LOADBALANCER

DEPLOYMENT GUIDE

Load Balancing Pharos Blueprint®

Version 1.2.1

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/enterprise.

Some features may not be available or fully supported in all cloud platforms due to platform specific limitations. For more details, please refer to the "Main Differences to our Standard (Non-Cloud) Product" section in the appropriate cloud platform Quick Start Guide or check with Loadbalancer.org support.

3. Software Versions Supported

3.1. Loadbalancer.org Appliance

- V8.9.1 and later

> ℹ Note
>
> The screenshots used throughout this document aim to track the latest Loadbalancer.org software version. If you're using an older version, or the very latest, the screenshots presented here may not match your 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

> ℹ 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

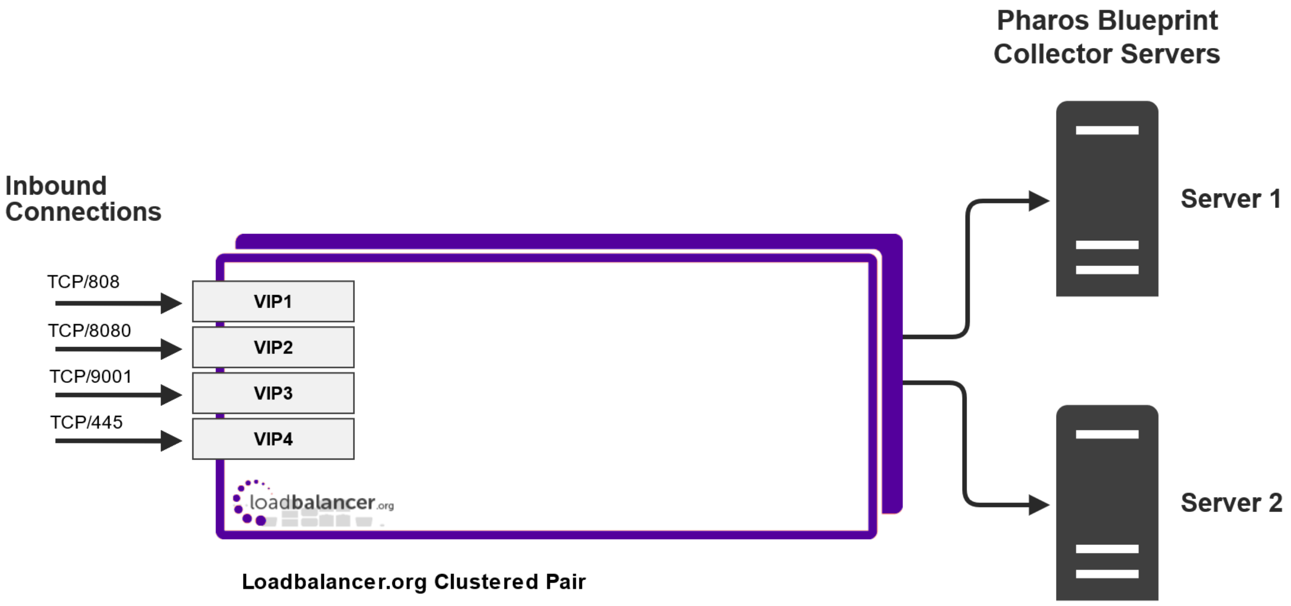
2 or more Collector servers are configured to create a load balanced pool. Clients then connect to this pool via Virtual Services (VIPs).

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 Solve the ARP Problem.

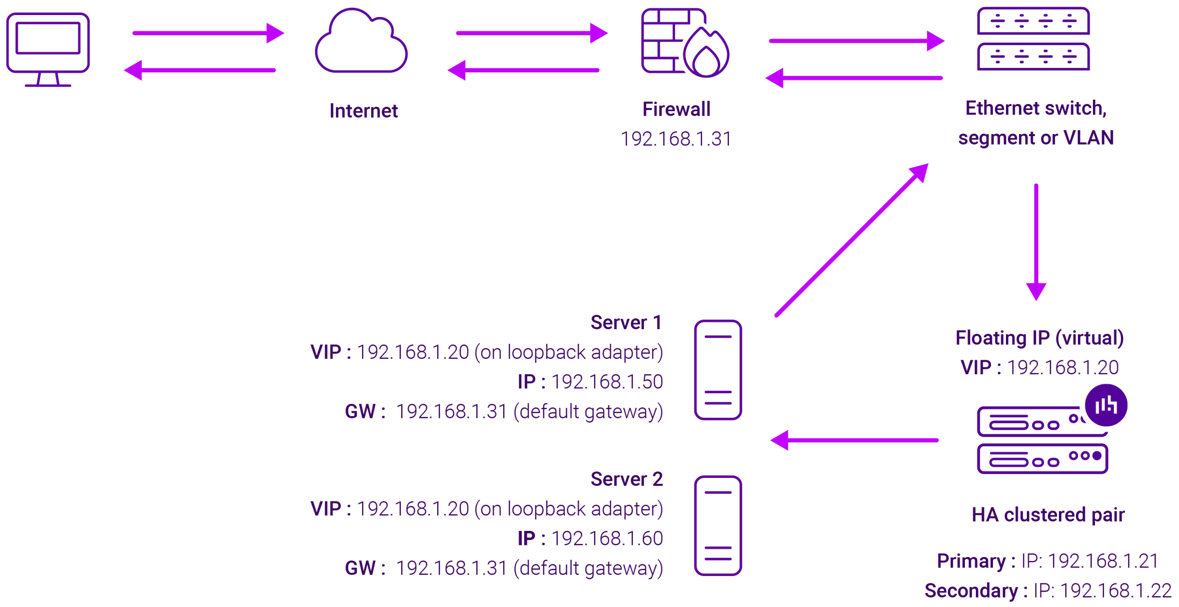
Where it’s not feasible to use layer 4 DR mode, layer 7 SNAT mode should be used. Whilst this mode does not have the raw throughput of layer 4 methods, it still enables high performance load balancing and requires no changes to the Collector Servers.

Each Mode is described below.

5.5.1. Layer 4 DR Mode

Layer 4 DR (Direct Routing) mode is a very high performance solution that requires little change to your existing infrastructure. The image below shows an example network diagram for this mode.

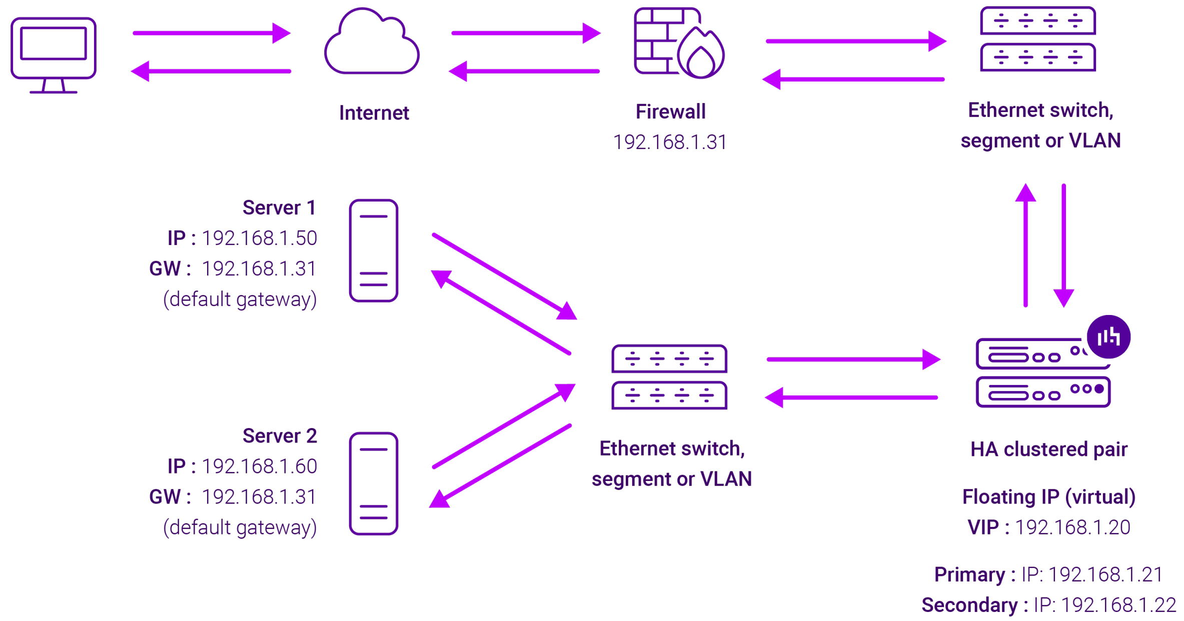
> ℹ Note — Kemp, Brocade, Barracuda & A10 Networks call this *Direct Server Return* and F5 call it *nPath*.


