Appliance Quick Start Guide

Version 8.5.8 Revision 1.0.0

loadbalancer.org

Table of Contents

1. About this Guide

This quick start guide provides enough information to deploy the appliance, configure a simple load balanced test environment and test and verify its functionality.

> Note
>
> Please also refer to the Administration Manual for much more detailed information on setting up the appliance and configuring a load balancing solution. For information on configuring the appliance for specific applications, please refer to our extensive library of Deployment Guides.

2. Appliance Configuration Overview

Initial network configuration is carried out at the console using the Network Setup Wizard.

Once an IP address has been allocated, load balanced services can be configured using the WebUI, either using the Setup Wizard (for Layer 7 services) or by manually defining the Virtual Services (VIPs) and associated Real Servers (RIPs).

By default, the WebUI is accessible on HTTPS port **9443.** HTTP access on port **9080** can also be enabled if required - please refer to the "Appliance Security" section below.

We always recommend that where possible two appliances are deployed as a clustered pair for high availability and resilience, this avoids introducing a single point of failure to your network.

We recommend that the master is fully configured first, then the slave should be added. Once a pair is configured, load balanced services must be configured & modified on the master appliance. The slave appliance will then be kept in sync automatically. More information on configuring an HA pair can be found in the section Configuring HA - Adding a Slave Appliance.

3. Appliance Security

Security Mode

To control how the appliance is accessed and which features are enabled, 3 security modes are provided:

- **Secure -** this is the default mode. In this mode:
  - the WebUI is accessible on HTTPS port **9443.** If you attempt to access the WebUI on HTTP port **9080** you will be redirected to HTTPS port **9443**
  - access to the "Execute Shell Command" menu option is disabled
  - the ability to edit the firewall script & the lockdown wizard is disabled
  - 'root' user console & SSH password access are disabled
- **Custom -** In this mode, the security options can be configured to suit your requirements
- **Secure - Permanent -** this mode is the same as Secure, but the change is **irreversible**

> Important
>
> Only set the security mode to **Secure - Permanent** if you are 100% sure this is what you want!

To configure the Security Mode:

1. Using the WebUI, navigate to: *Local Configuration > Security*
2. Select the required *Appliance Security Mode*
3. If **Custom** is selected, configure the other options to suit your requirements
4. Click **Update**

Note | More information on all available options can be found here.

Passwords

The password for the '**loadbalancer**' WebUI user account and the '**root**' Linux user account are set during the Network Setup Wizard. These can also be changed at any time as explained below:

1 - the 'root' Linux account:

As explained above, 'root' user console & SSH password access are disabled by default. If enabled, the 'root' password should be changed at the console, or via an SSH session using the following command:

```
passwd
```

2 - the 'loadbalancer' WebUI account:

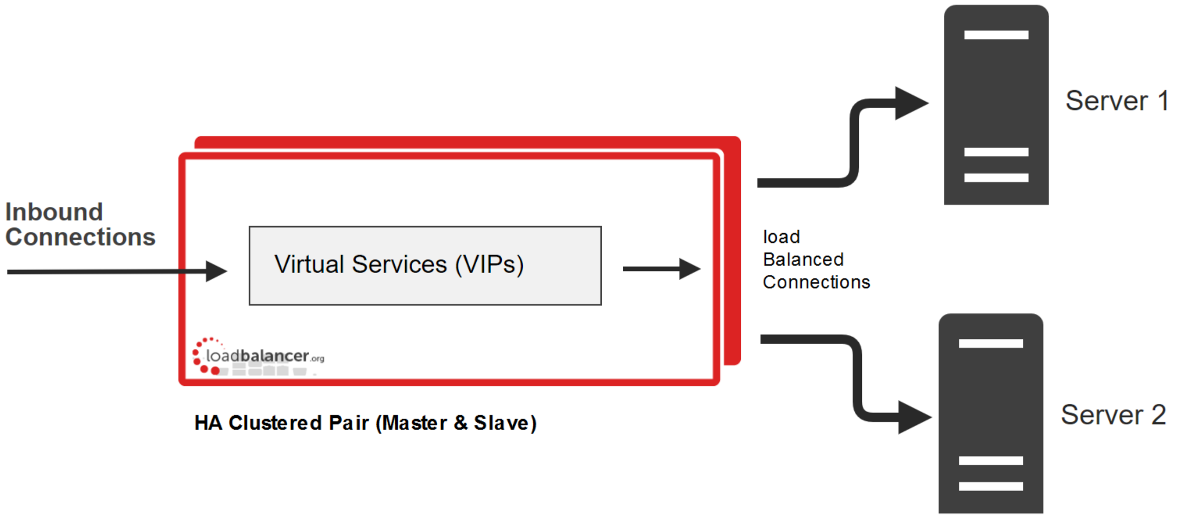
This can be changed using the WebUI menu option: *Maintenance > Passwords*

Security Lockdown Script

The appliance also includes a security lockdown command (lbsecure) that enables passwords to be set, network access to be locked down and SSH key regeneration in one simple step. This command can be run on a single appliance or an HA pair. More information about the command can be found here.

4. Deployment Concept

Once deployed, clients connect to the Virtual Service(s) (VIPs) on the load balancer rather than connecting directly to one of the load balanced servers. These connections are then distributed between the load balanced servers according to the load balancing algorithm selected.



Note

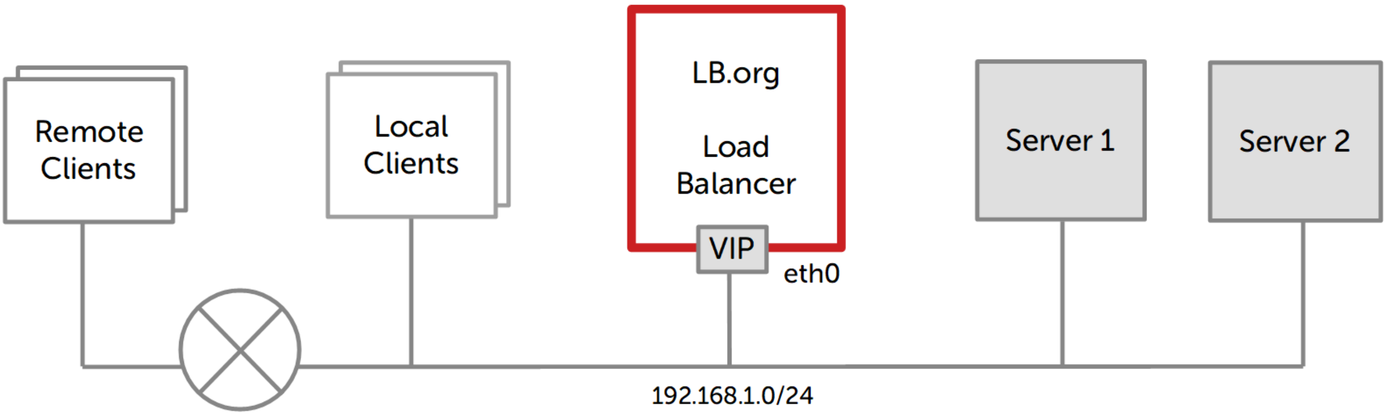
We always recommend that 2 appliances are deployed as an active/passive HA pair. The slave appliance automatically takes over if the master unit fails. Please refer to the section Configuring HA - Adding a Slave Appliance for more information on configuring HA using 2 appliances.

5. One-Arm and Two-Arm Topologies

The number of 'arms' is a descriptive term for how many interfaces are used to connect a device to a network. It’s common for a load balancer that uses a routing method (NAT) to have a two-arm configuration. Proxy based load balancers (SNAT) commonly use a one-arm configuration..

