LOADBALANCER

DEPLOYMENT GUIDE

Load Balancing GE HealthCare Centricity PACS

Version 1.0

Table of Contents

1. About this Guide

This guide details the steps required to configure a load balanced GE HealthCare Centricity PACS environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Centricity PACS configuration changes that are required to enable load balancing.

1.1. Acronyms Used in the Guide

Acronym	Description
EA	Enterprise Archive
ZFP	Zero Footprint
UV	Universal Viewer
DAS	Data Acquisition System
WFM	Work Flow Manager
CCG	Centricity Clinical Gateway

2. Prerequisites

1. Have access to the VMware Hypervisor environment to enable the Loadbalancer.org Virtual Appliance (VA) to be deployed and configured.
2. Have sufficient available Hypervisor CPU and memory resources to allocate to the VA based on the required throughput - for details refer to Virtual Hardware Resource Requirements.
3. Ensure that firewalls and other network devices are configured to allow management and other required access to the VA - for details of all ports used refer to Ports Used by the Appliance.
4. Ensure that firewalls and other network devices are configured to allow client/test access to all Virtual Services (VIPs).
5. Ensure that firewalls and other network devices are configured to allow load balancer access to all Centricity PACS servers.
6. Have IP addresses for the VA and all required Virtual Services.
7. Have access to the Centricity PACS servers to enable the ARP problem to be solved for Layer 4 DR mode VIPs - for details refer to Configuring Centricity PACS for Load Balancing.

3. Software Versions Supported

3.1. Loadbalancer.org Appliance

- V8.9.0 & later

3.2. GE HealthCare Centricity PACS

- All versions

4. Load Balancing Centricity PACS

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

4.1. Virtual Services (VIP) Requirements

To provide load balancing and HA for Centricity PACS, the following VIPs are required:

Ref.	VIP Name	Mode	Port(s)	Persistence Mode	Health Check
VIP 1	EA_XDS_Service	L4 DR	80	None	HTTP (GET)
VIP 2	EA_Dicom_Service	L4 DR	104	None	HTTP (GET)
VIP 3	EA_Secure_Dicom_Service	L4 DR	2762	None	HTTP (GET)
VIP 4	EA_HL7_Service	L4 DR	2575	None	HTTP (GET)
VIP 5	EA_Secure_HL7_Service	L4 DR	2576	None	HTTP (GET)
VIP 6	EA_Study_Management_Service	L4 DR	443	None	HTTP (GET)
VIP 7	DB_MT	L4 SNAT	All ports except 20000	Source IP	Connect to port
VIP 8	DB_DBVIP	L4 SNAT	20000	Source IP	ICMP Ping
VIP 9	DAS_Pool	L4 DR	4100,8080,104	None	HTTP (GET)
VIP 10	ZFP	L7 SNAT	443	Source IP	HTTPS (GET)
VIP 11	UV	L7 SNAT	443	Source IP	HTTPS (GET)
VIP 12	Dakota	L7 SNAT	SP1: 8080, SP2: 8443	Source IP	SP1: Connect to port, SP2: HTTPS (GET)
VIP 13	WFM_Play_Group	L7 SNAT	SP1: 8080, SP2: 9443	Source IP	HTTPS (GET)
VIP 14	WFM_tomcat_Group	L7 SNAT	SP1: 9096, SP2: 9096,3443	Source IP	HTTPS (GET)
VIP 15	XE_Standalone	L7 SNAT	8443,9449	Source IP	HTTPS (GET)
VIP 16	CCG_IB_2101	L7 SNAT	2101	Last Successful	Connect to port
VIP 17	CCG_IB_2102	L7 SNAT	2102	Last Successful	Connect to port
VIP 18	PORT_CCG_IB_2103	L7 SNAT	2103	Last Successful	Connect to port
VIP 19	PORT_CCG_IB_2104	L7 SNAT	2104	Last Successful	Connect to port

4.2. SSL Termination

SSL Termination is configured on the load balancer for the following VIPs:

- VIP 12 - **Dakota**
- VIP 13 - **WFM_Play_Group**

This provides a corresponding HTTPS Virtual Service for the VIP. Certificates in PEM or PFX format can be uploaded to the load balancer.

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)

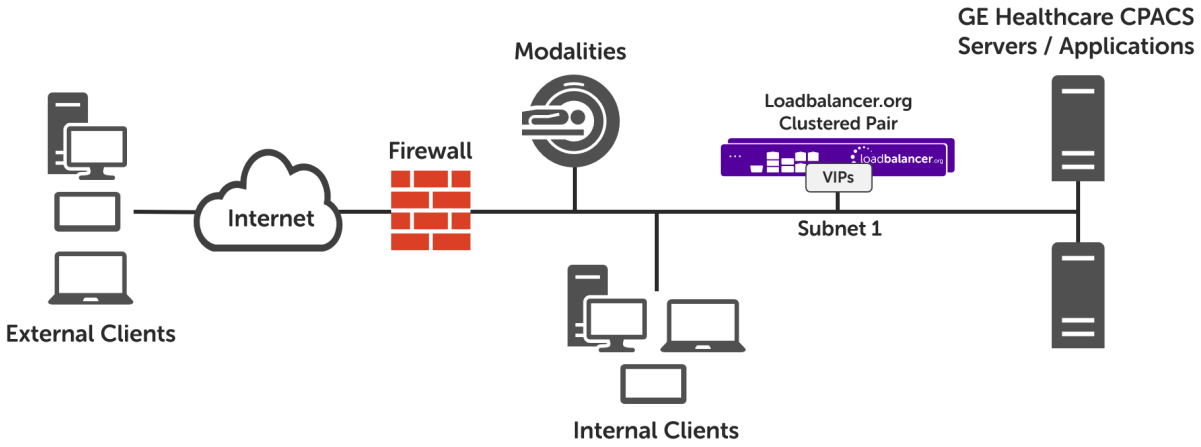
> **Note** The ports used for SSH, GSLB, SNMP, the WebUI, the fallback page, the gateway service and the shuttle service can be changed if required. For more information, please refer to Service Socket Addresses.

6. Deployment Concept

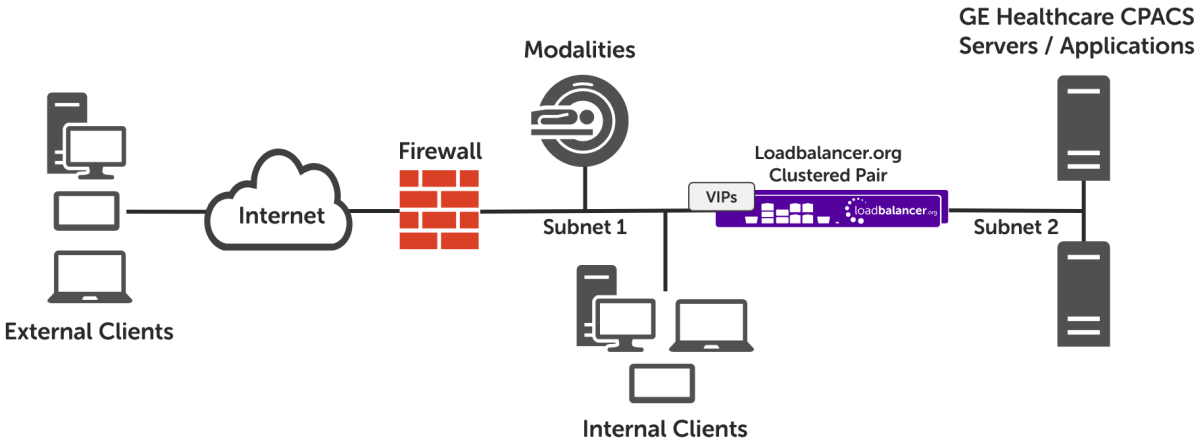
The load balancer can be deployed in either non-routed (single interface) mode or routed (dual interface) mode.

> **Note** Non-routed mode is used for the configuration presented in this guide.

6.1. Non-Routed / Single-arm Mode



6.2. Routed / Two-arm Mode



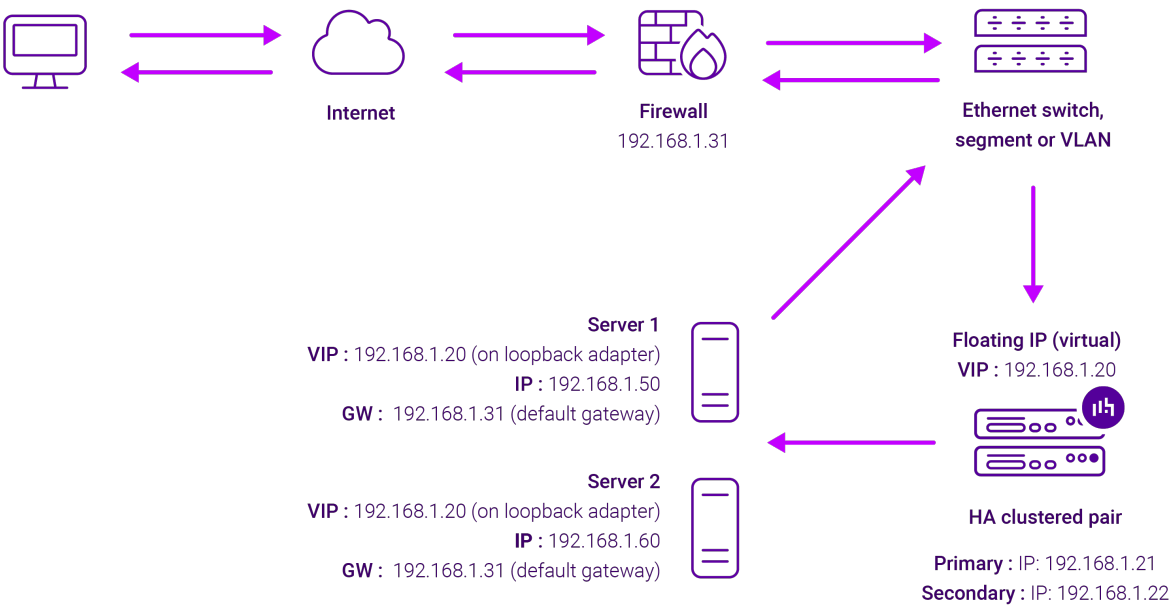
7. Load Balancer Deployment Methods

For Centricity PACS, both layer 4 DR mode and layer 7 SNAT mode are used. These modes are described below and are used for the configurations presented in this guide.

7.1. 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.

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



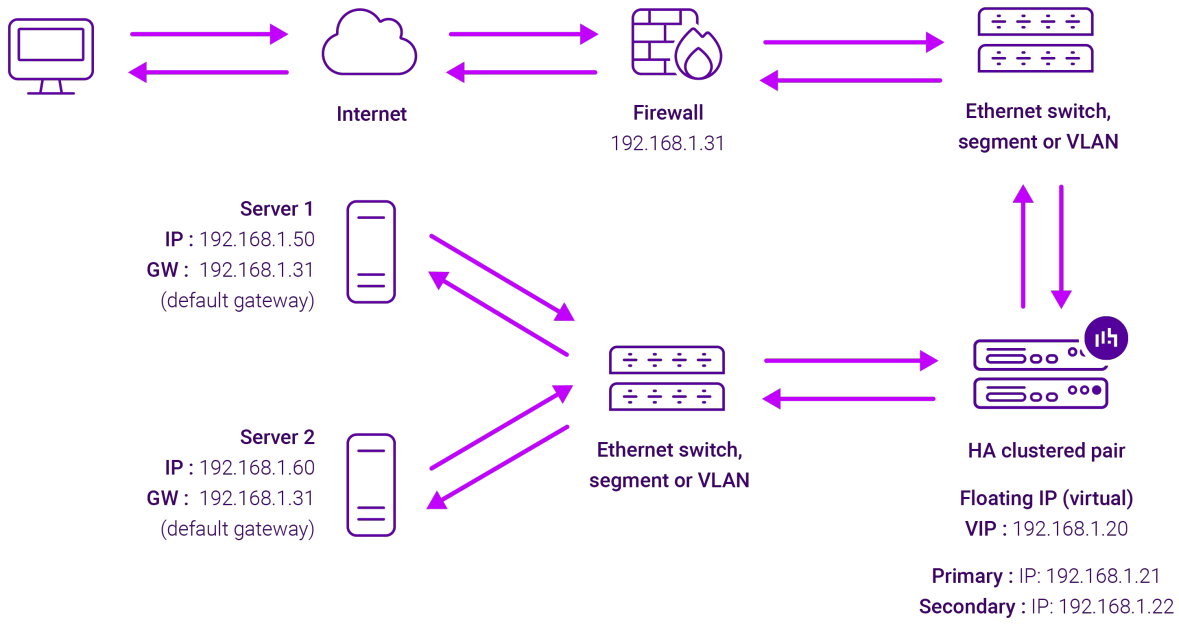
- DR mode works by changing the destination MAC address of the incoming packet to match the selected Real Server on the fly which is very fast.
- When the packet reaches the Real Server it expects the Real Server to own the Virtual Services IP address (VIP). This means that each Real Server (and the 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.

> **Note** For additional information on how the MAC address is modified in relation to the traffic flow between the load balancer, the load balanced backend servers and the Modality, please refer DR Mode Packet Manipulation in the appendix.

7.2. 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.

8. Configuring Centricity PACS for Load Balancing

8.1. Layer 7 SNAT Mode

Layer 7 SNAT mode VIPs do not require any mode specific configuration changes to the load balanced Real Servers (Centricity PACS Servers).

8.2. Layer 4 DR Mode

Layer 4 DR mode VIPs require the "ARP problem" to be solved on each load balanced Real Server (Centricity PACS Server). This enables DR mode to work correctly.

The "ARP problem" must be solved on each Real Server associated with the following VIPs:

- VIP 1 - **EA_XDS_Service**
- VIP 2 - **EA_Dicom_Service**
- VIP 3 - **EA_Secure_Dicom_Service**
- VIP 4 - **EA_HL7_Service**
- VIP 5 - **EA_Secure_HL7_Service**
- VIP 6 - **EA_Study_Management_Service**
- VIP 9 - **DAS_Pool**

Detailed steps on solving the "ARP problem" for Linux and Windows 2012 & later are presented below.

8.2.1. Solving the ARP Problem for Linux

There are two different approaches on how to configure a Linux server for correct operation when DR mode load balancing is in use:

- Modifying the server's ARP behavior and adding the relevant VIP addresses to the loopback interface
- Using NAT to convince the server to accept and reply to packets addressed to the relevant VIP addresses

Four independent methods are described below along with instructions. Each method follows one of the two approaches above. The specific method chosen will depend on technical requirements, the Linux distribution in use, and personal preferences.

The first method involves setting kernel parameters to alter the server's ARP behavior and adding IP addresses to the loopback interface. This method should be universally applicable to any Linux server **making this the preferred method**.

If setting kernel parameters and adding IP addresses is not possible for some reason, the remaining three methods describe setting up a server for DR mode operation by using NAT via the **redirect** target/statement. The specific instructions depend on the packet filtering framework and tooling in use, which varies between Linux distributions. Methods are presented for iptables, nftables, and the `firewall-cmd` tool.

8.2.1.1. Method 1: ARP Behavior and Loopback Interface Changes

This is the preferred method as it should be applicable to any Linux server and doesn't require any additional packet filtering or NAT considerations.

Each real server needs the loopback interface to be configured with the virtual IP addresses (VIPs) of the relevant load balanced services. This is often just a single VIP address, but the logic described below can be extended to cover multiple VIPs on a server. Having the VIPs on the loopback interface allows the server to accept inbound load balanced packets that are addressed to a VIP.

The server **must not** respond to ARP requests for the VIP addresses. The server also **must not** use ARP to announce the fact that it owns the VIP addresses. This is necessary to prevent IP address conflicts, as ***all*** of the real servers ***and*** the load balancer will own the VIP addresses. Only the load balancer should announce ownership of the VIPs.

To configure the behavior described above, follow all of the steps below on each real server.

Step 1 of 4: Re-configuring ARP behavior

This step is only applicable if IPv4-based virtual services are in use.

Add the following lines to the file `/etc/sysctl.conf` (create this file if it does not already exist):

```
net.ipv4.conf.all.arp_ignore=1
net.ipv4.conf.eth0.arp_ignore=1
net.ipv4.conf.eth1.arp_ignore=1
net.ipv4.conf.all.arp_announce=2
net.ipv4.conf.eth0.arp_announce=2
net.ipv4.conf.eth1.arp_announce=2
```

Adjust the commands shown above to suit the server's network configuration, e.g. a different number of network interfaces or a different interface naming convention.

> **Note**
>
> For Linux distros such as Debian 12+, Ubuntu 24.10+ and OpenSUSE that are using systemd and are running systemd-sysctl, `/usr/lib/sysctl.d/50-default.conf` should be modified rather than `/etc/sysctl.conf`.

> **Note**
>
> For reference, the effect of these kernel parameter changes on the server is as follows:
>
> - `arp_ignore=1`: This configures the server to only reply to an ARP request if the request's target IP address is local to the incoming interface. This can never be true for VIP addresses on the loopback interface, as the loopback interface can never be an incoming interface for ARP requests from other devices. Hence, ARP requests for VIP addresses are always ignored.
> - `arp_announce=2`: This prevents the server from sending an ARP request out of an interface ***A*** where the ARP request's sender/source address is stated to be an IP address that is local to some other interface ***B***. For example, this prevents the server from sending an ARP request ***from*** a VIP address (which is local to the loopback interface) out of `eth0`, which would announce that the server owns the VIP address.

Step 2 of 4: Re-configuring duplicate address detection (DAD) behavior

This step is only applicable if IPv6-based virtual services are in use.

Add the following lines to the file `/etc/sysctl.conf` (create this file if it does not already exist):

```
net.ipv6.conf.lo.dad_transmits=0
```

```
net.ipv6.conf.lo.accept_dad=0
```

> **Note**
>
> For Linux distros such as Debian 12+, Ubuntu 24.10+ and OpenSUSE that are using systemd and are running systemd-sysctl, `/usr/lib/sysctl.d/50-default.conf` should be modified rather than `/etc/sysctl.conf`.

> **Note**
>
> For reference, the effect of these kernel parameter changes on the server is as follows:
>
> - `dad_transmits=0`: This prevents a given interface from sending out duplicate address detection probes in order to test the uniqueness of unicast IPv6 addresses. Any IPv6 VIP addresses will *not* be unique, so this mechanism is disabled.
> - `accept_dad=0`: This prevents a given interface from accepting duplicate address detection messages. This prevents any IPv6 VIP addresses from being marked as duplicate addresses.

Step 3 of 4: Applying the new settings

To apply the new settings, either reboot the real server or execute the following command to immediately apply the changes:

```
/sbin/sysctl -p
```

> **Note**
>
> Steps 1, 2, and 3 can be replaced by instead modifying the necessary kernel variables by writing directly to their corresponding files under `/proc/sys/`. Note that changes made in this way ***will not persist across reboots***.
>
> Execute the following commands (as root) to implement these temporary changes (adapting the number of interfaces and interface names as needed):
>
> ```
> echo 1 > /proc/sys/net/ipv4/conf/all/arp_ignore
> echo 1 > /proc/sys/net/ipv4/conf/eth0/arp_ignore
> echo 1 > /proc/sys/net/ipv4/conf/eth1/arp_ignore
> echo 2 > /proc/sys/net/ipv4/conf/all/arp_announce
> echo 2 > /proc/sys/net/ipv4/conf/eth0/arp_announce
> echo 2 > /proc/sys/net/ipv4/conf/eth1/arp_announce
> echo 0 > /proc/sys/net/ipv6/conf/lo/dad_transmits
> echo 0 > /proc/sys/net/ipv6/conf/lo/accept_dad
> ```

Step 4 of 4: Adding the virtual IP addresses (VIPs) to the loopback interface

Each of the VIP addresses must be permanently added to the loopback interface. VIPs must be added with a network prefix of /32 for IPv4 addresses or /128 for IPv6 addresses. The IP addresses can be added using the usual configuration files and tools for modifying network interfaces, which vary between different Linux distributions.

As an alternative, the `ip` command can be used as a universal way to add IP addresses to any Linux server. Note that addresses added in this way ***will not persist across reboots***. To make these addresses permanent, add the

`ip` commands to an appropriate startup script such as `/etc/rc.local`.

Execute the following `ip` command for each IPv4 VIP:

```
ip addr add dev lo <IPv4-VIP>/32
```

Execute the following `ip` command for each IPv6 VIP:

```
ip addr add dev lo <IPv6-VIP>/128
```

To check that the VIPs have been successfully added, execute the command:

```
ip addr ls
```

To remove an IPv4 VIP from the loopback adapter, execute the command:

```
ip addr del dev lo <IPv4-VIP>/32
```

To remove an IPv6 VIP from the loopback adapter, execute the command:

```
ip addr del dev lo <IPv6-VIP>/128
```

8.2.1.2. Method 2: NAT "redirect" via iptables

iptables can be used on each real server to identify incoming packets that are addressed to a virtual IP address (VIP) and redirect those packets to the server itself. This is achieved using the **REDIRECT** target in iptables, which performs the necessary NAT to make this possible. This allows a real server to accept packets addressed to a VIP without the server owning the VIP.

Execute the following command to put the necessary iptables rule in place to redirect traffic for a single IPv4 VIP address. Note that iptables rules added in this way ***will not persist across reboots***. To make such a rule permanent, either add the rule to an iptables firewall script, if one is provided with the Linux distribution in question, or add the command to an appropriate startup script such as `/etc/rc.local` on each real server.

```
iptables -t nat -A PREROUTING -d <IPv4-VIP> -j REDIRECT
```

The VIP address should be changed to match the virtual service in question, for example:

```
iptables -t nat -A PREROUTING -d 10.0.0.21 -j REDIRECT
```

The example above will redirect any incoming packets destined for 10.0.0.21 (the virtual service) locally, i.e. to the primary address of the incoming interface on the real server.

If a real server is responsible for serving ***multiple*** VIPs then additional iptables rules should be added to cover each VIP.

For an IPv6 VIP address, a command like the following should be used:

```
ip6tables -t nat -A PREROUTING -d <IPv6-VIP> -j REDIRECT
```

The VIP address should be changed to match the virtual service in question, for example:

```
ip6tables -t nat -A PREROUTING -d 2001:db8::10 -j REDIRECT
```

> **Note** Method 2 may not be appropriate when using IP-based virtual hosting on a web server. This is because an iptables **REDIRECT** rule will redirect incoming packets to the ***primary address*** of the incoming interface on the web server rather than any of the virtual hosts that are configured. Where this is an issue, use method 1 instead.

8.2.1.3. Method 3: NAT "redirect" via nftables

nftables is the modern Linux kernel packet filtering framework. It is supported on all major Linux distributions and has replaced iptables as the default framework on most major distributions.

nftables can be used on each real server to identify incoming packets that are addressed to a virtual IP address (VIP) and redirect those packets to the server itself. This is achieved using the **redirect** statement in nftables, which performs the necessary NAT to make this possible. This allows a real server to accept packets addressed to a VIP without the server owning the VIP.

Use a script like the following to put the necessary nftables structures in place to redirect traffic for both IPv4 and IPv6 VIP addresses. To make such a configuration permanent, either add the `inet nat` table to an nftables firewall script, if one is provided with the Linux distribution in question, or configure a script like the following to execute as a startup script on each real server.

```
#!/usr/sbin/nft -f

table inet nat {
    chain prerouting {
        comment "Allow server to accept packets destined for VIP addresses";
        type nat hook prerouting priority -100; policy accept;
        ip daddr <IPv4-VIP> redirect comment "Description"
        ip6 daddr <IPv6-VIP> redirect comment "Description"
    }
}
```

The VIP addresses and comments should be changed to match the virtual services in question, for example:

```
#!/usr/sbin/nft -f

table inet nat {
    chain prerouting {
```

```
        comment "Allow server to accept packets destined for VIP addresses";
        type nat hook prerouting priority -100; policy accept;
        ip daddr 10.0.0.21 redirect comment "VIP 1: HTTP"
        ip6 daddr 2001:db8::10 redirect comment "VIP 2: HTTPS"
    }
}
```

The example above will redirect any incoming packets destined for 10.0.0.21 or 2001:db8::10 (the virtual services) locally, i.e. to the primary address of the incoming interface (for each IP version) on the real server.

Note that **Linux kernels prior to 5.2** may not support performing NAT (which is required for the **redirect** statement) in an inet family table. In this scenario, use either an ip or an ip6 family table instead, or both if a mixture of IPv4 and IPv6 VIPs are in use on the same server. Also note that older kernels may not support the use of comments in chains.

Note that **Linux kernels prior to 4.18** require explicitly registering both prerouting and postrouting chains in order for the implicit NAT of the **redirect** statement to be correctly performed in both the inbound and outbound directions.

A legacy-friendly setup may look like the following:

```
#!/usr/sbin/nft -f

table ip nat {
    chain prerouting {
        type nat hook prerouting priority -100; policy accept;
        ip daddr 10.0.0.21 counter redirect comment "VIP 1: HTTP"
    }

    chain postrouting {
        type nat hook postrouting priority 100; policy accept;
    }
}

table ip6 nat {
    chain prerouting {
        type nat hook prerouting priority -100; policy accept;
        ip6 daddr 2001:db8::10 counter redirect comment "VIP 2: HTTPS"
    }

    chain postrouting {
        type nat hook postrouting priority 100; policy accept;
    }
}
```

> **Note**
>
> Method 3 may not be appropriate when using IP-based virtual hosting on a web server. This is because an nftables **redirect** statement will redirect incoming packets to the *primary address* of the incoming interface on the web server rather than any of the virtual hosts that are configured. Where this is an issue, use method 1 instead.

8.2.1.4. Method 4: NAT "redirect" via firewall-cmd

Some recent versions of Linux distributions make use of firewalld as a high-level firewall configuration framework. In this case, while it may actually be iptables performing the work at a lower level, it may be preferred to implement the iptables NAT solution described in method 2 in firewalld, as opposed to directly manipulating iptables. This is achieved by using the `firewall-cmd` tool provided by firewalld and executing a command like the following on each real server:

```
firewall-cmd --permanent --direct --add-rule ipv4 nat PREROUTING 0 -d <IPv4-VIP> -j REDIRECT
```

The VIP address should be changed to match the virtual service in question, for example:

```
firewall-cmd --permanent --direct --add-rule ipv4 nat PREROUTING 0 -d 10.0.0.50 -j REDIRECT
```

To apply the new configuration, reload the firewall rules like so:

```
firewall-cmd --reload
```

Configuration applied in this way will be permanent and will persist across reboots.

> **Note** Method 4 may not be appropriate when using IP-based virtual hosting on a web server. This is because an iptables **REDIRECT** rule will redirect incoming packets to the ***primary address*** of the incoming interface on the web server rather than any of the virtual hosts that are configured. Where this is an issue, use method 1 instead.

