loadbalancer.org

Load Balancing Microsoft Sharepoint 2010 / 2013

Deployment Guide

v1.5.2

Copyright © Loadbalancer.org

Table of Contents

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 relevant Administration Manual:

- v7 Administration Manual
- v8 Administration Manual

2. Loadbalancer.org Appliances Supported

All our products can be used with Sharepoint 2010 & 2013. The complete list of models is shown below:

Discontinued Models	Current Models *
Enterprise R16	Enterprise R20
Enterprise VA R16	Enterprise MAX
Enterprise VA	Enterprise 10G
Enterprise R320	Enterprise Ultra
	Enterprise VA R20
	Enterprise VA MAX
	Enterprise AWS
	Enterprise AZURE **

* For full specifications of these models please refer to: http://www.loadbalancer.org/products/hardware

** Some features may not be supported, please check with Loadbalancer.org support

3. Loadbalancer.org Software Versions Supported

- v7.6.4 and later

4. Microsoft Sharepoint Software Versions Supported

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

5. Sharepoint Server

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 what were roles in prior versions of the product can now be viewed simply as components, so as opposed to assigning a specific role to a server, components are placed on an agnostic machine, independent of any specific role definition. For example, in the past the role of indexer or query server was assigned to a machine, now the search topology is extended by assigning one or more search components, such as Query or Crawl to a machine. Roles are a concept that do not necessarily apply in 2010 & 2013, instead a machine is generic and flexible to provide a multitude of services. Components and services are 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 trialing 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 please refer to: http://technet.microsoft.com/en-us/library/ee667264.aspx

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 good performance and is simple to configure since it requires no configuration changes to the 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 Sharepoint server (please see the Administration Manual and search for "DR mode considerations"), for NAT mode the default gateway of the Sharepoint servers must be the load balancer.

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*	Central Admin	Custom port for Central Administration Website (HTTP)
8443**	Central Admin	Custom port for Central Administration Website (HTTPS)

* 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

** In the lab environment, the Central Administration website was extended to the Custon Zone and configured for HTTPS on port 8443. System administrators are then able to access the Central Administration website over HTTP and HTTPS

For a full Sharepoint Server port list, please refer to:
http://technet.microsoft.com/en-us/library/cc262849.aspx

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.

For more details please refer to the following Technet article:
http://technet.microsoft.com/en-us/library/jj219758(v=office.15).aspx

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.

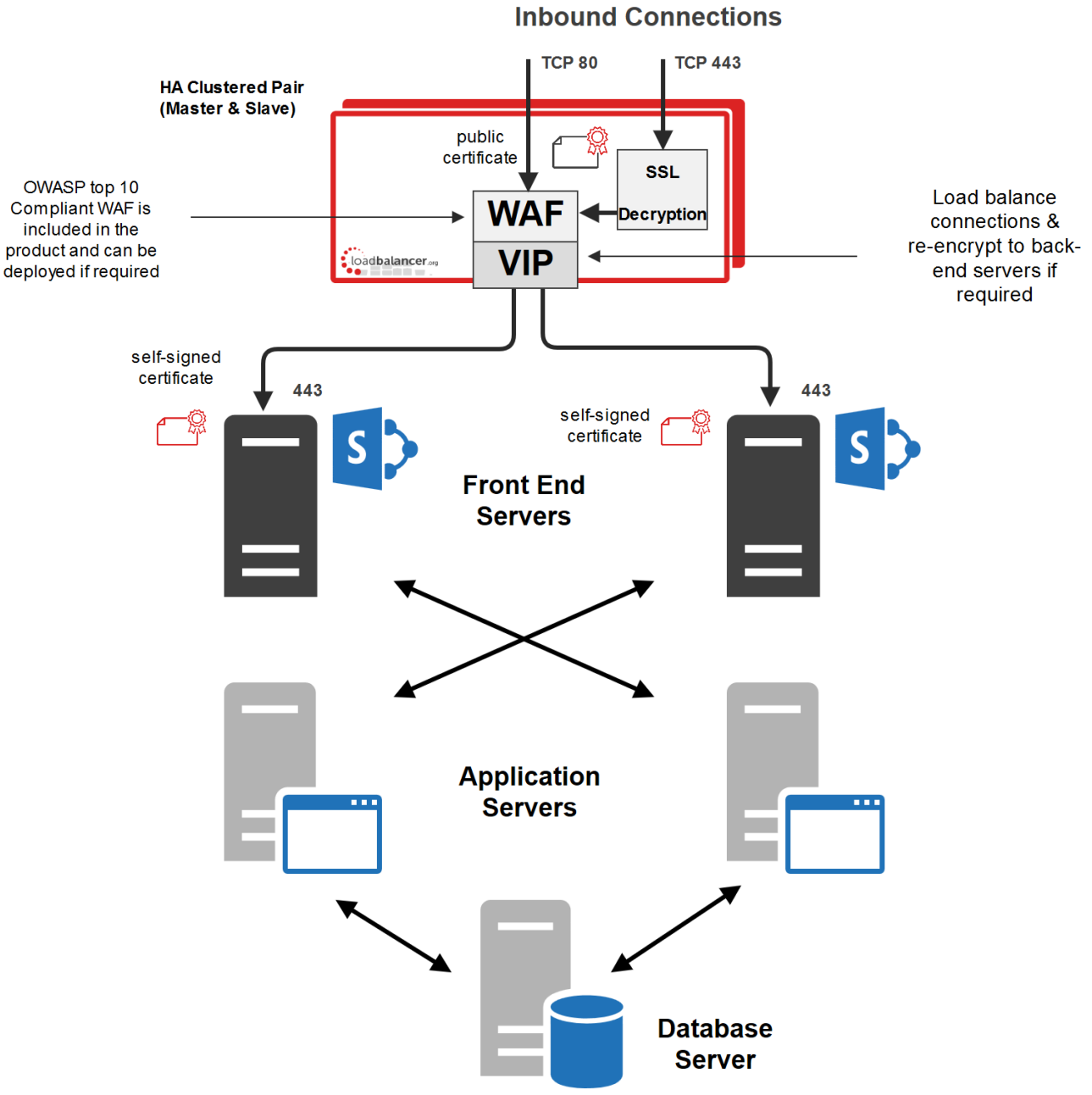
The list below shows the general approach used in this guide:

- **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

> Note:
>
> In the lab setup used for this guide, the Front-End Web Servers have a single IP address. Also all VIPs configured on the load balancer use the same IP address with different ports. The VIPs could also be configured using different IP addresses if needed.

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 section 1 in the appendix on page 23 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 please refer to the following Microsoft link:

http://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. For more details on the Sharepoint search/query architecture the following Microsoft link provides a useful insight:

http://blogs.msdn.com/b/russmax/archive/2010/04/16/search-2010-architecture-and-scale-part-2-query.aspx

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. For more details on the built-in service application load balancer, please refer to the following Microsoft link:

http://blogs.msdn.com/b/dtaylor/archive/2011/02/23/sharepoint-2010-service-application-load-balancer.aspx

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 the Sharepoint Search architecture and configuring crawl please refer to the following Microsoft articles:

http://blogs.msdn.com/b/russmax/archive/2010/04/16/search-2010-architecture-and-scale-part-1-crawl.aspx

http://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 SQL database clustering and mirroring for Sharepoint please refer to the following Microsoft links:

Planning for availability: http://technet.microsoft.com/en-us/library/cc748824.aspx

Sharepoint SQL Server availability: http://technet.microsoft.com/en-us/library/dd207313(v=office.15).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 Microsoft links:

http://technet.microsoft.com/en-us/library/cc261814(v=office.15).aspx

http://blogs.msdn.com/b/sharepoint_strategery/archive/2013/05/27/alternate-access-mappings-explained.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

Install the Software:

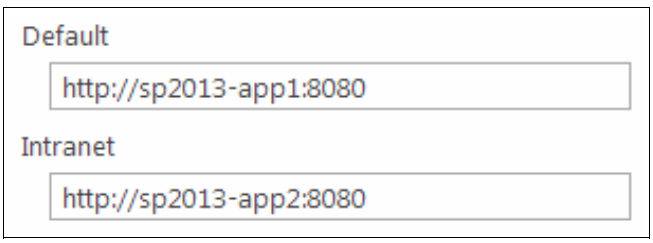
- Install & prepare Microsoft SQL Server
- Install Sharepoint on both Application Servers. Install Central Administration on both servers setting the port to 8080. Use the 'Complete' install option, run the Configuration Wizard and deploy all Service Applications. Later, these services can be enabled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

  Use the Advanced Settings option to install Central Admin:

- 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

Configure the Central Administration site for load balancing:

- Edit the Public URL's to ensure that both Application Servers are listed as shown below:

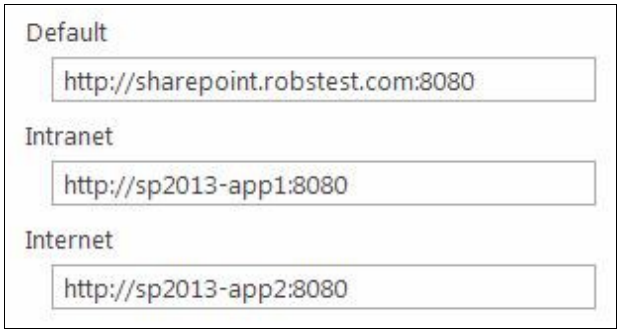


  Once configured the AAM's are set as follows:

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)

- Now edit the public URL's again and add **http://sharepoint.robstest.com:8080**. Also ensure that this URL is set as the Default Zone as shown below:

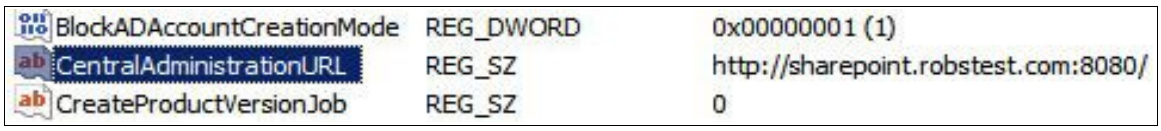


Once configured the AAM's are set as follows:

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:



- Now 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

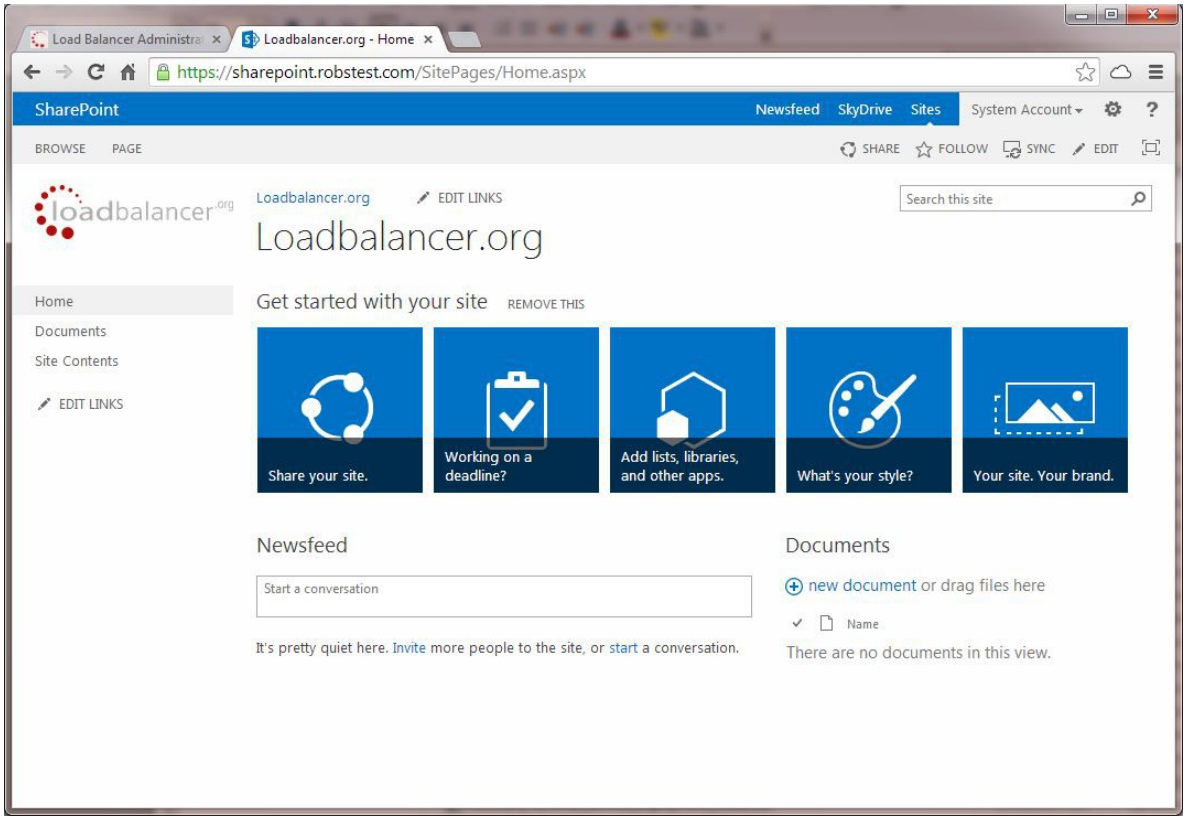
- On one of the application servers create a CSR for CN=sharepoint.robstest.com, then complete

the request once a signed certificate is obtained

- Export the certificate & private key and import to the other Application Server
- Using IIS Manager on both Application Servers ensure that the HTTPS bindings correctly refer to the sharepoint.robstest.com certificate

Configure the User Portal Web Application & Top Level Default Site:

- Create a new Web Application for the Sharepoint User Portal on Port 80
- Create a new top level Site Collection under the User Portal Web Application
  so 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 pages 25).

- Now 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

- 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

Configure DNS:

- 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 pages 20).

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

Useful links:

Building a 3 Tier farm:

http://blogs.technet.com/b/meamcs/archive/2012/05/30/prepare-sharepoint-farm-part-4-install-and-configure-sharepoint-farm-3-tier.aspx

9. Loadbalancer.org Appliance – the Basics

VIRTUAL APPLIANCE DOWNLOAD & DEPLOYMENT

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 and XEN and has been optimized for each Hypervisor. By default, the VA is allocated 1 CPU, 2GB of RAM and has an 8GB 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 the Administration Manual and the ReadMe.txt text file included in the VA download for more detailed information on deploying the VA using various Hypervisors.

INITIAL NETWORK CONFIGURATION

The IP address, subnet mask, default gateway and DNS settings can be configured in several ways as detailed below:

Method 1 - Using the Network Setup Wizard at the console

After boot up, follow the instructions on the console to configure the IP address, subnet mask, default gateway and DNS settings.

Method 2 - Using the WebUI

Using a browser, connect to the WebUI on the default IP address/port: **http://192.168.2.21:9080**

To set the IP address & subnet mask, use: *Local Configuration > Network Interface Configuration*

To set the default gateway, use: *Local Configuration > Routing*

To configure DNS settings, use: *Local Configuration > Hostname & DNS*

Method 3 - Using Linux commands

At the console, set the initial IP address using the following command:

```
ip addr add <IP address>/<mask> dev eth0
```

At the console, set the initial default gateway using the following command:

```
route add default gw <IP address> <interface>
```

At the console, set the DNS server using the following command:

```
echo nameserver <IP address> >> /etc/resolv.conf
```

> Note:
>
> If method 3 is used, you must also configure these settings using the WebUI, otherwise the settings will be lost after a reboot.