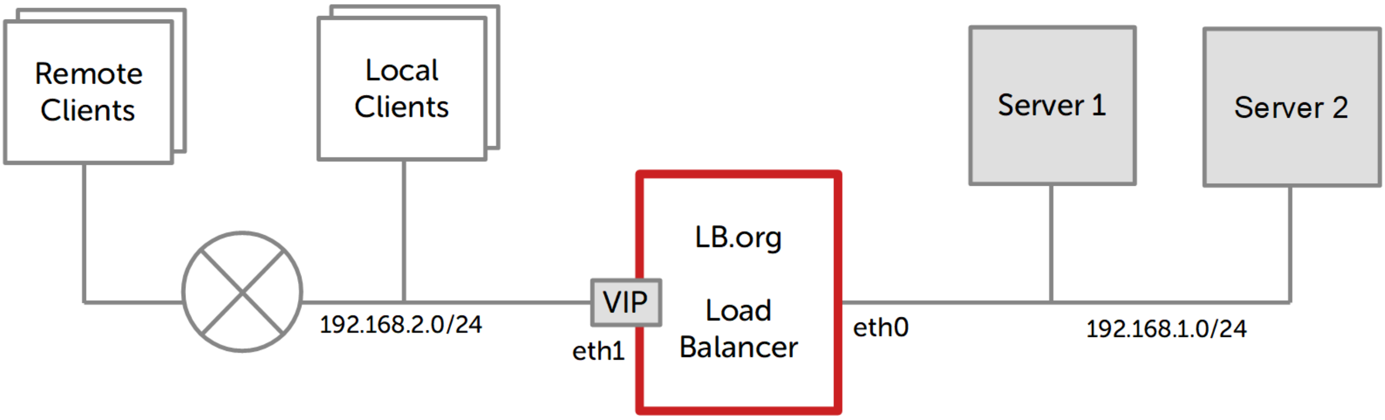
One Arm

In this mode, the VIP and the load balanced servers are located in a single subnet. The load balancer requires a single network interface adapter - eth0 in the diagram below.



Two Arm

In this mode, 2 subnets are used. The VIP is located in one subnet and the load balanced servers are located in the other subnet. The load balancer requires 2 interfaces - eth0 and eth1 in the diagram below. Note that this can be achieved by using two network adapters, or by creating VLANs on a single adapter.



6. Supported Load Balancing Methods

The Loadbalancer.org appliance is one of the most flexible load balancers available. The design allows different load balancing modules to utilize the core high availability framework of the appliance. Multiple load balancing methods can be used at the same time or in combination with each other. The table below describes the methods supported by the appliance.

Layer	Method	Comments	Topology	Note
Layer 4	DR (Direct Routing)	Ultra-fast local server based load balancing • Requires solving the 'ARP Problem' on the Real Servers - more details about the ARP problem are available here.	One-Arm (*)	(1)
Layer 4	NAT (Network Address Translation)	Fast Layer 4 load balancing • The appliance must be the default gateway for the Real Servers	One or Two-Arm	(1)
Layer 4	TUN	Similar to DR but works across IP encapsulated tunnels	One-Arm	(2)
Layer 4	SNAT (Source Network Address Translation)	Fast layer 4 SNAT supporting both TCP & UDP • Requires no Real Server changes	One or Two-Arm	(3)
Layer 7	SSL Termination (Pound & STunnel)	Usually required in order to process cookie persistence in HTTPS streams on the load balancer • SSL Termination is processor intensive	One or Two-Arm	(4)
Layer 7	SNAT (Source Network Address Translation using HAProxy)	Layer 7 allows greater flexibility including full SNAT and remote server load balancing, cookie insertion and URL switching • Very simple to implement • Requires no Real Server changes • Not as fast as Layer 4 methods	One or Two-Arm	(4)

(*) DR mode can also be used in a multi-homed configuration where real servers are located in different subnets. In this case, the load balancer must have an interface in the same subnet to enable layer 2 connectivity which is required for DR mode to operate.

Note	Comment
(1)	Recommended for high performance fully transparent and scalable solutions

Note	Comment
(2)	Only required for Direct Routing implementation across routed networks (rarely used)
(3)	Recommended when you want to load balance both TCP and UDP but you’re unable to use DR mode or NAT mode due to network topology or Real Server related reasons
(4)	Recommended if HTTP cookie persistence is required, also used for several Microsoft applications such as Exchange, Sharepoint & Remote Desktop Services and for overall deployment simplicity since real servers can be on any accessible subnet and no Real-Server changes are required

7. Appliance Deployment

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 1 CPU, 2GB 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 the Administration Manual and view the ReadMe.txt text file included in the VA download for more detailed information on deploying the VA using various Hypervisors.

Note

For the VA, 4 NICs are included but only eth0 is connected by default at power up. If the other NICs are required, these should be connected using the network configuration screen within the Hypervisor.

Hardware Appliance

For details of all hardware models and for information on installing and connecting the appliance, please click here.

Cloud Appliance

AWS

For details of deploying and configuring the Amazon Web Services (AWS) appliance please refer to the AWS Quick Start Guide.

Azure

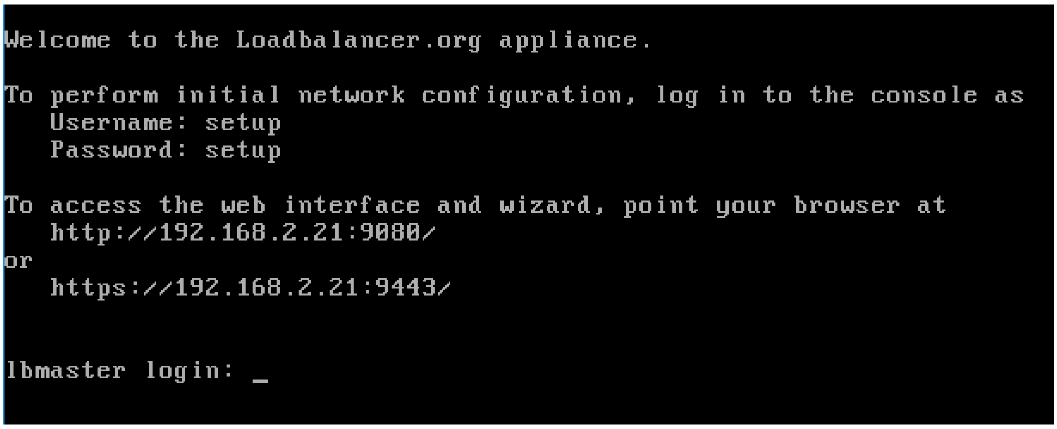
For details of deploying and configuring the Microsoft Azure appliance please refer to the Azure Quick Start Guide.

Google Cloud Platform

For details of deploying and configuring the Google Cloud appliance please refer to the GCP Quick Start Guide.

8. Configuring Initial Network Settings

After power up, the following startup message is displayed on the appliance console:



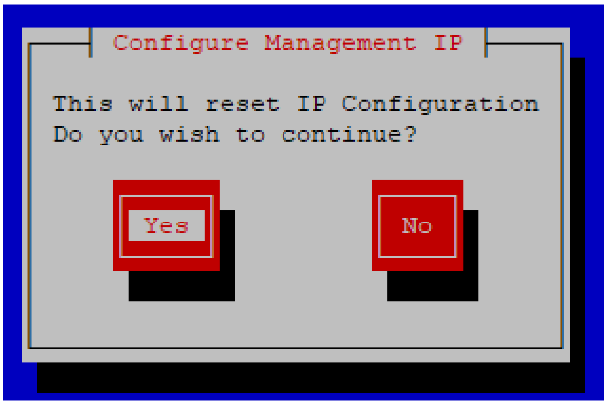
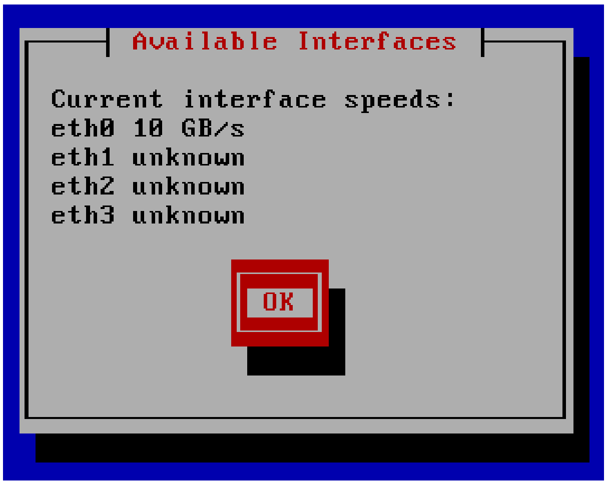
```
Welcome to the Loadbalancer.org appliance.

To perform initial network configuration, log in to the console as
   Username: setup
   Password: setup

To access the web interface and wizard, point your browser at
   http://192.168.2.21:9080/
or
   https://192.168.2.21:9443/


lbmaster login: _
```