Internet
Firewall
192.168.1.31
Ethernet switch,
segment or VLAN
Server 1
VIP : 192.168.1.20 (on loopback adapter)
IP : 192.168.1.50
GW : 192.168.1.31 (default gateway)
Server 2
VIP : 192.168.1.20 (on loopback adapter)
IP : 192.168.1.60
GW : 192.168.1.31 (default gateway)
Floating IP (virtual)
VIP : 192.168.1.20
HA clustered pair
Primary : IP: 192.168.1.21
Secondary : IP: 192.168.1.22

- 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 each Real Server (and the load balanced application) must respond to both the Real Server's own IP address and the VIP.
- The Real Server should not respond to ARP requests for the VIP. Only the load balancer should do this. Configuring the Real Server 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 mode for HTTP and much faster for other applications such as Remote Desktop Services, streaming media and FTP.
- The load balancer must have an interface in the same subnet as the Real Servers to ensure layer 2 connectivity which is required for DR mode to operate.
- 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.

5.5.2. 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. The image below shows an example network diagram for this mode.



- Because layer 7 SNAT mode is a full proxy, Real Servers in the cluster can be on any accessible network 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, **eth1** is typically used for client side connections and **eth0** is used for Real Server connections, although this is not mandatory since any interface can be used for any purpose.
- 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 servers and other network and administrative 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.

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 SSL 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.

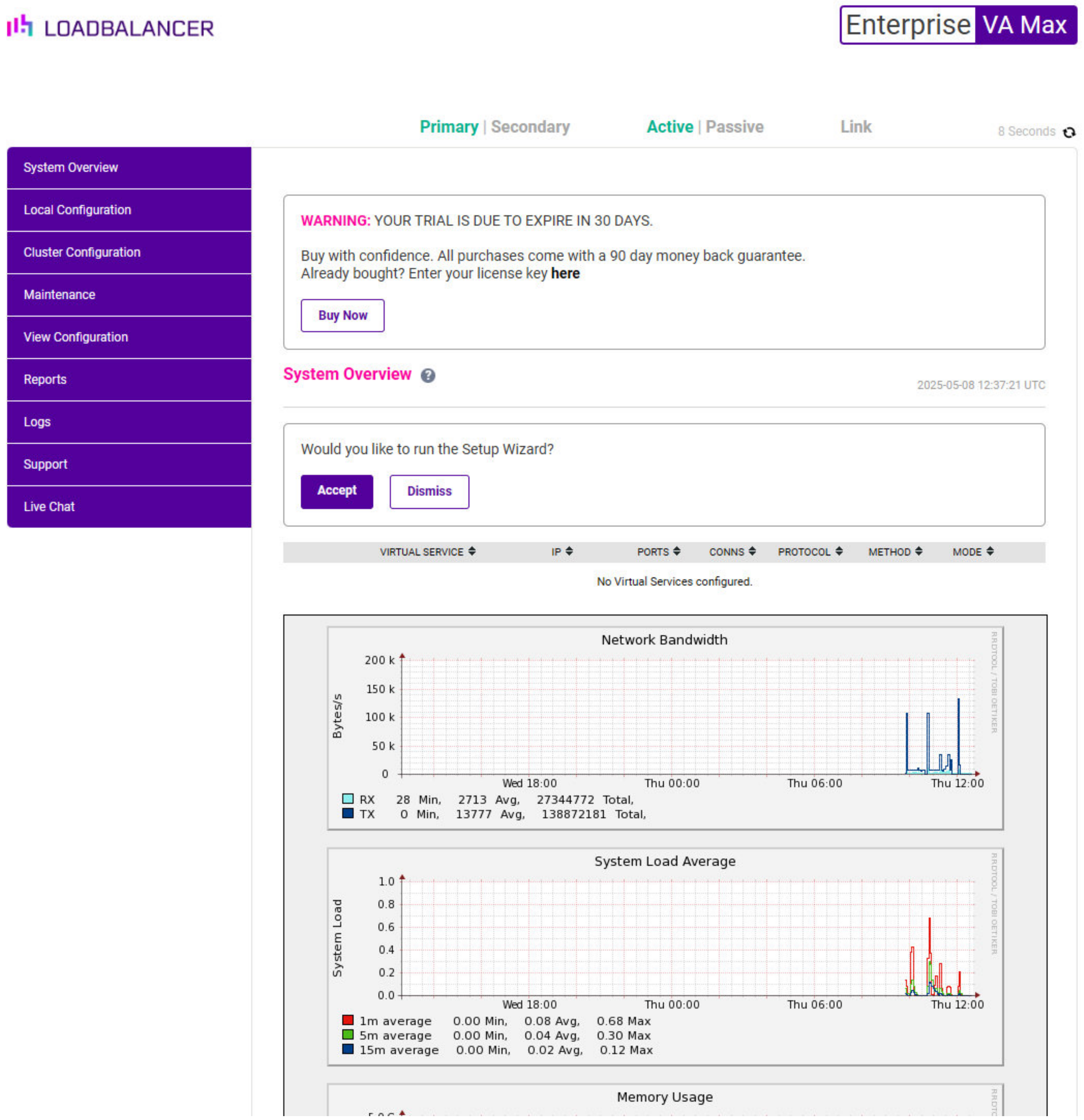
   Note If you need to change the port, IP address or protocol that the WebUI listens on, please refer to Service Socket Addresses.

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:



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

2025-05-08 12:37:21 UTC

Would you like to run the Setup Wizard?

No Virtual Services configured.

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.

6.3.1. 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 creating 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

We recommend that the appliance is kept up to date to ensure that you benefit from the latest bug fixes, security updates and feature improvements. Both online and offline update are supported.

Note

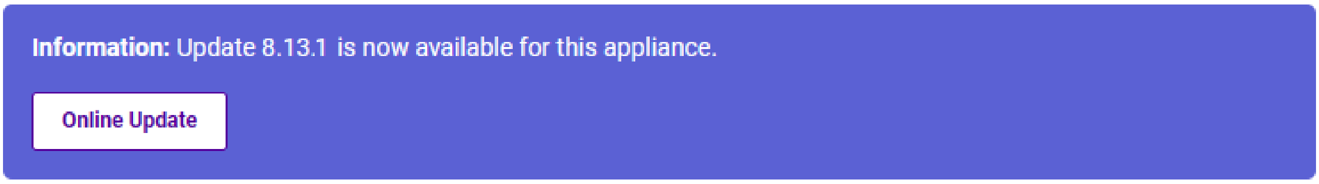
For full details, please refer to Appliance Software Update in the Administration Manual.

Note

Services may need to be restarted/reloaded after the update process completes or in some cases a full appliance restart may be required. We therefore recommend performing the update during a maintenance window.

6.4.1. Online Update

The appliance periodically contacts the Loadbalancer.org update server (**update.loadbalancer.org**) and checks for updates. This is the default behavior and can be disabled if preferred. If an update is found, a notification similar to the example below will be displayed at the top of the WebUI:

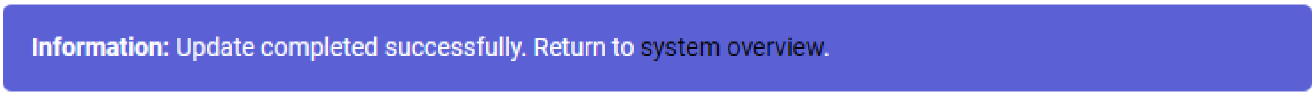

Information: Update 8.13.1 is now available for this appliance.

