LOADBALANCER

DEPLOYMENT GUIDE

Load Balancing Pharos Blueprint®

Version 1.2.0

Table of Contents

1. About this Guide

This guide details the steps required to configure a load balanced Pharos Blueprint environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Pharos Blueprint 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 Pharos Blueprint. For full specifications of available models please refer to: https://www.loadbalancer.org/products.

Some features may not be supported in all cloud platforms due to platform specific limitations, please check with Loadbalancer.org support for further details.

3. Software Versions Supported

3.1. Loadbalancer.org Appliance

- 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.

3.2. Pharos Blueprint

- Pharos Blueprint Enterprise v5.3 and later

4. Pharos Blueprint

Pharos Blueprint gives you critical insights into your print environment and workflows, empowering you to successfully manage print and its related costs. Blueprint is a single system with the flexibility to work with a mix and match of equipment manufacturers and device models. Blueprint makes it easy to manage your entire print environment. Blueprint delivers secure printing and significant cost savings and waste reduction. It provides the information you need to optimize your equipment fleet, improve employee printing habits, and take meaningful action today and throughout the future.

5. Load Balancing Pharos Blueprint

> **Note** It's highly recommended that you have a working Pharos Blueprint environment first before implementing the load balancer.

5.1. Load Balancing & HA Requirements

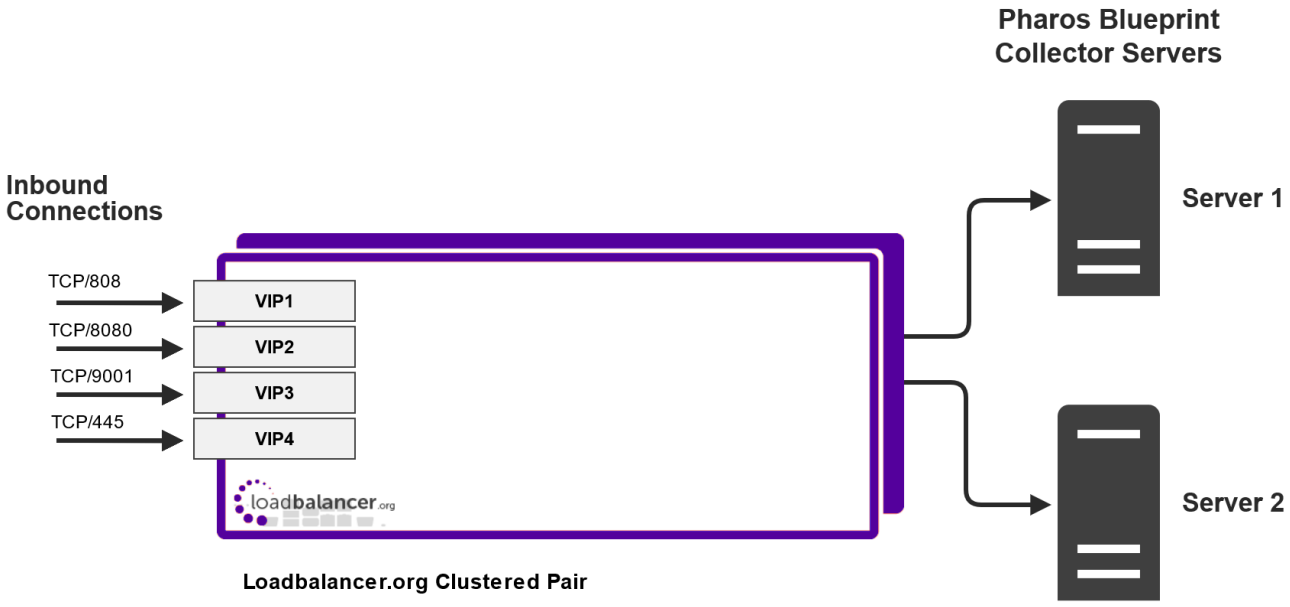
2 or more Collector servers are configured to create a load balanced pool. Clients then connect to this pool via Virtual Services (VIPs).

5.2. Port Requirements

The following tables show the ports that are load balanced:

Port	Protocols	Use
808	TCP	Server to Server Communications (Analyst to Collector, Collector to Collector) Administrator to Server Communications 808 is used by the Administrator to the TaskMaster. It is encrypted. Anything the Administrator tool wants is pulled by TaskMaster service and given to Administrator over 808
8080	TCP	Server to Server Communications (Analyst to Collector, Collector to Collector) Administrator to Server Communications 8080 is how Collectors upload their transaction info and provide status update/health check info to the Analyst, and how the Analyst updates its own health check Client to Server Communication (View waiting print jobs)
9001	TCP	Used for inter-server communications between the Pharos Systems Secure Release Service and the MobilePrint Worker service
445	TCP	Microsoft Print/SMB Services

5.3. Pharos Blueprint Deployment Concept



VIP = **V**irtual **IP** Addresses

5.4. Virtual Service (VIP) Requirements

To provide load balancing and HA for Pharos Blueprint, 4 VIPs are used. Three VIPs for the Pharos Blueprint services, and a fourth for the underlying Microsoft print services.

5.5. Supported Load Balancer Deployment Methods

For Pharos Blueprint, both layer 4 DR mode and layer 7 SNAT mode can be used, although for maximum throughput the preferred method is Layer 4 DR Mode (Direct Routing, aka DSR / Direct Server Return). This is a very high performance solution that requires little change to your existing infrastructure. It is necessary to solve "the ARP problem" on the Collector Servers. This is a straightforward process, and is detailed in Solving the ARP Problem.

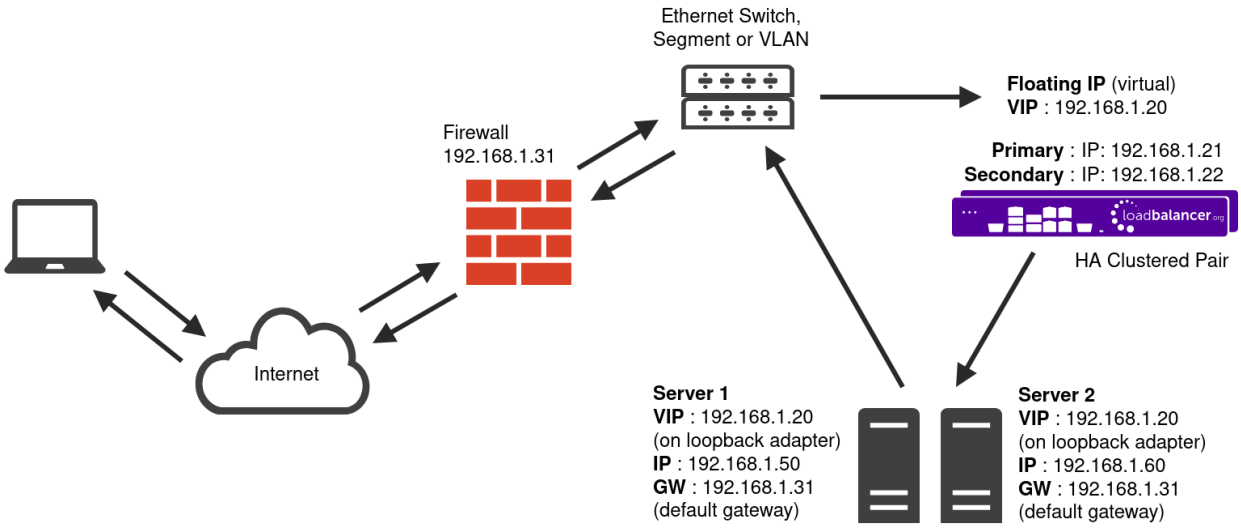
Where it's not feasible to use layer 4 DR mode, layer 7 SNAT mode should be used. Whilst this mode does not have the raw throughput of layer 4 methods, it still enables high performance load balancing and requires no changes to the Collector Servers.

Each Mode is described below.

Layer 4 DR Mode

One-arm direct routing (DR) mode is a very high performance solution that requires little change to your existing infrastructure.

