Affinity)

Enabling persistence ensures that clients continue to connect to the same server when connecting into the Sharepoint farm.

Sharepoint 2010

For Sharepoint 2010 we recommend using IP persistence for simplicity and compatibly across protocols.

Sharepoint 2013

Persistence is no longer required for Sharepoint 2013. This is because the Distributed Cache service maintains authentication information across all Sharepoint 2013 Web Servers and therefore a particular client no longer needs to persist to the same Server.

Load Balancer Virtual Service (VIP) Requirements

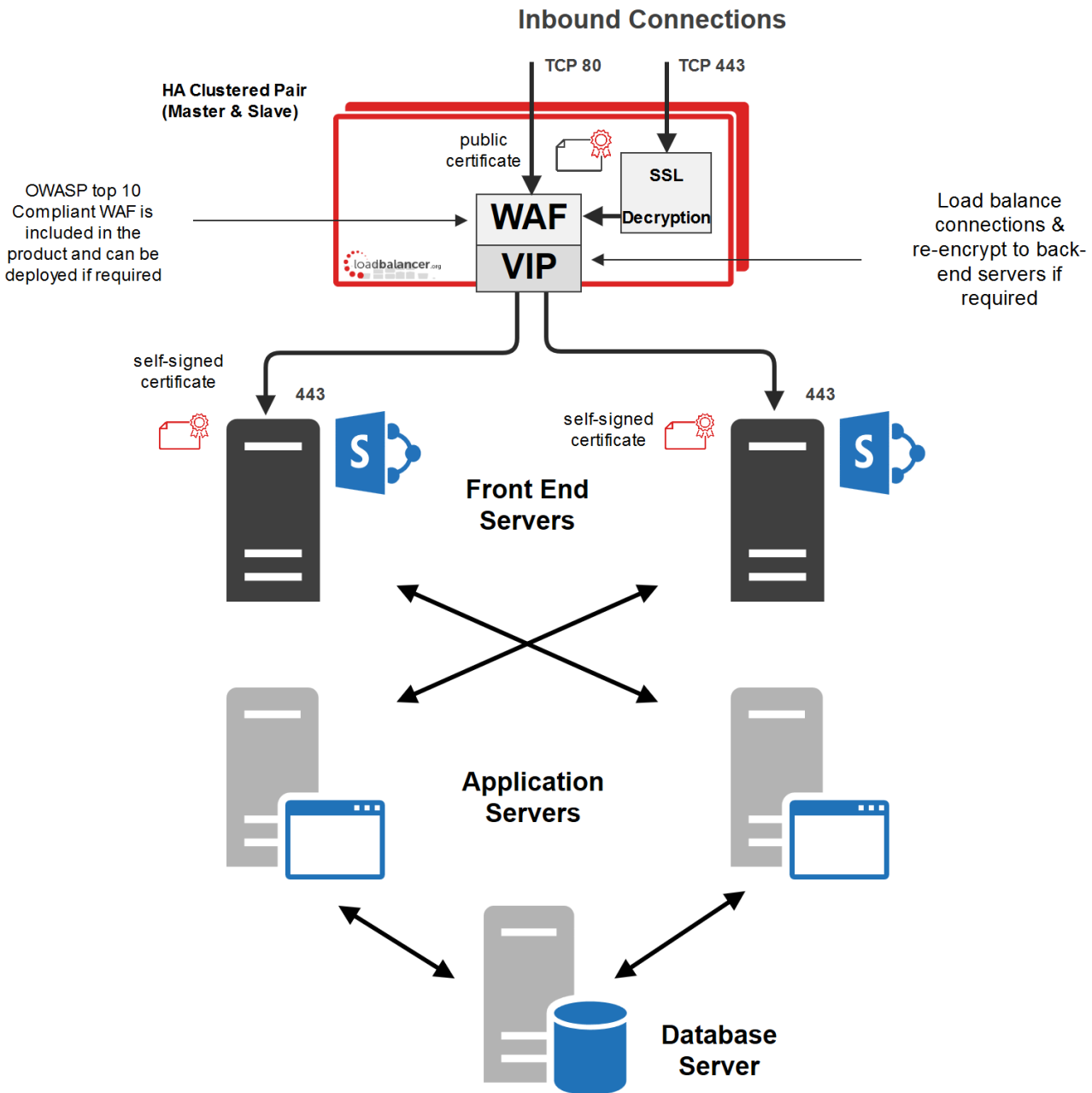
It is possible to configure a single VIP that includes all required ports as listed in the table above. However, to enable more granular control and improved health-check monitoring, multiple Virtual Services are recommended.