Click **Online Update**. A summary of all new features, improvements, bug fixes and security updates included in the update will be displayed. Click **Update** at the bottom of the page to start the update process.

Important

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

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


Information: Update completed successfully. Return to system overview.

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

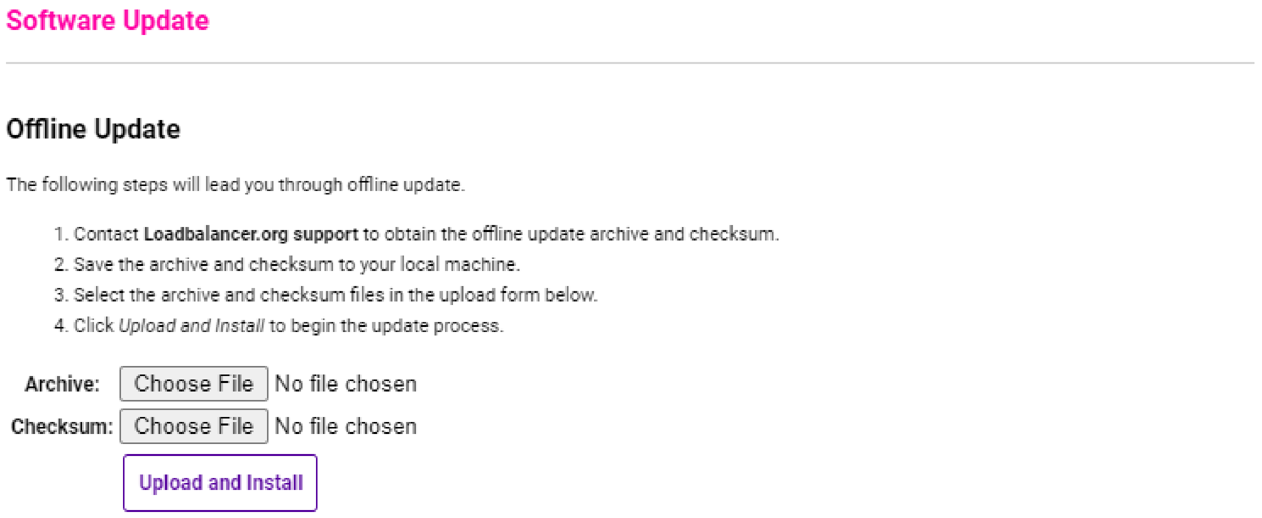
6.4.2. Offline Update

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

To check for the latest version, please refer to our product roadmap page available here. To obtain the latest offline update files contact support@loadbalancer.org.

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:



Software Update

Offline Update

The following steps will lead you through offline update.

1. Contact **Loadbalancer.org support** to obtain the offline update archive and checksum.
2. Save the archive and checksum to your local machine.
3. Select the archive and checksum files in the upload form below.
4. Click *Upload and Install* to begin the update process.

Archive: Choose File No file chosen

Checksum: Choose File No file chosen

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 / GSLB
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	9000 *	Gateway service (Centralized/Portal Management)
TCP	9080 *	WebUI - HTTP (disabled by default)
TCP	9081 *	Nginx fallback page
TCP	9443 *	WebUI - HTTPS
TCP	25565 *	Shuttle service (Centralized/Portal Management)

ℹ Note

The ports used for SSH, GSLB, SNMP, the WebUI, the fallback page, the gateway service and the shuttle service can be changed if required. For more information, please refer to Service Socket Addresses.

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. Prepare the Pharos Blueprint Servers for Load Balancing

7.1.1. Solve the ARP Problem

If layer 4 DR mode is used, the "ARP problem" must be solved on each load balanced Collector Server. This enables DR mode to work correctly. The exact steps required depend on the particular operating system in use. The section below detail the steps for Windows 2012 & later. For other operating systems, please refer to DR Mode Considerations in the Administration Manual.

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.

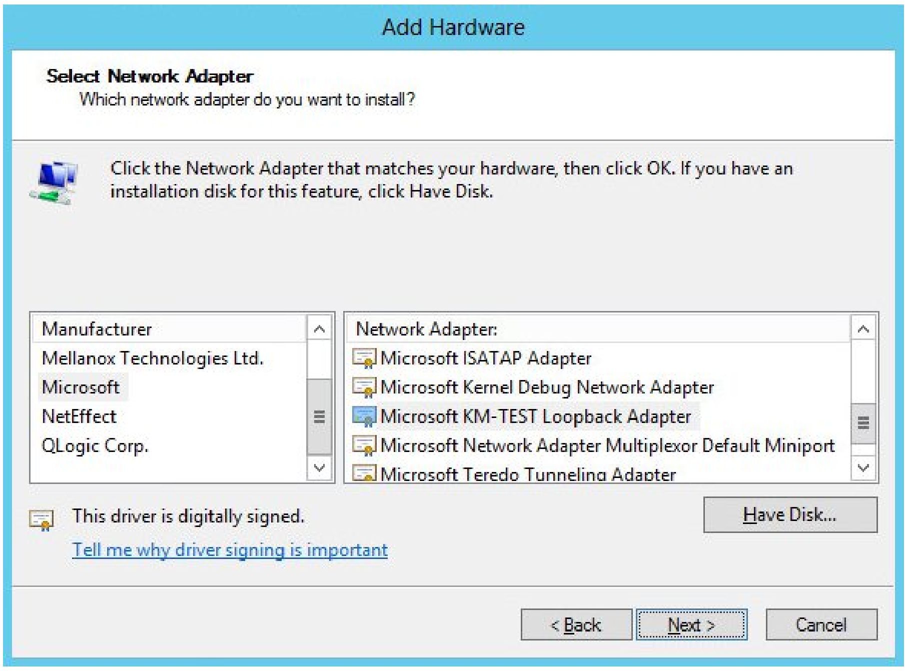
In addition, the strong/weak host behavior must be configured on each Real Server. The weak host model allows packets with any IP to be sent or received via an interface. The strong host model only allows packets with an IP belonging to the interface to be sent or received.

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**.



Add Hardware

Select Network Adapter

Which network adapter do you want to install?

Click the Network Adapter that matches your hardware, then click OK. If you have an installation disk for this feature, click Have Disk.

Manufacturer	Network Adapter:
Mellanox Technologies Ltd.	Microsoft ISATAP Adapter
Microsoft	Microsoft Kernel Debug Network Adapter
NetEffect	Microsoft KM-TEST Loopback Adapter
QLogic Corp.	Microsoft Network Adapter Multiplexor Default Miniport
	Microsoft Teredo Tunneling Adapter

This driver is digitally signed.

Tell me why driver signing is important

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

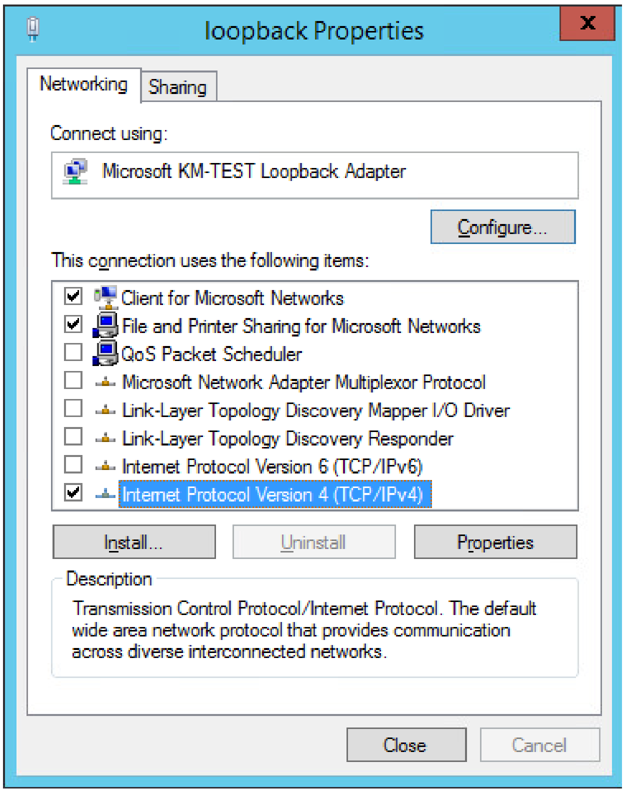
1. Open Control Panel and click **Network and Sharing Center**.
2. Click **Change adapter settings**.
3. Right-click the new Loopback Adapter and select **Properties**.