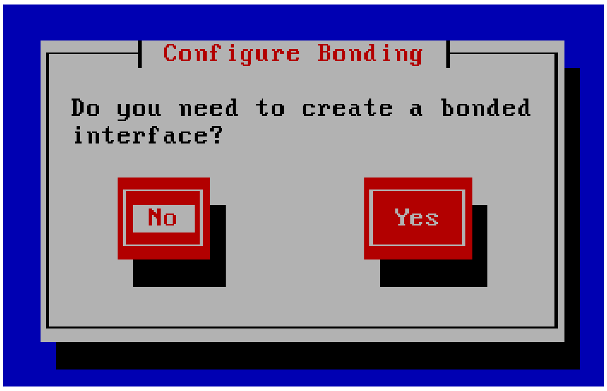
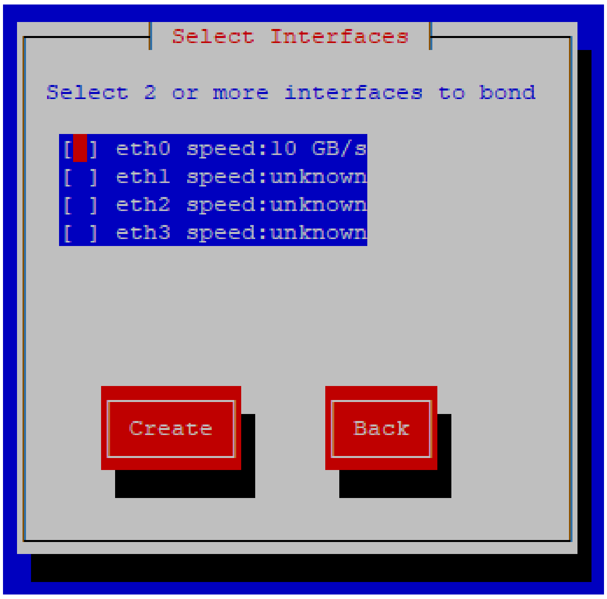
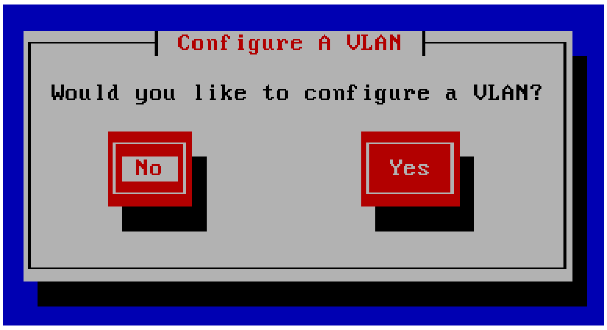
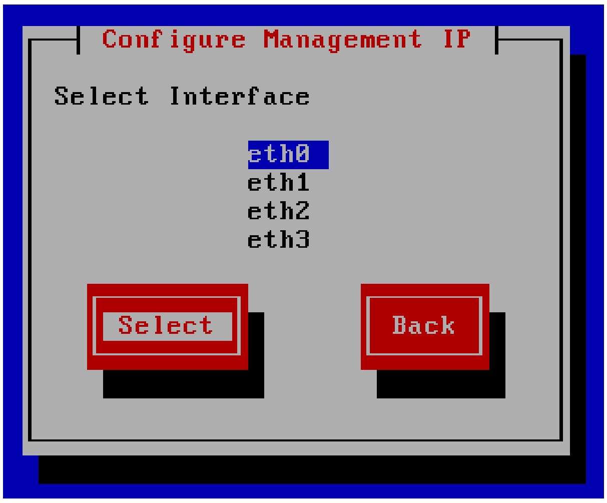
As mentioned in the text, initial network settings are configured using the Network Setup Wizard. The wizard starts automatically when you login as the 'setup' user at the appliance console.

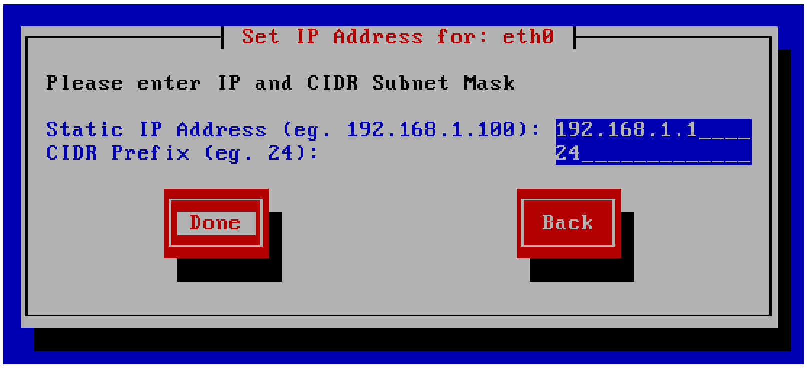
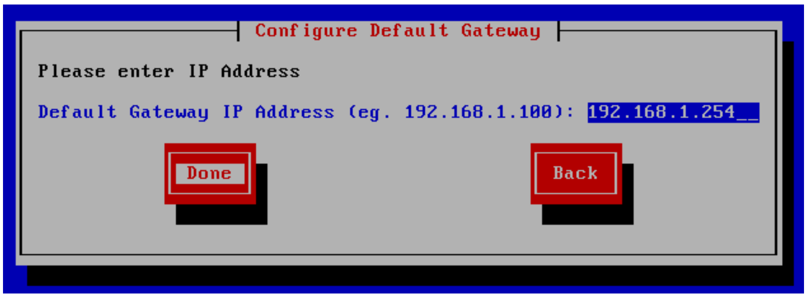
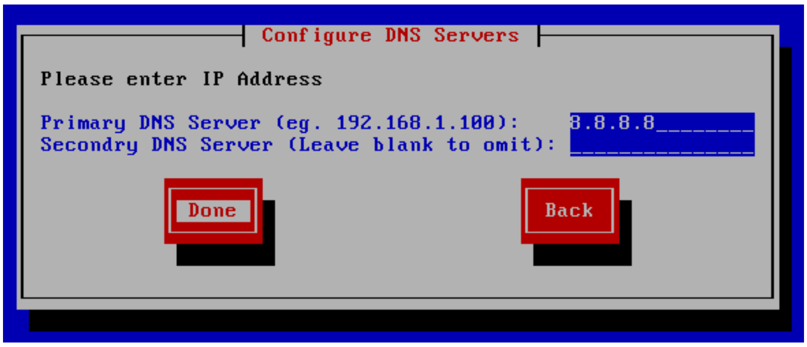
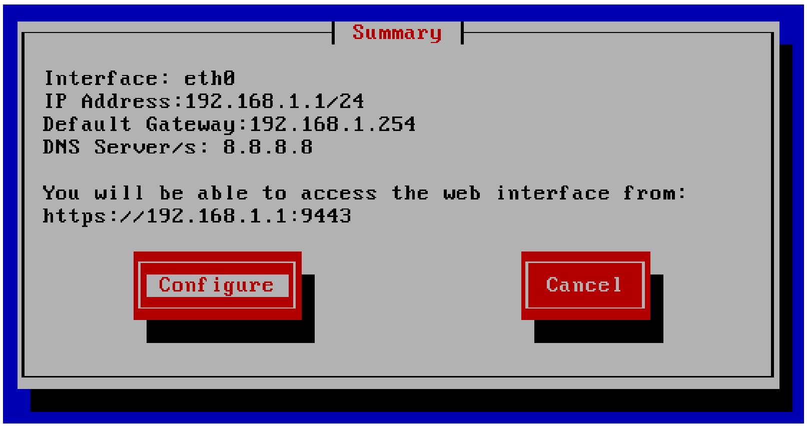
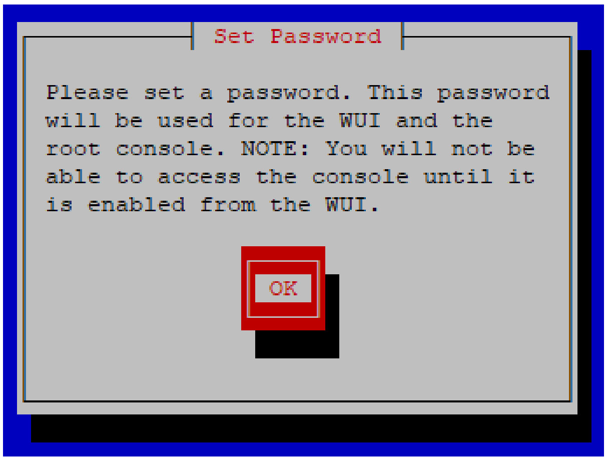
login to the console:

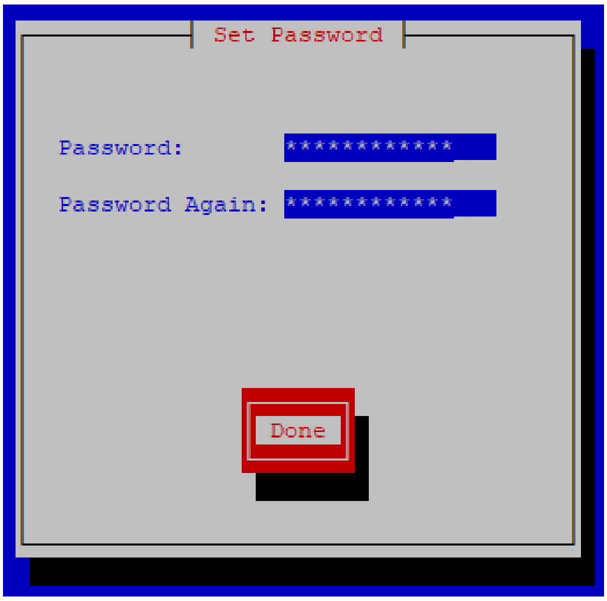
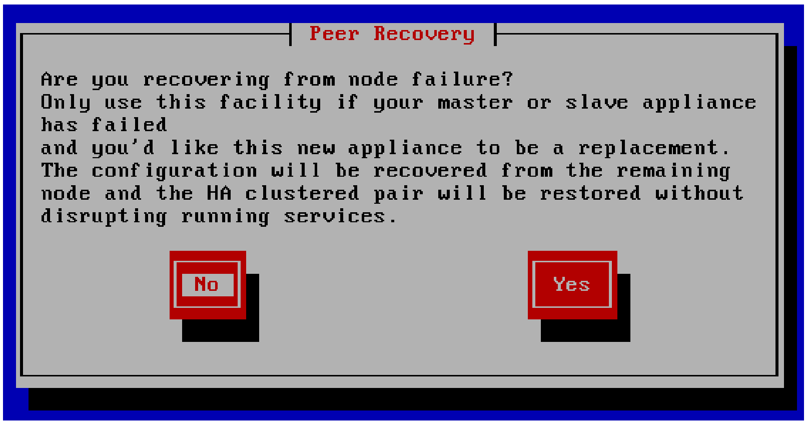
Username: setup
Password: setup

A series of screens will be displayed that allow network settings to be configured:

 Configure Management IP This will reset IP Configuration Do you wish to continue? 	To continue with the Network Setup Wizard select **Yes** and hit <ENTER> to continue.
 Available Interfaces Current interface speeds: eth0 10 GB/s eth1 unknown eth2 unknown eth3 unknown 	A list of available interfaces will be shown, hit <ENTER> to continue.

 Configure Bonding Do you need to create a bonded interface? 	Select **Yes** If you want to configure a bonded interface, if not leave **No** selected, then hit <ENTER> to continue. If you select **Yes**, the screen shown below will be displayed:
 Select Interfaces Select 2 or more interfaces to bond [ ] eth0 speed:10 GB/s [ ] eth1 speed:unknown [ ] eth2 speed:unknown [ ] eth3 speed:unknown 	Using the space bar, select the interfaces you'd like to include in the bond, then click **Create**.
 Configure A VLAN Would you like to configure a VLAN? 	Select **Yes** If you want to configure a VLAN, if not leave **No** selected, then hit <ENTER> to continue. If you select **Yes** you'll be prompted to enter a VLAN Tag ID.
 Configure Management IP Select Interface eth0 eth1 eth2 eth3 	Select the interface that will be used to manage the appliance, select **Select** and hit <ENTER> to continue.

 Set IP Address for: eth0 Please enter IP and CIDR Subnet Mask Static IP Address (eg. 192.168.1.100): 192.168.1.1____ CIDR Prefix (eg. 24): 24_____________ 	Enter the required management IP address and CIDR prefix, select **Done** and hit <ENTER> to continue. Note A subnet mask such as 255.255.255.0 is not valid, in this case enter 24 instead.
 Configure Default Gateway Please enter IP Address Default Gateway IP Address (eg. 192.168.1.100): 192.168.1.254__ 	Enter the default gateway address, select **Done** and hit <ENTER> to continue.
 Configure DNS Servers Please enter IP Address Primary DNS Server (eg. 192.168.1.100): 8.8.8.8________ Secondry DNS Server (Leave blank to omit): _______________ 	Define the required DNS server(s), select **Done** and hit <ENTER> to continue.
 Summary Interface: eth0 IP Address:192.168.1.1/24 Default Gateway:192.168.1.254 DNS Server/s: 8.8.8.8 You will be able to access the web interface from: https://192.168.1.1:9443 	A summary of all settings is displayed, if everything looks good hit <ENTER> to continue, all settings will then be applied.
 Set Password Please set a password. This password will be used for the WUI and the root console. NOTE: You will not be able to access the console until it is enabled from the WUI. 	Hit <ENTER> to continue.

 Set Password Password: ************ Password Again: ************ Done	Enter the password you'd like to use for the 'loadbalancer' WebUI user account and the 'root' Linux user account, select **Done** and hit <ENTER> to continue.
 Peer Recovery Are you recovering from node failure? Only use this facility if your master or slave appliance has failed and you'd like this new appliance to be a replacement. The configuration will be recovered from the remaining node and the HA clustered pair will be restored without disrupting running services. No Yes	At this stage you'll be asked if you're recovering from node (i.e. master or slave) failure. If you're simply deploying a new appliance, select **No** and hit <ENTER> to continue. Note More details on node recovery using this option can be found here.

9. Accessing the WebUI

The WebUI is accessed using a web browser. Appliance authentication is based on Apache .htaccess files. User admin 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. 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 click here.

