loadbalancer.org

# Load Balancing RSA Authentication Manager

## Deployment Guide

v1.2.2

# Table of Contents

# 1. About this Guide

This guide details the steps required to configure a load balanced RSA Authentication Manager environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any RSA Authentication Manager 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 Authentication Manager. 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. RSA Authentication Manager Software Versions Supported

- RSA Authentication Manager – v8.0 & later

# 5. RSA Authentication Manager

RSA Authentication Manager is a multi-factor authentication solution that verifies authentication requests and centrally administers authentication policies for enterprise networks. Authentication Manager can be used to to manage security tokens (RSA SecureID Tokens), users, multiple applications, agents, and resources across physical sites, and to help secure access to network and web-accessible applications, such as SSL-VPNs and web portals.

# 6. Load Balancing Authentication Manager

> Note:
>
> It's highly recommended that you have a working RSA Authentication Manager environment first before implementing the load balancer.

## LOAD BALANCING & HA REQUIREMENTS

A load balancer distributes authentication requests and facilitates failover between multiple Web Tier Servers. Adding a load balancer to your deployment provides the following benefits:

- The load balancer distributes Risk Based Authentication (RBA) requests between the primary and the replica Web Tiers.
- The load balancer can be configured to forward Self-Service Console requests coming through the HTTPS port to the Web Tier or the primary instance hosting the Self-Service Console. If the primary in stance is not functioning and a replica instance is promoted to take its place, users can continue to use the same URL for the Self-Service Console.
- Provides failover if one of the Authentication Manager instances or Web Tiers experiences downtime.

## PERSISTENCE (AKA SERVER AFFINITY)

The load balancer must send a client to the same server repeatedly during a session. The load balancer must send the client to the same Authentication Manager instance or Web Tier server, depending on your deployment scenario, during an authentication session.

## X-FORWARDED-FOR HEADERS

Since the load balancer acts as a proxy, all Web Tier requests appear to come from the load balancer. RSA/EMC recommend that X-Forwarded-For headers should be enabled on the load balancer – this is the default configuration for layer 7 VIPs.

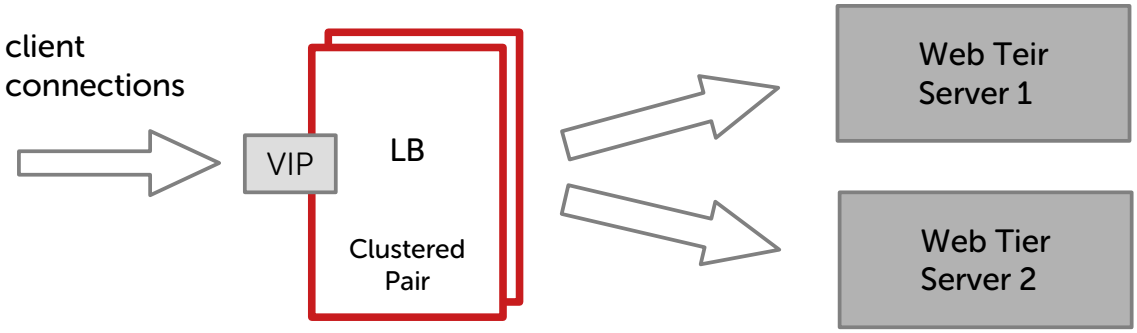
## PORT REQUIREMENTS

The following table shows the port list that must be load balanced.

| TCP Port | Uses |
|---|---|
| 443 or 7023 | HTTPS or HTTPS alternative port |

# 7. Deployment Concept

To load balance the Web Tier, a single VIP is required as shown below. Clients then connect to the Virtual Service (VIP) on the load balancer rather than connecting directly to a one of the Web Tier servers. These connections are then load balanced across the Web Tier servers distribute the load according to the load balancing algorithm selected.




VIPs = **V**irtual **IP** Addresses

> 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 15 for more details on configuring a clustered pair.