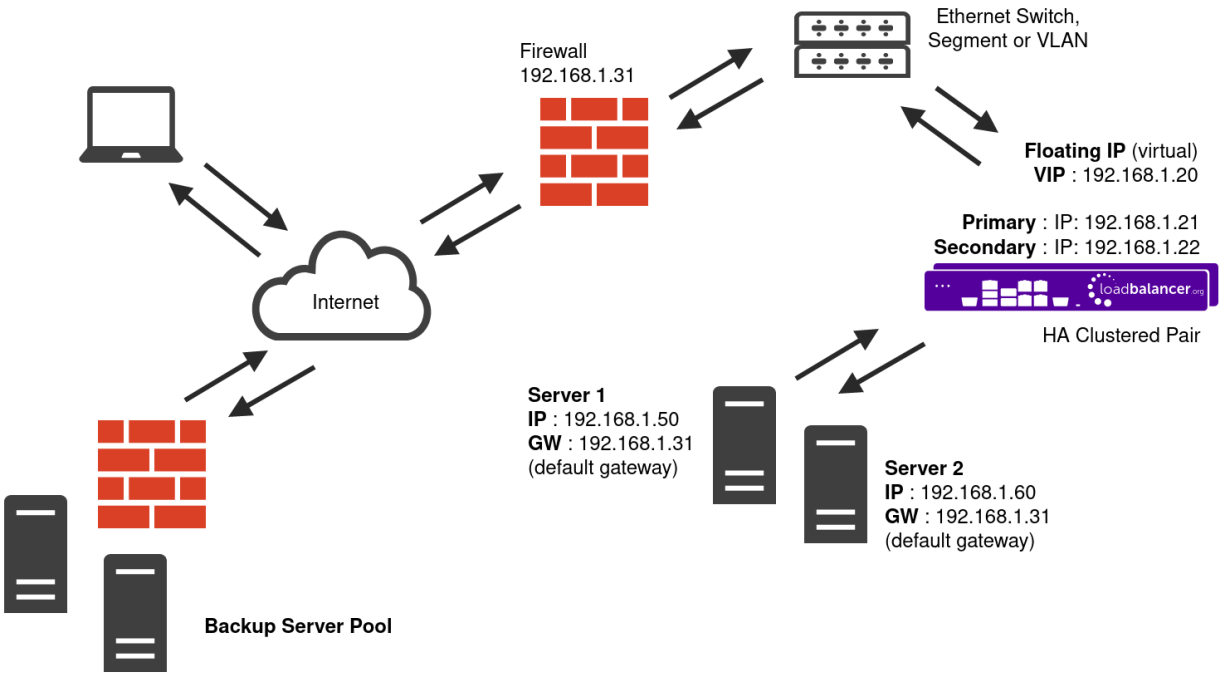
> **Note** Kemp, Brocade, Barracuda & A10 Networks call this *Direct Server Return* and F5 call it *nPath*.



- DR mode works by changing the destination MAC address of the incoming packet to match the selected Real Server on the fly which is very fast.
- When the packet reaches the Real Server it expects the Real Server to own the Virtual Services IP address (VIP). This means that you need to ensure that the Real Server (and the load balanced application) respond to both the Real Server's own IP address and the VIP.
- The Real Servers should not respond to ARP requests for the VIP. Only the load balancer should do this. Configuring the Real Servers in this way is referred to as ***Solving the ARP problem***. For more information please refer to DR Mode Considerations.
- On average, DR mode is 8 times quicker than NAT for HTTP, 50 times quicker for Terminal Services and much, much faster for streaming media or FTP.
- The load balancer must have an Interface in the same subnet as the Real Servers to ensure layer 2 connectivity required for DR mode to work.
- The VIP can be brought up on the same subnet as the Real Servers, or on a different subnet provided that the load balancer has an interface in that subnet.
- Port translation is not possible with DR mode, e.g. VIP:80 → RIP:8080 is not supported.
- DR mode is transparent, i.e. the Real Server will see the source IP address of the client.

Layer 7 SNAT Mode

Layer 7 SNAT mode uses a proxy (HAProxy) at the application layer. Inbound requests are terminated on the load balancer and HAProxy generates a new corresponding request to the chosen Real Server. As a result, Layer 7 is typically not as fast as the Layer 4 methods. Layer 7 is typically chosen when either enhanced options such as SSL termination, cookie based persistence, URL rewriting, header insertion/deletion etc. are required, or when the network topology prohibits the use of the layer 4 methods.



- Because layer 7 SNAT mode is a full proxy, any server in the cluster can be on any accessible subnet including across the Internet or WAN.
- Layer 7 SNAT mode is not transparent by default, i.e. the Real Servers will not see the source IP address of the client, they will see the load balancer's own IP address by default, or any other local appliance IP address if preferred (e.g. the VIP address). This can be configured per layer 7 VIP. If required, the load balancer can be configured to provide the actual client IP address to the Real Servers in 2 ways. Either by inserting a header that contains the client's source IP address, or by modifying the Source Address field of the IP packets and replacing the IP address of the load balancer with the IP address of the client. For more information on these methods please refer to Transparency at Layer 7.
- Layer 7 SNAT mode can be deployed using either a one-arm or two-arm configuration. For two-arm deployments, **eth0** is normally used for the internal network and **eth1** is used for the external network although this is not mandatory.
- Requires no mode-specific configuration changes to the load balanced Real Servers.
- Port translation is possible with Layer 7 SNAT mode, e.g. VIP:80 → RIP:8080 is supported.
- You should not use the same RIP:PORT combination for layer 7 SNAT mode VIPs and layer 4 SNAT mode VIPs because the required firewall rules conflict.

6. Loadbalancer.org Appliance – the Basics

6.1. 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.

6.2. 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.

6.3. Accessing the Appliance WebUI

The WebUI is accessed using a web browser. By default, users are authenticated using Apache authentication. Users can also be authenticated against LDAP, LDAPS, Active Directory or Radius - for more information, please refer to External Authentication.

> **Note** There are certain differences when accessing the WebUI for the cloud appliances. For details, please refer to the relevant Quick Start / Configuration Guide.

> **Note** A number of compatibility issues have been found with various versions of Microsoft Internet Explorer and Edge. The WebUI has been tested and verified using both Chrome & Firefox.

1. Using a browser, navigate to the following URL:

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

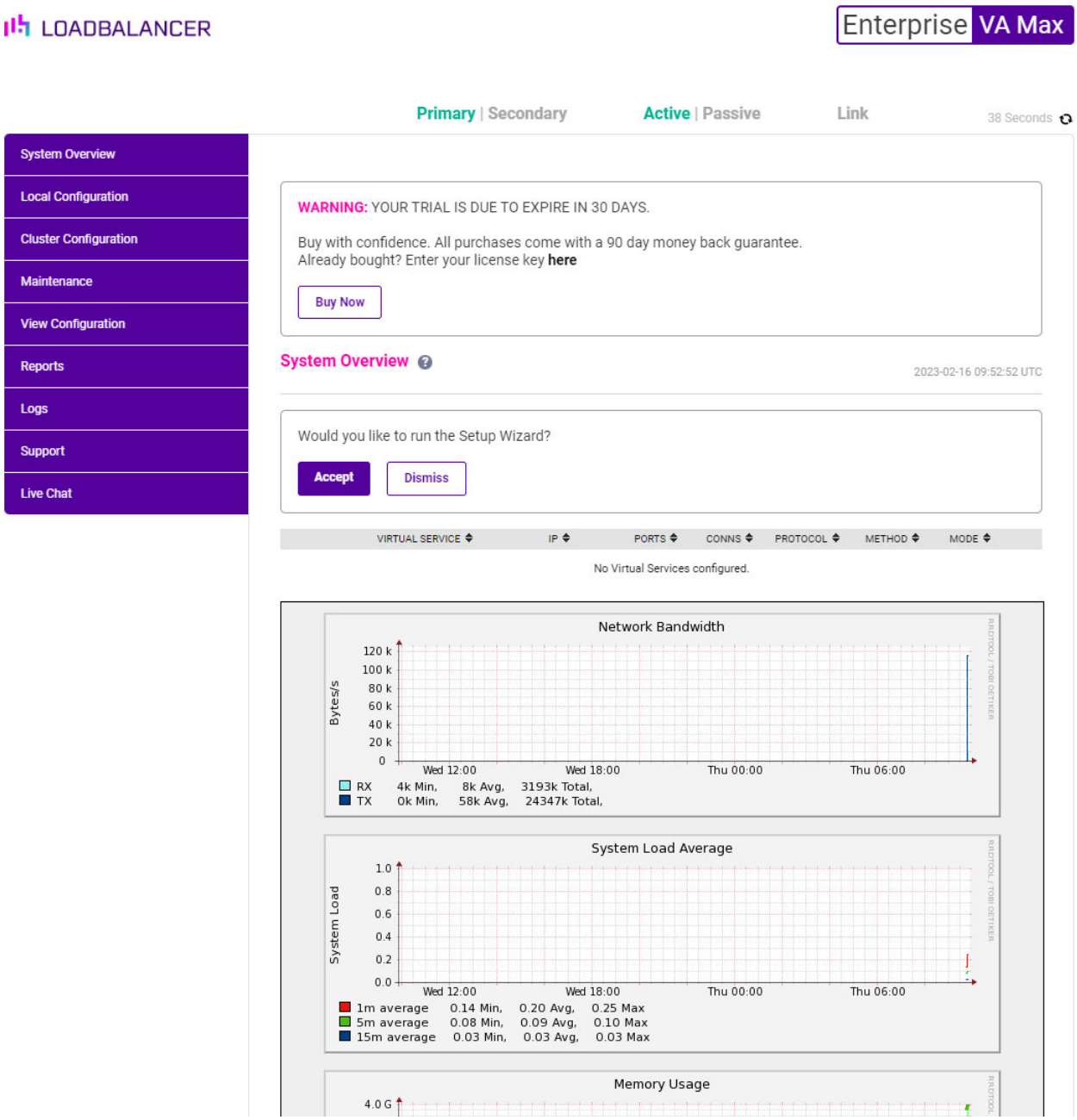
   > **Note** You'll receive a warning about the WebUI's certificate. This is due to the default self signed certificate that is used. If preferred, you can upload your own certificate - for more information, please refer to Appliance Security Features.

