

Load Balancing GE HealthCare True PACS

Version 1.0



Table of Contents

1. About this Guide	6
1.1. Acronyms Used in the Guide	6
2. Prerequisites	6
3. Software Versions Supported	6
3.1. Loadbalancer.org Appliance	6
3.2. GE HealthCare TP	6
4. Load Balancing TP	6
4.1. Virtual Services (VIP) Requirements	7
4.2. SSL Termination	9
5. Ports Used by the Appliance	9
6. Deployment Concept	9
7. Load Balancer Deployment Methods	10
7.1. Layer 7 SNAT Mode	10
8. Configuring TP for Load Balancing	11
8.1. Layer 7 SNAT Mode	11
9. Appliance Installation & Configuration for TP	11
9.1. Overview	11
9.2. Virtual Appliance Installation	12
9.2.1. Download & Extract the Appliance	12
9.2.2. Virtual Hardware Resource Requirements	12
9.2.3. VMware vSphere Client	12
9.2.3.1. Upgrading to the latest Hardware Version	12
9.2.3.2. Installing the Appliance using vSphere Client	12
9.2.3.3. Configure Network Adapters	16
9.2.3.4. Start the Appliance	16
9.3. Configuring Initial Network Settings	16
9.4. Accessing the Appliance WebUI	21
9.4.1. Main Menu Options	22
9.5. Appliance Software Update	22
9.5.1. Determining the Current Software Version	23
9.5.2. Checking for Updates using Online Update	23
9.5.3. Using Offline Update	23
9.6. Configuring the Appliance Security Mode	24
9.7. Appliance Network Configuration	24
9.7.1. Verify Network Connections	24
9.7.2. Configuring Hostname & DNS	25
9.7.3. Configuring NTP	25
9.8. Configuring Load Balanced Services	26
9.8.1. Certificates	26
9.8.1.1. Upload the CA Certificate for mTLS	26
9.8.1.2. Upload Certificate(s) for use with Front-end mTLS	26
9.8.1.3. Upload Certificate(s) for use with Back-end mTLS	27
9.8.2. VIP 1 - WFC_RMAMQP	28
9.8.2.1. Virtual Service (VIP) Configuration	28
9.8.2.2. Define the Associated Real Servers (RIPs)	29
9.8.3. VIP 2 - WFC_443	30
9.8.3.1. Virtual Service (VIP) Configuration	30
9.8.3.2. Define the Associated Real Servers (RIPs)	33

9.8.4. VIP 2-B1 - WFC_inference_443	33
9.8.4.1. Virtual Service (VIP) Configuration	33
9.8.4.2. Define the Associated Real Servers (RIPs)	34
9.8.5. VIP 2-B2 - WFC_profiling_443	35
9.8.5.1. Virtual Service (VIP) Configuration	35
9.8.5.2. Define the Associated Real Servers (RIPs)	36
9.8.6. VIP 2-B3 - WFC_patient_443	37
9.8.6.1. Virtual Service (VIP) Configuration	37
9.8.6.2. Define the Associated Real Servers (RIPs)	38
9.8.7. VIP 2-B4 - WFC_CCS_443	39
9.8.7.1. Virtual Service (VIP) Configuration	39
9.8.7.2. Define the Associated Real Servers (RIPs)	40
9.8.8. VIP 2-B5 - WFC_auth_443	41
9.8.8.1. Virtual Service (VIP) Configuration	41
9.8.8.2. Define the Associated Real Servers (RIPs)	42
9.8.9. VIP 2-B6 - WFC_outboundhl7_443	43
9.8.9.1. Virtual Service (VIP) Configuration	43
9.8.9.2. Define the Associated Real Servers (RIPs)	44
9.8.10. VIP 2-B7 - WFC_inboundnotification_443	45
9.8.10.1. Virtual Service (VIP) Configuration	45
9.8.10.2. Define the Associated Real Servers (RIPs)	46
9.8.11. VIP 2-B8 - WFC_eventnotificationmanager_443	46
9.8.11.1. Virtual Service (VIP) Configuration	46
9.8.11.2. Define the Associated Real Servers (RIPs)	47
9.8.12. VIP 2-B9 - WFC_outboundeventpolling_443	48
9.8.12.1. Virtual Service (VIP) Configuration	48
9.8.12.2. Define the Associated Real Servers (RIPs)	49
9.8.13. VIP 2-B10 - WFC_metadata_443	50
9.8.13.1. Virtual Service (VIP) Configuration	50
9.8.13.2. Define the Associated Real Servers (RIPs)	51
9.8.14. VIP 2-B11 - WFC_studymanagement_443	52
9.8.14.1. Virtual Service (VIP) Configuration	52
9.8.14.2. Define the Associated Real Servers (RIPs)	53
9.8.15. VIP 2-B12 - WFC_xe_443	54
9.8.15.1. Virtual Service (VIP) Configuration	54
9.8.15.2. Define the Associated Real Servers (RIPs)	55
9.8.16. VIP 2-B13 - WFC_recordmanager_443	56
9.8.16.1. Virtual Service (VIP) Configuration	56
9.8.16.2. Define the Associated Real Servers (RIPs)	57
9.8.17. VIP 3 - WFC_http	58
9.8.17.1. Virtual Service (VIP) Configuration	58
9.8.17.2. Define the Associated Real Servers (RIPs)	62
9.8.18. VIP 3-B1 - WFC_inference_80	62
9.8.18.1. Virtual Service (VIP) Configuration	62
9.8.18.2. Define the Associated Real Servers (RIPs)	63
9.8.19. VIP 3-B2 - WFC_profiling_80	63
9.8.19.1. Virtual Service (VIP) Configuration	63
9.8.19.2. Define the Associated Real Servers (RIPs)	64
9.8.20. VIP 3-B3 - WFC_CCS_80	65
9.8.20.1. Virtual Service (VIP) Configuration	65
9.8.20.2. Define the Associated Real Servers (RIPs)	66

9.8.21. VIP 3-B4 - WFC_auth_80	67
9.8.21.1. Virtual Service (VIP) Configuration	67
9.8.21.2. Define the Associated Real Servers (RIPs)	68
9.8.22. VIP 3-B5 - WFC_outboundeventpolling_80	68
9.8.22.1. Virtual Service (VIP) Configuration	68
9.8.22.2. Define the Associated Real Servers (RIPs)	69
9.8.23. VIP 3-B6 - WFC_inboundnotification_80	70
9.8.23.1. Virtual Service (VIP) Configuration	70
9.8.23.2. Define the Associated Real Servers (RIPs)	71
9.8.24. VIP 3-B7 - WFC_eventnotificationmanager_80	72
9.8.24.1. Virtual Service (VIP) Configuration	72
9.8.24.2. Define the Associated Real Servers (RIPs)	73
9.8.25. VIP 3-B8 - WFC_metadata_80	73
9.8.25.1. Virtual Service (VIP) Configuration	73
9.8.25.2. Define the Associated Real Servers (RIPs)	74
9.8.26. VIP 3-B9 - WFC_patient_80	75
9.8.26.1. Virtual Service (VIP) Configuration	75
9.8.26.2. Define the Associated Real Servers (RIPs)	76
9.8.27. VIP 3-B10 - WFC_masterfileapp_80	77
9.8.27.1. Virtual Service (VIP) Configuration	77
9.8.27.2. Define the Associated Real Servers (RIPs)	78
9.8.28. VIP 3-B11 - WFC_masterfiledata_80	78
9.8.28.1. Virtual Service (VIP) Configuration	78
9.8.28.2. Define the Associated Real Servers (RIPs)	79
9.8.29. VIP 3-B12 - WFC_studymanagement_80	80
9.8.29.1. Virtual Service (VIP) Configuration	80
9.8.29.2. Define the Associated Real Servers (RIPs)	81
9.8.30. VIP 3-B13 - WFC_xe_80	82
9.8.30.1. Virtual Service (VIP) Configuration	82
9.8.30.2. Define the Associated Real Servers (RIPs)	83
9.8.31. VIP 4 - WFC_10443	83
9.8.31.1. Virtual Service (VIP) Configuration	83
9.8.31.2. Define the Associated Real Servers (RIPs)	85
9.8.32. VIP 4-B1 - WFC_masterfiledata_10443	85
9.8.32.1. Virtual Service (VIP) Configuration	85
9.8.32.2. Define the Associated Real Servers (RIPs)	86
9.8.33. VIP 4-B2 - WFC_masterfileapp_10443	87
9.8.33.1. Virtual Service (VIP) Configuration	87
9.8.33.2. Define the Associated Real Servers (RIPs)	88
9.8.34. VIP 4-B3 - WFC_xeui_10443	89
9.8.34.1. Virtual Service (VIP) Configuration	89
9.8.34.2. Define the Associated Real Servers (RIPs)	90
9.8.35. VIP 5 - WFM_karaf_Group	91
9.8.35.1. Virtual Service (VIP) Configuration	91
9.8.35.2. Define the Associated Real Servers (RIPs)	92
9.8.36. VIP 6 - SR_https_vs	93
9.8.36.1. Virtual Service (VIP) Configuration	93
9.8.36.2. Define the Associated Real Servers (RIPs)	94
9.8.37. Finalizing the Configuration	94
10. Testing & Verification	95
11. Configuring HA - Adding a Secondary Appliance	97

11.1. Non-Replicated Settings	97
11.2. Configuring the HA Clustered Pair	98
12. Optional Appliance Configuration	99
12.1. SNMP Configuration	99
12.2. Configuring Email Alerts for Virtual Services	101
12.2.1. Layer 4	101
12.2.1.1. Global Layer 4 Email Settings	101
12.2.1.2. VIP Level Settings	101
12.2.2. Layer 7	102
12.3. Configuring Email Alerts for Heartbeat	103
12.4. Configuring a Smart Host (SMTP relay)	103
13. Technical Support	104
14. Further Documentation	104
15. Appendix	105
15.1. Enabling Layer 7 Transparency	105
15.1.1. TProxy Topology Requirements - One-arm Deployments	105
15.1.2. TProxy Topology Requirements - Two-arm Deployments	105
15.1.3. Configuring a floating IP Address for the True PACS Servers' Default Gateway	106
16. Document Revision History	107

1. About this Guide

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

1.1. Acronyms Used in the Guide

Acronym	Description
TP	True PACS
WFC	Workflow Core
CCS	Centralized Configuration Service

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 TP servers.
6. Have IP addresses for the VA and all required Virtual Services.

3. Software Versions Supported

3.1. Loadbalancer.org Appliance

- V8.9.0 & later

3.2. GE HealthCare TP

- All versions

4. Load Balancing TP

Note

It's highly recommended that you have a working TP environment first before implementing the load balancer.



4.1. Virtual Services (VIP) Requirements

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

Ref.	VIP Name	Mode/Type	Port(s)	Persistence Mode	Health Check
VIP 1	WFC_RMQAMQP	L7 SNAT	8081	None	Connect to Port
VIP 2	WFC_443	L7 SNAT	8443	None	No Checks, Always On
VIP 2-B1	WFC_inference_443	Backend Only	-	None	HTTPS (GET)
VIP 2-B2	WFC_profiling_443	Backend Only	-	None	HTTPS (GET)
VIP 2-B3	WFC_patient_443	Backend Only	-	None	HTTPS (GET)
VIP 2-B4	WFC_CCS_443	Backend Only	-	None	HTTPS (GET)
VIP 2-B5	WFC_auth_443	Backend Only	-	None	HTTPS (GET)
VIP 2-B6	WFC_outboundhl7_443	Backend Only	-	None	HTTPS (GET)
VIP 2-B7	WFC_inboundnotification_443	Backend Only	-	None	HTTPS (GET)
VIP 2-B8	WFC_eventnotificationmanager_443	Backend Only	-	None	HTTPS (GET)
VIP 2-B9	WFC_outboundeventpolling_443	Backend Only	-	None	HTTPS (GET)
VIP 2-B10	WFC_metadata_443	Backend Only	-	None	HTTPS (GET)
VIP 2-B11	WFC_studymanagement_443	Backend Only	-	None	HTTPS (GET)
VIP 2-B12	WFC_xe_443	Backend Only	-	None	HTTPS (GET)
VIP 2-B13	WFC_recordmanager_443	Backend Only	-	None	HTTPS (GET)
VIP 3	WFC_http	L7 SNAT	80	None	No Checks, Always On
VIP 3-B1	WFC_inference_80	Backend Only	-	None	HTTPS (GET)
VIP 3-B2	WFC_profiling_80	Backend Only	-	None	HTTPS (GET)
VIP 3-B3	WFC_CCS_80	Backend Only	-	None	HTTPS (GET)
VIP 3-B4	WFC_auth_80	Backend Only	-	None	HTTPS (GET)
VIP 3-B5	WFC_outboundeventpolling_80	Backend Only	-	None	HTTPS (GET)
VIP 3-B6	WFC_inboundnotification_80	Backend Only	-	None	HTTPS (GET)
VIP 3-B7	WFC_eventnotificationmanager_80	Backend Only	-	None	HTTPS (GET)
VIP 3-B8	WFC_metadata_80	Backend Only	-	None	HTTPS (GET)
VIP 3-B9	WFC_patient_80	Backend Only	-	None	HTTPS (GET)
VIP 3-B10	WFC_masterfileapp_80	Backend Only	-	None	HTTPS (GET)
VIP 3-B11	WFC_masterfiledata_80	Backend Only	-	None	HTTPS (GET)
VIP 3-B12	WFC_studymanagement_80	Backend Only	-	None	HTTPS (GET)



Ref.	VIP Name	Mode/Type	Port(s)	Persistence Mode	Health Check Mode
VIP 3-B13	WFC_xe_80	Backend Only	-	None	HTTP (GET)
VIP 4	WFC_10443	L7 SNAT	8082	None	No Checks, Always On
VIP 4-B1	WFC_masterfiledata_10443	Backend Only	-	None	HTTPS (GET)
VIP 4-B2	WFC_masterfileapp_10443	Backend Only	-	None	HTTPS (GET)
VIP 4-B3	WFC_xeui_10443	Backend Only	-	None	HTTPS (GET)
VIP 5	WFM_karaf_Group	L7 SNAT	9094	Source IP	HTTPS (GET)
VIP 6	SR_https_vs	L7 SNAT	3080	None	HTTPS (GET)

Note

VIPs with references in the format **VIP <number>-B<number>** are *Backend Only* VIPs. These are used to define a pool of Real Servers. ACL's are then used by the 'parent' VIP to determine which *Backend Only* VIP should be selected based on the requested URL.