# 8. Load Balancer Deployment Method

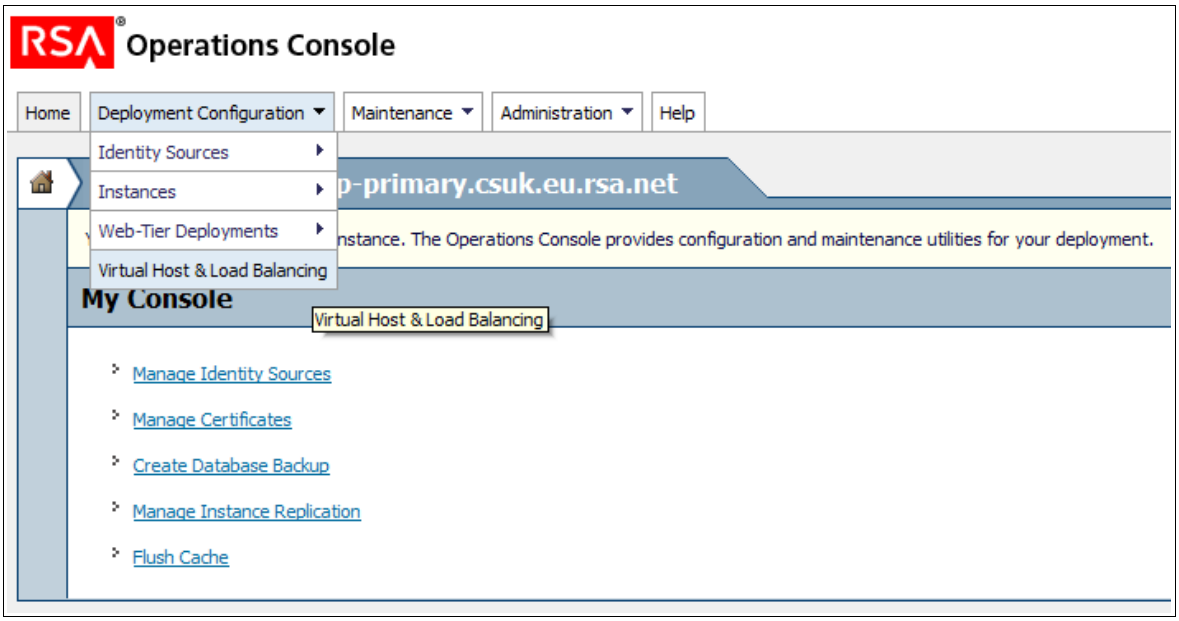
## LAYER 7 SNAT MODE

Layer 7 load balancing uses a proxy (HAProxy) at the application layer. Inbound requests are terminated on the load balancer, and HAProxy generates a new request to the chosen RSA Server. Return traffic passes via the load balancer. Since layer 7 works as a proxy, there is not need to set the appliance as the gateway.

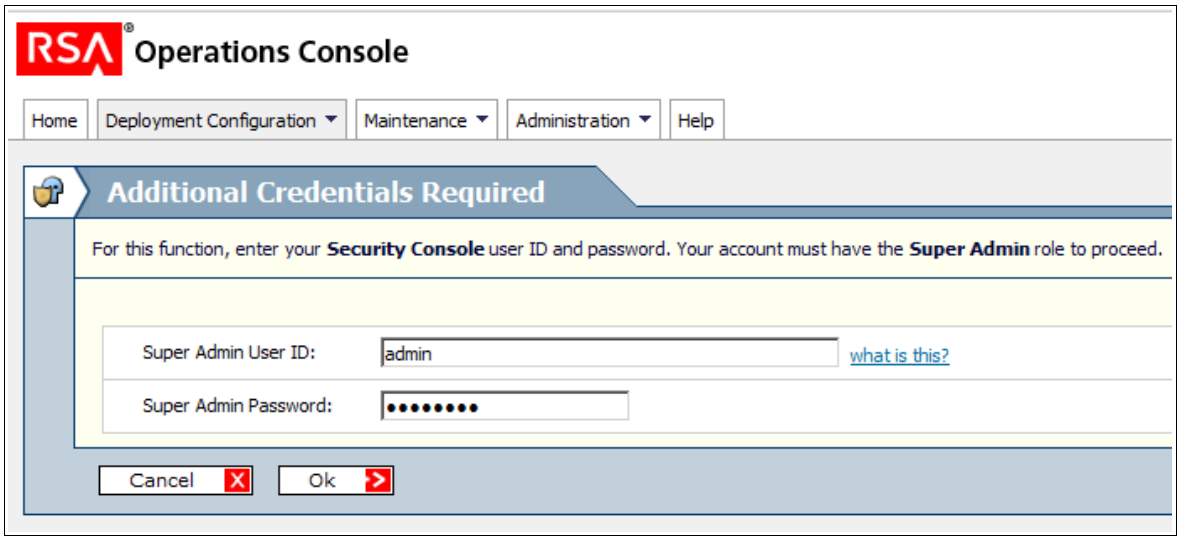
This method is non-transparent, i.e. the load balancer proxies the application traffic to the Web Tier Servers so that the source IP address of all traffic is the load balancer