8.2.2. Windows Server 2012 & Later

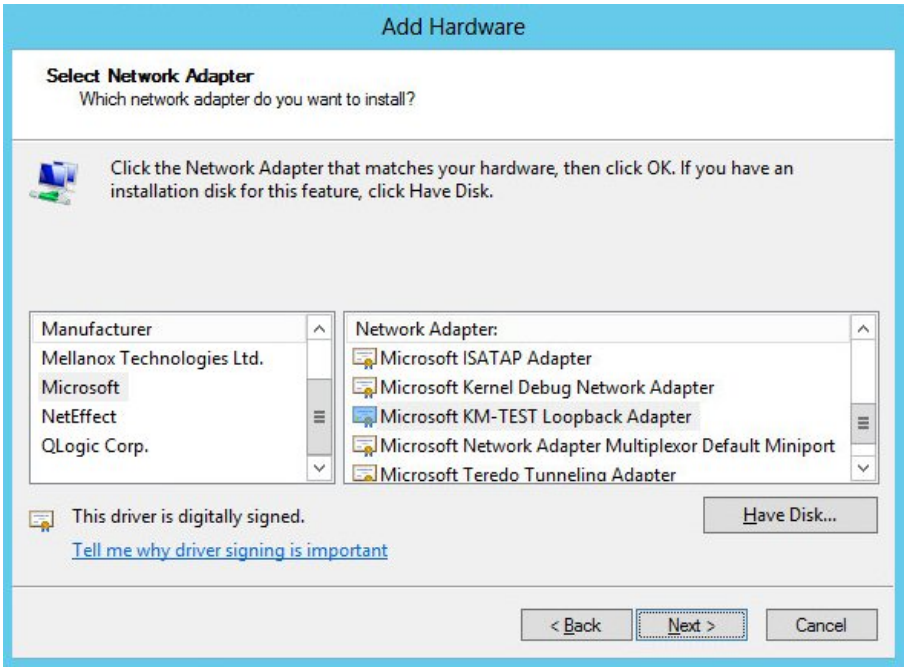
Windows Server 2012 and later support Direct Routing (DR) mode through the use of the Microsoft Loopback Adapter that must be installed and configured on each load balanced (Real) Server. The IP address configured on the Loopback Adapter must be the same as the Virtual Service (VIP) address. This enables 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.

8.2.2.1. Step 1 of 3: Install the Microsoft Loopback Adapter

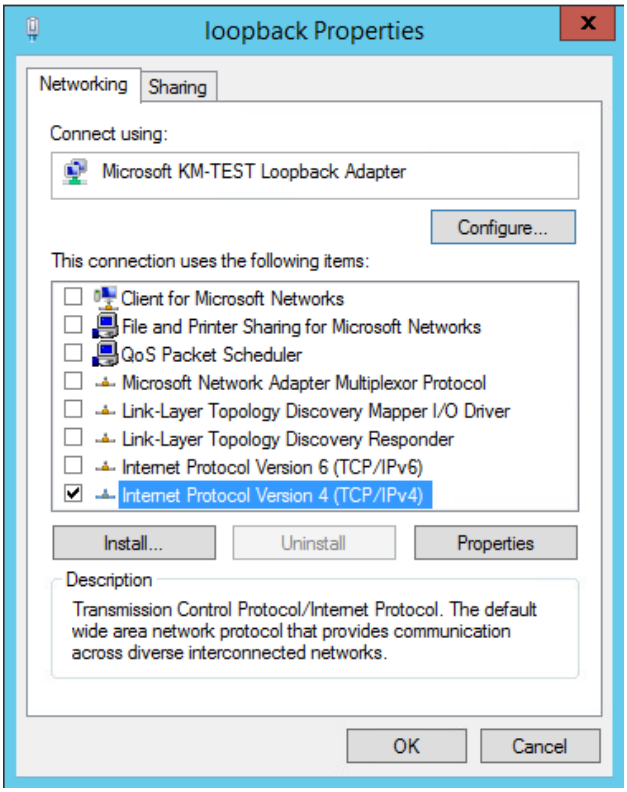
1. Click **Start**, then run **hdwwiz** to start the Hardware Installation Wizard.
2. Once the Wizard has started, click **Next**.
3. Select **Install the hardware that I manually select from a list (Advanced)**, click **Next**.
4. Select **Network adapters**, click **Next**.



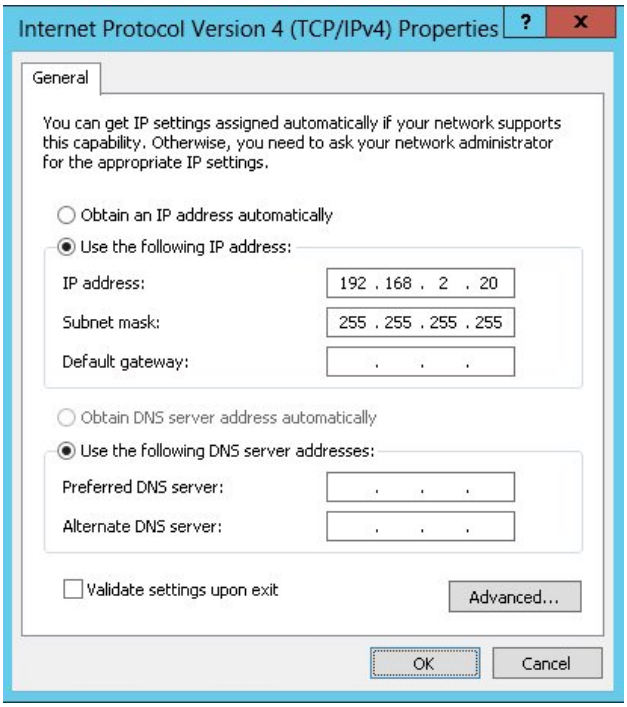
5. Select **Microsoft** & **Microsoft KM-Test Loopback Adapter**, click **Next**.
6. Click **Next** to start the installation, when complete click **Finish**.

8.2.2.2. 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**.
4. Uncheck all items except **Internet Protocol Version 4 (TCP/IPv4)** as shown below:



5. 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.

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

8.2.2.3. 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:

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

Option 2 - Using PowerShell Cmdlets

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

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

9. Appliance Installation & Configuration for Centricity PACS

9.1. Overview

For Centricity PACS deployments, 2 load balancer appliances must be installed and configured and then paired to create an active/passive HA clustered pair.

The following is an overview of the installation and configuration process:

1. Deploy 2 Virtual Appliances - refer to Section 9.2
2. Configure the management IP address and other network settings on **both** appliances - refer to Section 9.3
3. Run a software update check on **both** appliances - refer to Section 9.5
4. Configure the appliance security mode on **both** appliances - refer to Section 9.6
5. Verify network connections and configure any additional settings on **both** appliances - refer to Section 9.7
6. Configure the required load balanced services on the **Primary** appliance - refer to Section 9.8
7. Restart services on the **Primary** appliance - refer to Section 9.8.22
8. Verify that everything is working as expected on the **Primary** appliance - refer to Section 10
9. Configure the HA Pair on the **Primary** appliance - this will replicate all load balanced services to the Secondary appliance, once configured the Secondary appliance will be kept in-sync automatically - refer to Section 11

10. Configure any required optional settings on **both** appliances - refer to Section 12

9.2. Virtual Appliance Installation

9.2.1. Download & Extract the Appliance

1. Download the Virtual Appliance.
2. Unzip the contents of the file to your chosen location.

9.2.2. Virtual Hardware Resource Requirements

The resource requirements depend on the particular virtual appliance used. The following GE HealthCare VAs are available:

- **v1000** - 2 vCPUs, 4GB RAM, 20GB Drive
- **v4000** - 4 vCPUs, 8GB RAM, 20GB Drive
- **vUltimate** - 8 vCPUs, 16GB RAM, 20GB Drive

Please refer to the technical documentation for the site to determine which appliance to use and obtain the download link.

9.2.3. VMware vSphere Client

The steps below apply to VMware ESX/ESXi & vSphere Client v6.7 and later.

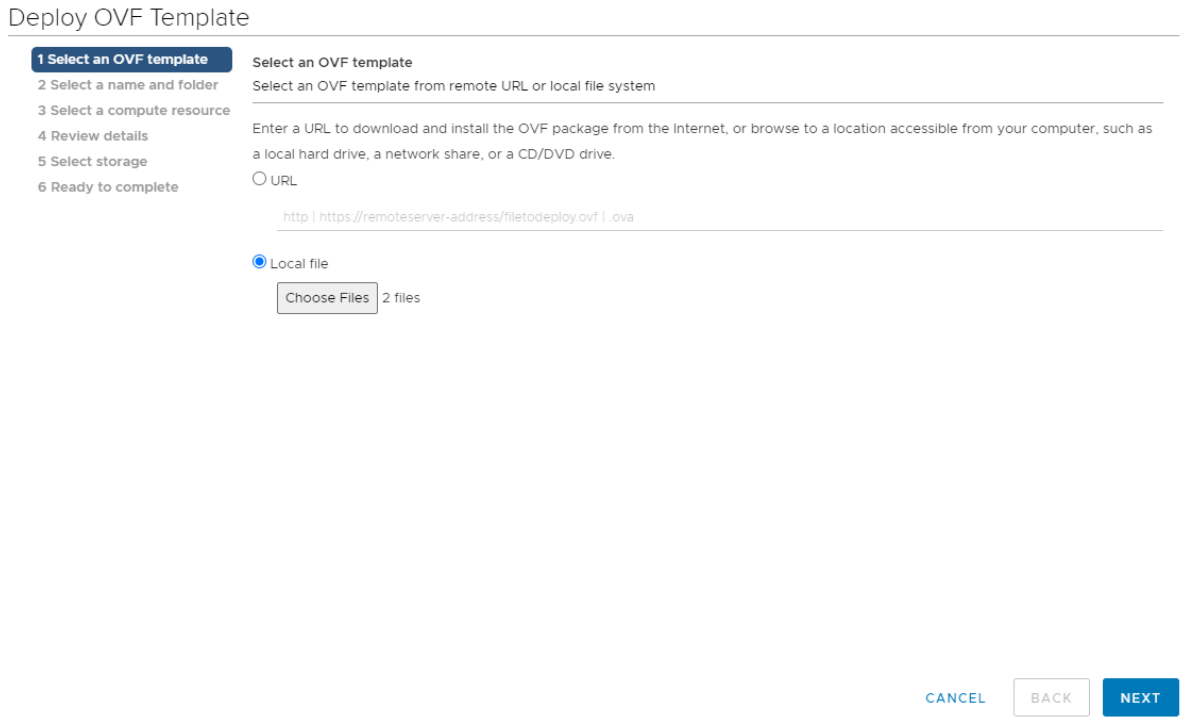
9.2.3.1. Upgrading to the latest Hardware Version

When the appliance is deployed, the virtual hardware version is set to 11. This enables compatibility with ESX version 6.0 and later. You can upgrade to a later hardware version if required.

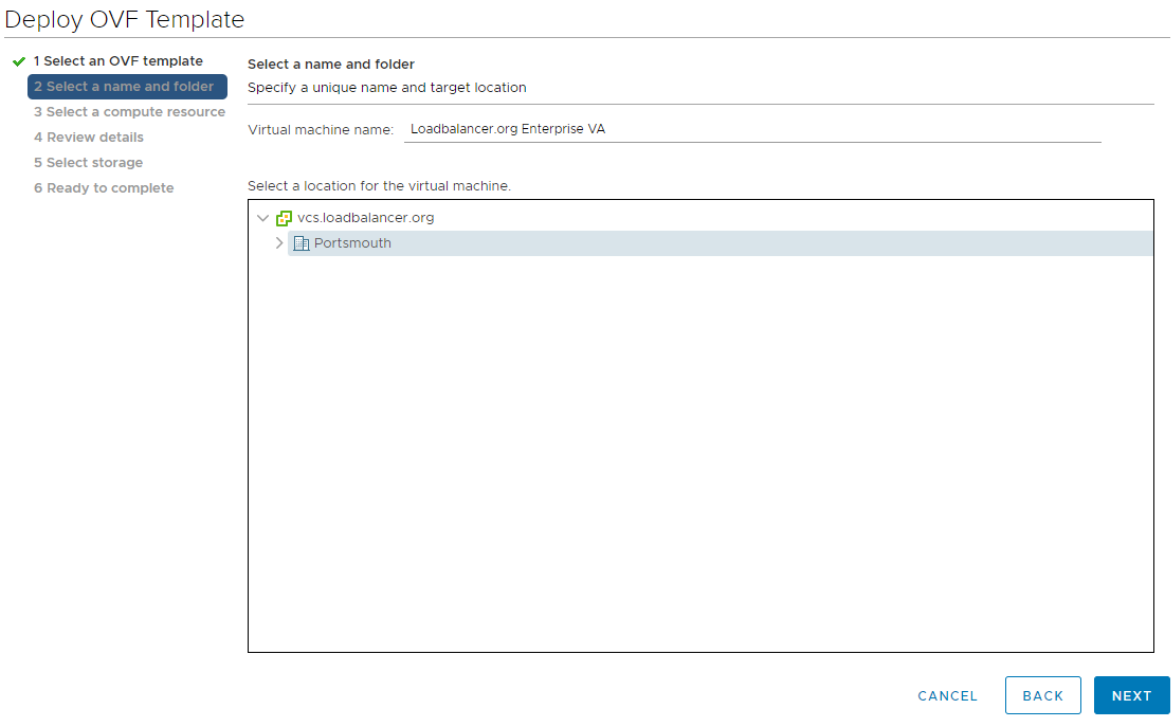
> **Note** Create a snapshot or backup of the virtual machine first before upgrading.

9.2.3.2. Installing the Appliance using vSphere Client

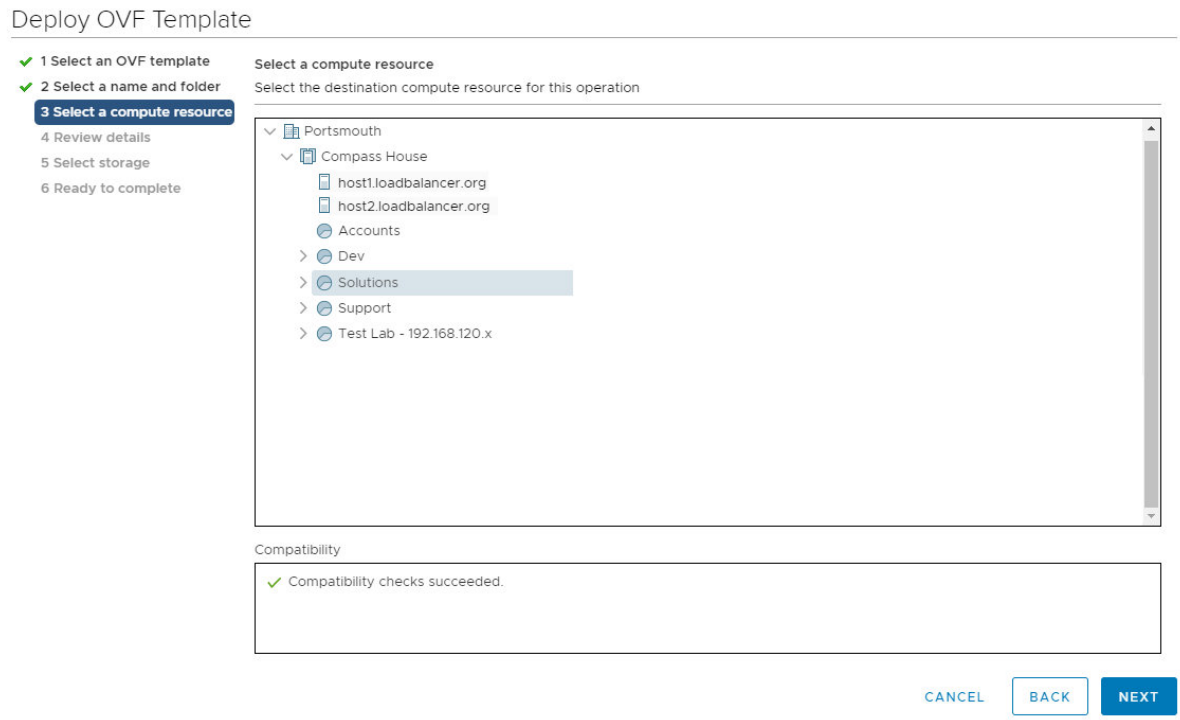
1. Right-click the inventory object where the appliance is to be located and select **Deploy OVF Template**.
2. In the **Select an OVF Template** screen, select the **Local File** option, click **Browse**, navigate to the download location, select the **.ova** file and click **Next**.



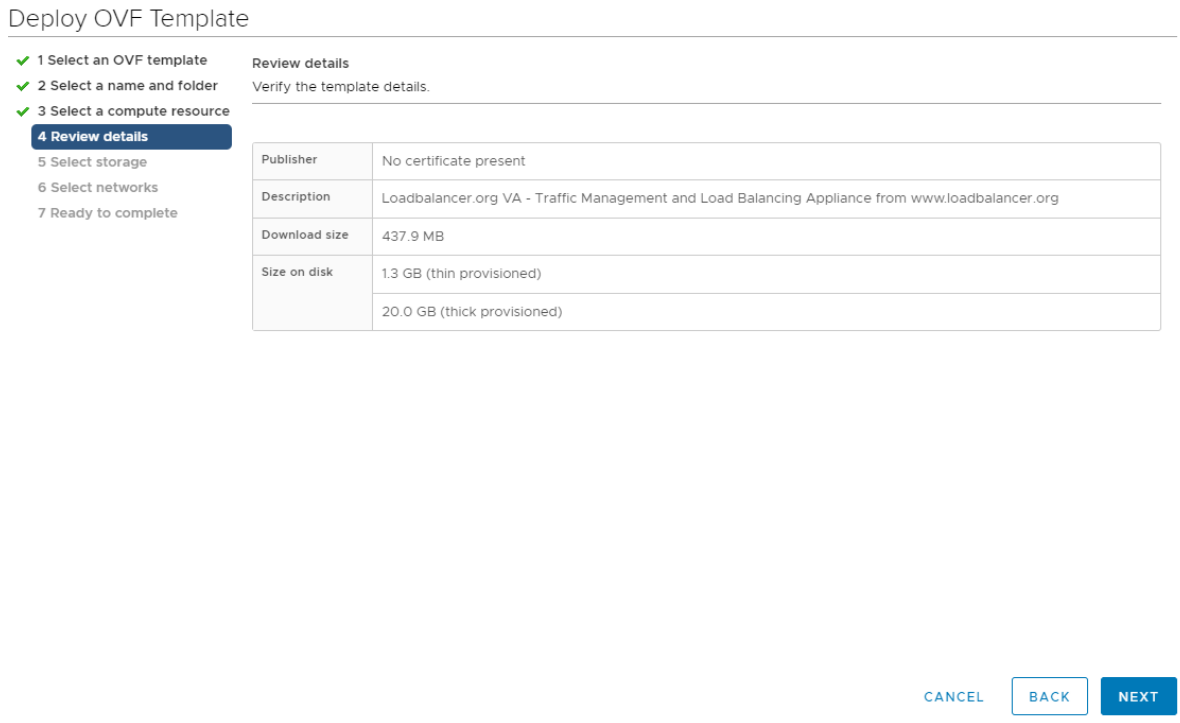
3. In the **Select a name and folder** screen, type a suitable name for the appliance - this can be up to 80 characters in length.
4. Select the required location for the appliance - by default this will be the location of the inventory object from where the wizard was started and click **Next**.



5. In the **Select a compute resource** screen, select the required compute resource for the appliance - by default this will be the inventory object from where the wizard was started and click **Next**.

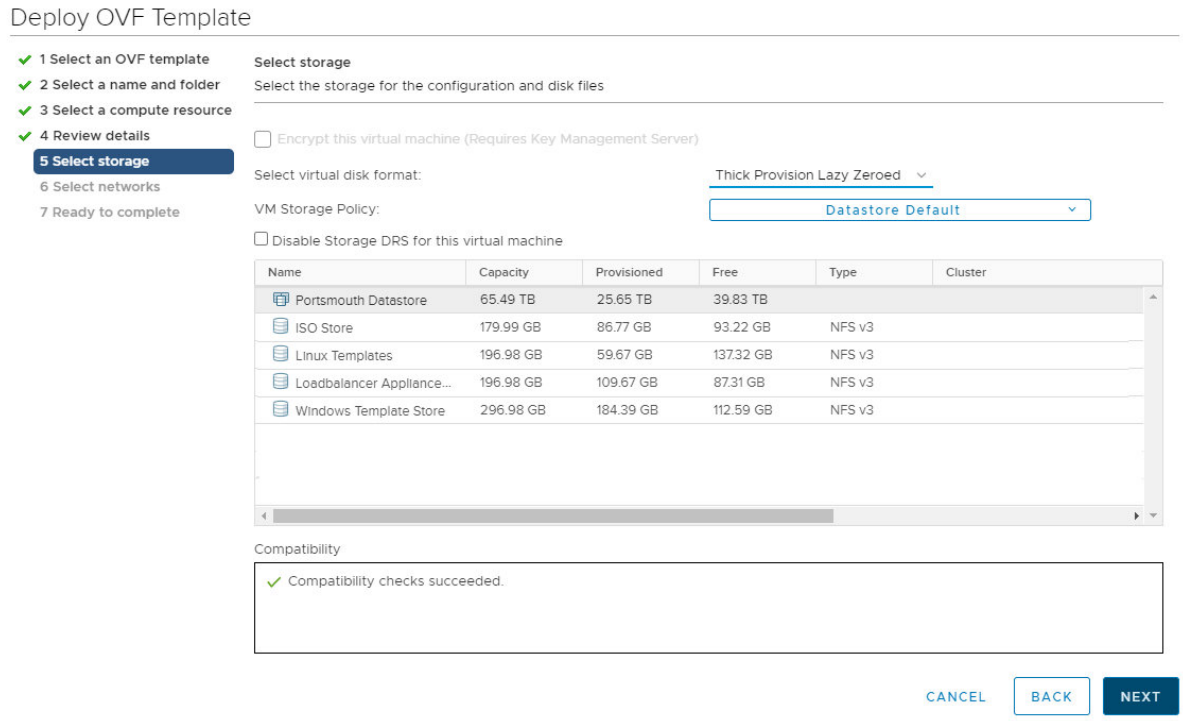


6. In the **Review details** screen, verify the template details and click **Next**.

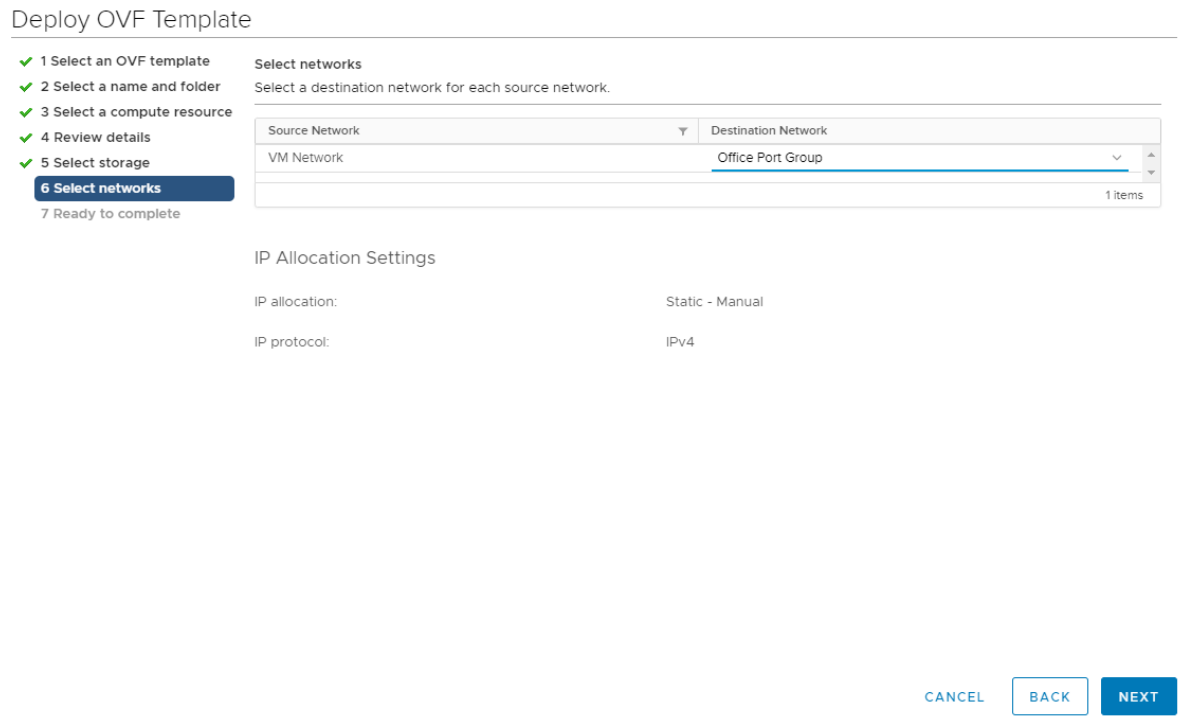


7. In the **Select Storage** screen, first select the required storage location for the appliance.
8. Now select the required disk format and click **Next**.

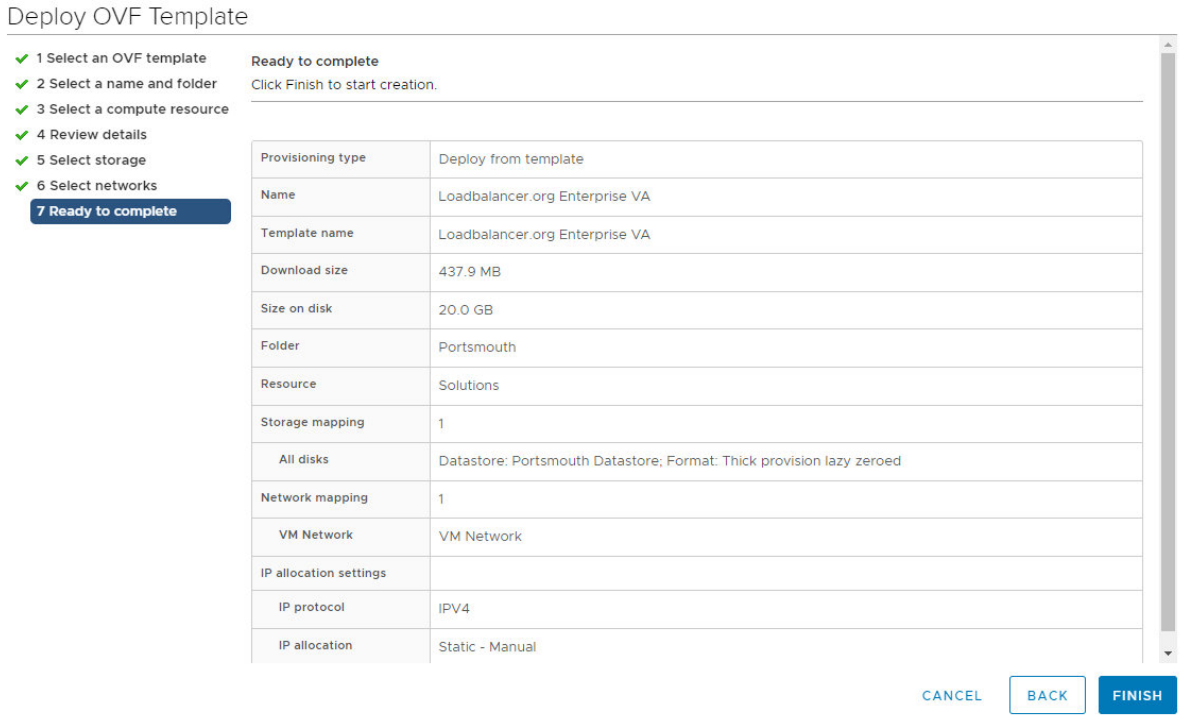
> **Note** Loadbalancer.org recommends selecting a thick provision format. By default the appliance disk is 20GB.



