LOADBALANCER

DEPLOYMENT GUIDE

# Load Balancing GE HealthCare Centricity Cardio Workflow

Version 1.2

# Table of Contents

# 1. About this Guide

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

## 1.1. Acronyms Used in the Guide

| Acronym | Description |
|---|---|
| CCW | Centricity Cardio Workflow |
| CCG | Centricity Clinical Gateway |
| CCG_IB | Centricity Clinical Gateway Inbound |
| EMR | Electronic Medical Record |

# 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 CCW servers.
6. Have IP addresses for the VA and all required Virtual Services.
7. Have access to the CCW servers to enable the ARP problem to be solved for Layer 4 DR mode VIPs - for details refer to Configuring CCW for Load Balancing.

# 3. Software Versions Supported

## 3.1. Loadbalancer.org Appliance

- V8.9.0 & later

## 3.2. GE HealthCare CCW

- All versions

# 4. Load Balancing CCW

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

## 4.1. Virtual Services (VIP) Requirements

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

| Reference | VIP Name | Mode | Port(s) | Persistence Mode | Health Check |
|---|---|---|---|---|---|
| VIP 1 | CCW_WEB_443 | L7 SNAT | 443 | Source IP | Connect to Port |
| VIP 2 | CCW_WEB_8443 | L7 SNAT | 8443 | HTTP Cookie | Connect to Port |
| VIP 3 | CCW_WEB_44301 | L7 SNAT | 44301 | Source IP | Connect to Port |
| VIP 4 | CCW_WEB_8070-49200-49201 | L7 SNAT | 8070, 49200, 49201 | Source IP | Connect to Port |
| VIP 5 | CCW_NOTIFICATION | L7 SNAT | 44300 | Last Successful | HTTPS (GET) |
| VIP 6 | CCW_DICOMSERVICE_VS | L4 DR | 104 | None | DICOM C-Echo |
| VIP 7 | CCW_DICOMSERVER_VS | L4 DR | 1230 | None | DICOM C-Echo |
| VIP 8 | CCW_DICOM_1115 | L4 DR | 1115 | None | DICOM C-Echo |
| VIP 9 | CCW_DICOM_1299 | L4 DR | 1299 | None | DICOM C-Echo |
| VIP 10 | EMR_INBOUND | L7 SNAT | 4001 | Last Successful | Connect to Port |
| VIP 11 | PORT_EMR_IB | L7 SNAT | 4002 | Last Successful | Connect to Port |

Additional VIPs required for Centricity Cardio Enterprise:

> **Note** Clicking on the VIP reference will open the relevant page in the Centricity PACS deployment guide.

| Ref. | Remote Ref. | VIP Name | Mode | Port(s) | Persist Mode | Health Check |
|---|---|---|---|---|---|---|
| VIP 12 | VIP 1 | EA_XDS_Service | L4 DR | 80 | None | HTTP (GET) |
| VIP 13 | VIP 11 | UV | L7 SNAT | 443 | Source IP | HTTPS (GET) |
| VIP 14 | VIP 12 | Dakota | L7 SNAT | SP1: 8080, SP2: 8443 | Source IP | SP1: Connect to port, SP2: HTTPS (GET) |

Additional VIPs required for True PACS Card Solution:

> **Note** Clicking on the VIP reference will open the relevant page in the Centricity PACS deployment guide or for VIP 20, the Datalogue deployment guide.

| Ref. | Remote Ref. | VIP Name | Mode | Port(s) | Persist Mode | Health Check |
|---|---|---|---|---|---|---|
| VIP 15 | VIP 1 | EA_XDS_Service | L4 DR | 80 | None | HTTP (GET) |
| VIP 16 | VIP 11 | UV | L7 SNAT | 443 | Source IP | HTTPS (GET) |
| VIP 17 | VIP 12 | Dakota | L7 SNAT | SP1: 8080, SP2: 8443 | Source IP | SP1: Connect to port, SP2: HTTPS (GET) |
| VIP 18 | VIP 13 | WFM_Play_Group | L7 SNAT | 8080 | Source IP | HTTPS (GET) |
| VIP 19 | VIP 14 | WFM_tomcat_Group | L7 SNAT | SP1: 8080, SP2: 9443 | Source IP | HTTPS (GET) |
| VIP 20 | VIP 16 | ZFP | L7 SNAT | 443 | Source IP | HTTPS (GET) |

Additional VIPs required for WFC Services:

> **Note** Clicking on the VIP reference will open the relevant page in the TRUE PACS deployment guide.

| Ref. | Remote Ref. | VIP Name | Mode / Type | Port(s) | Persist Mode | Health Check |
|---|---|---|---|---|---|---|
| VIP 21 | VIP 1 | WFC_RMQAMQP | L7 SNAT | 8081 | None | Connect to Port |
| VIP 22 | VIP 2 | WFC_443 | L7 SNAT | 8443 | None | No Checks, Always On |
| VIP 23 | VIP 2-B1 | WFC_inference_443 | Backend Only | - | None | HTTPS (GET) |
| VIP 24 | VIP 2-B2 | WFC_profiling_443 | Backend Only | - | None | HTTPS (GET) |
| VIP 25 | VIP 2-B3 | WFC_patient_443 | Backend Only | - | None | HTTPS (GET) |
| VIP 26 | VIP 2-B4 | WFC_CCS_443 | Backend Only | - | None | HTTPS (GET) |
| VIP 27 | VIP 2-B5 | WFC_auth_443 | Backend Only | - | None | HTTPS (GET) |
| VIP 28 | VIP 2-B6 | WFC_outboundhl7_443 | Backend Only | - | None | HTTPS (GET) |
| VIP 29 | VIP 2-B7 | WFC_inboundnotification_443 | Backend Only | - | None | HTTPS (GET) |
| VIP 30 | VIP 2-B8 | WFC_eventnotificationmanager_443 | Backend Only | - | None | HTTPS (GET) |
| VIP 31 | VIP 2-B9 | WFC_outboundeventpolling_443 | Backend Only | - | None | HTTPS (GET) |

| Ref. | Remote Ref. | VIP Name | Mode / Type | Port(s) | Persist Mode | Health Check |
|---|---|---|---|---|---|---|
| VIP 32 | VIP 2-B10 | WFC_metadata_443 | Backend Only | - | None | HTTPS (GET) |
| VIP 33 | VIP 2-B11 | WFC_studymanagement_443 | Backend Only | - | None | HTTPS (GET) |
| VIP 34 | VIP 2-B12 | WFC_xe_443 | Backend Only | - | None | HTTPS (GET) |
| VIP 35 | VIP 2-B13 | WFC_recordmanager_443 | Backend Only | - | None | HTTPS (GET) |
| VIP 36 | VIP 3 | WFC_http | L7 SNAT | 80 | None | No Checks, Always On |
| VIP 37 | VIP 3-B1 | WFC_inference_80 | Backend Only | - | None | HTTPS (GET) |
| VIP 38 | VIP 3-B2 | WFC_profiling_80 | Backend Only | - | None | HTTPS (GET) |
| VIP 39 | VIP 3-B3 | WFC_CCS_80 | Backend Only | - | None | HTTPS (GET) |
| VIP 40 | VIP 3-B4 | WFC_auth_80 | Backend Only | - | None | HTTPS (GET) |
| VIP 41 | VIP 3-B5 | WFC_outboundeventpolling_80 | Backend Only | - | None | HTTPS (GET) |
| VIP 42 | VIP 3-B6 | WFC_inboundnotification_80 | Backend Only | - | None | HTTPS (GET) |
| VIP 43 | VIP 3-B7 | WFC_eventnotificationmanager_80 | Backend Only | - | None | HTTPS (GET) |
| VIP 44 | VIP 3-B8 | WFC_metadata_80 | Backend Only | - | None | HTTPS (GET) |
| VIP 45 | VIP 3-B9 | WFC_patient_80 | Backend Only | - | None | HTTPS (GET) |
| VIP 46 | VIP 3-B10 | WFC_masterfileapp_80 | Backend Only | - | None | HTTPS (GET) |
| VIP 47 | VIP 3-B11 | WFC_masterfiledata_80 | Backend Only | - | None | HTTPS (GET) |
| VIP 48 | VIP 3-B12 | WFC_studymanagement_80 | Backend Only | - | None | HTTPS (GET) |
| VIP 49 | VIP 3-B13 | WFC_xe_80 | Backend Only | - | None | HTTP (GET) |
| VIP 50 | VIP 4 | WFC_10443 | L7 SNAT | 8082 | None | Connect to Port |

| Ref. | Remote Ref. | VIP Name | Mode / Type | Port(s) | Persist Mode | Health Check |
|---|---|---|---|---|---|---|
| VIP 51 | VIP 4-B1 | WFC_masterfiledata_10443 | Backend Only | - | None | HTTPS (GET) |
| VIP 52 | VIP 4-B2 | WFC_masterfileapp_10443 | Backend Only | - | None | HTTPS (GET) |
| VIP 53 | VIP 4-B3 | WFC_xeui_10443 | Backend Only | - | None | HTTP (GET) |
| VIP 54 | VIP 5 | WFM_karaf_Group | L7 SNAT | 9094 | Source IP | HTTPS (GET) |

### 4.2. Last Successful Persistence

With this persistence mode, traffic will always be sent to the same server until that server fails. When used together with the **First** scheduler, traffic will initially always be sent to the first server in the list. If the first server fails, traffic will then be sent to the second server in the list, etc. When the first server is brought back on-line, traffic will continue to be sent to the second server until either the stick table is cleared or the second server is halted.

> **Note** For details on how to clear a stick table, please refer to Last Successful - Clearing the Stick Table.

## 5. Ports Used by the Appliance

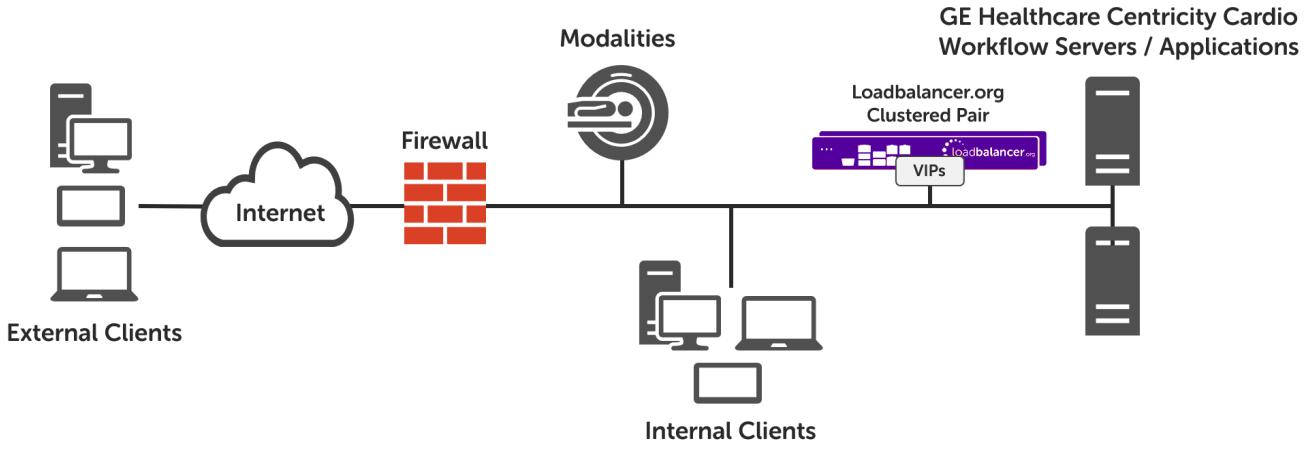
By default, the appliance uses the following TCP & UDP ports:

| 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



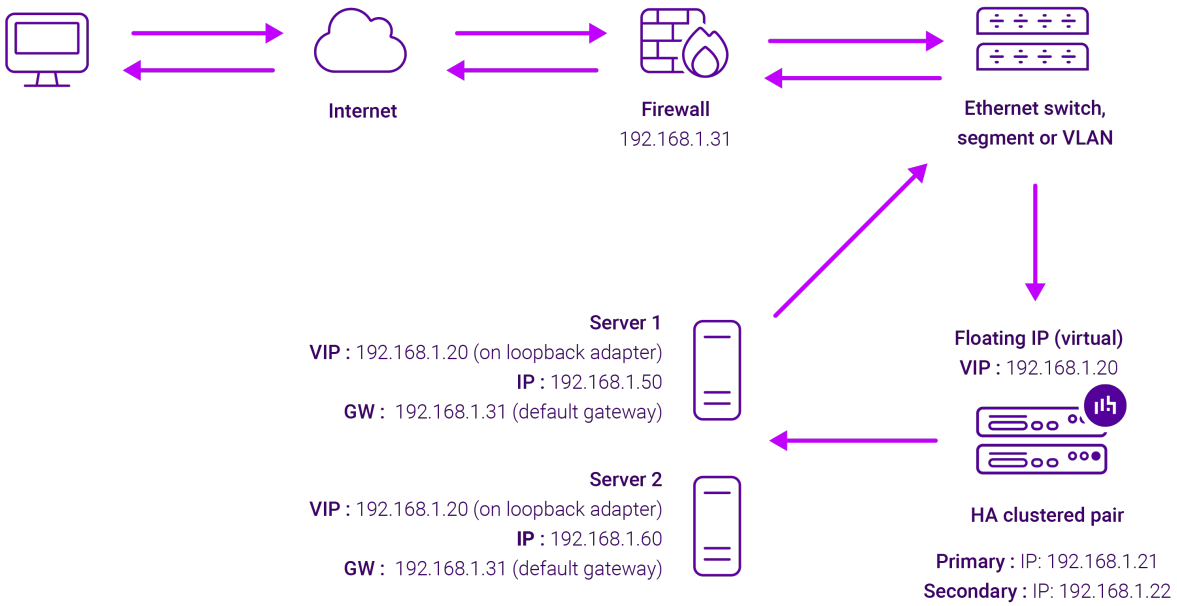

# 7. Load Balancer Deployment Methods

For CCW, 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*.

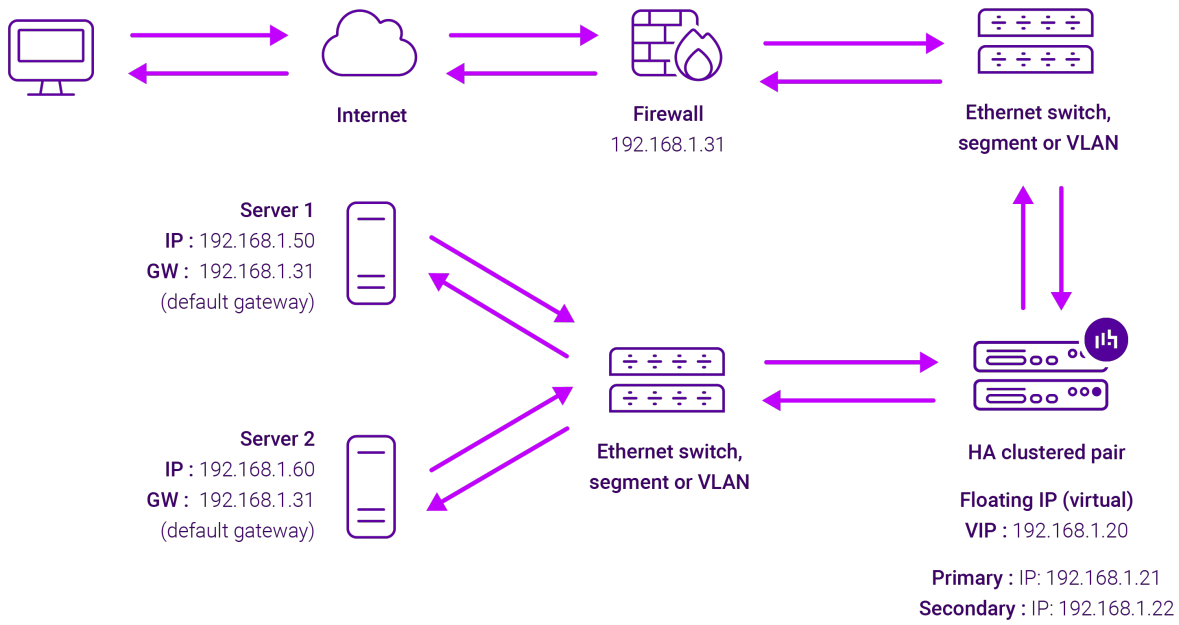


- DR mode works by changing the destination MAC address of the incoming packet to match the selected Real Server on the fly which is very fast.
- When the packet reaches the Real Server it expects the Real Server to own the Virtual Services IP address (VIP). This means that each Real Server (and the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

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

- VIP 6 - **CCW_DICOMSERVICE_VS**
- VIP 7 - **CCW_DICOMSERVER_VS**
- VIP 8 - **CCW_DICOM_1115**
- VIP 9 - **CCW_DICOM_1299**

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

### 8.2.1. Windows Server 2012 & Later

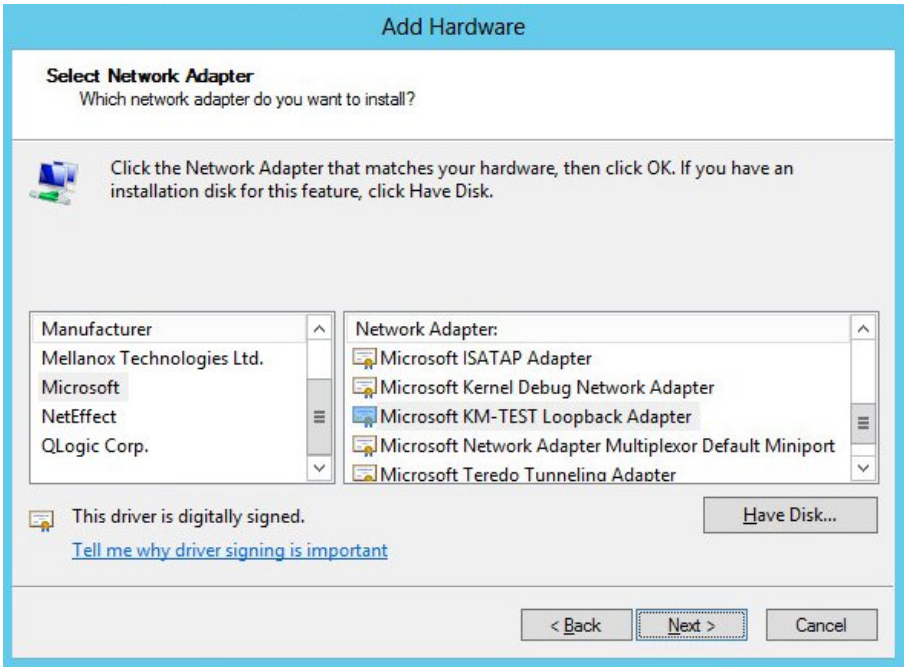
Windows Server 2012 and later support Direct Routing (DR) mode through the use of the Microsoft Loopback Adapter that must be installed and configured on each load balanced (Real) Server. The IP address configured on the Loopback Adapter must be the same as the Virtual Service (VIP) address. This enables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

#### 8.2.1.1. Step 1 of 3: Install the Microsoft Loopback Adapter

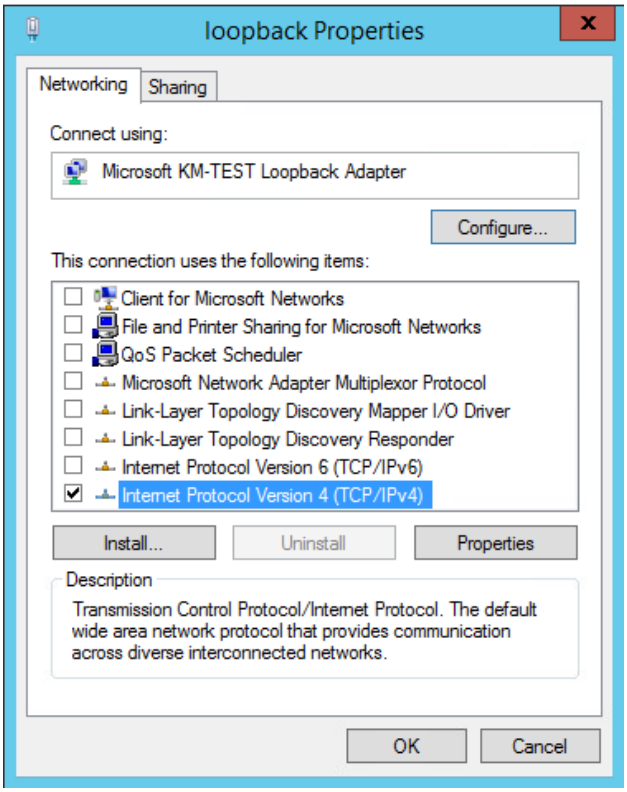
1. Click **Start**, then run **hdwwiz** to start the Hardware Installation Wizard.
2. Once the Wizard has started, click **Next**.
3. Select **Install the hardware that I manually select from a list (Advanced)**, click **Next**.
4. Select **Network adapters**, click **Next**.