2. Log in to the WebUI using the following credentials:

   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:



3. You'll be asked if you want to run the Setup Wizard. Click **Dismiss** if you're following a guide or want to configure the appliance manually. Click **Accept** to start the Setup Wizard.

> **Note** The Setup Wizard can only be used to configure Layer 7 services.

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

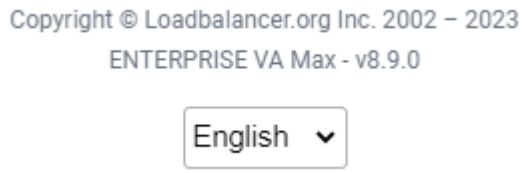
Logs - View various appliance logs
Support - Create a support download, contact the support team & access useful links
Live Chat - Start a live chat session with one of our Support Engineers

6.4. Appliance Software Update

To ensure that the appliance(s) are running the latest software version, we recommend a software update check is performed.

Determining the Current Software Version

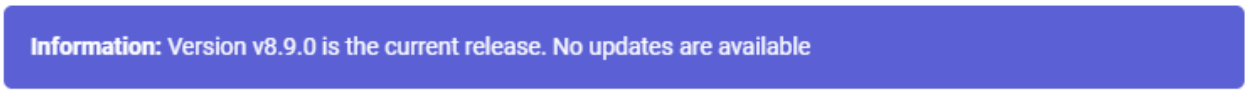
The software version is displayed at the bottom of the WebUI as shown in the example below:



Checking for Updates using Online Update

> **Note** By default, the appliance periodically contacts the Loadbalancer.org update server and checks for updates. An update check can also be manually triggered as detailed below.

1. Using the WebUI, navigate to: *Maintenance > Software Update*.
2. Select **Online Update**.
3. If the latest version is already installed, a message similar to the following will be displayed:



4. If an update is available, you'll be presented with a list of new features, improvements, bug fixes and security related updates.
5. Click **Online Update** to start the update process.

> **Note** Do not navigate away whilst the update is ongoing, this may cause the update to fail.

6. Once complete (the update can take several minutes depending on download speed and upgrade version) the following message will be displayed:

7. If services need to be reloaded/restarted or the appliance needs a full restart, you'll be prompted accordingly.

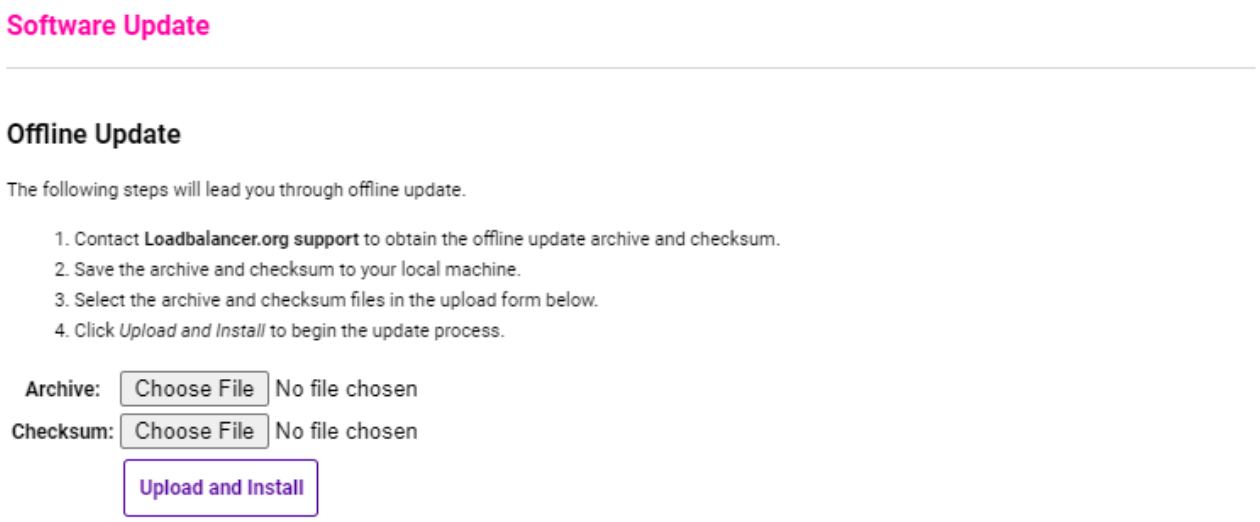
Using Offline Update

If the load balancer does not have access to the Internet, offline update can be used.

> **Note** Please contact support@loadbalancer.org to check if an update is available and obtain the latest offline update files.

To perform an offline update:

1. Using the WebUI, navigate to: ***Maintenance > Software Update***.
2. Select **Offline Update**.
3. The following screen will be displayed:



4. Select the ***Archive*** and ***Checksum*** files.
5. Click **Upload and Install**.
6. If services need to be reloaded/restarted or the appliance needs a full restart, you'll be prompted accordingly.

6.5. 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 Primary & Secondary appliances in HA mode
TCP	7778	HAProxy persistence table replication
TCP	9080	WebUI - HTTP (disabled by default)

Protocol	Port	Purpose
TCP	9081	Nginx fallback page
TCP	9443	WebUI - HTTPS

6.6. 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, and adding a secondary unit is covered in Configuring HA - Adding a Secondary Appliance.

7. Load Balancing Pharos Blueprint – Using Layer 4 DR Mode

7.1. STEP 1 – Prepare the Pharos Blueprint Servers for Load Balancing

A) Prerequisites

For a load balanced Pharos Blueprint environment, each Collector Server must comply with the following requirements:

- Be a member of a Microsoft Windows Domain
- Have the **Print and Document Service** role / **Print Server** service installed
- Have all required printers installed and shared – the share names and permissions must be the same across all servers
- Have Pharos Blueprint installed

B) Solve the ARP Problem on Each server

When using layer 4 DR mode, the "ARP problem" must be solved on each Collector server for DR mode to work. For detailed steps on solving the ARP problem for Windows, please refer to Solving the ARP Problem for more information.

For a detailed explanation of DR mode and the nature of the ARP problem, please refer to Layer 4 DR Mode.

C) Enable Print Server Load Balancing

To enable the load balanced Collector Servers to be accessed via a shared name (**blueprintservice** is the example used in this guide), the following steps must be completed:

Windows 2019

Host entries must be added to the local hosts file on each Collector Server. For example, if you have 2 Collector Servers: 192.168.81.11 and 192.168.81.12, add the following entries to the hosts files:

On the 192.168.81.11 server:

```
192.168.81.11 blueprintservice
192.168.81.11 blueprintservice.yourdomain.com
```

On the 192.168.81.12 server:

```
192.168.81.12 blueprintservice
192.168.81.12 blueprintservice.yourdomain.com
```

where **bluprintservice** is the DNS name clients use to access the load balanced Collector Servers.