In addition, the following CPACS Virtual Services may also be needed depending on the specific site requirements:

Note

Clicking on the VIP reference will open the relevant page in the CPACS deployment guide.

Ref.	Remote Ref.	VIP Name	Mode	Port(s)	Persist Mode	Health Check
VIP 7	VIP 1	EA_XDS_Service	L4 DR	80	None	HTTP (GET)
VIP 8	VIP 2	EA_Dicom_Service	L4 DR	104	None	HTTP (GET)
VIP 9	VIP 3	EA_Secure_Dicom_Service	L4 DR	2762	None	HTTP (GET)
VIP 10	VIP 4	EA_HL7_Service	L4 DR	2575	None	HTTP (GET)
VIP 11	VIP 5	EA_Secure_HL7_Service	L4 DR	2576	None	HTTP (GET)
VIP 12	VIP 6	EA_Study_Management_Service	L4 DR	443	None	HTTP (GET)
VIP 13	VIP 10	ZFP	L7 SNAT	443	Source IP	HTTPS (GET)
VIP 14	VIP 11	UV	L7 SNAT	443	Source IP	HTTPS (GET)
VIP 15	VIP 12	Dakota	L7 SNAT	SP1: 8080, SP2: 8443	Source IP	SP1: Connect to port, SP2: HTTPS (GET)
VIP 16	VIP 13	WFM_Play_Group	L7 SNAT	SP1: 8080, SP2: 9443	Source IP	HTTPS (GET)
VIP 17	VIP 14	WFM_tomcat_Group	L7 SNAT	SP1: 9096, SP2: 9096,3443	Source IP	HTTPS (GET)
VIP 18	VIP 15	XE_Standalone	L7 SNAT	8443,9449	Source IP	HTTPS (GET)



4.2. SSL Termination

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

- VIP1 - **WFC_RMQAMQP**
- VIP2 - **WFC_443**
- VIP4 - **WFC_10443**

And for the Following CPACS VIPs:

- VIP 15 - **Dakota**
- VIP 16 - **WFM_Play_Group**

This provides a corresponding HTTPS Virtual Service for these VIPs. 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:

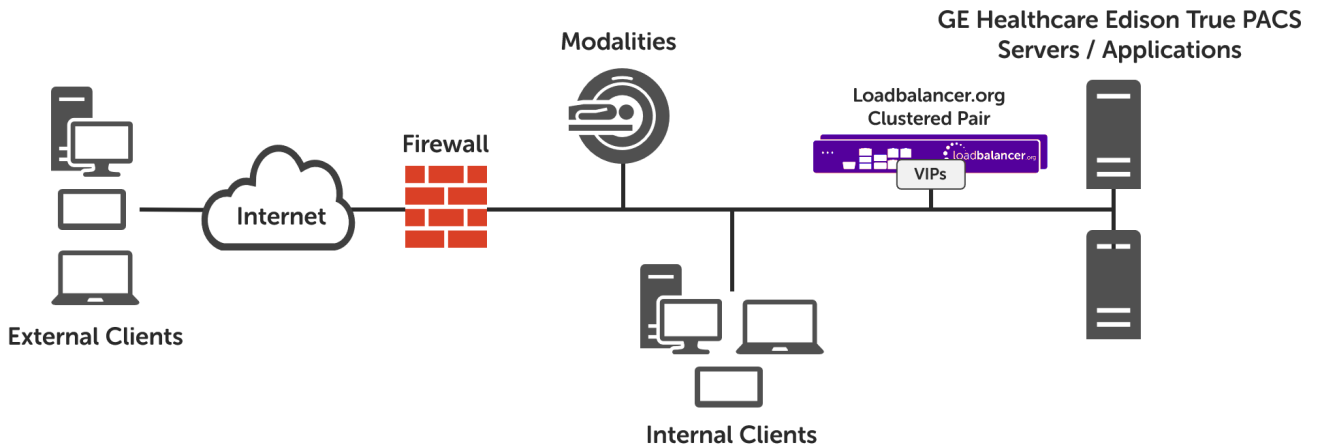
Protocol	Port	Purpose
TCP	22 *	SSH
TCP & UDP	53 *	DNS / GSLB
TCP & UDP	123	NTP
TCP & UDP	161 *	SNMP
UDP	6694	Heartbeat between Primary & Secondary appliances in HA mode
TCP	7778	HAProxy persistence table replication
TCP	9000 *	Gateway service (Centralized/Portal Management)
TCP	9080 *	WebUI - HTTP (disabled 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





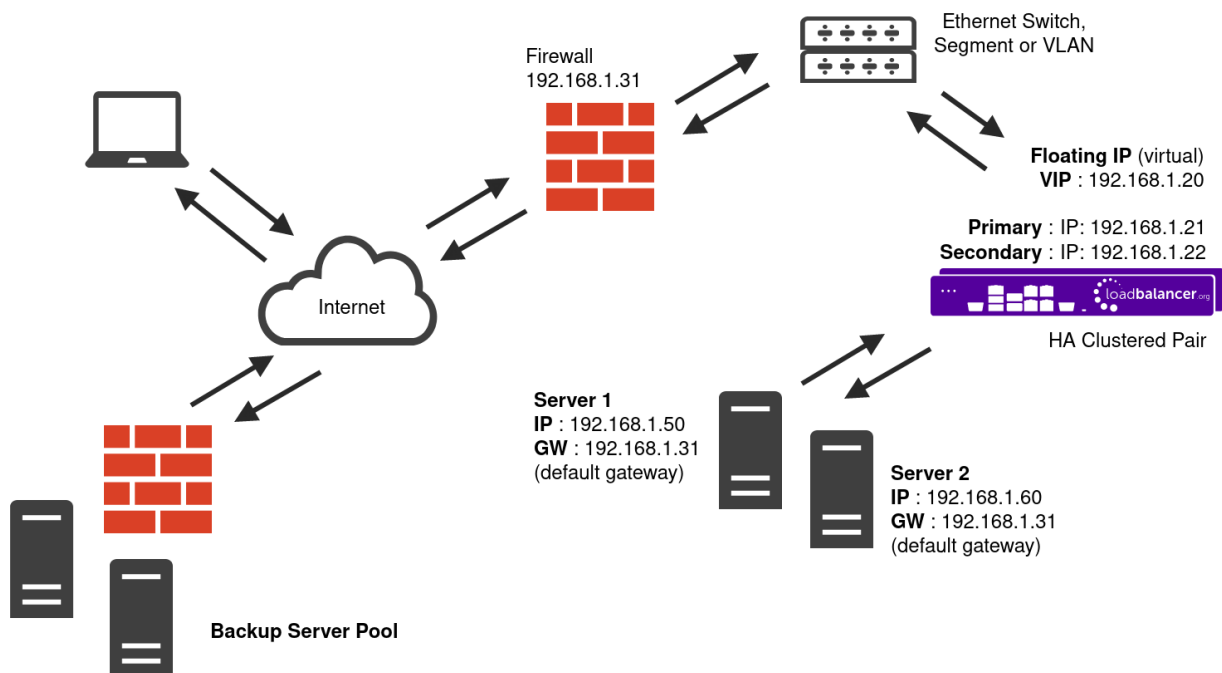
VIP = **V**irtual **IP** Address

7. Load Balancer Deployment Methods

For TP, layer 7 SNAT mode is used. This mode is described below and is used for the configurations presented in this guide.

7.1. Layer 7 SNAT Mode

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



- Because layer 7 SNAT mode is a full proxy, any server in the cluster can be on any accessible subnet including across the Internet or WAN.

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

8. Configuring TP 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 (TP Servers).

9. Appliance Installation & Configuration for TP

9.1. Overview

For TP 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 9.8.37](#)
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

By default, the GE HealthCare appliance is allocated the following resources:

- 4 vCPUs
- 8GB RAM
- 20GB disk

These settings can be left at their default values unless advised otherwise.

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**.



Deploy OVF Template

1 Select an OVF template | Select an OVF template

2 Select a name and folder | Select an OVF template from remote URL or local file system

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

2 files

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**.

Deploy OVF Template

✓ **1 Select an OVF template** | **Select a name and folder**

2 **Select a name and folder** | Specify a unique name and target location

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Virtual machine name:

Select a location for the virtual machine.

▼ vcs.loadbalancer.org

> Portsmouth

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**.



Deploy OVF Template

✓ 1 Select an OVF template
✓ 2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select a compute resource
Select the destination compute resource for this operation

Portsmouth

- Compass House
 - host1.loadbalancer.org
 - host2.loadbalancer.org
- Accounts
- Dev
- Solutions
- Support
- Test Lab - 192.168.120.x

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

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

Deploy OVF Template

✓ 1 Select an OVF template
✓ 2 Select a name and folder
✓ 3 Select a compute resource
4 Review details
5 Select storage
6 Select networks
7 Ready to complete

Review details
Verify the template details.

Publisher	No certificate present
Description	Loadbalancer.org VA - Traffic Management and Load Balancing Appliance from www.loadbalancer.org
Download size	437.9 MB
Size on disk	1.3 GB (thin provisioned) 20.0 GB (thick provisioned)

CANCEL BACK NEXT

7. In the **Configuration** screen, select the required CPU/RAM deployment configuration and click **Next**.



Note

These settings can be changed after deployment if needed.

Deploy OVF Template

Configuration
Select a deployment configuration

- 2 CPUs/4 GB RAM
- 4 CPUs/8 GB RAM
- 8 CPUs/16 GB RAM

Description
2 CPUs and 4 GB RAM.

3 Items

CANCEL BACK NEXT

8. In the **Select Storage** screen, first select the required storage location for the appliance.

9. 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.

Deploy OVF Template

Select storage
Select the storage for the configuration and disk files

Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thick Provision Lazy Zeroed

VM Storage Policy: Datastore Default

Disable Storage DRS for this virtual machine

Name	Capacity	Provisioned	Free	Type	Cluster
Portsmouth Datastore	65.49 TB	25.65 TB	39.83 TB		
ISO Store	179.99 GB	86.77 GB	93.22 GB	NFS v3	
Linux Templates	196.98 GB	59.67 GB	137.32 GB	NFS v3	
Loadbalancer Appliance...	196.98 GB	109.67 GB	87.31 GB	NFS v3	
Windows Template Store	296.98 GB	184.39 GB	112.59 GB	NFS v3	

Compatibility
 Compatibility checks succeeded.

CANCEL BACK NEXT

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



Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- 6 Select networks**
- 7 Ready to complete

Select networks

Select a destination network for each source network.

Source Network	Destination Network
VM Network	Office Port Group

IP Allocation Settings

IP allocation: Static - Manual
IP protocol: IPv4

CANCEL BACK NEXT

11. 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.

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- ✓ 6 Select networks
- 7 Ready to complete**

Ready to complete

Click Finish to start creation.

Provisioning type	Deploy from template
Name	Loadbalancer.org Enterprise VA
Template name	Loadbalancer.org Enterprise VA
Download size	437.9 MB
Size on disk	20.0 GB
Folder	Portsmouth
Resource	Solutions
Storage mapping	1
All disks	Datastore: Portsmouth Datastore; Format: Thick provision lazy zeroed
Network mapping	1
VM Network	VM Network
IP allocation settings	
IP protocol	IPv4
IP allocation	Static - Manual

CANCEL BACK FINISH

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:



```

Welcome to the Loadbalancer.org appliance.

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

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

lbmaster login:

```

As mentioned in the text, 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.