1. Using a browser, access the WebUI using the following URL:

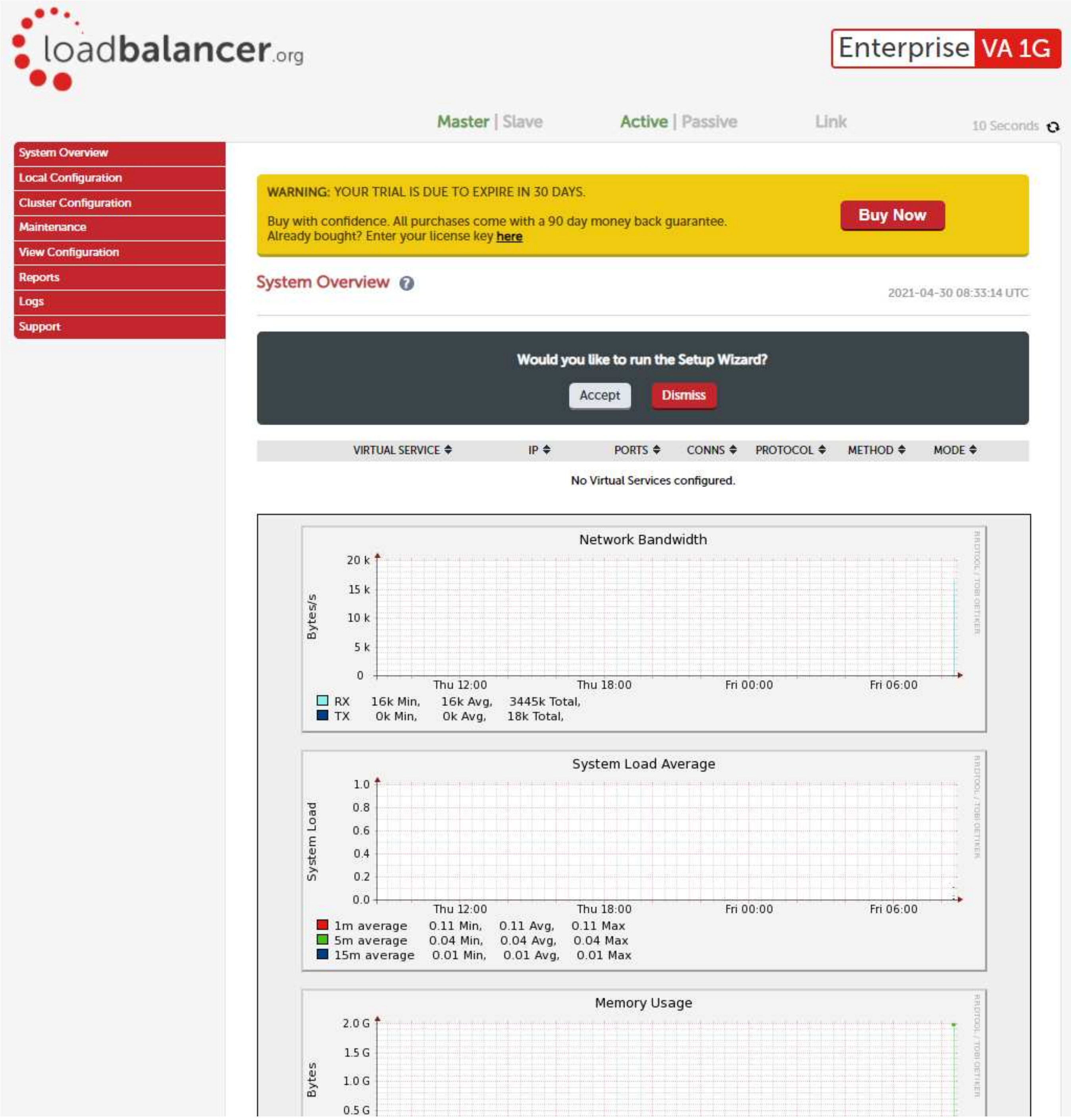
   https://<IP-address-configured-during-network-setup-wizard>:9443/lbadmin/

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:



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**

System Overview

2021-04-30 08:33:14 UTC

Would you like to run the Setup Wizard?

VIRTUAL SERVICE	IP	PORTS	CONNS	PROTOCOL	METHOD	MODE

No Virtual Services configured.

```
RX    16k Min,   16k Avg,   3445k Total,
TX     0k Min,    0k Avg,     18k Total,
```

```
1m average    0.11 Min,   0.11 Avg,   0.11 Max
5m average    0.04 Min,   0.04 Avg,   0.04 Max
15m average   0.01 Min,   0.01 Avg,   0.01 Max
```

Note | The WebUI for the VA is shown, the hardware and cloud appliances are very similar. The yellow licensing related message is platform & model dependant.

3. You'll be asked if you want to run the Setup Wizard. If you click **Accept** the Layer 7 Virtual Service configuration wizard will start. If you want to configure the appliance manually, simple click **Dismiss**.

Main Menu Options

System Overview - Displays a graphical summary of all VIPs, RIPs and key appliance statistics

Local Configuration - Configure local host settings such as IP address, DNS, system time etc.
Cluster Configuration - Configure load balanced services such as VIPs & RIPs
Maintenance - Perform maintenance tasks such as service restarts and taking backups
View Configuration - Display the saved appliance configuration settings
Reports - View various appliance reports & graphs
Logs - View various appliance logs
Support - Create a support download, contact the support team & access useful links

10. Ports Used by the Appliance

By default, the appliance uses the following TCP & UDP ports:

Protocol	Port	Purpose
TCP	22	SSH
TCP & UDP	53	DNS
TCP & UDP	123	NTP
TCP & UDP	161	SNMP
UDP	6694	Heartbeat between master & slave appliances in HA mode
TCP	7778	HAProxy persistence table replication
TCP	9080	WebUI - HTTP (disabled by default)
TCP	9081	Nginx fallback page
TCP	9443	WebUI - HTTPS

11. Licensing

The trial runs for 30 days and is completely unrestricted during this time. After 30 days, the appliance continues to work but it’s no longer possible to make changes to the configuration. If you need more time to complete your evaluation, please contact sales@loadbalancer.org who will be able to provide guidance on how to extent the trial using a simple command.

When a license is purchased, you’ll be provided with a license key file by our sales team. You can then simply apply this license to your appliance.

To install the license:

1. Using the WebUI, navigate to: *Local Configuration > License Key*
2. Browse to the license file provided when the appliance was purchased
3. Click **Install License Key**

12. Software Updates

Loadbalancer.org continually develop and add new and improved features to the appliance. These updates can be applied during the trial to ensure you have the very latest version of our software for your evaluation.

To run Software Update:

1. Using the WebUI, navigate to: *Maintenance > Software Update*
2. Choose **Online Update** if the appliance has Internet access
3. If updates are available, you'll be presented with a list of changes, click the **Online Update** button at the bottom of the page to start the update

Note

If your appliance does not have Internet access, please contact support@loadbalancer.org for details of how to obtain the offline update files.

13. Configuring & Testing a Simple Load Balanced Test Environment

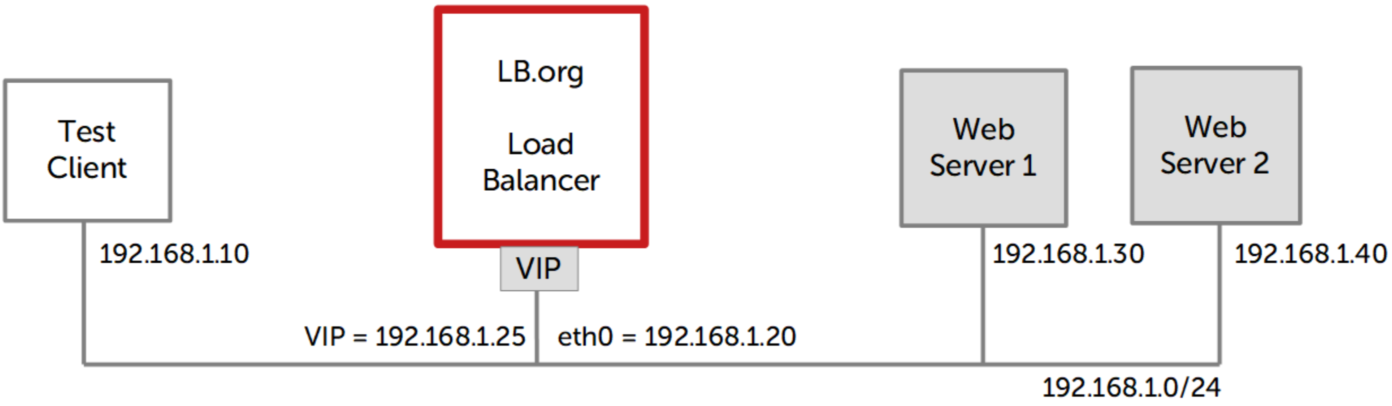
This example illustrates how to quickly configure a simple load balanced test environment using the Network Setup Wizard at the console to configure network settings, and the Setup Wizard from the WebUI to configure the layer 7 virtual service.