Windows 2012 & 2016

Configure the following Registry entries:

```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
Value: DisableLoopbackCheck
Type: REG_DWORD
Data: 1
```

```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
Value: DisableStrictNameChecking
Type: REG_DWORD
Data: 1
```

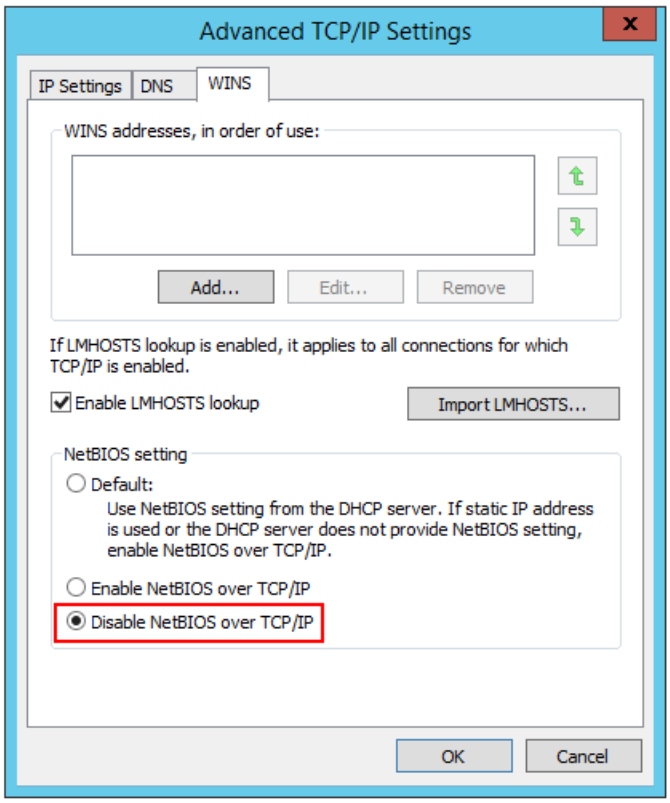
```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
Value: OptionalNames
Type: REG_MULTI_SZ
Data: blueprintservice
```

> **Note** In the example presented here, **blueprintservice** is the name that will be used to access the load balanced Collector Servers via the VIPs created on the load balancer. This can be set to any appropriate name. Whatever name is used, it must resolve to the IP address used for the VIPs.

D) Configure Name Resolution

To enable clients to connect via the load balancer, DNS name resolution must be configured. Create a DNS Host (A) record for the printer share name (**blueprintservice** in this example) that points at the IP address used for the VIPs (**192.168.81.10** in this example).

In addition, NetBIOS over TCP/IP should be disabled on **all** interfaces on each Collector Server as shown below:



E) Reboot Each Server

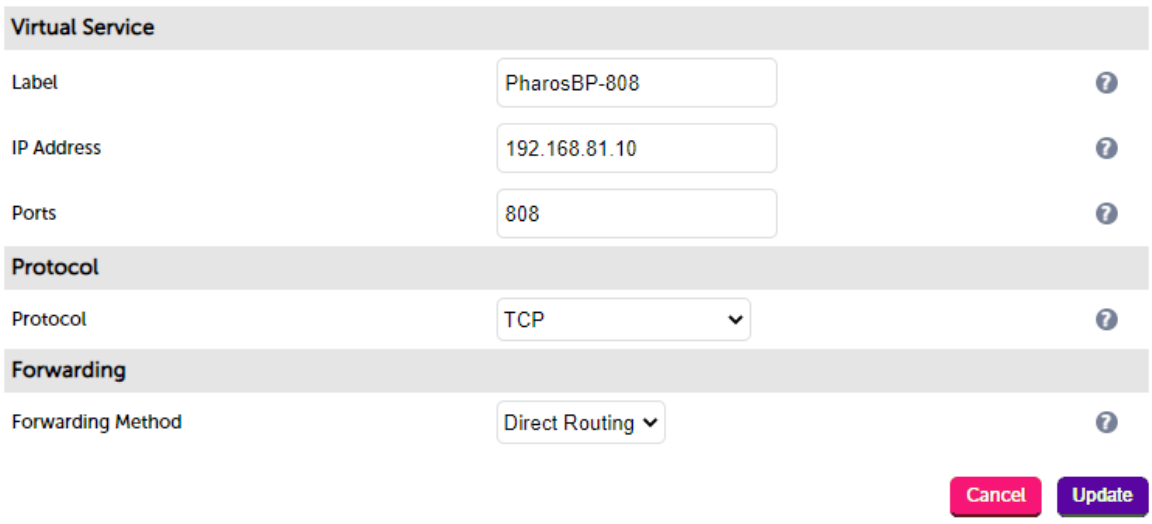
To apply all settings, reboot each Collector Server.

7.2. STEP 2 – Configure the VIPs & RIPs

VIP1 – Port 808

Define the VIP

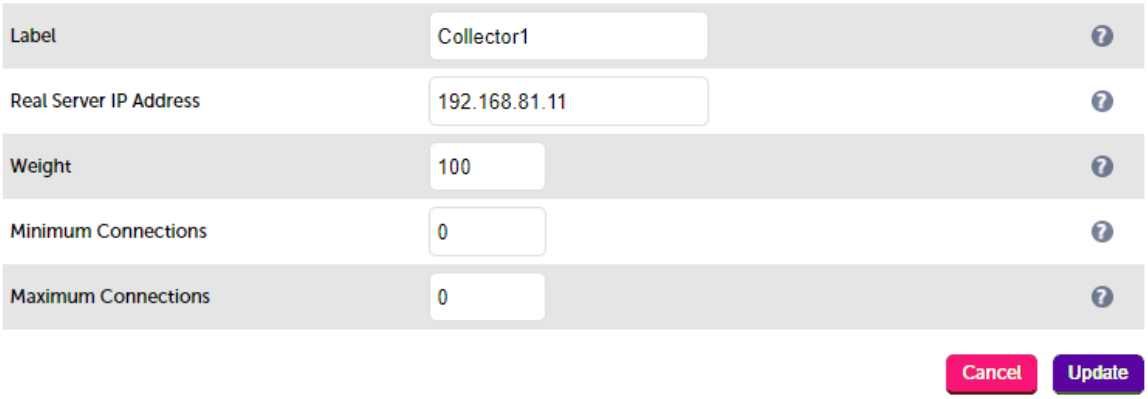
1. Using the WebUI, navigate to *Cluster Configuration > Layer 4 – Virtual Services* and click **Add a new Virtual Service**.



2. Define the *Label* (i.e. the name) for the virtual service as required, e.g. **PharosBP-808**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.81.10**.
4. Set *Ports* to **808**.
5. Leave *Protocol* set to **TCP**.
6. Leave *Forwarding Method* set to **Direct Routing**.
7. Click **Update**.
8. Now click **Modify** next to the newly created VIP.
9. Scroll down to the *Persistence* section and uncheck the *Enable* checkbox.
10. Click **Update**.

Define the Real Servers (RIPs)

1. Using the WebUI, navigate to *Cluster Configuration > Layer 4 – Real Servers* and click on **Add a new Real Server** next to the newly created VIP.



2. Define the *Label* (i.e. the name) for the Real Server as required, e.g. **Collector1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.81.11**.
4. Click *Update*.
5. Repeat these steps to add additional Collector Servers as required.

VIP2 – Port 8080

- Click **Modify** next to the *PharosBP-808* VIP just created, then click **Duplicate Service**.
- Change the VIP *label* to an appropriate name, e.g. **PharosBP-8080**.
- Change the VIP *Ports* to 8080.
- Leave all other settings the same.
- Click **Update** to save the new VIP.

VIP3 – Port 9001

- Again, duplicate the *PharosBP-808* VIP.
- Change the VIP *label* to an appropriate name, e.g. **PharosBP-9001**.
- Change the VIP *Ports* to 9001.
- Leave all other settings the same.
- Click **Update** to save the new VIP.

VIP4 – Port 445

- Again, duplicate the *PharosBP-808* VIP.
- Change the VIP *label* to an appropriate name, e.g. **PharosBP-445**.
- Change the VIP *Ports* to 445.
- Leave all other settings the same.
- Click **Update** to save the new VIP.

8. Load Balancing Pharos Blueprint – Using Layer 7 SNAT Mode

8.1. STEP 1 – Prepare the Pharos Blueprint Servers for Load Balancing

A) Prerequisites

For a load balanced Pharos Blueprint environment, each Collector Server must comply with the following requirements:

- Be a member of a Microsoft Windows Domain
- Have the **Print and Document Service** role / **Print Server** service installed
- Have all required printers installed and shared – the share names and permissions must be the same across all servers
- Have Pharos Blueprint installed

B) Enable Print Server Load Balancing

To enable the load balanced Collector Servers to be accessed via a shared name (**blueprintservice** is the example used in this guide), the following steps must be completed:

Windows 2019

Host entries must be added to the local hosts file on each Collector Server. For example, if you have 2 Collector Servers: 192.168.81.11 and 192.168.81.12, add the following entries to the hosts files:

On the 192.168.81.11 server:

```
192.168.81.11 blueprintservice
```

```
192.168.81.11 blueprintservice.yourdomain.com
```

On the 192.168.81.12 server:

```
192.168.81.12 blueprintservice
192.168.81.12 blueprintservice.yourdomain.com
```

where **bluprintservice** is the DNS name clients use to access the load balanced Collector Servers.