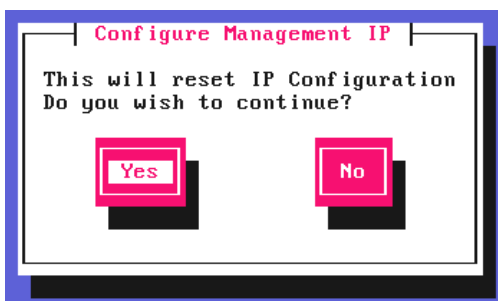
login to the console:

Username: setup

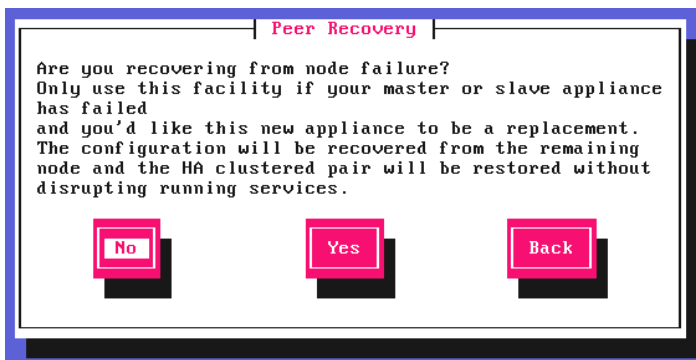
Password: setup

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.



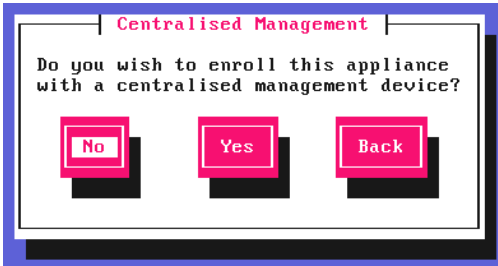
In the **Peer Recovery** screen, leave **No** selected and hit <ENTER> to continue.



In the **Centralized Management** screen, if you have been provided with Management Server details select **Yes**,



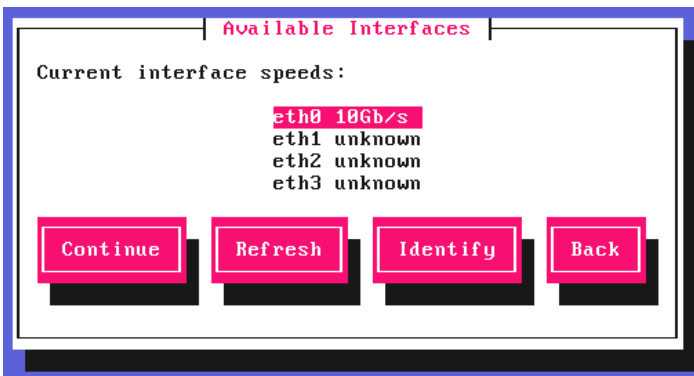
otherwise leave **No** selected, then hit <ENTER> to continue.



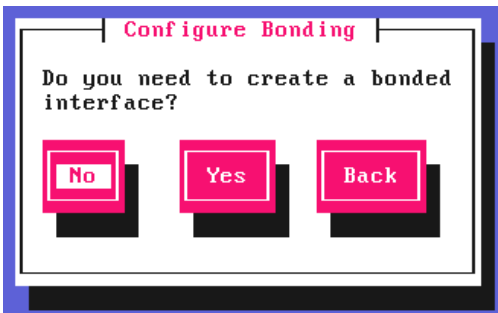
Note

For information on how to modify Centralized Management settings via the WebUI, please refer to [Portal Management & Appliance Adoption](#).

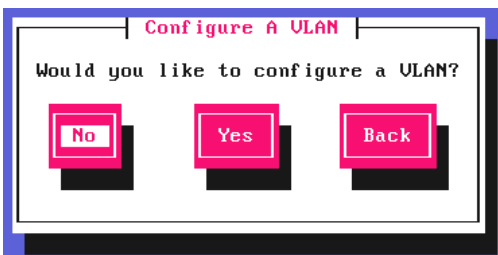
In the **Available Interfaces** screen, a list of available interfaces will be displayed, hit <ENTER> to continue.



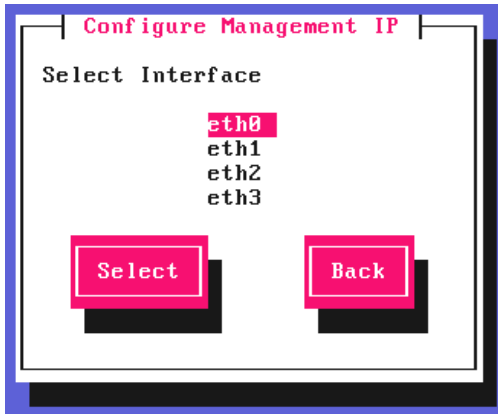
In the **Configure Bonding** screen, leave **No** selected, then hit <ENTER> to continue.



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.



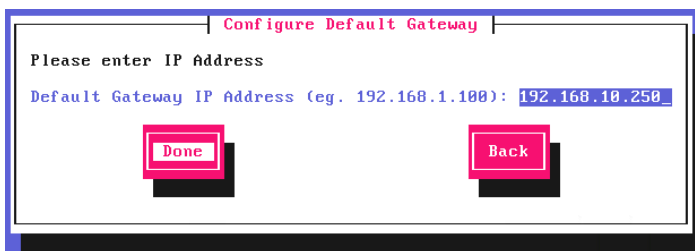
In the **Set IP address** screen, specify the required management address in the *Static IP Address & CIDR Prefix* fields, select **Done** and hit <ENTER> to continue.



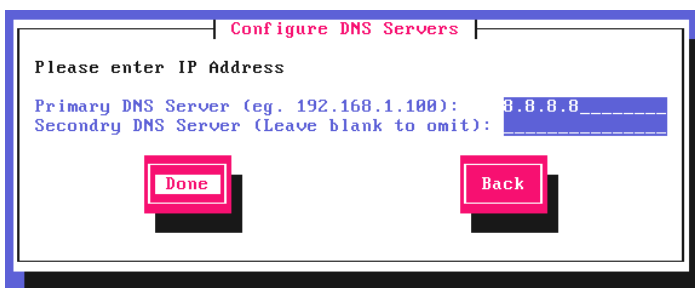
Note

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.



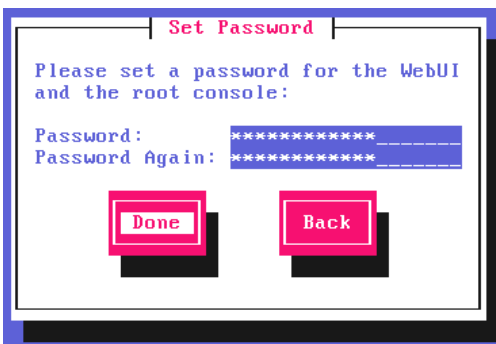
In the **Configure DNS Servers** screen, configure the required DNS server(s), select **Done** and hit <ENTER> to continue.



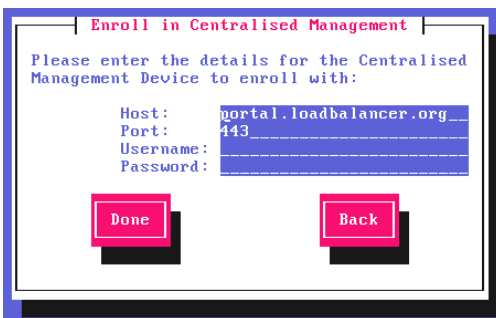
In the **Set Password** screen, hit <ENTER> to continue.



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.



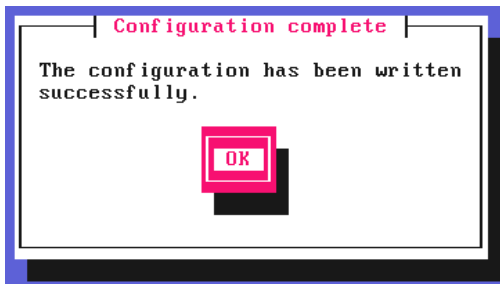
If you selected **Yes** when asked if you want to enroll for Centralized Management, you'll now be prompted for the details. Default values for the *Host* and *Port* are set and can be changed if required. Enter the *Username* and *Password* for the management server account you'd like the appliance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



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:

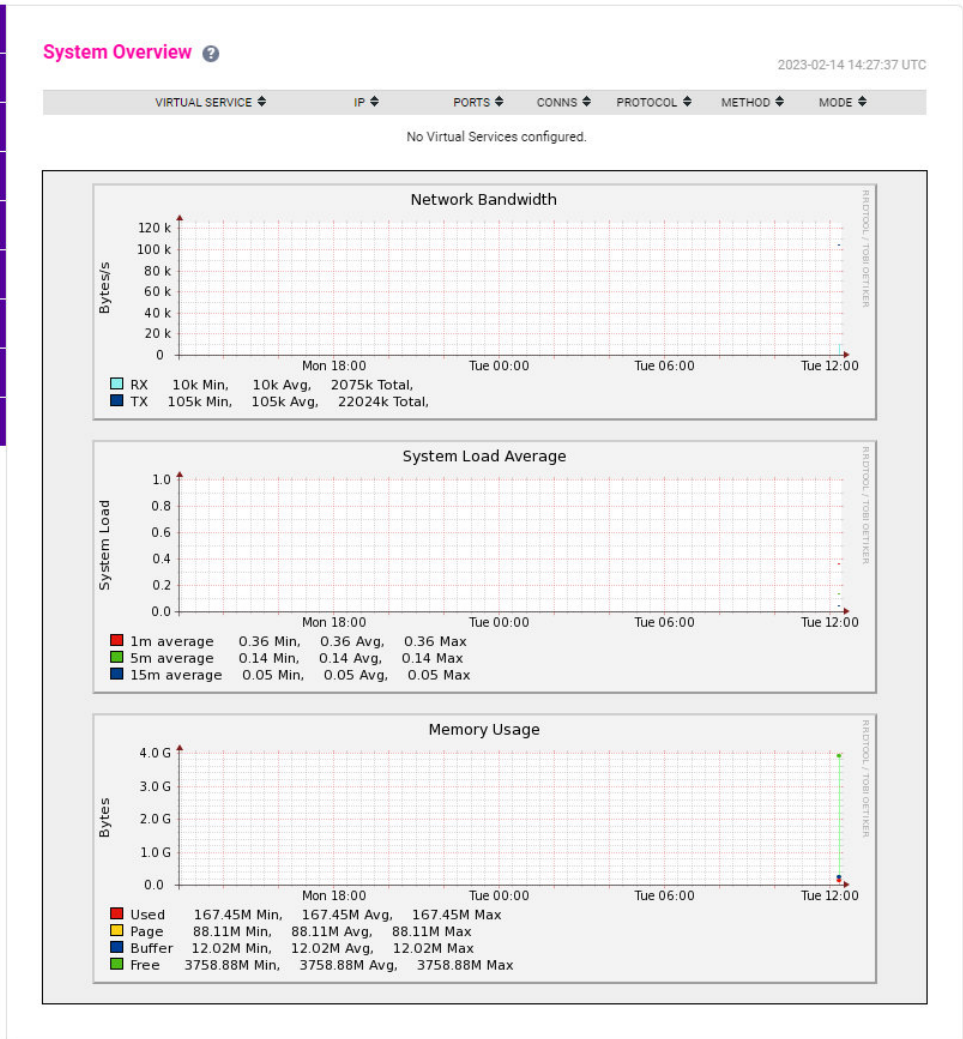
Primary | Secondary

Active | Passive

Link

12 Seconds

- System Overview
- Local Configuration
- Cluster Configuration
- Maintenance
- View Configuration
- Reports
- Logs
- Support
- Live Chat



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 taking backups

View Configuration - Display the saved appliance configuration settings

Reports - View various appliance reports & graphs

Logs - View various appliance logs

Support - Create a support download, contact the support team & access useful links

Live Chat - Start a live chat session with one of our Support Engineers

9.5. Appliance Software Update

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

9.5.1. Determining the Current Software Version

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

Copyright © Loadbalancer.org Inc. 2002 – 2024
ENTERPRISE VA Max - v8.11.1

English ▼

9.5.2. Checking for Updates using Online Update

Note

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

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

Information: Version v8.11.2 is the current release. No updates are available

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

Note

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

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

Information: Update completed successfully.

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

9.5.3. Using Offline Update

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

Note

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

To perform an offline update:



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

Software Update

Offline Update

The following steps will lead you through offline update.

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

Archive: No file chosen
Checksum: No file chosen

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

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 TP 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*.



IP Address Assignment

eth0 10 GB/s

eth0 192.168.10.10/24 MTU 1500 bytes

eth1 MTU 1500 bytes

eth2 MTU 1500 bytes

eth3 MTU 1500 bytes

Configure Interfaces

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 the CA Certificate for mTLS

Note

These certificates are selected using the *CA Certificate* dropdown when configuring Virtual Services with SSL termination and the *Verify Server Certificate* dropdown when configuring Real Servers.