ACCESSING THE WEB USER INTERFACE (WEBUI)

The WebUI can be accessed via HTTP at the following URL: **http://192.168.2.21:9080/lbadmin**
** Note the port number → **9080***

The WebUI can be accessed via HTTPS at the following URL: **https://192.168.2.21:9443/lbadmin**
** Note the port number → **9443***

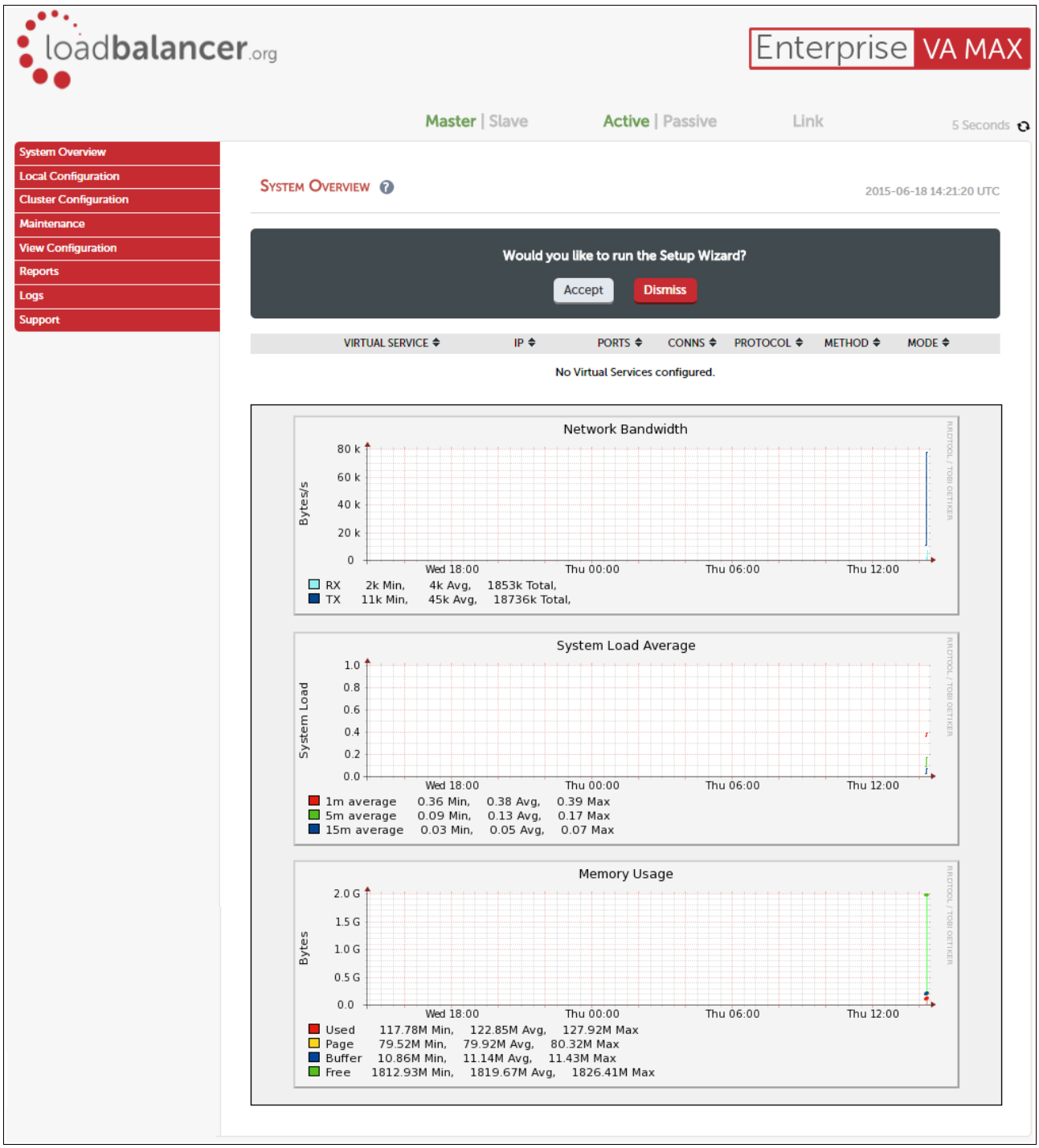
(replace 192.168.2.21 with the IP address of your load balancer if it's been changed from the default)

Login using the following credentials:

Username: loadbalancer
Password: loadbalancer

> Note:
> To change the password , use the WebUI menu option: *Maintenance > Passwords.*

Once logged in, the WebUI will be displayed as shown on the following page:



HA CLUSTERED PAIR CONFIGURATION

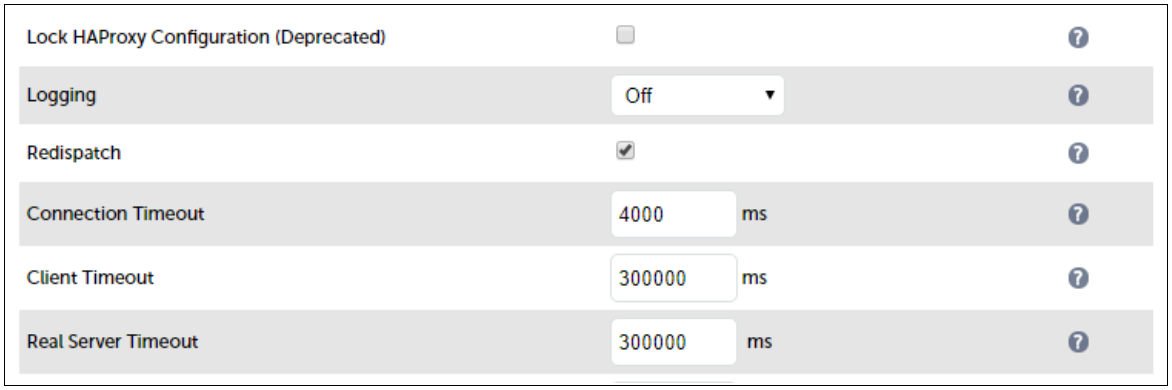
Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary slave unit is covered in section 1 of the Appendix on page 23.

10. Appliance Configuration for Sharepoint

STEP1 – 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*



2. Change *Client Timeout* to **300000** as shown above (i.e. 5 minutes)
   *N.B. You can also enter **5m** rather than 300000*

3. Change *Real Server Timeout* to **300000** as shown above (i.e. 5 minutes)
   *N.B. You can also enter **5m** rather than 300000*

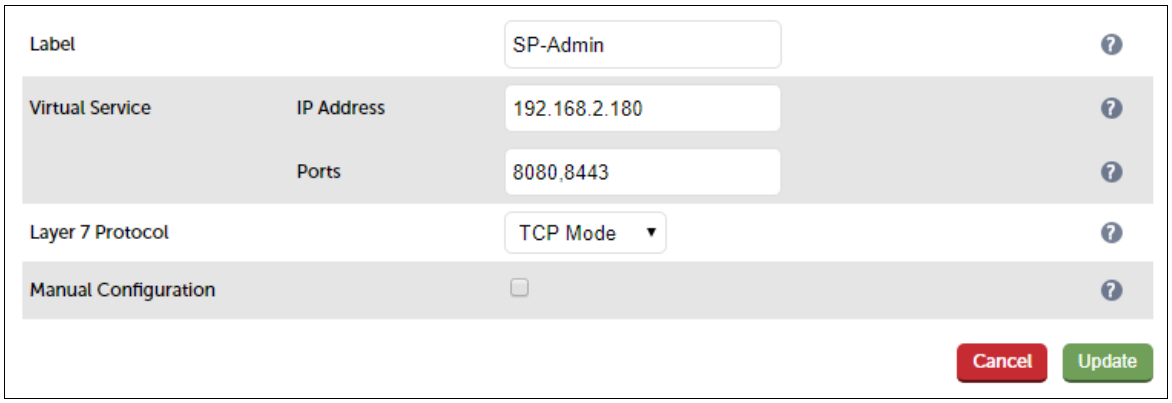
4. Click the **Update** button to save the settings

STEP2 – 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.

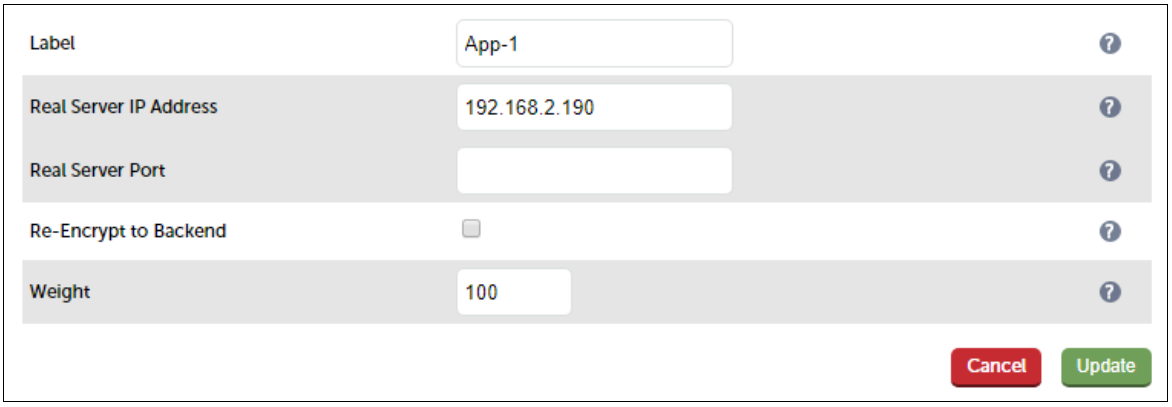
1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a New Virtual Service**
2. Enter the following details:



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. Now click **Modify** next to the newly created VIP
9. Set *Balance Mode* as required – **Weighted Least Connections** is recommended
10. ***For Sharepoint 2010*** **-** Ensure *Persistence Mode* is set to **Source IP**
11. ***For Sharepoint 2013*** **-** Ensure *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:



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

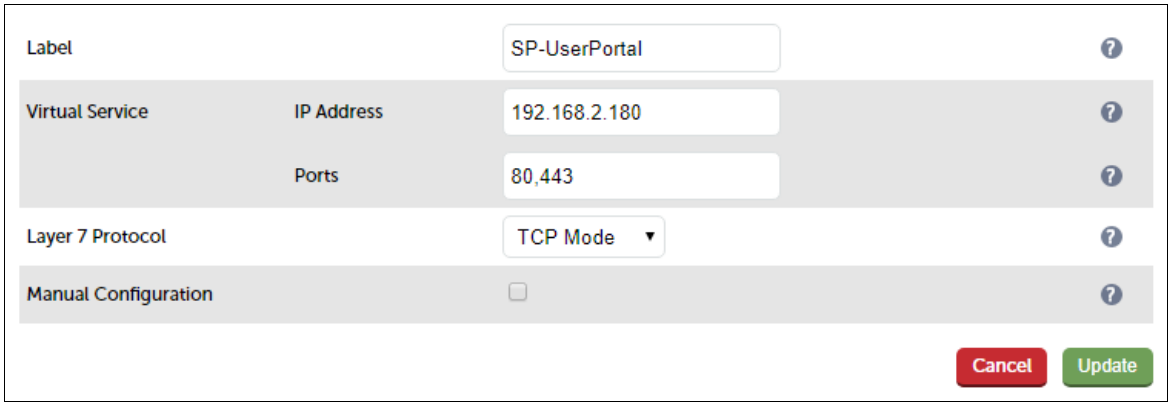
> Note:
>
> Because SNAT is a full proxy, any server in the cluster can be on any accessible subnet including across the Internet or WAN.

STEP3 – 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:



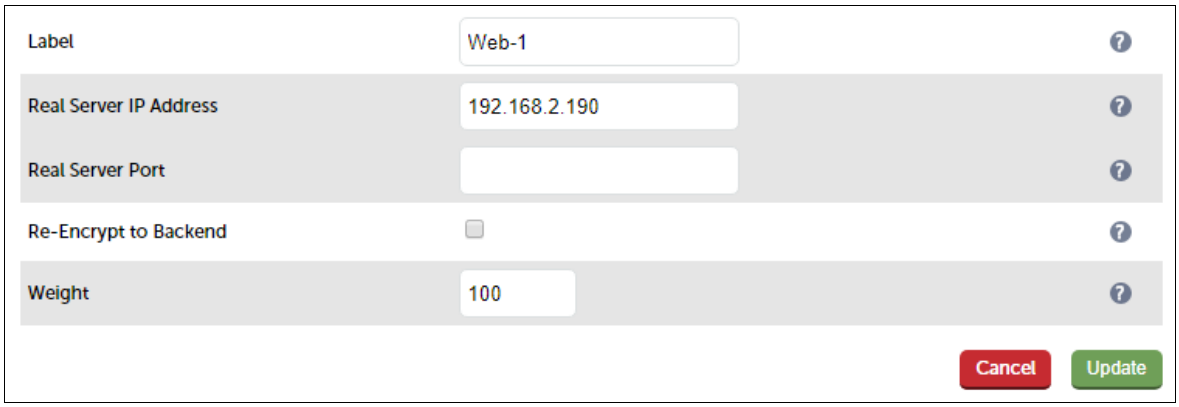
3. Enter an appropriate label for the VIP, e.g. **SP-UserPortal**
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.2.180**
5. Set the *Virtual Service Ports* field to **80,443**
6. Change *Layer 7 Protocol* to **TCP Mode**
7. Click **Update**
8. Now click **Modify**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

> Note:
>
> Please refer to section 2 in the appendix on page 25 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:



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 for the Layer 7 based VIPs, HAProxy must be restarted as follows:

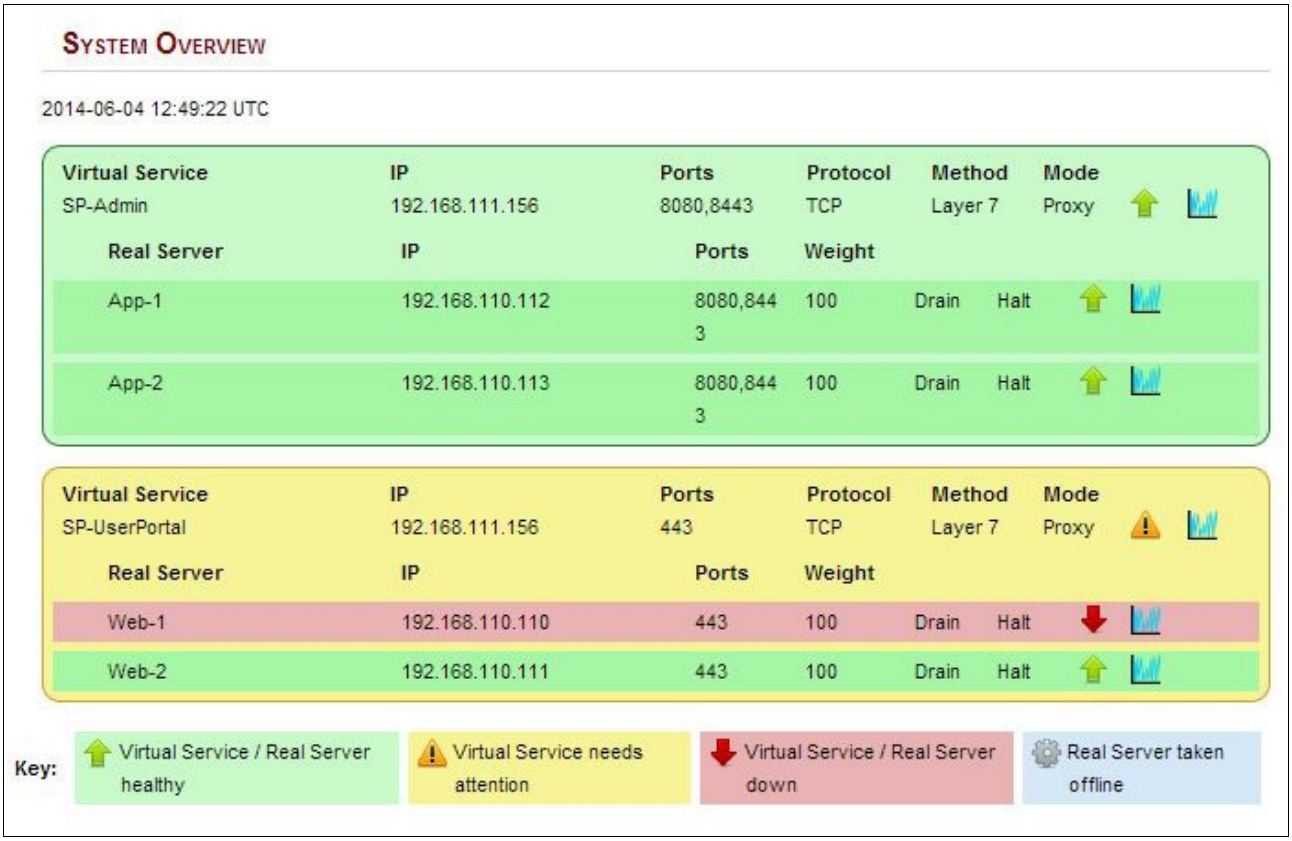
1. Using the WebUI, navigate to: *Maintenance > Restart Services* and click **Restart HAProxy**

11. Testing & Validation

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:



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. The 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: http://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

1 – CLUSTERED PAIR CONFIGURATION – ADDING A SLAVE UNIT

If you initially configured just the master unit and now need to add a slave - our recommended procedure, please refer to the relevant section below for more details:

> Note:
>
> A number of settings are not replicated as part of the master/slave pairing process and therefore must be manually configured on the slave appliance. These are listed below:
>
> - Hostname & DNS settings
> - Network settings including IP addresses, bonding configuration and VLANs
> - Routing configuration including default gateways and static routes
> - Date & time settings
> - Physical – Advanced Configuration settings including Internet Proxy IP address & port, Firewall table size, SMTP relay and Syslog server
> - SNMP settings
> - Graphing settings
> - Firewall Script & Firewall Lockdown Script settings
> - Software updates

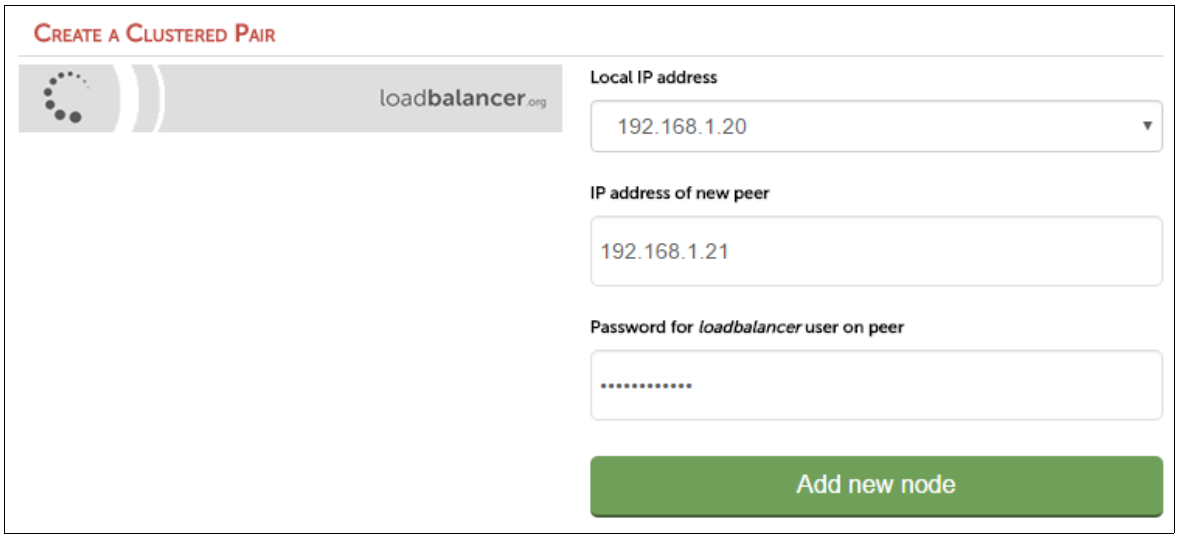
Version 7:

Please refer to **Chapter 8 – Appliance Clustering for HA** in the v7 Administration Manual.