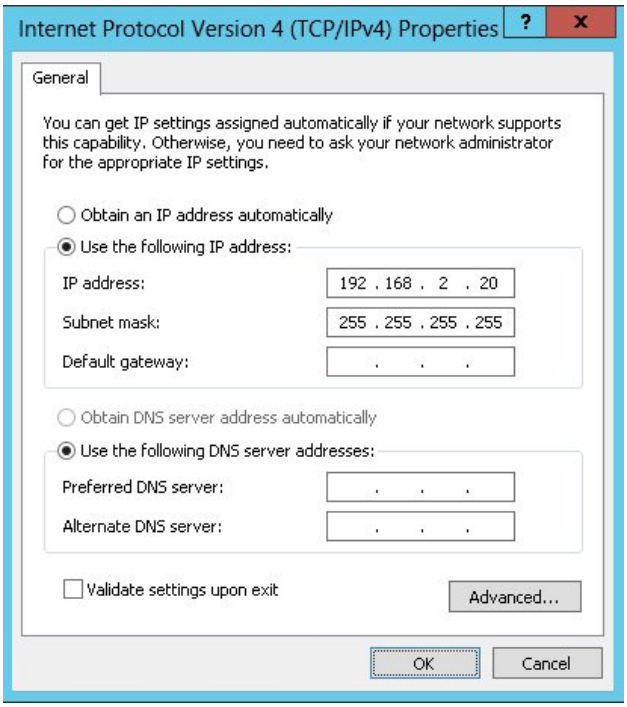

5. Select **Microsoft** & **Microsoft KM-Test Loopback Adapter**, click **Next**.
6. Click **Next** to start the installation, when complete click **Finish**.

### 8.2.1.2. 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.

### 8.2.1.3. 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 CCW

## 9.1. Overview

For CCW 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 9.8.14
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.

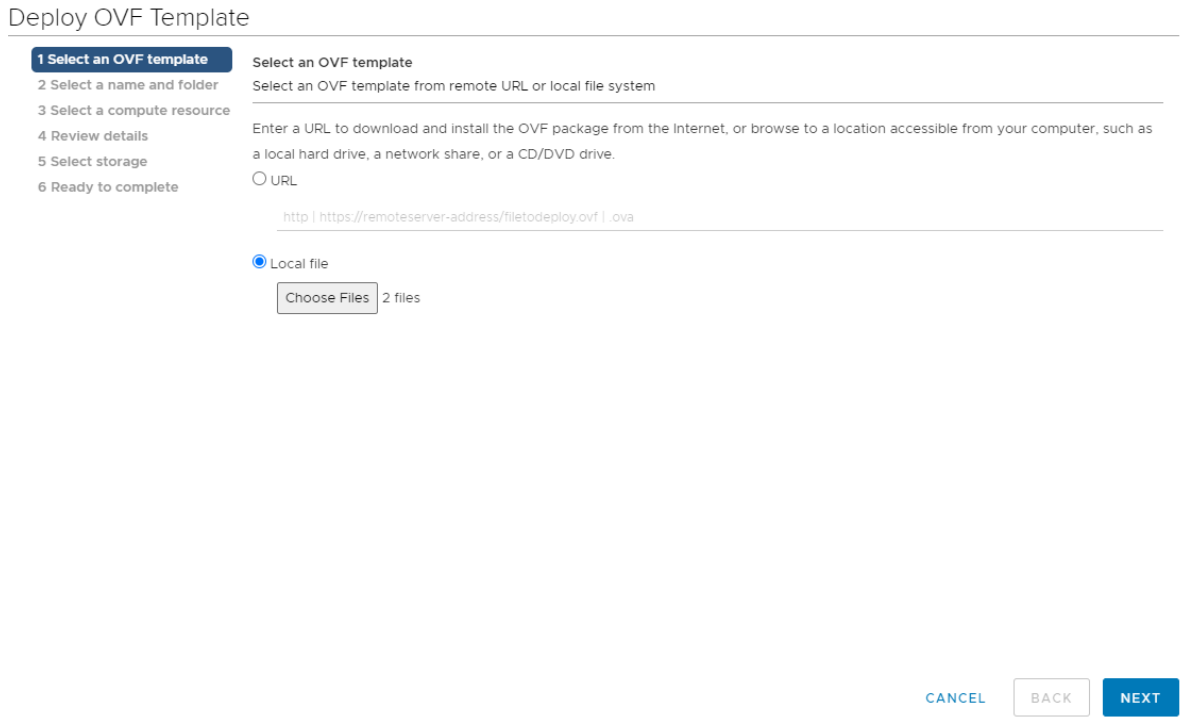
#### 9.2.3.1. Upgrading to the latest Hardware Version

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.

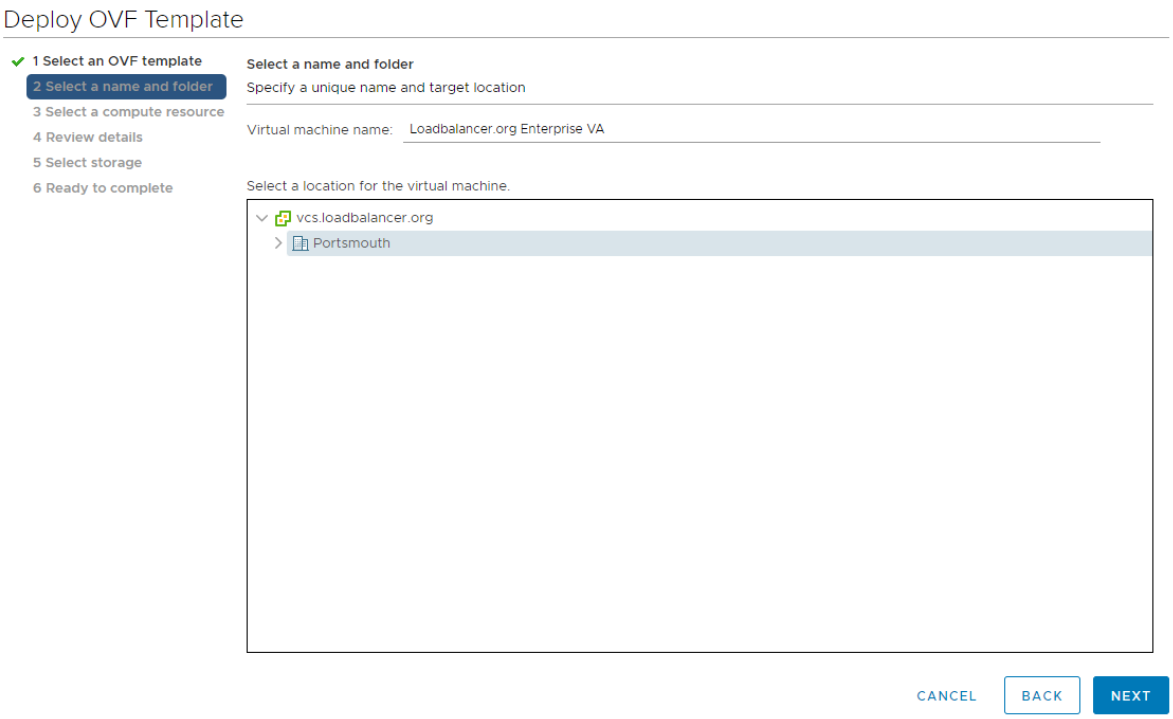
> **Note** Create a snapshot or backup of the virtual machine first before upgrading.

#### 9.2.3.2. Installing the Appliance using vSphere Client

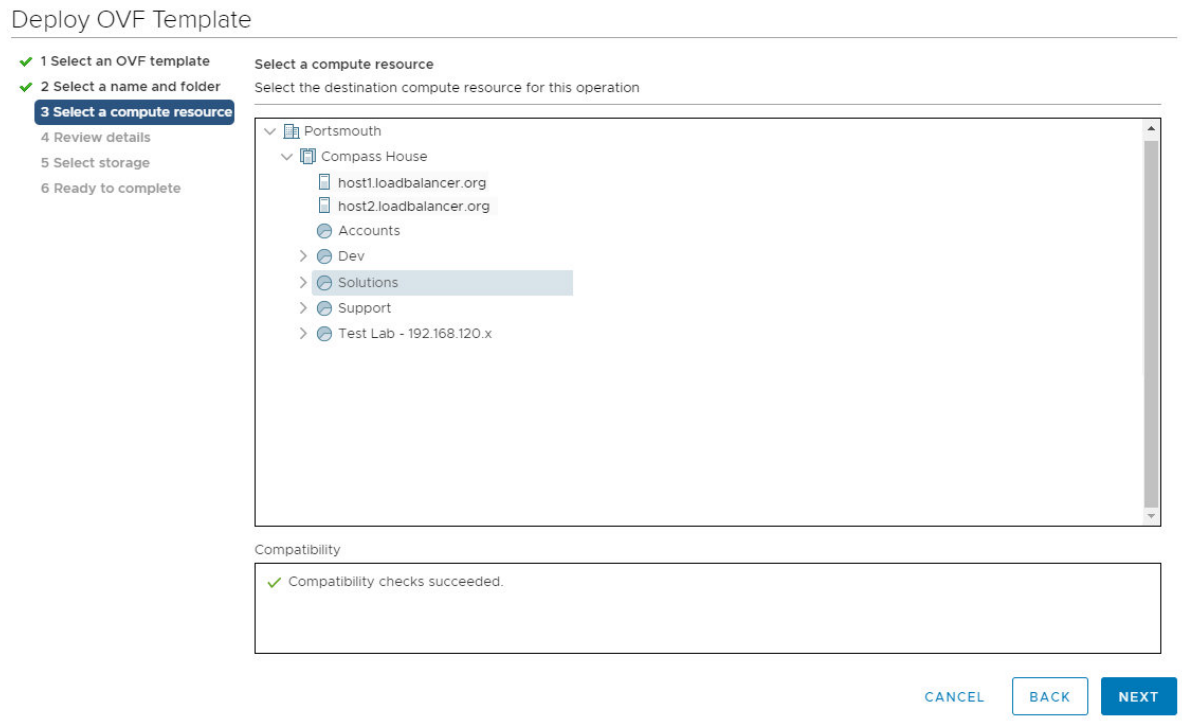
1. Right-click the inventory object where the appliance is to be located and select **Deploy OVF Template**.
2. In the **Select an OVF Template** screen, select the **Local File** option, click **Browse**, navigate to the download location, select the **.ova** file and click **Next**.



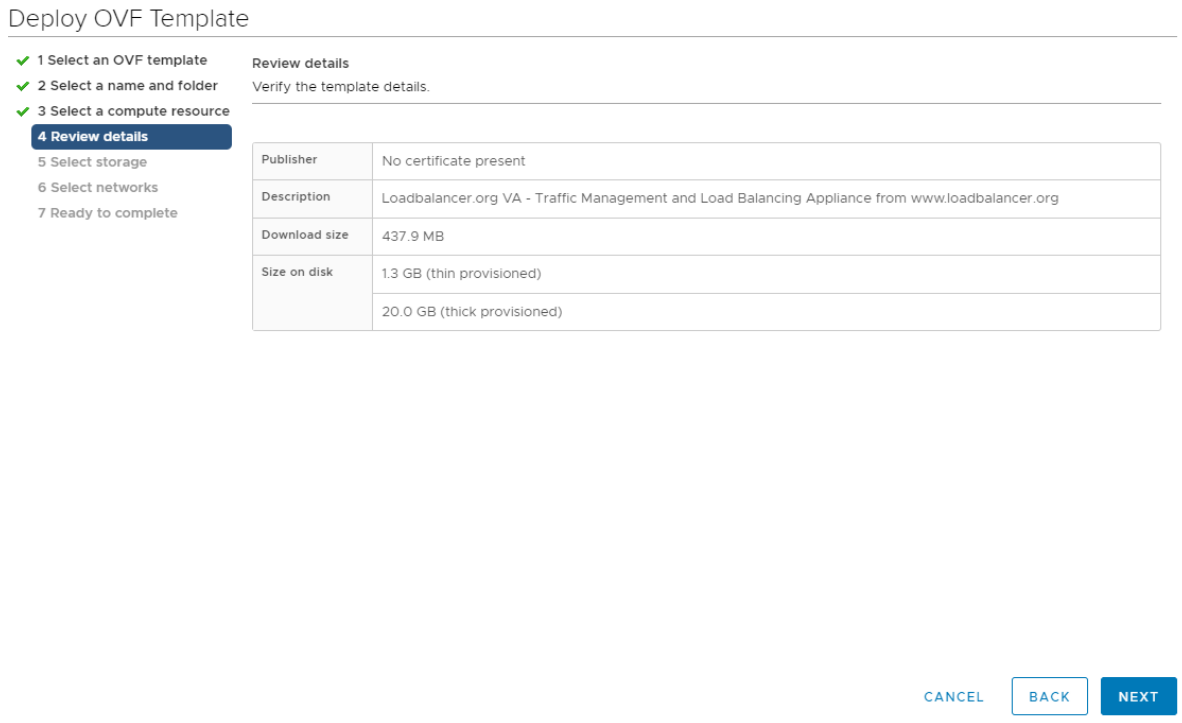

3. In the **Select a name and folder** screen, type a suitable name for the appliance - this can be up to 80 characters in length.
4. Select the required location for the appliance - by default this will be the location of the inventory object from where the wizard was started and click **Next**.




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**.

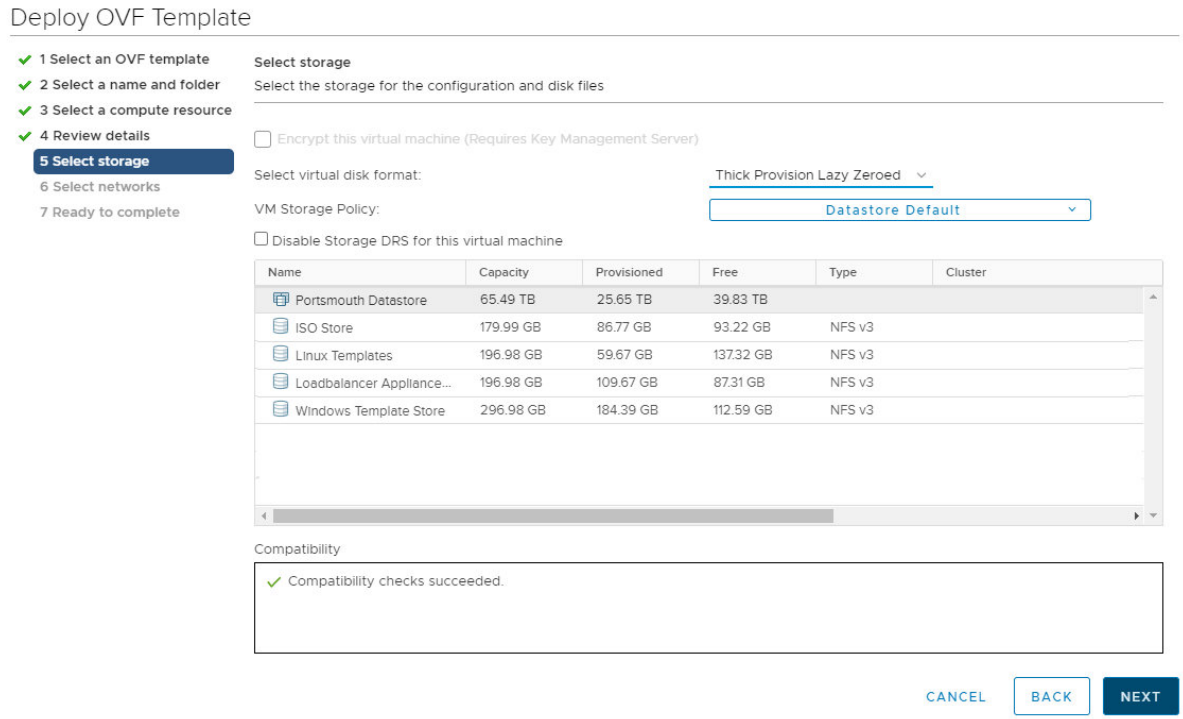



6. In the **Review details** screen, verify the template details and click **Next**.

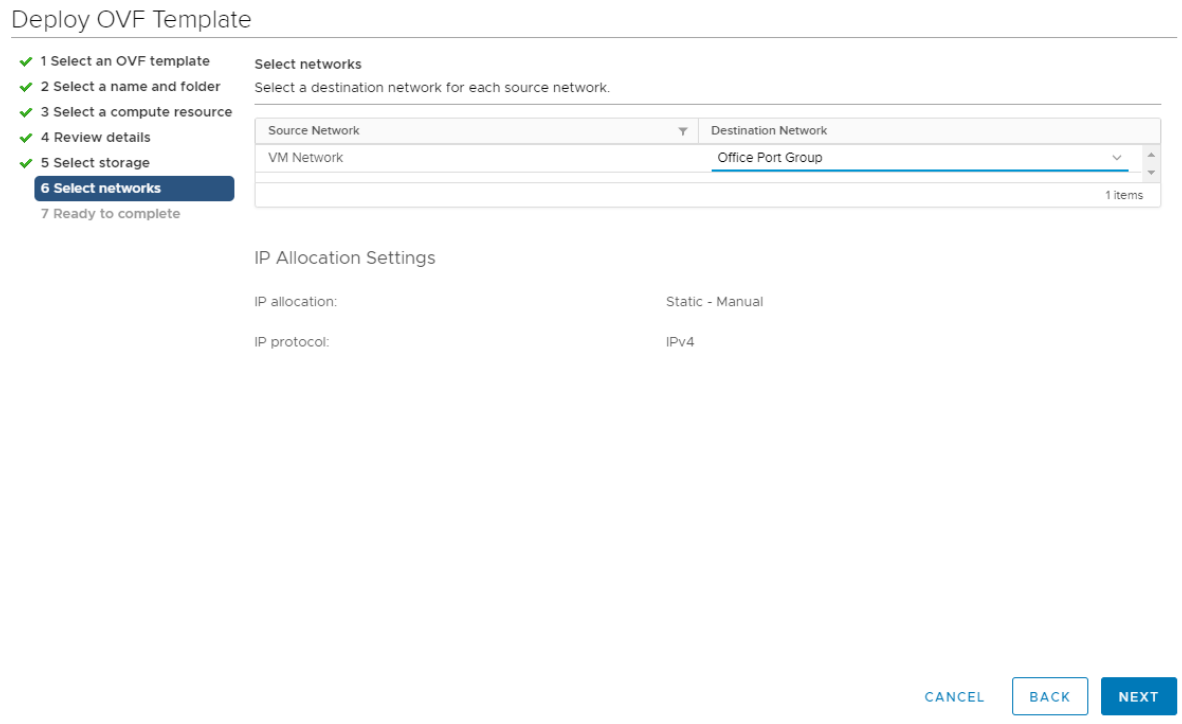



7. In the **Select Storage** screen, first select the required storage location for the appliance.
8. Now select the required disk format and click **Next**.

