FUJIFILM SYNAPSE

AN EDGENEXUS ADC DEPLOYMENT GUIDE

EDGE NEXUS

Contents

Document Properties

Document Number: 2.0.6.24.21.09.06

Document Creation Date: June 1, 2021

Document Last Edited: June 24, 2021

Document Author: Jay Savoor

Document Last Edited by:

Document Referral: Choose an item. - Version Click or tap here to enter text.

Document Disclaimer

Screenshots and graphics in this manual may differ slightly from your product due to differences in your product release version. Edgenexus ensures that they make every reasonable effort to ensure that the information in this document is complete and accurate. Edgenexus assumes no liability for any errors. Edgenexus makes changes and corrections to the information in this document in future releases when the need arises.

Copyrights

Trademarks

Edgenexus Support

If you have any technical questions regarding this product, please raise a support ticket at: support@edgenexus.io

Introduction

This application deployment guide is intended for persons administering the FujiFilm Synapse and its load balancing. This document contains specific general suggestions and guidance, which may or may not be relevant for use within your organization.

Synapse is a Fujifilm technology that is based on their PCAS, or Picture Archiving and Communication System. It allows diagnosis using high-quality image processing without the need for traditional film. The Synapse system consists of the following components:

- Windows IIS Server
- Database Server
- Storage Server
- DICOM (Digital Imaging and Communications in Medicine) Server
- Hospital Information System (HIS) Server

The EdgeADC is deployed as a pair of appliances and can be in a virtualized or physical environment. They operate in a high-availability (HA) environment and provide you the level of redundancy and resilience required for mission-critical systems.

The EdgeADC is fully capable of load-balancing your FujiFilm Synapse, and this guide explains how to set this up.

Application versions supported

This document supports the following FujiFilm Synapse versions:

- All

Acronyms used

VIP – Virtual IP

VS – Virtual Service

RS – Real Server

VIPs, Ports, and Other Bits

When load balancing FujiFilm Synapse, the following VIPs will be needed for operations.

Fuji Film Module	Explanation	Port	Protocol	ADC Service Type
Fuji Film Synapse PACS Web UI	Synapse PACS is a 100% web-based, intuitive and scalable solution to meet your exact needs anywhere and at any time, with on-demand access providing images in less than 2 seconds	80 443	TCP TCP	Layer 4 TCP Layer 4 TCP
Fuji Film Synapse VNA DICOM	Synapse VNA is the true-VNA application for the content management of images and medical information at the enterprise level; it is an open storage solution, secure, scalable, standard-based, and focused on medical data, DICOM, and native non-DICOM objects coming from any medical department system.	80 104	TCP TCP	Layer 4 TCP DICOM
Fuji Film Synapse Mobility	Synapse Mobility is a zero-footprint Universal Viewer that supports Synapse VNA with a full suite of collaboration tools and embedded cloud-based image sharing that allows clinicians to access patient information anytime and anywhere, from various platforms or using a mobile device.	8080 8443	TCP TCP	HTTP HTTP
Fuji Film Synapse CWM REST	Synapse Clinical Workflow Manager (CWM) is the FUJIFILM solution that allows any Medical Institution to manage all the workflow related to their Imaging Department.	80	TCP	HTTP

Sizing the EdgeADC

The ADC can operate in either physical or virtual deployments. The reverse proxy engine within the ADC is optimized for speed and efficiency. The ADC will use all available threads automatically.

In virtualized environments, we recommend that you set the ADC to 4 vCPU with 8GB RAM, to begin with, and scale up when you need to.

We recommend that you utilize the hardware platforms from our partners in physical environments, with the base system being a quad-core Intel Xeon with 8GB RAM.

In both cases, 50GB of disk storage space should be sufficient.

Deployment Scenarios

Connections to the FujiFilm Synapse system occur by clients connecting to the VIP or Virtual IP service created on the ADC. The ADC then load-balances the connections to the nodes configured within the ADC and linked to the VIP.