> 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:



Connect using:

Microsoft KM-TEST Loopback Adapter

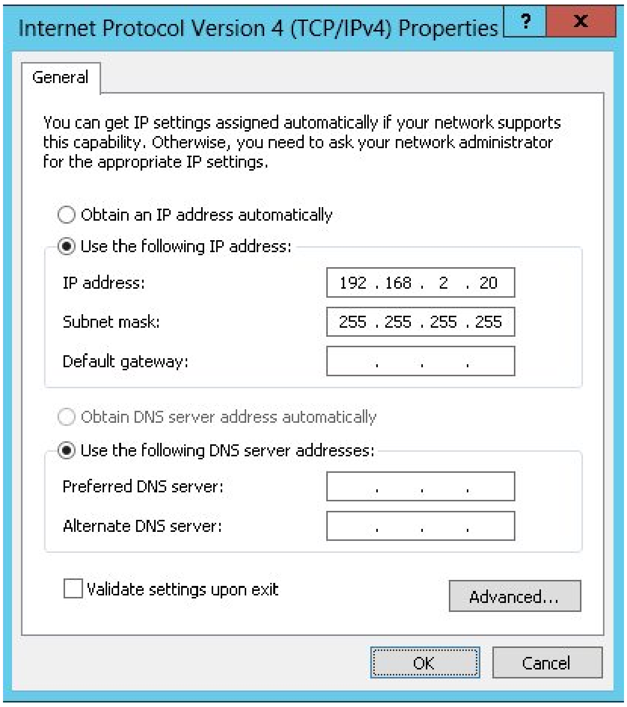
This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
□ QoS Packet Scheduler
□ Microsoft Network Adapter Multiplexor Protocol
□ Link-Layer Topology Discovery Mapper I/O Driver
□ Link-Layer Topology Discovery Responder
□ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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:



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 2 . 20
Subnet mask: 255 . 255 . 255 . 255
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

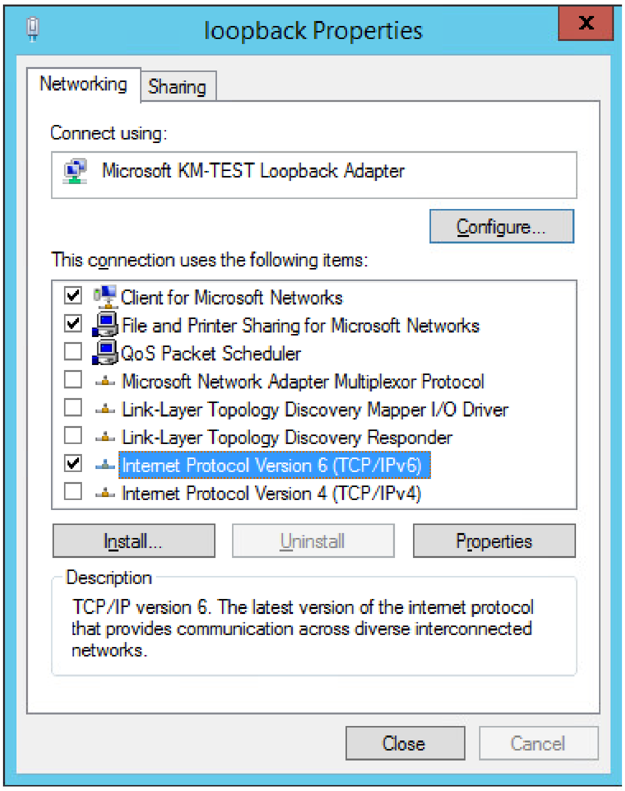
Note **192.168.2.20** is an example, make sure you specify the correct VIP address.

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:



Connect using:

Microsoft KM-TEST Loopback Adapter

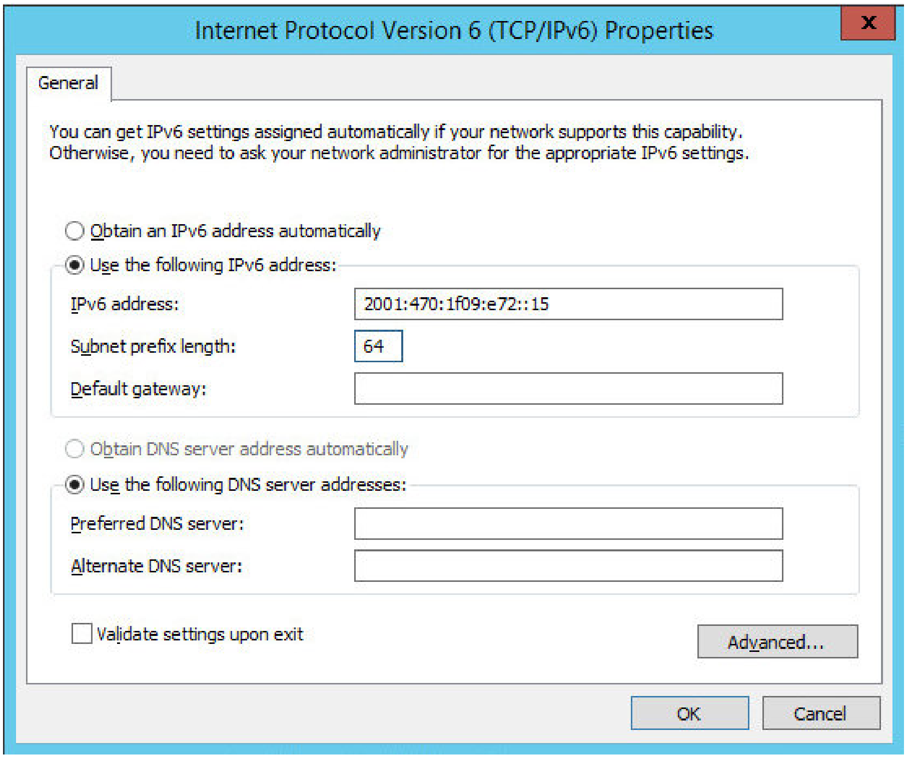
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- □ QoS Packet Scheduler
- □ Microsoft Network Adapter Multiplexor Protocol
- □ Link-Layer Topology Discovery Mapper I/O Driver
- □ Link-Layer Topology Discovery Responder
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- □ Internet Protocol Version 4 (TCP/IPv4)

Description

TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.

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:



Internet Protocol Version 6 (TCP/IPv6) Properties

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

○ Obtain an IPv6 address automatically

● Use the following IPv6 address:

IPv6 address: 2001:470:1f09:e72::15

Subnet prefix length: 64

Default gateway:

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

□ Validate settings upon exit

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

ℹ 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.

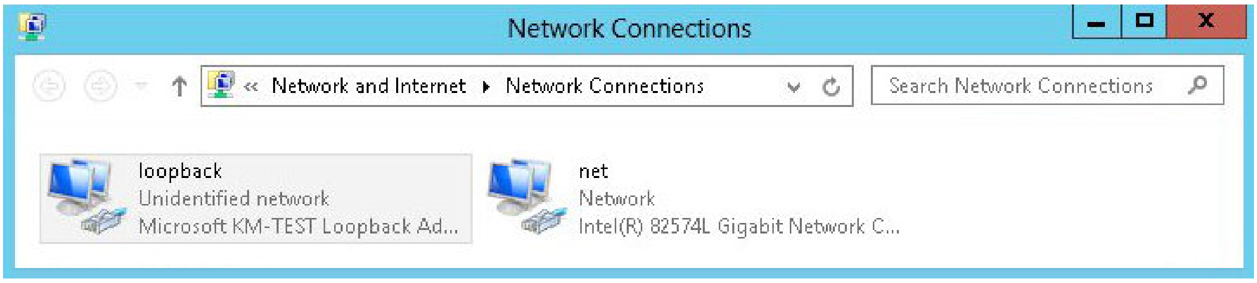
3. Click **OK** then click **Close** to save and apply the new settings.