9. In the **Select Networks** screen, select the required destination network using the drop-down next to **VM Network** and click **Next**.



10. In the **Ready to complete** screen, review the settings and click **Finish** to create the virtual appliance. To change a setting, use the **Back** button to navigate back through the screens as required.



9.2.3.3. Configure Network Adapters

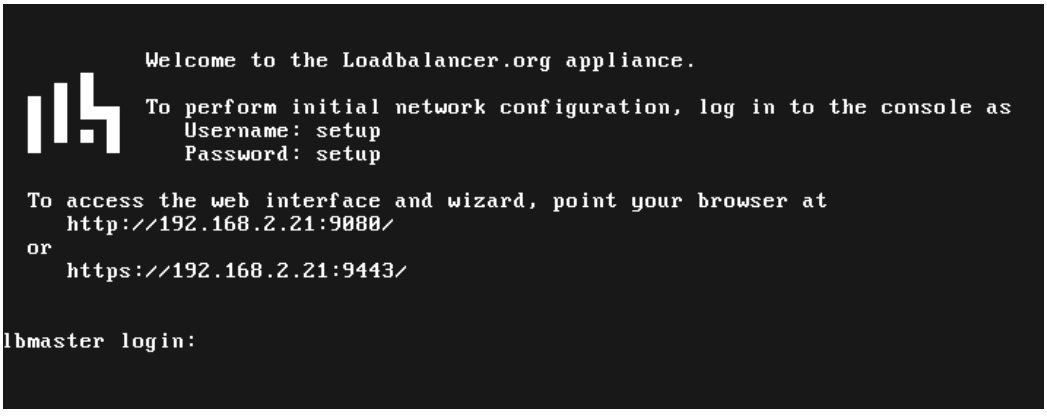
The appliance has 4 network adapters. By default only the first adapter is connected which is the requirement for GE HealthCare deployments. This will be **eth0** when viewed in the appliance WebUI.

9.2.3.4. Start the Appliance

Now power up the appliance.

9.3. Configuring Initial Network Settings

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



As mentioned in the text, to perform initial network configuration, login as the "setup" user at the appliance console.

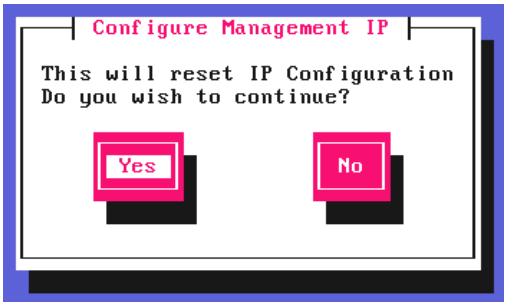
Once logged in, the Network Setup Wizard will start automatically. This will enable you to configure the management IP address and other network settings for the appliance.

login to the console:

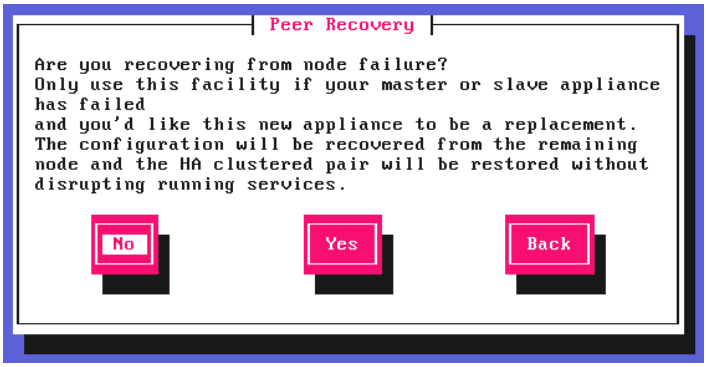
Username: setup
Password: setup

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

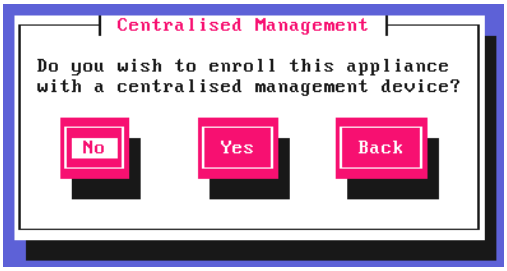
In the **Configure Management IP** screen, leave **Yes** selected and hit **Enter** to continue.



In the **Peer Recovery** screen, leave **No** selected and hit **Enter** to continue.

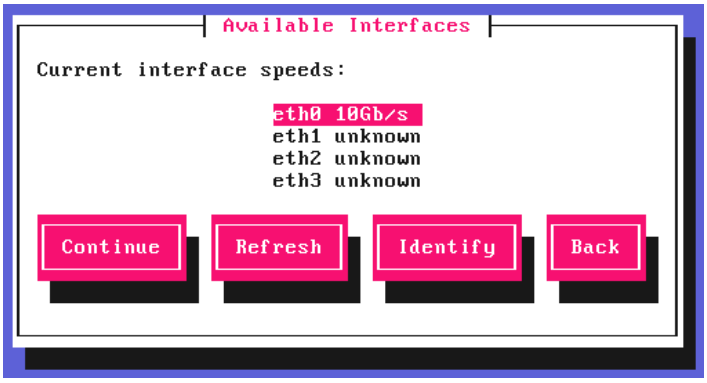


In the **Centralized Management** screen, if you have been provided with Management Server details select **Yes**, otherwise leave **No** selected, then hit **Enter** to continue.

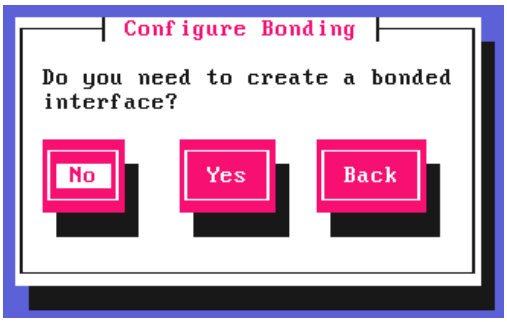


> **Note** For information on how to modify Centralized Management settings via the WebUI, please refer to Portal Management & Appliance Adoption.

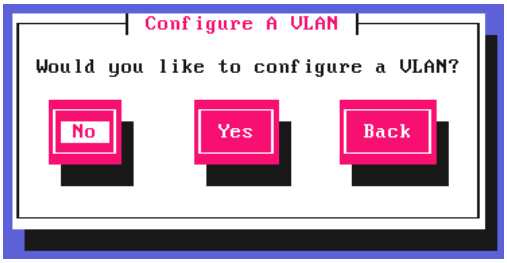
In the **Available Interfaces** screen, a list of available interfaces will be displayed, hit **Enter** to continue.



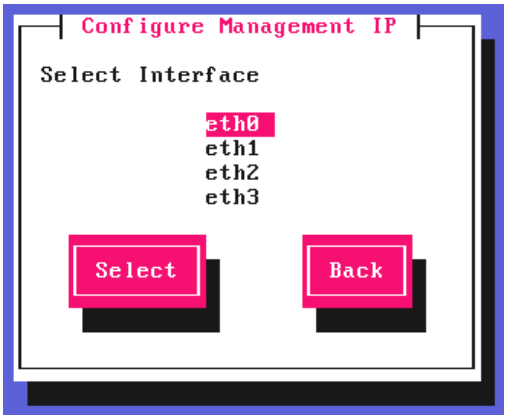
In the **Configure Bonding** screen, leave **No** selected, then hit **Enter** to continue.



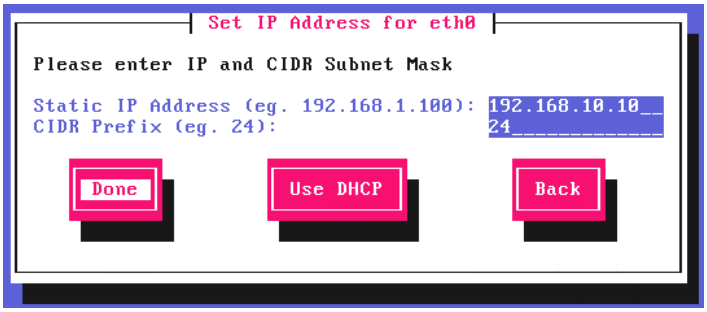
In the **Configure a VLAN** screen, leave **No** selected, then hit **Enter** to continue.



In the **Configure Management IP** screen, select **eth0** and hit **Enter** to continue.

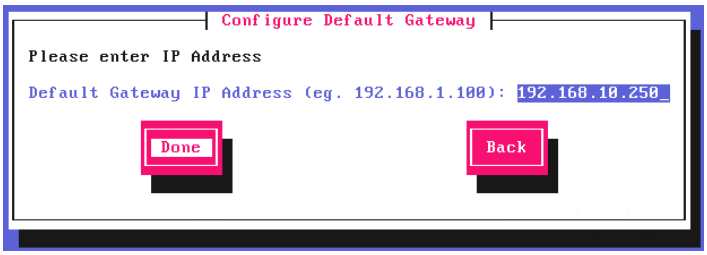


In the **Set IP address** screen, specify the required management address in the *Static IP Address* & *CIDR Prefix* fields, select **Done** and hit **Enter** to continue.

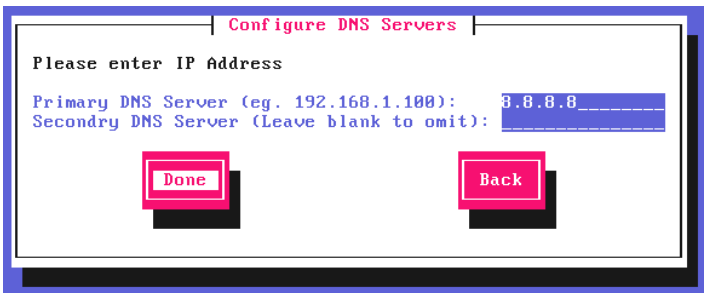


> **Note** A subnet mask such as 255.255.255.0 is not valid, in this case enter 24 instead.

In the **Configure Default Gateway** screen, enter the required *Default Gateway IP Address*, select **Done** and hit **Enter** to continue.

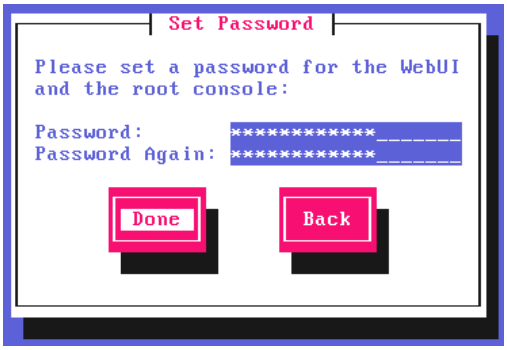


In the **Configure DNS Servers** screen, configure the required DNS server(s), select **Done** and hit **Enter** to continue.

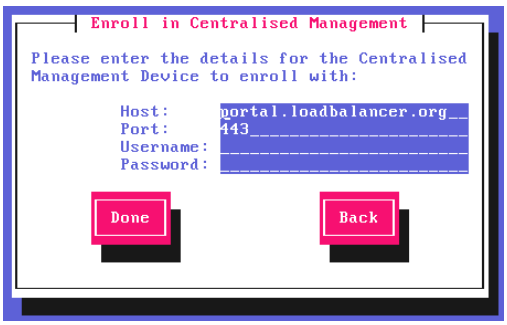


In the **Set Password** screen, hit **Enter** to continue.

Enter the *Password* you'd like to use for the **loadbalancer** WebUI user account and the **root** Linux user account. Repeat the password, select **Done** and hit **Enter** to continue.

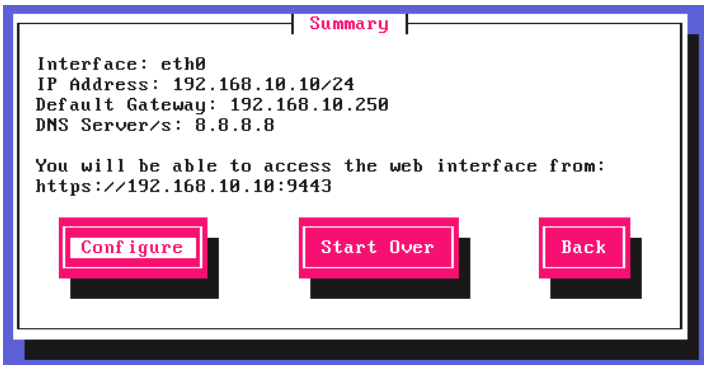


If you selected **Yes** when asked if you want to enroll for Centralized Management, you'll now be prompted for the details. Default values for the *Host* and *Port* are set and can be changed if required. Enter the *Username* and *Password* for the management server account you'd like the appliance to be associated with, select **Done** and hit **Enter** to continue.

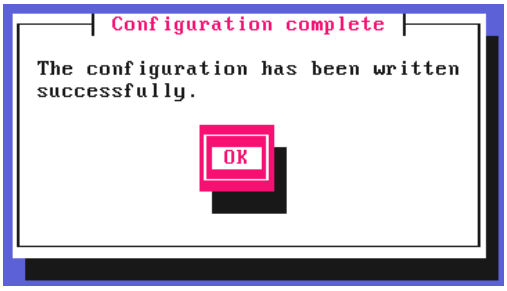


In the **Summary** screen, check all settings. If everything is correct, leave **Configure** selected and hit **Enter** to continue. All settings will be applied. If you need to change a setting, use the **Back** button.

> **Note** For v8.13.2 and later, once the settings have been applied the appliance will check if a software update is available. If an update is found, it will be installed automatically.



Once the configuration has been written, the **Configuration Complete** screen and message will be displayed. Click **OK** to exit the wizard and return to the command prompt.



9.4. 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.

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.

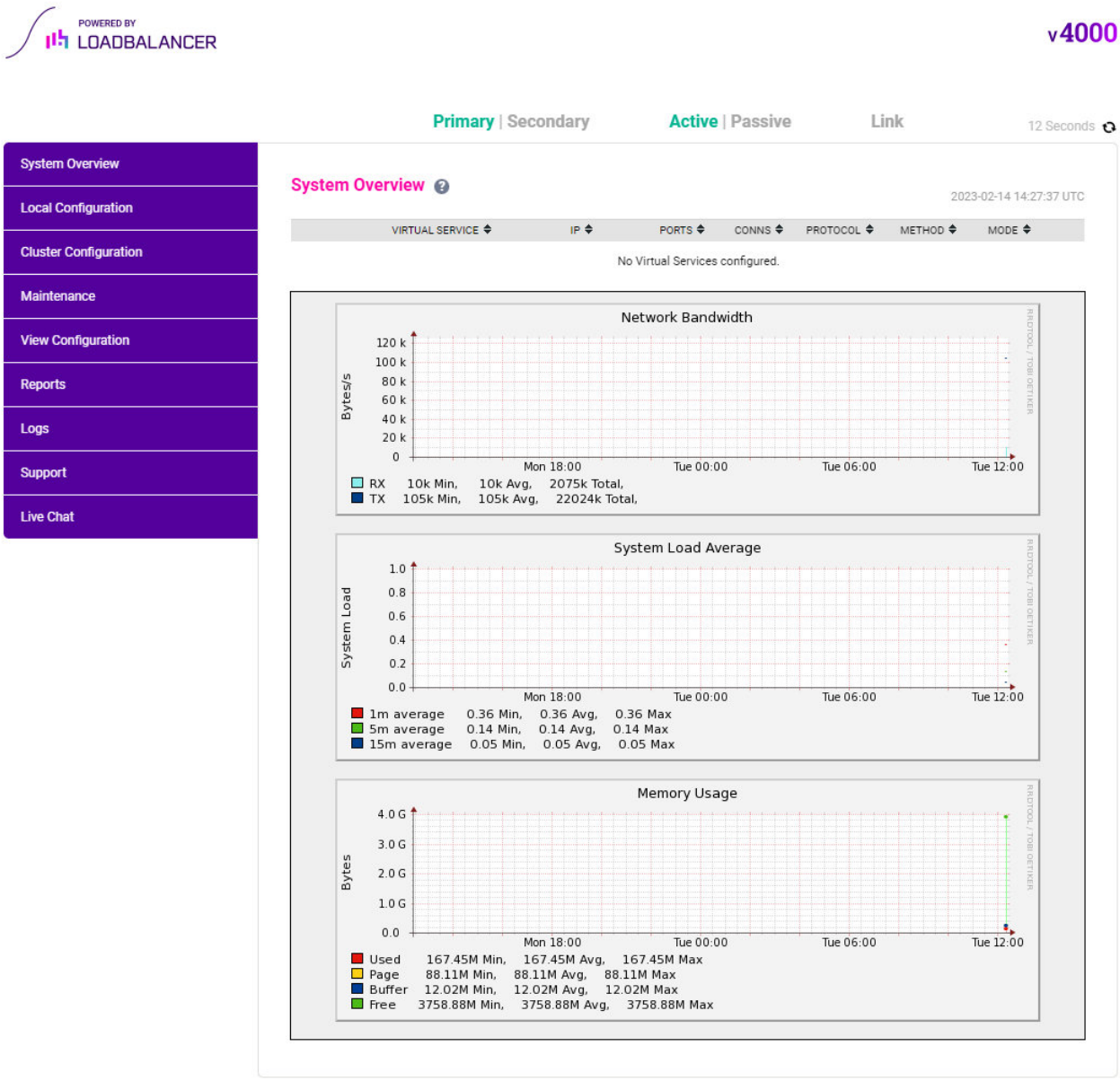
   > **Note** If you need to change the port, IP address or protocol that the WebUI listens on, please refer to Service Socket Addresses.

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:



9.4.1. 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

9.5. Appliance Software Update

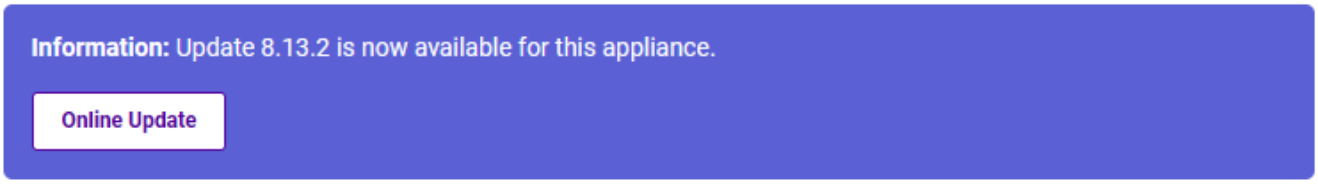
We recommend that the appliance is kept up to date to ensure that you benefit from the latest bug fixes, security updates and feature improvements. Both online and offline update are supported.

> **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.

9.5.1. Online Update

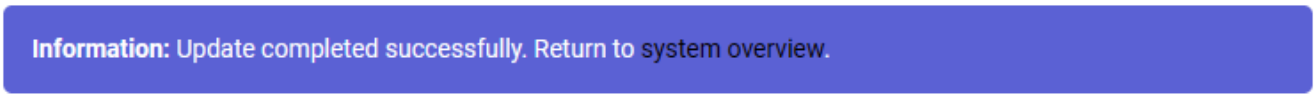
The appliance periodically contacts the Loadbalancer.org update server (**update.loadbalancer.org**) and checks for updates. This is the default behavior and can be disabled if preferred. If an update is found, a notification similar to the example below will be displayed at the top of the WebUI:



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:



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

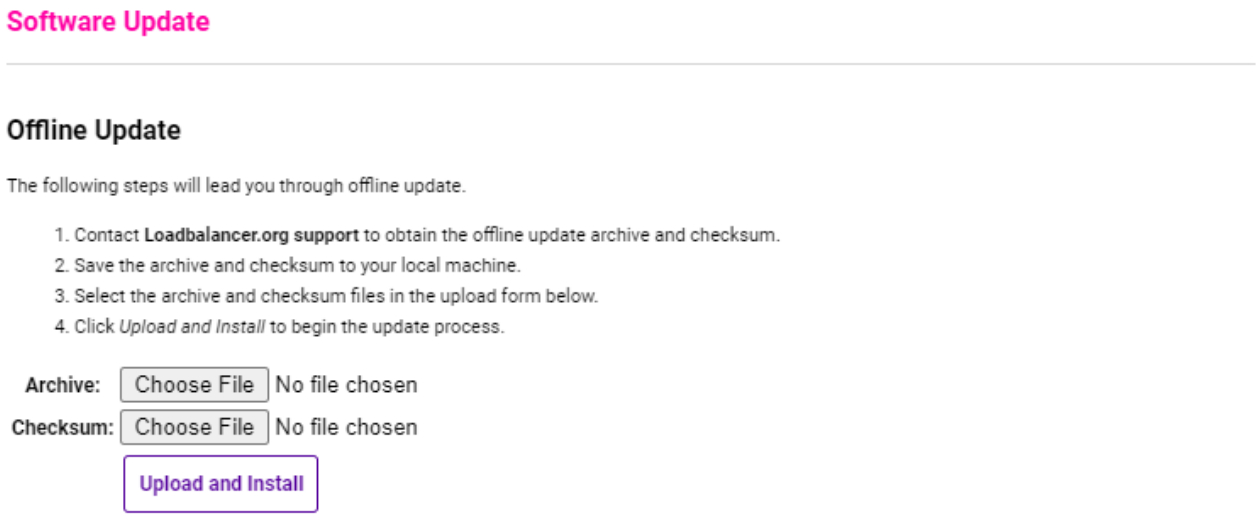
9.5.2. Offline Update

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:



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.

9.6. Configuring the Appliance Security Mode

To enable shell commands to be run from the WebUI, the appliance Security Mode must be configured:

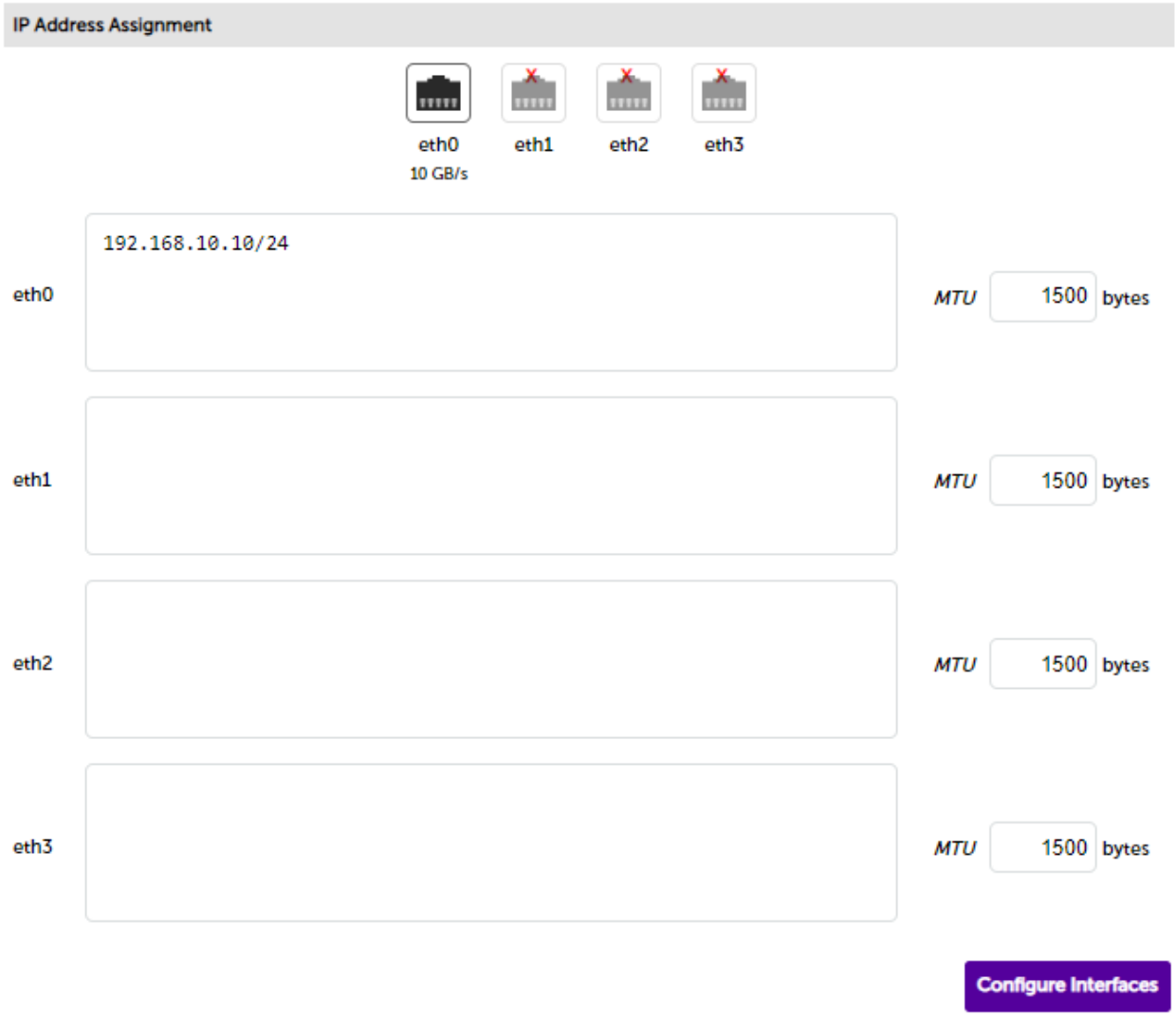
1. Using the WebUI, navigate to: *Local Configuration > Security*.
2. Set *Appliance Security Mode* to **Custom**.
3. Click **Update**.

9.7. Appliance Network Configuration

The standard Centricity PACS network configuration requires 1 network adapter.

9.7.1. Verify Network Connections

1. Verify that the adapter is connected to the appropriate virtual switch/network using the Hypervisor management tool.
2. Using the appliance WebUI navigate to: *Local Configuration > Network Interface Configuration*.



3. Verify that the network is configured as required.

> **Note** The IP address/CIDR prefix for **eth0** was set during the Network Setup Wizard and will be shown here, e.g. **192.168.10.10/24**.

9.7.2. Configuring Hostname & DNS

1. Using the WebUI, navigate to: *Local Configuration > Hostname & DNS*.
2. Set the required *Hostname* and *Domain Name*.
3. Configure additional DNS servers if required.
4. Click **Update**.

9.7.3. Configuring NTP

1. Using the WebUI, navigate to: *Local Configuration > System Date & Time*.
2. Select the required *System Timezone*.
3. Define the required NTP servers.