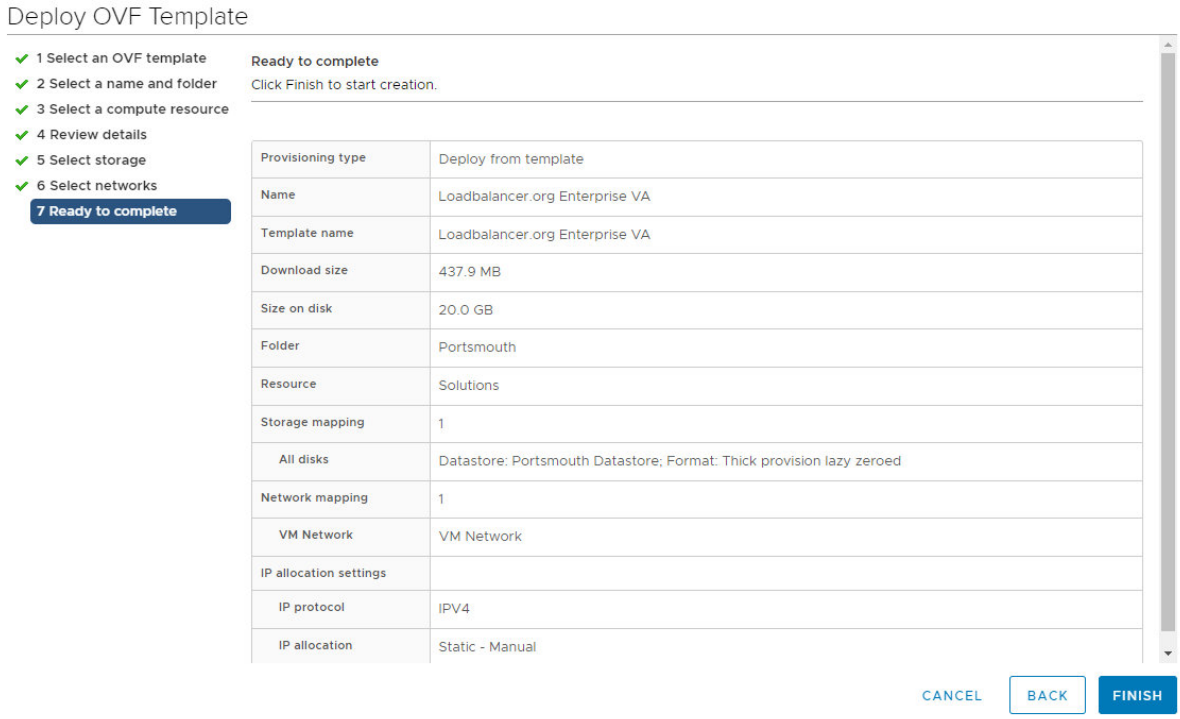
> **Note** Loadbalancer.org recommends selecting a thick provision format. By default the appliance disk is 20GB.




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

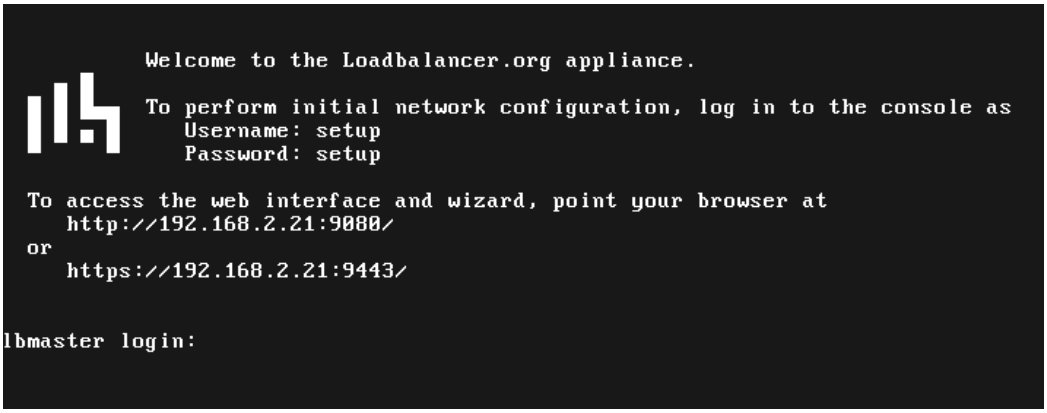
The appliance has 4 network adapters. By default only the first adapter is connected which is the requirement for GE HealthCare deployments. This will be **eth0** when viewed in the appliance WebUI.

### 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.

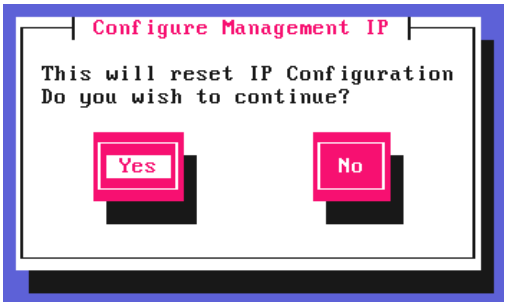
Once logged in, the Network Setup Wizard will start automatically. This will enable you to configure the management IP address and other network settings for the appliance.

login to the console:

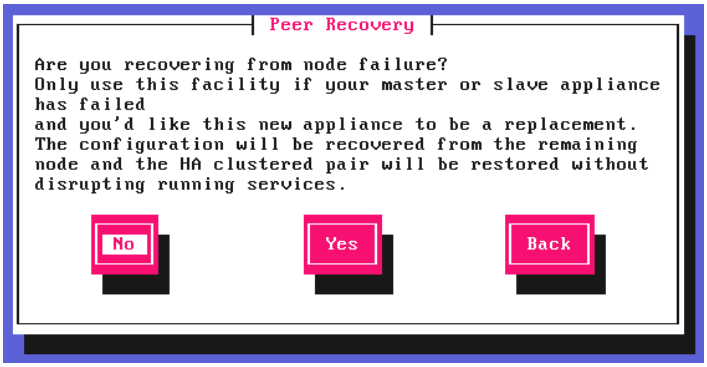
**Username:** setup
**Password:** setup

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

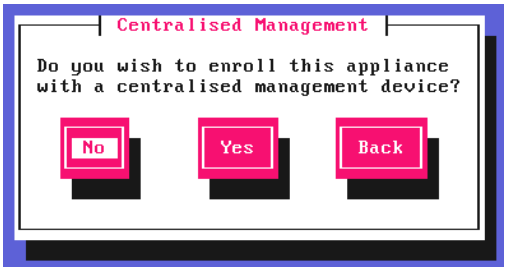
In the **Configure Management IP** screen, leave **Yes** selected and hit **Enter** to continue.




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

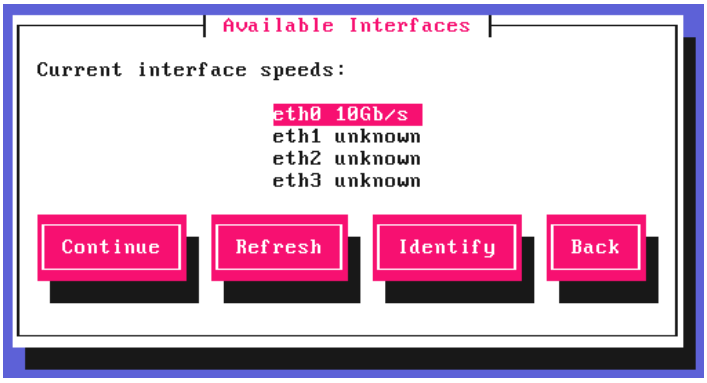



In the **Centralized Management** screen, if you have been provided with Management Server details select **Yes**, otherwise leave **No** selected, then hit **Enter** to continue.

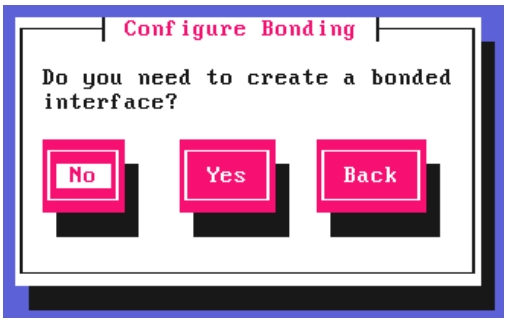



> **Note** For information on how to modify Centralized Management settings via the WebUI, please refer to Portal Management & Appliance Adoption.

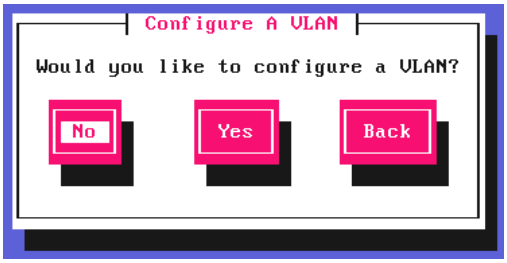
In the **Available Interfaces** screen, a list of available interfaces will be displayed, hit **Enter** to continue.



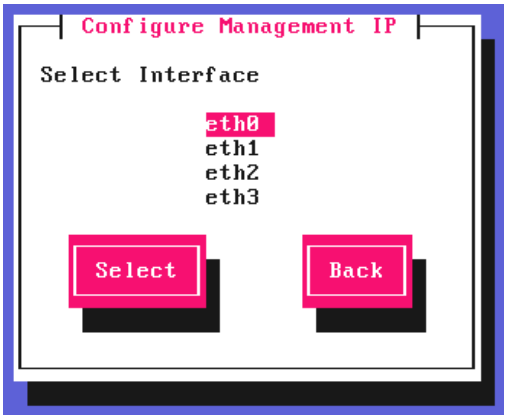

In the **Configure Bonding** screen, leave **No** selected, then hit **Enter** to continue.



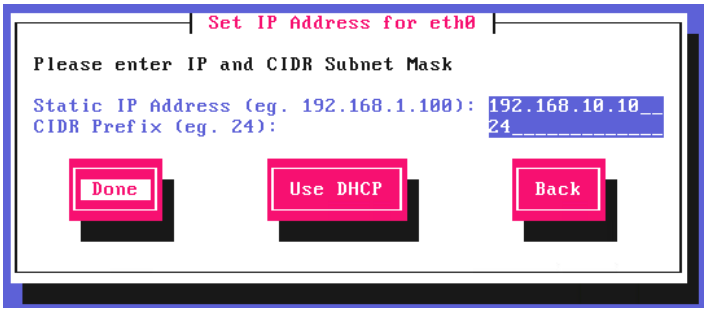

In the **Configure a VLAN** screen, leave **No** selected, then hit **Enter** to continue.




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

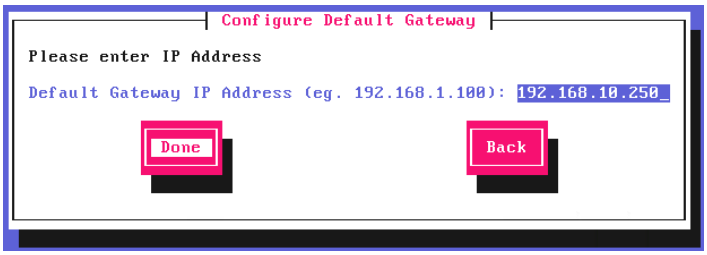



In the **Set IP address** screen, specify the required management address in the *Static IP Address* & *CIDR Prefix* fields, select **Done** and hit **Enter** to continue.

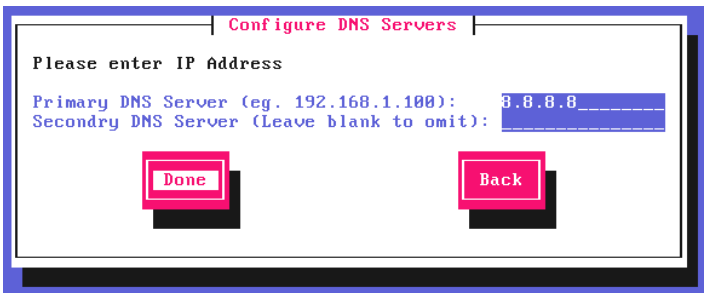



> **Note** A subnet mask such as 255.255.255.0 is not valid, in this case enter 24 instead.

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

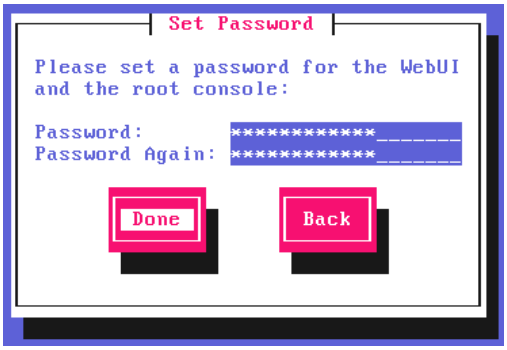



In the **Configure DNS Servers** screen, configure the required DNS server(s), select **Done** and hit **Enter** to continue.

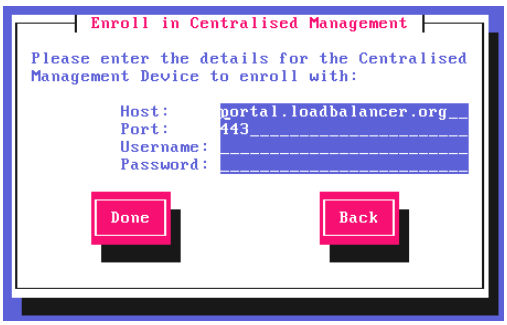



In the **Set Password** screen, hit **Enter** to continue.


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.

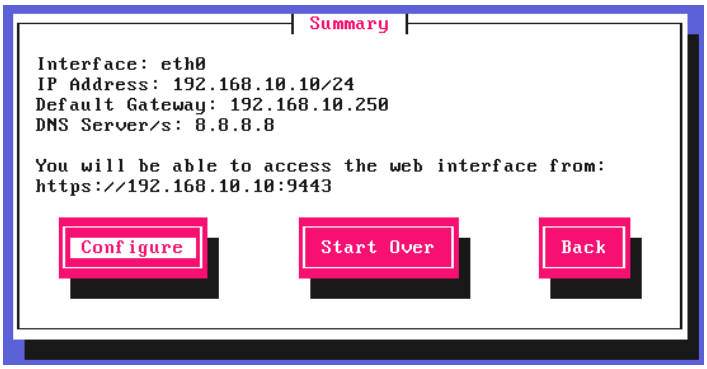



If you selected **Yes** when asked if you want to enroll for Centralized Management, you'll now be prompted for the details. Default values for the *Host* and *Port* are set and can be changed if required. Enter the *Username* and *Password* for the management server account you'd like the appliance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

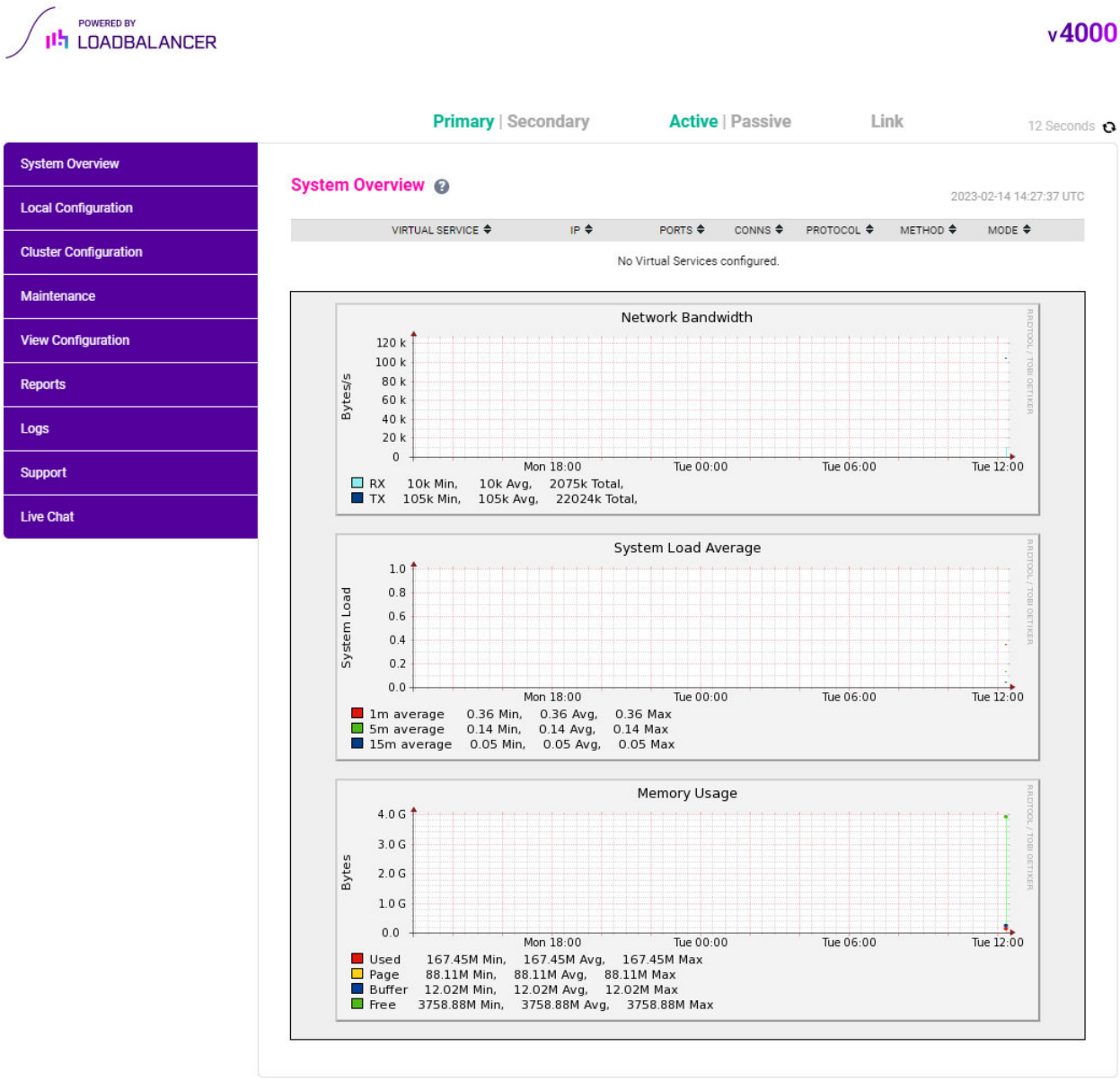
   > **Note** If you need to change the port, IP address or protocol that the WebUI listens on, please refer to Service Socket Addresses.

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

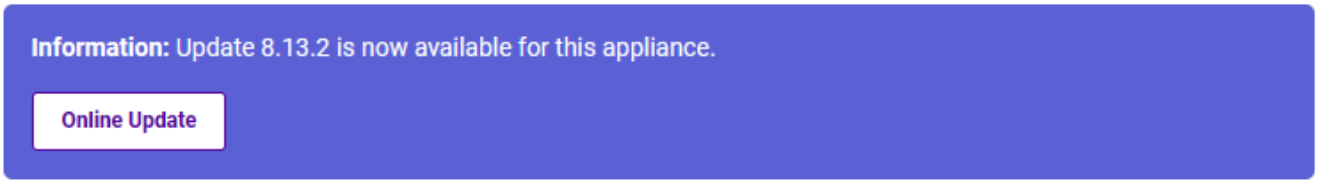
We recommend that the appliance is kept up to date to ensure that you benefit from the latest bug fixes, security updates and feature improvements. Both online and offline update are supported.