Note

Layer 7 SNAT mode is used in the example. As mentioned earlier, this is not the fastest mode but is very simple to deploy and requires no changes to the Real Servers.

The following diagram and table describe the environment:

IP Address	Device	Notes
192.168.1.10	Test Client	
192.168.1.20	Load Balancer	the load balancers own IP address
192.168.1.25	Load Balancer	the Virtual IP address (VIP), the IP address the clients connect to
192.168.1.30	Web Server 1	
192.168.1.40	Web Server 2	



STEP 1 - Deploy the Appliance

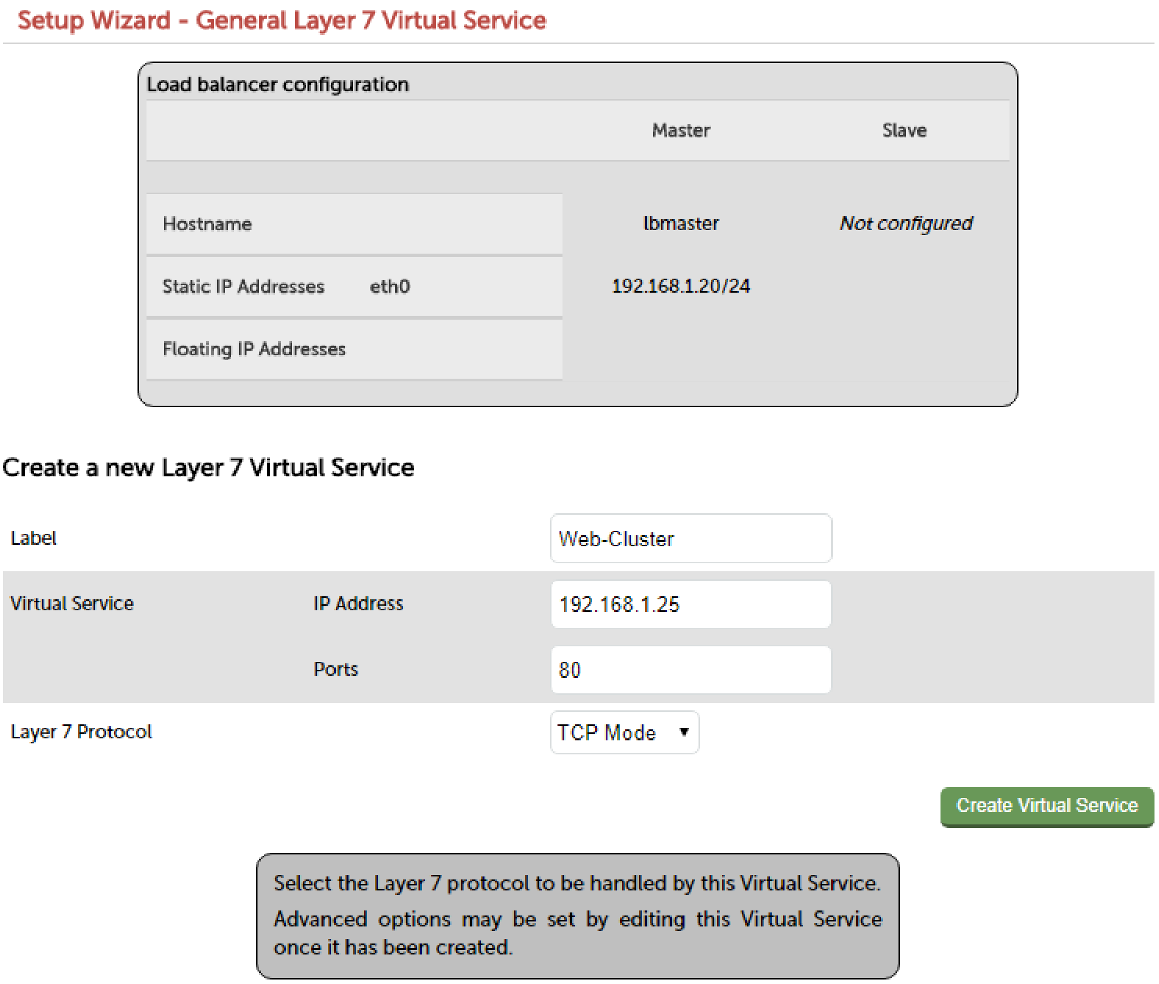
- Please refer to the Appliance Deployment section for more details

STEP 2 - Run the Network Setup Wizard

- Please refer to the Configuring Initial Network Settings section for more details

STEP 3 - Run the WebUI Setup Wizard

1. Open the WebUI and start the wizard by clicking the **Accept** button, or by using the WebUI menu option: *Cluster Configuration > Setup Wizard* and clicking **General Layer 7 Virtual Service**
2. Define the required Virtual Service settings as shown in the example below:



Setup Wizard - General Layer 7 Virtual Service

Load balancer configuration

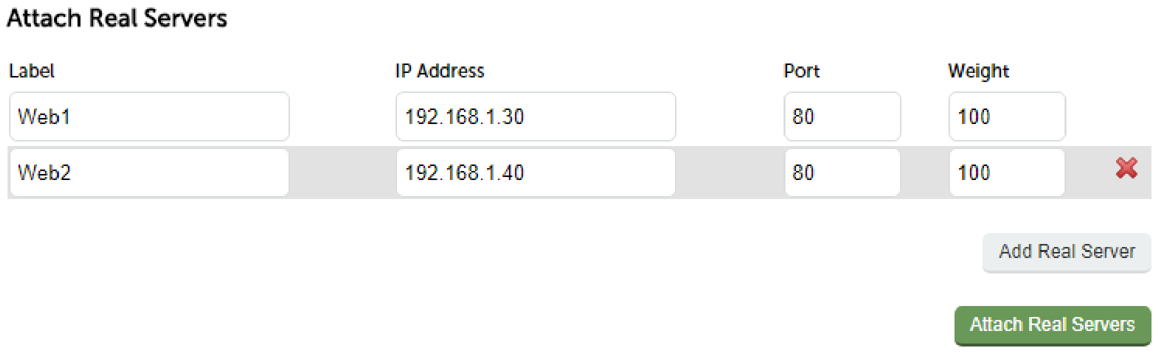
		Master	Slave
Hostname		lbmaster	*Not configured*
Static IP Addresses	eth0	192.168.1.20/24	
Floating IP Addresses			

Create a new Layer 7 Virtual Service

Label		Web-Cluster
Virtual Service	IP Address	192.168.1.25
	Ports	80
Layer 7 Protocol		TCP Mode ▼

Select the Layer 7 protocol to be handled by this Virtual Service. Advanced options may be set by editing this Virtual Service once it has been created.