# RSA Authentication Manager Configuration

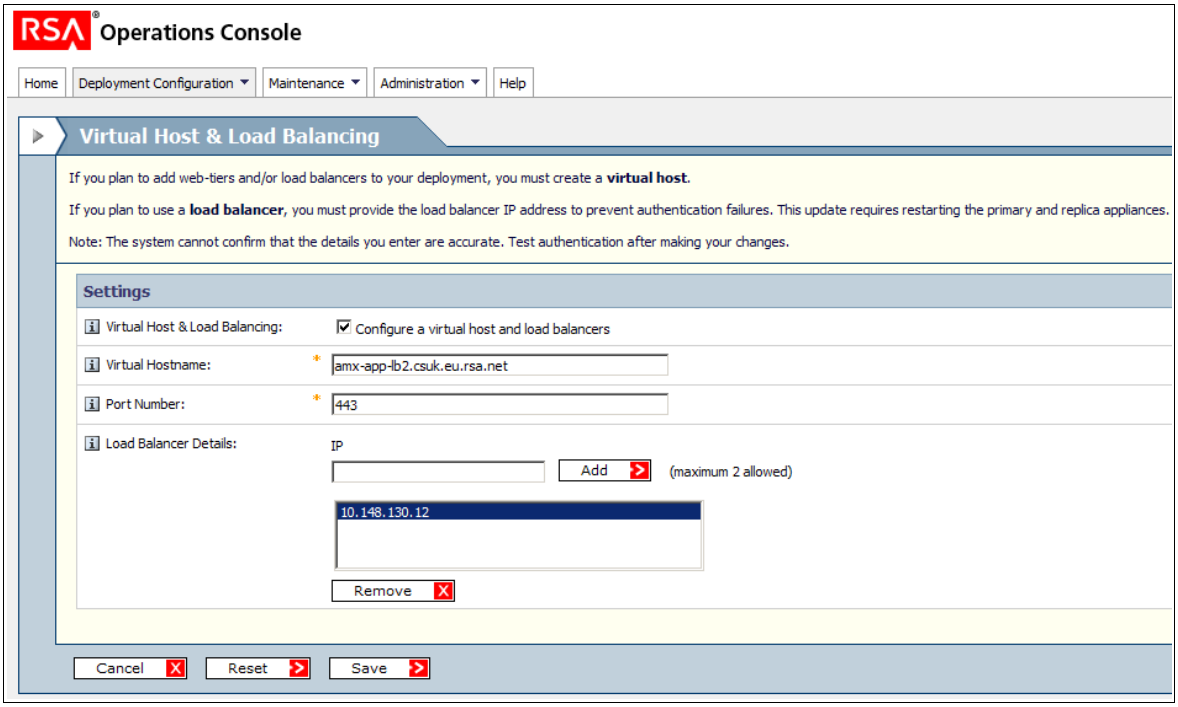
1. Log on to the Operation console and go to: *Deployment Configuration -> Virtual Host & Load Balancing*