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:



Network Connections
« Network and Internet ▸ Network Connections
Search Network Connections

loopback
Unidentified network
Microsoft KM-TEST Loopback Ad...

net
Network
Intel(R) 82574L Gigabit Network C...

ⓘ 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
```

7.1.2. Enable Print and Document Server Load Balancing

When load balancing Microsoft print and document servers, a number of additional configuration steps must be followed to allow them to be load balanced and accessed via a shared name. The exact steps required depend on the particular version of Windows Server being used as detailed below.

Pre-Requisites

1. Each Server must be joined to the same domain as the client PCs.

2. Each Server must have the **Print and Document Service** role installed.
3. All printers must be installed & shared on each Server using exactly the same share names, settings and permissions.

> ℹ Note
>
> A number of issues have been reported when using Type 4 print drivers, so whenever possible we recommend using Type 3 drivers. Type 4 drivers are usually bundled with the operating system or are downloaded from Windows update, whereas Type 3 drivers are typically downloaded from the printer manufacturer's website.

Enable access via Hostname

To enable the load balanced Print and Document Servers to be accessed via an appropriate hostname, complete the following steps:

> ℹ Note
>
> The configuration steps below assume the hostname for the VIP is **blueprintservice** and the domain name is **lbtestdom.com**. Change these to suit your environment.

Windows 2019 & Later

For Windows 2019 & later, local host file entries and a single Registry Key must be added to each Server:

1. Add the following host entries to the local hosts file on each Server:

```
<Real Server IP address> blueprintservice
<Real Server IP address> blueprintservice.lbtestdom.com
```

For example, if you have 2 Print and Document Servers - 192.168.81.11 and 192.168.81.12, the following entries must be added:

On the 192.168.81.11 server:

```
192.168.81.11 blueprintservice
192.168.81.11 blueprintservice.lbtestdom.com
```

On the 192.168.81.12 server:

```
192.168.81.12 blueprintservice
192.168.81.12 blueprintservice.lbtestdom.com
```

2. Add the following Registry Key to each Server:

> ℹ Note
>
> In the example presented here, **blueprintservice** is the hostname that will be used to access the load balanced Servers via the virtual service (VIP) created on the load balancer. This can be set to be any appropriate name, although whatever name is used, it must be the **same name** that is used for the DNS entry described in the "Configure DNS Name

Resolution" section below.

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

Windows 2012 & 2016

For Windows 2012 & 2016, the following Registry Keys must be added to each Server:

> ℹ Note
>
> In the example presented here, **blueprintservice** is the hostname that will be used to access the load balanced Servers via the virtual service (VIP) created on the load balancer. This can be set to be any appropriate name, although whatever name is used, it must be the **same name** that is used for the DNS entry described in the "Configure DNS Name Resolution" section below.

```
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
```

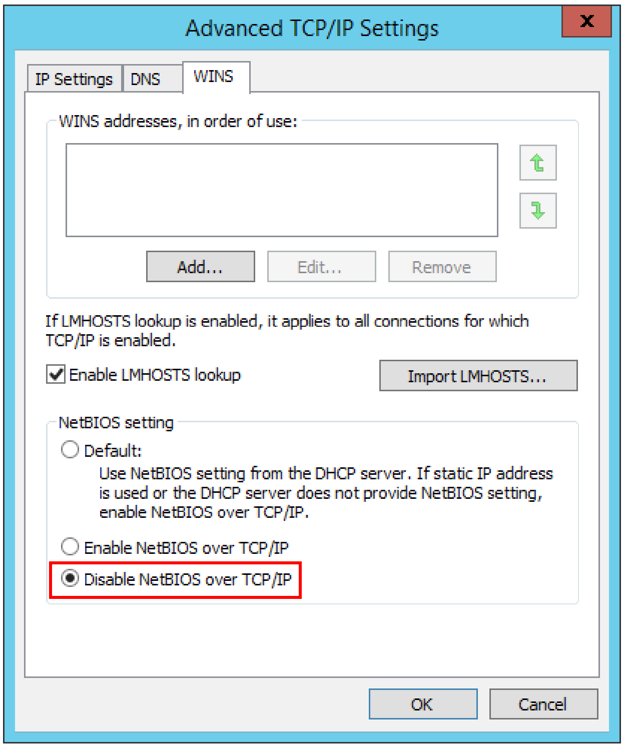
```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
Value: OptionalNames
Type: REG_MULTI_SZ
Data: blueprintservice
```

Configure DNS Name Resolution

1. Create a DNS Host (A) record that points to the VIP address. The hostname used must match the value set for the REG_MULTI_SZ **OptionalNames** registry entry, in this example: **blueprintservice** → **192.168.81.10**.

Disable NetBIOS over TCP/IP

1. On each Server, disable NetBIOS over TCP/IP on **all** interfaces:



Advanced TCP/IP Settings

IP Settings | DNS | WINS

WINS addresses, in order of use:

Add... Edit... Remove

If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☑ Enable LMHOSTS lookup   Import LMHOSTS...

NetBIOS setting

○ Default:
Use NetBIOS setting from the DHCP server. If static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.

○ Enable NetBIOS over TCP/IP

● Disable NetBIOS over TCP/IP

OK Cancel

Server Reboot

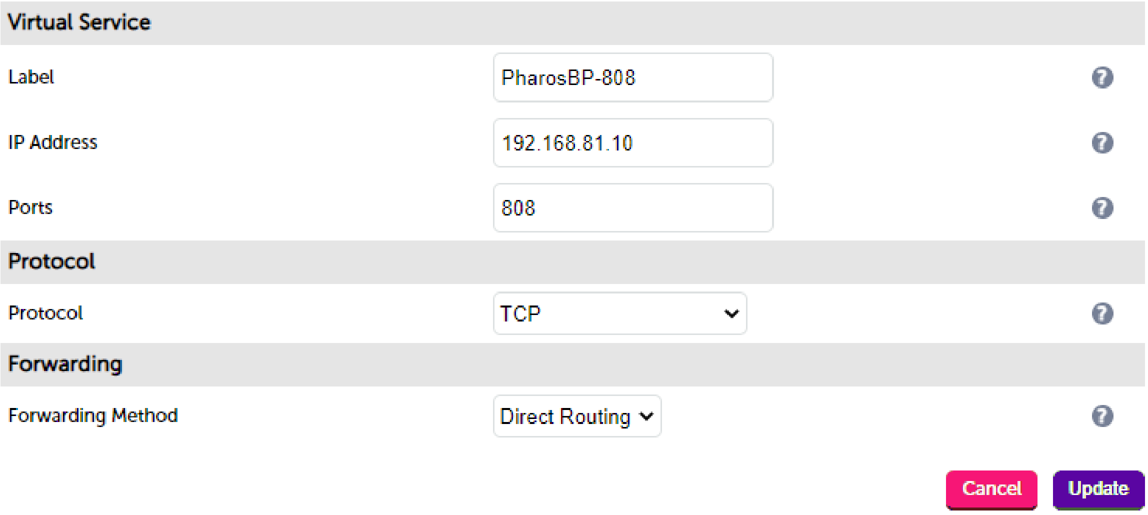
To apply the changes, reboot each Server.

7.2. Configure the Virtual Services

7.2.1. 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**.



Virtual Service	
Label	PharosBP-808
IP Address	192.168.81.10
Ports	808
Protocol	
Protocol	TCP
Forwarding	
Forwarding Method	Direct Routing

Cancel Update

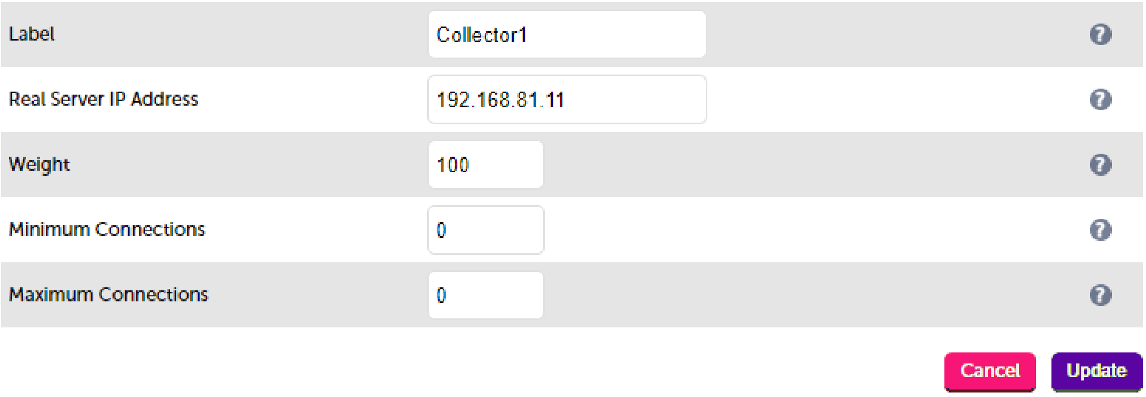
2. Define the *Label* (i.e. the name) for the virtual service as required, e.g. **PharosBP-808**.

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.



Label	Collector1
Real Server IP Address	192.168.81.11
Weight	100
Minimum Connections	0
Maximum Connections	0

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.

7.2.2. 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.

7.2.3. 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.

7.2.4. 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. Prepare the Pharos Blueprint Servers for Load Balancing

8.1.1. Enable Print and Document Server Load Balancing

When load balancing Microsoft print and document servers, a number of additional configuration steps must be followed to allow them to be load balanced and accessed via a shared name. The exact steps required depend on the particular version of Windows Server being used as detailed below.

Pre-Requisites

1. Each Server must be joined to the same domain as the client PCs.
2. Each Server must have the **Print and Document Service** role installed.
3. All printers must be installed & shared on each Server using exactly the same share names, settings and permissions.

> ℹ Note
>
> A number of issues have been reported when using Type 4 print drivers, so whenever possible we recommend using Type 3 drivers. Type 4 drivers are usually bundled with the operating system or are downloaded from Windows update, whereas Type 3 drivers are typically downloaded from the printer manufacturer’s website.

Enable access via Hostname

To enable the load balanced Print and Document Servers to be accessed via an appropriate hostname, complete the following steps:

> ℹ Note
>
> The configuration steps below assume the hostname for the VIP is **blueprintservice** and the domain name is **lbtestdom.com**. Change these to suit your environment.

Windows 2019 & Later

For Windows 2019 & later, local host file entries and a single Registry Key must be added to each Server:

1. Add the following host entries to the local hosts file on each Server:

   ```
   <Real Server IP address> blueprintservice
   <Real Server IP address> blueprintservice.lbtestdom.com
   ```

   For example, if you have 2 Print and Document Servers - 192.168.81.11 and 192.168.81.12, the following entries must be added:

   On the 192.168.81.11 server:

   ```
   192.168.81.11 blueprintservice
   192.168.81.11 blueprintservice.lbtestdom.com
   ```

   On the 192.168.81.12 server:

   ```
   192.168.81.12 blueprintservice
   192.168.81.12 blueprintservice.lbtestdom.com
   ```

2. Add the following Registry Key to each Server:

   > ℹ Note
   >
   > In the example presented here, **blueprintservice** is the hostname that will be used to access the load balanced Servers via the virtual service (VIP) created on the load balancer. This can be set to be any appropriate name, although whatever name is used, it must be the **same name** that is used for the DNS entry described in the "Configure DNS Name Resolution" section below.

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

Windows 2012 & 2016

For Windows 2012 & 2016, the following Registry Keys must be added to each Server:

> ℹ Note
>
> In the example presented here, **blueprintservice** is the hostname that will be used to access the load balanced Servers via the virtual service (VIP) created on the load balancer. This can be set to be any appropriate name, although whatever name is used, it must be the **same name** that is used for the DNS entry described in the "Configure DNS Name Resolution" section below.