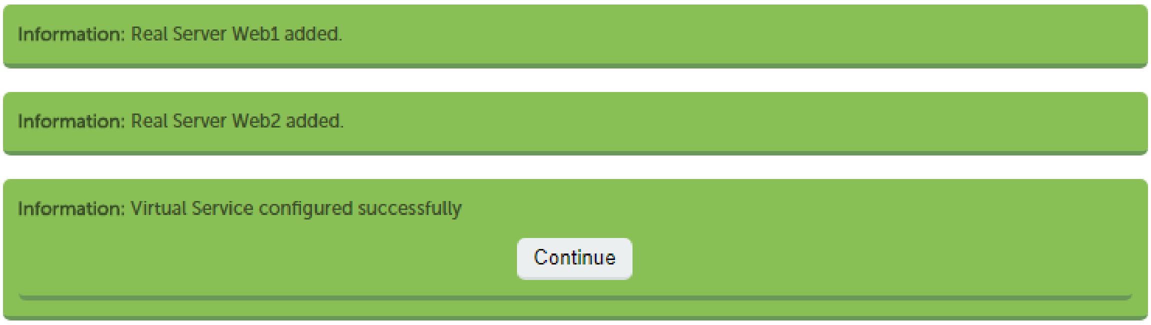
3. Click **Create Virtual Service**
4. Now continue and add the associated load balanced servers (Real Servers) as shown below:



Attach Real Servers

Label	IP Address	Port	Weight	
Web1	192.168.1.30	80	100	
Web2	192.168.1.40	80	100	✗

- Use the **Add Real Server** button to define additional Real Servers and use the red cross to delete Real Servers
- Once you're happy, click **Attach Real Servers** to create the new Virtual Service & Real Servers
- A confirmation message will be displayed as shown in the example below:



Information: Real Server Web1 added.

Information: Real Server Web2 added.

Information: Virtual Service configured successfully

5. Click **Continue**
6. Finally, reload HAProxy using the **Reload HAProxy** button in the blue box at the top of the screen or by using the WebUI menu option: *Maintenance > Restart Services* and clicking **Reload HAProxy**

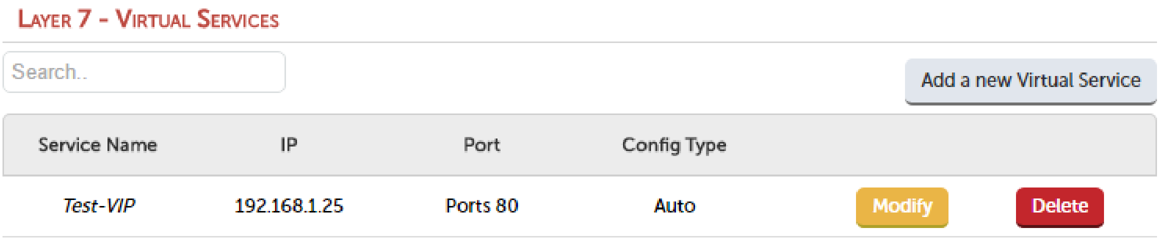
Note | Running the wizard again will permit additional Layer 7 VIPs and associated RIPs to be defined.

Note | To restore manufacturer's settings use the WebUI menu option: *Maintenance > Backup & Restore > Restore Manufacturer's Defaults*. This will reset the IP address to 192.168.2.21/24.

Note | By default, Real Server health-checks are set to use a TCP port connect. If you need a more robust check, this can be changed by modifying the configuration as explained below. Please refer to Chapter 8 in the Administration Manual for more information on configuring health-checks.

STEP 4 - Viewing & Modifying the Configuration

1. The VIP created by the wizard can be seen using the WebUI menu option: *Cluster Configuration > Layer 7 - Virtual Services* as shown below:



LAYER 7 - VIRTUAL SERVICES

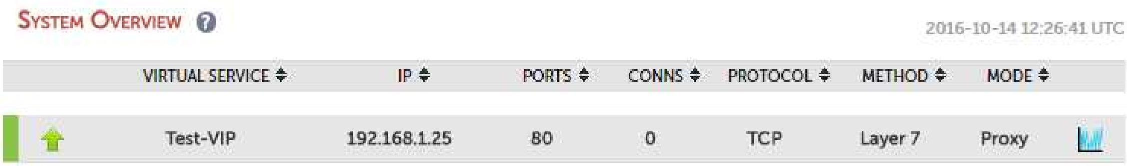
Service Name	IP	Port	Config Type		
Test-VIP	192.168.1.25	Ports 80	Auto	Modify	Delete

2. Clicking the **Modify** button allows all VIP setting to be modified
3. If changes are made, click the **Update** button to save the changes, then use the **Reload HAProxy** button at the top of the screen to apply the changes
4. Additional VIPs can be added by running the Setup Wizard again, or by clicking the **Add a new Virtual Service** button to define the VIP manually

Note | Real Servers can be added manually using the WebUI menu option: *Cluster Configuration > Layer 7 - Real Servers*.

STEP 5 - Checking the Status using System Overview

1. Using the WebUI, navigate to: *System Overview* to view the newly created VIP & RIPs:

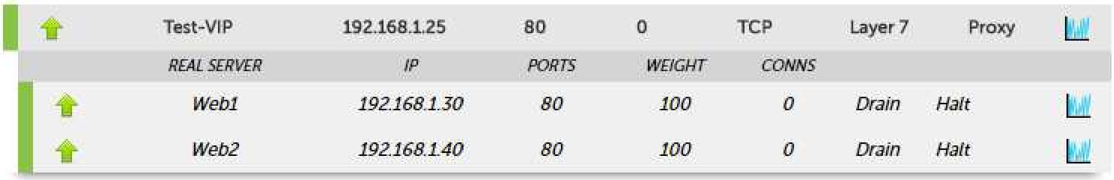


SYSTEM OVERVIEW

2016-10-14 12:26:41 UTC

	VIRTUAL SERVICE	IP	PORTS	CONNS	PROTOCOL	METHOD	MODE
↑	Test-VIP	192.168.1.25	80	0	TCP	Layer 7	Proxy

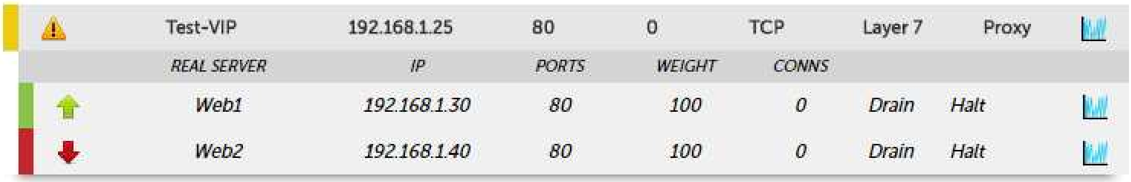
2. To view the RIPs, click anywhere on the horizontal gray area to expand the VIP as shown below:



↑	Test-VIP	192.168.1.25	80	0	TCP	Layer 7	Proxy
	REAL SERVER	*IP*	*PORTS*	*WEIGHT*	*CONNS*		
↑	*Web1*	*192.168.1.30*	*80*	*100*	*0*	*Drain*	*Halt*
↑	*Web2*	*192.168.1.40*	*80*	*100*	*0*	*Drain*	*Halt*

STEP 6 - Verification & Testing

1. Verify that both Real Servers are up. In the example below, Web2 is failing its health-check:



⚠	Test-VIP	192.168.1.25	80	0	TCP	Layer 7	Proxy
	REAL SERVER	*IP*	*PORTS*	*WEIGHT*	*CONNS*		
↑	*Web1*	*192.168.1.30*	*80*	*100*	*0*	*Drain*	*Halt*
↓	*Web2*	*192.168.1.40*	*80*	*100*	*0*	*Drain*	*Halt*

- This should be investigated and corrected, possible steps include:
  - Check that the application/service is running on the Real Server
  - Make sure you can ping the Real Server from the load balancer
  - Verify that you can connect to the application port from the load balancer. This can be done using telnet at the console or via an SSH session:

```
telnet 192.168.1.40 80
```

2. Once both servers are up (shown green) browse to the VIP address and verify that you see the web page from each Real Server:
   - Halt Web1 using the *Halt* option for Web1 in the System Overview and verify that content is served by Web2 on a browser refresh (CTRL-F5)
   - Halt Web2 using the *Halt* option for Web2 in the System Overview and verify that content is served by Web1 on a browser refresh (CTRL-F5)

Note

For more configuration examples using Layer 7 SNAT mode and also Layer 4 DR mode, Layer 4 NAT mode & Layer 4 SNAT mode please refer to Chapter 11 in the Administration Manual.