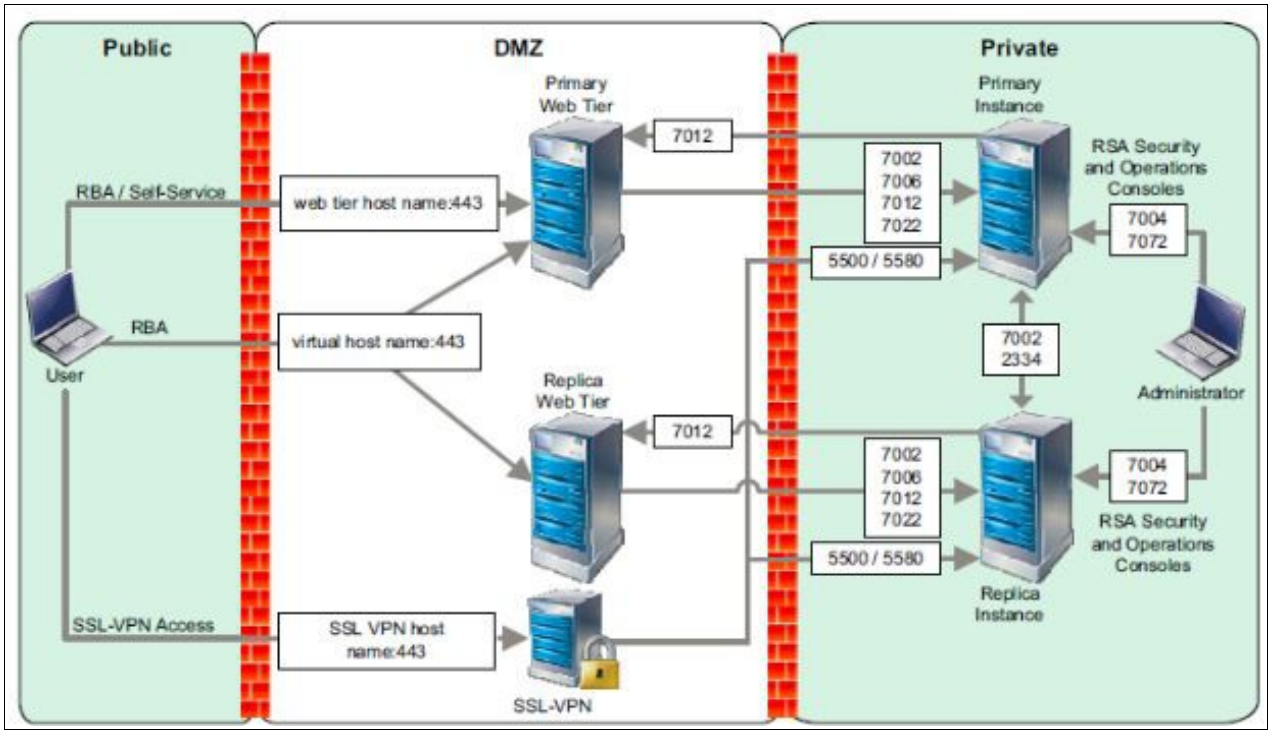

2. Enter your SuperAdmin credentials and click OK

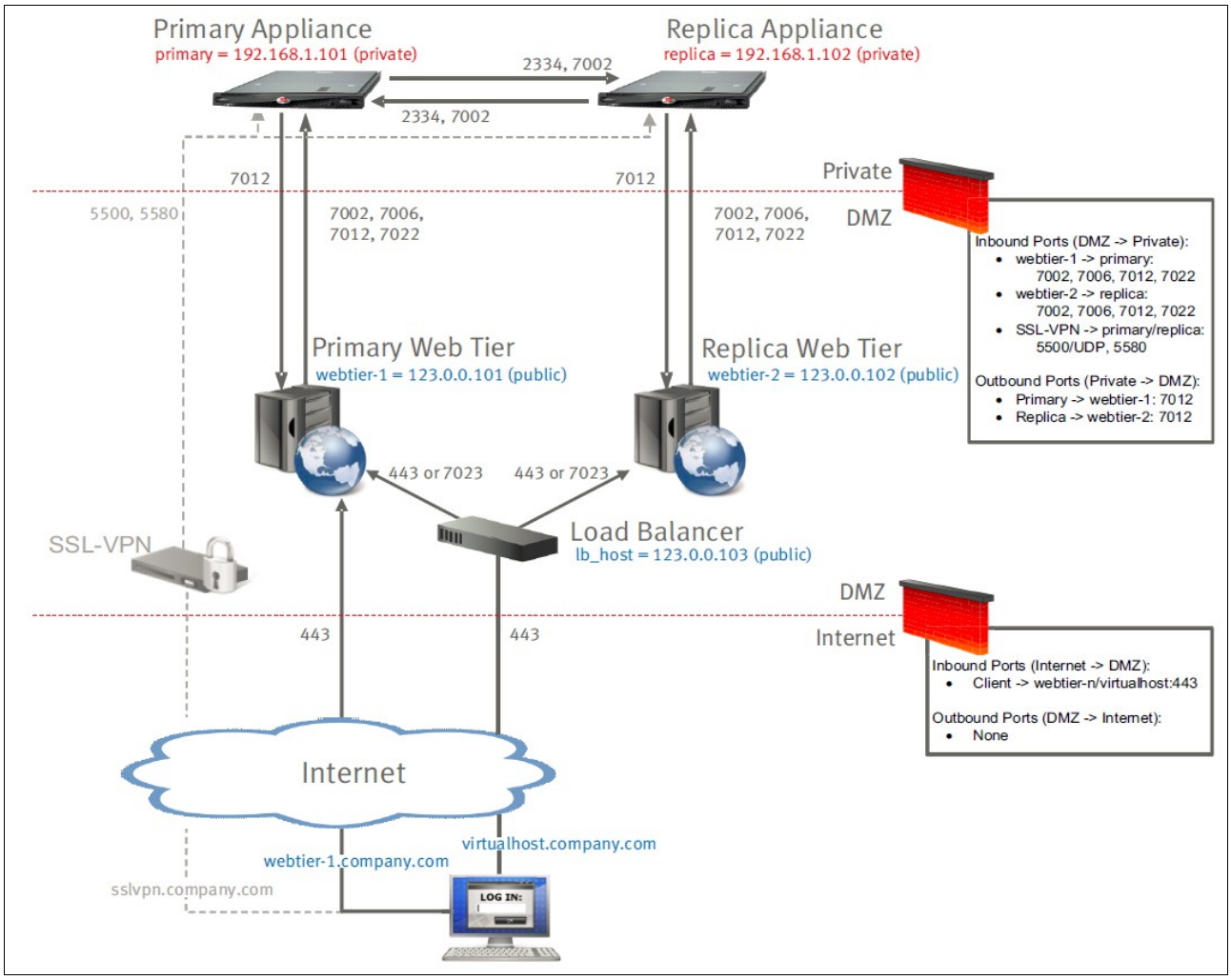



3. Check the box: *Configure a virtual host and load balancers* then fill in the FQHN (Fully Qualified Host Name) of your Load Balancer and the IP Address, leave the default port number to 443 and finally click on save