> **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

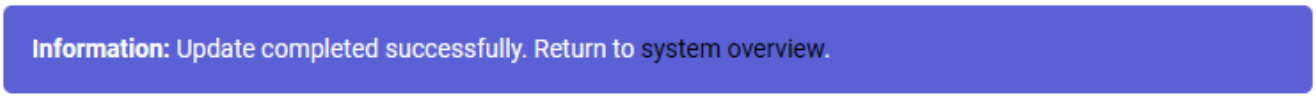
The appliance periodically contacts the Loadbalancer.org update server (**update.loadbalancer.org**) and checks for updates. This is the default behavior and can be disabled if preferred. If an update is found, a notification similar to the example below will be displayed at the top of the WebUI:




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.

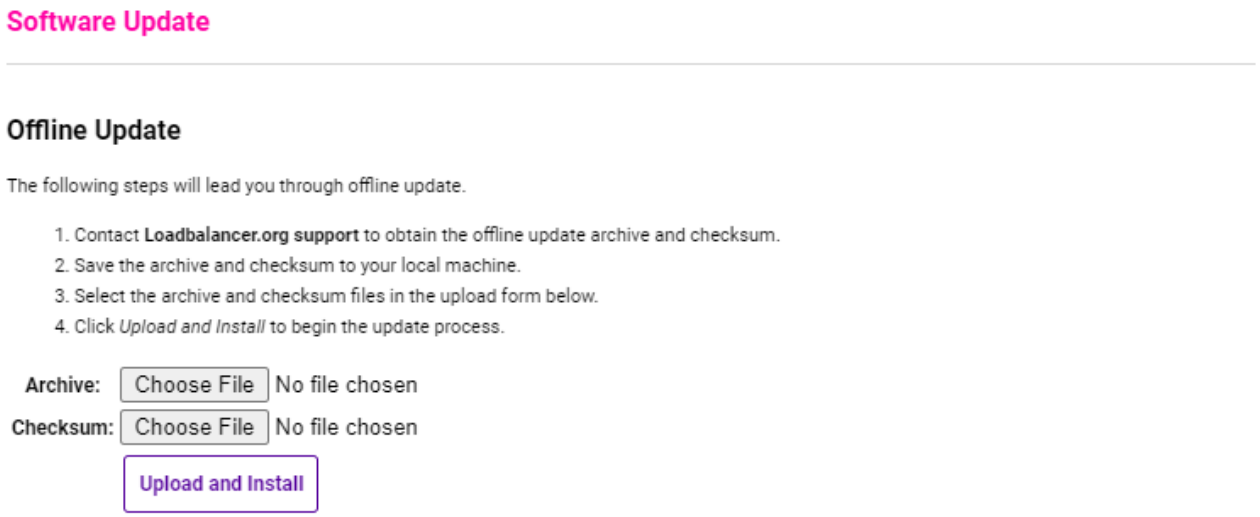
### 9.5.2. Offline Update

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:

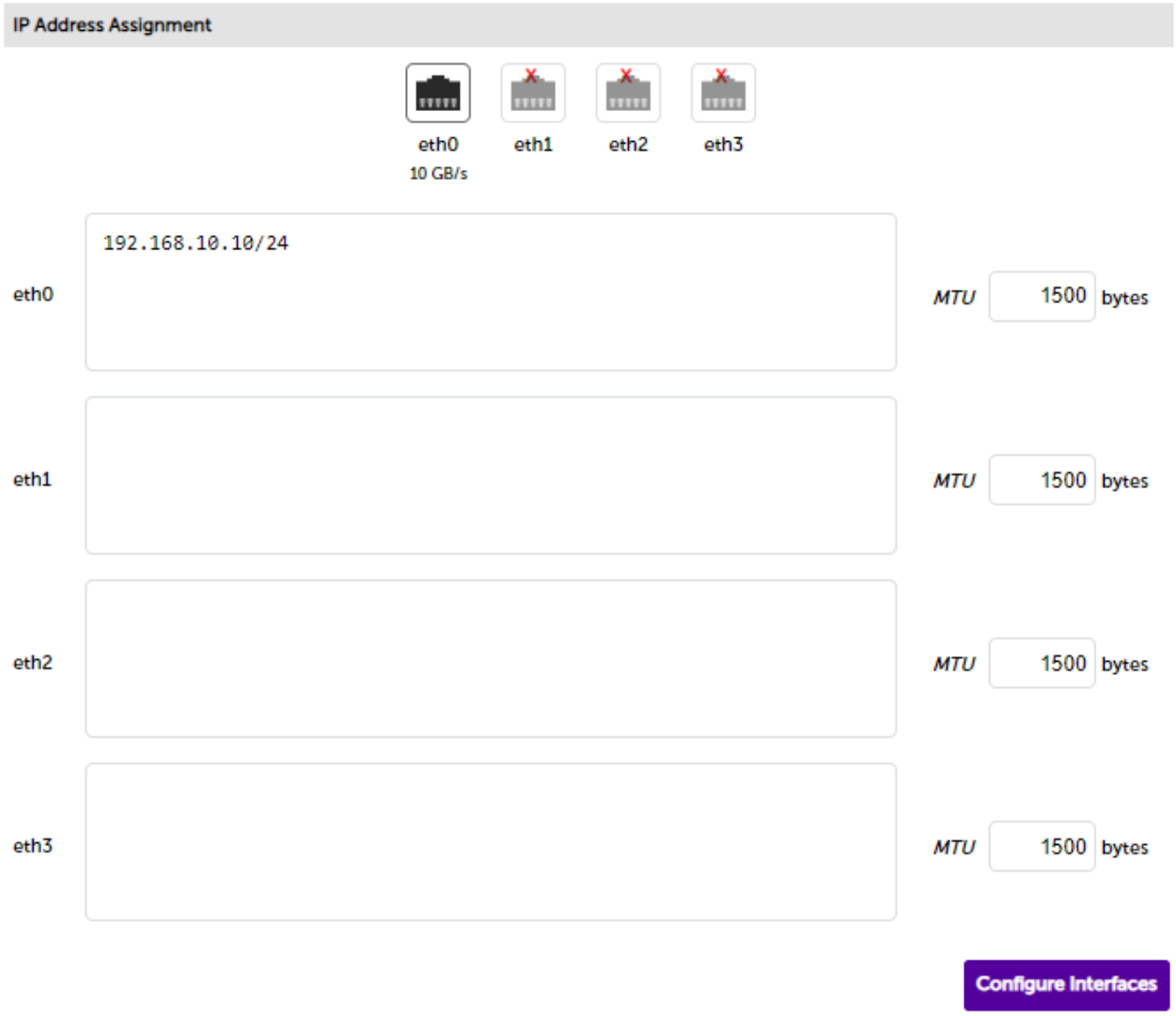
1. Using the WebUI, navigate to: *Local Configuration > Security*.
2. Set *Appliance Security Mode* to **Custom**.
3. Click **Update**.

## 9.7. Appliance Network Configuration

The standard CCW 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. Custom Health Check Configuration

Customized **DICOM C-Echo** health checks are used for VIP6, VIP7, VIP8 and VIP9. To configure these custom checks follow the steps below:

> **Note** If the following DICOM health checks are configured in exactly the same way, a single DICOM health check can be used for these VIPs.

> **Note** Please check the local site's CCW Application Servers when configuring values for **aet** and **aec** in the Health Check Scripts.

#### 9.8.1.1. C_Echo-104

1. Using the WebUI, navigate to *Cluster Configuration > Health Check Scripts* and click **Add New Health Check**.
2. Enter the following details:

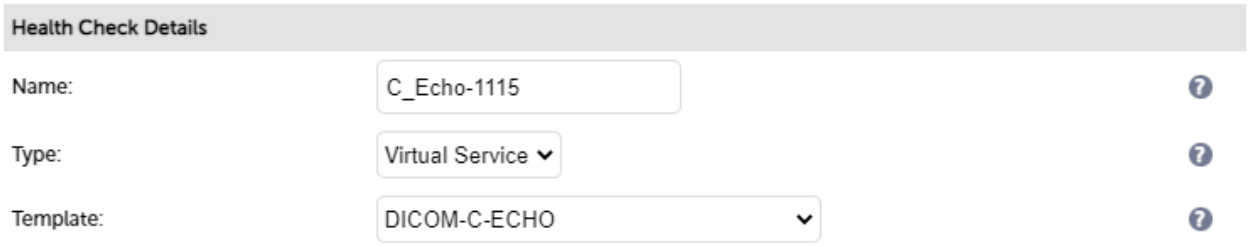

   - Specify an appropriate *Label* for the health check, e.g. **C_Echo-104**.
   - Set *Type* to **Virtual Service**.
   - Using the *Template* dropdown select **DICOM-C-ECHO** from the list.
   - Change the following lines in the script to suit your requirements:

```
aet=LOADBALANCER
aec=LB-SCP
```

3. Click **Update** to save the new health check script.

#### 9.8.1.2. C_Echo-1115

1. Using the WebUI, navigate to *Cluster Configuration > Health Check Scripts* and click **Add New Health Check**.
2. Enter the following details:




- Specify an appropriate *Label* for the health check, e.g. **C_Echo-1115**.
- Set *Type* to **Virtual Service**.
- Using the *Template* dropdown select **DICOM-C-ECHO** from the list.
- Change the following lines in the script to suit your requirements:

```
aet=LOADBALANCER
aec=LB-SCP
```

3. Click **Update** to save the new health check script.

### 9.8.1.3. C_Echo-1230

1. Using the WebUI, navigate to *Cluster Configuration > Health Check Scripts* and click **Add New Health Check**.
2. Enter the following details:

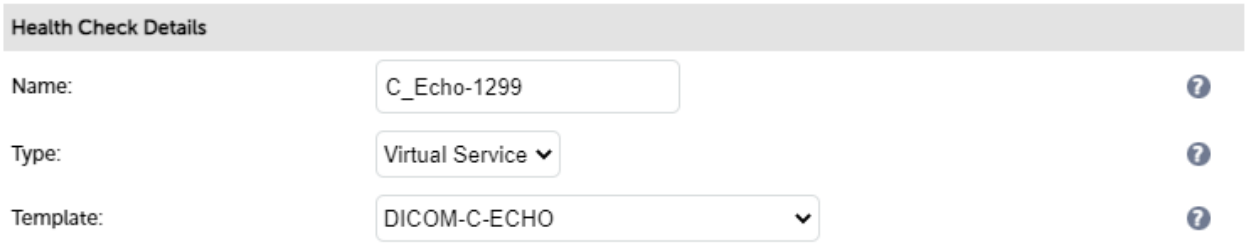

- Specify an appropriate *Label* for the health check, e.g. **C_Echo-1230**.
- Set *Type* to **Virtual Service**.
- Using the *Template* dropdown select **DICOM-C-ECHO** from the list.
- Change the following lines in the script to suit your requirements:

```
aet=LOADBALANCER
aec=LB-SCP
```

3. Click **Update** to save the new health check script.

### 9.8.1.4. C_Echo-1299

1. Using the WebUI, navigate to *Cluster Configuration > Health Check Scripts* and click **Add New Health Check**.
2. Enter the following details:




- Specify an appropriate *Label* for the health check, e.g. **C_Echo-1299**.
- Set *Type* to **Virtual Service**.
- Using the *Template* dropdown select **DICOM-C-ECHO** from the list.
- Change the following lines in the script to suit your requirements:

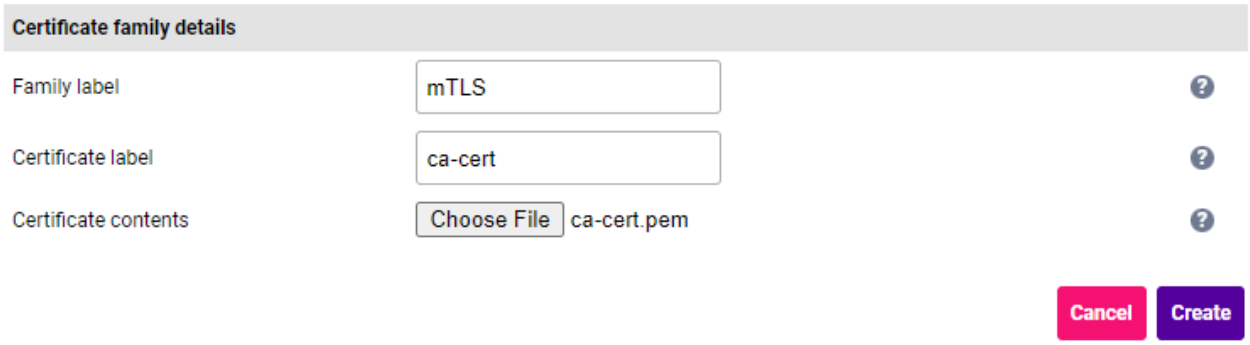
```
aet=LOADBALANCER
aec=LB-SCP
```

3. Click **Update** to save the new health check script.

## 9.8.2. CA Certificate Family & Client Certificate Configuration for mTLS

**Create the CA Certificate Family:**

1. Using the WebUI, navigate to *Cluster Configuration > CA Certificate Families*.
2. Click **Create Family** and enter the following details:



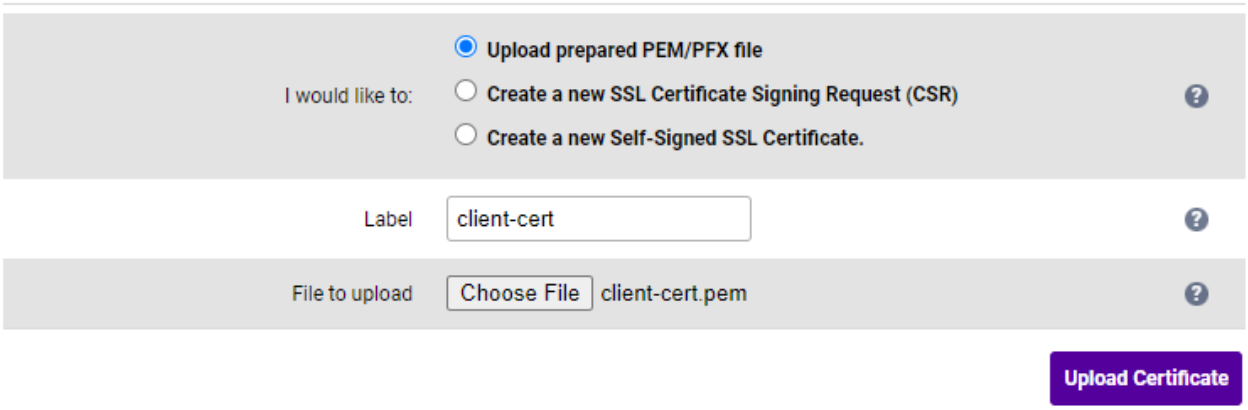

- Specify an appropriate *Family label*, e.g. **mTLS**.
- Specify an appropriate *Certificate label*, e.g. **ca-cert**.
- Click **Choose File** and select the relevant PEM file.

3. Click **Create**.

**Add the Client Certificate:**

1. Using the WebUI, navigate to *Cluster Configuration > SSL Certificate*.
2. Click **Add a new SSL Certificate**.

3. Select the **Upload prepared PEM/PFX file** option.
4. Enter the following details:

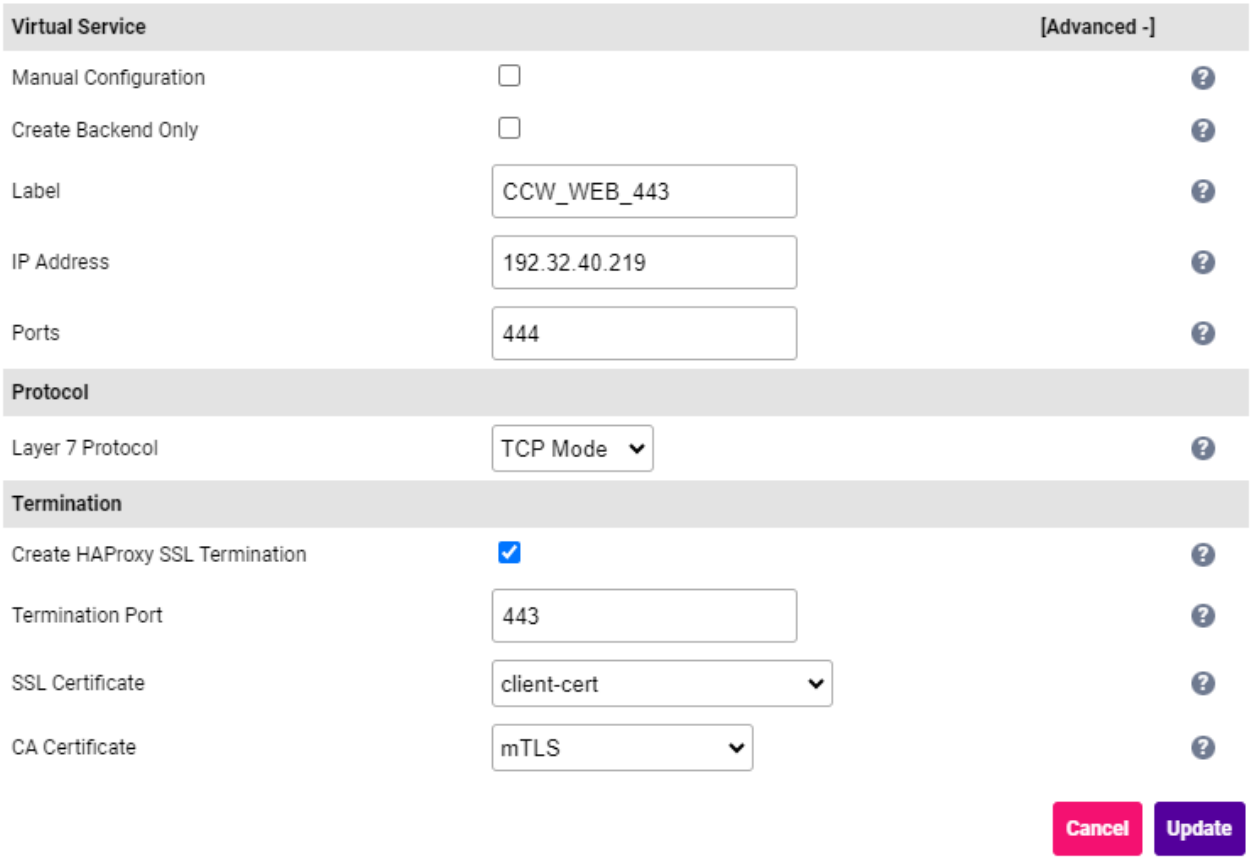



   - Specify an appropriate *label* (name), e.g. **client-cert**.
   - Click **Choose File** and select the relevant PEM or PFX file.
5. Click **Upload Certificate**.

### 9.8.3. VIP 1 - CCW_WEB_443

#### 9.8.3.1. 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]**.
3. Enable (check) the *Create HAProxy SSL Termination* checkbox.
4. Enter the following details:

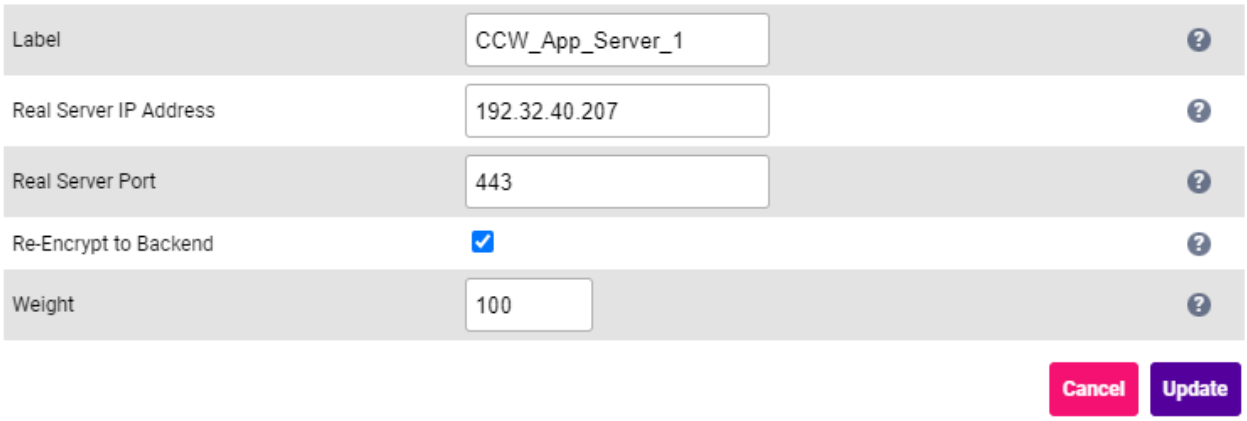



- Specify an appropriate *Label* for the Virtual Service, e.g. **CCW_WEB_443**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.32.40.219**.
- Set the *Ports* field to **444**.
- Set the *Layer 7 Protocol* to **TCP Mode**.
- In the *Termination* section:
  - Set the *Termination Port* to **443**.
  - Set the *SSL Certificate* to **client-cert**.
  - Set the *CA Certificate* to **mTLS**.