Virtual Service Methods

The configuration of Fujifilm Synapse within the ADC uses the following load balancing methods.

SSL Passthrough
In this mode, the traffic enters the ADC on port 443 using SSL. The traffic is sent onto the nodes without inspection. ADC service type Layer 4 TCP is used.

SSL Bridging
In this mode, the SSL traffic is terminated in the ADC and then re-encrypted before passing to the nodes. When this mode is chosen, you will need to have the SSL certificate installed on the nodes and install it in the ADC. This mode is the recommended best practice method for security reasons. ADC service type HTTP is used.

The following pages will take you through the VIP configuration. Please take care to configure correctly to avoid issues in operations.

The configuration stages that need to be followed are:

1. Creating the flightPATH rule for Synapse Mobility
2. Creating the VIP and VS set for Synapse VNA
3. Creating the VIP and VS for Synapse Mobility

These stages are explained in the sections that follow.

Collaboration flightPATH for Synapse Mobility

Users connecting to the Mobility service and collaborating the images with others will use a URL.

This URL will contain the '/h/' parameter that conforms to the Real Server ID. When the ADC sees this, it knows that the user should be connected to the Real Server with that ID definition.

The flightPATH rule ensures that once connected to the ADC, the '/h/' portion of the URL is removed, the user is then connected to the appropriate Real Server with the PATH being replaced by the '$remainder$' portion of the original URL.

We recommend that you look through the section on flightPATH in the ADC administration guide. There you will find the description on how to create flightPATH rules and the use of flightPATH variables.

- Navigate to Library in the left navigation pane
- Click on flightPATH and click on the option
- This action will open the flightPATH section on the right
- There are four sections to the flightPATH configurator: Details, Condition, Evaluation, and Action.
- In the Details section, click Add New
- A new entry line is created for the flightPATH rule.
- Enter a name and description. As an example:

flightPATH Name	Description
Collaboration flightPATH	Flightpath to allow collaboration using Mobility Viewer

- In the Condition section, click Add New
- A new entry line is created
- Enter details as follows:

Condition	Match	Sense	Check	Value
Path		Does	Start	/h/

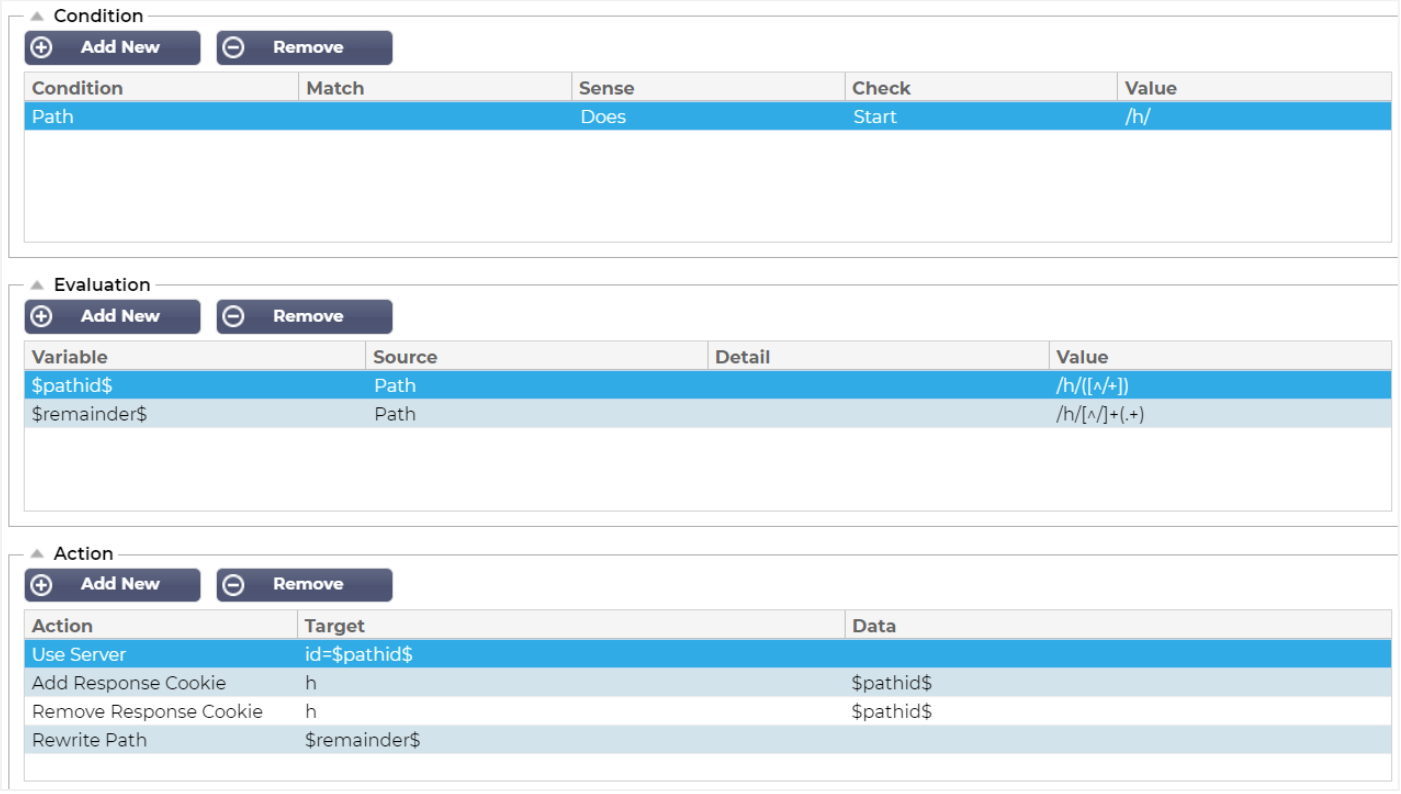
- Next, we have to specify the evaluations to be performed.
- Click the Add New button in the Evaluations section.
- A new entry line is created
- Enter details as follows:

Variable	Source	Detail	Value
$pathid$	Path		/h/([^/+])
$remainder$	Path		/h/[^/]+(.+)

- The final stage is to define the actions.
- Click on the Add New button in the Actions section.
- A blank entry line is created.
- Proceed to create the following actions specified below, clicking the Update button followed by the Add New until all the actions are completed.

Condition	Target	Data
Use Server	Id=$pathid$	
Add Response Cookie	h	$pathid$
Remove Response Cookie	h	$pathid$
Rewrite Path	$remainder$	

- That completes the flightPATH definition and should look like the image below.