The list below shows the general approach used in this guide:

- **VIP-1:** For the Load balanced Sharepoint Central Administration site running on the selected port. In this guide, HTTP port 8080 & HTTPS port 8443.
- **VIP-2:** For the load balanced Sharepoint User Portal, typically running on the default ports: HTTP (80) & HTTPS (443).
- **VIP-3** etc.: Used for additional Sharepoint Web Applications/IIS sites that require a different IP address to be used.

7. Lab Deployment Architecture

There are multiple ways to deploy Sharepoint depending on a number of factors including number of end-users, physical server topology options/preferences etc. For the lab environment used in this guide, the following 3-tier redundant topology was used. Once configured, clients then connect to the Virtual Services (VIPs) on the load balancer rather than connecting directly to one of the Sharepoint servers. These connections are then load balanced across the Sharepoint servers to distribute the load according to the load balancing algorithm selected.



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.

Lab Environment Notes

Planning for High Availability

The following table shows Microsoft's general guidance to achieve high availability:

Server	Preferred redundancy strategy within a farm
Front-End Web Server	Deploy multiple front-end Web servers within a farm, and use Load Balancing
Application Server	Deploy multiple application servers within a farm
Database Server	Deploy database servers by using clustering or high-availability database mirroring

For more details on HA architecture please refer to the following Microsoft link: <https://technet.microsoft.com/en->

[us/library/cc748824.aspx](https://technet.microsoft.com/en-us/library/cc748824.aspx)

Front-End Web Servers

Two Front-end Web Servers are used to provide redundancy. These servers are load balanced by the Loadbalancer.org appliances (clustered pair for high availability). The servers also run the query related components so the index is also located on these servers. Therefore the index files should be located on a disk which has the capacity and performance required. Multiple query components can be added for fault tolerance and improved performance.

Application Servers

Two application servers are used to provide redundancy. Both servers run the same service applications which enables built in load balancing. This distributes requests from the Web Servers on a round-robin basis.

In the lab setup, these servers also run the crawl components. Multiple crawl components can be added for fault tolerance and improved performance. For more details on configuring crawl please refer to the following Microsoft article: [https://technet.microsoft.com/en-us/library/dd335962\(v=office.14\).aspx](https://technet.microsoft.com/en-us/library/dd335962(v=office.14).aspx)

Database Server

In a live environment the SQL back-end should be mirrored, clustered or made redundant in any other appropriate way. For more details on HA please refer to the following URL: <https://technet.microsoft.com/en-us/library/cc748824.aspx>

8. Sharepoint Installation & Configuration

Installation Considerations

Central Administration Website

For improved resilience and redundancy the Central Administration website can also be load balanced. This requires that the Central Administration component is installed on multiple servers – this is done during initial installation of the software by selecting the Advanced Settings, Host Central Administration Website & checking "Use this machine to host the website". In the lab environment used for this guide, Central Administration is installed on both Application Servers.

Alternate Access Mappings/Zones

Alternative Access Mappings must be setup correctly to ensure that users are able to connect consistently without receiving broken links and experiencing other issues. These are configured automatically when new Web Applications are created and extended using Central Administration. If manual changes are made later to Sharepoint or IIS, the mappings may also need to be adjusted manually.

Microsoft recommends extending a Web Application to a new IIS web site for each zone required. This provides a backing IIS Web site. Its not generally recommended to reuse the same IIS web site for multiple zones. For more information please refer to the following URL: [https://technet.microsoft.com/en-us/library/cc261814\(v=office.15\).aspx](https://technet.microsoft.com/en-us/library/cc261814(v=office.15).aspx)

Authentication

Sharepoint supports various authentication methods, the method used in this guide is NTLM.