5. Click **Update** to create the Virtual Service.
6. Now click **Modify** next to the newly created VIP.
7. Scroll to the *Persistence* section.
   - Ensure that the *Persistence Mode* is set to **Source IP**.
8. Scroll to the *Health Checks* section.
   - Ensure that the *Health_Check* is set to **Connect to Port**.
9. Leave all other settings at their default value.
10. Click **Update**.

### 9.8.3.2. 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:

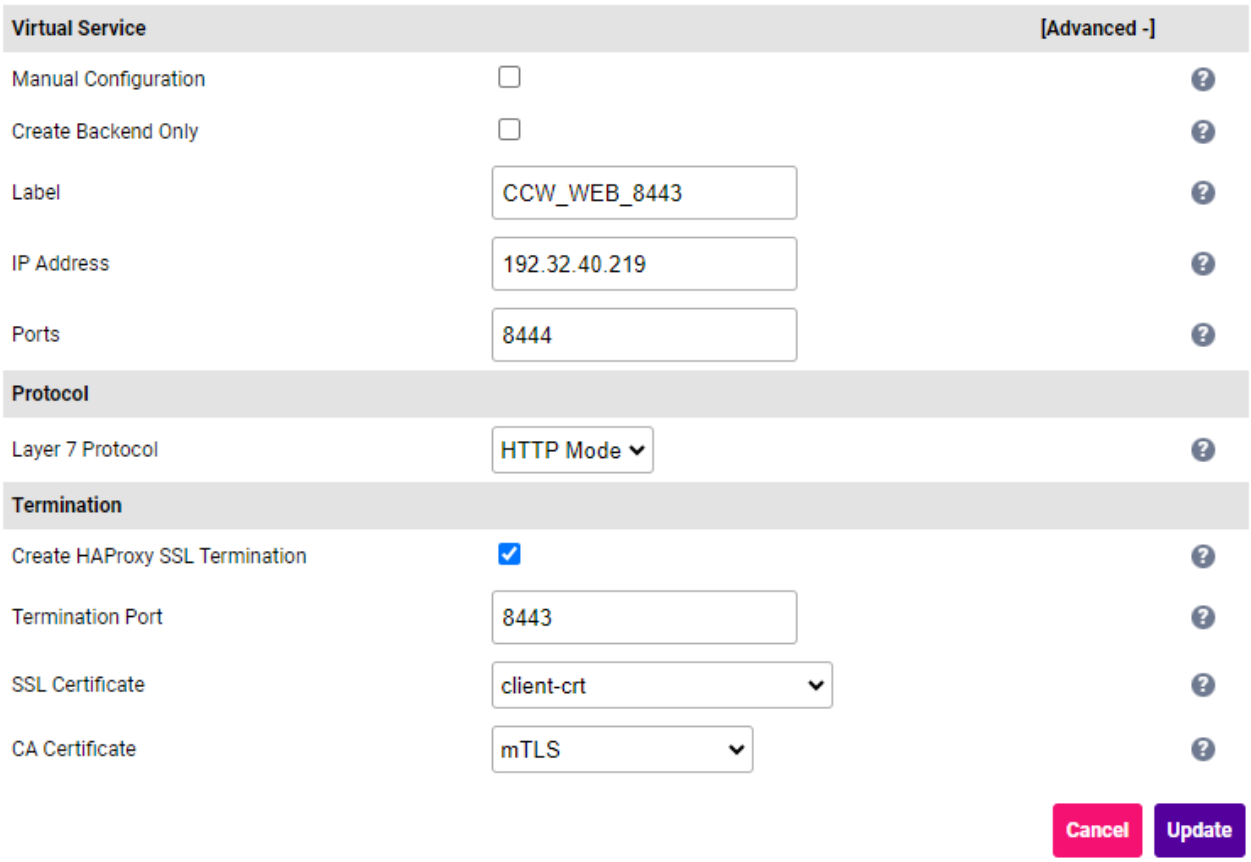



   - Specify an appropriate *Label* for the RIP, e.g. **CCW_App_Server_1**.
   - Set the *Real Server IP Address* field to the required IP address, e.g. **192.32.40.207**.
   - Set the *Real Server Port* field to **443**.
   - Enable (check) the *Re-Encrypt to Backend* checkbox.
3. Leave all other settings at their default value.
4. Click **Update**.
5. Now click **Modify** next to the newly created RIP.
6. Set the *Verify Server Certificate* to **mTLS**.
7. Set the *Send Client Certificate* to **client-cert**.
8. Repeat these steps to add additional Real Server(s).

## 9.8.4. VIP 2 - CCW_WEB_8443

### 9.8.4.1. 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]**.
3. Enable (check) the *Create HAProxy SSL Termination* checkbox.
4. Enter the following details:

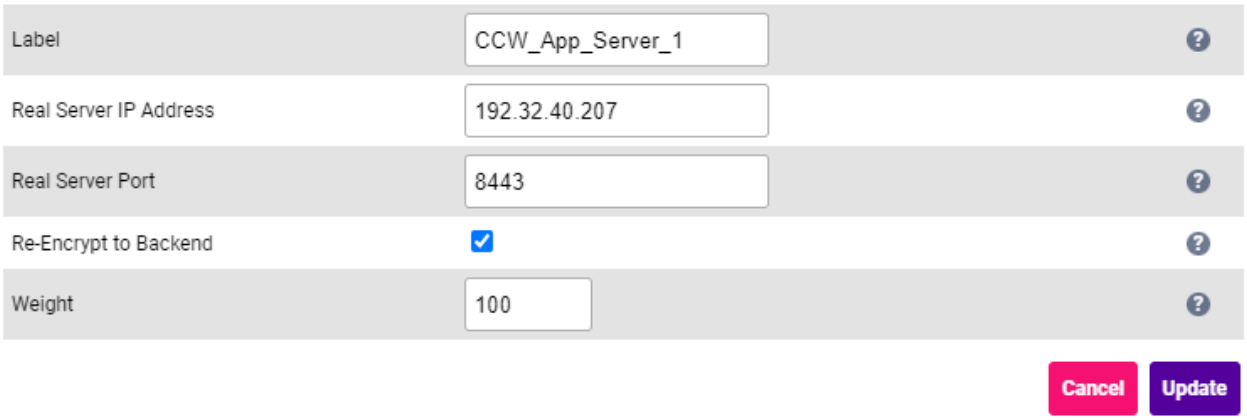



- Specify an appropriate *Label* for the Virtual Service, e.g. **CCW_WEB_8443**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.32.40.219**.
- Set the *Ports* field to **8444**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.
- In the *Termination* section:
  - Set the *Termination Port* to **8443**.
  - Set the *SSL Certificate* to **client-cert**.
  - Set the *CA Certificate* to **mTLS**.

5. Click **Update** to create the Virtual Service.
6. Now click **Modify** next to the newly created VIP.
7. Scroll to the *Persistence* section.
   - Set the *Persistence Mode* to **HTTP Cookie**.
8. Scroll to the *Health Checks* section.
   - Ensure that the *Health_Check* is set to **Connect to Port**.
9. Leave all other settings at their default value.
10. Click **Update**.

### 9.8.4.2. 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:

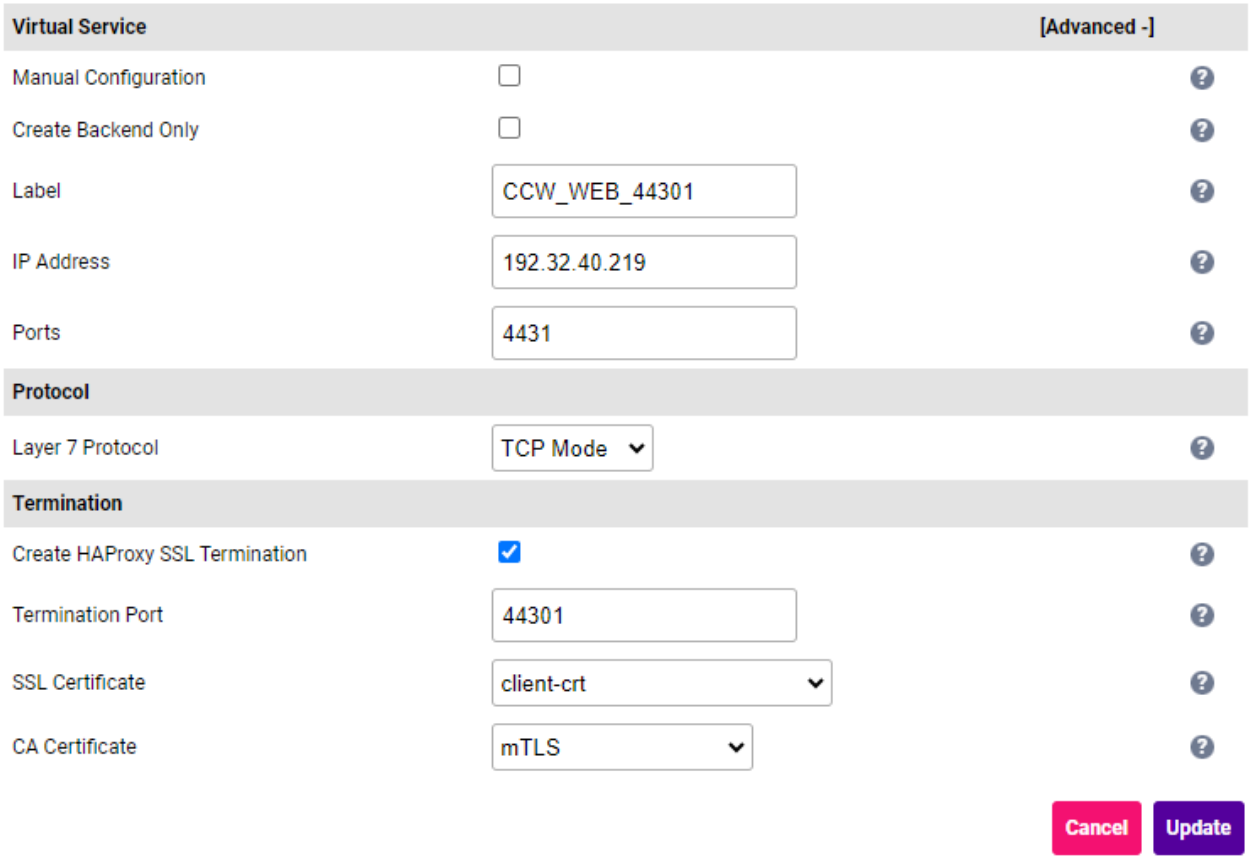



   - Specify an appropriate *Label* for the RIP, e.g. **CCW_App_Server_1**.
   - Set the *Real Server IP Address* field to the required IP address, e.g. **192.32.40.207**.
   - Set the *Real Server Port* field to **8443**.
   - Enable (check) the *Re-Encrypt to Backend* checkbox.
3. Leave all other settings at their default value.
4. Click **Update**.
5. Now click **Modify** next to the newly created RIP.
6. Set the *Verify Server Certificate* to **mTLS**.
7. Set the *Send Client Certificate* to **client-cert**.
8. Repeat these steps to add additional Real Server(s).

## 9.8.5. VIP 3 - CCW_WEB_44301

### 9.8.5.1. 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]**.
3. Enable (check) the *Create HAProxy SSL Termination* checkbox.
4. Enter the following details:

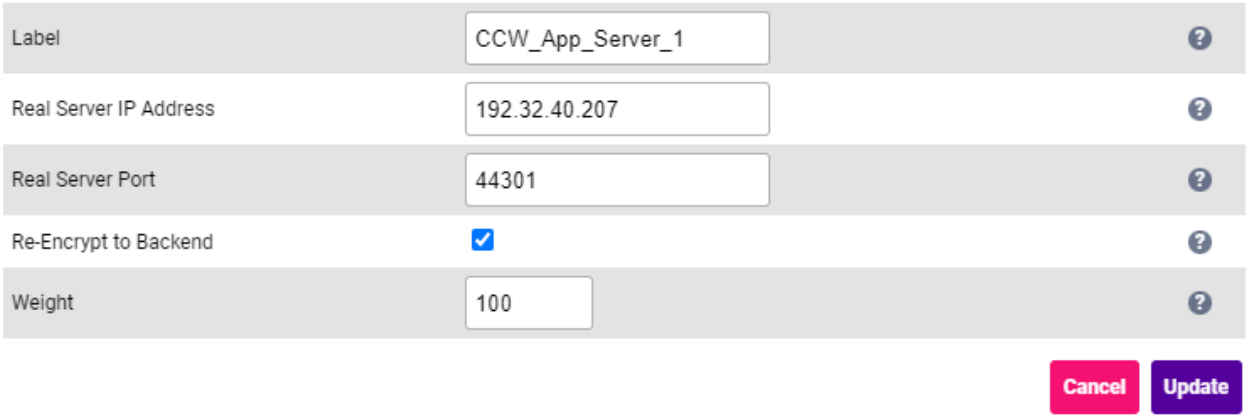



- Specify an appropriate *Label* for the Virtual Service, e.g. **CCW_WEB_44301**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.32.40.219**.
- Set the *Ports* field to **4431**.
- Set the *Layer 7 Protocol* to **TCP Mode**.
- In the *Termination* section:
  - Leave the *Termination Port* set to **44301**.
  - Set the *SSL Certificate* to **client-cert**.
  - Set the *CA Certificate* to **mTLS**.

5. Click **Update** to create the Virtual Service.
6. Now click **Modify** next to the newly created VIP.
7. Scroll to the *Persistence* section.
   - Ensure that the *Persistence Mode* is set to **Source IP**.
8. Scroll to the *Health Checks* section.
   - Ensure that the *Health_Check* is set to **Connect to Port**.
9. Leave all other settings at their default value.
10. Click **Update**.

### 9.8.5.2. 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:

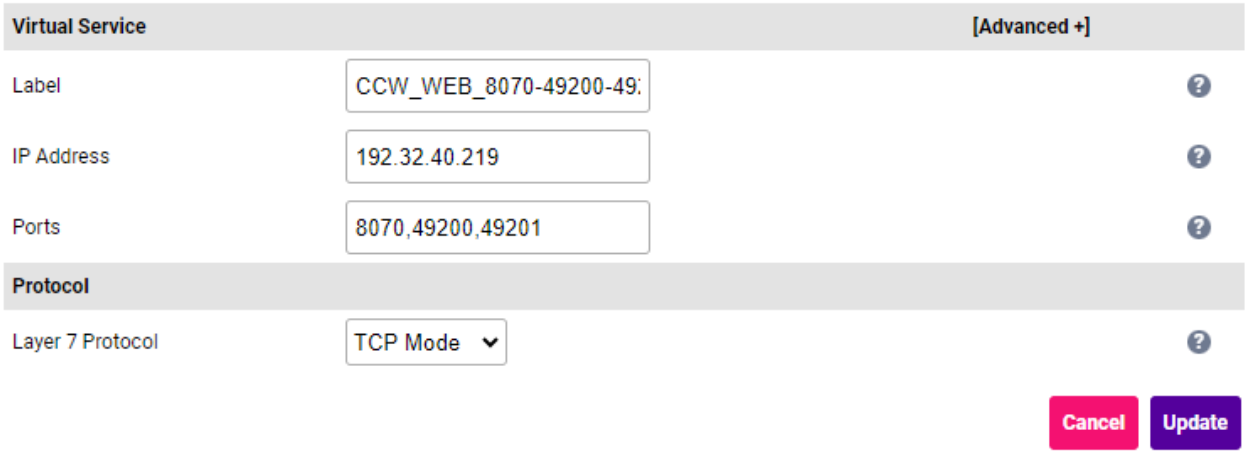



   - Specify an appropriate *Label* for the RIP, e.g. **CCW_App_Server_1**.
   - Set the *Real Server IP Address* field to the required IP address, e.g. **192.32.40.207**.
   - Set the *Real Server Port* field to **44301**.
   - Enable (check) the *Re-Encrypt to Backend* checkbox.
3. Leave all other settings at their default value.
4. Click **Update**.
5. Now click **Modify** next to the newly created RIP.
6. Set the *Verify Server Certificate* to **mTLS**.
7. Set the *Send Client Certificate* to **client-cert**.
8. Repeat these steps to add additional Real Server(s).

## 9.8.6. VIP 4 - CCW_WEB_8070-49200-49201

### 9.8.6.1. 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:

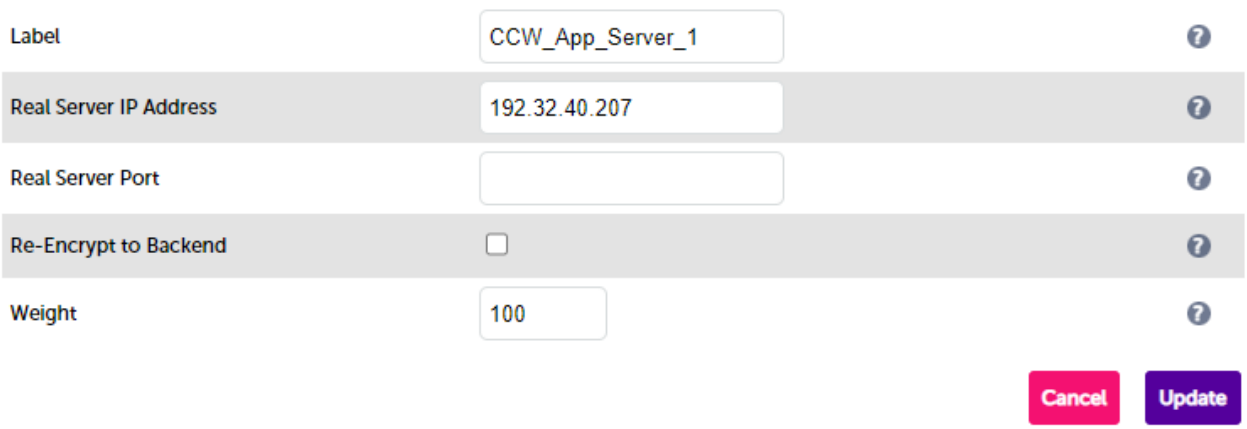



- Specify an appropriate *Label* for the Virtual Service, e.g. **CCW_WEB_8070-49200-49201**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.32.40.219**.
- Set the *Ports* field to **8070,49200,49201**.
- Set the *Layer 7 Protocol* to **TCP Mode**.

3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Persistence* section.
   - Ensure that the *Persistence Mode* is set to **Source IP**.
6. Scroll to the *Health Checks* section.
   - Ensure that the *Health_Check* is set to **Connect to Port**.
7. Leave all other settings at their default value.
8. Click **Update**.