```
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
```

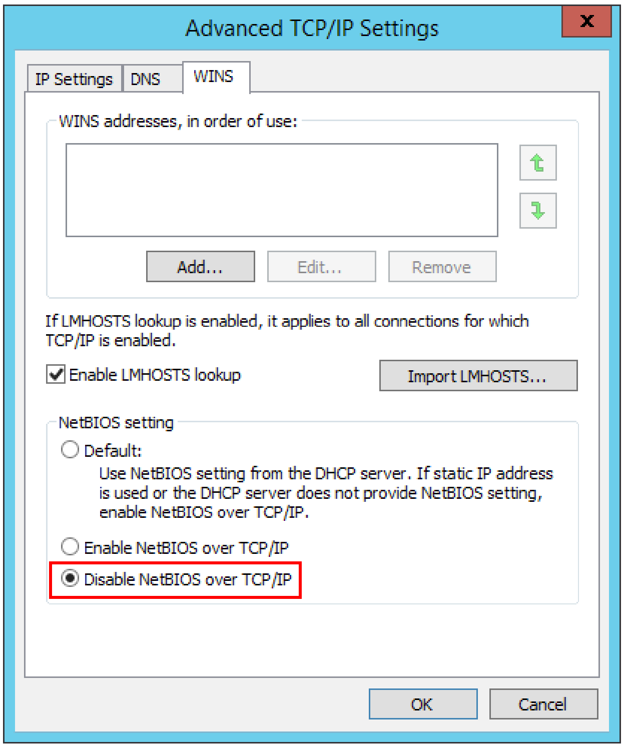
```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
Value: OptionalNames
Type: REG_MULTI_SZ
Data: blueprintservice
```

Configure DNS Name Resolution

1. Create a DNS Host (A) record that points to the VIP address. The hostname used must match the value set for the REG_MULTI_SZ **OptionalNames** registry entry, in this example: **blueprintservice** → **192.168.81.10**.

Disable NetBIOS over TCP/IP

1. On each Server, disable NetBIOS over TCP/IP on **all** interfaces:



If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☑ Enable LMHOSTS lookup

○ Default:
Use NetBIOS setting from the DHCP server. If static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.

○ Enable NetBIOS over TCP/IP

● Disable NetBIOS over TCP/IP

Server Reboot

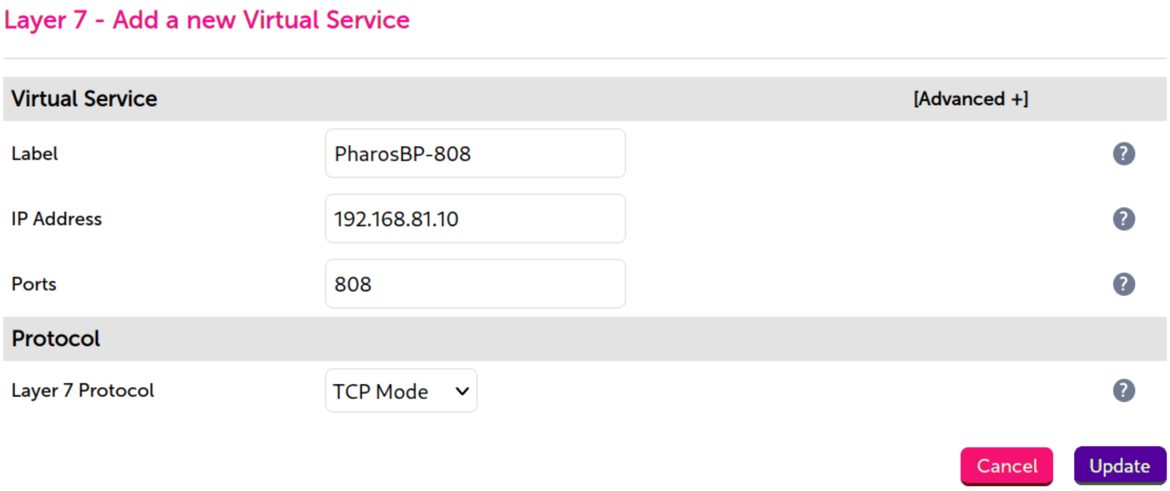
To apply the changes, reboot each Server.

8.2. Configure the Virtual Services

8.2.1. 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**.



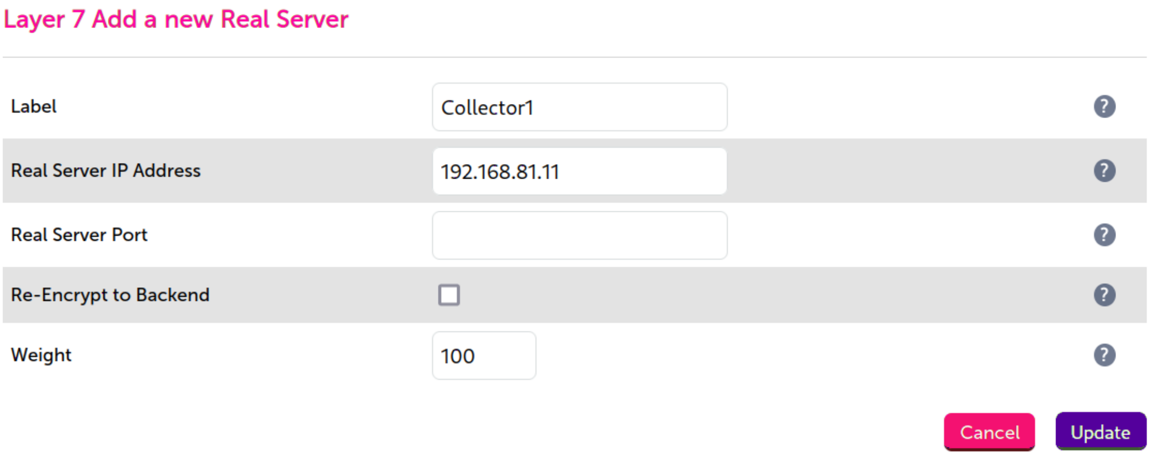
Layer 7 - Add a new Virtual Service

Virtual Service	[Advanced +]
Label	PharosBP-808
IP Address	192.168.81.10
Ports	808
Protocol	
Layer 7 Protocol	TCP Mode

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.



Layer 7 Add a new Real Server

Label	Collector1
Real Server IP Address	192.168.81.11
Real Server Port	
Re-Encrypt to Backend	□
Weight	100

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.

8.2.2. 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.

8.2.3. 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.

8.2.4. 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.

8.2.5. 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 by browsing to the relevant DNS name, in this guide **blueprintservice**.

e.g.

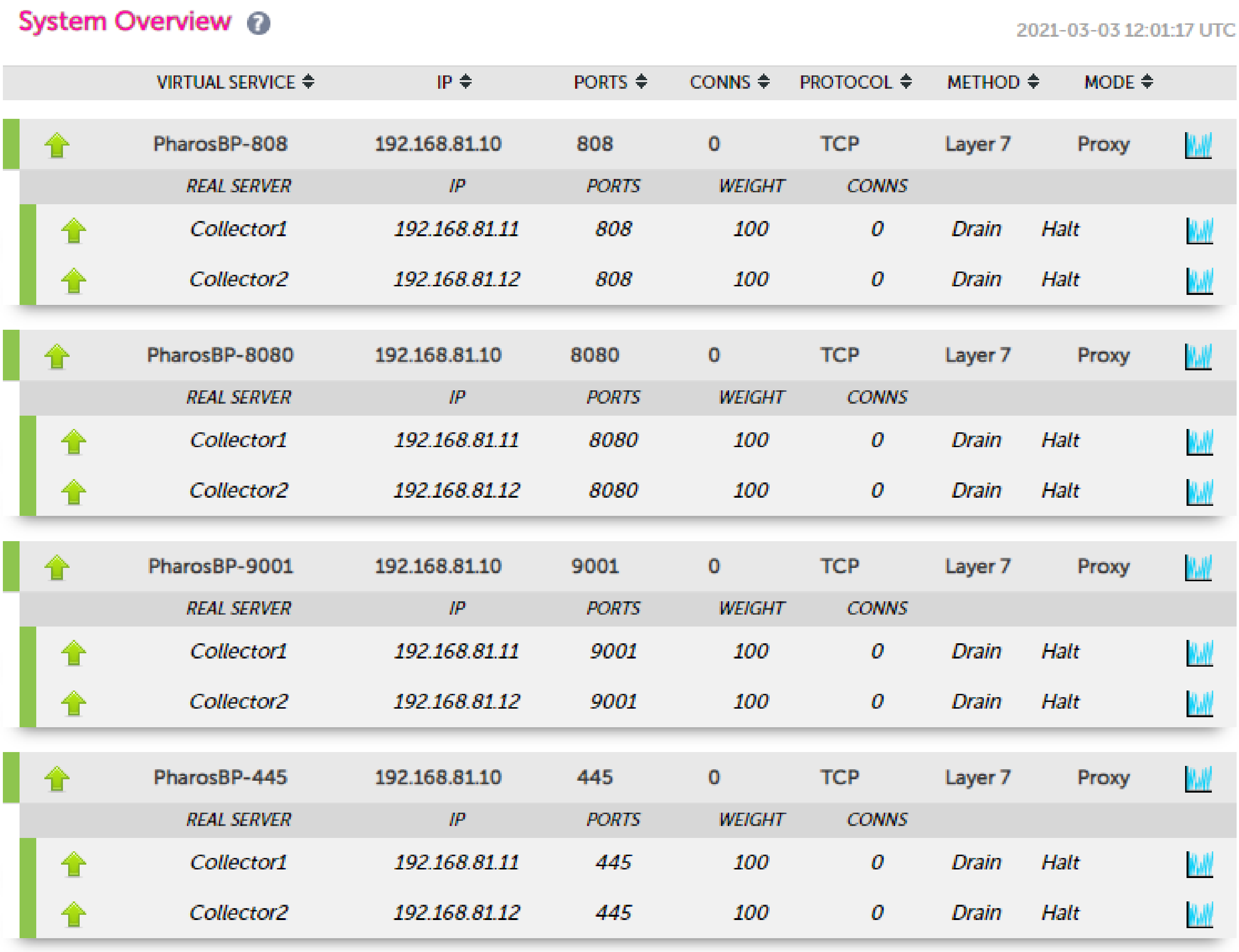
```
\\blueprintservice