SSL Certificates

For performance scalability, installing SSL certificates on the Sharepoint Servers is recommended rather than terminating SSL on the load balancer. For the lab setup a trial Thawte certificate was used. The Common Name

was set to sharepoint.robstest.com.

Service Applications

For a three-tier infrastructure, Service Applications should be distributed between the servers in each tier according to the topology in use. The complete installation option and the Configuration Wizard should be used to provision all service applications on each server. Central Administration can then be used to configure where each service runs.

DNS Configuration

DNS records must be configured that point to the Virtual Services on the load balancer. For the lab setup, Internal DNS entries were created for 'sharepoint.robstest.com' on the domains DNS server and external DNS entries were created on the local hosts file of a non domain member test PC.

Lab Environment Installation

Site & Zone Structure

Site	Zone	Protocol	Ports	Notes	Host Header Value	Certificate CN
Central Administration	Default	HTTP	8080	-	-	-
Central Administration	Custom	HTTPS	8443	Extended site	-	sharepoint.robstest.com
Sharepoint User Portal	Default	HTTP	80	-	sharepoint.robstest.com	-
Sharepoint User Portal	Custom	HTTPS	443	Extended site	-	sharepoint.robstest.com

Installation Steps

1. Install the Software:
 - a. Install & prepare Microsoft SQL Server.
 - b. Install Sharepoint on both Application Servers. Install Central Administration on both servers setting the port to 8080. Use the 'Complete' install option, run the Configuration Wizard and deploy all Service Applications. Later, these services can be enabled or disabled as required.
 - c. Use the Advanced Settings option to install Central Admin:



- d. Install Sharepoint on the Front End Web Servers. Use the 'Complete' install option, run the Configuration Wizard and deploy all Service Applications. Later, these services can be enabled or disabled as required.

2. Configure the Central Administration site for load balancing:

- a. Edit the Public URLs to ensure that both Application Servers are listed as shown below:

Default

Intranet

Once configured the AAMs are set as follows:

Internal URL	Zone	Public URL for Zone
http://sp2013-app1:8080	Default	http://sp2013-app1:8080
http://sp2013-app2:8080	Intranet	http://sp2013-app2:8080

(see <http://www.harbar.net/articles/spca.aspx> for more details)

- b. Edit the public URLs again and add <http://sharepoint.robstest.com:8080>. Also ensure that this URL is set as the Default Zone as shown below:

Default




Intranet

Internet

3. Confirm that the AAMs are set as follows:

Internal URL	Zone	Public URL for Zone
http://sharepoint.robstest.com:8080	Default	http://sharepoint.robstest.com:8080
http://sp2013-app1:8080	Intranet	http://sp2013-app1:8080
http://sp2013-app2:8080	Internet	http://sp2013-app2:8080

Note | These settings ensure that the **CentralAdministrationURL** registry key is set correctly as shown below:

 BlockADAccountCreationMode	REG_DWORD	0x00000001 (1)
 CentralAdministrationURL	REG_SZ	http://sharepoint.robstest.com:8080/
 CreateProductVersionJob	REG_SZ	0