Windows 2012 & 2016

Configure the following Registry entries:

```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
Value: DisableLoopbackCheck
Type: REG_DWORD
Data: 1
```

```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
Value: DisableStrictNameChecking
Type: REG_DWORD
Data: 1
```

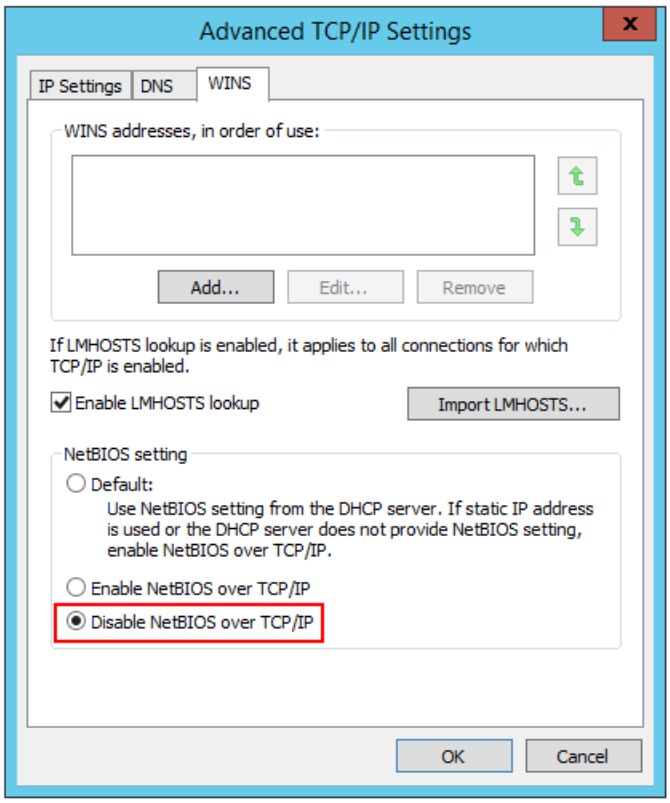
```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
Value: OptionalNames
Type: REG_MULTI_SZ
Data: blueprintservice
```

> **Note** In the example presented here, **blueprintservice** is the name that will be used to access the load balanced Collector Servers via the VIPs created on the load balancer. This can be set to any appropriate name. Whatever name is used, it must resolve to the IP address used for the VIPs.

C) Configure Name Resolution

To enable clients to connect via the load balancer, DNS name resolution must be configured. Create a DNS Host (A) record for the printer share name (**blueprintservice** in this example) that points at the IP address used for the VIPs (**192.168.81.10** in this example).

In addition, NetBIOS over TCP/IP should be disabled on **all** interfaces on each Collector Server as shown below:



D) Reboot Each Server

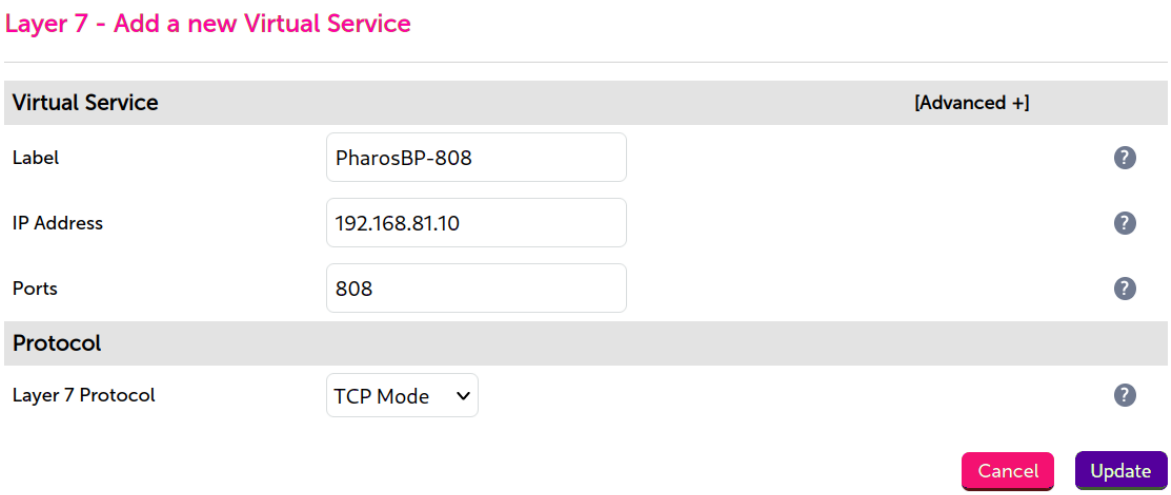
To apply all settings, reboot each Collector Server.

8.2. STEP 2 – Configure the VIPs & RIPs

VIP1 – Port 808

Define the VIP

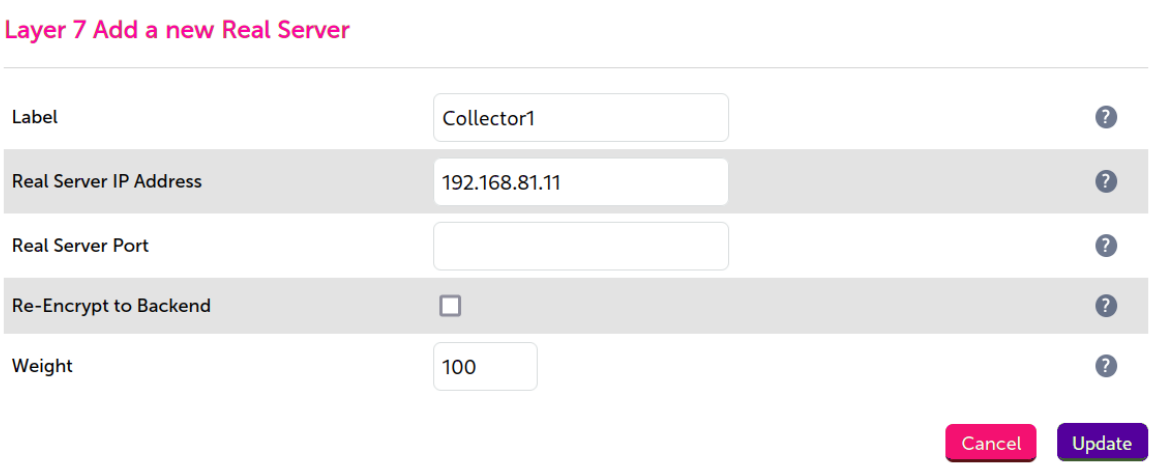
1. Using the WebUI, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a new Virtual Service**.



2. Define the *Label* (i.e. the name) for the virtual service as required, e.g. **PharosBP-808**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.81.10**.
4. Set *Ports* to **808**.
5. Change *Layer 7 Protocol* to **TCP Mode**.
6. Click **Update**.
7. Now click **Modify** next to the newly created VIP.
8. Scroll down to the *Persistence* section and change *Persistence Mode* to **None**.
9. Click **Update**.

Define the Real Servers (RIPs)

1. Using the WebUI, navigate to *Cluster Configuration > Layer 7 – Real Servers* and click on **Add a new Real Server** next to the newly created VIP.



2. Define the *Label* (i.e. the name) for the Real Server as required, e.g. **Collector1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.81.11**.
4. Leave *Real Server Port* blank.
5. Click **Update**.
6. Repeat these steps to add additional Collector Servers as required.

VIP2 – Port 8080

- Click **Modify** next to the *PharosBP-808* VIP just created, then click **Duplicate Service**.
- Change the VIP *label* to an appropriate name, e.g. **PharosBP-8080**.
- Change the VIP *Ports* to 8080.
- Leave all other settings the same.
- Click **Update** to save the new VIP.

VIP3 – Port 9001

- Again, duplicate the *PharosBP-808* VIP.
- Change the VIP *label* to an appropriate name, e.g. **PharosBP-9001**.
- Change the VIP *Ports* to 9001.
- Leave all other settings the same.
- Click **Update** to save the new VIP.

VIP4 – Port 445

- Again, duplicate the *PharosBP-808* VIP.
- Change the VIP *label* to an appropriate name, e.g. **PharosBP-445**.
- Change the VIP *Ports* to 445.
- Leave all other settings the same.
- Click **Update** to save the new VIP.

Finalize Settings – Reload HAProxy

To apply settings and activate the new VIPs, click the **Reload** button in the "Commit changes" box at the top of the screen.

9. Testing & Verification

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

9.1. Testing the Load Balanced Servers

The load balanced servers can be tested either by browsing to the chosen DNS name, in this guide **blueprintservice**.

e.g.