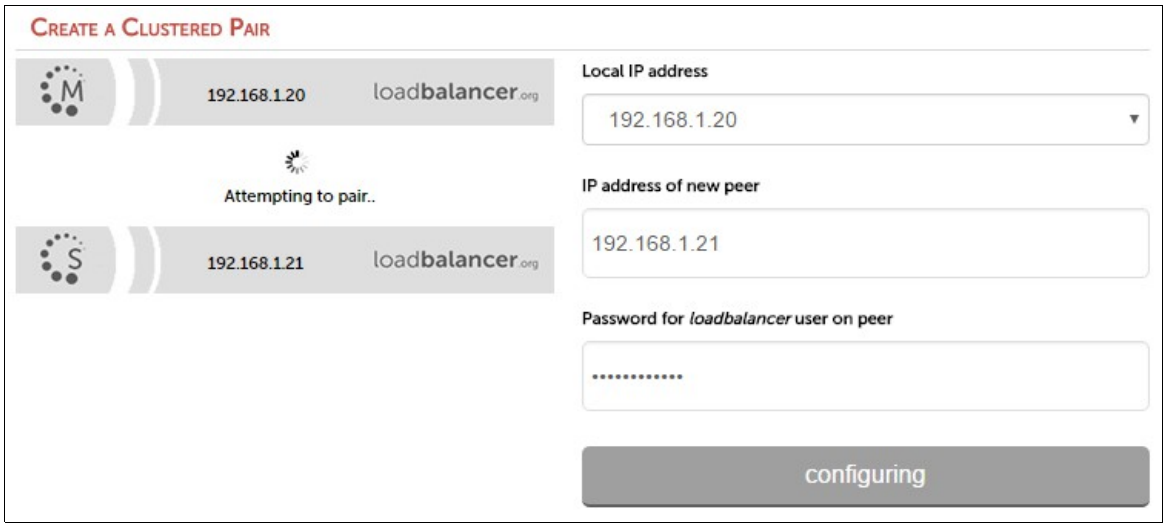
Version 8:

To add a slave node – i.e. create a highly available clustered pair:

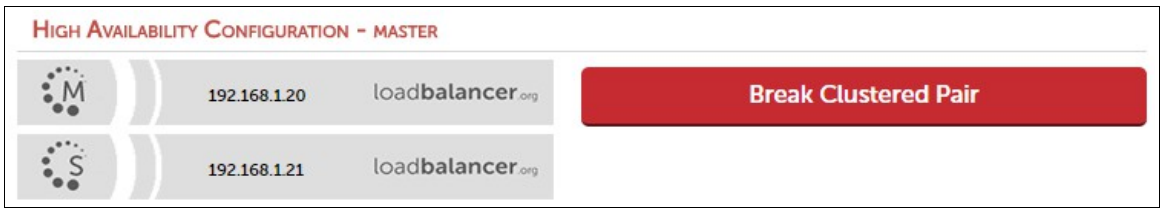
- Deploy a second appliance that will be the slave and configure initial network settings
- Using the WebUI, navigate to: *Cluster Configuration > High-Availability Configuration*



- Specify the IP address and the *loadbalancer* users password (the default is 'loadbalancer') for the slave (peer) appliance as shown above
- Click **Add new node**
- The pairing process now commences as shown below:



- Once complete, the following will be displayed:



- 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 master appliance will also automatically restart heartbeat on the slave appliance.

> Note:
>
> Please refer to chapter 9 – Appliance Clustering for HA in the Administration Manual for more detailed information on configuring HA with 2 appliances.

2 – CONFIGURING A 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, HAProxy must be restarted:

- Using the WebUI, navigate to: *Maintenance > Restart Services and click* ***Restart HAProxy***

3 - COMPANY CONTACT INFORMATION

Website	URL: www.loadbalancer.org
North America (US)	Loadbalancer.org, Inc. 4250 Lancaster Pike, Suite 120 Wilmington DE 19805 USA Tel: +1 888.867.9504 Fax: +1 302.213.0122 Email (sales): sales@loadbalancer.org Email (support): support@loadbalancer.org
North America (Canada)	Loadbalancer.org Ltd 300-422 Richards Street Vancouver, BC V6B 2Z4 Canada Tel: +1 866.998.0508 Fax: +1 302.213.0122 Email (sales): sales@loadbalancer.org Email (support): support@loadbalancer.org
Europe (UK)	Loadbalancer.org Ltd. Compass House North Harbour Business Park Portsmouth, PO6 4PS UK Tel: +44 (0)330 3801064 Fax: +44 (0)870 4327672 Email (sales): sales@loadbalancer.org Email (support): support@loadbalancer.org
Europe (Germany)	Loadbalancer.org GmbH Tengstraße 27 D-80798 München Germany Tel: +49 (0)89 2000 2179 Fax: +49 (0)30 920 383 6495 Email (sales): vertrieb@loadbalancer.org Email (support): support@loadbalancer.org