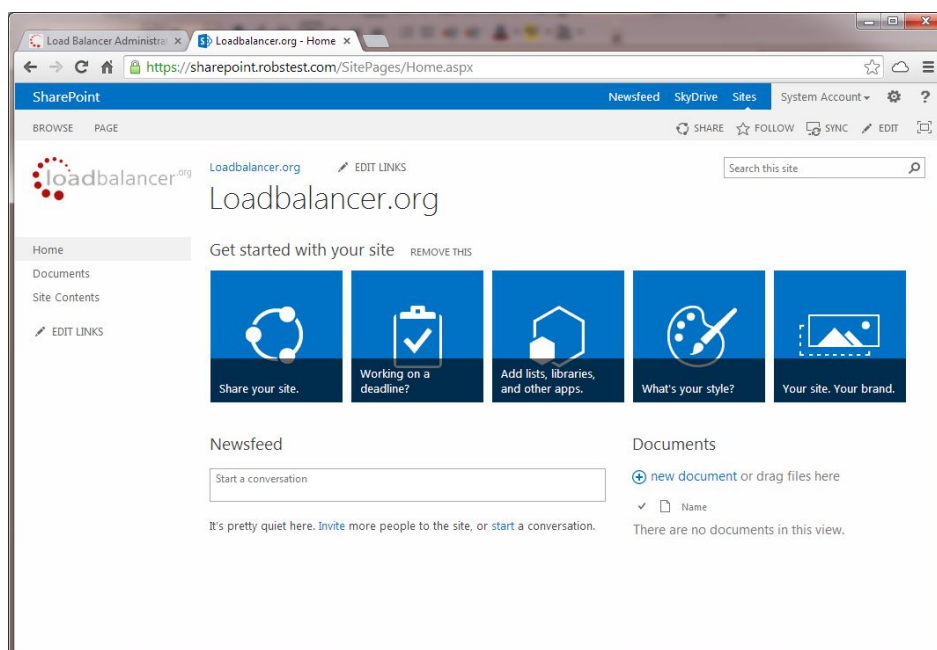
- a. Extend the Central Administration Web Application to the Custom Zone on port 8443, using SSL. Once done a corresponding AAM is automatically configured as shown below:

Internal URL	Zone	Public URL for Zone
http://sharepoint.robstest.com:8080	Default	http://sharepoint.robstest.com:8080
http://sp2013-app1:8080	Intranet	http://sp2013-app1:8080
http://sp2013-app2:8080	Internet	http://sp2013-app2:8080
https://sharepoint.robstest.com:8443	Custom	https://sharepoint.robstest.com:8443

- b. On one of the application servers create a CSR for CN=sharepoint.robstest.com, then complete the request once a signed certificate is obtained.
 - c. Export the certificate & private key and import to the other Application Server.
 - d. Using IIS Manager on both Application Servers ensure that the HTTPS bindings correctly refer to the sharepoint.robstest.com certificate.
4. Configure the User Portal Web Application & Top Level Default Site:
- a. Create a new Web Application for the Sharepoint User Portal on Port 80.
 - b. Create a new top level Site Collection under the User Portal Web Application.

Navigating to: <http://sharepoint.robstest.com/>

opens: https://sharepoint.robstest.com/_layouts/15/start.aspx#/



Note | The lab setup has a HTTP to HTTPS redirect for the User Portal (see [Configuring an HTTP to HTTPS Redirect for the User Portal](#)).

- c. Extend the User Portal Web Application to the Custom Zone on port 443, using SSL. Once done a corresponding AAM is automatically configured as shown below:

Internal URL	Zone	Public URL for Zone
http://sharepoint.robstest.com	Default	http://sharepoint.robstest.com
https://sharepoint.robstest.com	Custom	https://sharepoint.robstest.com

- d. Using IIS Manager on both Front End Web Servers import the **sharepoint.robstest.com** certificate and ensure that the HTTPS bindings correctly refer to this certificate.

5. Configure DNS:

- a. Create internal & external DNS entries for **sharepoint.robstest.com**. This should point to the IP address of the Virtual Service that's created on the load balancer (see **STEP 3 – Configure the Load Balanced User Portal Site**).

Accessing Sharepoint

With the configuration described above, the following table shows how Sharepoint is accessed in the lab environment:

Site	HTTP	HTTPS
Sharepoint User Portal	http://sharepoint.robstest.com	https://sharepoint.robstest.com
Central Administration	http://sharepoint.robstest.com:8080	https://sharepoint.robstest.com:8443

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:

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

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:

- System Overview
- Local Configuration
- Cluster Configuration
- Maintenance
- View Configuration
- Reports
- Logs
- Support
- Live Chat

WARNING: YOUR TRIAL IS DUE TO EXPIRE IN 30 DAYS.