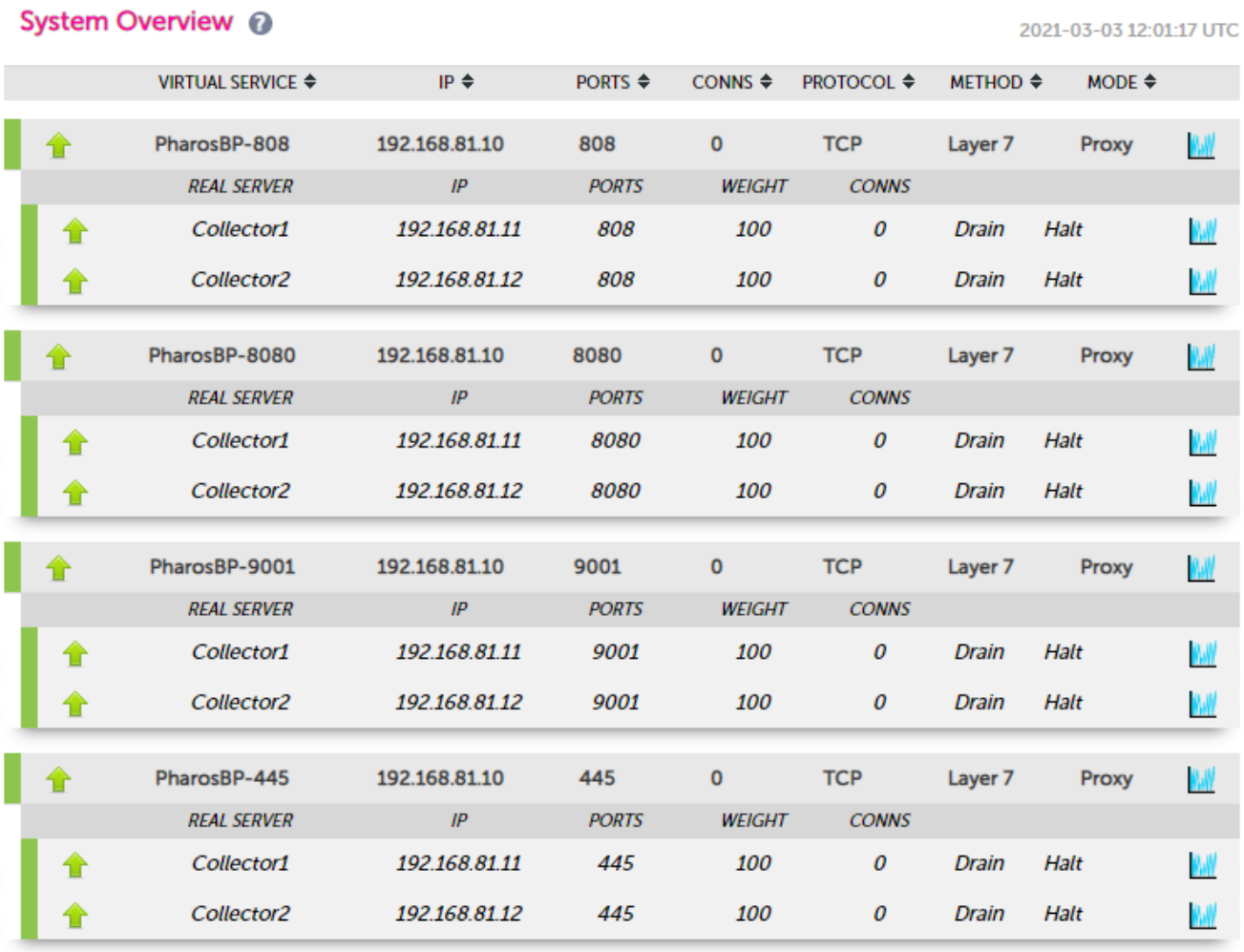
```
\\blueprintservice

\\blueprintservice.yourdomain.com
```

The shared printers that have been configured on the Collector Servers should be visible. Open/connect to the shared printers.

9.2. Using System Overview

The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & RIPs (i.e. the Pharos Blueprint 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 all Real Servers are healthy and available to accept connections.



> **Note** This example shows layer 7 VIPs. A layer 4 configuration will look very similar.

If a particular server fails its health check, that server will be displayed red rather than green.

10. 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.

11. Further Documentation

For additional information, please refer to the Administration Manual.

12. Appendix

12.1. Solving the ARP Problem

When using Layer 4 DR mode, the ARP problem must be solved. This involves configuring each Real Server to be able to receive traffic destined for the VIP, and ensuring that each Real Server does not respond to ARP requests for the VIP address – only the load balancer should do this.

Windows Server 2012 & Later

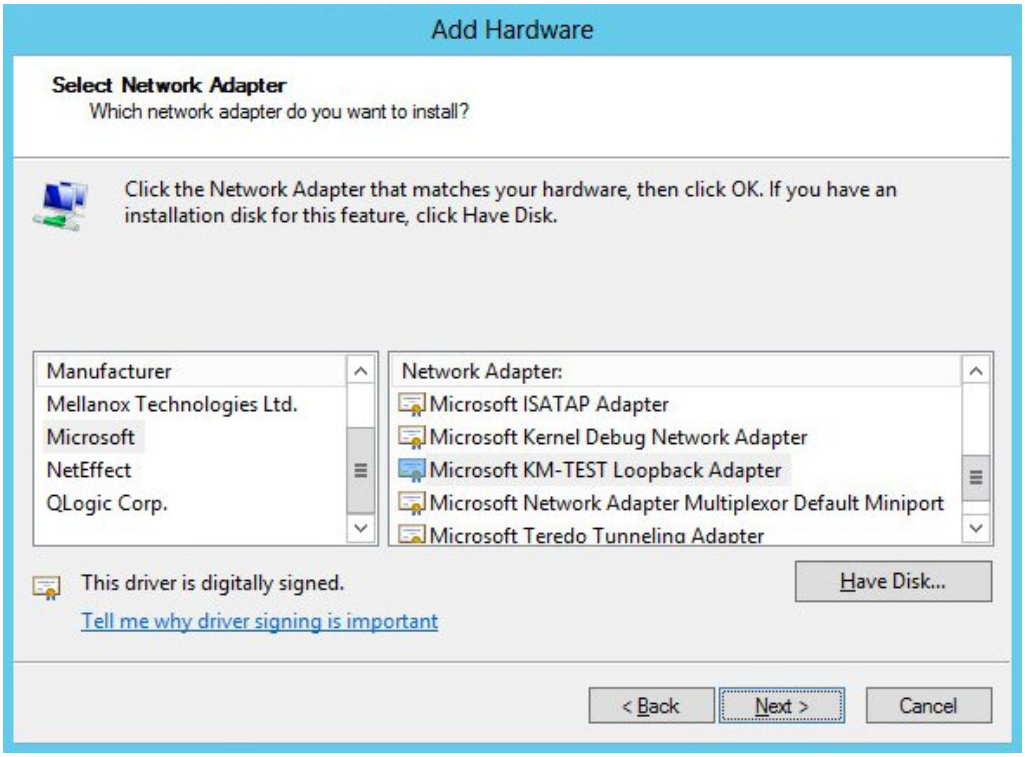
Windows Server 2012 and later support Direct Routing (DR) mode through the use of the Microsoft Loopback Adapter that must be installed and configured on each load balanced (Real) Server. The IP address configured on the Loopback Adapter must be the same as the Virtual Service (VIP) address. This enables the server to receive packets that have their destination set as the VIP address. If a Real Server is included in multiple DR mode VIPs, an IP address for each VIP must be added to the Loopback Adapter.

In addition, steps must be taken to set the strong/weak host behavior on each Real Server. This is used to either prevent or allow interfaces to receive packets destined for a different interface on the same server.

> **Important** The following 3 steps must be completed on ***all*** Real Servers associated with the VIP.

Step 1 of 3: Install the Microsoft Loopback Adapter

1. Click **Start**, then run **hdwwiz** to start the Hardware Installation Wizard.
2. Once the Wizard has started, click **Next**.
3. Select **Install the hardware that I manually select from a list (Advanced)**, click **Next**.
4. Select **Network adapters**, click **Next**.



5. Select **Microsoft** & **Microsoft KM-Test Loopback Adapter**, click **Next**.
6. Click **Next** to start the installation, when complete click **Finish**.