4. Click **Set Timezone & NTP**.

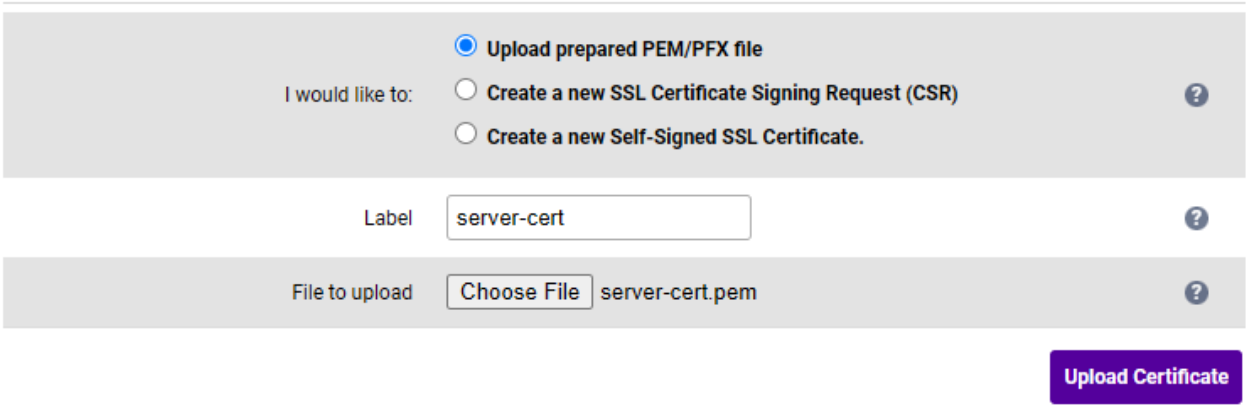
9.8. Configuring Load Balanced Services

9.8.1. Certificates

9.8.1.1. Upload Certificate(s) for use with SSL Termination

> **Note** These certificates are selected using the *SSL Certificate* dropdown when configuring Virtual Services.

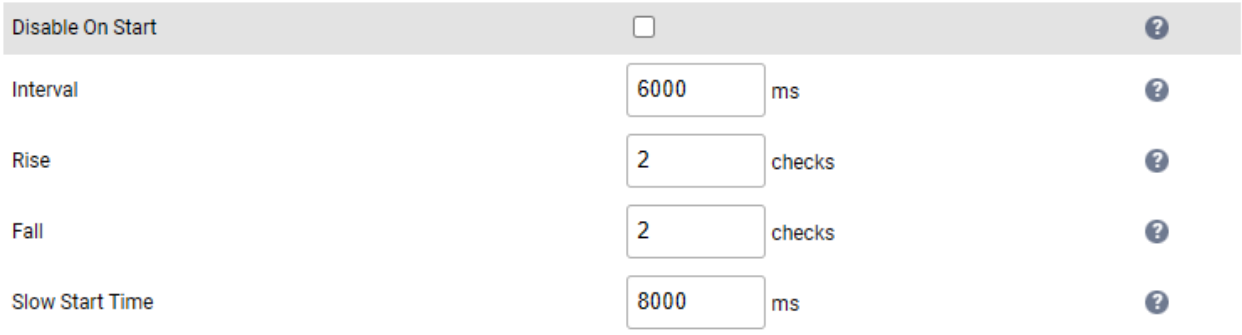
1. Using the WebUI, navigate to *Cluster Configuration > SSL Certificate* and click **Add a new SSL Certificate**.
2. Select the option **Upload prepared PEM/PFX file**.
3. Enter the following details:



   - Specify an appropriate *Label*, e.g. **server-cert**.
   - Click **Choose File**.
   - Browse to and select the relevant PEM or PFX file.
   - For PFX files specify the password if required.
4. Click **Upload Certificate**.
5. Repeat these steps if additional certificates must be uploaded.

9.8.2. Layer 7 Global Settings

1. Using the WebUI, navigate to *Cluster Configuration > Layer 7 - Advanced Configuration*.
2. Set the health check *Interval* to **6000** (ms) as shown below.

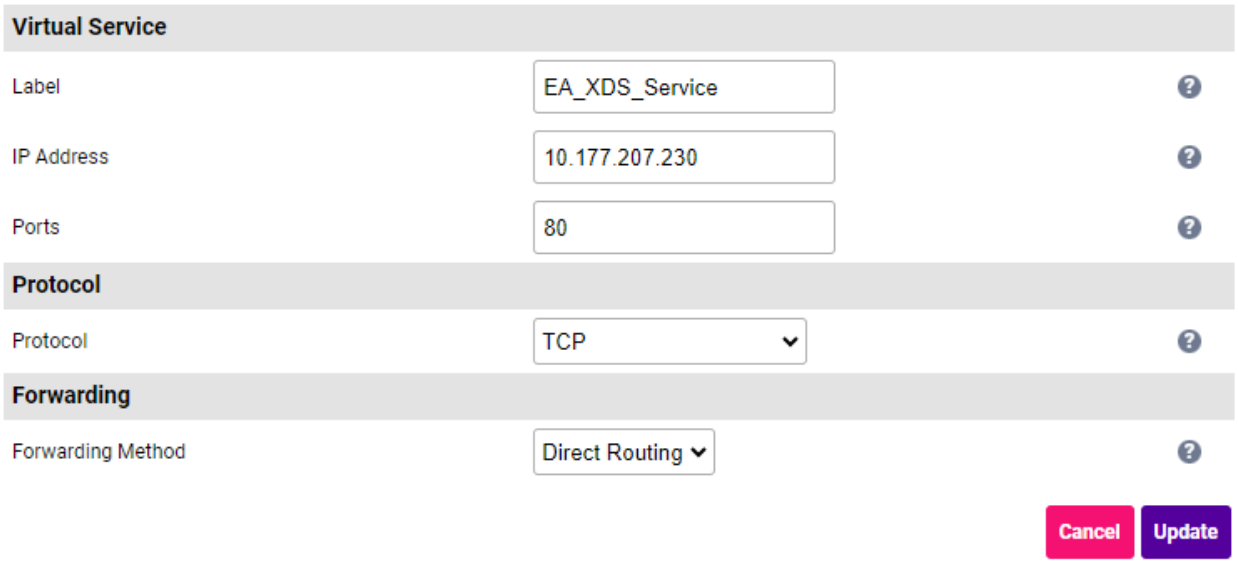


3. Scroll to the bottom of the page and click **Update**.

9.8.3. VIP 1 - EA_XDS_Service

9.8.3.1. Virtual Service (VIP) Configuration

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

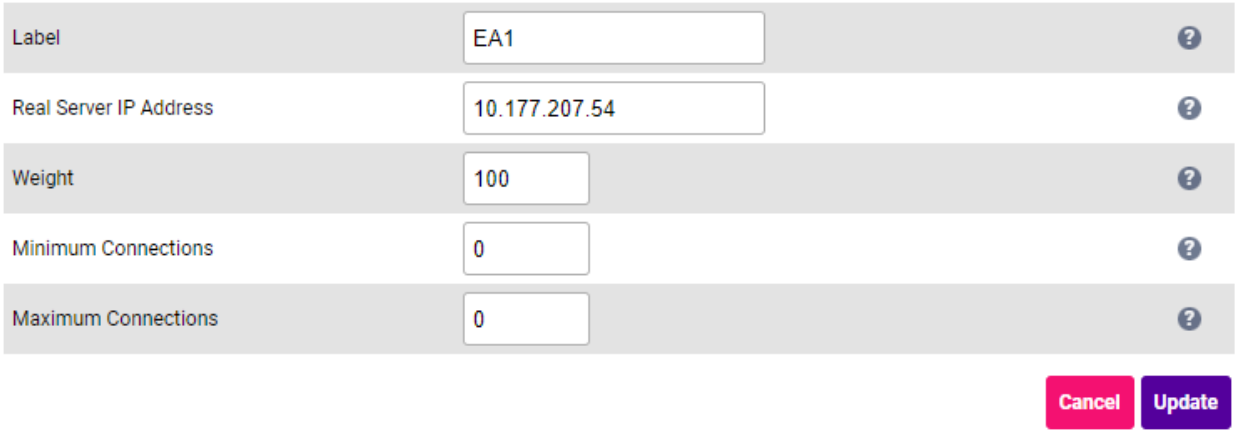


   - Specify an appropriate *Label* for the Virtual Service, e.g. **EA_XDS_Service**.
   - Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.177.207.230**.
   - Set the *Ports* field to **80**.
   - Leave the *Protocol* set to **TCP**.
   - Leave the *Forwarding Method* set to **Direct Routing**.
3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Connection Distribution Method* section.
   - Set the *Balance Mode* to **Weighted Round Robin**.

6. Scroll to the *Persistence* section.
    - Ensure that the *Enable* checkbox is unchecked (disabled).
7. Scroll to the *Health Checks* section.
    - Set *Check Type* to **Negotiate**.
    - Ensure that the *Check Port* is set to **80**.
    - Ensure that the *Protocol* is set to **HTTP**.
    - Set the *Request to send* to **/ea/api/v1/system/health**.
    - Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.
8. Leave all other settings at their default value.
9. Click **Update**.

9.8.3.2. Define the Associated Real Servers (RIPs)

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

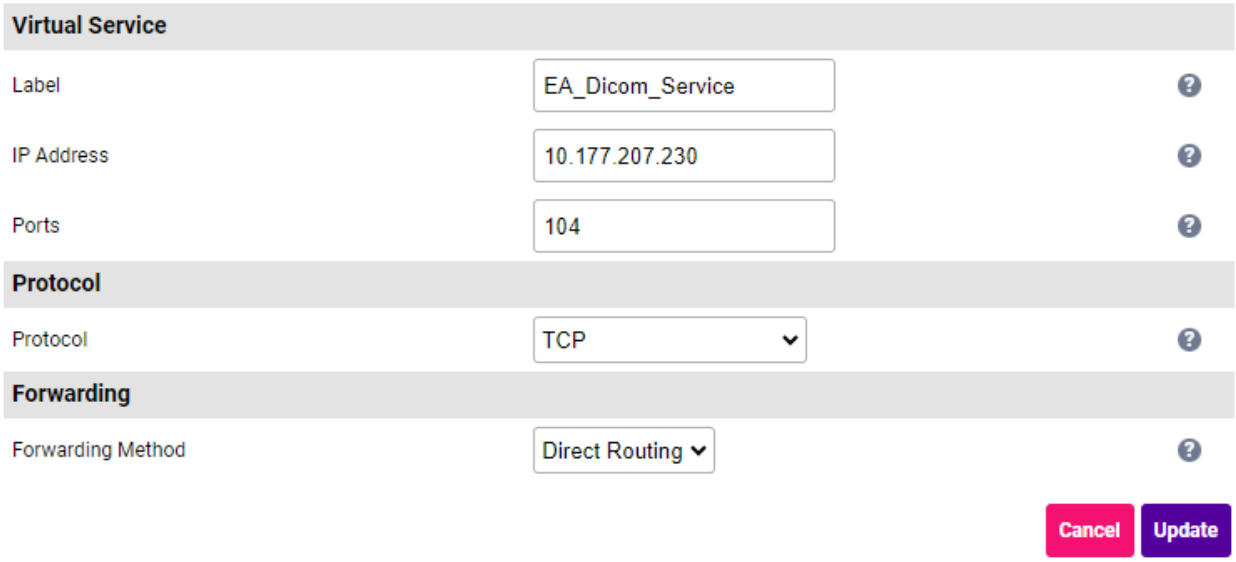


    - Specify an appropriate *Label* for the RIP, e.g. **EA1**.
    - Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.207.54**.
3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Servers.

9.8.4. VIP 2 - EA_Dicom_Service

9.8.4.1. Virtual Service (VIP) Configuration

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



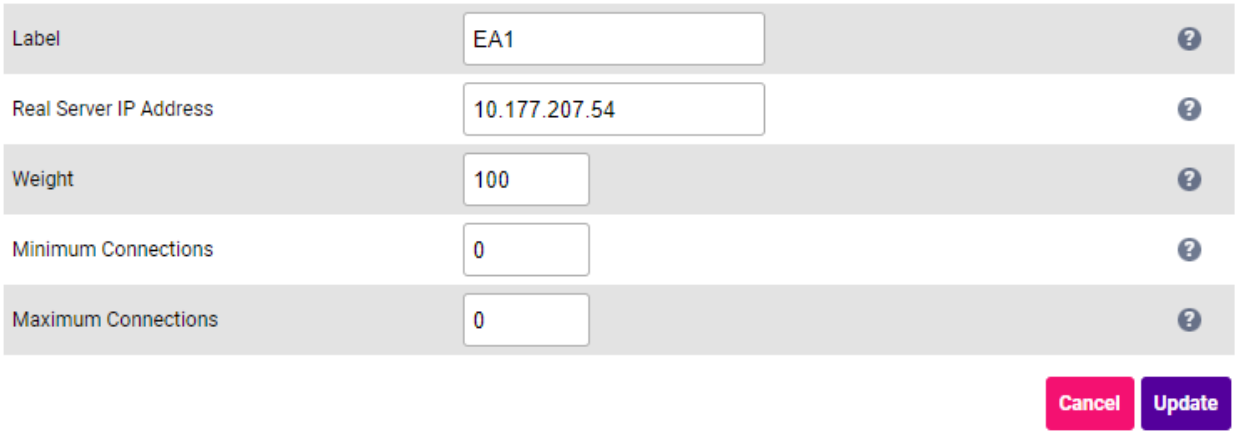
- Specify an appropriate *Label* for the Virtual Service, e.g. **EA_Dicom_Service**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.177.207.230**.
- Set the *Ports* field to **104**.
- Leave the *Protocol* set to **TCP**.
- Leave the *Forwarding Method* set to **Direct Routing**.

3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Connection Distribution Method* section.
   - Set the *Balance Mode* to **Weighted Round Robin**.
6. Scroll to the *Persistence* section.
   - Ensure that the *Enable* checkbox is unchecked (disabled).
7. Scroll to the *Health Checks* section.
   - Set *Check Type* to **Negotiate**.
   - Ensure that the *Check Port* is set to **80**.
   - Ensure that the *Protocol* is set to **HTTP**.
   - Set the *Request to send* to **/ea/api/v1/system/health**.
   - Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.
8. Leave all other settings at their default value.
9. Click **Update**.

9.8.4.2. Define the Associated Real Servers (RIPs)

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

2. Enter the following details:



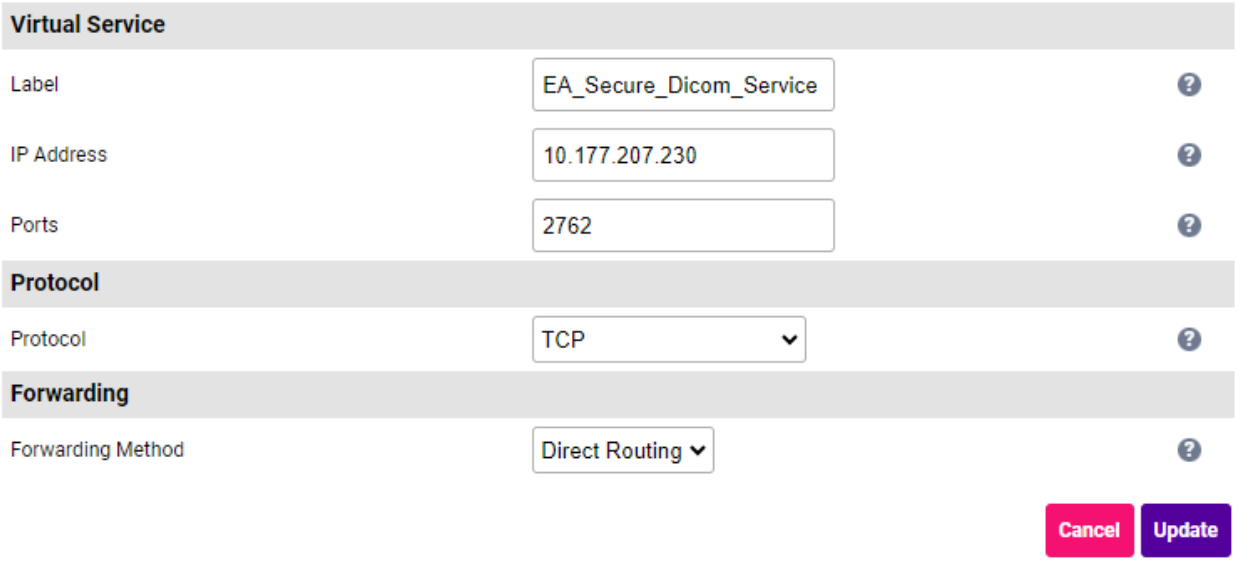
- Specify an appropriate *Label* for the RIP, e.g. **EA1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.207.54**.

3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Servers.

9.8.5. VIP 3 - EA_Secure_Dicom_Service

9.8.5.1. Virtual Service (VIP) Configuration

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



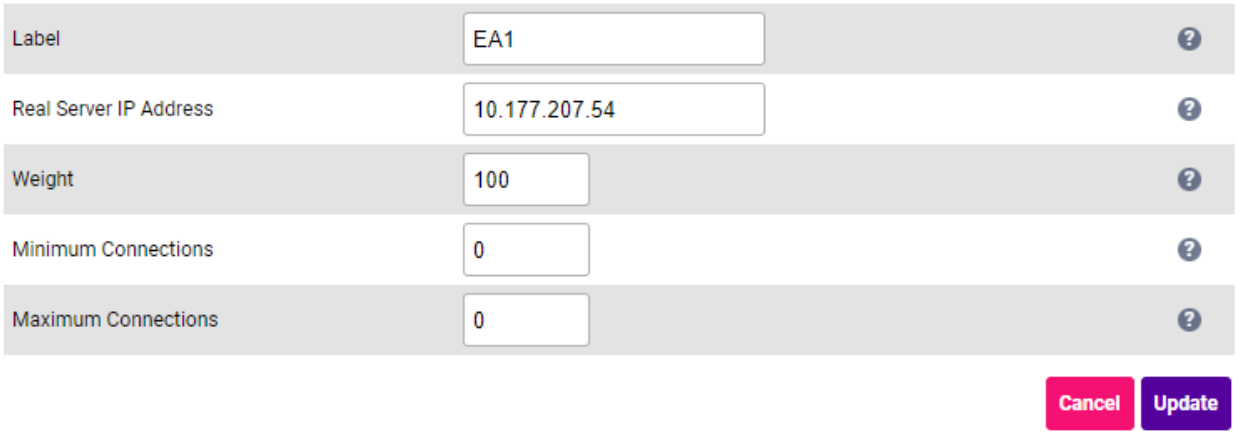
- Specify an appropriate *Label* for the Virtual Service, e.g. **EA_Secure_Dicom_Service**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.177.207.230**.

- Set the *Ports* field to **2762**.
- Leave the *Protocol* set to **TCP**.
- Leave the *Forwarding Method* set to **Direct Routing**.

3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Connection Distribution Method* section.
   - Set the *Balance Mode* to **Weighted Round Robin**.
6. Scroll to the *Persistence* section.
   - Ensure that the *Enable* checkbox is unchecked (disabled).
7. Scroll to the *Health Checks* section.
   - Set *Check Type* to **Negotiate**.
   - Ensure that the *Check Port* is set to **80**.
   - Ensure that the *Protocol* is set to **HTTP**.
   - Set the *Request to send* to **/ea/api/v1/system/health**.
   - Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.
8. Leave all other settings at their default value.
9. Click **Update**.

9.8.5.2. Define the Associated Real Servers (RIPs)

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



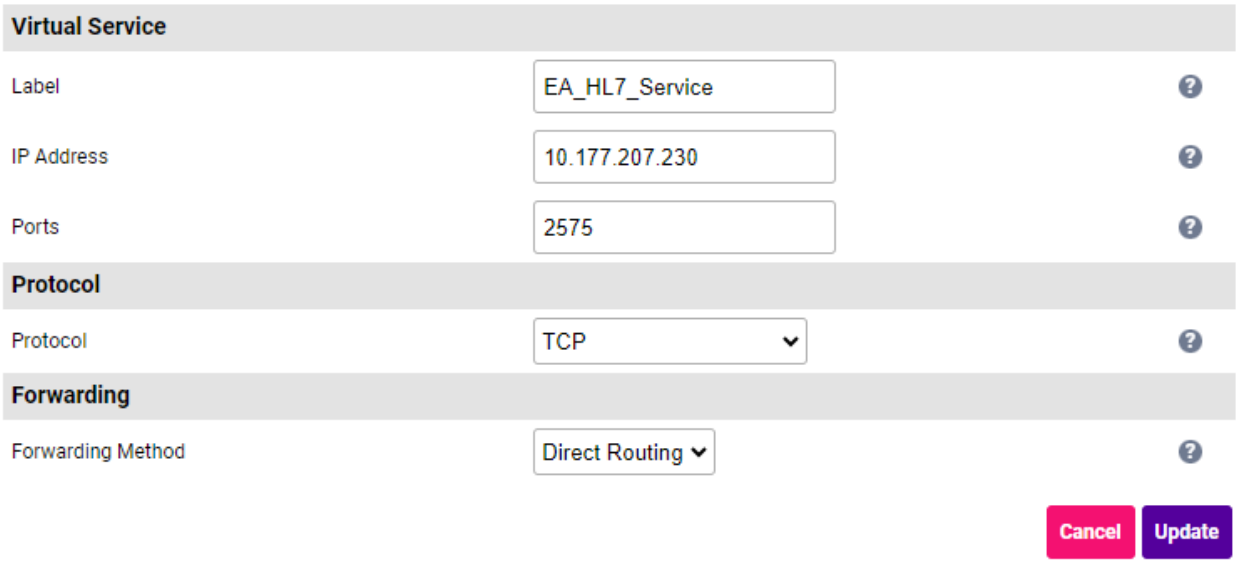
   - Specify an appropriate *Label* for the RIP, e.g. **EA1**.
   - Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.207.54**.
3. Leave all other settings at their default value.

4. Click **Update**.
5. Repeat these steps to add additional Real Servers.

9.8.6. VIP 4 - EA_HL7_Service

9.8.6.1. Virtual Service (VIP) Configuration

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



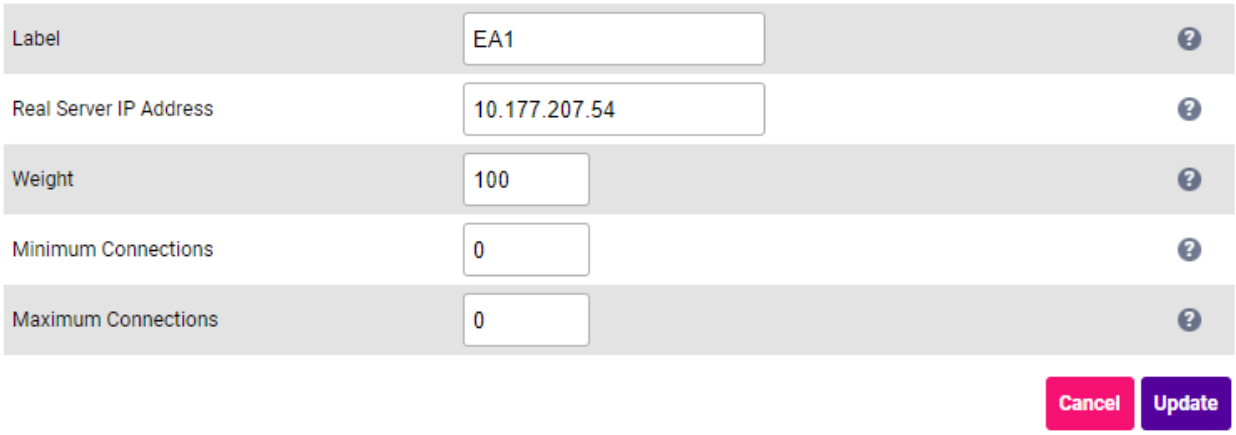
   - Specify an appropriate *Label* for the Virtual Service, e.g. **EA_HL7_Service**.
   - Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.177.207.230**.
   - Set the *Ports* field to **2575**.
   - Leave the *Protocol* set to **TCP**.
   - Leave the *Forwarding Method* set to **Direct Routing**.
3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Connection Distribution Method* section.
   - Set the *Balance Mode* to **Weighted Round Robin**.
6. Scroll to the *Persistence* section.
   - Ensure that the *Enable* checkbox is unchecked (disabled).
7. Scroll to the *Health Checks* section.
   - Set *Check Type* to **Negotiate**.
   - Ensure that the *Check Port* is set to **80**.
   - Ensure that the *Protocol* is set to **HTTP**.

- Set the *Request to send* to **/ea/api/v1/system/health**.
- Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.

8. Leave all other settings at their default value.
9. Click **Update**.

9.8.6.2. Define the Associated Real Servers (RIPs)

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



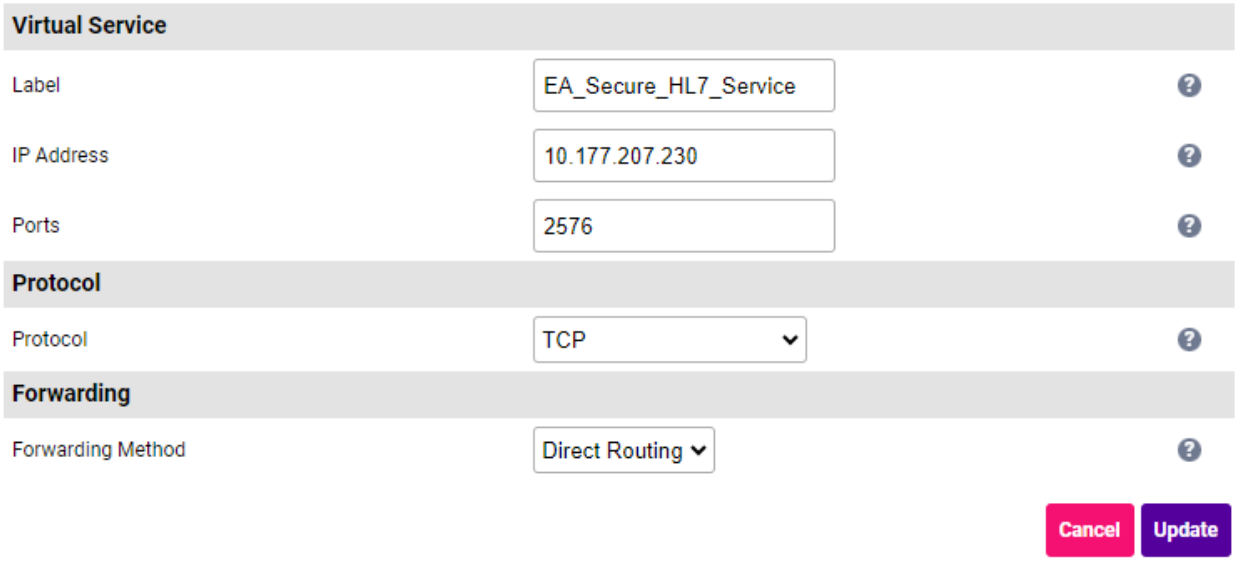
- Specify an appropriate *Label* for the RIP, e.g. **EA1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.207.54**.

3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Servers.

9.8.7. VIP 5 - EA_Secure_HL7_Service

9.8.7.1. Virtual Service (VIP) Configuration

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



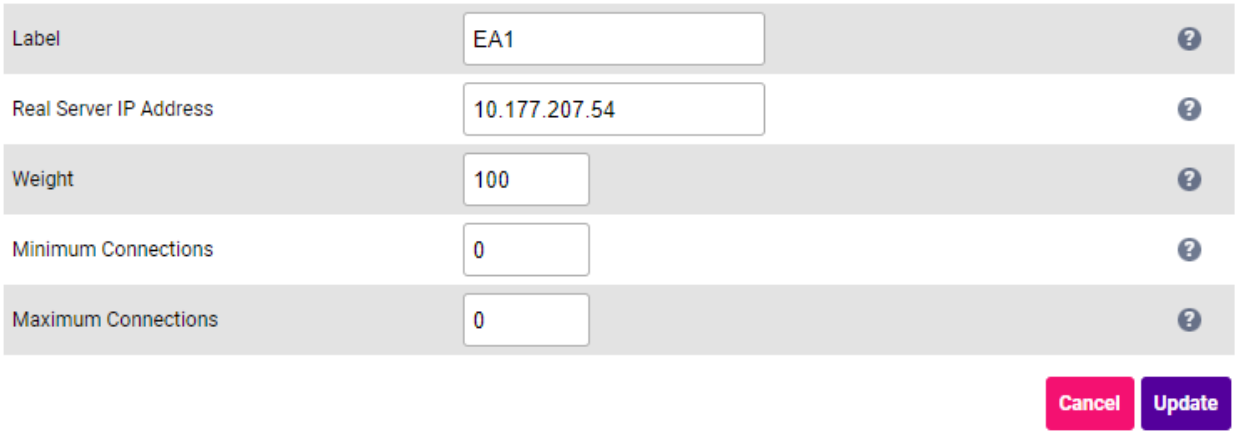
- Specify an appropriate *Label* for the Virtual Service, e.g. **EA_Secure_HL7_Service**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.177.207.230**.
- Set the *Ports* field to **2576**.
- Leave the *Protocol* set to **TCP**.
- Leave the *Forwarding Method* set to **Direct Routing**.