\\blueprintservice.lbtestdom.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.



System Overview

2021-03-03 12:01:17 UTC

	VIRTUAL SERVICE	IP	PORTS	CONNS	PROTOCOL	METHOD	MODE
↑	PharosBP-808	192.168.81.10	808	0	TCP	Layer 7	Proxy
	REAL SERVER	*IP*	*PORTS*	*WEIGHT*	*CONNS*		
↑	*Collector1*	*192.168.81.11*	*808*	*100*	*0*	*Drain*	*Halt*
↑	*Collector2*	*192.168.81.12*	*808*	*100*	*0*	*Drain*	*Halt*
↑	PharosBP-8080	192.168.81.10	8080	0	TCP	Layer 7	Proxy
	REAL SERVER	*IP*	*PORTS*	*WEIGHT*	*CONNS*		
↑	*Collector1*	*192.168.81.11*	*8080*	*100*	*0*	*Drain*	*Halt*
↑	*Collector2*	*192.168.81.12*	*8080*	*100*	*0*	*Drain*	*Halt*
↑	PharosBP-9001	192.168.81.10	9001	0	TCP	Layer 7	Proxy
	REAL SERVER	*IP*	*PORTS*	*WEIGHT*	*CONNS*		
↑	*Collector1*	*192.168.81.11*	*9001*	*100*	*0*	*Drain*	*Halt*
↑	*Collector2*	*192.168.81.12*	*9001*	*100*	*0*	*Drain*	*Halt*
↑	PharosBP-445	192.168.81.10	445	0	TCP	Layer 7	Proxy
	REAL SERVER	*IP*	*PORTS*	*WEIGHT*	*CONNS*		
↑	*Collector1*	*192.168.81.11*	*445*	*100*	*0*	*Drain*	*Halt*
↑	*Collector2*	*192.168.81.12*	*445*	*100*	*0*	*Drain*	*Halt*

> **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. 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 fully configured first, then the Secondary appliance can be added to create an HA pair. Once the HA pair is configured, load balanced services must be configured and modified on the Primary appliance. The Secondary appliance will be automatically kept in sync.