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

Certificate family details		
Family label	<input type="text" value="mTLS"/>	?
Certificate label	<input type="text" value="ca-cert"/>	?
Certificate contents	<input type="button" value="Choose File"/> ca-cert.pem	?

- 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**.

9.8.1.2. Upload Certificate(s) for use with Front-end mTLS

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:

I would like to:

Upload prepared PEM/PFX file

Create a new SSL Certificate Signing Request (CSR) ?

Create a new Self-Signed SSL Certificate.

Label ?

File to upload server-cert.pem ?

- 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.

9.8.1.3. Upload Certificate(s) for use with Back-end mTLS

Note

These certificates are selected using the *Send Client Certificate* dropdown when configuring Real Servers.

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:

I would like to:

Upload prepared PEM/PFX file

Create a new SSL Certificate Signing Request (CSR) ?

Create a new Self-Signed SSL Certificate.

Label ?

File to upload client-cert.pem ?

- Specify an appropriate *Label*, e.g. **client-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 the above steps if additional certificates must be uploaded.

9.8.2. VIP 1 - WFC_RMQAMQP

9.8.2.1. 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 to the *Termination* section.
 - Enable (check) the *Create HAProxy SSL Termination* checkbox.
4. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input type="checkbox"/>	?
Label	<input type="text" value="WFC_RMQAMQP"/>	?
IP Address	<input type="text" value="10.177.215.149"/>	?
Ports	<input type="text" value="8081"/>	?
Protocol		[Advanced +]
Layer 7 Protocol	<input type="text" value="TCP Mode"/>	?
Termination		
Create HAProxy SSL Termination	<input checked="" type="checkbox"/>	?
Termination Port	<input type="text" value="5672"/>	?
SSL Certificate	<input type="text" value="server-cert"/>	?
CA Certificate	<input type="text" value="mTLS"/>	?

- Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_RMQAMQP**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.177.215.149**.
- Set the *Ports* field to **8081**.
- Set the *Layer 7 Protocol* to **TCP Mode**.
- Set the *Termination Port* to **5672**.
- Set the *SSL Certificate* to the appropriate certificate, e.g. **server-cert**.
- Set the *CA Certificate* to the appropriate certificate, e.g. **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 *Balance Mode* to **Weighted Round Robin**.
8. Scroll to the *Persistence* section.
 - Ensure that the *Persistence Mode* is set to **None**.
9. Scroll to the *Health Checks* section and click **[Advanced]**.
 - Set the *Check Type* to **Connect to Port**.
 - Set the *Check Port* to **4672**.
10. Scroll to the *SSL* section.
 - Ensure that *Enable Backend Encryption* is enabled (checked).
11. Leave all other settings at their default value.
12. Click **Update**.

9.8.2.2. 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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="5672"/>	?
Re-Encrypt to Backend	<input checked="" type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
 - Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
 - Set the *Real Server Port* field to **5672**.
 - Ensure that *Re-Encrypt to Backend* is enabled (checked).
3. Leave all other settings at their default value.
 4. Click **Update**.

5. Now click **Modify** next to the newly created Real Server.
6. Set the *Send Client Certificate* dropdown to the required certificate, e.g. **client-cert**.
7. Click **Update**.
8. Repeat these steps to add additional Real Server(s).

9.8.3. VIP 2 - WFC_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]** in the *Virtual Service* heading bar.
3. Scroll to to the *Termination* section.
 - Enable (check) the *Create HAProxy SSL Termination* checkbox.
4. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input type="checkbox"/>	?
Label	<input type="text" value="WFC_443"/>	?
IP Address	<input type="text" value="10.177.215.149"/>	?
Ports	<input type="text" value="8443"/>	?
Protocol		[Advanced +]
Layer 7 Protocol	<input style="border: none; border-bottom: 1px solid #ccc;" type="text" value="HTTP Mode"/> ▼	?
Termination		
Create HAProxy SSL Termination	<input checked="" type="checkbox"/>	?
Termination Port	<input type="text" value="443"/>	?
SSL Certificate	<input style="border: none; border-bottom: 1px solid #ccc;" type="text" value="server-cert"/> ▼	?
CA Certificate	<input style="border: none; border-bottom: 1px solid #ccc;" type="text" value="mTLS"/> ▼	?

Cancel
Update

- Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_443**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.177.215.149**.
- Set the *Ports* field to **8443**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.
- Set the *Termination Port* to **443**.



- Set the *SSL Certificate* to the appropriate certificate, e.g. **server-cert**.
- Set the *CA Certificate* to the appropriate certificate, e.g. **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 *Balance Mode* to **Weighted Round Robin**.

8. Scroll to the *Persistence* section.

- Ensure that the *Persistence Mode* is set to **None**.

9. Scroll to the *Health Checks* section.

- Set the *Check Type* to **No checks, Always On**.

10. Scroll to the *ACL Rules* section.

11. Using the **Add Rule** button, add the following ACL rules:

- **Rule 1**

```
Type:          path_reg
Bool:          Equals
URL/Text:      /api/v[0-9]*/configstore
Action:        Use Backend
Location/Value: WFC_CCS_443
```

- **Rule 2**

```
Type:          path_reg
Bool:          Equals
URL/Text:      /api/v[0-9]*/inference
Action:        Use Backend
Location/Value: WFC_inference_443
```

- **Rule 3**

```
Type:          path_reg
Bool:          Equals
URLText:       /api/v[0-9]*/profiling
Action:        Use Backend
Location/Value: WFC_profiling_443
```

- **Rule 4**

```
Type:          path_reg
Bool:          Equals
URLText:       /api/v[0-9]*/inboundnotification
Action:        Use Backend
```



Location/Value: WFC_inboundnotification_443

▪ Rule 5

Type: path_reg
Bool: Equals
URLText: /api/v[0-9]*/outboundeventpolling
Action: Use Backend
Location/Value: WFC_outboundeventpolling_443

▪ Rule 6

Type: path_reg
Bool: Equals
URLText: /api/v[0-9]*/outboundh17
Action: Use Backend
Location/Value: WFC_outboundh17_443

▪ Rule 7

Type: path_reg
Bool: Equals
URLText: /api/v[0-9]*/patient
Action: Use Backend
Location/Value: WFC_patient_443

▪ Rule 8

Type: path_reg
Bool: Equals
URLText: /api/v[0-9]*/auth
Action: Use Backend
Location/Value: WFC_auth_443

▪ Rule 9

Type: path_reg
Bool: Equals
URLText: /api/v[0-9]*/eventnotificationmanager
Action: Use Backend
Location/Value: WFC_eventnotificationmanager_443

▪ Rule 10

Type: path_reg
Bool: Equals
URLText: /api/v[0-9]*/metadata
Action: Use Backend



Location/Value: WFC_metadata_443

▪ Rule 11

Type: path_reg
Bool: Equals
URLText: /api/v[0-9]*/studymanagement
Action: Use Backend
Location/Value: WFC_studymanagement_443

▪ Rule 12

Type: path_beg
Bool: Equals
URLText: /XERService
Action: Use Backend
Location/Value: WFC_xe_443

▪ Rule 13

 **Note** This rule is only applicable for SP2.

Type: path_reg
Bool: Equals
URLText: /api/v[0-9]*/recordmanager
Action: Use Backend
Location/Value: WFC_recordmanager_443

12. Leave all other settings at their default value.

13. Click **Update**.

9.8.3.2. Define the Associated Real Servers (RIPs)

This VIP has no associated Real Servers. Instead, the ACLs defined above are used to route traffic to the appropriate Backend Only Virtual Service.

9.8.4. VIP 2-B1 - WFC_inference_443

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. Enter the following details:



Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_inference_443"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

- Select (Check) **Create Backend Only**.
- Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_inference_443**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.

4. Click **Update** to create the Virtual Service.

5. Now click **Modify** next to the newly created VIP.

6. Scroll to the *Connection Distribution Method* section.

- Set *Balance Mode* to **Weighted Round Robin**.

7. Scroll to the *Persistence* section.

- Ensure that the *Persistence Mode* is set to **None**.

8. Scroll to the *Health Checks* section.

- Set the *Check Type* to **Negotiate HTTPS (GET)**.
- Set the *Request to Send* according to the Service Pack installed:
 - For SP1, set *Request to Send* to **/api/v1/inference/health**.
 - For SP2, set *Request to Send* to **/api/v1/inference/health/tenant/<tenantid>**.



Note

tenantid is a site specific setting, please check with the GE Healthcare engineers for this setting at the appropriate site.

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

9. Scroll to the *SSL* section.

- Ensure that *Enable Backend Encryption* is enabled (checked).

10. Leave all other settings at their default value.

11. 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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="443"/>	?
Re-Encrypt to Backend	<input checked="" type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
- Set the *Real Server Port* field to **443**.
- Ensure that *Re-Encrypt to Backend* is enabled (checked).

3. Leave all other settings at their default value.

4. Click **Update**.

5. Now click **Modify** next to the newly created Real Server.

6. Set the *Send Client Certificate* dropdown to the required certificate, e.g. **client-cert**.

7. Click **Update**.

8. Repeat these steps to add additional Real Server(s).

9.8.5. VIP 2-B2 - WFC_profiling_443

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. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_profiling_443"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

- Select (Check) **Create Backend Only**.
- Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_profiling_443**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.

4. Click **Update** to create the Virtual Service.

5. Now click **Modify** next to the newly created VIP.

6. Scroll to the *Connection Distribution Method* section.

- Set *Balance Mode* to **Weighted Round Robin**.

7. Scroll to the *Persistence* section.

- Ensure that the *Persistence Mode* is set to **None**.

8. Scroll to the *Health Checks* section.

- Set the *Check Type* to **Negotiate HTTPS (GET)**.
- Set the *Request to Send* according to the Service Pack installed:
 - For SP1, set *Request to Send* to **/api/v1/profiling/health**.
 - For SP2, set *Request to Send* to **/api/v1/profiling/health/tenant/<tenantid>**.



Note

tenantid is a site specific setting, please check with the GE Healthcare engineers for this setting at the appropriate site.

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

9. Scroll to the *SSL* section.

- Ensure that *Enable Backend Encryption* is enabled (checked).

10. Leave all other settings at their default value.

11. 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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="443"/>	?
Re-Encrypt to Backend	<input checked="" type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
- Set the *Real Server Port* field to **443**.
- Ensure that *Re-Encrypt to Backend* is enabled (checked).

3. Leave all other settings at their default value.

4. Click **Update**.

5. Now click **Modify** next to the newly created Real Server.

6. Set the *Send Client Certificate* dropdown to the required certificate, e.g. **client-cert**.

7. Click **Update**.

8. Repeat these steps to add additional Real Server(s).

9.8.6. VIP 2-B3 - WFC_patient_443

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. Click **[Advanced]**.

3. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_patient_443"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

- Select (Check) **Create Backend Only**.
- Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_patient_443**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.

4. Click **Update** to create the Virtual Service.

5. Now click **Modify** next to the newly created VIP.

6. Scroll to the *Connection Distribution Method* section.

- Set *Balance Mode* to **Weighted Round Robin**.

7. Scroll to the *Persistence* section.

- Ensure that the *Persistence Mode* is set to **None**.

8. Scroll to the *Health Checks* section.

- Set the *Check Type* to **Negotiate HTTPS (GET)**.
- Set the *Request to Send* according to the Service Pack installed:
 - For SP1, set *Request to Send* to **/api/v1/patient/health**.
 - For SP2, set *Request to Send* to **/api/v1/patient/health/tenant/<tenantid>**.



Note

tenantid is a site specific setting, please check with the GE Healthcare engineers for this setting at the appropriate site.

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

9. Scroll to the *SSL* section.

- Ensure that *Enable Backend Encryption* is enabled (checked).

10. Leave all other settings at their default value.

11. 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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="443"/>	?
Re-Encrypt to Backend	<input checked="" type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
- Set the *Real Server Port* field to **443**.
- Ensure that *Re-Encrypt to Backend* is enabled (checked).

3. Leave all other settings at their default value.

4. Click **Update**.

5. Now click **Modify** next to the newly created Real Server.

6. Set the *Send Client Certificate* dropdown to the required certificate, e.g. **client-cert**.

7. Click **Update**.

8. Repeat these steps to add additional Real Server(s).

9.8.7. VIP 2-B4 - WFC_CCS_443

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. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_CCS_443"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

- Select (Check) **Create Backend Only**.
- Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_CCS_443**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.

4. Click **Update** to create the Virtual Service.

5. Now click **Modify** next to the newly created VIP.

6. Scroll to the *Connection Distribution Method* section.

- Set *Balance Mode* to **Weighted Round Robin**.

7. Scroll to the *Persistence* section.

- Ensure that the *Persistence Mode* is set to **None**.

8. Scroll to the *Health Checks* section.

- Set the *Check Type* to **Negotiate HTTPS (GET)**.
- Set the *Request to Send* according to the Service Pack installed:
 - For SP1, set *Request to Send* to **/api/v1/configstore/health**.
 - For SP2, set *Request to Send* to **/api/v1/configstore/health/admin/serviceconfig**.
- Set the *Response expected* drop-down to **Equals** and the value to **UP**.