## RSA AUTHENTICATION MANAGER TOPOLOGY DIAGRAMS






# 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***

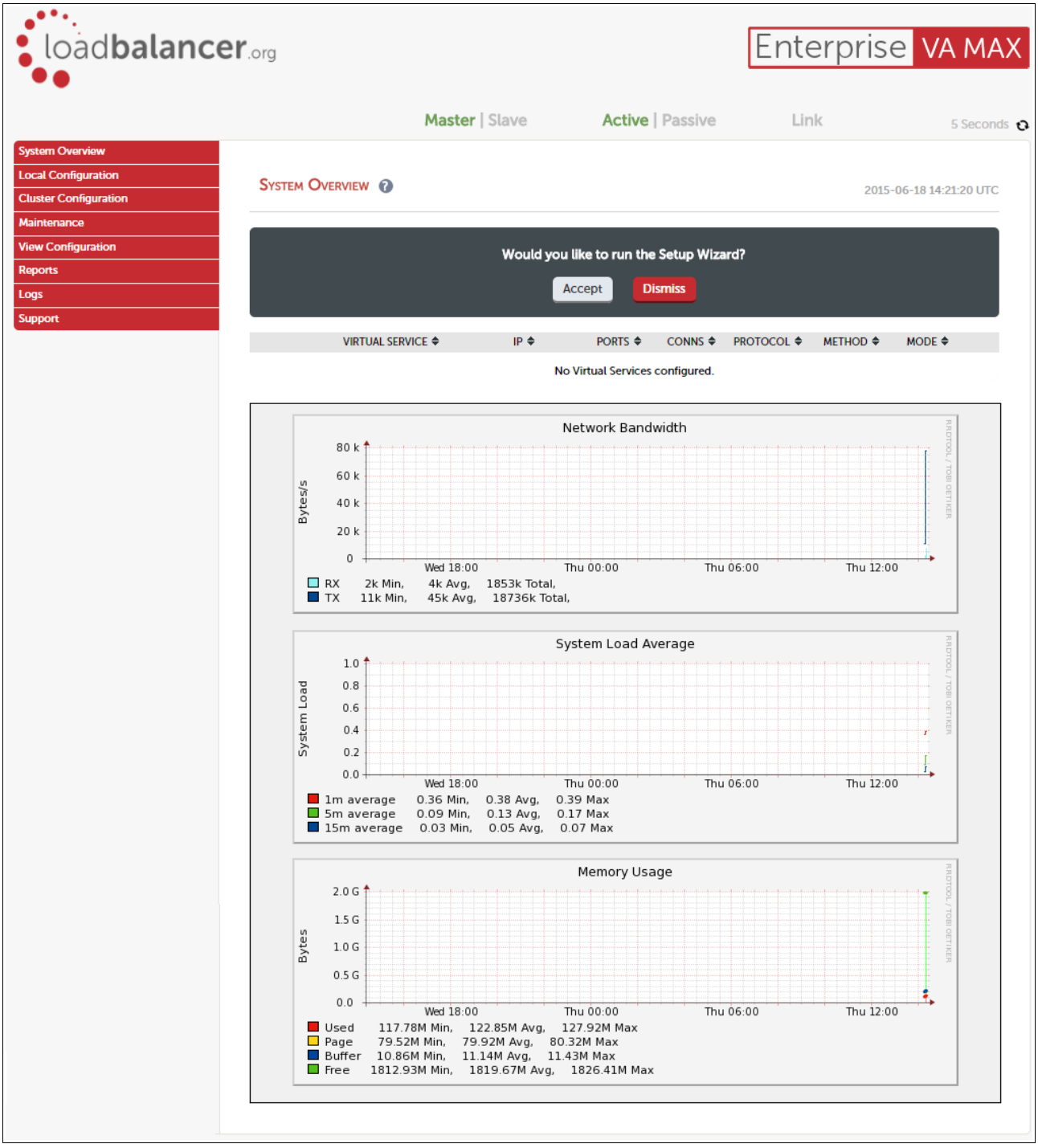
*(replace 192.168.2.21 with the IP address of your load balancer if it's been changed from the default)*

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 below:




(shows v8.2.x)

## HA CLUSTERED PAIR CONFIGURATION

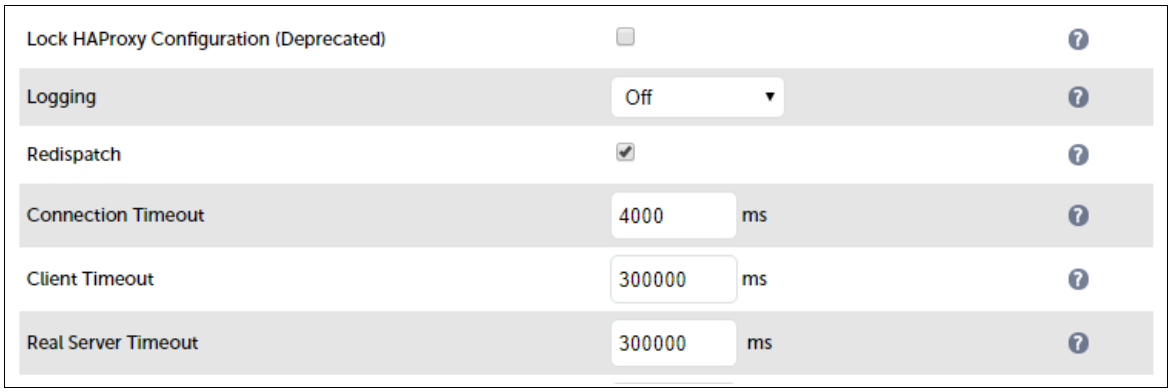
Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary slave unit is covered in section 1 of the Appendix on page 15.