Condition	Match	Sense	Check	Value
Path		Does	Start	/h/

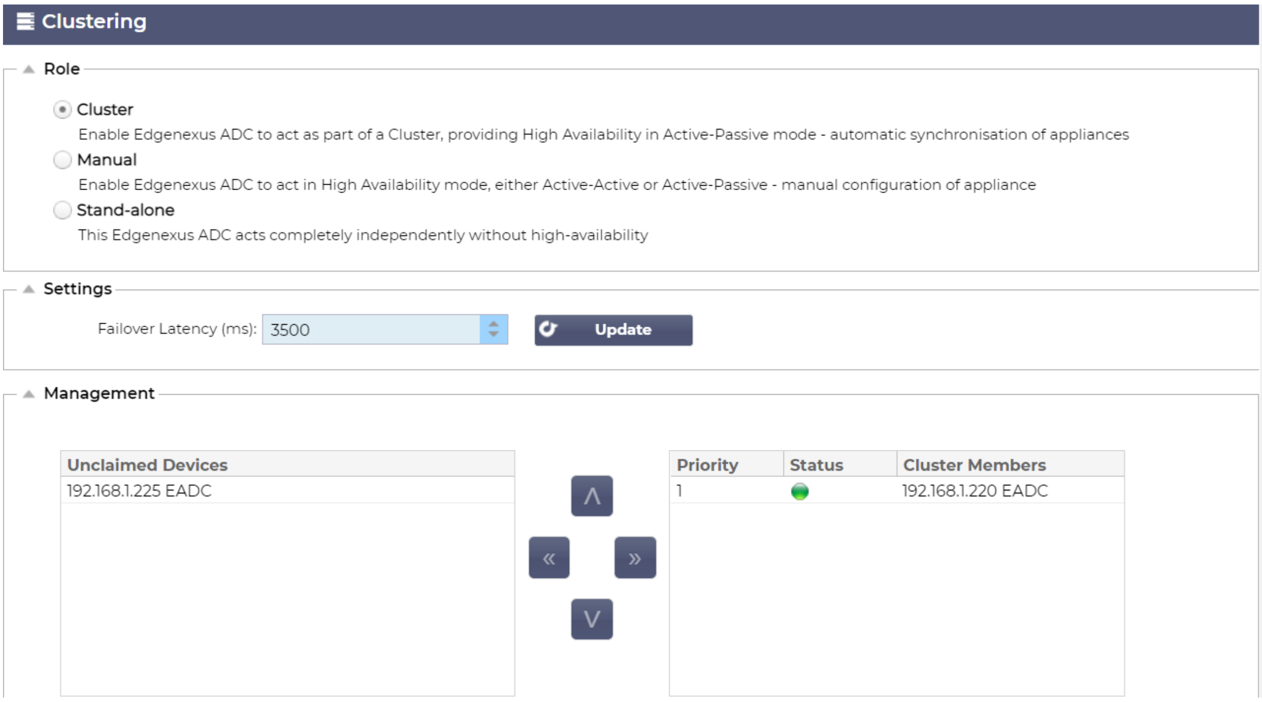
Variable	Source	Detail	Value
$pathid$	Path		/h/([^/+])
$remainder$	Path		/h/[^/]+(.+)

Action	Target	Data
Use Server	id=$pathid$	
Add Response Cookie	h	$pathid$
Remove Response Cookie	h	$pathid$
Rewrite Path	$remainder$	

Clustering the EdgeADC

The EdgeADC can operate as a stand-alone appliance, and it is incredibly reliable. However, in terms of best practice, we must accept that it is as critical as the servers it is load balancing, and we would therefore recommend placing it in a cluster.

- First, stand up a second EdgeADC in the same subnet as the primary.
- Once you have licensed it logon to your Primary EdgeADC
- Proceed to System > Clustering
- You should see the page as below.



Clustering

Role

● Cluster
Enable Edgenexus ADC to act as part of a Cluster, providing High Availability in Active-Passive mode - automatic synchronisation of appliances

○ Manual
Enable Edgenexus ADC to act in High Availability mode, either Active-Active or Active-Passive - manual configuration of appliance

○ Stand-alone
This Edgenexus ADC acts completely independently without high-availability