3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Connection Distribution Method* section.
   - Set the *Balance Mode* to **Weighted Round Robin**.
6. Scroll to the *Persistence* section.
   - Ensure that the *Enable* checkbox is unchecked (disabled).
7. Scroll to the *Health Checks* section.
   - Set *Check Type* to **Negotiate**.
   - Ensure that the *Check Port* is set to **80**.
   - Ensure that the *Protocol* is set to **HTTP**.
   - Set the *Request to send* to **/ea/api/v1/system/health**.
   - Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.
8. Leave all other settings at their default value.
9. Click **Update**.

9.8.7.2. Define the Associated Real Servers (RIPs)

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

2. Enter the following details:



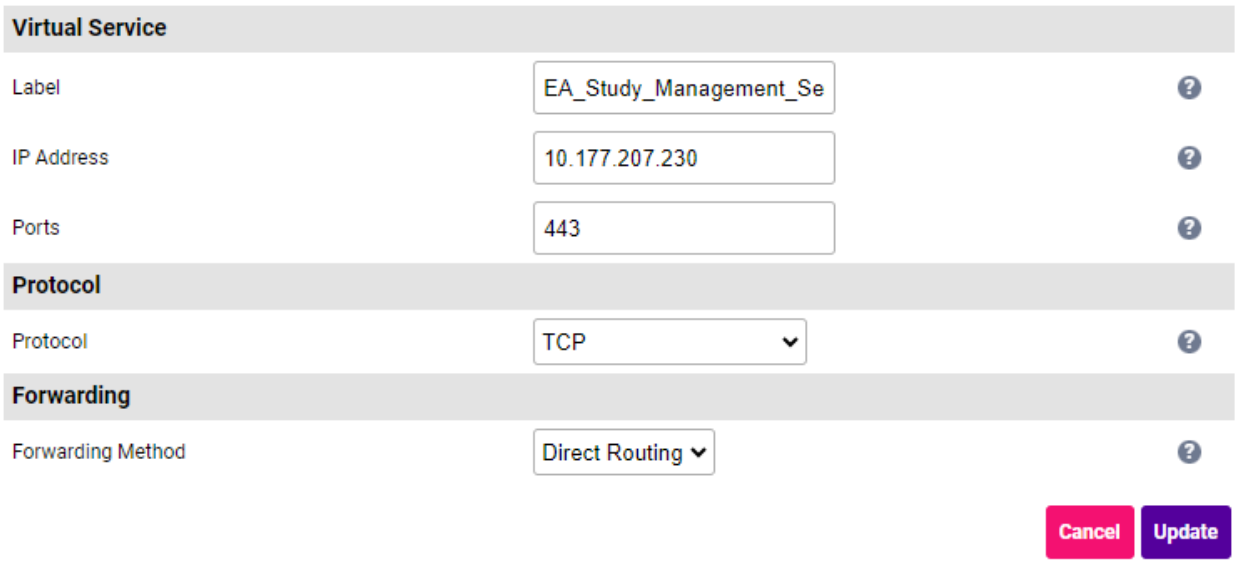
- Specify an appropriate *Label* for the RIP, e.g. **EA1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.207.54**.

3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Servers.

9.8.8. VIP 6 - EA_Study_Management_Service

9.8.8.1. Virtual Service (VIP) Configuration

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



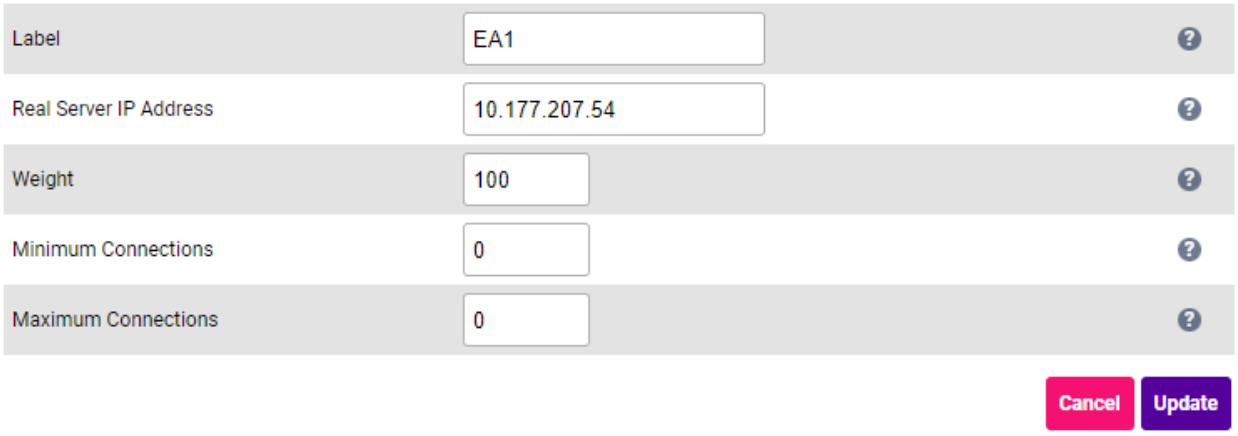
- Specify an appropriate *Label* for the Virtual Service, e.g. **EA_Study_Management_Service**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.177.207.230**.

- Set the *Ports* field to **443**.
- Leave the *Protocol* set to **TCP**.
- Leave the *Forwarding Method* set to **Direct Routing**.

3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Connection Distribution Method* section.
   - Set the *Balance Mode* to **Weighted Round Robin**.
6. Scroll to the *Persistence* section.
   - Ensure that the *Enable* checkbox is unchecked (disabled).
7. Scroll to the *Health Checks* section.
   - Set *Check Type* to **Negotiate**.
   - Ensure that the *Check Port* is set to **80**.
   - Ensure that the *Protocol* is set to **HTTP**.
   - Set the *Request to send* to **/ea/api/v1/system/health**.
   - Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.
8. Leave all other settings at their default value.
9. Click **Update**.

9.8.8.2. Define the Associated Real Servers (RIPs)

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



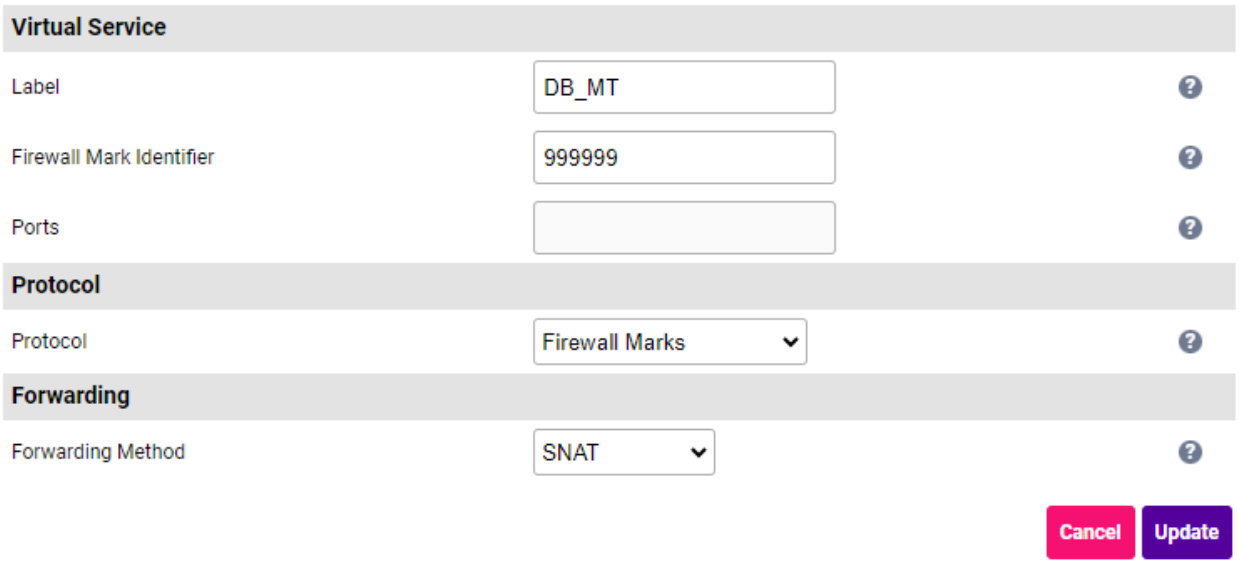
   - Specify an appropriate *Label* for the RIP, e.g. **EA1**.
   - Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.207.54**.
3. Leave all other settings at their default value.

4. Click **Update**.
5. Repeat these steps to add additional Real Servers.

9.8.9. VIP 7 - DB_MT

9.8.9.1. Virtual Service (VIP) Configuration

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



   - Specify an appropriate *Label* for the Virtual Service, e.g. **DB_MT**.
   - Clear the *Ports* field by removing the "80".
   - Set the *Protocol* to **Firewall Marks**, the *IP Address* field will be renamed as *Firewall Mark Identifier* and the *Ports* field will be greyed out (disabled) as this is not used with Firewall Marks.
   - Set the *Firewall Mark Identifier* to **999999**.
   - Set the *Forwarding Method* set to **SNAT**.
3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Connection Distribution Method* section.
   - Set the *Balance Mode* to **Weighted Round Robin**.
6. Scroll to the *Persistence* section.
   - Ensure that the *Enable* checkbox is enabled (checked).
   - Set the *Timeout* to **60000**, i.e. 60000 seconds.
   - Set the *Granularity* to **0**.

> **Note** *Granularity* Explanation: Specify the granularity with which clients are grouped for

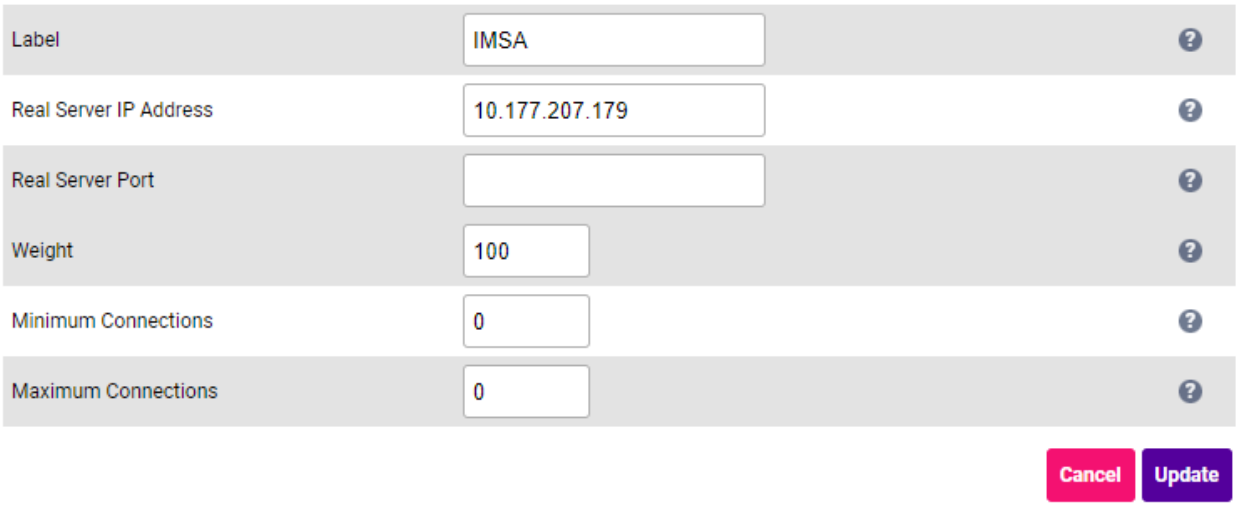
persistent Virtual Services. The source address of the request is masked with this netmask to direct all clients from a network to the same Real Server. The default is 255.255.255.255, that is, the persistence granularity is per client host. Less specific netmasks may be used to resolve problems with non-persistent cache clusters on the client side.

7. Scroll to the *Health Checks* section.
   - Set *Check Type* to **Connect to port**.
   - Set the *check Port* to **80**.
8. Leave all other settings at their default value.
9. Click **Update**.

> **Note** When the protocol is set to Firewall Marks, the firewall script must also be configured accordingly. This is done as a single step in section Section 9.8.10.2 in combination with the configuration required for VIP 8 - DB_DBVIP.

9.8.9.2. Define the Associated Real Servers (RIPs)

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



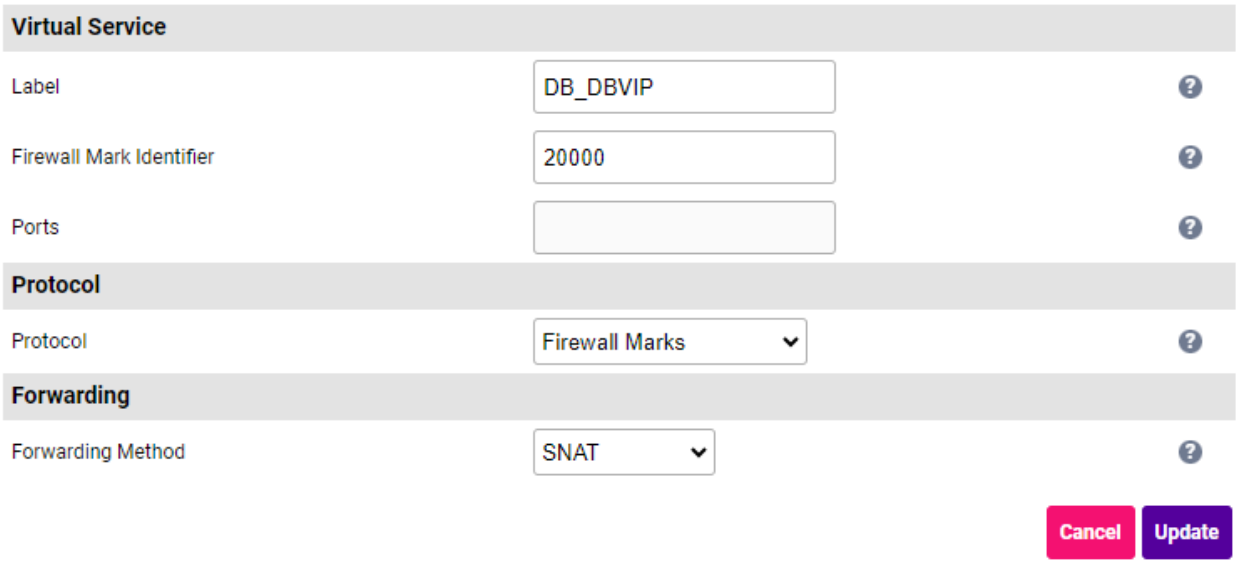
   - Specify an appropriate *Label* for the RIP, e.g. **IMSA**.
   - Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.207.179**.
   - Leave the *Real Server Port* field blank.
   - Set the *Weight* as follows:
     - For the first Real Server, set the *Weight* to **65535**.
     - For the second Real Server, set the *Weight* to **1**.
3. Leave all other settings at their default value.

4. Click **Update**.
5. Repeat these steps to add additional Real Servers.

9.8.10. VIP 8 - DB_DBVIP

9.8.10.1. Virtual Service (VIP) Configuration

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



   - Specify an appropriate *Label* for the Virtual Service, e.g. **DB_DBVIP**.
   - Clear the *Ports* field by removing the "80".
   - Set the *Protocol* to **Firewall Marks**, the *IP Address* field will be renamed as *Firewall Mark Identifier* and the *Ports* field will be greyed out (disabled) as this is not used with Firewall Marks.
   - Set the *Firewall Mark Identifier* to **20000**.
   - Set the *Forwarding Method* set to **SNAT**.
3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Connection Distribution Method* section.
   - Set the *Balance Mode* to **Weighted Round Robin**.
6. Scroll to the *Persistence* section.
   - Ensure that the *Enable* checkbox is enabled (checked).
   - Set the *Timeout* to **57600**, i.e. 57600 seconds.
7. Scroll to the *Health Checks* section.
   - Set *Check Type* to **Ping server**.

8. Leave all other settings at their default value.
9. Click **Update**.

9.8.10.2. Firewall Marks Configuration

Step 1 - Configure the Firewall Script

1. Using the WebUI, navigate to: *Maintenance > Firewall Script* and scroll to the *Manual Firewall Marks* section.
2. Copy/paste the following into the bottom of the section.

> **Important** The IP addresses for **DB_VIP** and **LB_ADR** will need to be modified according to the specific site requirements.

```
DB_VIP="10.177.207.161"
DB_PORT="20000"

LB_ADR="10.177.200.100"

iptables -t mangle -A PREROUTING -p tcp -d $DB_VIP --dport $DB_PORT -j MARK --set-mark 20000
iptables -t mangle -A PREROUTING -p tcp -d $DB_VIP ! --dport $DB_PORT -j MARK --set-mark 999999

iptables -I POSTROUTING -t nat -m ipvs --vaddr $DB_VIP -j SNAT --to-source $LB_ADR
```

As shown below:

Firewall Script

```
27
28  ########################  Manual Firewall Marks  ############################
29
30  # Example: Associate HTTP and HTTPS with Firewall Mark 1:
31  #VIP1="10.0.0.66"
32  #iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 80 -j MARK --set-mark 1
33  #iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 443 -j MARK --set-mark 1
34
35  # A Virtual Service may then be created in the web interface, using 1 as the
36  # service address.
37
38  #It is also possible to bind TCP and UDP protocols together with a firewall mark.
39  #VIP1="192.168.64.27"
40  #iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 80 -j MARK --set-mark 1
41  #iptables -t mangle -A PREROUTING -p udp -d $VIP1 --dport 300 -j MARK --set-mark 1
42
43
44  DB_VIP="10.177.207.161"
45  DB_PORT="20000"
46
47  LB_ADR="10.177.200.100"
48
49  iptables -t mangle -A PREROUTING -p tcp -d $DB_VIP --dport $DB_PORT -j MARK --set-mark 20000
50  iptables -t mangle -A PREROUTING -p tcp -d $DB_VIP ! --dport $DB_PORT -j MARK --set-mark 999999
51
52  iptables -I POSTROUTING -t nat -m ipvs --vaddr $DB_VIP -j SNAT --to-source $LB_ADR
53
54
55  ##########################  Packet Filtering  ################################
56
57  # You should always use a network perimeter firewall to lock down all
    # external access to the load balancer except the required Virtual Services
```

Update

3. Click **Update**.

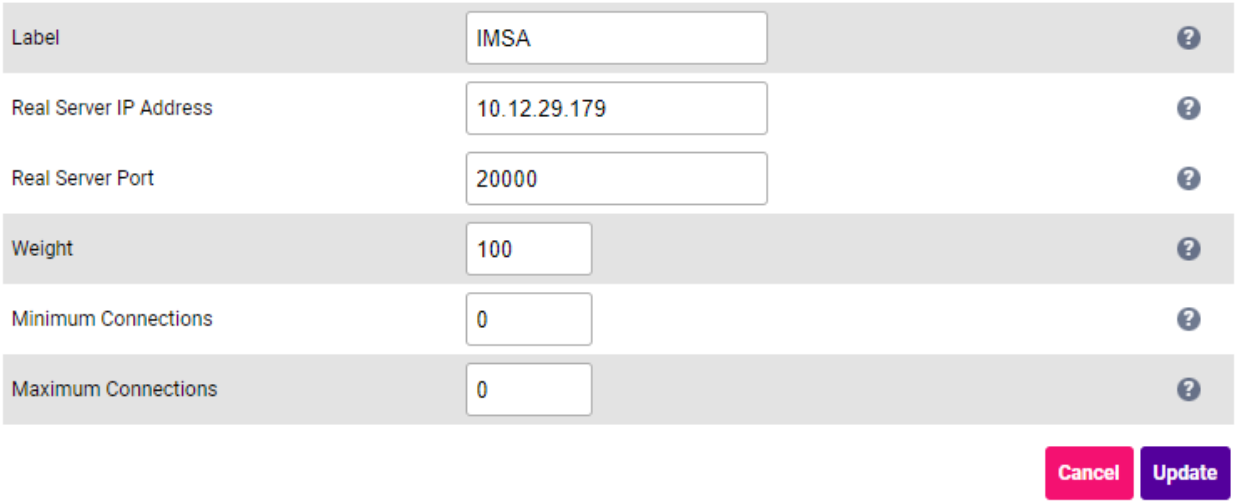
Step 2 - Add the Floating IP Address

> **Note** If you're modifying an existing layer 4 VIP, the floating IP will already exist so this step can be skipped.

1. Using the WebUI, navigate to: *Cluster Configuration > Floating IPs*.
2. Add a floating IP that corresponds to the required VIP, e.g. **10.177.207.161**.
3. Click **Add Floating IP**.

9.8.10.3. Define the Associated Real Servers (RIPs)

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



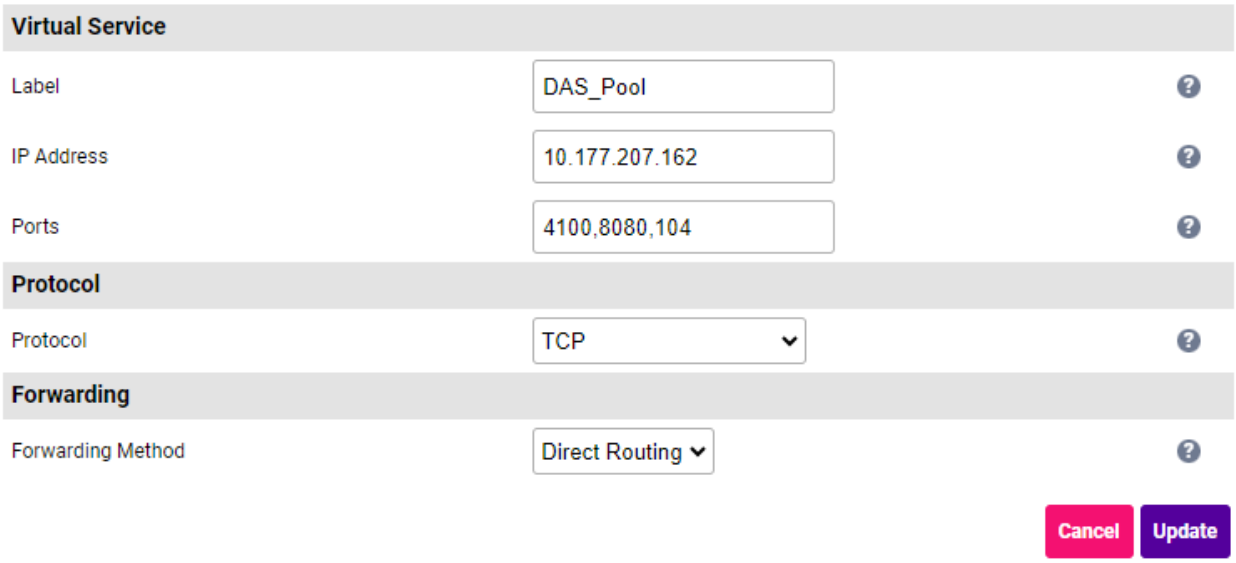
   - Specify an appropriate *Label* for the RIP, e.g. **IMSA**.
   - Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.207.179**.
   - Set the *Real Server Port* field to **20000**.
   - Set *Maximum Connections* to **1990**.
3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Servers.

9.8.11. VIP 9 - DAS_Pool

9.8.11.1. Virtual Service (VIP) Configuration

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

2. Enter the following details:

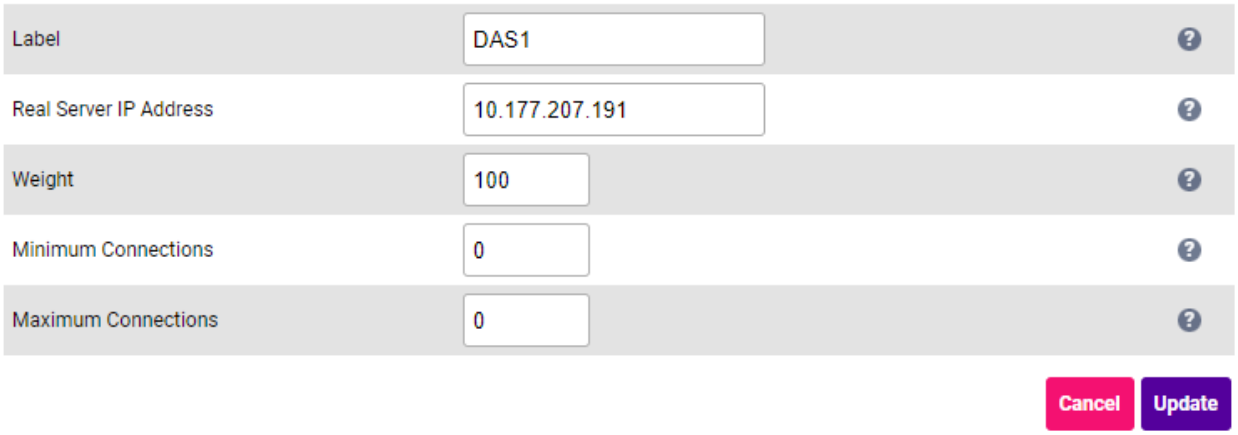


- Specify an appropriate *Label* for the Virtual Service, e.g. **DAS_Pool**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.177.207.162**.
- Set the *Ports* field to **4100,8080,104**.
- Leave the *Protocol* set to **TCP**.
- Leave the *Forwarding Method* set to **Direct Routing**.

3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Connection Distribution Method* section.
   - Set the *Balance Mode* to **Weighted Round Robin**.
6. Scroll to the *Persistence* section.
   - Ensure that the *Enable* checkbox is unchecked (disabled)
7. Scroll to the *Health Checks* section.
   - Set *Check Type* to **Negotiate**.
   - Ensure that the *Check Port* is set to **8080**.
   - Ensure that the *Protocol* is set to **HTTP**.
   - Set the *Request to send* to **/das/health/status**.
   - Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.
8. Leave all other settings at their default value.
9. Click **Update**.