Buy with confidence. All purchases come with a 90 day money back guarantee.
Already bought? Enter your license key [here](#)

Buy Now

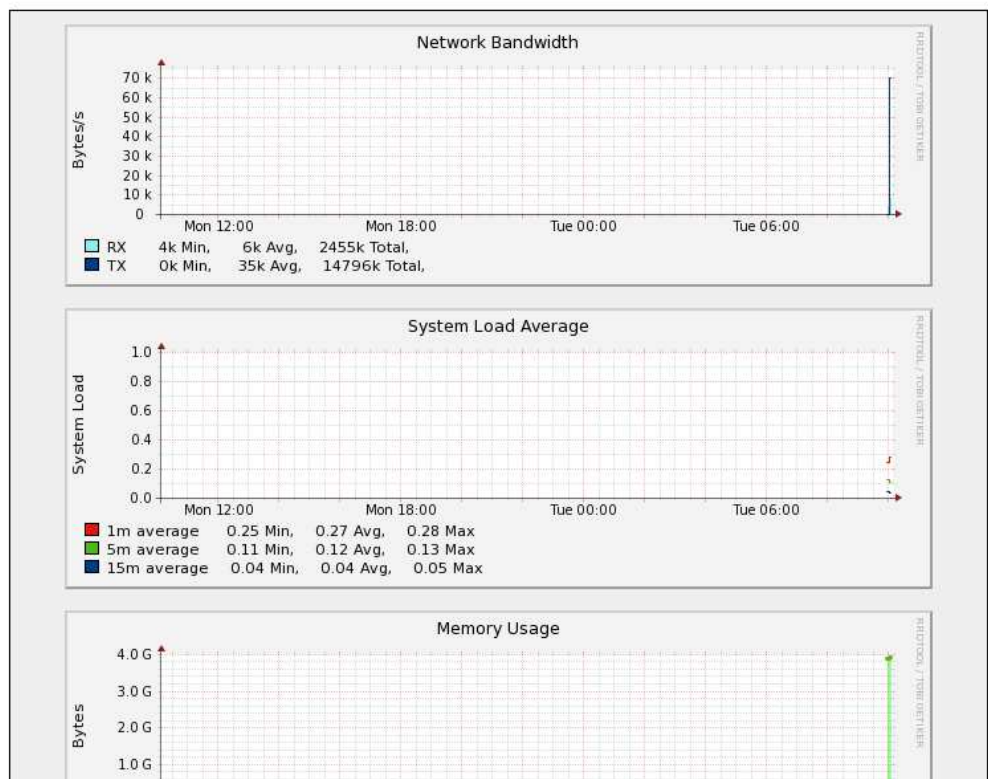
System Overview

2022-06-14 10:07:30 UTC

Would you like to run the Setup Wizard?

VIRTUAL SERVICE IP PORTS CONNS PROTOCOL METHOD MODE

No Virtual Services configured.



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.

- 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 [Configuring HA - Adding a Secondary Appliance](#).

10. Appliance Configuration for Sharepoint

STEP 1 – Configure Layer 7 Global Settings

To ensure that client connections remain open during periods of inactivity, the Client and Real Server Timeout values must be changed from their default values of 43 seconds and 45 seconds respectively to 5 minutes. To do this follow the steps below:

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Advanced Configuration*:

Lock HAProxy Configuration (Deprecated)	<input type="checkbox"/>	?
Logging	Off ▼	?
Redispatch	<input checked="" type="checkbox"/>	?
Connection Timeout	4000 ms	?
Client Timeout	5m ms	?
Real Server Timeout	5m ms	?

2. Change *Client Timeout* to **5m** (i.e. 5 minutes) as shown above.
3. Change *Real Server Timeout* to **5m** (i.e. 5 minutes) as shown above.
4. Click the **Update** button to save the settings.

STEP 2 – Configure the Load Balanced Central Admin Site

Create the Virtual Service (VIP)

This VIP is used to provide access to the Central Administration website on ports 8080 & 8443.

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

Layer 7 - Add a new Virtual Service

Virtual Service		[Advanced +]
Label	<input type="text" value="SP-Admin"/>	?
IP Address	<input type="text" value="192.168.2.180"/>	?
Ports	<input type="text" value="8080,8443"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="TCP Mode"/>	?