Note

For more information on verifying your test environment and ways to diagnose any issues you have please refer to Chapter 12 in the Administration Manual.

14. Configuring HA - Adding a Slave 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 master appliance is fully configured first, then the slave should be added. Once the master and slave are paired, all load balanced services configured on the master are automatically replicated to the slave 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 Master and one for the VIP when it's active on the Slave. 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 master) suffer a failure, the passive device (normally the slave) will take over.

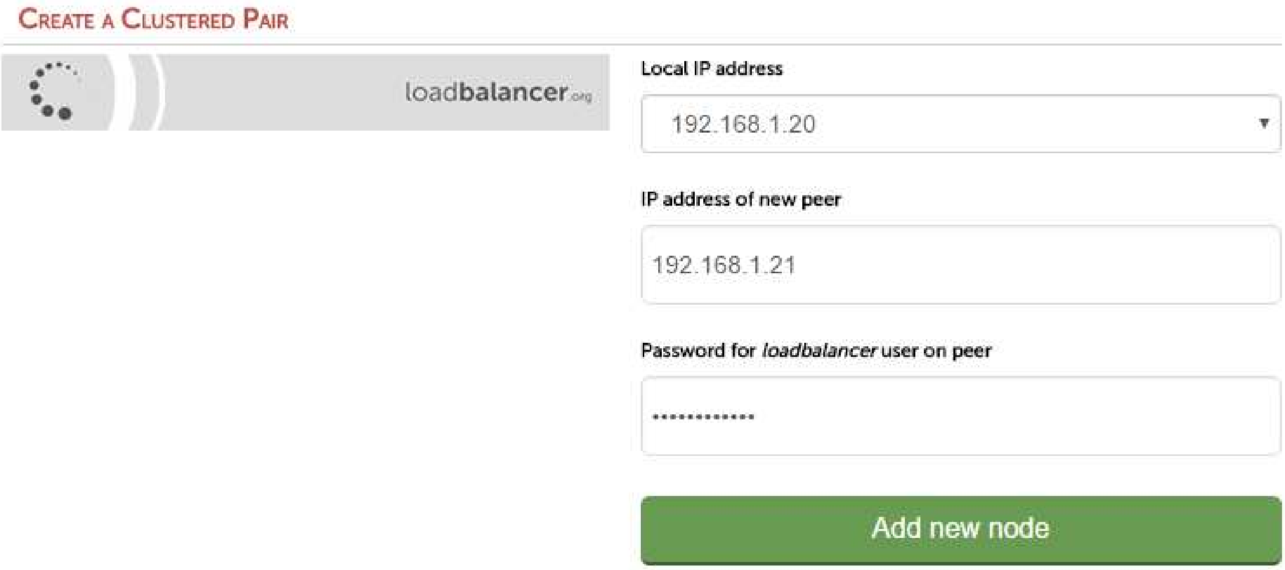
Note

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 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

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

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



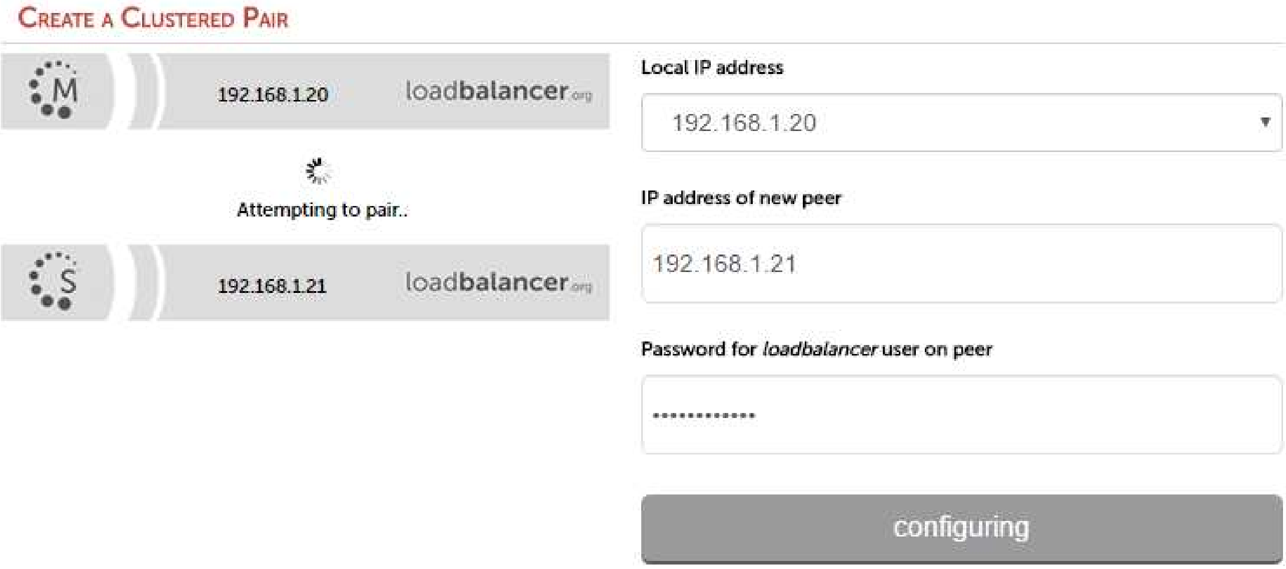
Create a Clustered Pair

Local IP address: 192.168.1.20

IP address of new peer: 192.168.1.21

Password for *loadbalancer* user on peer: ••••••••••••

3. Specify the IP address and the *loadbalancer* user's password for the slave (peer) appliance as shown above
4. Click **Add new node**
5. The pairing process now commences as shown below:



Create a Clustered Pair

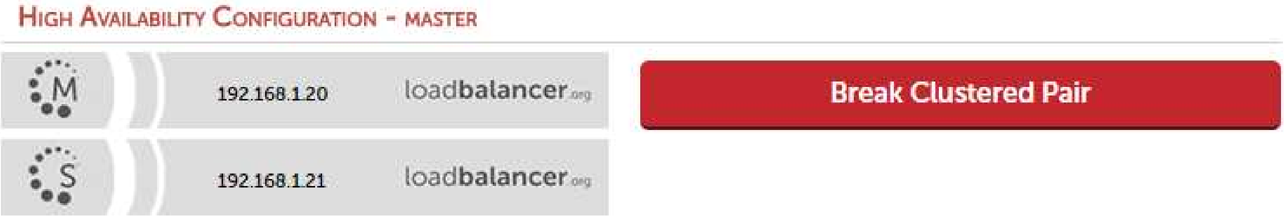
Local IP address: 192.168.1.20

IP address of new peer: 192.168.1.21

Password for *loadbalancer* user on peer: ••••••••••••

Attempting to pair..

6. Once complete, the following will be displayed:



High Availability Configuration - master

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

Note — For more details on configuring HA with 2 appliances, please refer to Chapter 9 in the Administration Manual.

15. More Information

Please refer to our website for the latest administration manual, deployment guides and all other documentation: https://www.loadbalancer.org/resources/manuals

16. Loadbalancer.org Technical Support

If you have any questions regarding the appliance or how to load balance your application, please don’t hesitate to contact our support team: support@loadbalancer.org

About Loadbalancer.org

Loadbalancer.org's mission is to ensure that its clients' businesses are never interrupted. The load balancer experts ask the right questions to get to the heart of what matters, bringing a depth of understanding to each deployment. Experience enables Loadbalancer.org engineers to design less complex, unbreakable solutions - and to provide exceptional personalized support.

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