### 9.8.6.2. 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:



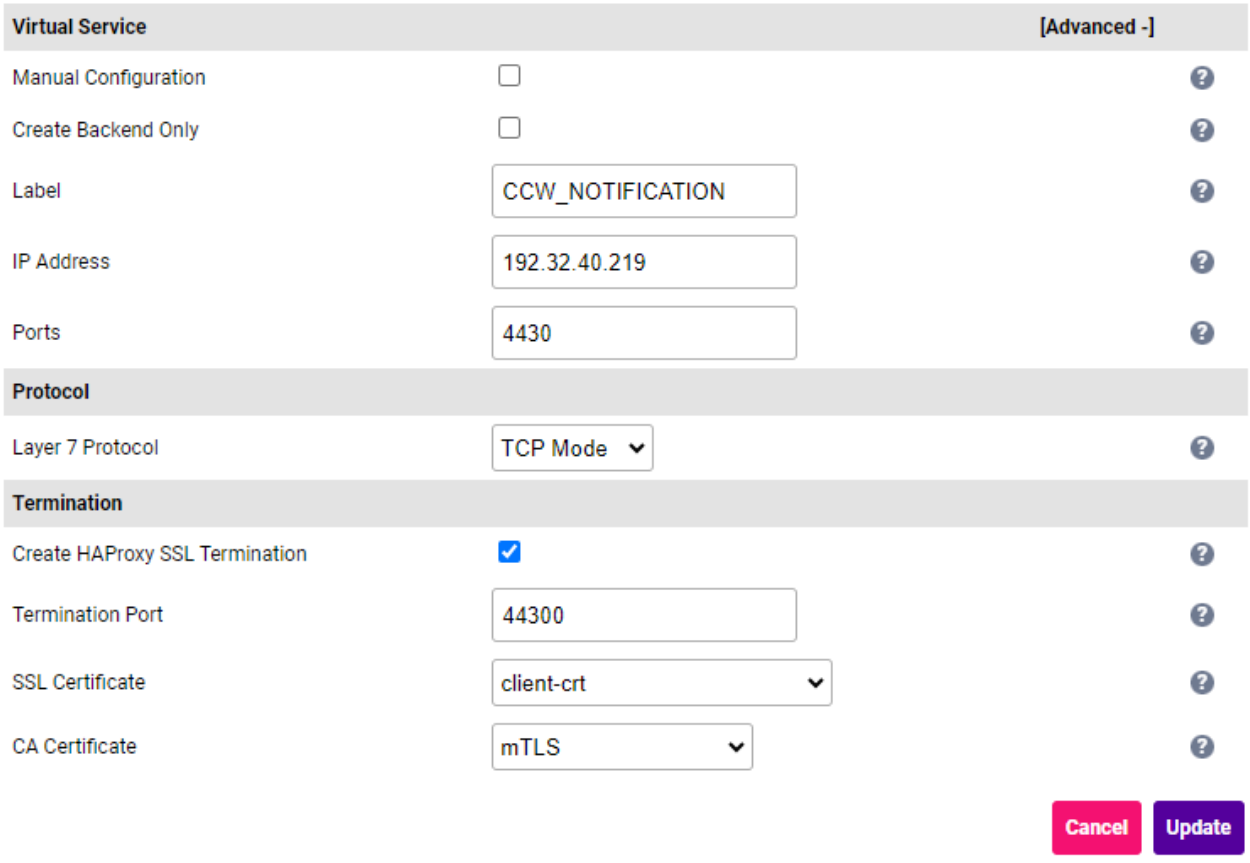
- Specify an appropriate *Label* for the RIP, e.g. **CCW_App_Server_1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.32.40.207**.
- Leave the *Real Server Port* field blank.

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

## 9.8.7. VIP 5 - CCW_NOTIFICATION

### 9.8.7.1. 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]**.
3. Enable (check) the *Create HAProxy SSL Termination* checkbox.
4. Enter the following details:



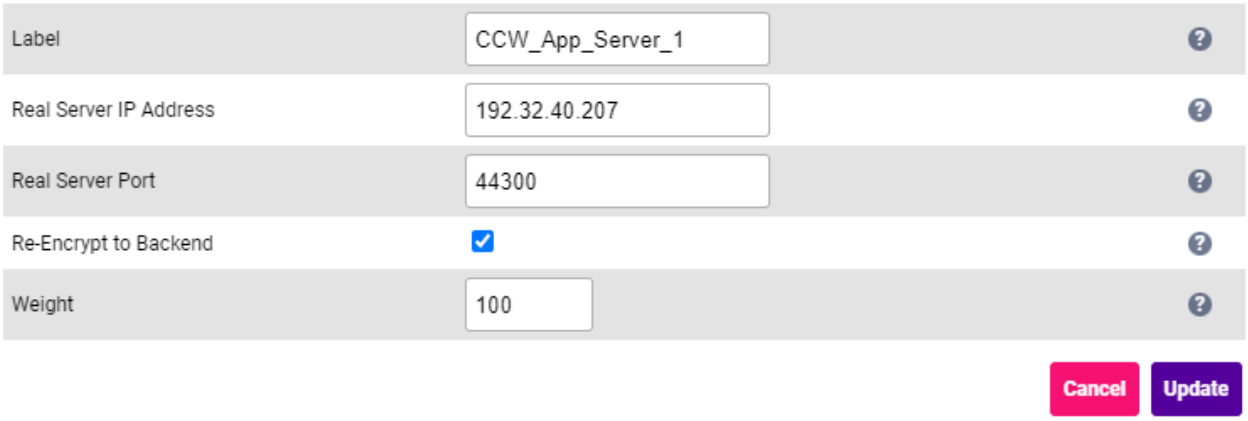

- Specify an appropriate *Label* for the Virtual Service, e.g. **CCW_NOTIFICATION**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.32.40.219**.
- Set the *Ports* field to **4430**.
- Set the *Layer 7 Protocol* to **TCP Mode**.

- In the *Termination* section:
  - Leave the *Termination Port* set to **44300**.
  - Set the *SSL Certificate* to **client-cert**.
  - Set the *CA Certificate* to **mTLS**.

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 **First**.
8. Scroll to the *Persistence* section and click **[Advanced]**.
   - Set the *Persistence Mode* to **Last Successful**.
   - Set the timeout to **720**.
9. Scroll to the *Health Checks* section.
   - Set the *Check Type* to **Negotiate HTTPS (GET)**.
   - Set *Request to send* to **/api/health/**.
   - Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.
10. Scroll down to the *Other* section and click **[Advanced]**.
    - Enable (check) the *Timeout* checkbox.
    - Set *Client Timeout* and *Real Server Timeout* to **12h** (12 hours).
11. Leave all other settings at their default value.
12. Click **Update**.

### 9.8.7.2. 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:



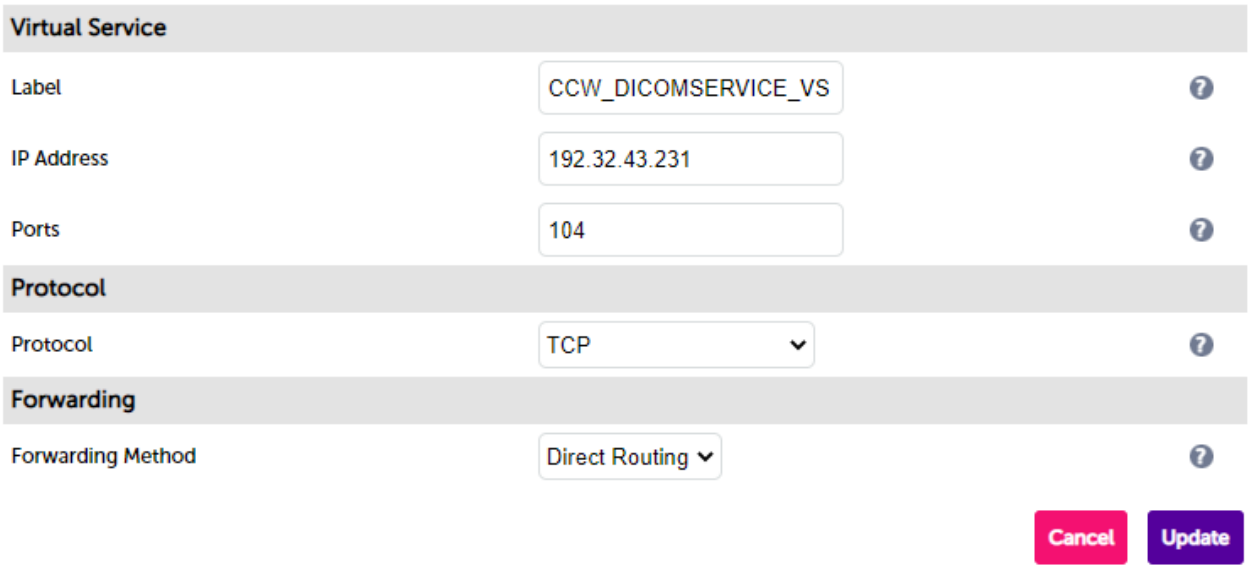
- Specify an appropriate *Label* for the RIP, e.g. **CCW_App_Server_1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.32.40.207**.
- Set the *Real Server Port* field to **44300**.
- Enable (check) the *Re-Encrypt to Backend* checkbox.

3. Leave all other settings at their default value.
4. Click **Update**.
5. Now click **Modify** next to the newly created RIP.
6. Set the *Verify Server Certificate* to **mTLS**.
7. Set the *Send Client Certificate* to **client-cert**.
8. Repeat these steps to add additional Real Server(s).

## 9.8.8. VIP 6 - CCW_DICOMSERVICE_VS

### 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:



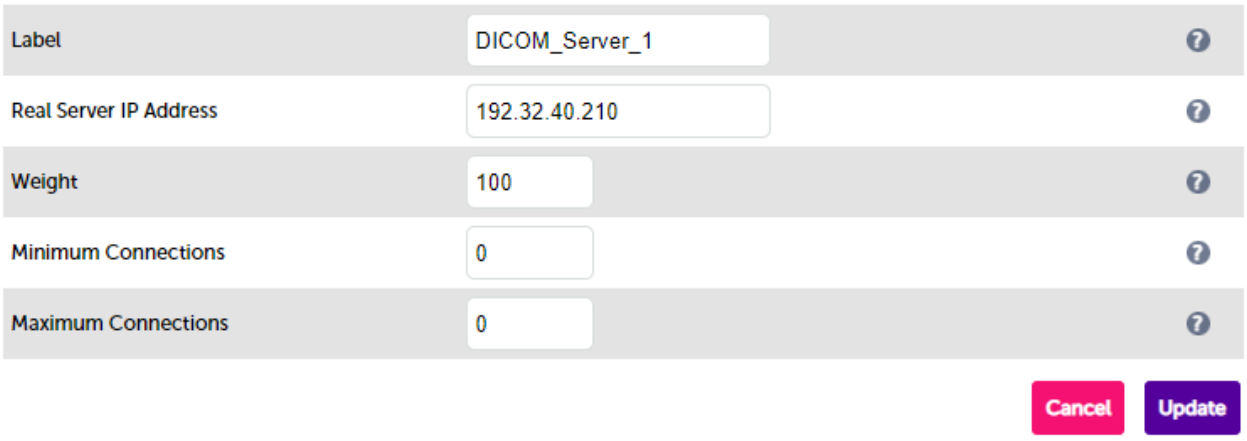

- Specify an appropriate *Label* for the Virtual Service, e.g. **CCW_DICOMSERVICE_VS**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.32.43.231**.
- Set the *Ports* field to **104**.
- Leave the *Protocol* set to **TCP**.
- Set the *Forwarding Method* set to **Direct Routing**.

3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.

5. Scroll to the *Persistence* section.
    - Ensure that the *Enable* checkbox is unchecked (disabled).
6. Scroll to the *Health Checks* section.
    - Set *Check Type* to **External Script**.
    - Set *External Script* to the health check created above, e.g. **C_Echo-104**.
7. Leave all other settings at their default value.
8. 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:

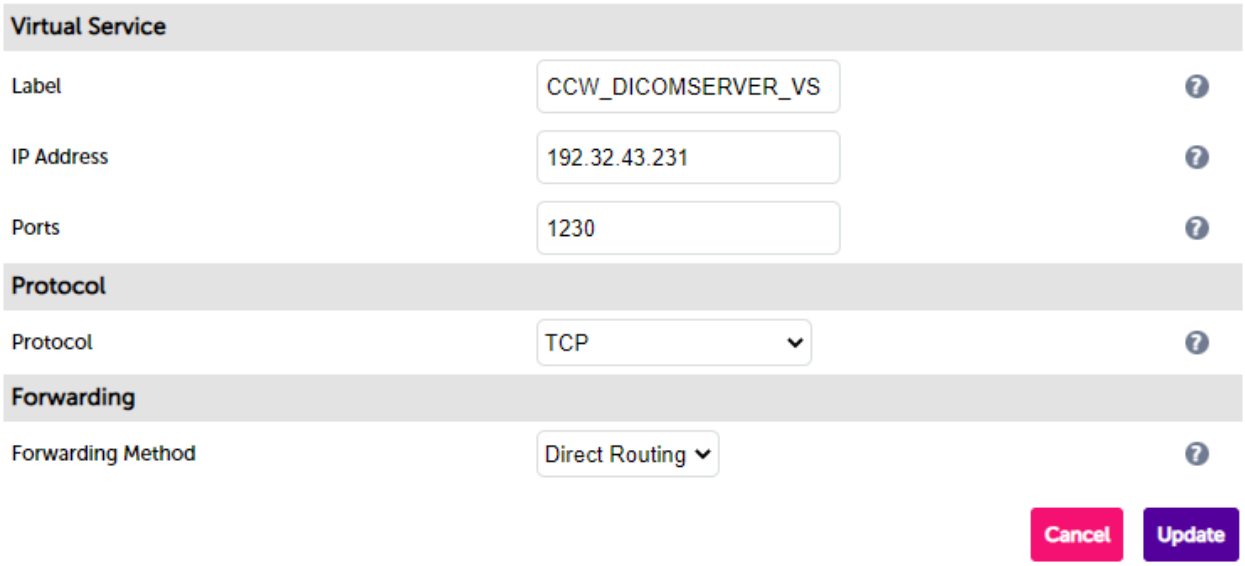



    - Specify an appropriate *Label* for the RIP, e.g. **DICOM_Server_1**.
    - Change the *Real Server IP Address* field to the required IP address, e.g. **192.32.40.210**.
3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Server(s).

### 9.8.9. VIP 7 - CCW_DICOMSERVER_VS

#### 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:

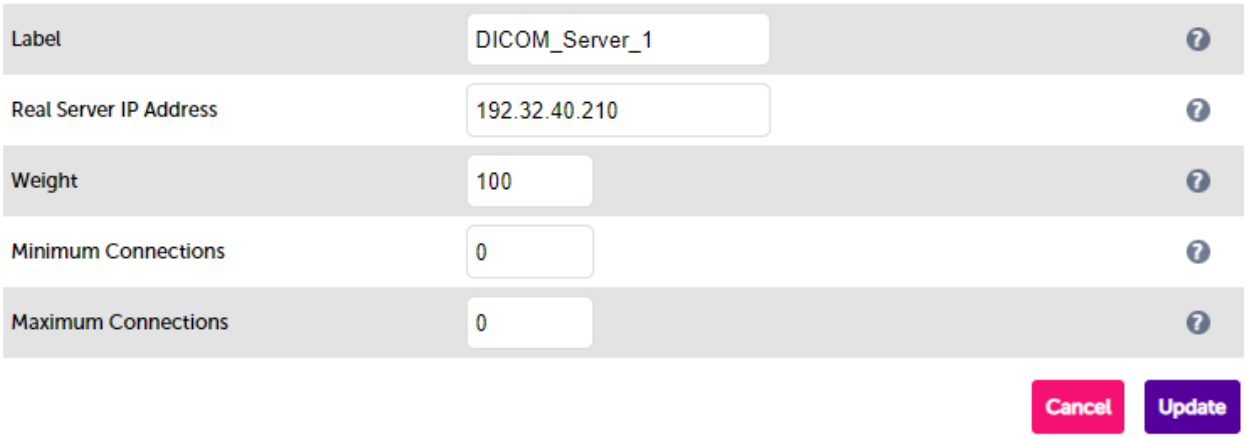



- Specify an appropriate *Label* for the Virtual Service, e.g. **CCW_DICOMSERVER_VS**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.32.43.231**.
- Set the *Ports* field to **1230**.
- Leave the *Protocol* set to **TCP**.
- Set the *Forwarding Method* set to **Direct Routing**.

3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Persistence* section.
   - Ensure that the *Enable* checkbox is unchecked (disabled).
6. Scroll to the *Health Checks* section.
   - Set *Check Type* to **External Script**.
   - Set *External Script* to the health check created above, e.g. **C_Echo-1230**.
7. Leave all other settings at their default value.
8. Click **Update**.

### 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:



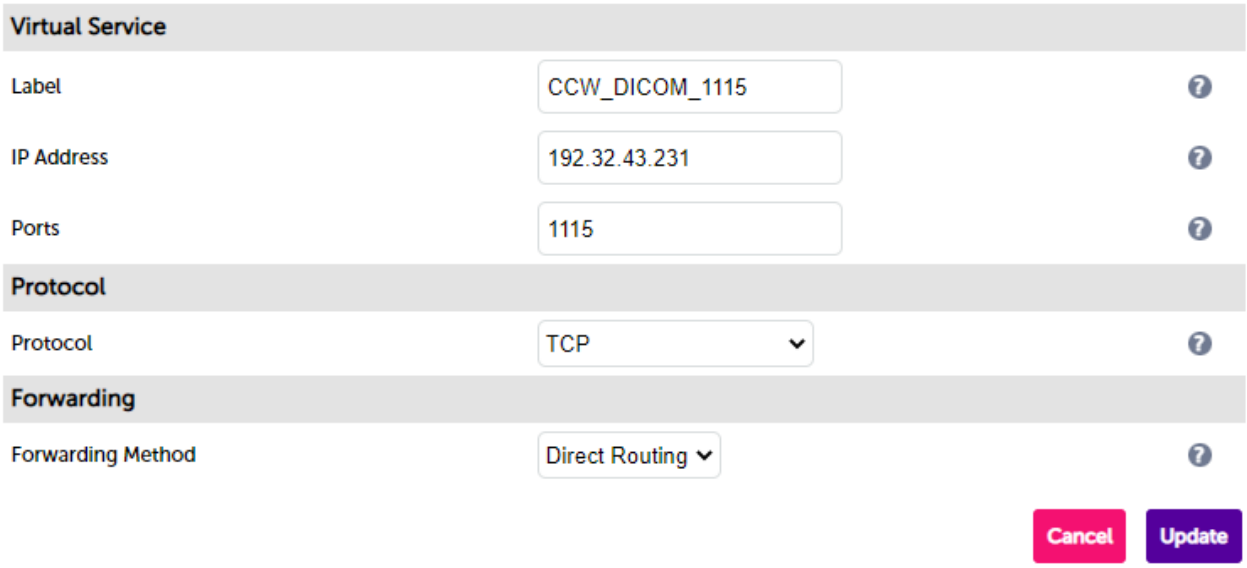

- Specify an appropriate *Label* for the RIP, e.g. **DICOM_Server_1**.
- Change the *Real Server IP Address* field to the required IP address, e.g. **192.32.40.210**.