Settings

Failover Latency (ms): 3500

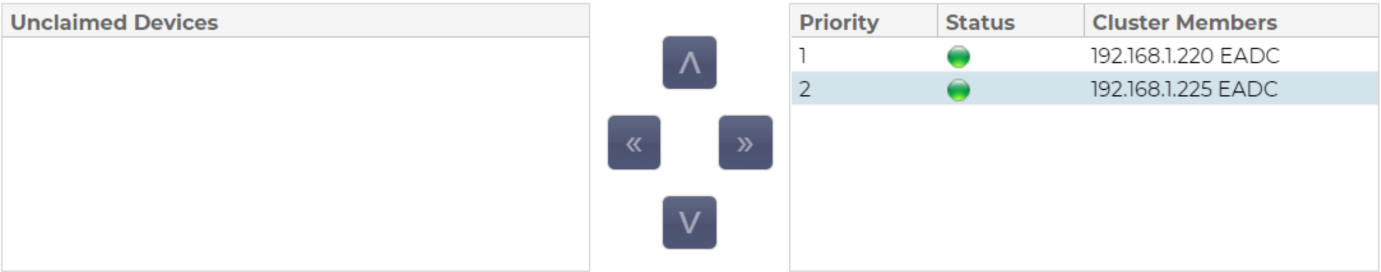
Update

Management

Unclaimed Devices
192.168.1.225 EADC

Priority	Status	Cluster Members
1	●	192.168.1.220 EADC

- You will notice that there are two panels within the Management panel. On the left is the Unclaimed panel. On the right is the Cluster showing the cluster members, their priority, and status.
- In between the two panels is a cluster of arrow buttons.
- Click on the EdgeADC that is in the Unclaimed Panel and click the RIGHT arrow button.
- This action moved the unclaimed EdgeADC into the cluster.
- Immediately it is moved across; the Primary will replicate its settings, including VIPs to the secondary. Note that any apps you have added to the Primary will not be replicated to the Secondary – examples are WAF, GSLB, etc.
- After clustering, the Management panel should look like the one below.