Step 2 of 3: Configure the Loopback Adapter

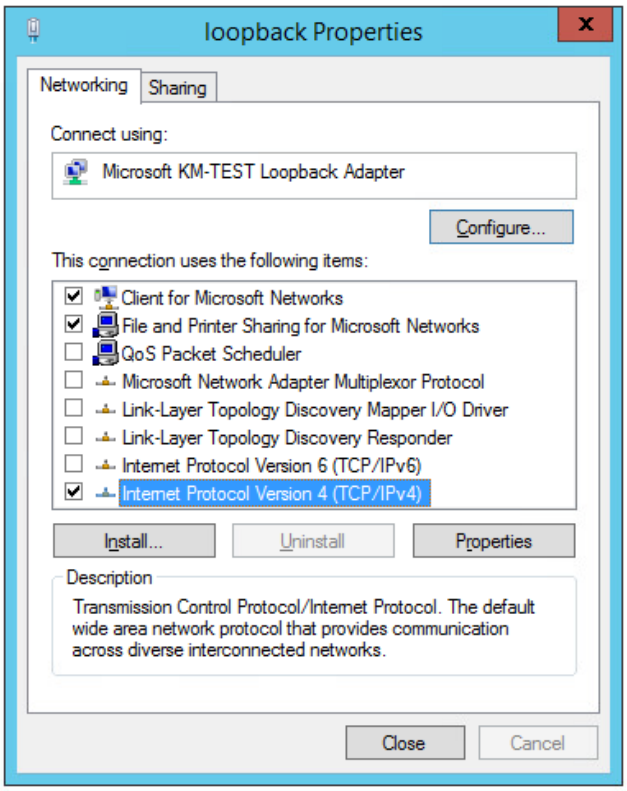
1. Open Control Panel and click **Network and Sharing Center**.
2. Click **Change adapter settings**.
3. Right-click the new Loopback Adapter and select **Properties**.

> **Note** You can configure IPv4 or IPv6 addresses or both depending on your requirements.

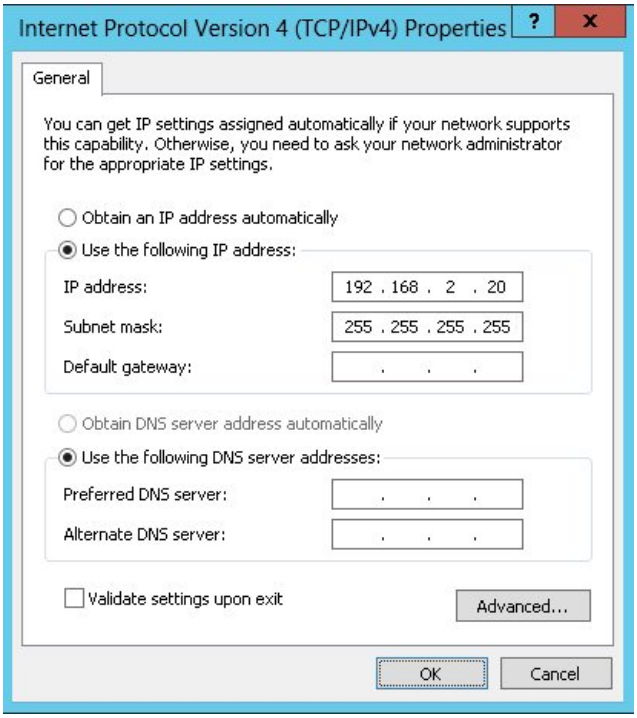
> **Important** when configuring the loopback adapter properties, make sure that **Client for Microsoft Networks** and **File & Printer Sharing for Microsoft Networks** is also checked as shown below.

IPv4 Addresses

1. Uncheck all items except **Client for Microsoft Networks**, **File & Printer Sharing for Microsoft Networks** and **Internet Protocol Version 4 (TCP/IPv4)** as shown below:



2. Ensure that **Internet Protocol Version (TCP/IPv4)** is selected, click **Properties** and configure the IP address to be the same as the Virtual Service address (VIP) with a subnet mask of **255.255.255.255**, e.g. **192.168.2.20/255.255.255.255** as shown below:



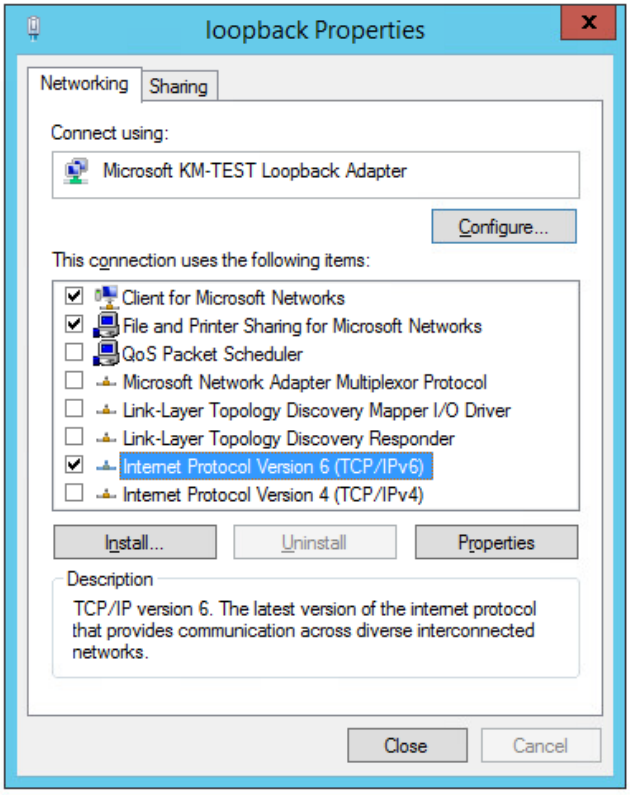
> **Note** **192.168.2.20** is an example, make sure you specify the correct VIP address.

> **Note** If a Real Server is included in multiple DR mode VIPs, an IP address for each VIP must be added to the Loopback Adapter.

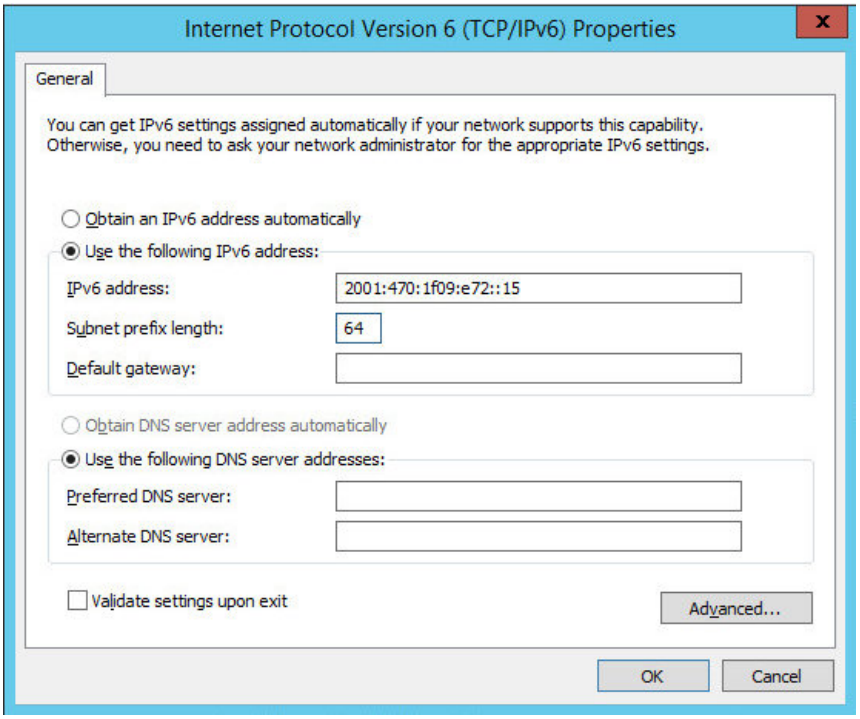
3. Click **OK** then click **Close** to save and apply the new settings.

IPv6 Addresses

1. Uncheck all items except **Client for Microsoft Networks**, **File & Printer Sharing for Microsoft Networks** and **Internet Protocol Version 6 (TCP/IPv6)** as shown below:



2. Ensure that **Internet Protocol Version (TCP/IPv6)** is selected, click **Properties** and configure the IP address to be the same as the Virtual Service (VIP) and set the ***Subnet Prefix Length*** to be the same as your network setting, e.g. **2001:470:1f09:e72::15/64** as shown below:



> **Note** **2001:470:1f09:e72::15/64** is an example, make sure you specify the correct VIP address.

> **Note** If a Real Server is included in multiple DR mode VIPs, an IP address for each VIP must be

added to the Loopback Adapter.