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

## 9.8.10. VIP 8 - CCW_DICOM_1115

### 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:



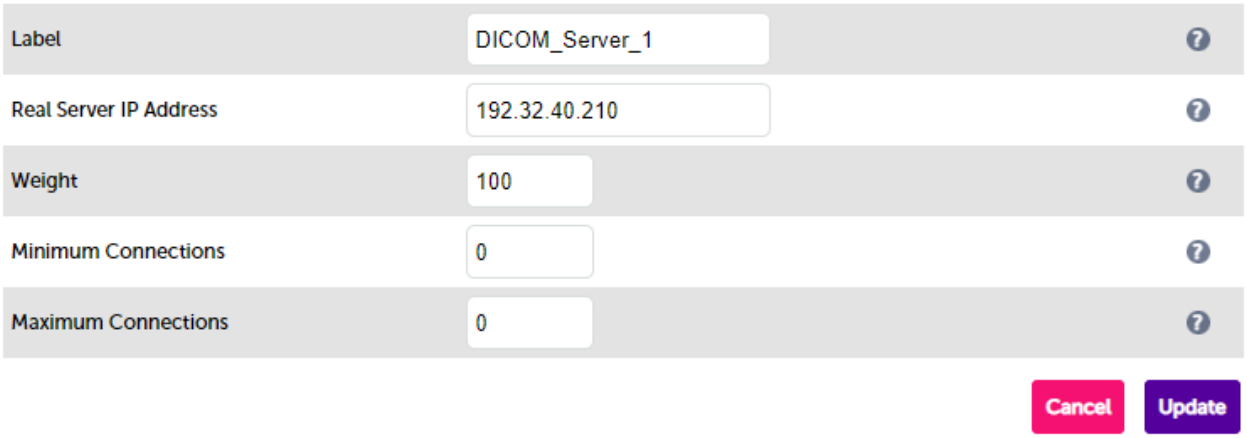

- Specify an appropriate *Label* for the Virtual Service, e.g. **CCW_DICOM_1115**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.32.43.231**.
- Set the *Ports* field to **1115**.

- Leave the *Protocol* set to **TCP**.
- Set 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 *Persistence* section.
   - Ensure that the *Enable* checkbox is unchecked (disabled).
6. Scroll to the *Health Checks* section.
   - Set *Check Type* to **External Script**.
   - Set *External Script* to the health check created above, e.g. **C_Echo-1115**.
7. Leave all other settings at their default value.
8. Click **Update**.

#### 9.8.10.2. 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:



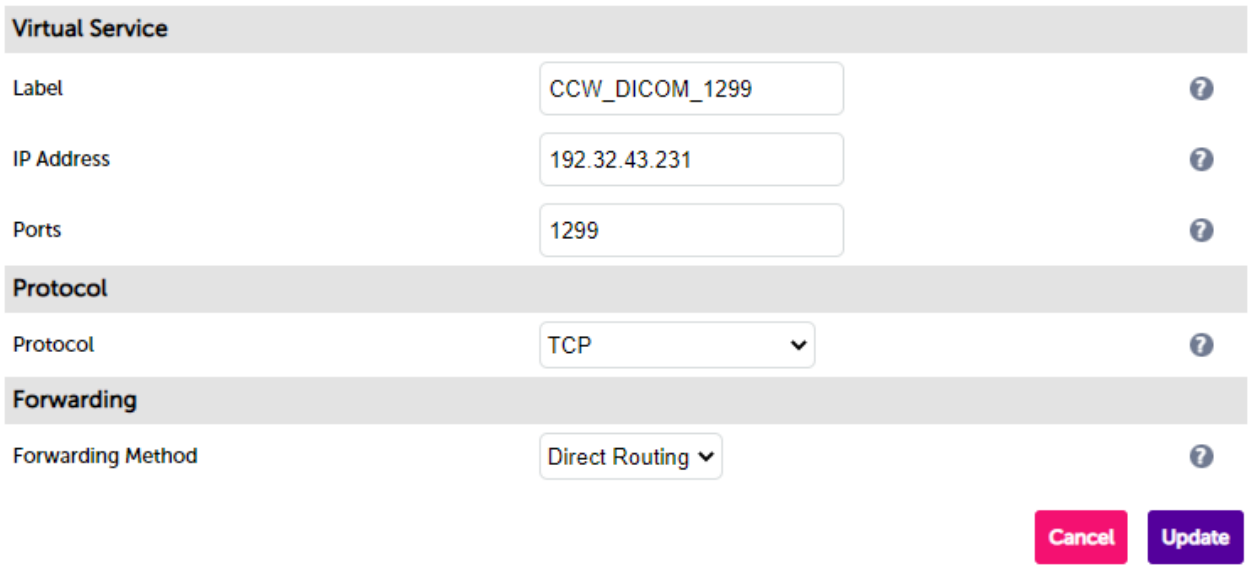

   - Specify an appropriate *Label* for the RIP, e.g. **DICOM_Server_1**.
   - Change the *Real Server IP Address* field to the required IP address, e.g. **192.32.40.210**.
3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Server(s).

### 9.8.11. VIP 9 - CCW_DICOM_1299

#### 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:

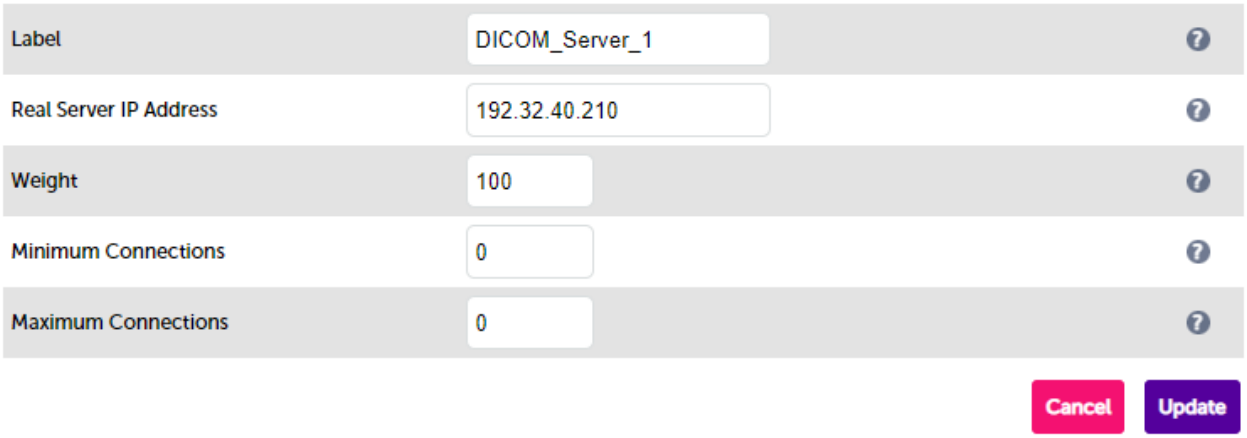



- Specify an appropriate *Label* for the Virtual Service, e.g. **CCW_DICOM_1299**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.32.43.231**.
- Set the *Ports* field to **1299**.
- Leave the *Protocol* set to **TCP**.
- Set the *Forwarding Method* set to **Direct Routing**.

3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Persistence* section.
   - Ensure that the *Enable* checkbox is unchecked (disabled).
6. Scroll to the *Health Checks* section.
   - Set *Check Type* to **External Script**.
   - Set *External Script* to the health check created above, e.g. **C_Echo-1299**.
7. Leave all other settings at their default value.
8. 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:



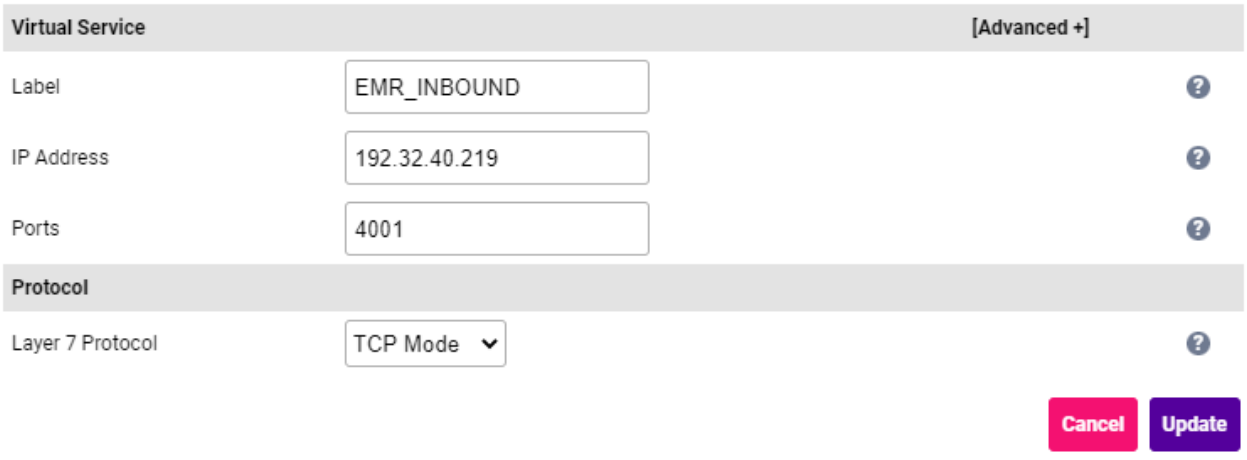

- Specify an appropriate *Label* for the RIP, e.g. **DICOM_Server_1**.
- Change the *Real Server IP Address* field to the required IP address, e.g. **192.32.40.210**.

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

## 9.8.12. VIP 10 - EMR_INBOUND

### 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:



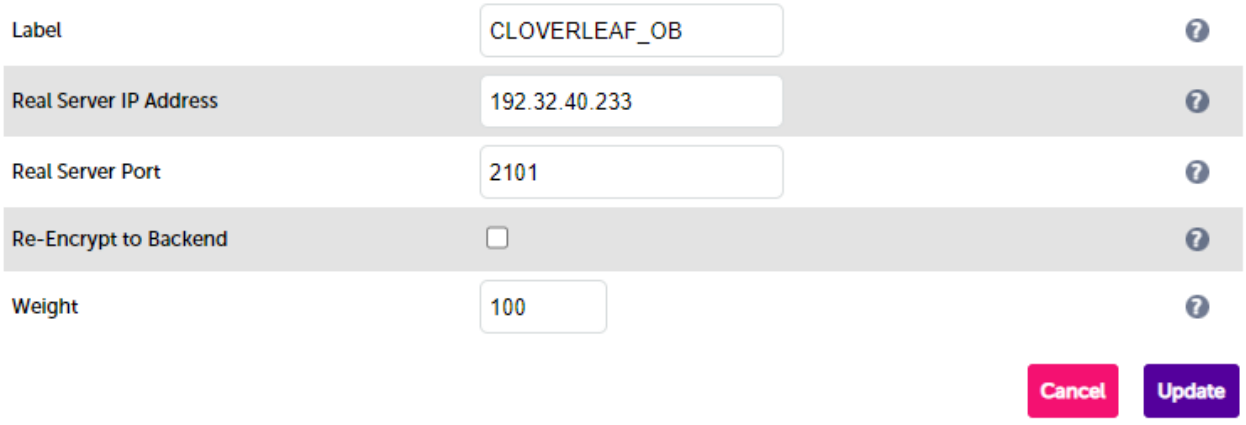

- Specify an appropriate *Label* for the Virtual Service, e.g. **EMR_INBOUND**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.32.40.219**.
- Set the *Ports* field to **4001**.
- Set the *Layer 7 Protocol* to **TCP Mode**.

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**.

#### 9.8.12.2. 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:



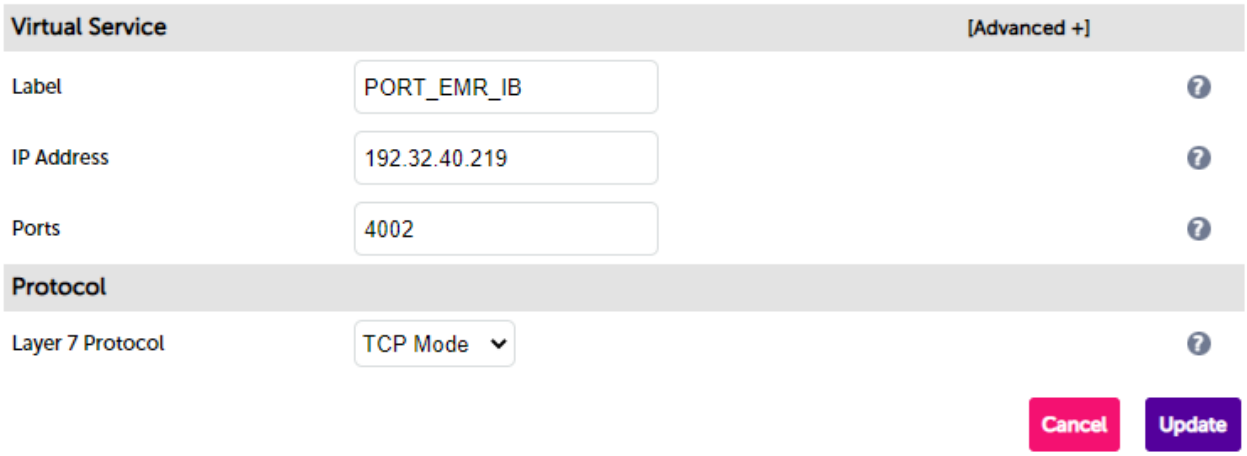

   - Specify an appropriate *Label* for the RIP, e.g. **CLOVERLEAF_OB**.
   - Set the *Real Server IP Address* field to the required IP address, e.g. **192.32.40.233**.
   - Set the *Real Server Port* field to **2101**.
3. Leave all other settings at their default value.
4. Click **Update**.
5. Repeat these steps to add additional Real Server(s).

### 9.8.13. VIP 11 - PORT_EMR_IB

#### 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**.

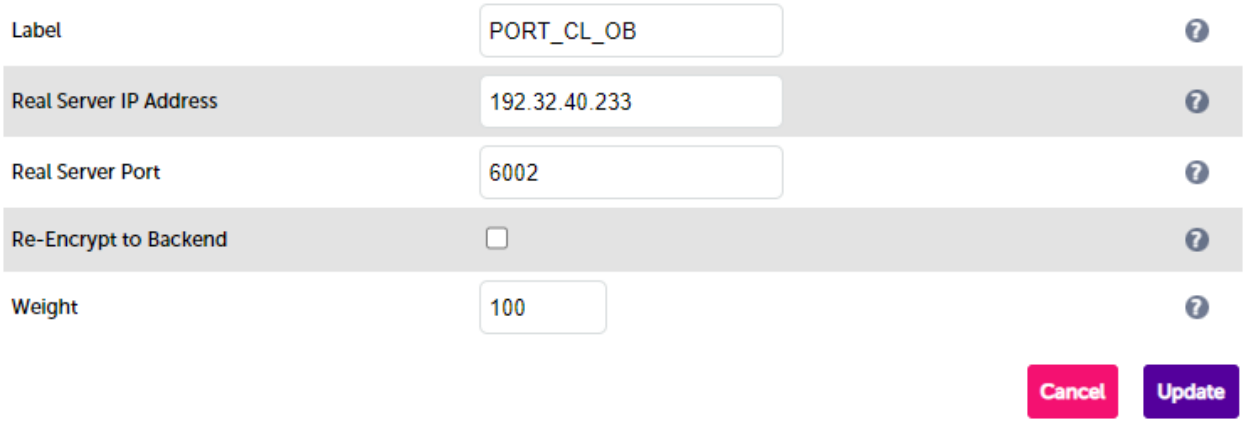
2. Enter the following details:




   - Specify an appropriate *Label* for the Virtual Service, e.g. **Port_EMR_IB**.
   - Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.32.40.219**.
   - Set the *Ports* field to **4002**.
   - 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**.

### 9.8.13.2. 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. **PORT_CL_OB**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **192.32.40.233**.
- Set the *Real Server Port* field to **6002**.

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

### 9.8.14. Finalizing the Configuration

To apply the new settings, HAProxy 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 CCW 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:

System Overview

2022-10-06 11:10:12 UTC

| VIRTUAL SERVICE | IP | PORTS | CONNS | PROTOCOL | METHOD | MODE |
|---|---|---|---|---|---|---|
| CCW_WEB_443 | 192.32.40.219 | 444 | 0 | TCP | Layer 7 | Proxy |
| CCW_WEB_8443 | 192.32.40.219 | 8444 | 0 | HTTP | Layer 7 | Proxy |
| CCW_WEB_44301 | 192.32.40.219 | 4431 | 0 | TCP | Layer 7 | Proxy |
| CCW_WEB_8070-492.. | 192.32.40.219 | 8070,4920.. | 0 | TCP | Layer 7 | Proxy |
| CCW_NOTIFICATION.. | 192.32.40.219 | 4430 | 0 | TCP | Layer 7 | Proxy |
| CCW_DICOMSERVICE.. | 192.32.43.231 | 104 | 0 | TCP | Layer 4 | DR |
| *REAL SERVER* | *IP* | *PORTS* | *WEIGHT* | *CONNS* | | |
| *DICOM Server 1* | *192.32.40.210* | *104* | *100* | *0* | *Drain* | *Halt* |
| *DICOM Server 2* | *192.32.40.211* | *104* | *100* | *0* | *Drain* | *Halt* |
| CCW_DICOMSERVER | 192.32.43.231 | 1230 | 0 | TCP | Layer 4 | DR |
| CCW_DICOM_1115 | 192.32.43.231 | 1115 | 0 | TCP | Layer 4 | DR |
| CCW_DICOM_1299 | 192.32.43.231 | 1299 | 0 | TCP | Layer 4 | DR |
| CCG_IB_2101 | 192.32.40.219 | 2101 | 0 | TCP | Layer 7 | Proxy |
| CCG_IB_2102 | 192.32.40.219 | 2102 | 0 | TCP | Layer 7 | Proxy |
| EMR_Inbound | 192.32.40.219 | 4001 | 0 | TCP | Layer 7 | Proxy |
| Port_EMR_IB | 192.32.40.219 | 4002 | 0 | TCP | Layer 7 | Proxy |
| Port_CCG_IB_2103.. | 192.32.40.219 | 2103 | 0 | TCP | Layer 7 | Proxy |
| Port_CCG_IB_2104.. | 192.32.40.219 | 2104 | 0 | TCP | Layer 7 | Proxy |

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:

| CCW_DICOMSERVICE.. | 192.32.43.231 | 104 | 0 | TCP | Layer 4 | DR |
|---|---|---|---|---|---|---|
| *REAL SERVER* | *IP* | *PORTS* | *WEIGHT* | *CONNS* | | |
| *DICOM Server 1* | *192.32.40.210* | *104* | *100* | *0* | *Drain* | *Halt* |
| *DICOM Server 2* | *192.32.40.211* | *104* | *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

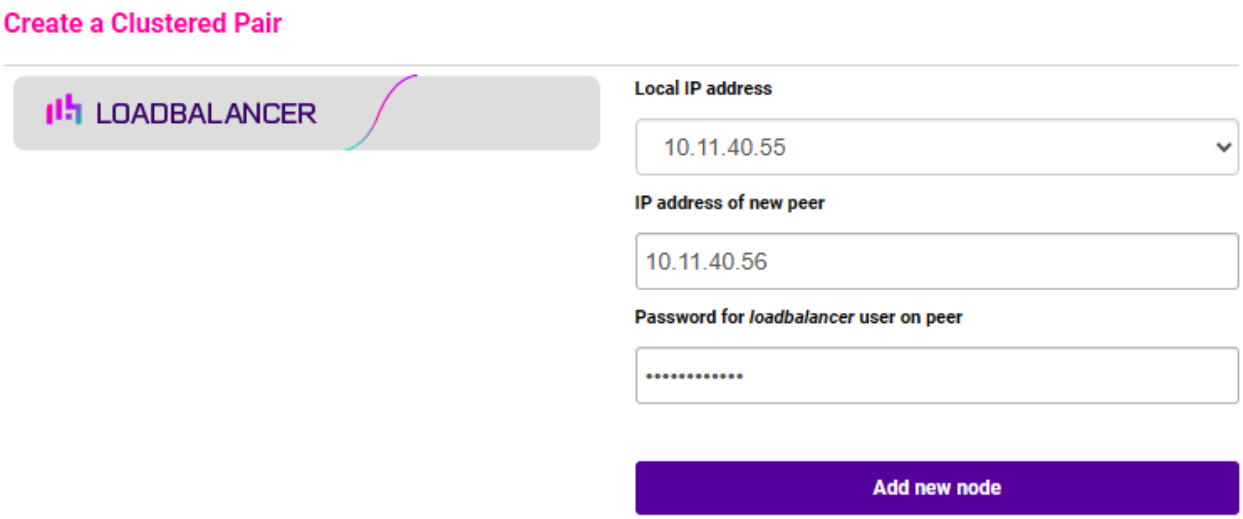
A number of settings are not replicated as part of the Primary/Secondary pairing process and therefore must be manually configured on the Secondary appliance. These are listed by WebUI menu option in the table below:

| 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 |
| 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 |

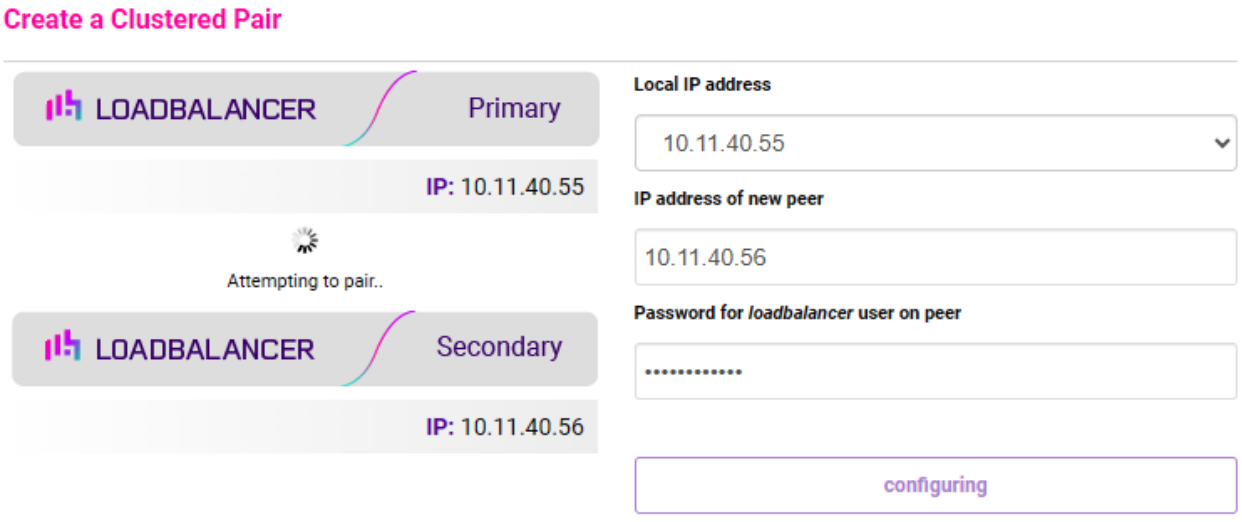
> **Important** Make sure that where any of the above have been configured on the Primary appliance, they're also configured on the Secondary.