> **Note** For Enterprise Azure, the HA pair should be configured first. For more information, please refer to the Azure Quick Start/Configuration Guide available in the documentation library

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.

12.1.1. 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	Interface IP addresses, bonding configuration and VLANs
Local Configuration	Routing	Default gateways and static routes
Local Configuration	System Date & time	Time and date related settings
Local Configuration	Physical – Advanced Configuration	Various appliance settings
Local Configuration	Portal Management	Portal management settings
Local Configuration	Security	Security settings
Local Configuration	SNMP Configuration	SNMP settings
Local Configuration	Graphing	Graphing settings
Local Configuration	License Key	Appliance licensing
Maintenance	Backup & Restore	Local XML backups
Maintenance	Software Updates	Appliance software updates
Maintenance	Fallback Page	Fallback page configuration
Maintenance	Firewall Script	Firewall (iptables) configuration
Maintenance	Firewall Lockdown Wizard	Appliance management lockdown settings

Important

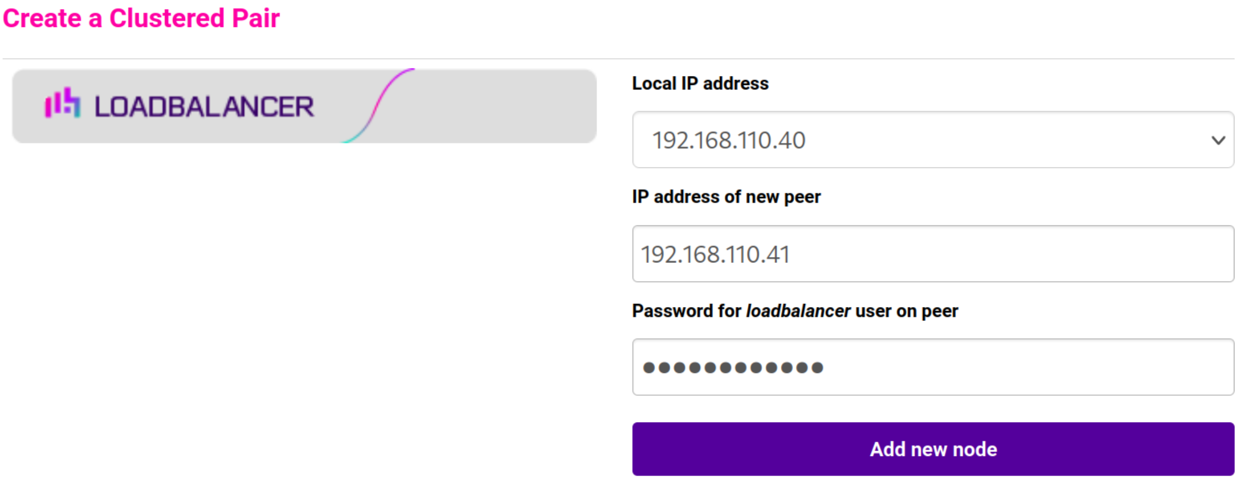
Make sure that where any of the above have been configured on the Primary appliance, they're also configured on the Secondary.

12.1.2. Configuring the 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*.



Create a Clustered Pair

Local IP address

192.168.110.40

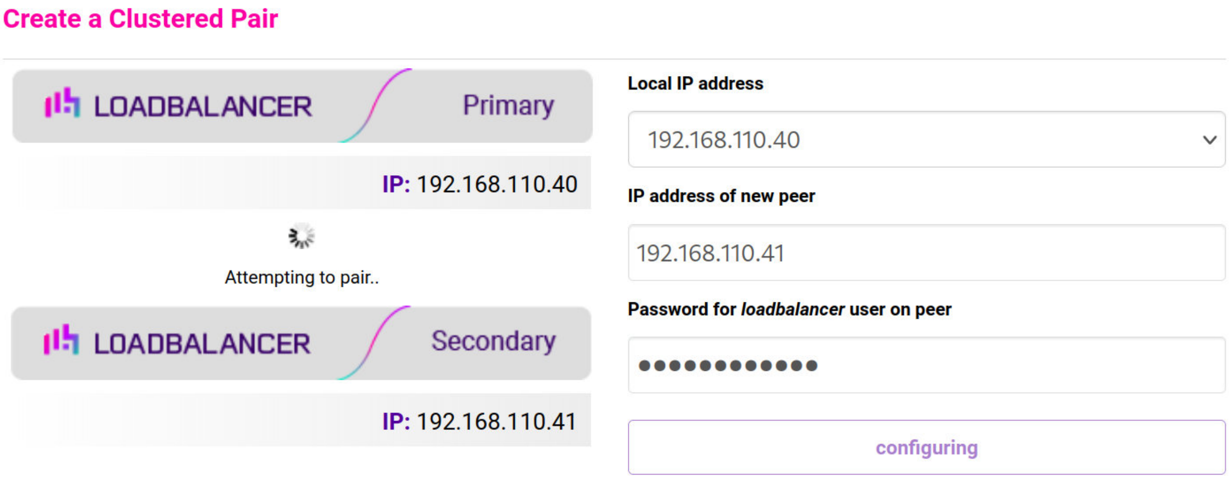
IP address of new peer

192.168.110.41

Password for *loadbalancer* user on peer

●●●●●●●●●●●●

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:



Create a Clustered Pair

IP: 192.168.110.40

Attempting to pair..

IP: 192.168.110.41

Local IP address

192.168.110.40

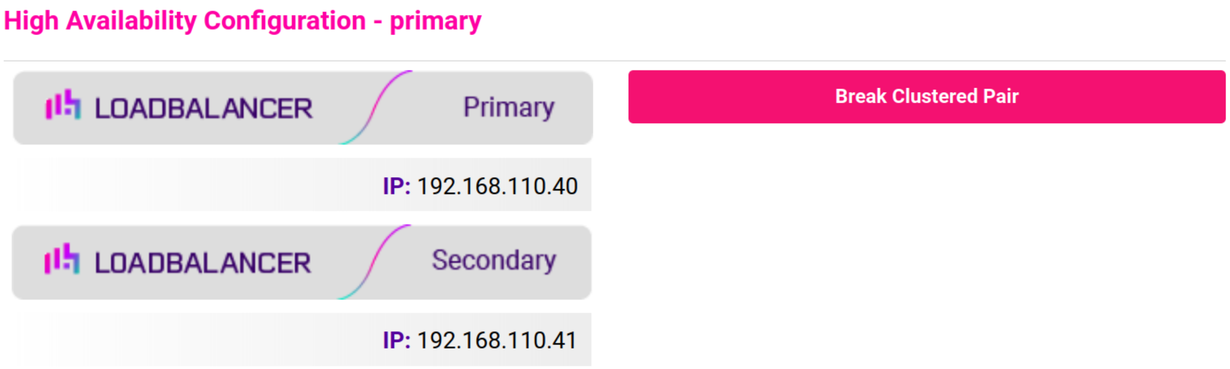
IP address of new peer

192.168.110.41

Password for *loadbalancer* user on peer

●●●●●●●●●●●●

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



High Availability Configuration - primary

IP: 192.168.110.40

IP: 192.168.110.41

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.

> ℹ Note
>
> Clicking the **Restart Heartbeat** button on the Primary appliance will also automatically restart heartbeat on the Secondary appliance.

> ℹ Note
>
> For more details on configuring HA with 2 appliances, please refer to Appliance Clustering for HA.

> ℹ 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
1.2.1	19 February 2025	Modified guide to use common Microsoft Print and Document Server configuration component	Document standardisation	RJC

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.