9.8.11.2. Define the Associated Real Servers (RIPs)

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

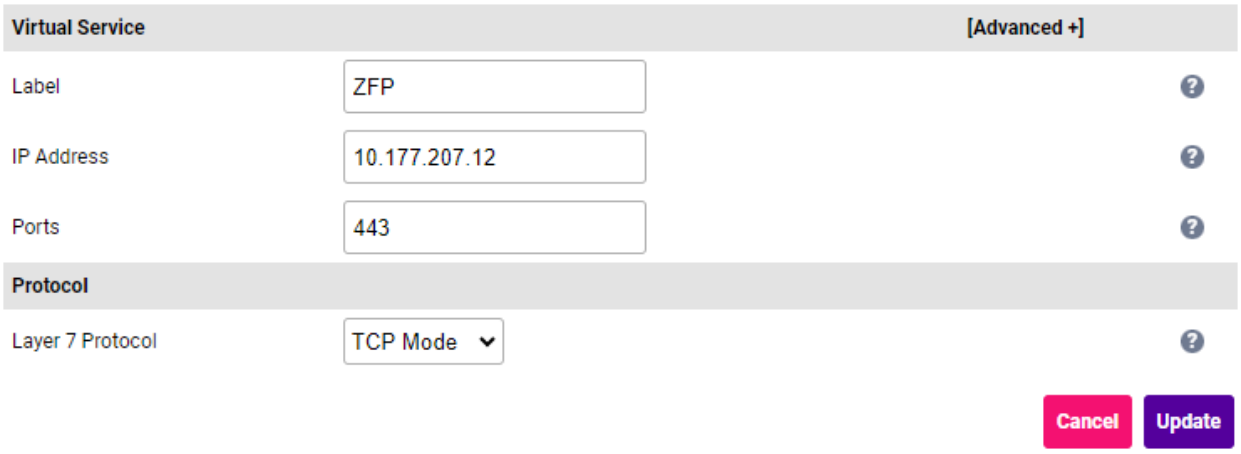


   - Specify an appropriate *Label* for the RIP, e.g. **DAS1**.
   - Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.207.191**.
3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Servers.

9.8.12. VIP 10 - ZFP

9.8.12.1. Virtual Service (VIP) Configuration

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



   - Specify an appropriate *Label* for the Virtual Service, e.g. **ZFP**.
   - Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.177.207.12**.

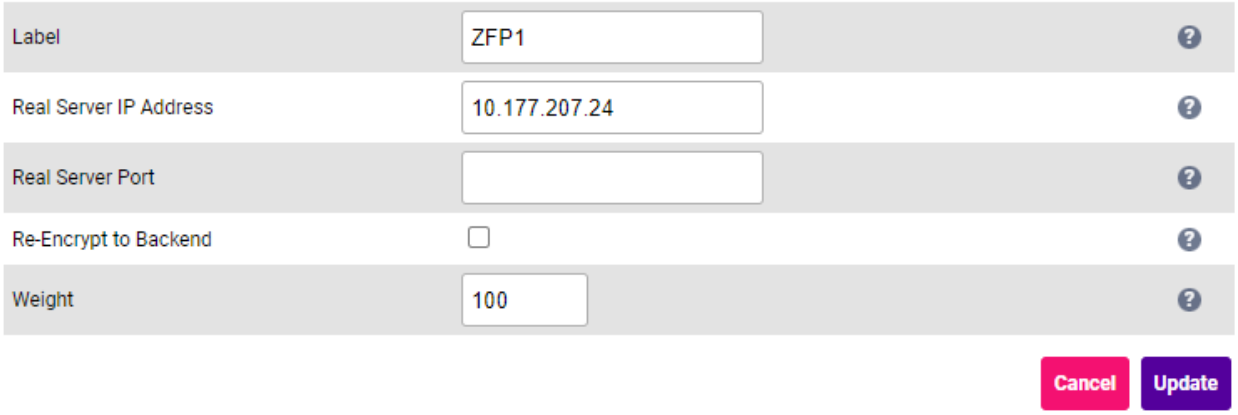
- Set the *Ports* field to **443**.
- Set the *Layer 7 Protocol* to **TCP Mode**.

3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Connection Distribution Method* section.
   - Set the *Balance Mode* to **Weighted Round Robin**.
6. Scroll to the *Persistence* section.
   - Ensure that the *Persistence Mode* is set to **Source IP**.
   - Set the *Persistence Timeout* to **33**, i.e. 33 minutes.
7. Scroll to the *Health Checks* section.
   - Set the *Health Check* to **Negotiate HTTPS (GET)**.
   - Set the *Request to send* to **ZFPHealthMonitor/api/HealthCheck**.
   - Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.
8. Leave all other settings at their default value.
9. Click **Update**.

> **Note** VIP 10 - ZFP also requires the layer 7 health check interval to be changed from 4 to 6 seconds. To change this setting, please refer to Layer 7 Global Settings.

9.8.12.2. Define the Associated Real Servers (RIPs)

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



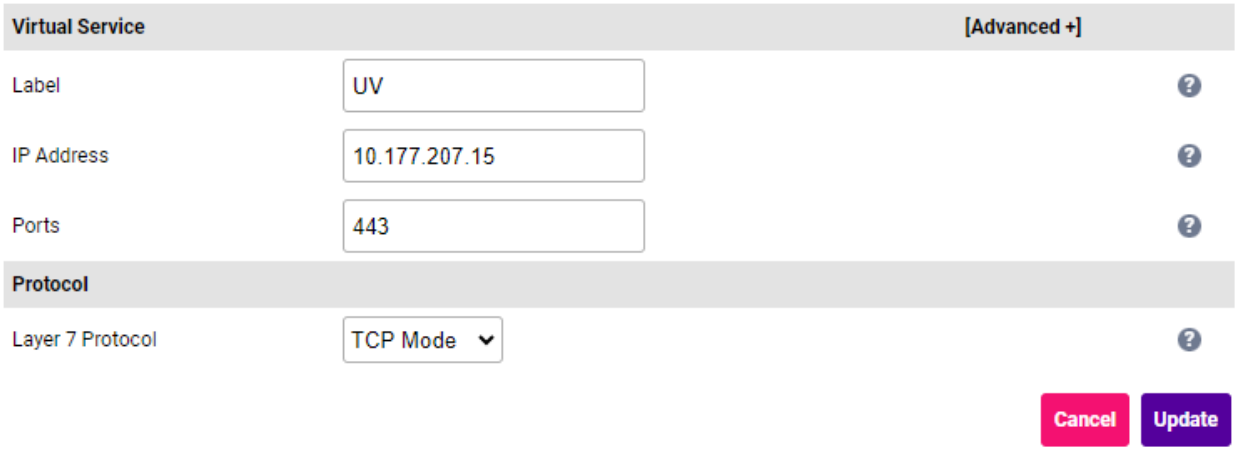
- Specify an appropriate *Label* for the RIP, e.g. **ZFP1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.207.24**.
- Leave the *Real Server Port* field blank.

3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Servers.

9.8.13. VIP 11 - UV

9.8.13.1. Virtual Service (VIP) Configuration

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



   - Specify an appropriate *Label* for the Virtual Service, e.g. **UV**.
   - Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.177.207.15**.
   - Set the *Ports* field to **443**.
   - Set the *Layer 7 Protocol* to **TCP Mode**.
3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Connection Distribution Method* section.
   - Set the *Balance Mode* to **Weighted Round Robin**.
6. Scroll to the *Persistence* section and click **[Advanced]**.
   - Ensure that the *Persistence Mode* is set to **Source IP**.
   - Set the *Persistence Timeout* to **33**, i.e. 33 minutes.
7. Scroll to the *Health Checks* section.
   - Set the *Health Check* to **Negotiate HTTPS (GET)**.
   - Set the *Request to Send* according to the Service Pack installed:
     - For SP1, set *Request to Send* to **/uv/health**.

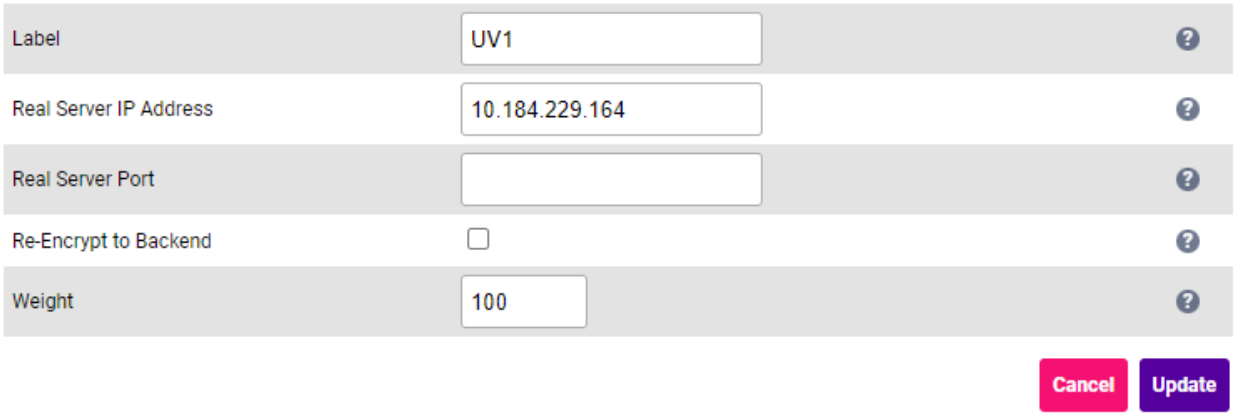
- For SP2, set *Request to Send* to **/v1/health**.

- Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.

8. Leave all other settings at their default value.
9. Click **Update**.

9.8.13.2. Define the Associated Real Servers (RIPs)

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



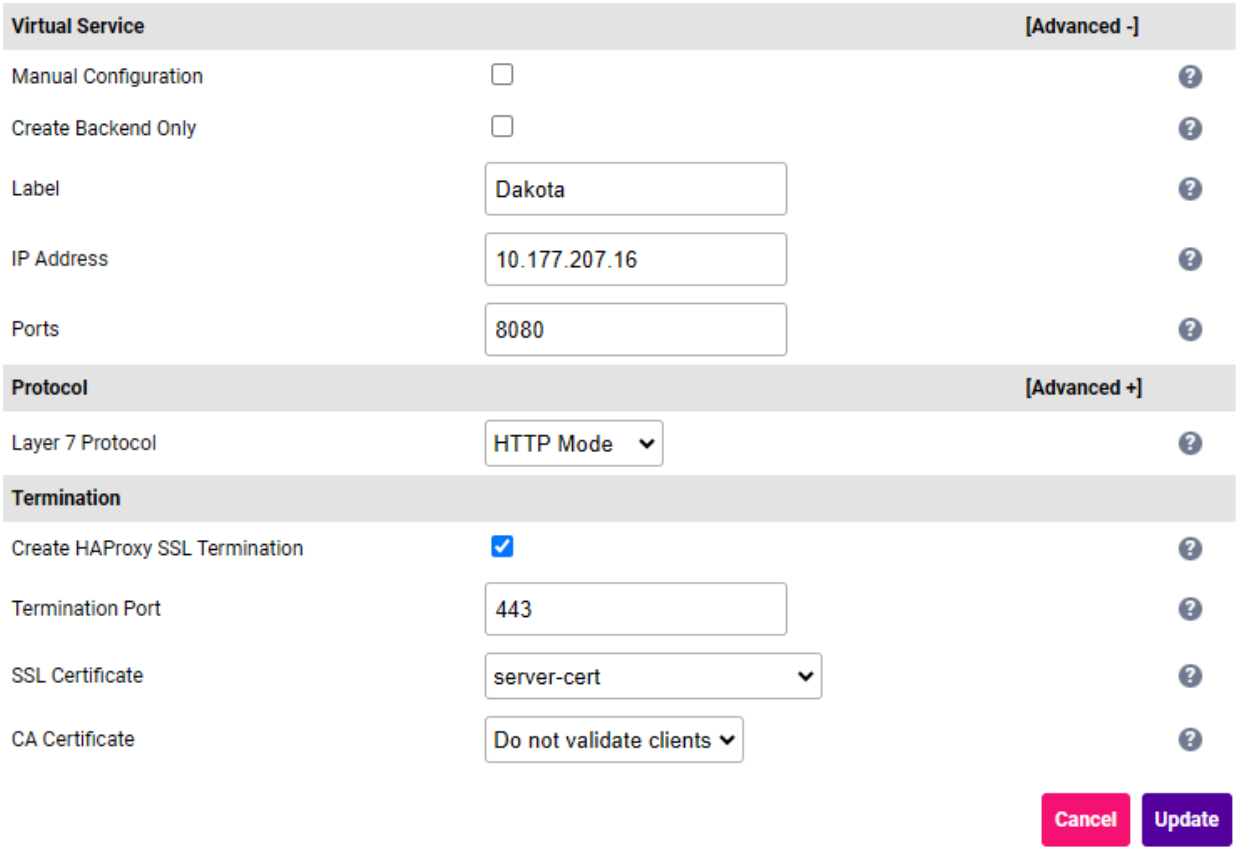
- Specify an appropriate *Label* for the RIP, e.g. **UV1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **10.184.229.164**.
- Leave the *Real Server Port* field blank.

3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Servers.

9.8.14. VIP 12 - Dakota

9.8.14.1. Virtual Service (VIP) Configuration

1. Using the WebUI, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a new Virtual Service**.
2. Click **[Advanced]** in the *Virtual Service* heading bar.
3. Scroll to the *Termination* section.
   - Enable (check) the *Create HAProxy SSL Termination* checkbox.
4. Enter the following details:



- Specify an appropriate *Label* for the Virtual Service, e.g. **Dakota**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.177.207.16**.
- Set the *Ports* field according to the Service Pack installed:
  - For SP1:
    - Set *Ports* to **8080**.
    - Set the *Layer 7 Protocol* to **HTTP Mode**.
  - For SP2
    - Set *Ports* to **8443**.
    - Set the *Layer 7 Protocol* to **TCP Mode**.
- Set the *Termination Port* to **443**.
- Set the *SSL Certificate* to the appropriate certificate, e.g. **server-cert**.

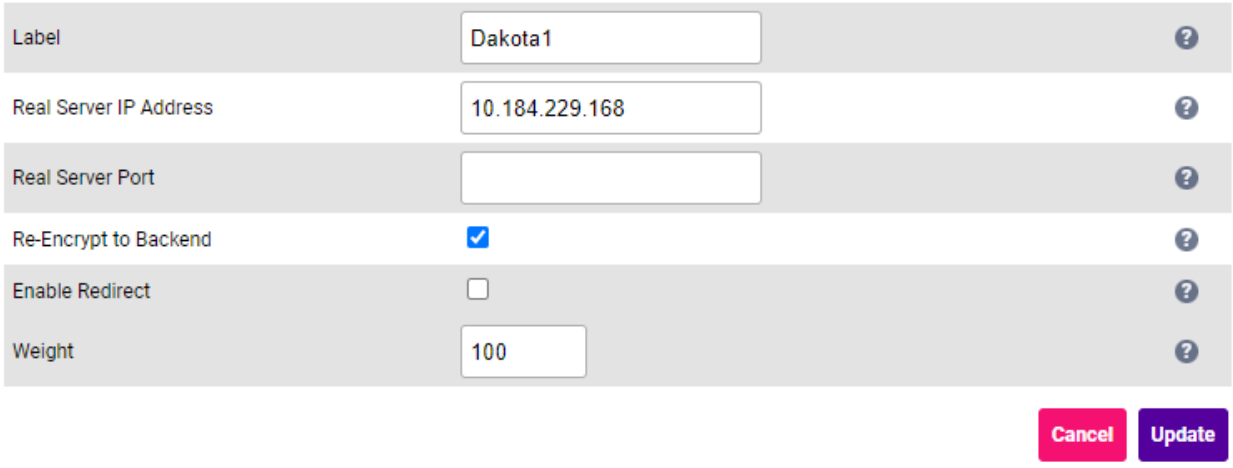
5. Click **Update** to create the Virtual Service.
6. Now click **Modify** next to the newly created VIP.
7. Scroll to the *Connection Distribution Method* section.
   - Set the *Balance Mode* to **Weighted Round Robin**.
8. Scroll to the *Persistence* section and click **[Advanced]**.
   - Ensure that the *Persistence Mode* is to **Source IP**.

- Set the *Persistence Timeout* to **2000**, i.e. 2000 minutes.

9. Scroll to the *Health Checks* section.
   - Configure the health checks according to the Service Pack installed:
     - For SP1:
       - Set the *Health Check* to **Connect to port**.
     - For SP2:
       - Set the *Health Check* to **HTTPS (GET)**.
       - Set *Request to Send* to **/health**.
       - Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.
10. Scroll to the *SSL* section.
    - Enable (check) the *Enable Backend Encryption* checkbox.
11. Leave all other settings at their default value.
12. Click **Update**.

9.8.14.2. Define the Associated Real Servers (RIPs)

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



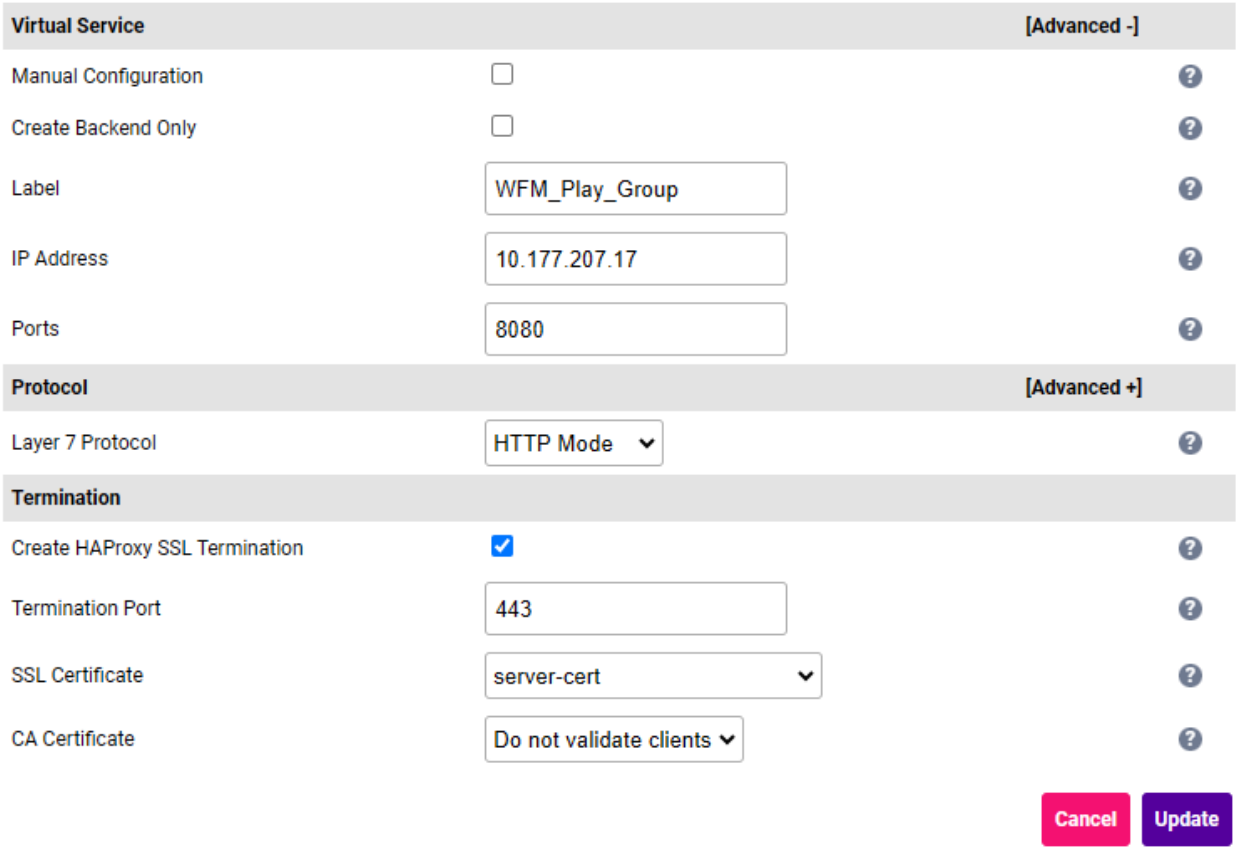
   - Specify an appropriate *Label* for the RIP, e.g. **Dakota1**.
   - Set the *Real Server IP Address* field to the required IP address, e.g. **10.184.229.168**.
   - Leave the *Real Server Port* field blank.
   - Ensure that the *Re-Encrypt to Backend* checkbox is enabled (checked).
3. Leave all other settings at their default value.
4. Click **Update**.

5. Repeat these steps to add additional Real Servers.

9.8.15. VIP 13 - WFM_Play_Group

9.8.15.1. Virtual Service (VIP) Configuration

1. Using the WebUI, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a new Virtual Service**.
2. Click **[Advanced]** in the *Virtual Service* heading bar.
3. Scroll to the *Termination* section.
   - Enable (check) the *Create HAProxy SSL Termination* checkbox.
4. Enter the following details:

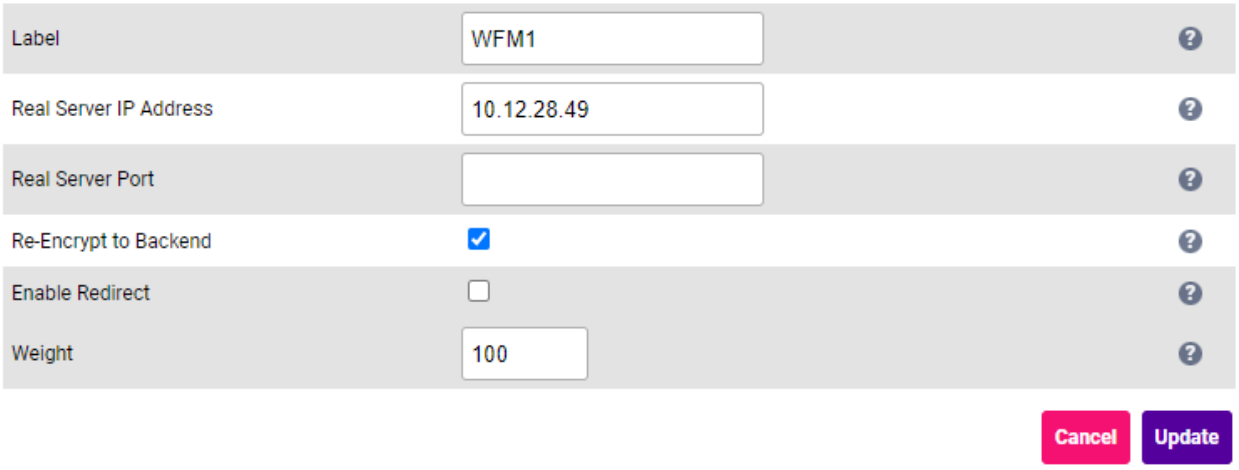


   - Specify an appropriate *Label* for the Virtual Service, e.g. **WFM_Play_Group**.
   - Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.177.207.17**.
   - Set the *Ports* field according to the Service Pack installed:
     - For SP1:
       - Set *Ports* to **8080**.
       - Set the *Layer 7 Protocol* to **HTTP Mode**.
     - For SP2
       - Set *Ports* to **9443**.

        - Set the *Layer 7 Protocol* to **TCP Mode**.
    - Set the *Termination Port* to **443**.
    - Set the *SSL Certificate* to the appropriate certificate, e.g. **server-cert**.
5. Click **Update** to create the Virtual Service.
6. Now click **Modify** next to the newly created VIP.
7. Scroll to the *Connection Distribution Method* section.
    - Set the *Balance Mode* to **Weighted Round Robin**.
8. Scroll to the *Persistence* section and click **[Advanced]**.
    - Ensure that the *Persistence Mode* is to **Source IP**.
    - Set the *Persistence Timeout* to **33**, i.e. 33 minutes.
9. Scroll to the *Health Checks* section.
    - Set the *Health Check* to **HTTPS (GET)**.
    - Configure the health checks according to the Service Pack installed:
        - For SP1:
            - Set *Request to Send* to **/status/check**.
        - For SP2:
            - Set *Request to Send* to **/health**.
            - Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.
10. Scroll to the *SSL* section.
    - Enable (check) the *Enable Backend Encryption* checkbox.
11. Leave all other settings at their default value.
12. Click **Update**.

9.8.15.2. Define the Associated Real Servers (RIPs)

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



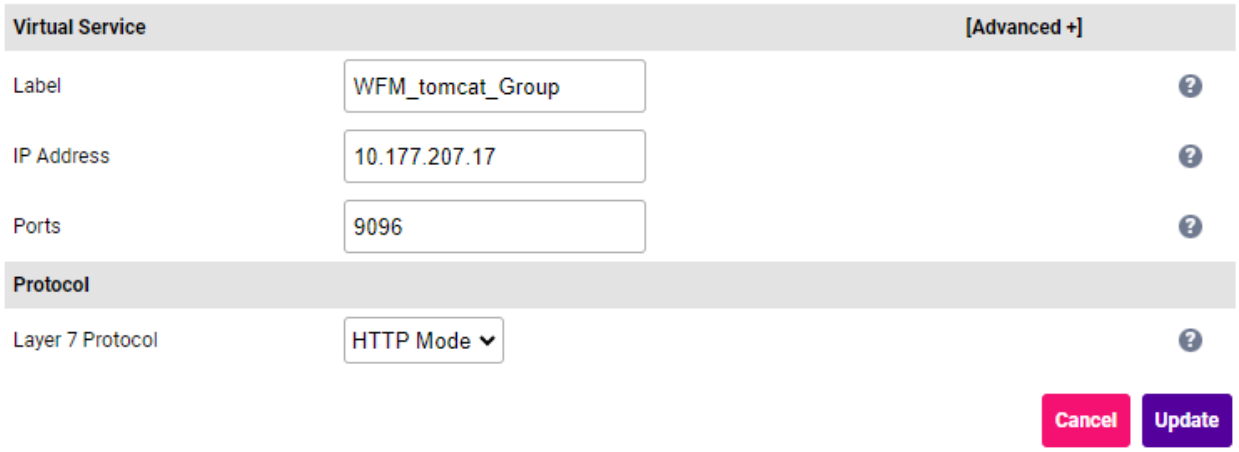
- Specify an appropriate *Label* for the RIP, e.g. **WFM1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **10.12.28.49**.
- Leave the *Real Server Port* field blank.
- Ensure that the *Re-Encrypt to Backend* checkbox is enabled (checked).

3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Servers.

9.8.16. VIP 14 - WFM_tomcat_Group

9.8.16.1. Virtual Service (VIP) Configuration

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



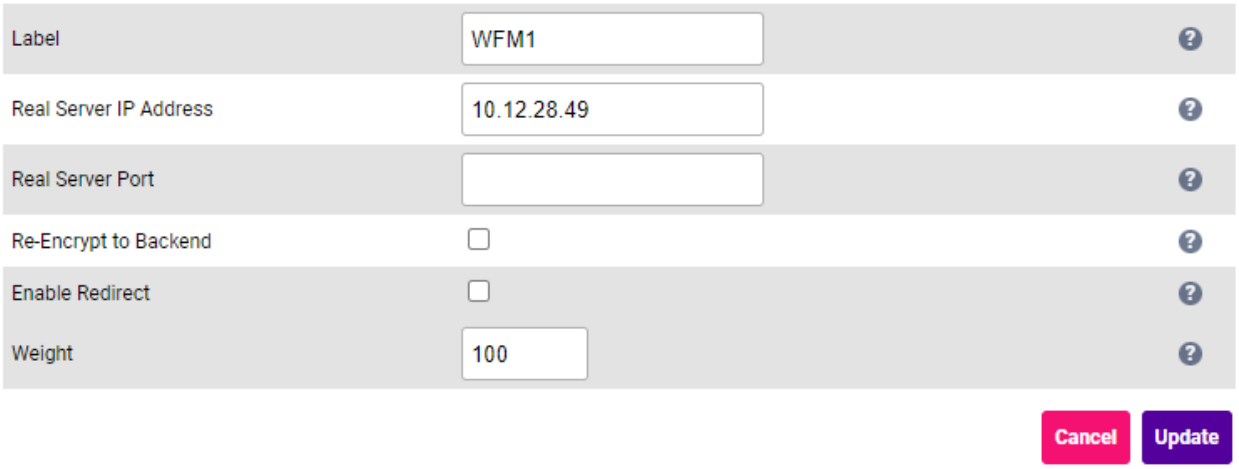
- Specify an appropriate *Label* for the Virtual Service, e.g. **WFM_tomcat_Group**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.177.207.17**.