3. Enter an appropriate label for the VIP, e.g. **SP-Admin**.
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.2.180**.
5. Set the *Virtual Service Ports* field to **8080,8443**.
6. Change *Layer 7 Protocol* to **TCP Mode**.
7. Click **Update**.
8. Click **Modify** next to the newly created VIP.
9. Set *Balance Mode* as required – **Weighted Least Connections** is recommended.
10. **For Sharepoint 2010** – Ensure that *Persistence Mode* is set to **Source IP**.
11. **For Sharepoint 2013** – Ensure that *Persistence Mode* is set to **None**.
12. Click **Update**.

Define the Real Servers (RIPs)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a New Real Server** next to the newly created Virtual Service.
2. Enter the following details:

Layer 7 Add a new Real Server

Label	<input type="text" value="App-1"/>	?
Real Server IP Address	<input type="text" value="192.168.2.190"/>	?
Real Server Port	<input type="text"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

3. Enter an appropriate label for the RIP, e.g. **App-1**.
4. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.2.190**.
5. Leave the *Real Server Port* field blank.
6. Click **Update**.
7. Repeat the above steps to add your other Application Servers.

Note

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

STEP 3 – Configure the Load Balanced User Portal Site

Create the Virtual Service (VIP)

This VIP is used to provide access to the User Portal website on ports 80 & 443.

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

Layer 7 - Add a new Virtual Service

Virtual Service		[Advanced +]
Label	<input type="text" value="SP-UserPortal"/>	?
IP Address	<input type="text" value="192.168.2.180"/>	?
Ports	<input type="text" value="80,443"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="TCP Mode"/>	?

3. Enter an appropriate label for the VIP, e.g. **SP-UserPortal**.
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.2.180**.
5. Set the *Virtual Service Ports* field to **80,443**.
6. Change *Layer 7 Protocol* to **TCP Mode**.
7. Click **Update**.
8. Click **Modify** next to the newly created VIP.
9. Set *Balance Mode* as required – **Weighted Least Connections** is recommended.
10. **For Sharepoint 2010** – Ensure that *Persistence Mode* is set to **Source IP**.
11. **For Sharepoint 2013** – Ensure that *Persistence Mode* is set to **None**.
12. Click **Update**.

Note | Please refer to [Configuring an HTTP to HTTPS Redirect for the User Portal](#) for details on configuring a HTTP to HTTPS redirect for the User Portal.

Define the Real Servers (RIPs)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a New Real Server** next to the newly created Virtual Service.
2. Enter the following details:

Layer 7 Add a new Real Server

Label	<input type="text" value="Web-1"/>	?
Real Server IP Address	<input type="text" value="192.168.2.190"/>	?
Real Server Port	<input type="text"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

3. Enter an appropriate label for the RIP, e.g. **Web-1**.
4. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.2.190**.
5. Leave the *Real Server Port* field blank.
6. Click **Update**.
7. Repeat the above steps to add your other Web Front End Servers.

Note | Because SNAT is a full proxy, any server in the cluster can be on any accessible subnet including across the Internet or WAN.

STEP 4 – Finalizing the Configuration

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

11. Testing & Verification

Note | For additional guidance on diagnosing and resolving any issues you may have, please also refer to [Diagnostics & Troubleshooting](#).

It's important to verify that the load balancer is working as expected. Network cables on the Front-End Web Servers can be removed to simulate a sever failure.

The System Overview in the WebUI can then be used to check that the server has been marked down (colored red). Also, when the cable is plugged back in, the server should return to normal status (colored green).

Alternatively, IIS can be used to stop a website on one of the web servers. For example, stopping the IIS User Portal site on Web-1 will cause the system overview to mark **SP-UserPortal/Web-1** as down (red) as shown below:

System Overview ? 2020-06-09 13:10:50 UTC

VIRTUAL SERVICE	IP	PORTS	CONNS	PROTOCOL	METHOD	MODE	
SP-Admin	192.168.2.180	8080,8443	0	HTTP	Layer 7	Proxy	
<i>REAL SERVER</i>							
App-1	192.168.2.190	8080,8443	100	0	Drain	Halt	
App-2	192.168.2.191	8080,8443	100	0	Drain	Halt	
SP-UserPortal	192.168.2.180	80,443	0	TCP	Layer 7	Proxy	
<i>REAL SERVER</i>							
Web-1	192.168.2.200	80,443	100	0	Drain	Halt	
Web-2	192.168.2.201	80,443	100	0	Drain	Halt	

SP-UserPortal/Web-2 is still healthy (green), so all requests will now be routed here.