# 10. Appliance Configuration for RSA Authentication Manager

## CONFIGURE LAYER 7 GLOBAL SETTINGS

To ensure that client connections remain open during periods of inactivity, the Client Timeout and 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*



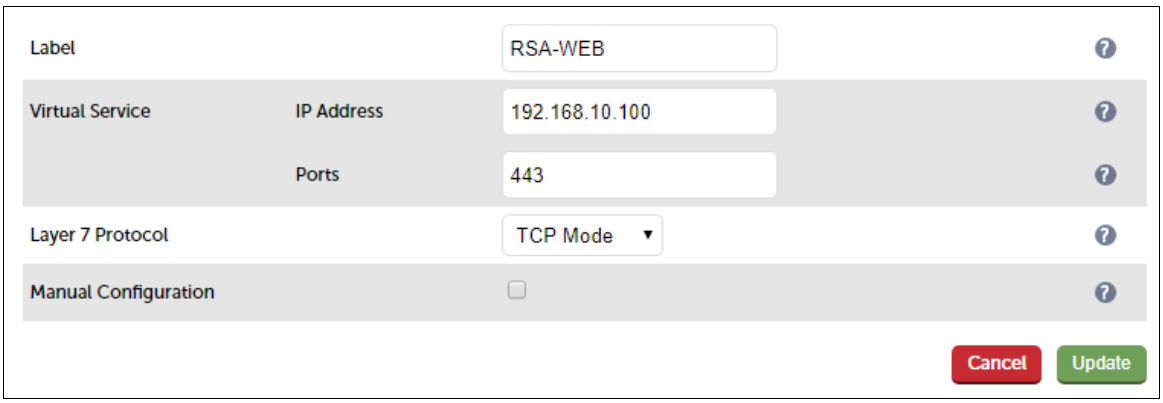

2. Change *Client Timeout* to **300000** as shown above (i.e. 5 minutes)
   *N.B. You can also enter **5m** rather than 300000*

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

## CONFIGURE THE VIRTUAL SERVICE (VIP)

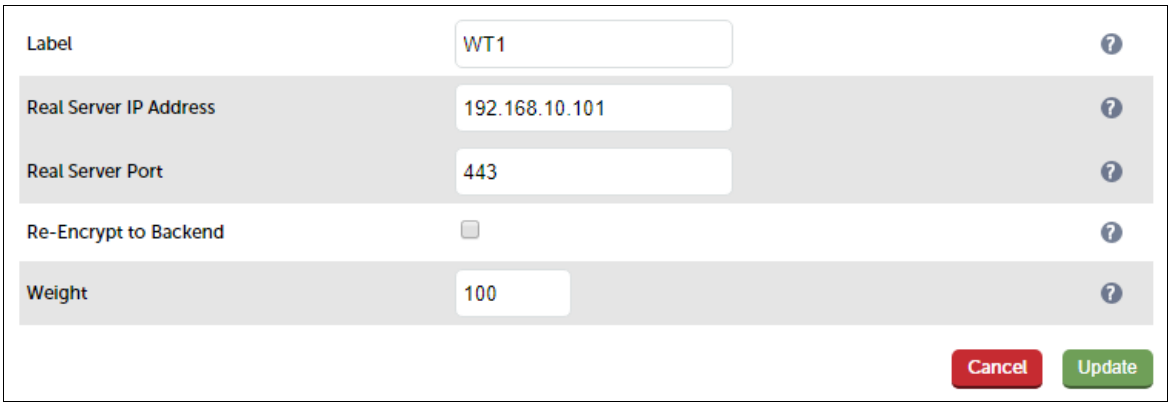
1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Virtual Service* and click **Add a New Virtual Service**
2. Enter the following details:



3. Enter an appropriate label for the VIP, e.g. **RSA-WEB**
4. Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.10.100**
5. Set the *Virtual Service Ports* field to **443**
6. 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 VIP
2. Enter the following details:




3. Enter an appropriate label for the RIP, e.g. **WT1**
4. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.10.101**
5. Change the *Real Server Port* field to **443**
6. Click **Update**
7. Repeat the above steps to add your other Web Tier server(s)

## FINALIZING THE CONFIGURATION

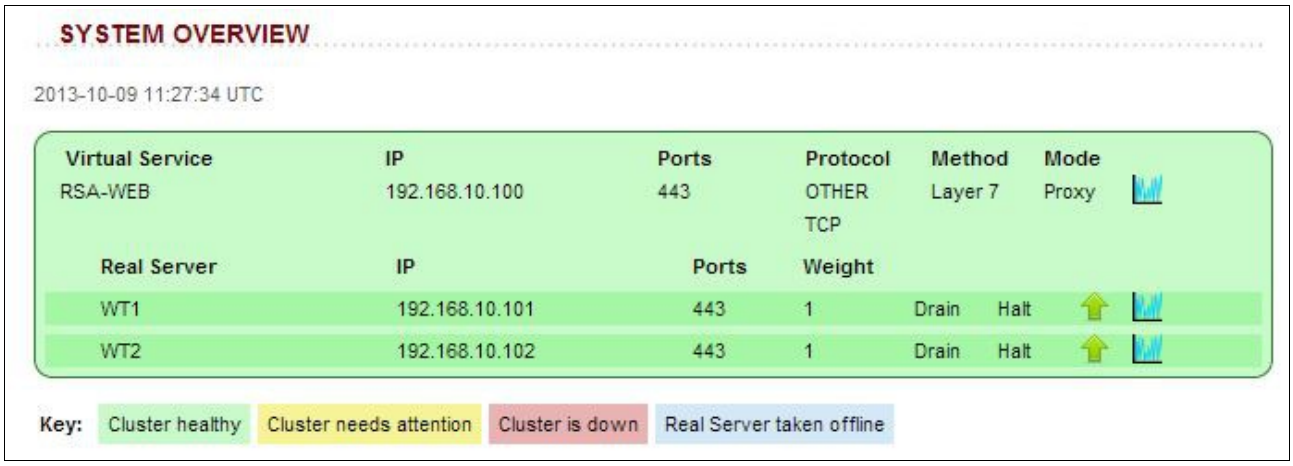
To apply the new settings, HAProxy must be restarted as follows:

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

# 11. Testing & Verification

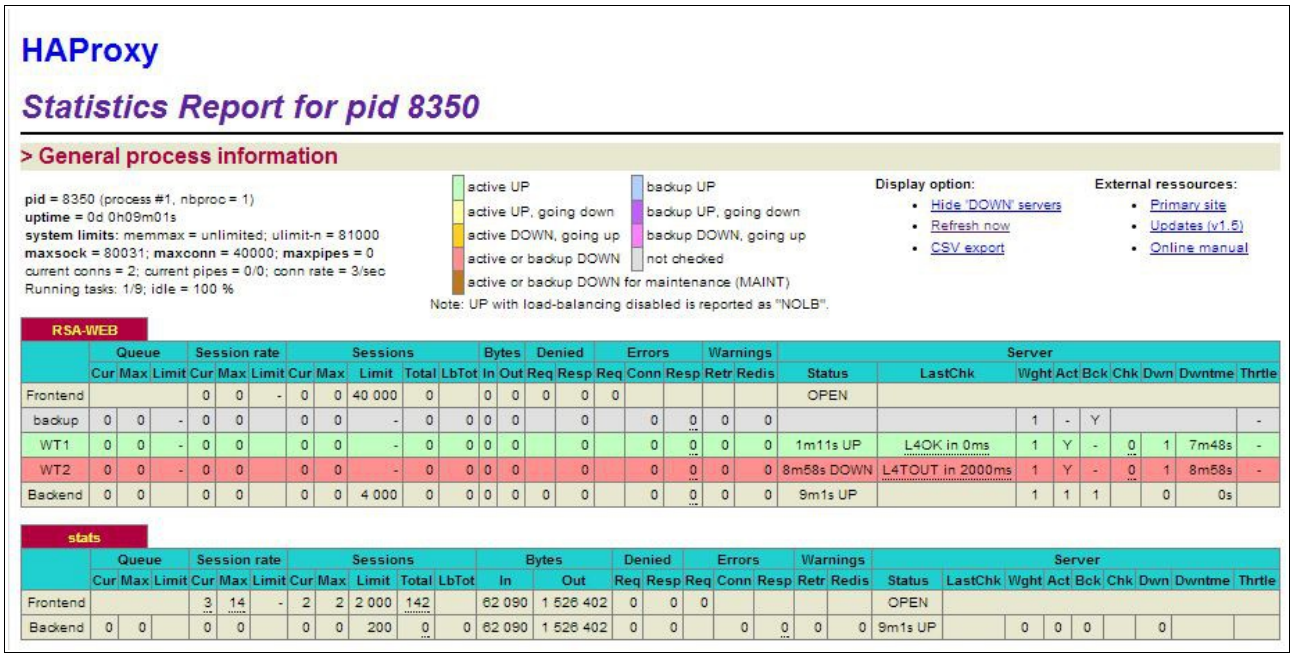
## USING SYSTEM OVERVIEW

The System Overview is accessed using the WebUI. It shows a graphical view of the VIP and the RIPs (i.e. the Web Tier Servers) and shows the state/health of each server as well as the state of the each cluster as a whole. The example below shows that both servers are healthy and available to accept connections.




## LAYER 7 STATISTICS REPORT

The Layer 7 Statistics report gives a summary of all layer 7 configuration and running stats as shown below. This can be accessed in the WebUI using the option: *Reports > Layer 7 Status*. In this example, WT1 is up and available, WT2 is down.




## APPLIANCE LOGS

Logs can be very useful when trying to diagnose issues. Layer 7 logging is not enabled by default (because its extremely verbose) and can be enabled using the WebUI option: *Cluster Configuration > Layer 7 – Advanced Configuration*, and then viewed using the option: *Logs > Layer 7*.