- Set the *Ports* field according to the Service Pack installed:
  - For SP1:
    - Set *Ports* to **9096**.
  - For SP2
    - Set *Ports* to **9096,3443**.
- Set the *Layer 7 Protocol* to **TCP Mode**.

3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Connection Distribution Method* section.
   - Set the *Balance Mode* to **Weighted Round Robin**.
6. Scroll to the *Persistence* section.
   - Set the *Persistence Mode* to **Source IP**.
   - Set the *Persistence Timeout* to **33**, i.e. 33 minutes.
7. Scroll to the *Health Checks* section.
   - Set the *Health Check* to **Negotiate HTTPS (GET)**.
   - Set the *Request to Send* according to the Service Pack installed:
     - For SP1, set *Request to Send* to **/status/check**.
     - For SP2, set *Request to Send* to **/health**.
   - Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.
8. Leave all other settings at their default value.
9. Click **Update**.

9.8.16.2. Define the Associated Real Servers (RIPs)

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



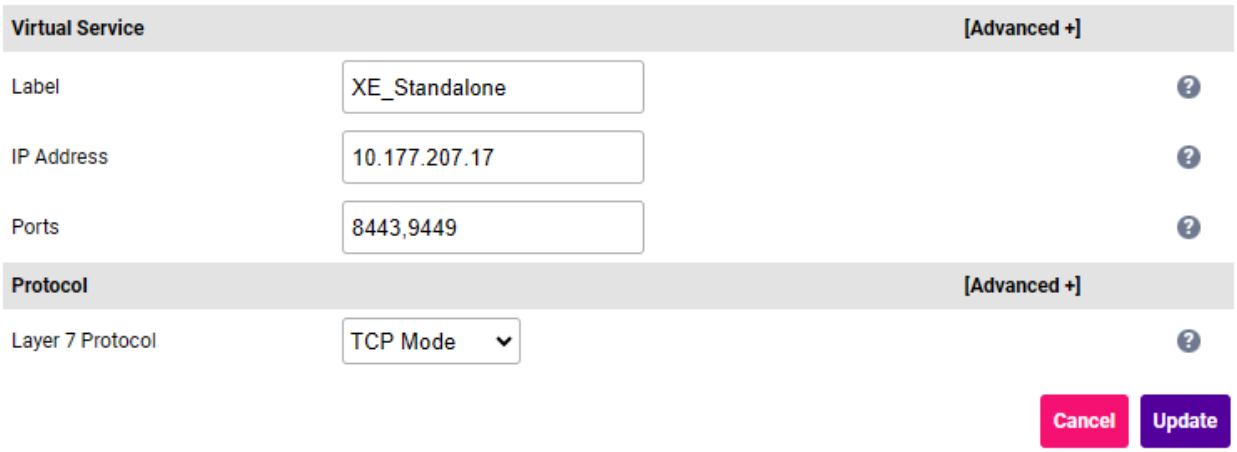
- Specify an appropriate *Label* for the RIP, e.g. **WFM1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **10.12.28.49**.
- Leave the *Real Server Port* field blank.

3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Servers.

9.8.17. VIP 15 - XE_Standalone

9.8.17.1. Virtual Service (VIP) Configuration

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

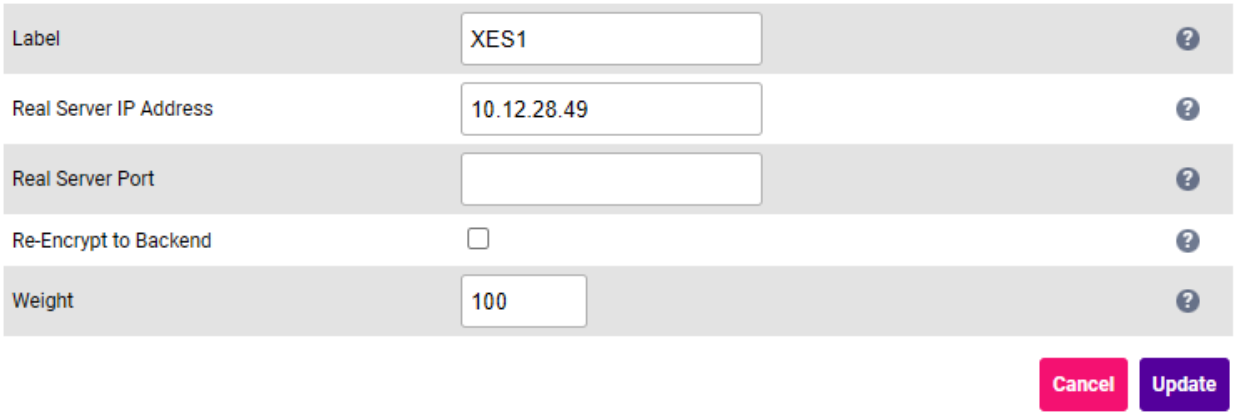


- Specify an appropriate *Label* for the Virtual Service, e.g. **XE_Standalone**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.177.207.17**.
- Set the *Ports* field to **8443,9449**.
- Set the *Layer 7 Protocol* to **TCP Mode**.

3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Connection Distribution Method* section.
   - Set the *Balance Mode* to **Weighted Round Robin**.
6. Scroll to the *Persistence* section and click **[Advanced]**.
   - Ensure that the *Persistence Mode* is set to **Source IP**.
   - Set the *Persistence Timeout* to **33**, i.e. 33 minutes.
7. Scroll to the *Health Checks* section and click **[Advanced]**.
   - Set the *Health Check* to **Negotiate HTTPS (GET)**.
   - Set the *Request to Send* to **/XERService/api/v1/health**.
   - Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.
   - Set the *Check Port* to **9449**.
8. Leave all other settings at their default value.
9. Click **Update**.

9.8.17.2. Define the Associated Real Servers (RIPs)

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

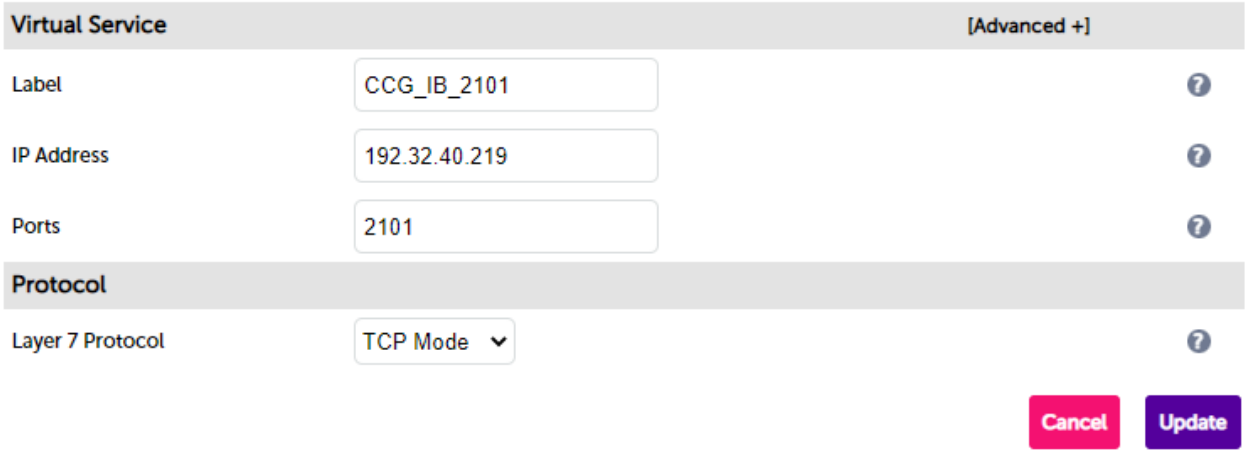


   - Specify an appropriate *Label* for the RIP, e.g. **XES1**.
   - Set the *Real Server IP Address* field to the required IP address, e.g. **10.12.28.49**.
   - Leave the *Real Server Port* field blank.
3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Servers.

9.8.18. VIP 16 - CCG_IB_2101

9.8.18.1. Virtual Service (VIP) Configuration

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

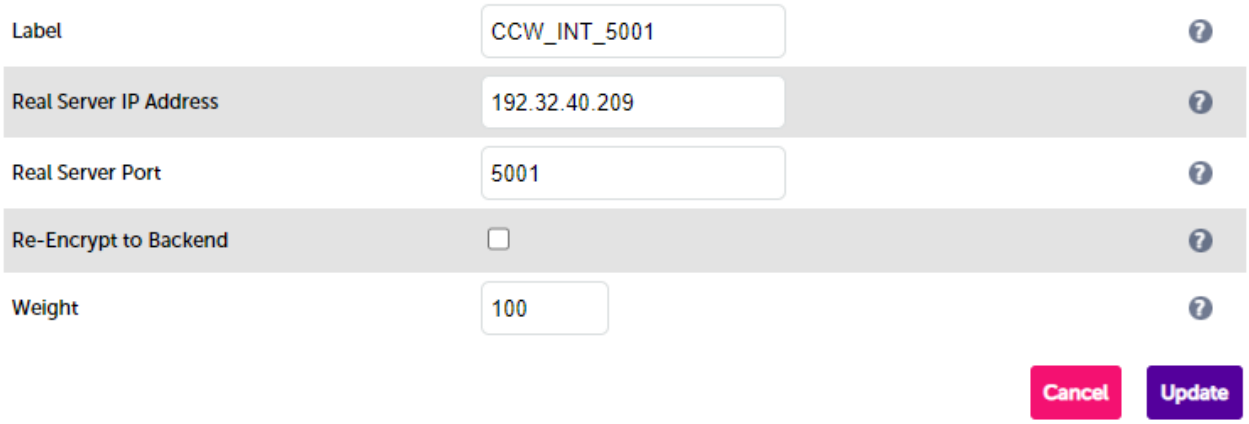


   - Specify an appropriate *Label* for the Virtual Service, e.g. **CCG_IB_2101**.
   - Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.32.40.219**.
   - Set the *Ports* field to **2101**.
   - Set the *Layer 7 Protocol* to **TCP Mode**.
3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Connection Distribution Method* section.
   - Set the *Balance Mode* to **First**.
6. Scroll to the *Persistence* section.
   - Set the *Persistence Mode* to **Last Successful**.
7. Scroll to the *Health Checks* section.
   - Set the *Health Check* to **Connect to Port**.
8. Scroll to the *Fallback Server* section.
   - Click the **[Advanced]** option and select (check) the *Disable Fallback Server* option.
9. Leave all other settings at their default value.
10. Click **Update**.

9.8.18.2. Define the Associated Real Servers (RIPs)

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

2. Enter the following details:



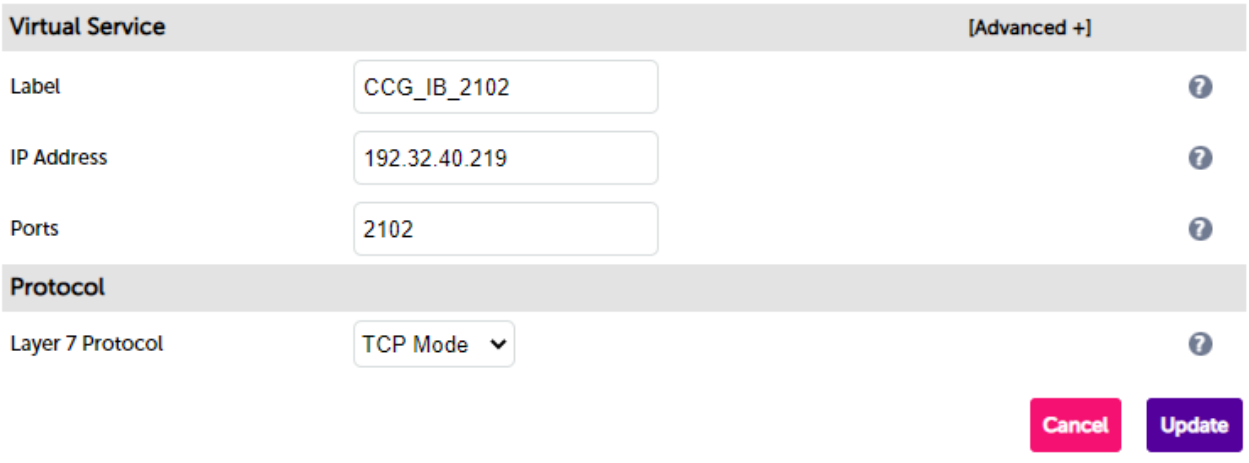
- Specify an appropriate *Label* for the RIP, e.g. **CCW_INT_5001**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.32.40.209**.
- Set the *Real Server Port* field to **5001**.

3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Server(s).

9.8.19. VIP 17 - CCG_IB_2102

9.8.19.1. Virtual Service (VIP) Configuration

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



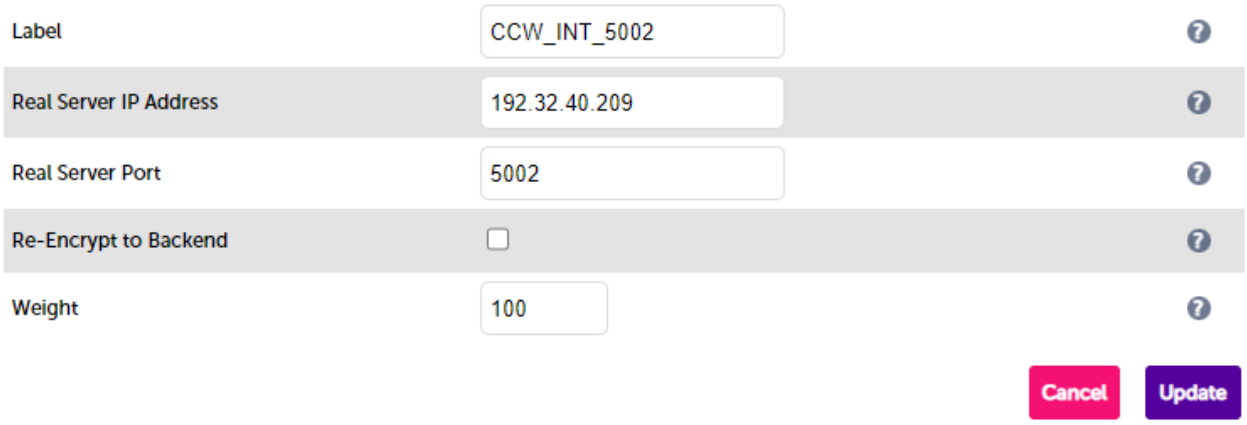
- Specify an appropriate *Label* for the Virtual Service, e.g. **CCG_IB_2102**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.32.40.219**.
- Set the *Ports* field to **2102**.

- Set the *Layer 7 Protocol* to **TCP Mode**.

3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Connection Distribution Method* section.
   - Set the *Balance Mode* to **First**.
6. Scroll to the *Persistence* section.
   - Set the *Persistence Mode* to **Last Successful**.
7. Scroll to the *Health Checks* section.
   - Set the *Health Check* to **Connect to Port**.
8. Scroll to the *Fallback Server* section.
   - Click the **[Advanced]** option and select (check) the *Disable Fallback Server* option.
9. Leave all other settings at their default value.
10. Click **Update**.

9.8.19.2. Define the Associated Real Servers (RIPs)

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

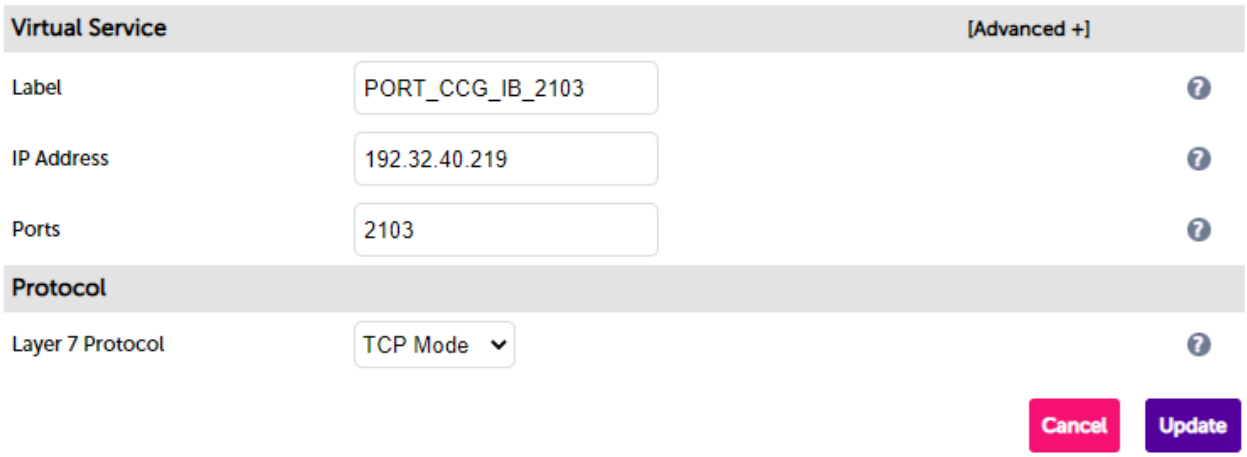


   - Specify an appropriate *Label* for the RIP, e.g. **CCW_INT_5002**.
   - Set the *Real Server IP Address* field to the required IP address, e.g. **192.32.40.209**.
   - Set the *Real Server Port* field to **5002**.
3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Server(s).

9.8.20. VIP 18 - PORT_CCG_IB_2103

9.8.20.1. Virtual Service (VIP) Configuration

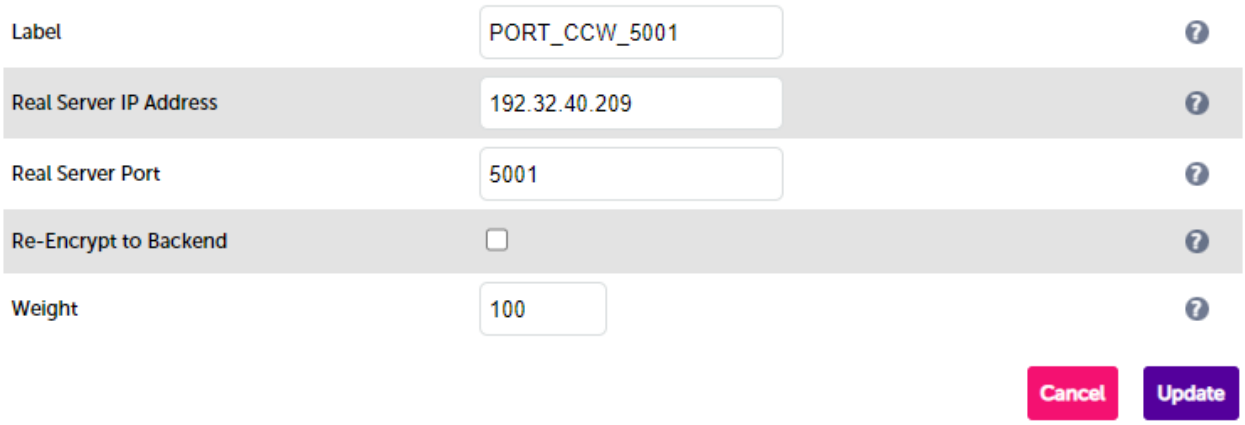
1. Using the WebUI, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a new Virtual Service**.
2. Enter the following details:



   - Specify an appropriate *Label* for the Virtual Service, e.g. **PORT_CCG_IB_2103**.
   - Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.32.40.219**.
   - Set the *Ports* field to **2103**.
   - Set the *Layer 7 Protocol* to **TCP Mode**.
3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Connection Distribution Method* section.
   - Set the *Balance Mode* to **First**.
6. Scroll to the *Persistence* section.
   - Set the *Persistence Mode* to **Last Successful**.
7. Scroll to the *Health Checks* section.
   - Set the *Health Check* to **Connect to Port**.
8. Scroll to the *Fallback Server* section.
   - Click the **[Advanced]** option and select (check) the *Disable Fallback Server* option.
9. Leave all other settings at their default value.
10. Click **Update**.

9.8.20.2. Define the Associated Real Servers (RIPs)

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



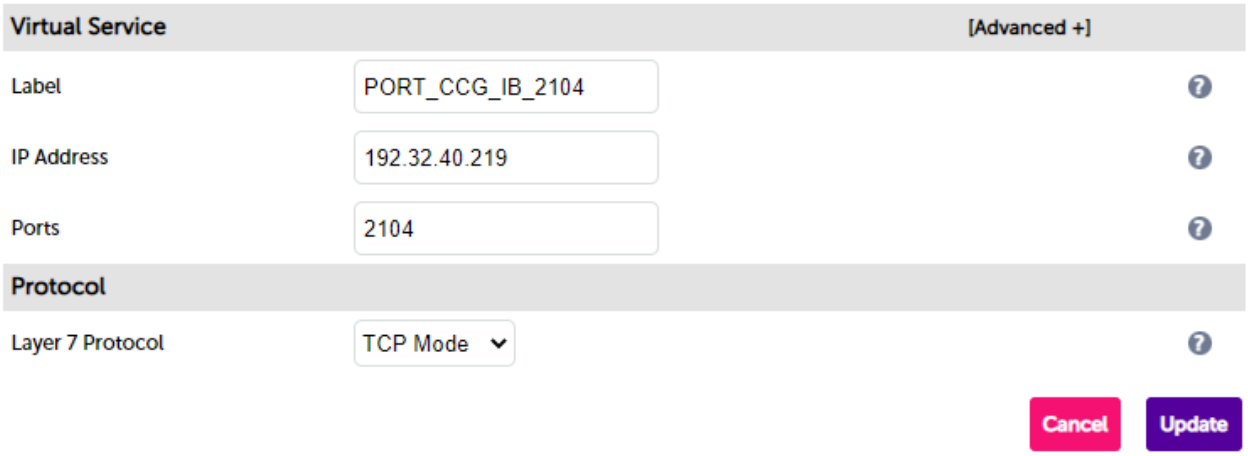
- Specify an appropriate *Label* for the RIP, e.g. **Port_CCW_5001**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.32.40.209**.
- Set the *Real Server Port* field to **5001**.

3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Server(s).

9.8.21. VIP 19 - PORT_CCG_IB_2104

9.8.21.1. Virtual Service (VIP) Configuration

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

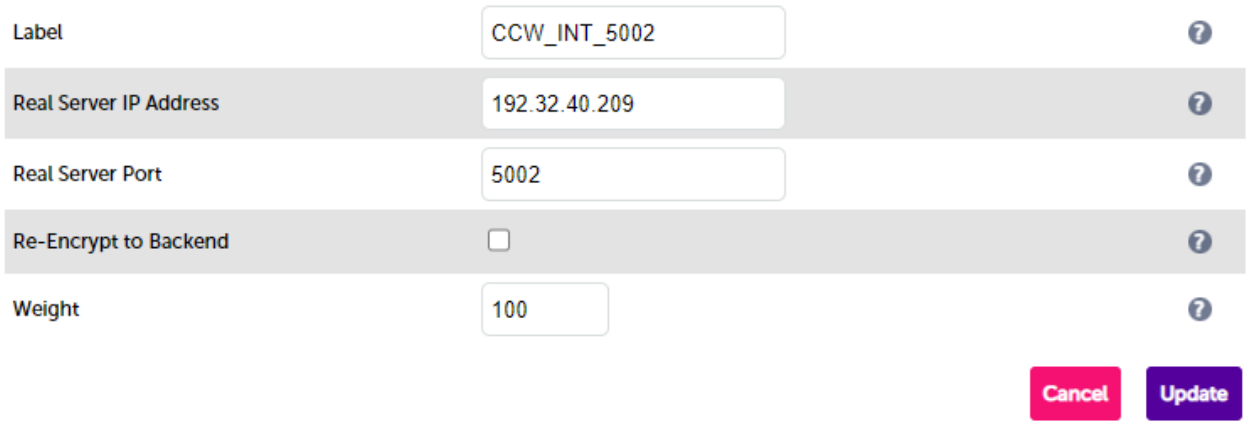


- Specify an appropriate *Label* for the Virtual Service, e.g. **PORT_CCG_IB_2104**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.32.40.219**.
- Set the *Ports* field to **2104**.
- Set the *Layer 7 Protocol* to **TCP Mode**.

3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Connection Distribution Method* section.
   - Set the *Balance Mode* to **First**.
6. Scroll to the *Persistence* section.
   - Set the *Persistence Mode* to **Last Successful**.
7. Scroll to the *Health Checks* section.
   - Set the *Health Check* to **Connect to Port**.
8. Scroll to the *Fallback Server* section.
   - Click the **[Advanced]** option and select (check) the *Disable Fallback Server* option.
9. Leave all other settings at their default value.
10. Click **Update**.

9.8.21.2. Define the Associated Real Servers (RIPs)

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



   - Specify an appropriate *Label* for the RIP, e.g. **CCW_INT_5002**.
   - Set the *Real Server IP Address* field to the required IP address, e.g. **192.32.40.209**.
   - Set the *Real Server Port* field to **5002**.
3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Server(s).

9.8.22. Finalizing the Configuration

To apply the new settings, HAProxy & STunnel must be reloaded. This can be done using the button in the

"Commit changes" box at the top of the screen or by using the ***Restart Services*** menu option:

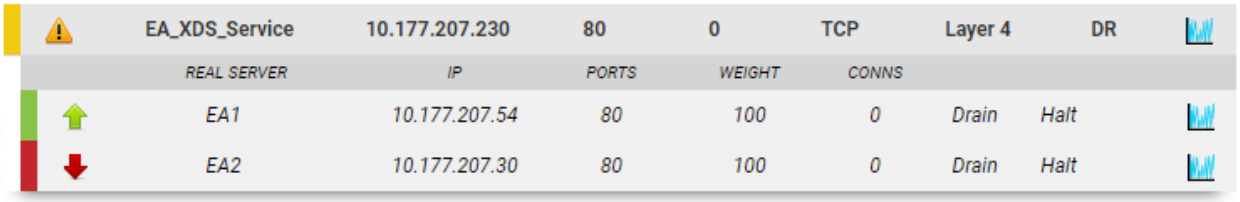
1. Using the WebUI, navigate to: ***Maintenance > Restart Services***.
2. Click **Reload HAProxy**.

10. Testing & Verification

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

The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & RIPs (i.e. the Centricity PACS servers) and shows the state/health of each server as well as the state of each cluster as a whole. The example below shows that all servers are healthy (green) and available to accept connections:

If one of the servers within a cluster fails its health check, that server will be colored red and the cluster will be colored yellow as shown below:



	EA_XDS_Service	10.177.207.230	80	0	TCP	Layer 4	DR	
	REAL SERVER	IP	PORTS	WEIGHT	CONNS			
	EA1	10.177.207.54	80	100	0	Drain	Halt	
	EA2	10.177.207.30	80	100	0	Drain	Halt	

If the services are up (green) verify that clients can connect to the VIPs and access all services.

> **Note** Make sure that DNS points at the VIP rather than individual servers.