9. Scroll to the *SSL* section.

- Ensure that *Enable Backend Encryption* is enabled (checked).

10. Leave all other settings at their default value.

11. 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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="443"/>	?
Re-Encrypt to Backend	<input checked="" type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
 - Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
 - Set the *Real Server Port* field to **443**.
 - Ensure that *Re-Encrypt to Backend* is enabled (checked).
3. Leave all other settings at their default value.
 4. Click **Update**.
 5. Now click **Modify** next to the newly created Real Server.
 6. Set the *Send Client Certificate* dropdown to the required certificate, e.g. **client-cert**.
 7. Click **Update**.
 8. Repeat these steps to add additional Real Server(s).

9.8.8. VIP 2-B5 - WFC_auth_443

9.8.8.1. 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. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_auth_443"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

- Select (Check) **Create Backend Only**.
 - Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_auth_443**.
 - Set the *Layer 7 Protocol* to **HTTP Mode**.
4. Click **Update** to create the Virtual Service.
 5. Now click **Modify** next to the newly created VIP.
 6. Scroll to the *Connection Distribution Method* section.
 - Set *Balance Mode* to **Weighted Round Robin**.
 7. Scroll to the *Persistence* section.
 - Ensure that the *Persistence Mode* is set to **None**.
 8. Scroll to the *Health Checks* section.
 - Set the *Check Type* to **Negotiate HTTPS (GET)**.
 - Set *Request to Send* to **/api/v1/auth/health**.
 - Set the *Response expected* drop-down to **Equals** and the value to **UP**.
 9. Scroll to the *SSL* section.
 - Ensure that *Enable Backend Encryption* is enabled (checked).
 10. Leave all other settings at their default value.
 11. Click **Update**.

9.8.8.2. 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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="443"/>	?
Re-Encrypt to Backend	<input checked="" type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.

- Set the *Real Server Port* field to **443**.
 - Ensure that *Re-Encrypt to Backend* is enabled (checked).
3. Leave all other settings at their default value.
 4. Click **Update**.
 5. Now click **Modify** next to the newly created Real Server.
 6. Set the *Send Client Certificate* dropdown to the required certificate, e.g. **client-cert**.
 7. Click **Update**.
 8. Repeat these steps to add additional Real Server(s).

9.8.9. VIP 2-B6 - WFC_outboundhl7_443

9.8.9.1. 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. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_outboundhl7_443"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

- Select (Check) **Create Backend Only**.
 - Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_outboundhl7_443**.
 - Set the *Layer 7 Protocol* to **HTTP Mode**.
4. Click **Update** to create the Virtual Service.
 5. Now click **Modify** next to the newly created VIP.
 6. Scroll to the *Connection Distribution Method* section.
 - Set *Balance Mode* to **Weighted Round Robin**.
 7. Scroll to the *Persistence* section.
 - Ensure that the *Persistence Mode* is set to **None**.
 8. Scroll to the *Health Checks* section.

- Set the *Check Type* to **Negotiate HTTPS (GET)**.
- Set the *Request to Send* according to the Service Pack installed:
 - For SP1, set *Request to Send* to **/api/v1/outboundhl7/health**.
 - For SP2, set *Request to Send* to **/api/v1/outboundhl7/health/tenant/<tenantid>**.







 **Note**

tenantid is a site specific setting, please check with the GE Healthcare engineers for this setting at the appropriate site.

- Set the *Response expected* drop-down to **Equals** and the value to **UP**.
9. Scroll to the **SSL** section.
 - Ensure that *Enable Backend Encryption* is enabled (checked).
 10. Leave all other settings at their default value.
 11. Click **Update**.

9.8.9.2. 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:

Label	<input type="text" value="WFC-1"/>	
Real Server IP Address	<input type="text" value="10.177.206.194"/>	
Real Server Port	<input type="text" value="443"/>	
Re-Encrypt to Backend	<input checked="" type="checkbox"/>	
Enable Redirect	<input type="checkbox"/>	
Weight	<input type="text" value="100"/>	

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
 - Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
 - Set the *Real Server Port* field to **443**.
 - Ensure that *Re-Encrypt to Backend* is enabled (checked).
3. Leave all other settings at their default value.
 4. Click **Update**.
 5. Now click **Modify** next to the newly created Real Server.

6. Set the *Send Client Certificate* dropdown to the required certificate, e.g. **client-cert**.
7. Click **Update**.
8. Repeat these steps to add additional Real Server(s).

9.8.10. VIP 2-B7 - WFC_inboundnotification_443

9.8.10.1. 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. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_inboundnotification_44"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

- Select (Check) **Create Backend Only**.
 - Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_inboundnotification_443**.
 - Set the *Layer 7 Protocol* to **HTTP Mode**.
4. Click **Update** to create the Virtual Service.
 5. Now click **Modify** next to the newly created VIP.
 6. Scroll to the *Connection Distribution Method* section.
 - Set *Balance Mode* to **Weighted Round Robin**.
 7. Scroll to the *Persistence* section.
 - Ensure that the *Persistence Mode* is set to **None**.
 8. Scroll to the *Health Checks* section.
 - Set the *Check Type* to **Negotiate HTTPS (GET)**.
 - Set the *Request to Send* according to the Service Pack installed:
 - For SP1, set *Request to Send* to **/api/v1/inboundnotification/health**.
 - For SP2, set *Request to Send* to **/api/v1/inboundnotification/health/tenant/<tenant id>**.



Note

tenant id is a site specific setting, please check with the GE Healthcare



engineers for this setting at the appropriate site.

- Set the *Response expected* drop-down to **Equals** and the value to **UP**.
9. Scroll to the **SSL** section.
 - Ensure that *Enable Backend Encryption* is enabled (checked).
 10. Leave all other settings at their default value.
 11. Click **Update**.

9.8.10.2. 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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="443"/>	?
Re-Encrypt to Backend	<input checked="" type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

Cancel **Update**

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
 - Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
 - Set the *Real Server Port* field to **443**.
 - Ensure that *Re-Encrypt to Backend* is enabled (checked).
3. Leave all other settings at their default value.
 4. Click **Update**.
 5. Now click **Modify** next to the newly created Real Server.
 6. Set the *Send Client Certificate* dropdown to the required certificate, e.g. **client-cert**.
 7. Click **Update**.
 8. Repeat these steps to add additional Real Server(s).

9.8.11. VIP 2-B8 - WFC_eventnotificationmanager_443

9.8.11.1. Virtual Service (VIP) Configuration



- Using the WebUI, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a new Virtual Service**.
- Click **[Advanced]**.
- Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_eventnotificationmana"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

- Select (Check) **Create Backend Only**.
 - Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_eventnotificationmanager_443**.
 - Set the *Layer 7 Protocol* to **HTTP Mode**.
- Click **Update** to create the Virtual Service.
 - Now click **Modify** next to the newly created VIP.
 - Scroll to the *Connection Distribution Method* section.
 - Set *Balance Mode* to **Weighted Round Robin**.
 - Scroll to the *Persistence* section.
 - Ensure that the *Persistence Mode* is set to **None**.
 - Scroll to the *Health Checks* section.
 - Set the *Check Type* to **Negotiate HTTPS (GET)**.
 - Set the *Request to Send* to **/api/v1/eventnotificationmanager/health**.
 - Set the *Response expected* drop-down to **Equals** and the value to **UP**.
 - Scroll to the *SSL* section.
 - Ensure that *Enable Backend Encryption* is enabled (checked).
 - Leave all other settings at their default value.
 - Click **Update**.

9.8.11.2. Define the Associated Real Servers (RIPs)

- 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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="443"/>	?
Re-Encrypt to Backend	<input checked="" type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
- Set the *Real Server Port* field to **443**.
- Ensure that *Re-Encrypt to Backend* is enabled (checked).

3. Leave all other settings at their default value.

4. Click **Update**.

5. Now click **Modify** next to the newly created Real Server.

6. Set the *Send Client Certificate* dropdown to the required certificate, e.g. **client-cert**.

7. Click **Update**.

8. Repeat these steps to add additional Real Server(s).

9.8.12. VIP 2-B9 - WFC_outbouncventpolling_443

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. Click **[Advanced]**.
3. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_outbouneventpolling_"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

- Select (Check) **Create Backend Only**.
- Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_outbouneventpolling_443**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.

4. Click **Update** to create the Virtual Service.

5. Now click **Modify** next to the newly created VIP.

6. Scroll to the *Connection Distribution Method* section.

- Set *Balance Mode* to **Weighted Round Robin**.

7. Scroll to the *Persistence* section.

- Ensure that the *Persistence Mode* is set to **None**.

8. Scroll to the *Health Checks* section.

- Set the *Check Type* to **Negotiate HTTPS (GET)**.
- Set the *Request to Send* according to the Service Pack installed:
 - For SP1, set *Request to Send* to **/api/v1/outbouneventpolling/health**.
 - For SP2, set *Request to Send* to **/api/v1/outbouneventpolling/health/tenant/<tenant id>**.



Note

tenant id is a site specific setting, please check with the GE Healthcare engineers for this setting at the appropriate site.

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

9. Scroll to the *SSL* section.

- Ensure that *Enable Backend Encryption* is enabled (checked).

10. Leave all other settings at their default value.

11. 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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="443"/>	?
Re-Encrypt to Backend	<input checked="" type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
- Set the *Real Server Port* field to **443**.
- Ensure that *Re-Encrypt to Backend* is enabled (checked).

3. Leave all other settings at their default value.

4. Click **Update**.

5. Now click **Modify** next to the newly created Real Server.

6. Set the *Send Client Certificate* dropdown to the required certificate, e.g. **client-cert**.

7. Click **Update**.

8. Repeat these steps to add additional Real Server(s).

9.8.13. VIP 2-B10 - WFC_metadata_443

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. Click **[Advanced]**.

3. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_metadata_443"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

- Select (Check) **Create Backend Only**.
- Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_metadata_443**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.

4. Click **Update** to create the Virtual Service.

5. Now click **Modify** next to the newly created VIP.

6. Scroll to the *Connection Distribution Method* section.

- Set *Balance Mode* to **Weighted Round Robin**.

7. Scroll to the *Persistence* section.

- Ensure that the *Persistence Mode* is set to **None**.

8. Scroll to the *Health Checks* section.

- Set the *Check Type* to **Negotiate HTTPS (GET)**.
- Set the *Request to Send* according to the Service Pack installed:
 - For SP1, set *Request to Send* to **/api/v1/metadata/health**.
 - For SP2, set *Request to Send* to **/api/v1/metadata/health/tenant/<tenant id>**.



Note

tenant id is a site specific setting, please check with the GE Healthcare engineers for this setting at the appropriate site.

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

9. Scroll to the *SSL* section.

- Ensure that *Enable Backend Encryption* is enabled (checked).

10. Leave all other settings at their default value.

11. 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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="443"/>	?
Re-Encrypt to Backend	<input checked="" type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
- Set the *Real Server Port* field to **443**.
- Ensure that *Re-Encrypt to Backend* is enabled (checked).

3. Leave all other settings at their default value.

4. Click **Update**.

5. Now click **Modify** next to the newly created Real Server.

6. Set the *Send Client Certificate* dropdown to the required certificate, e.g. **client-cert**.

7. Click **Update**.

8. Repeat these steps to add additional Real Server(s).

9.8.14. VIP 2-B11 - WFC_studymanagement_443

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]**.

3. Enter the following details:



Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_studymanagement_44"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

- Select (Check) **Create Backend Only**.
- Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_studymanagement_443**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.

4. Click **Update** to create the Virtual Service.

5. Now click **Modify** next to the newly created VIP.

6. Scroll to the *Connection Distribution Method* section.

- Set *Balance Mode* to **Weighted Round Robin**.

7. Scroll to the *Persistence* section.

- Ensure that the *Persistence Mode* is set to **None**.

8. Scroll to the *Health Checks* section.

- Set the *Check Type* to **Negotiate HTTPS (GET)**.
- Set the *Request to Send* according to the Service Pack installed:
 - For SP1, set *Request to Send* to **/api/v1/studymanagement/health**.
 - For SP2, set *Request to Send* to **/api/v1/studymanagement/health/tenant/<tenant id>**.



Note

tenant id is a site specific setting, please check with the GE Healthcare engineers for this setting at the appropriate site.

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

9. Scroll to the *SSL* section.

- Ensure that *Enable Backend Encryption* is enabled (checked).

10. Leave all other settings at their default value.

11. 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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="443"/>	?
Re-Encrypt to Backend	<input checked="" type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
- Set the *Real Server Port* field to **443**.
- Ensure that *Re-Encrypt to Backend* is enabled (checked).

3. Leave all other settings at their default value.

4. Click **Update**.

5. Now click **Modify** next to the newly created Real Server.

6. Set the *Send Client Certificate* dropdown to the required certificate, e.g. **client-cert**.

7. Click **Update**.

8. Repeat these steps to add additional Real Server(s).

9.8.15. VIP 2-B12 - WFC_xe_443

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]**.
3. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_xe_443"/>	?
Protocol		[Advanced +]
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

- Select (Check) **Create Backend Only**.
- Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_xe_443**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.