The System Overview also enables the servers to be taken offline using the Drain and Halt options. This enables servers to be removed from the cluster to perform maintenance tasks etc. Once again, requests will then only be sent to the remaining operational server.

12. 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.

13. Further Documentation

The Administration Manual contains much more information about configuring and deploying the appliance. It's available here: <https://pdfs.loadbalancer.org/loadbalanceradministrationv8.pdf>.

14. Conclusion

Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced Sharepoint 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:

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

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

loadbalancer.org

Local IP address
192.168.110.40

IP address of new peer
192.168.110.41

Password for *loadbalanceruser* on peer
.....

Add new node

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:

CREATE A CLUSTERED PAIR

192.168.110.40 loadbalancer.org

Attempting to pair..

192.168.110.41 loadbalancer.org

Local IP address
192.168.110.40

IP address of new peer
192.168.110.41

Password for *loadbalanceruser* on peer
.....

configuring

6. Once complete, the following will be displayed on the Primary appliance:

High Availability Configuration - primary



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](#).

Configuring an HTTP to HTTPS Redirect for the User Portal

An additional later 7 VIP is required that listens on HTTP port 80 on the same IP address. The VIP is then configured to redirect connections to HTTPS port 443.

e.g. <http://sharepoint.robstest.com/>

should be auto-redirected to:

<https://sharepoint.robstest.com/>

The steps:

1. Create another Layer 7 VIP with the following settings:
 - Label: **SP-UserPortalRedirect**
 - Virtual Service IP Address: <same as the VIP that's listening on port 443>
 - Virtual Service Ports: **80**
 - Layer 7 Protocol: **HTTP Mode**
 - Persistence Mode: **None**
 - Force to HTTPS: **Yes**

Note | This additional VIP will be shown purple/green to indicate that it's being used for HTTP to HTTPS redirection.

2. Remove port 80 from the user portal VIP – otherwise a configuration error message will be displayed since there would be a conflict.
3. Apply the new settings – to apply the new settings, reload HAProxy as using the reload button in the blue box at the top of the screen.

16. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.6.0	17 October 2019	Styling and layout	General styling updates	RJC
1.6.1	9 June 2020	New title page Updated Canadian contact details New screenshots for creating VIPs and of the System Overview in 'Testing & Verification'	Branding update Change to Canadian contact details Changes to the appliance WebUI	AH
1.6.2	17 August 2021	Removed links to various Microsoft articles Various minor updates	No longer available on the Microsoft website Consistency across documentation library	RJC
1.7.0	1 January 2022	Converted the document to AsciiDoc	Move to new documentation system	AH, RJC, ZAC
1.7.1	28 September 2022	Updated layer 7 VIP and RIP creation screenshots	Reflect changes in the web user interface	AH

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.



United Kingdom

Loadbalancer.org Ltd.
Compass House, North Harbour
Business Park, Portsmouth, PO6 4PS
UK: +44 (0) 330 380 1064
sales@loadbalancer.org
support@loadbalancer.org

Canada

Loadbalancer.org Appliances Ltd.
300-422 Richards Street, Vancouver,
BC, V6B 2Z4, Canada
TEL: +1 866 998 0508
sales@loadbalancer.org
support@loadbalancer.org

United States

Loadbalancer.org, Inc.
4550 Linden Hill Road, Suite 201
Wilmington, DE 19808, USA
TEL: +1 833.274.2566
sales@loadbalancer.org
support@loadbalancer.org

Germany

Loadbalancer.org GmbH
Tengstraße 2780798,
München, Germany
TEL: +49 (0)89 2000 2179
sales@loadbalancer.org
support@loadbalancer.org