3. Click **OK** then click **Close** to save and apply the new settings.

Step 3 of 3: Configure the strong/weak host behavior

The strong/weak host behavior can be configured using either of the following 2 methods:

- Option 1 - Using Network Shell (netsh) commands
- Option 2 - Using PowerShell cmdlets

The commands in this section assume that the LAN Adapter is named "**net**" and the Loopback Adapter is named "**loopback**" as shown in the example below:

> **Important** Either adjust the commands to use the names allocated to your LAN and loopback adapters, or rename the adapters before running the commands. Names are case sensitive so make sure that the interface names used in the commands match the adapter names exactly.

Option 1 - Using Network Shell (netsh) Commands

To configure the correct strong/weak host behavior run the following commands:

For IPv4 addresses:

```
netsh interface ipv4 set interface "net" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostsend=enabled
```

For IPv6 addresses:

```
netsh interface ipv6 set interface "net" weakhostreceive=enabled
netsh interface ipv6 set interface "loopback" weakhostreceive=enabled
netsh interface ipv6 set interface "loopback" weakhostsend=enabled
netsh interface ipv6 set interface "loopback" dadtransmits=0
```

Option 2 - Using PowerShell Cmdlets

For IPv4 addresses:

```
Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled
-DadTransmits 0 -AddressFamily IPv4
```

```
Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled -AddressFamily IPv4
```

For IPv6 Addresses:

```
Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled
-DadTransmits 0 -AddressFamily IPv6
```

```
Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled -AddressFamily IPv6
```

12.2. 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 is configured first and 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

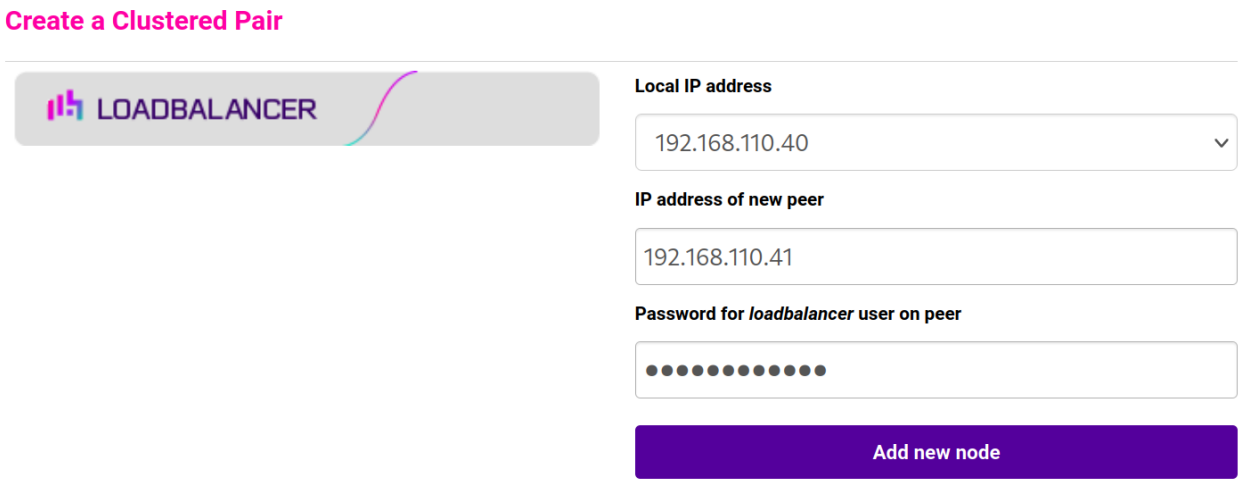
WebUI Main Menu Option	Sub Menu Option	Description
Local Configuration	Physical – Advanced Configuration	Various settings including Internet Proxy, Management Gateway, Firewall connection tracking table size, NIC offloading, SMTP relay, logging and Syslog Server
Local Configuration	Security	Appliance 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.

Adding a Secondary Appliance - Create an HA Clustered Pair

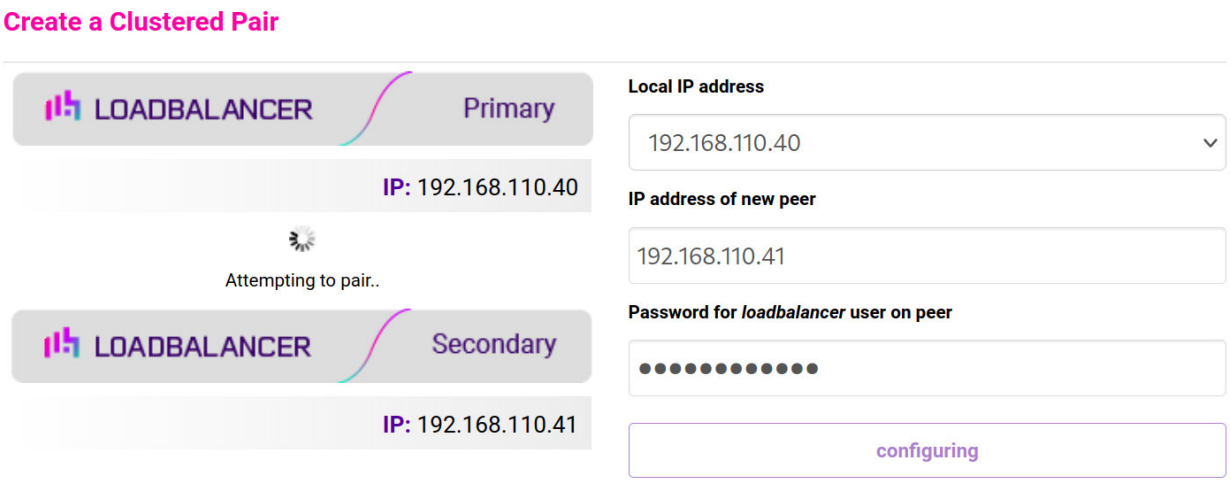
> **Note** If you have already run the firewall lockdown wizard on either appliance, you'll need to ensure that it is temporarily disabled on both appliances whilst performing the pairing process.

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*.

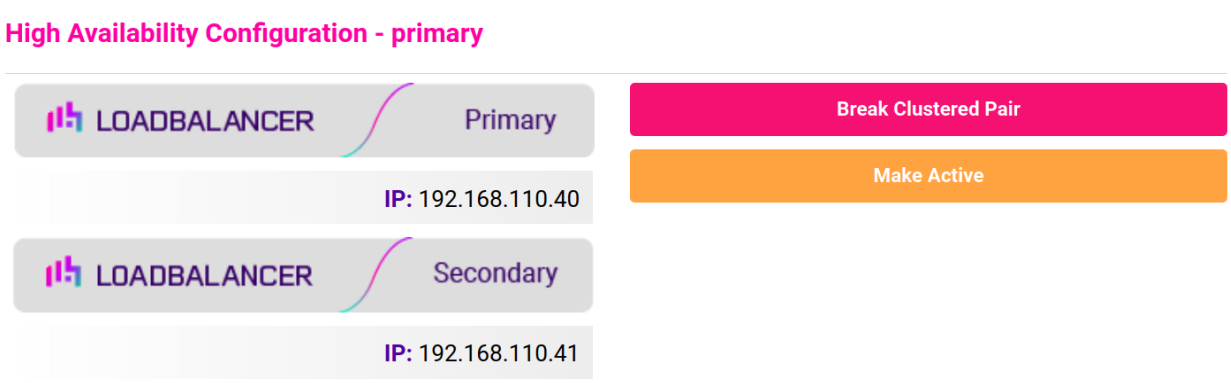


3. Specify the IP address and the *loadbalancer* user's password for the Secondary (peer) appliance as shown in the example above.

4. Click **Add new node**.
5. The pairing process now commences as shown below:



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



7. To finalize the configuration, restart heartbeat and any other services as prompted in the "Commit changes" 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.

13. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.0.0	3 March 2021	Initial version		RJC
1.0.1	25 March 2021	Added section "Loadbalancer.org Appliance – the Basics"	Not included in the initial version	RJC
1.1.0	1 October 2021	Converted the document to AsciiDoc	Move to new documentation system	AH,RJC,ZAC
1.1.1	28 September 2022	Updated layer 7 VIP and RIP creation screenshots	Reflect changes in the web user interface	AH
1.1.2	5 January 2023	Combined software version information into one section Added one level of section numbering Added software update instructions Added table of ports used by the appliance Reworded 'Further Documentation' section Removed references to the colour of certain UI elements	Housekeeping across all documentation	AH
1.1.3	2 February 2023	Updated screenshots	Branding update	AH
1.1.4	7 March 2023	Removed conclusion section	Updates across all documentation	AH
1.2.0	24 March 2023	New document theme Modified diagram colours	Branding update	AH

LOADBALANCER

Visit us: www.loadbalancer.org

Phone us: +44 (0)330 380 1064

Phone us: +1 833 274 2566

Email us: info@loadbalancer.org

Follow us: @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.