4. Click **Update** to create the Virtual Service.

5. Now click **Modify** next to the newly created VIP.

6. Scroll to the *Connection Distribution Method* section.

- Set *Balance Mode* to **Weighted Round Robin**.

7. Scroll to the *Persistence* section.

- Ensure that the *Persistence Mode* is set to **None**.

8. Scroll to the *Health Checks* section.

- Set the *Check Type* to **Negotiate HTTPS (GET)**.
- Set the *Request to Send* to **/XERService/health**.
- Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.

9. Scroll to the *SSL* section.

- Ensure that *Enable Backend Encryption* is enabled (checked).

10. Leave all other settings at their default value.

11. 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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="443"/>	?
Re-Encrypt to Backend	<input checked="" type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
 - Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
 - Set the *Real Server Port* field to **443**.
 - Ensure that *Re-Encrypt to Backend* is enabled (checked).
3. Leave all other settings at their default value.
 4. Click **Update**.
 5. Now click **Modify** next to the newly created Real Server.
 6. Set the *Send Client Certificate* dropdown to the required certificate, e.g. **client-cert**.
 7. Click **Update**.
 8. Repeat these steps to add additional Real Server(s).

9.8.16. VIP 2-B13 - WFC_recordmanager_443

 **Note** This VIP is only required for SP2.

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. Click **[Advanced]**.
3. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_recordmanager_443"/>	?
Protocol		[Advanced +]
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

- Select (Check) **Create Backend Only**.
- Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_recordmanager_443**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.

4. Click **Update** to create the Virtual Service.

5. Now click **Modify** next to the newly created VIP.

6. Scroll to the *Connection Distribution Method* section.


- Set *Balance Mode* to **Weighted Round Robin**.

7. Scroll to the *Persistence* section.

- Ensure that the *Persistence Mode* is set to **None**.

8. Scroll to the *Health Checks* section.

- Set the *Check Type* to **Negotiate HTTPS (GET)**.
- Set the *Request to Send* to **/api/v1/recordmanager/health/tenant/<tenantid>**.

 **Note** **tenantid** is a site specific setting, please check with the GE Healthcare engineers for this setting at the appropriate site.

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

9. Scroll to the *SSL* section.

- Ensure that *Enable Backend Encryption* is enabled (checked).

10. Leave all other settings at their default value.

11. 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:



Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="443"/>	?
Re-Encrypt to Backend	<input checked="" type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
- Set the *Real Server Port* field to **443**.
- Ensure that *Re-Encrypt to Backend* is enabled (checked).

3. Leave all other settings at their default value.

4. Click **Update**.

5. Now click **Modify** next to the newly created Real Server.

6. Set the *Send Client Certificate* dropdown to the required certificate, e.g. **client-cert**.

7. Click **Update**.

8. Repeat these steps to add additional Real Server(s).

9.8.17. VIP 3 - WFC_http

 **Note** This VIP is only required for SP1.

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:

Virtual Service		[Advanced +]
Label	<input type="text" value="WFC_http"/>	?
IP Address	<input type="text" value="10.177.215.149"/>	?
Ports	<input type="text" value="80"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

- Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_http**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.177.215.149**.
- Set the *Ports* field to **80**.
- Set the *Layer 7 Protocol* to **HTTP 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 *Balance Mode* to **Weighted Round Robin**.

6. Scroll to the *Persistence* section.

- Ensure that the *Persistence Mode* is set to **None**.

7. Scroll to the *Health Checks* section.

- Set the *Check Type* to **No checks, Always On**.

8. Scroll to the *ACL Rules* section.

9. Using the **Add Rule** button, add the following ACL rules:

- **Rule 1**

```

Type:          path_reg
Bool:          Equals
URL/Text:      /api/v1/configstore
Action:        Use Backend
Location/Value: WFC_CCS_80

```

- **Rule 2**

```

Type:          path_reg
Bool:          Equals
URL/Text:      /api/v1/inference
Action:        Use Backend

```



Location/Value: WFC_inference_80

▪ Rule 3

Type: path_reg
Bool: Equals
URLText: /api/v1/profiling
Action: Use Backend
Location/Value: WFC_profiling_80

▪ Rule 4

Type: path_reg
Bool: Equals
URLText: /api/v1/inboundnotification
Action: Use Backend
Location/Value: WFC_inboundnotification_80

▪ Rule 5

Type: path_reg
Bool: Equals
URLText: /api/v1/outboundeventpolling
Action: Use Backend
Location/Value: WFC_outboundeventpolling_80

▪ Rule 6

Type: path_reg
Bool: Equals
URLText: /api/v1/outboundh17
Action: Use Backend
Location/Value: WFC_outboundh17_443

▪ Rule 7

Type: path_reg
Bool: Equals
URLText: /api/v1/patient
Action: Use Backend
Location/Value: WFC_patient_80

▪ Rule 8

Type: path_reg
Bool: Equals
URLText: /api/v1/auth
Action: Use Backend



Location/Value: WFC_auth_80

▪ Rule 9

Type: path_reg
Bool: Equals
URLText: /api/v1/eventnotificationmanager
Action: Use Backend
Location/Value: WFC_eventnotificationmanager_80

▪ Rule 10

Type: path_reg
Bool: Equals
URLText: /api/v1/metadata
Action: Use Backend
Location/Value: WFC_metadata_80

▪ Rule 11

Type: path_reg
Bool: Equals
URLText: /api/v1/studymanagement
Action: Use Backend
Location/Value: WFC_studymanagement_80

▪ Rule 12

Type: path_reg
Bool: Equals
URLText: /api/v1/masterfiledata
Action: Use Backend
Location/Value: WFC_masterfiledata_80

▪ Rule 13

Type: path_reg
Bool: Equals
URLText: /api/v1/masterfileapp
Action: Use Backend
Location/Value: WFC_masterfileapp_80

▪ Rule 14

Type: path_beg
Bool: Equals
URLText: /XERService
Action: Use Backend



Location/Value: WFC_xe_80

10. Leave all other settings at their default value.
11. Click **Update**.

9.8.17.2. Define the Associated Real Servers (RIPs)





This VIP has no associated Real Servers. Instead, the ACLs defined above are used to route traffic to the appropriate Backend Only Virtual Service.

9.8.18. VIP 3-B1 - WFC_inference_80

 **Note** This VIP is only required for SP1.

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. Click **[Advanced]**.
3. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	
Create Backend Only	<input checked="" type="checkbox"/>	
Label	<input type="text" value="WFC_inference_80"/>	
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	

Cancel **Update**

- Select (Check) **Create Backend Only**.
 - Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_inference_80**.
 - Set the *Layer 7 Protocol* to **HTTP Mode**.
4. Click **Update** to create the Virtual Service.
 5. Now click **Modify** next to the newly created VIP.
 6. Scroll to the *Connection Distribution Method* section.
 - Set *Balance Mode* to **Weighted Round Robin**.
 7. Scroll to the *Persistence* section.
 - Ensure that the *Persistence Mode* is set to **None**.
 8. Scroll to the *Health Checks* section.



- Set the *Check Type* to **Negotiate HTTPS (GET)**.
- Set the *Request to Send* to **/api/v1/inference/health**.
- Set the *Response expected* drop-down to **Equals** and the value to **UP**.

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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="80"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?


- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
- Set the *Real Server Port* field to **80**.

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 3-B2 - WFC_profiling_80

 **Note** This VIP is only required for SP1.

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. Click **[Advanced]**.
3. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_profiling_80"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

- Select (Check) **Create Backend Only**.
- Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_profiling_80**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.

4. Click **Update** to create the Virtual Service.

5. Now click **Modify** next to the newly created VIP.

6. Scroll to the *Connection Distribution Method* section.

- Set *Balance Mode* to **Weighted Round Robin**.

7. Scroll to the *Persistence* section.

- Ensure that the *Persistence Mode* is set to **None**.

8. Scroll to the *Health Checks* section.

- Set the *Check Type* to **Negotiate HTTP (GET)**.
- Set the *Request to Send* to **/api/v1/profiling/health**.
- Set the *Response expected* drop-down to **Equals** and the value to **UP**.

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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="80"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

Cancel
Update

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
 - Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
 - Set the *Real Server Port* field to **80**.
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 3-B3 - WFC_CCS_80

 **Note** This VIP is only required for SP1.

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. Click **[Advanced]**.
3. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_CCS_80"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

Cancel
Update

- Select (Check) **Create Backend Only**.



- Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_CCS_80**.
 - Set the *Layer 7 Protocol* to **HTTP Mode**.
4. Click **Update** to create the Virtual Service.
 5. Now click **Modify** next to the newly created VIP.
 6. Scroll to the *Connection Distribution Method* section.
 - Set *Balance Mode* to **Weighted Round Robin**.
 7. Scroll to the *Persistence* section.
 - Ensure that the *Persistence Mode* is set to **None**.
 8. Scroll to the *Health Checks* section.
 - Set the *Check Type* to **Negotiate HTTPS (GET)**.
 - Set the *Request to Send* to **/api/v1/configstore/health**.
 - Set the *Response expected* drop-down to **Equals** and the value to **UP**.
 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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="80"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
 - Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
 - Set the *Real Server Port* field to **80**.
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 3-B4 - WFC_auth_80

Note

This VIP is only required for SP1.

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. Click **[Advanced]**.
3. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_auth_80"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

Cancel **Update**

- Select (Check) **Create Backend Only**.
 - Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_auth_80**.
 - Set the *Layer 7 Protocol* to **HTTP Mode**.
4. Click **Update** to create the Virtual Service.
 5. Now click **Modify** next to the newly created VIP.
 6. Scroll to the *Connection Distribution Method* section.
 - Set *Balance Mode* to **Weighted Round Robin**.
 7. Scroll to the *Persistence* section.
 - Ensure that the *Persistence Mode* is set to **None**.
 8. Scroll to the *Health Checks* section.
 - Set the *Check Type* to **Negotiate HTTP (GET)**.
 - Set the *Request to Send* to **/api/v1/auth/health**.
 - Set the *Response expected* drop-down to **Equals** and the value to **UP**.
 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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="80"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
 - Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
 - Set the *Real Server Port* field to **80**.
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. VIP 3-B5 - WFC_outboundeventpolling_80

 **Note** This VIP is only required for SP1.

9.8.22.1. 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. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_outboundeventpolling_"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

- Select (Check) **Create Backend Only**.
- Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_outboundeventpolling_80**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.

4. Click **Update** to create the Virtual Service.

5. Now click **Modify** next to the newly created VIP.

6. Scroll to the *Connection Distribution Method* section.

- Set *Balance Mode* to **Weighted Round Robin**.

7. Scroll to the *Persistence* section.

- Ensure that the *Persistence Mode* is set to **None**.

8. Scroll to the *Health Checks* section.

- Set the *Check Type* to **Negotiate HTTPS (GET)**.
- Set the *Request to Send* to **/api/v1/outboundeventpolling/health**.
- Set the *Response expected* drop-down to **Equals** and the value to **UP**.

9. Leave all other settings at their default value.

10. Click **Update**.

9.8.22.2. 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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="80"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
- Set the *Real Server Port* field to **80**.

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

9.8.23. VIP 3-B6 - WFC_inboundnotification_80

 **Note** This VIP is only required for SP1.

9.8.23.1. 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. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_inboundnotification_80"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

- Select (Check) **Create Backend Only**.



- Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_inboundnotification_80**.
 - Set the *Layer 7 Protocol* to **HTTP Mode**.
4. Click **Update** to create the Virtual Service.
 5. Now click **Modify** next to the newly created VIP.
 6. Scroll to the *Connection Distribution Method* section.
 - Set *Balance Mode* to **Weighted Round Robin**.
 7. Scroll to the *Persistence* section.
 - Ensure that the *Persistence Mode* is set to **None**.
 8. Scroll to the *Health Checks* section.
 - Set the *Check Type* to **Negotiate HTTPS (GET)**.
 - Set the *Request to Send* to **/api/v1/inboundnotification/health**.
 - Set the *Response expected* drop-down to **Equals** and the value to **UP**.
 9. Leave all other settings at their default value.
 10. Click **Update**.

9.8.23.2. 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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="80"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
 - Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
 - Set the *Real Server Port* field to **80**.
3. Leave all other settings at their default value.
 4. Click **Update**.

5. Repeat these steps to add additional Real Server(s).

9.8.24. VIP 3-B7 - WFC_eventnotificationmanager_80

Note

This VIP is only required for SP1.

9.8.24.1. 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. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_eventnotificationmana"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

Cancel **Update**

- Select (Check) **Create Backend Only**.
 - Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_eventnotificationmanager_80**.
 - Set the *Layer 7 Protocol* to **HTTP Mode**.
4. Click **Update** to create the Virtual Service.
 5. Now click **Modify** next to the newly created VIP.
 6. Scroll to the *Connection Distribution Method* section.
 - Set *Balance Mode* to **Weighted Round Robin**.
 7. Scroll to the *Persistence* section.
 - Ensure that the *Persistence Mode* is set to **None**.
 8. Scroll to the *Health Checks* section.
 - Set the *Check Type* to **Negotiate HTTPS (GET)**.
 - Set the *Request to Send* to **/api/v1/eventnotificationmanager/health**.
 - Set the *Response expected* drop-down to **Equals** and the value to **UP**.
 9. Leave all other settings at their default value.
 10. Click **Update**.