# 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

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 RSA Authentication Manager 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

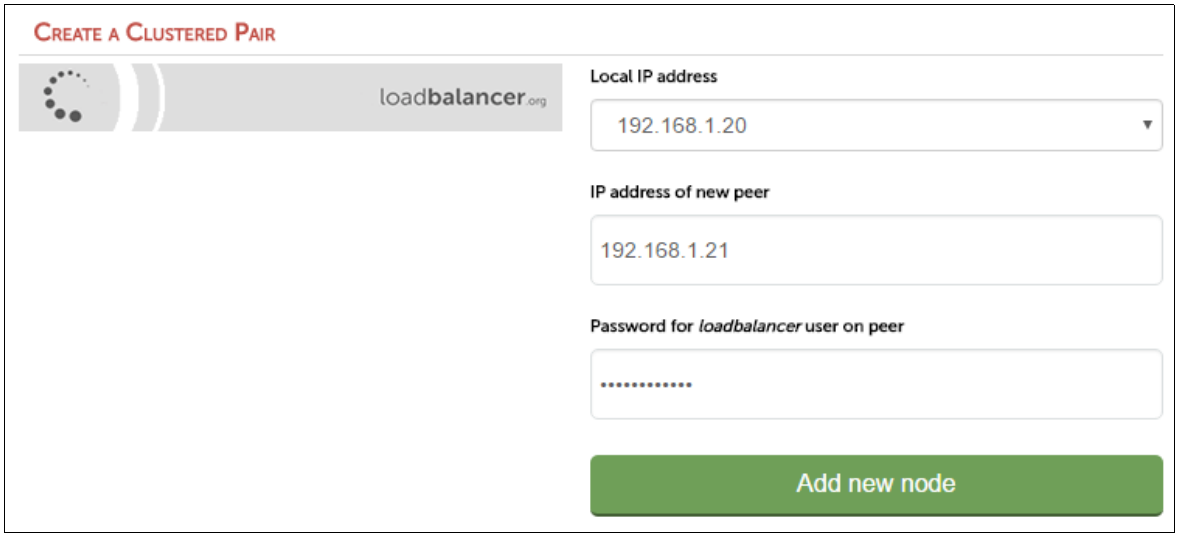
**Version 7:**

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

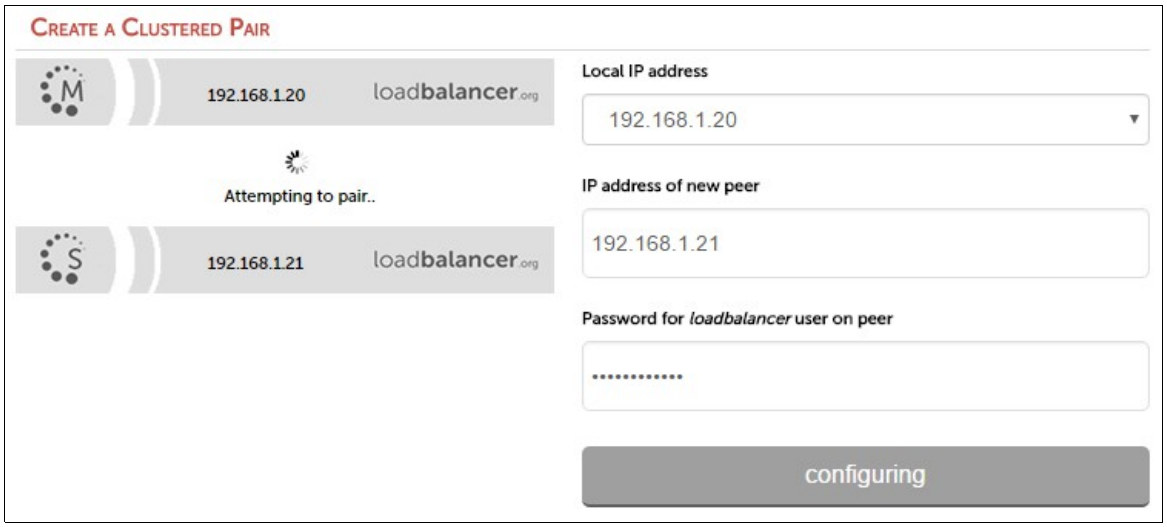
**Version 8:**

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

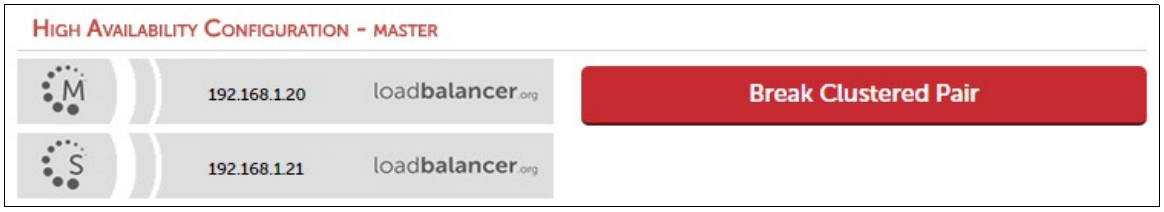
- Deploy a second appliance that will be the slave and configure initial network settings
- Using the WebUI, navigate to: *Cluster Configuration > High-Availability Configuration*



- 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 - COMPANY CONTACT INFORMATION

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