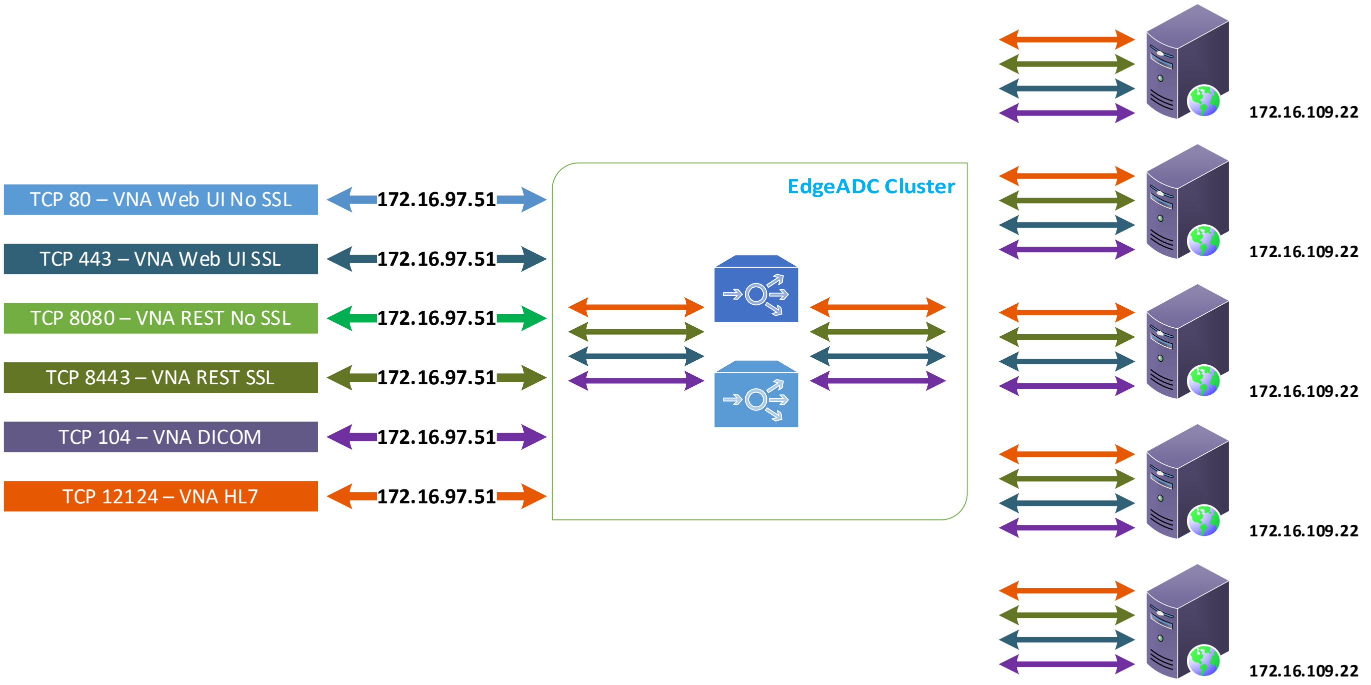


Unclaimed Devices

Priority	Status	Cluster Members
1	●	192.168.1.220 EADC
2	●	192.168.1.225 EADC

Configuring the VIP for VNA

The first VIP and VS we are going to create is the one that handles the VNA traffic. We will be showing the creation of an HTTPS VIP, but the detail for making the HTTP VIP/VS is almost the same. The method being used here is Layer 4 TCP and SSL Passthrough. In this method, the SSL traffic enters the ADC and is immediately sent to the nodes without any inspection.



In this exercise, we will be creating the VIPs and VSs for HTTPS traffic. The four VIP/VS definitions are explained below.

VNA PACS Web UI VIP/VS – SSL Bridging

- The first step is to create the VIP and initial VS for VNA Web UI using SSL.
- Log into the ADC and go to IP Services. This location should be the default entry point.
- Click Add Service
- You will see an empty row into which you will add values similar to the one below. The field values we provide are examples for your reference.

IP Address	Subnet Mask	Port	Service Name	Service Type
172.16.97.51	255.255.255.0	443	*VNA-WEB-UI-SSL*	Layer 4 TCP

So this has now created the initial VIP with the entry IP address of 172.16.97.51.

We will also be using Layer 4 TCP Service Type as we do not need to perform any traffic inspection.

- Now we will define the Real Servers (RS) section.
- Click on the Servers tab to display the Real Servers listing.
- There is a ready-created blank entry to aid you in adding the RS entries.
- Please enter the details relevant to your infrastructure following the examples we have provided below. In our case, we have three array nodes, but you may have more.

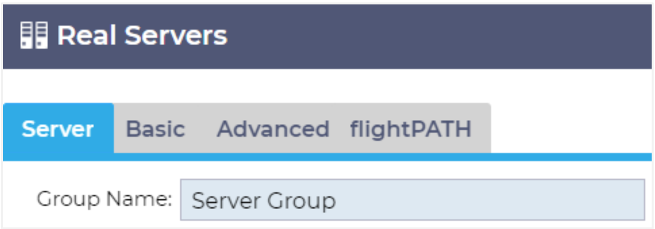
Address	Port	Weight	Calculated Weight	Notes	ID
172.16.109.22	443	100	100	VNA UI APP22	

- Click Update to save.
- Click the Copy Server button and make changes for the second array node.

Address	Port	Weight	Calculated Weight	Notes	ID
172.16.109.23	443	100	100	VNA UI APP22	

- Click Update to save.
- Repeat this process until you have created your Real Server set.
- Click Update to save.

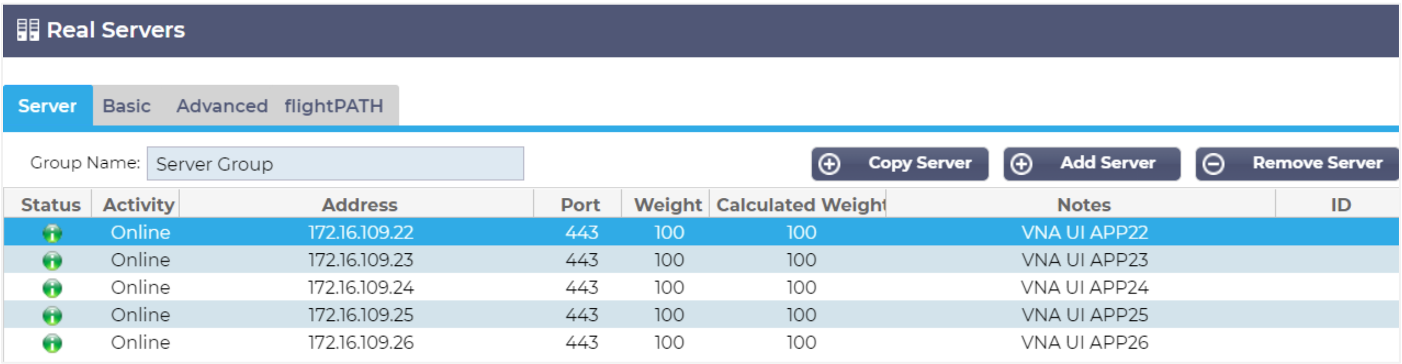
You can also add a name for the server group if you wish.