Once you have completed the verification process, continue to the next section and add a Secondary appliance to form the HA (active/passive) clustered pair.

11. 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.

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.

11.1. 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:

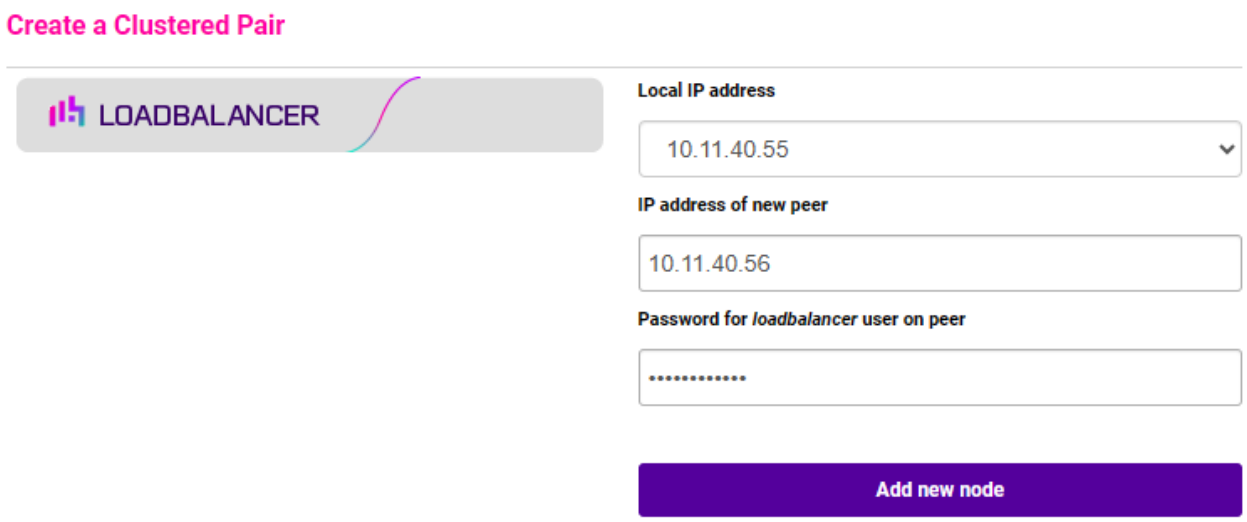
WebUI Main Menu Option	Sub Menu Option	Description
Local Configuration	Hostname & DNS	Hostname and DNS settings
Local Configuration	Network Interface Configuration	Interface IP addresses, bonding configuration and VLANs
Local Configuration	Routing	Default gateways and static routes
Local Configuration	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

WebUI Main Menu Option	Sub Menu Option	Description
Local Configuration	License Key	Appliance licensing
Maintenance	Backup & Restore	Local XML backups
Maintenance	Software Updates	Appliance software updates
Maintenance	Firewall Script	Firewall (iptables) configuration
Maintenance	Firewall Lockdown Wizard	Appliance management lockdown settings

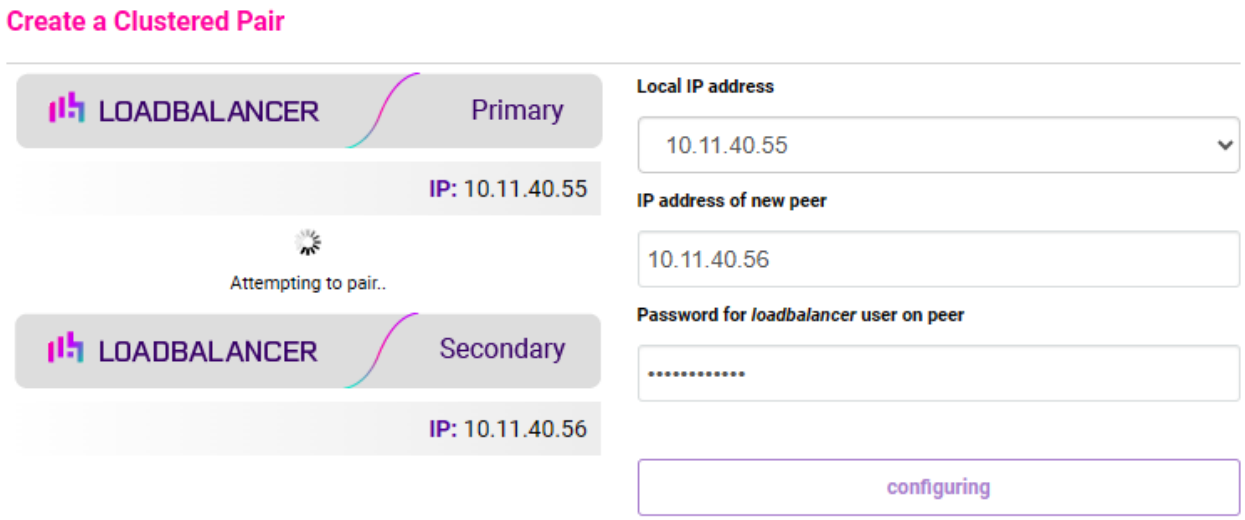
> **Important** Make sure that where any of the above have been configured on the Primary appliance, they're also configured on the Secondary.

11.2. Configuring the HA Clustered Pair

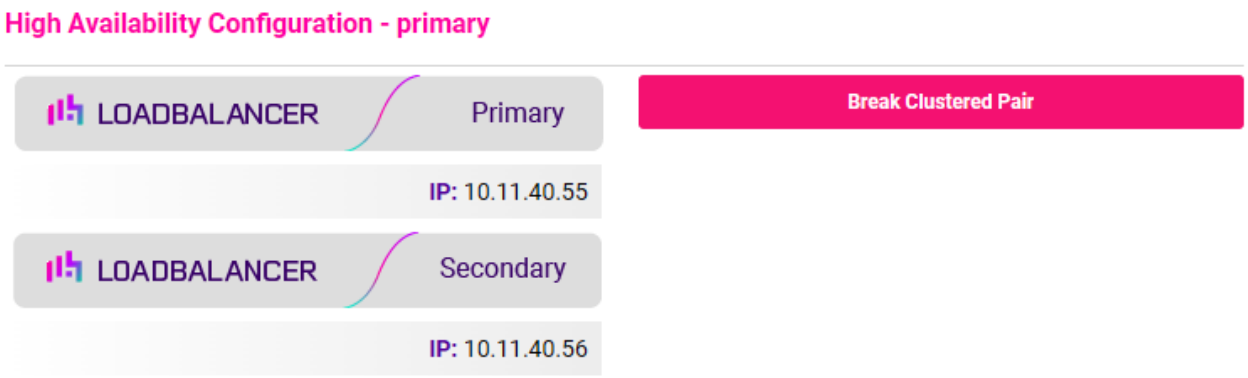
1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI on the Primary appliance, navigate to: ***Cluster Configuration > High-Availability Configuration***.



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.

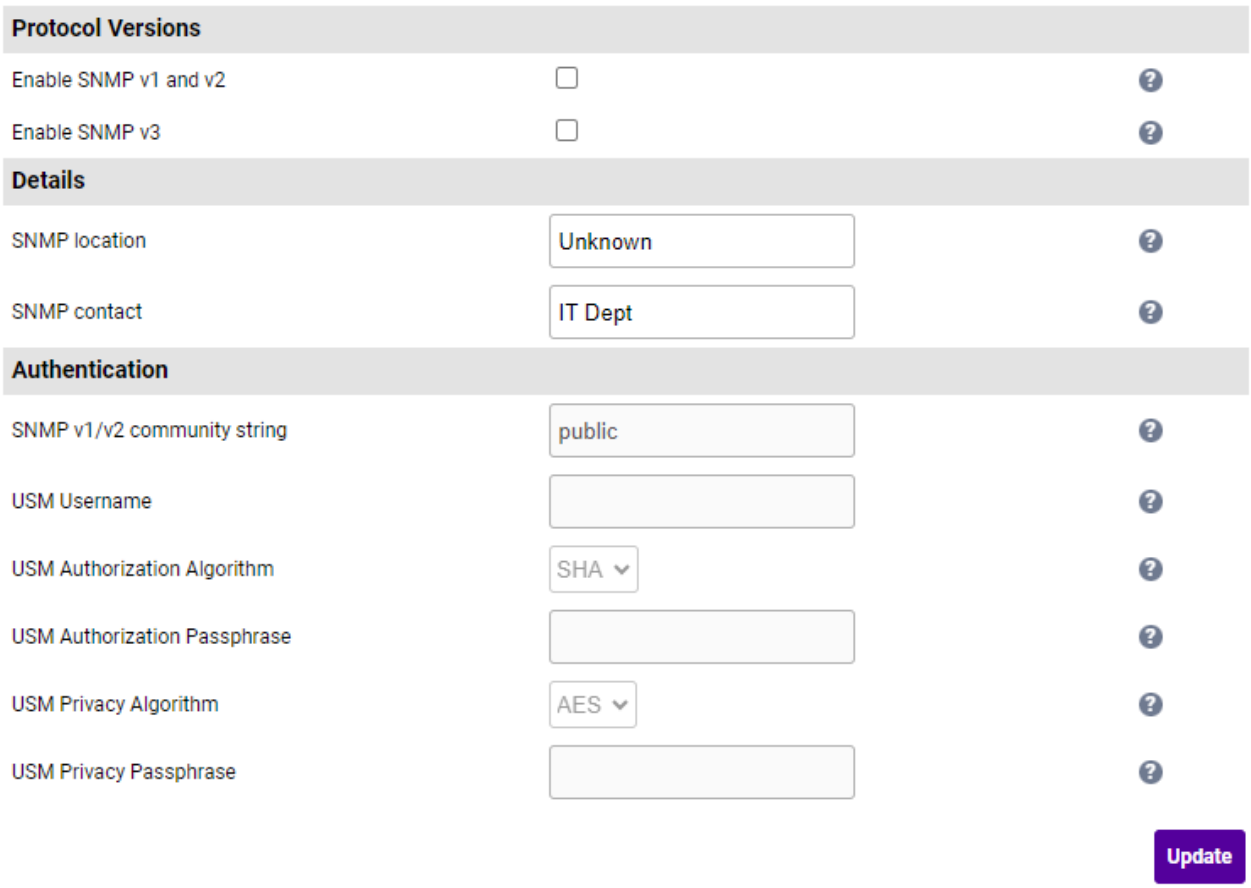
12. Optional Appliance Configuration

12.1. SNMP Configuration

The appliance supports SNMP v1, v2 and v3.

To configure SNMP:

1. Using the WebUI, navigate to: *Local Configuration > SNMP Configuration*.



2. Enable the required SNMP version(s).
3. Enter the required *SNMP location* and *SNMP contact*.
4. For SNMP v1 & v2:
   - Enter the required *SNMP v1/v2 community string*.
5. For SNMP v3:
   - Specify the *USM Username*.
   - Select the required *USM Authorization Algorithm*.
   - Specify the *USM Authorization Passphrase*, it should be at least 8 characters.
   - Select the required *USM Privacy Algorithm*.
   - Specify *USM Privacy Passphrase*, it should be at least 8 characters.
6. Click **Update**.
7. Restart SNMPD using the **Restart SNMPD** button at the top of the screen.

> **Note** Valid characters for the *Community string*, *USM Username*, *USM Authorization Passphrase* and *USM Privacy Passphrase* fields are: **a-z A-Z 0-9 [ ] # ~ _ * ! = - $ % ? { } @ : ; ^**

> **Note** For more information about the various OIDs and associated MIBs supported by the appliance, please refer to SNMP Reporting.

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

12.2. Configuring Email Alerts for Virtual Services

Email alerts can be configured for layer 4 and layer 7 Virtual Services. This enables emails to be sent when one or more of the associated Real Servers fail their health check and also when they subsequently start to pass their health check.

12.2.1. Layer 4

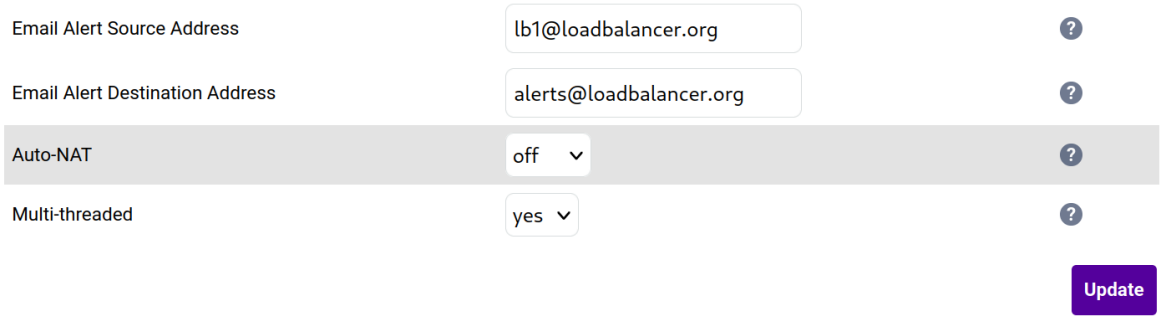
For layer 4 Virtual Services, settings can be configured globally for all VIPs or individually per VIP.

12.2.1.1. Global Layer 4 Email Settings

Once configured, these settings apply to all layer 4 VIPs by default.

To configure global email alert settings for layer 4 services:

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 Advanced Configuration*.



2. Enter an appropriate email address in the *Email Alert Source Address* field.

```
e.g. lb1@loadbalancer.org
```

3. Enter an appropriate email address in the *Email Alert Destination Address* field.

```
e.g. alerts@loadbalancer.org
```

4. Click **Update**.

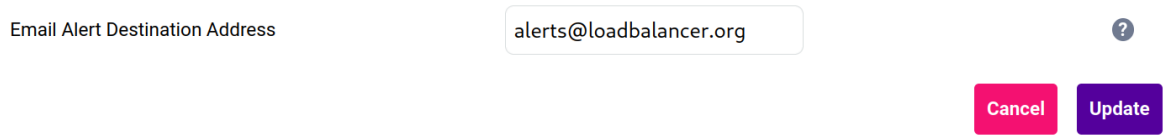
12.2.1.2. VIP Level Settings

> **Note** VIP level settings override the global settings.

Once configured, these settings apply to the individual VIP.

To configure VIP level email alerts:

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 Virtual Service* and click **Modify** next to the VIP to be configured.
2. Scroll down to the *Fallback Server* section.



3. Enter an appropriate email address in the *Email Alert Destination Address* field.

```
e.g. alerts@loadbalancer.org
```

4. Click **Update**.

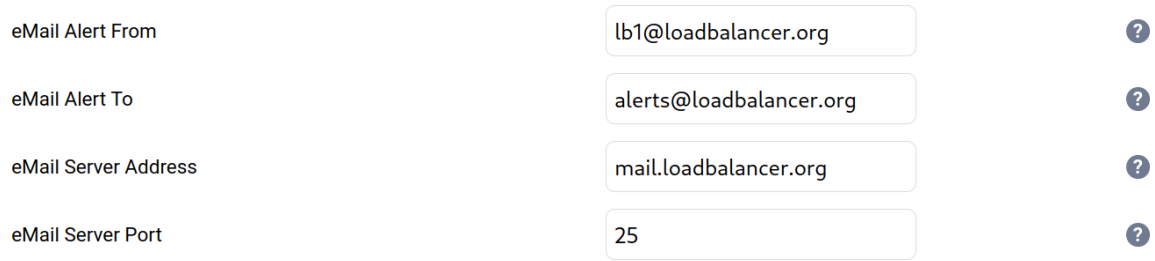
> **Note** You can set the *Email Alert Source Address* field as explained above if required to configure a default source address.

12.2.2. Layer 7

For layer 7 services, email settings are configured globally for all VIPs.

To configure global email alert settings for layer 7 services:

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 Advanced Configuration*.



2. Enter an appropriate email address in the *eMail Alert From* field.

```
e.g. lb1@loadbalancer.org
```

3. Enter an appropriate email address in the *eMail Alert To* field.

```
e.g. alerts@loadbalancer.org
```

4. Enter an appropriate IP address/FQDN in the *eMail Server Address* field.

```
e.g. mail.loadbalancer.org
```

5. Enter an appropriate port in the *eMail Server Port* field.

```
e.g. 25
```

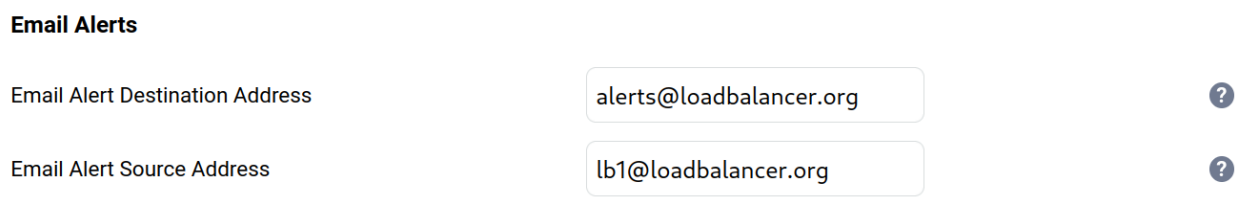
6. Click **Update**.

12.3. Configuring Email Alerts for Heartbeat

Email alerts can be setup for heartbeat once a clustered pair has been configured. This enables alerts to be sent when the primary/secondary communication state has changed. This can occur when the secondary appliance takes over from the primary, when the primary takes over from the secondary and also when there is a communication issue between the 2 appliances.

To configure email alert settings for Heartbeat:

1. Using the WebUI, navigate to: *Cluster Configuration > Heartbeat Configuration*.
2. Scroll down to the **Email Alerts** section.



3. Enter an appropriate email address in the *Email Alert Destination Address* field.
4. Enter an appropriate email address in the *Email Alert Source Address* field.
5. Click **Modify Heartbeat Configuration**.

12.4. Configuring a Smart Host (SMTP relay)

For Heartbeat (and layer 4 services), email alerts are sent from the load balancer directly to the mail server defined in the destination domain's DNS MX record by default. Alternatively, a custom smart host (mail relay server) can be specified. A smart host is an email server through which approved devices can send emails. Where possible, we recommend that you use a smart host for email alerts as this often helps improve the deliverability of emails.

To configure a Smart Host:

1. Using the WebUI, navigate to: *Local Configuration > Physical - Advanced Configuration*.
2. Scroll down to the *SMTP Relay* section.

3. Specify the FQDN or IP address of the *Smart Host*.
4. Click **Update**.

> **Note** By default the *Smart Host* is set as the destination email domain's DNS MX record when the *Email Alert Destination Address* is configured. It must either be left at its default setting or a custom smart host must be configured to enable email alerts to be sent.

13. Technical Support

If you require any assistance please contact support@loadbalancer.org.

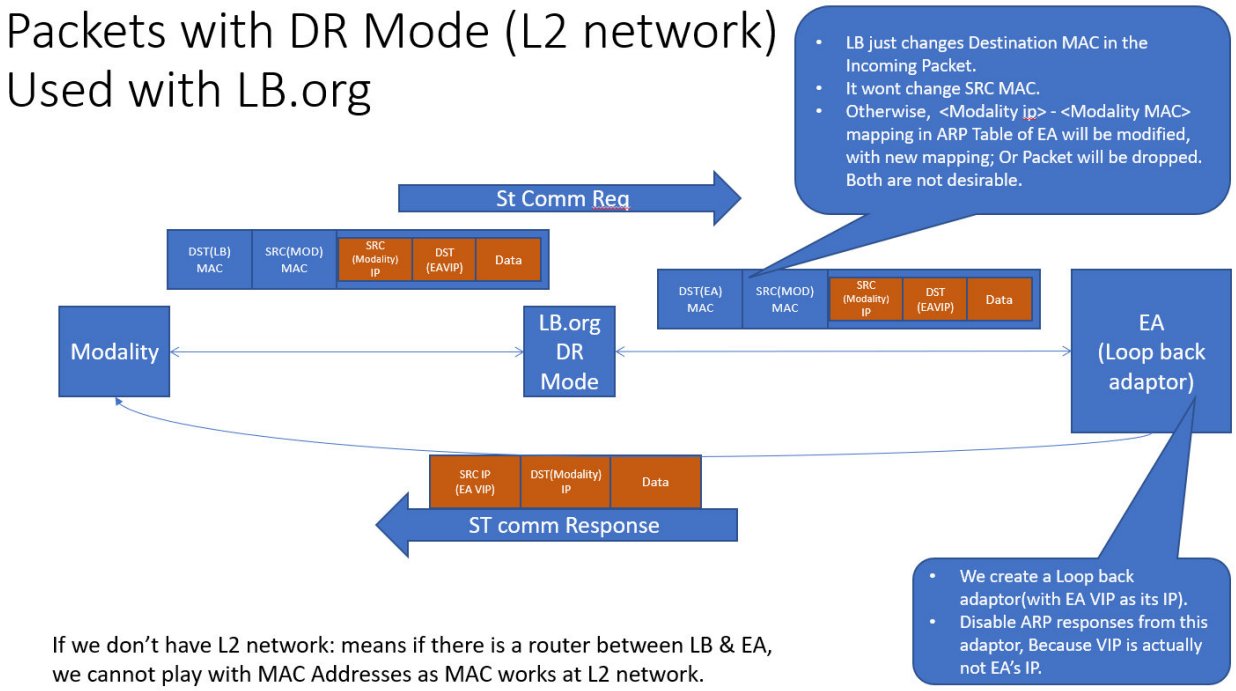
14. Further Documentation

For additional information, please refer to the Administration Manual.

15. Appendix

15.1. DR Mode Packet Manipulation

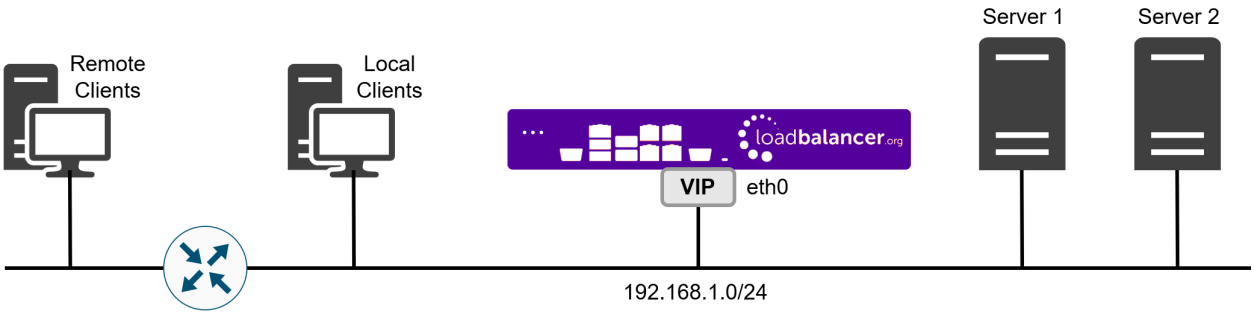
The following diagram shows the traffic flow between the load balancer, the load balanced backend servers and the Modality and how the destination MAC address is modified.



15.2. Enabling Layer 7 Transparency

If you require the source IP address of the client to be seen by the Centricity PACS servers, TProxy must be enabled. When TProxy is enabled, it's important to be aware of the topology requirements for TProxy to operate correctly. Both one-arm and two-arm topologies are supported:

15.2.1. TProxy Topology Requirements - One-arm Deployments

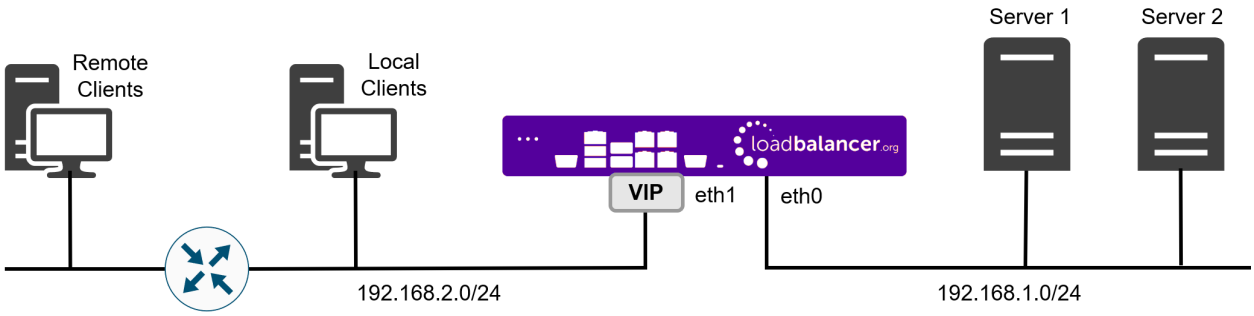


- Here, the VIP is brought up in the same subnet as the Real Servers.
- To support remote clients, the default gateway on the Real Servers must be an IP address on the load balancer and routing on the load balancer must be configured so that return traffic is routed back via the router.

> **Note** For an HA clustered pair, a floating IP should be added to the load balancer and used as the Real Server's default gateway. This ensures that the IP address can "float" (move) between Primary and Secondary appliances.

- To support local clients, return traffic would normally be sent directly to the client bypassing the load balancer which would break TProxy. To address this, the routing table on the Real Servers must be modified to force return traffic to go via the load balancer in the same way as one-arm NAT mode. For more information please refer to One-Arm (Single Subnet) NAT Mode.

15.2.2. TProxy Topology Requirements - Two-arm Deployments



- Here, 2 subnets are used. The VIP is located in one subnet and the load balanced Real Servers are located in the other. The load balancer requires 2 interfaces, one in each subnet.

> **Note** This can be achieved by using two network adapters, or by creating VLANs on a single adapter.

- The default gateway on the Real Servers must be an IP address on the load balancer.

> **Note** For an HA clustered pair, a floating IP should be added to the load balancer and used as the Real Server's default gateway. This ensures that the IP address can "float" (move) between Primary and Secondary appliances.

- Clients can be located in the same subnet as the VIP or any remote subnet provided they can route to the VIP.

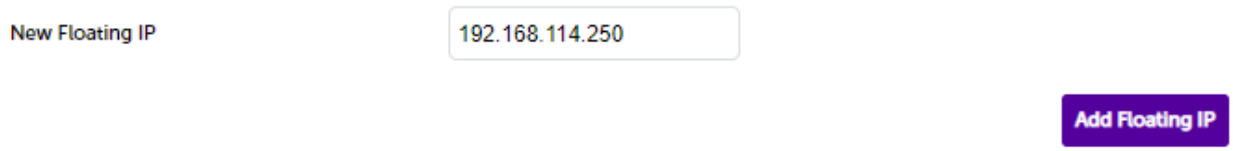
To enable TProxy for a particular layer 7 VIP:

- Click **Modify** next to the HAProxy VIP.
- Scroll down to the **Other** section and click **[Advanced]**.
- Enable (check) *Transparent Proxy*.
- Click **Update**.

15.2.3. Configuring a floating IP Address for the Centricity PACS Server's Default Gateway

For layer 7 SNAT mode with transparency, a floating IP address is used as the default gateway for the Real Servers.

1. Using the Appliance WebUI, navigate to: ***Cluster Configuration > Floating IPs***.
2. Enter the required address in the ***New Floating IP*** field, e.g. **192.168.114.250**.



3. Click **Add Floating IP**.

> **Important** The default gateway of each Centricity PACS Server that is a Real Server for a layer 7 SNAT mode transparent VIP should be set to use this address.

16. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.0	5 November 2025	Initial version		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.