9.8.24.2. 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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="80"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

Cancel **Update**

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
 - Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
 - Set the *Real Server Port* field to **80**.
3. Leave all other settings at their default value.
 4. Click **Update**.
 5. Repeat these steps to add additional Real Server(s).

9.8.25. VIP 3-B8 - WFC_metadata_80

 **Note** This VIP is only required for SP1.

9.8.25.1. 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. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_metadata_80"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

- Select (Check) **Create Backend Only**.
- Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_metadata_80**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.

4. Click **Update** to create the Virtual Service.

5. Now click **Modify** next to the newly created VIP.

6. Scroll to the *Connection Distribution Method* section.

- Set *Balance Mode* to **Weighted Round Robin**.

7. Scroll to the *Persistence* section.

- Ensure that the *Persistence Mode* is set to **None**.

8. Scroll to the *Health Checks* section.

- Set the *Check Type* to **Negotiate HTTP (GET)**.
- Set the *Request to Send* to **/api/v1/metadata/health**.
- Set the *Response expected* drop-down to **Equals** and the value to **UP**.

9. Leave all other settings at their default value.

10. Click **Update**.

9.8.25.2. 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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="80"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
- Set the *Real Server Port* field to **80**.

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

9.8.26. VIP 3-B9 - WFC_patient_80

 **Note** This VIP is only required for SP1.

9.8.26.1. 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. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_patient_80"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

- Select (Check) **Create Backend Only**.



- Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_patient_80**.
 - Set the *Layer 7 Protocol* to **HTTP Mode**.
4. Click **Update** to create the Virtual Service.
 5. Now click **Modify** next to the newly created VIP.
 6. Scroll to the *Connection Distribution Method* section.
 - Set *Balance Mode* to **Weighted Round Robin**.
 7. Scroll to the *Persistence* section.
 - Ensure that the *Persistence Mode* is set to **None**.
 8. Scroll to the *Health Checks* section.
 - Set the *Check Type* to **Negotiate HTTPS (GET)**.
 - Set the *Request to Send* to **/api/v1/patient/health**.
 - Set the *Response expected* drop-down to **Equals** and the value to **UP**.
 9. Leave all other settings at their default value.
 10. Click **Update**.

9.8.26.2. 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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="80"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
 - Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
 - Set the *Real Server Port* field to **80**.
3. Leave all other settings at their default value.
 4. Click **Update**.

5. Repeat these steps to add additional Real Server(s).

9.8.27. VIP 3-B10 - WFC_masterfileapp_80

Note

This VIP is only required for SP1.

9.8.27.1. 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. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_masterfileapp_80"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

Cancel **Update**

- Select (Check) **Create Backend Only**.
 - Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_masterfileapp_80**.
 - Set the *Layer 7 Protocol* to **HTTP Mode**.
4. Click **Update** to create the Virtual Service.
 5. Now click **Modify** next to the newly created VIP.
 6. Scroll to the *Connection Distribution Method* section.
 - Set *Balance Mode* to **Weighted Round Robin**.
 7. Scroll to the *Persistence* section.
 - Ensure that the *Persistence Mode* is set to **None**.
 8. Scroll to the *Health Checks* section.
 - Set the *Check Type* to **Negotiate HTTPS (GET)**.
 - Set the *Request to Send* to **/api/v1/masterfileapp/health**.
 - Set the *Response expected* drop-down to **Equals** and the value to **UP**.
 9. Leave all other settings at their default value.
 10. Click **Update**.



9.8.27.2. 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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="80"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

Cancel **Update**

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
 - Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
 - Set the *Real Server Port* field to **80**.
3. Leave all other settings at their default value.
 4. Click **Update**.
 5. Repeat these steps to add additional Real Server(s).

9.8.28. VIP 3-B11 - WFC_masterfiledata_80

 **Note** This VIP is only required for SP1.

9.8.28.1. 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. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_masterfiledata_80"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

- Select (Check) **Create Backend Only**.
- Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_masterfiledata_80**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.

4. Click **Update** to create the Virtual Service.

5. Now click **Modify** next to the newly created VIP.

6. Scroll to the *Connection Distribution Method* section.

- Set *Balance Mode* to **Weighted Round Robin**.

7. Scroll to the *Persistence* section.

- Ensure that the *Persistence Mode* is set to **None**.

8. Scroll to the *Health Checks* section.

- Set the *Check Type* to **Negotiate HTTPS (GET)**.
- Set the *Request to Send* to **/api/v1/masterfiledata/health**.
- Set the *Response expected* drop-down to **Equals** and the value to **UP**.

9. Leave all other settings at their default value.

10. Click **Update**.

9.8.28.2. 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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="80"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
- Set the *Real Server Port* field to **80**.

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

9.8.29. VIP 3-B12 - WFC_studymanagement_80

Note This VIP is only required for SP1.

9.8.29.1. 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. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_studymanagement_80"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

- Select (Check) **Create Backend Only**.

- Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_studymanagement_80**.
 - Set the *Layer 7 Protocol* to **HTTP Mode**.
4. Click **Update** to create the Virtual Service.
 5. Now click **Modify** next to the newly created VIP.
 6. Scroll to the *Connection Distribution Method* section.
 - Set *Balance Mode* to **Weighted Round Robin**.
 7. Scroll to the *Persistence* section.
 - Ensure that the *Persistence Mode* is set to **None**.
 8. Scroll to the *Health Checks* section.
 - Set the *Check Type* to **Negotiate HTTPS (GET)**.
 - Set the *Request to Send* to **/api/v1/studymanagement/health**.
 - Set the *Response expected* drop-down to **Equals** and the value to **UP**.
 9. Leave all other settings at their default value.
 10. Click **Update**.

9.8.29.2. 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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="80"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
 - Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
 - Set the *Real Server Port* field to **80**.
3. Leave all other settings at their default value.
 4. Click **Update**.

5. Repeat these steps to add additional Real Server(s).

9.8.30. VIP 3-B13 - WFC_xe_80

Note

This VIP is only required for SP1.

9.8.30.1. 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. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_xe_80"/>	?
Protocol		[Advanced +]
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

Cancel **Update**

- Select (Check) **Create Backend Only**.
 - Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_xe_80**.
 - Set the *Layer 7 Protocol* to **HTTP Mode**.
4. Click **Update** to create the Virtual Service.
 5. Now click **Modify** next to the newly created VIP.
 6. Scroll to the *Connection Distribution Method* section.
 - Set *Balance Mode* to **Weighted Round Robin**.
 7. Scroll to the *Persistence* section.
 - Ensure that the *Persistence Mode* is set to **None**.
 8. Scroll to the *Health Checks* section.
 - Set the *Check Type* to **Negotiate HTTP (GET)**.
 - Set the *Request to Send* to **/XERService/health**.
 - Set the *Response expected* drop-down to **Equals** and the value to **allServicesOperative**.
 9. Leave all other settings at their default value.
 10. Click **Update**.



9.8.30.2. 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:

Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="80"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
 - Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
 - Set the *Real Server Port* field to **80**.
3. Leave all other settings at their default value.
 4. Click **Update**.
 5. Repeat these steps to add additional Real Server(s).

9.8.31. VIP 4 - WFC_10443

9.8.31.1. 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 to the *Termination* section.
 - Enable (check) the *Create HAProxy SSL Termination* checkbox.
4. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input type="checkbox"/>	?
Label	<input type="text" value="WFC_10443"/>	?
IP Address	<input type="text" value="10.177.215.149"/>	?
Ports	<input type="text" value="8082"/>	?
Protocol		[Advanced +]
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?
Termination		
Create HAProxy SSL Termination	<input checked="" type="checkbox"/>	?
Termination Port	<input type="text" value="10443"/>	?
SSL Certificate	<input type="text" value="server-cert"/>	?
CA Certificate	<input type="text" value="Do not validate clients"/>	?

- Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_10443**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.177.215.149**.
- Set the *Ports* field to **8082**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.
- Set the *Termination Port* to **10443**.
- 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 *Balance Mode* to **Weighted Round Robin**.

8. Scroll to the *Persistence* section.

- Ensure that the *Persistence Mode* is set to **None**.

9. Scroll to the *Health Checks* section.

- Set the *Check Type* to **No Checks, Always On**.

10. Scroll to the *ACL Rules* section.

11. Using the **Add Rule** button, add the following ACL rules:

- **Rule 1**



```
Type:          path_reg
Bool:          Equals
URL/Text:     /api/v[0-9]*/masterfiledata
Action:       Use Backend
Location/Value: WFC_masterfiledata_10443
```

▪ Rule 2

```
Type:          path_reg
Bool:          Equals
URL/Text:     /api/v[0-9]*/masterfileapp
Action:       Use Backend
Location/Value: WFC_masterfileapp_10443
```

▪ Rule 3

```
Type:          path_beg
Bool:          Equals
URL/Text:     /xeui
Action:       Use Backend
Location/Value: WFC_xeui_10443
```

12. Scroll to the *Other* section.

- Set *Force to HTTPS* to **Yes**.
- Set the *HTTPS Redirect Code* to **301 (Moved Permanently)**.
- Set the *HTTPS Redirect Port* to **10443**.

13. Leave all other settings at their default value.

14. Click **Update**.

9.8.31.2. Define the Associated Real Servers (RIPs)

This VIP has no associated Real Servers. Instead, the ACLs defined above are used to route traffic to the appropriate Backend Only Virtual Service.

9.8.32. VIP 4-B1 - WFC_masterfiledata_10443

9.8.32.1. 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. Enter the following details:



Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_masterfiledata_10443"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

- Select (Check) **Create Backend Only**.
- Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_masterfiledata_10443**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.

4. Click **Update** to create the Virtual Service.

5. Now click **Modify** next to the newly created VIP.

6. Scroll to the *Connection Distribution Method* section.

- Set *Balance Mode* to **Weighted Round Robin**.

7. Scroll to the *Persistence* section.

- Ensure that the *Persistence Mode* is set to **None**.

8. Scroll to the *Health Checks* section.

- Set the *Check Type* to **Negotiate HTTPS (GET)**.
- Set the *Request to Send* to **/api/v1/masterfiledata/health**.
- Set the *Response expected* drop-down to **Equals** and the value to **UP**.

9. Scroll to the *SSL* section.

- Ensure that *Enable Backend Encryption* is enabled (checked).

10. Scroll to the *Other* section.

- Set *Use RIP name as Host Header* to **Yes**.

11. Leave all other settings at their default value.







12. Click **Update**.

9.8.32.2. 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:



Label	<input type="text" value="WFC-1"/>	
Real Server IP Address	<input type="text" value="10.177.206.194"/>	
Real Server Port	<input type="text" value="10443"/>	
Re-Encrypt to Backend	<input checked="" type="checkbox"/>	
Enable Redirect	<input type="checkbox"/>	
Weight	<input type="text" value="100"/>	

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
- Set the *Real Server Port* field to **10443**.
- Enable (check) *Re-Encrypt to Backend*.

3. Leave all other settings at their default value.

4. Click **Update**.

5. Now click **Modify** next to the newly created Real Server.

6. Set the *Verify Server Certificate* dropdown to the required certificate, e.g. **mTLS**.

7. Set the *Send Client Certificate* dropdown to the required certificate, e.g. **client-cert**.

8. Click **Update**.

9. Repeat these steps to add additional Real Server(s).

9.8.33. VIP 4-B2 - WFC_masterfileapp_10443

9.8.33.1. 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. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_masterfileapp_10443"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

- Select (Check) **Create Backend Only**.
- Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_masterfileapp_10443**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.

4. Click **Update** to create the Virtual Service.

5. Now click **Modify** next to the newly created VIP.

6. Scroll to the *Connection Distribution Method* section.

- Set *Balance Mode* to **Weighted Round Robin**.

7. Scroll to the *Persistence* section.

- Ensure that the *Persistence Mode* is set to **None**.

8. Scroll to the *Health Checks* section.

- Set the *Check Type* to **Negotiate HTTPS (GET)**.
- Set the *Request to Send* to **/api/v1/masterfileapp/health**.
- Set the *Response expected* drop-down to **Equals** and the value to **UP**.

9. Scroll to the *SSL* section.

- Ensure that *Enable Backend Encryption* is enabled (checked).

10. Scroll to the *Other* section.

- Set *Use RIP name as Host Header* to **Yes**.







11. Leave all other settings at their default value.

12. Click **Update**.

9.8.33.2. 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:

Label	<input type="text" value="WFC-1"/>	
Real Server IP Address	<input type="text" value="10.177.206.194"/>	
Real Server Port	<input type="text" value="10443"/>	
Re-Encrypt to Backend	<input checked="" type="checkbox"/>	
Enable Redirect	<input type="checkbox"/>	
Weight	<input type="text" value="100"/>	

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
- Set the *Real Server Port* field to **10443**.
- Enable (check) *Re-Encrypt to Backend*.