## 11.2. Configuring the HA Clustered Pair

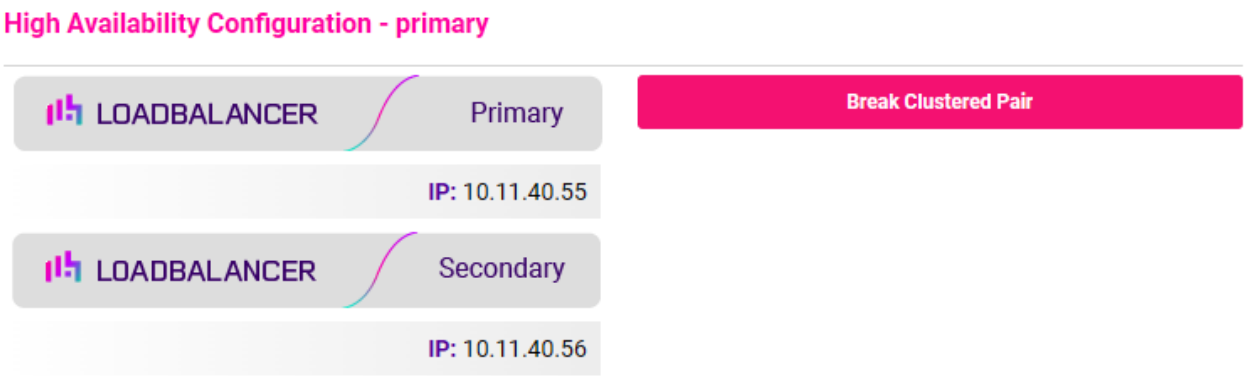
1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI on the Primary appliance, navigate to: *Cluster Configuration > High-Availability Configuration*.




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.

## 11.3. Last Successful - Clearing the Stick Table

VIP6 to VIP11 use the persistence type **Last Successful** which is described here. As mentioned, to allow traffic to be sent to the first server once it's back online, either the VIP's stick table must be cleared or the second server must be halted.

*To Clear a Stick Table:*

1. Using the WebUI, navigate to: *Reports > Layer 7 Stick Table*.
2. Select the relevant VIP using the drop-down.
3. Click **Clear Table**.

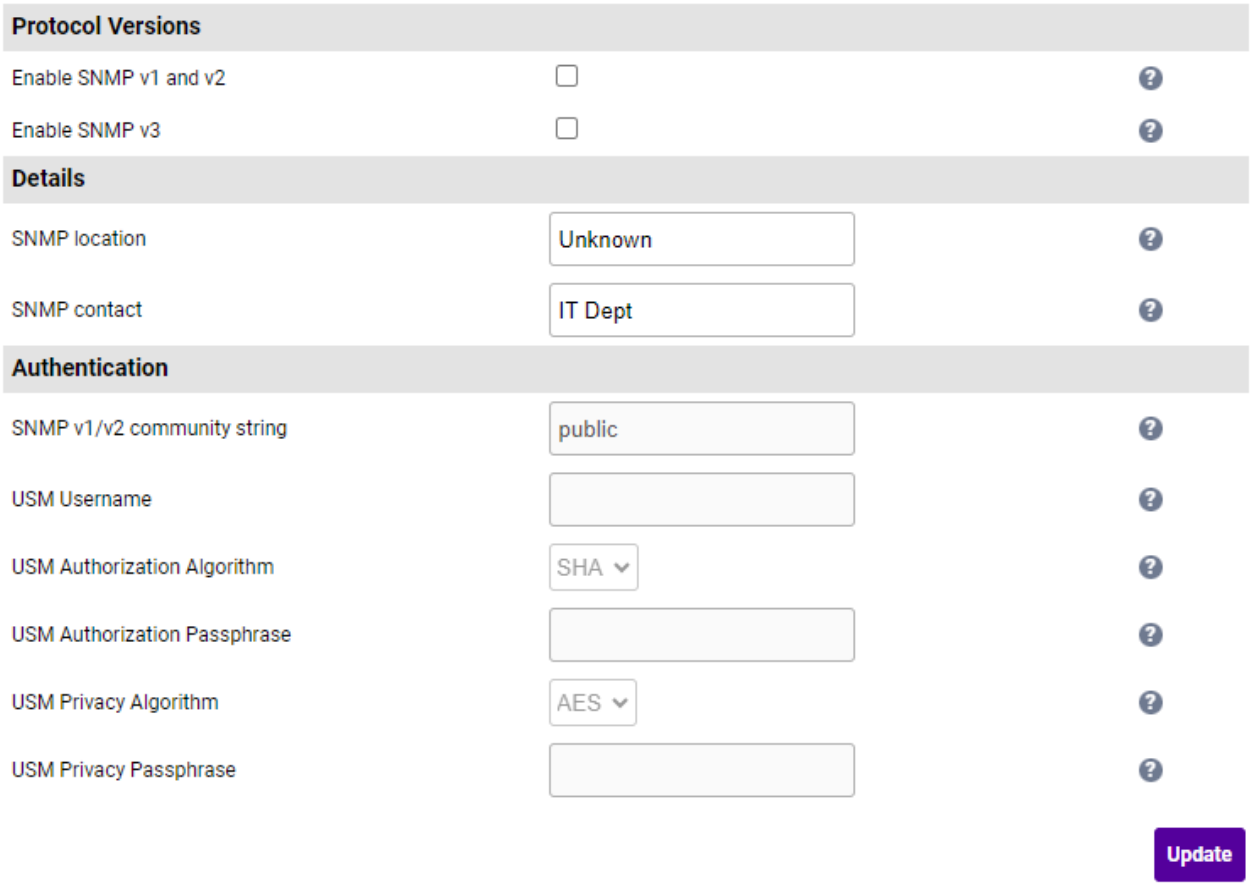
# 12. Optional Appliance Configuration

## 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

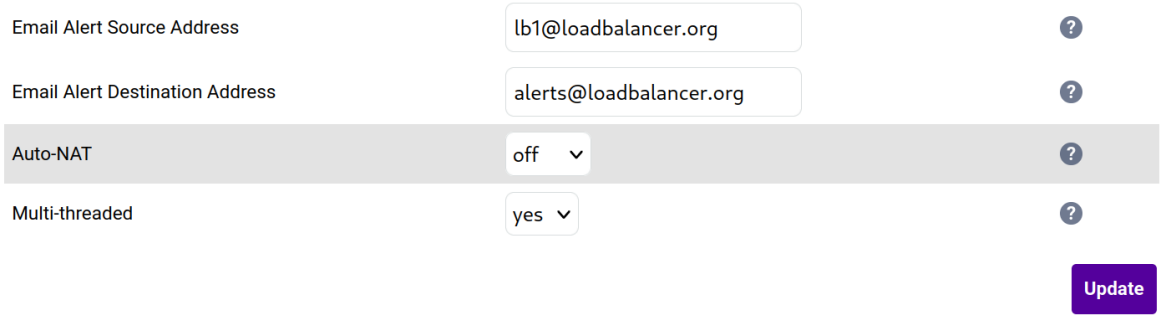
For layer 4 Virtual Services, settings can be configured globally for all VIPs or individually per VIP.

#### 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**.

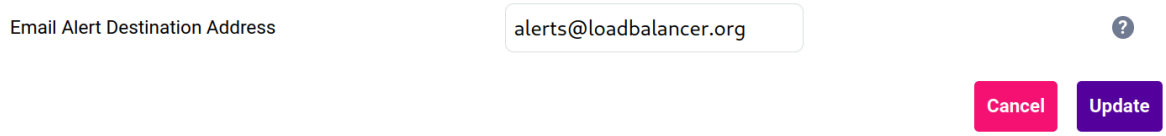
#### 12.2.1.2. VIP Level Settings

> **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**.

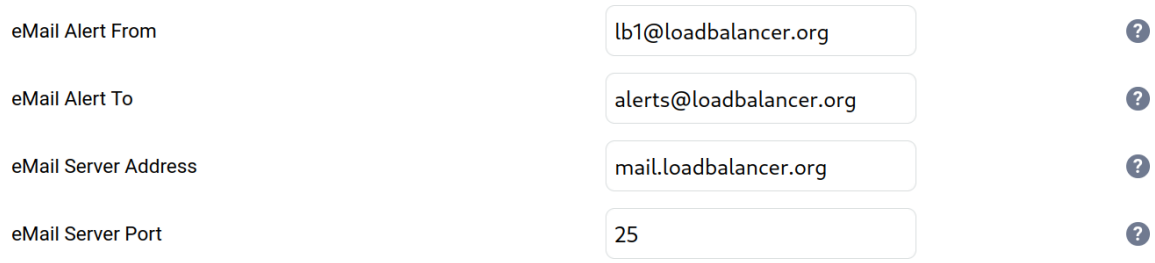
> **Note** You can set the *Email Alert Source Address* field as explained above if required to configure a default source address.

### 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
```

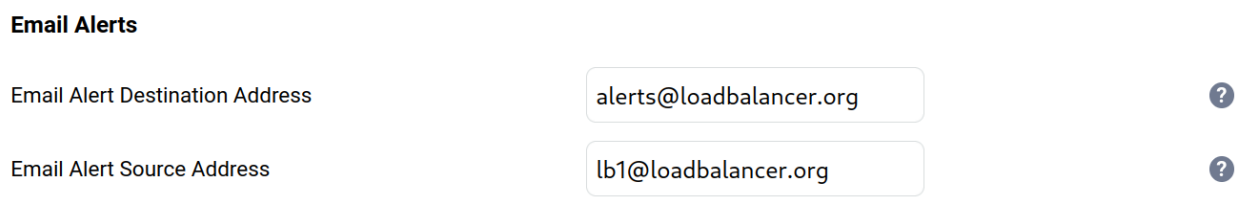
6. Click **Update**.

## 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.

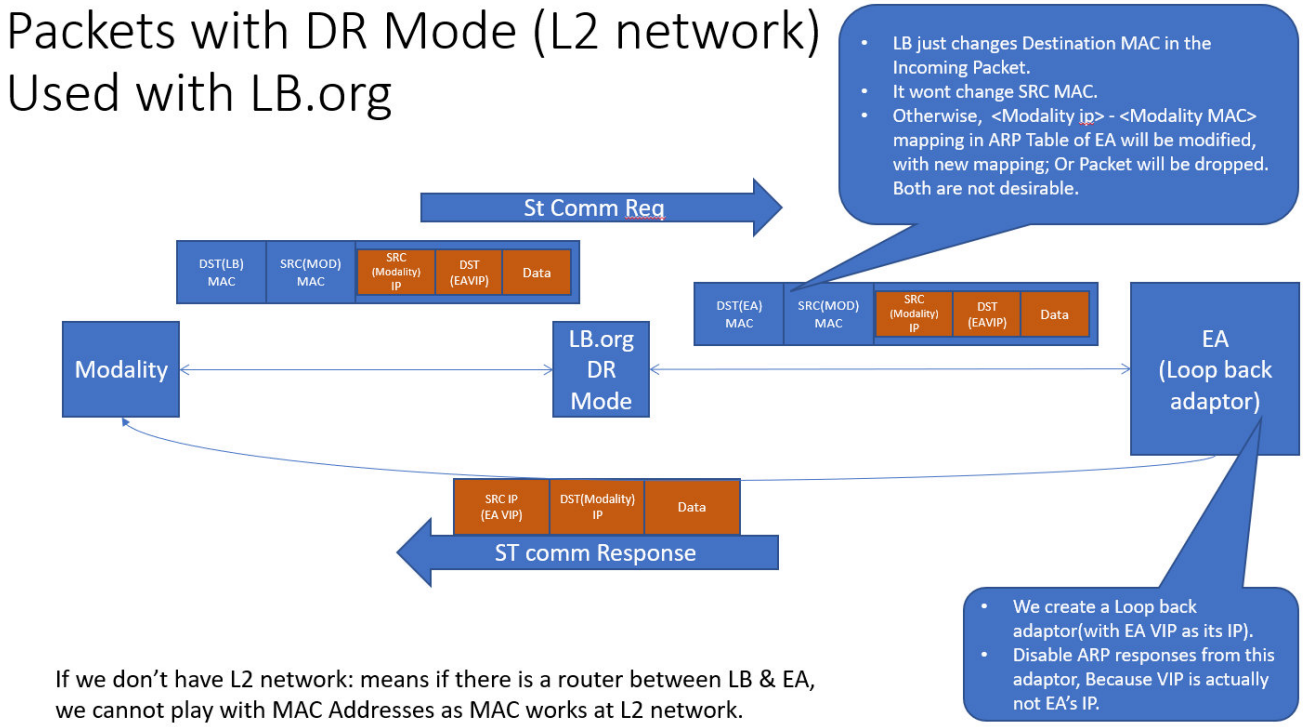
# 14. Further Documentation

For additional information, please refer to the Administration Manual.

# 15. Appendix

## 15.1. DR Mode Packet Manipulation

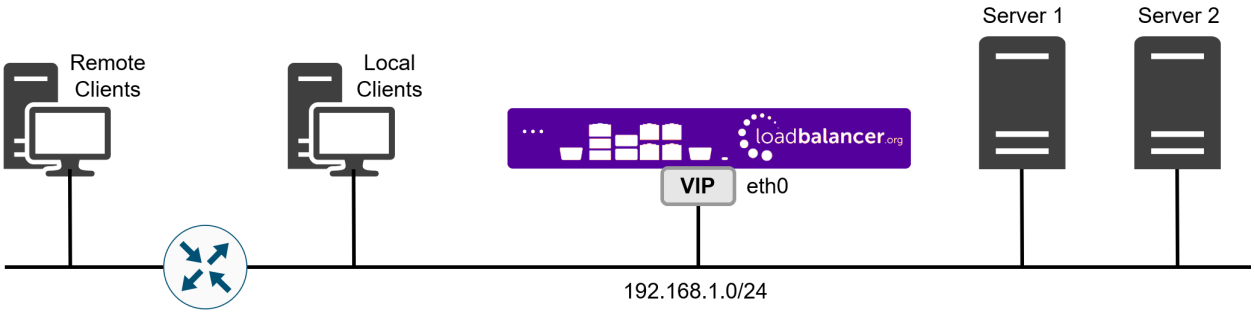
The following diagram shows the traffic flow between the load balancer, the load balanced backend servers and the Modality and how the destination MAC address is modified.




## 15.2. Enabling Layer 7 Transparency

If you require the source IP address of the client to be seen by the CCW 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

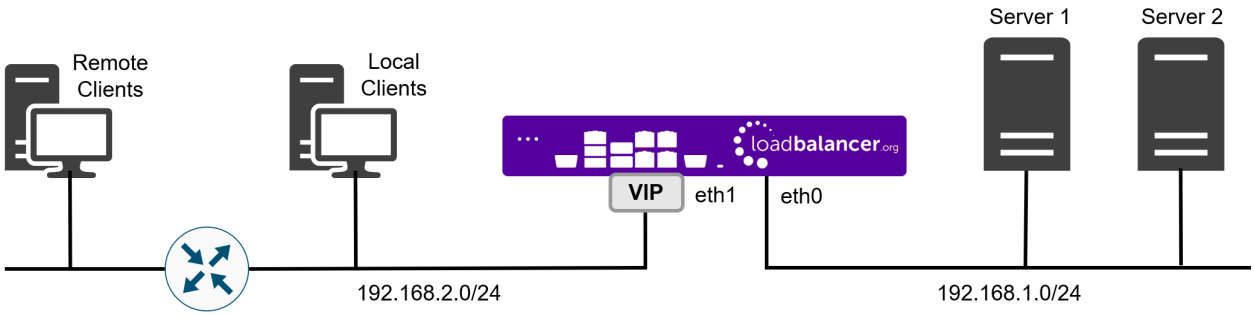



- Here, the VIP is brought up in the same subnet as the Real Servers.
- To support remote clients, the default gateway on the Real Servers must be an IP address on the load balancer and routing on the load balancer must be configured so that return traffic is routed back via the router.

> **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.

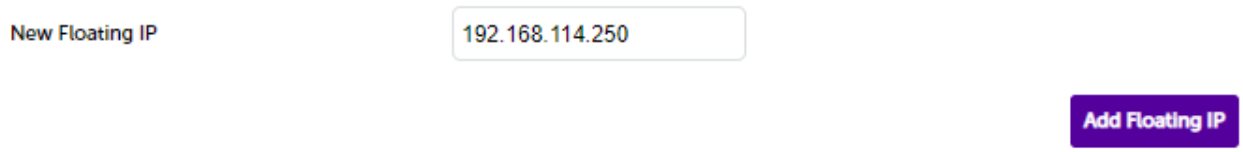
To enable TProxy for a particular layer 7 VIP:

- 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 CCW 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 CCW 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 | 26 September 2023 | Initial version | | RJC |
| 1.1 | 10 May 2024 | Removed various unnecessary VIPs<br><br>Added VIP table for Centricity Cardio Enterprise<br><br>Added VIP table for True PACS Card Solution<br><br>Added VIP table for WFC Services | Required updates | RJC |
| 1.2 | 25 March 2025 | Updated the "Virtual Hardware Resource Requirements" section to list the GE HealthCare virtual appliances that are available and the resource requirements for each<br><br>Removed the Configuration screen step from the "Installing the Appliance using vSphere Client" section since this does not apply to GE HealthCare VAs | Technical accuracy | 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.