3. Leave all other settings at their default value.

4. Click **Update**.

5. Now click **Modify** next to the newly created Real Server.

6. Set the *Verify Server Certificate* dropdown to the required certificate, e.g. **mTLS**.

7. Set the *Send Client Certificate* dropdown to the required certificate, e.g. **client-cert**.

8. Click **Update**.

9. Repeat these steps to add additional Real Server(s).

9.8.34. VIP 4-B3 - WFC_xeui_10443

9.8.34.1. 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. Enter the following details:

Virtual Service		[Advanced -]
Manual Configuration	<input type="checkbox"/>	?
Create Backend Only	<input checked="" type="checkbox"/>	?
Label	<input type="text" value="WFC_xeui_10443"/>	?
Protocol		[Advanced +]
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

- Select (Check) **Create Backend Only**.
- Specify an appropriate *Label* for the Virtual Service, e.g. **WFC_xeui_10443**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.

4. Click **Update** to create the Virtual Service.

5. Now click **Modify** next to the newly created VIP.

6. Scroll to the *Connection Distribution Method* section.

- Set *Balance Mode* to **Weighted Round Robin**.

7. Scroll to the *Persistence* section.

- Ensure that the *Persistence Mode* is set to **None**.

8. Scroll to the *Health Checks* section.

- Set the *Check Type* to **Negotiate HTTPS (GET)**.
- Set the *Request to Send* to **/xeui/api/admin/health**.
- Set the *Response expected* to **Equals** and the value to **allServicesOperative**.

9. Scroll to the *SSL* section.

- Ensure that *Enable Backend Encryption* is enabled (checked).

10. Scroll to the *Other* section.

- Set *Use RIP name as Host Header* to **Yes**.

11. Leave all other settings at their default value.

12. Click **Update**.

9.8.34.2. 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:



Label	<input type="text" value="WFC-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="10443"/>	?
Re-Encrypt to Backend	<input checked="" type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Specify an appropriate *Label* for the RIP, e.g. **WFC-1**.
- Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
- Set the *Real Server Port* field to **10443**.
- Enable (check) *Re-Encrypt to Backend*.

3. Leave all other settings at their default value.

4. Click **Update**.

5. Now click **Modify** next to the newly created Real Server.

6. Set the *Verify Server Certificate* dropdown to the required certificate, e.g. **mTLS**.

7. Set the *Send Client Certificate* dropdown to the required certificate, e.g. **client-cert**.

8. Click **Update**.

9. Repeat these steps to add additional Real Server(s).

9.8.35. VIP 5 - WFM_karaf_Group

9.8.35.1. 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:

Virtual Service		[Advanced +]
Label	<input type="text" value="WFM_karaf_Group"/>	?
IP Address	<input type="text" value="10.177.215.149"/>	?
Ports	<input type="text" value="9094"/>	?
Protocol		[Advanced +]
Layer 7 Protocol	<input type="text" value="TCP Mode"/>	?

- Specify an appropriate *Label* for the Virtual Service, e.g. **WFM_karaf_Group**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.177.215.149**.
- Set the *Ports* field to **9094**.
- 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 *Balance Mode* to **Weighted Round Robin**.

6. Scroll to the *Persistence* section.

- Ensure that the *Persistence Mode* is set to **Source IP**.

7. Scroll to the *Health Checks* section.

- Set the *Check Type* to **Negotiate HTTPS (GET)**.
- Set the *Request to Send* to **/status/check**.
- 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**.

9.8.35.2. 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:

Label	<input type="text" value="WFM-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="80"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Specify an appropriate *Label* for the RIP, e.g. **WFM-1**.
 - Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
 - Set the *Real Server Port* field to **80**.
3. Leave all other settings at their default value.
 4. Click **Update**.
 5. Repeat these steps to add additional Real Server(s).

9.8.36. VIP 6 - SR_https_vs

9.8.36.1. 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:

Virtual Service		[Advanced +]
Label	<input type="text" value="SR_https_vs"/>	?
IP Address	<input type="text" value="10.177.215.149"/>	?
Ports	<input type="text" value="3080"/>	?
Protocol		[Advanced +]
Layer 7 Protocol	<input type="text" value="TCP Mode"/>	?

- Specify an appropriate *Label* for the Virtual Service, e.g. **SR_https_vs**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.177.215.149**.
- Set the *Ports* field to **3080**.
- 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 *Balance Mode* to **Weighted Round Robin**.
6. Scroll to the *Persistence* section.
 - Ensure that the *Persistence Mode* is set to **None**.
7. Scroll to the *Health Checks* section.
 - Set the *Check Type* to **Negotiate HTTPS (GET)**.
 - Set the *Request to Send* to **/healthz/all**.
 - Set the *Response expected* drop-down to **Equals** and the value to **true**.
8. Leave all other settings at their default value.
9. Click **Update**.

9.8.36.2. 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:

Label	<input type="text" value="SR-1"/>	?
Real Server IP Address	<input type="text" value="10.177.206.194"/>	?
Real Server Port	<input type="text" value="3080"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Specify an appropriate *Label* for the RIP, e.g. **SR-1**.
 - Set the *Real Server IP Address* field to the required IP address, e.g. **10.177.206.194**.
 - Set the *Real Server Port* field to **3080**.
3. Leave all other settings at their default value.
 4. Click **Update**.
 5. Repeat these steps to add additional Real Server(s).

9.8.37. 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 accessed via the WebUI. It shows a graphical view of all VIPs & RIPs (i.e. the TP 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 TP servers are healthy (green) and available to accept connections:

	VIRTUAL SERVICE	IP	PORTS	CONNS	PROTOCOL	METHOD	MODE	
	WFC_RMQAMQP	10.177.214.109	8080	108	TCP	Layer 7	Proxy	
	WFC_443_MutualA..	10.177.214.109	8081	0	HTTP	Layer 7	Proxy	
	WFC_inference_44..	-	-	0	HTTP	Layer 7	Proxy	
	WFC_profiling_44..	-	-	0	HTTP	Layer 7	Proxy	
	WFC_inboundnotif..	-	-	0	HTTP	Layer 7	Proxy	
	WFC_outboundeven..	-	-	0	HTTP	Layer 7	Proxy	
	WFC_patient_443	-	-	0	HTTP	Layer 7	Proxy	
	WFC_CCS_443	-	-	0	HTTP	Layer 7	Proxy	
	WFC_auth_443	-	-	0	HTTP	Layer 7	Proxy	
	WFC_outboundhl7..	-	-	0	HTTP	Layer 7	Proxy	
	WFC_eventnotific..	-	-	0	HTTP	Layer 7	Proxy	
	WFC_metadata_443..	-	-	0	HTTP	Layer 7	Proxy	
	WFC_studymanagem..	-	-	0	HTTP	Layer 7	Proxy	
	WFC_recordmanage..	-	-	0	HTTP	Layer 7	Proxy	
	WFC_10443_No_Aut..	10.177.214.109	8082	0	HTTP	Layer 7	Proxy	
	WFC_masterfileda..	-	-	0	HTTP	Layer 7	Proxy	
	WFC_masterfileap..	-	-	0	HTTP	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:

		WFC_RMQAMQP	10.177.215.149	5672	0	TCP	Layer 7	Proxy	
		REAL SERVER	IP	PORTS	WEIGHT	CONNS			
		WFC-1	10.177.206.194	5672	100	0	Drain	Halt	
		WFC-2	10.12.28.114	5672	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 VIPs 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	Fallback Page	Fallback page configuration
Maintenance	Firewall Script	Firewall (iptables) configuration

WebUI Main Menu Option	Sub Menu Option	Description
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*.

Create a Clustered Pair

LOADBALANCER

Local IP address
192.168.110.40

IP address of new peer
192.168.110.41

Password for *loadbalancer* user on peer
●●●●●●●●

Add new node

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

Create a Clustered Pair

LOADBALANCER Primary
IP: 192.168.110.40

Attempting to pair..

LOADBALANCER Secondary
IP: 192.168.110.41

Local IP address
192.168.110.40

IP address of new peer
192.168.110.41

Password for *loadbalancer* user on peer
●●●●●●●●

configuring

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

High Availability Configuration - primary

The screenshot displays the 'High Availability Configuration - primary' interface. It features two Loadbalancer nodes: a Primary node with IP 192.168.110.40 and a Secondary node with IP 192.168.110.41. A red button labeled 'Break Clustered Pair' is visible on the right side of the interface.

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*.



Protocol Versions		
Enable SNMP v1 and v2	<input type="checkbox"/>	?
Enable SNMP v3	<input type="checkbox"/>	?
Details		
SNMP location	<input type="text" value="Unknown"/>	?
SNMP contact	<input type="text" value="IT Dept"/>	?
Authentication		
SNMP v1/v2 community string	<input type="text" value="public"/>	?
USM Username	<input type="text"/>	?
USM Authorization Algorithm	<input type="text" value="SHA"/>	?
USM Authorization Passphrase	<input type="text"/>	?
USM Privacy Algorithm	<input type="text" value="AES"/>	?
USM Privacy Passphrase	<input type="text"/>	?

Update

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](#).



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*.

Email Alert Source Address	<input type="text" value="lb1@loadbalancer.org"/>	
Email Alert Destination Address	<input type="text" value="alerts@loadbalancer.org"/>	
Auto-NAT	<input type="text" value="off"/>	
Multi-threaded	<input type="text" value="yes"/>	
<input type="button" value="Update"/>		

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



VIP level settings override the global settings.

Once configured, these settings apply to the individual VIP.

To configure VIP level email alerts:



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

Email Alert Destination Address ?

Cancel **Update**

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

e.g. alerts@loadbalancer.org

- 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:

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

eMail Alert From ?

eMail Alert To ?

eMail Server Address ?

eMail Server Port ?

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

e.g. lb1@loadbalancer.org

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

e.g. alerts@loadbalancer.org

- 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.

Email Alerts

Email Alert Destination Address

alerts@loadbalancer.org



Email Alert Source Address

lb1@loadbalancer.org



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](#).

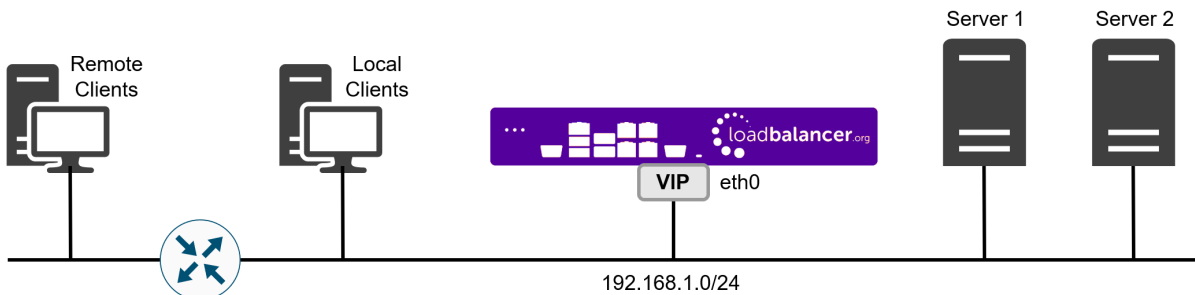


15. Appendix

15.1. Enabling Layer 7 Transparency

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

15.1.1. TProxy Topology Requirements - One-arm Deployments



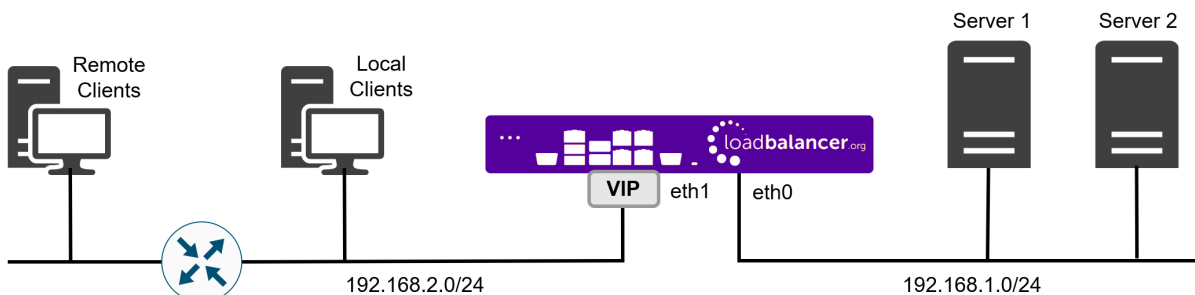
- Here, the VIP is brought up in the same subnet as the Real Servers.
- To support remote clients, the default gateway on the Real Servers must be an IP address on the load balancer and routing on the load balancer must be configured so that return traffic is routed back via the router.

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](#).

15.1.2. 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**.

15.1.3. Configuring a floating IP Address for the True PACS Servers' 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**.

New Floating IP

192.168.114.250

Add Floating IP

3. Click **Add Floating IP**.

 **Important**

The default gateway of each True PACS Server should be set to use this address.

16. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.0	18 July 2024	Initial version		RJC





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](https://twitter.com/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.