Group Name: Server Group

We have now defined our first VIP, and its two connected Real Server nodes. We have to do some more work yet to do.

At this stage, you should have a Real Servers section that looks like this.



Group Name: Server Group

Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
●	Online	172.16.109.22	443	100	100	VNA UI APP22	
●	Online	172.16.109.23	443	100	100	VNA UI APP23	
●	Online	172.16.109.24	443	100	100	VNA UI APP24	
●	Online	172.16.109.25	443	100	100	VNA UI APP25	
●	Online	172.16.109.26	443	100	100	VNA UI APP26	

The next stage is to configure the Basic tab.

- Click on the Basic tab within the Real Servers section.
- Make changes as follows:

Field	Value
Load Balancing Policy	IP List Based
Server Monitoring	TCP Connect
Caching Strategy	Off
Acceleration	Off
Virtual Service SSL Cert	Your SSL Certificate
Real Server SSL Cert	Any

- Click Update when done.

The next section that needs configuring is the Advanced tab.

Field	Value
Connectivity	Reverse Proxy
Cipher Options	Defaults
Client SSL Renegotiation	Enabled
Client SSL Resumption	Enabled
SNI Default Cert	None
Security Log	On
Connection Timeout (sec)	1800
Monitoring Interval (sec)	10
Monitoring Timeout (sec)	10
Monitoring In Count	2
Monitoring Out Count	2
Max Connections (per RS)	(leave blank)

Virtual Service for VNA REST using SSL

We will now create a Virtual Service (VS) using the same VIP

- Click on the VNA Web UI VIP you just created
- Click Copy Service
- You will see a copy of the service. Change the values to reflect the ones below. The field values we provide are examples for your reference.

IP Address	Subnet Mask	Port	Service Name	Service Type
172.16.97.51	255.255.255.0	8443	*VNA REST SSL*	Layer 4 TCP

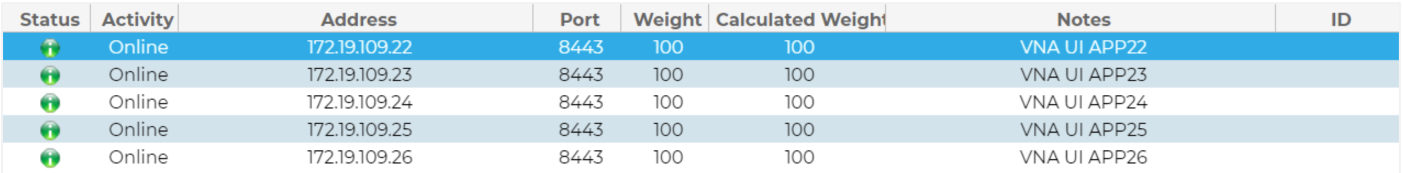
- Click Update

There is no need to define the Real Servers as we copied the VIP. But we do need to make changes to the Real Servers to reflect the port, and the Basic and Advanced tabs, as shown below.

- Click on the Servers tab to display the Real Servers listing.
- Please click and edit each Real Server and make the changes highlighted in RED.

Address	Port	Weight	Calculated Weight	Notes	ID
172.16.109.22	8443	100	100	VNA UI APP22	
172.16.109.23	8443	100	100	VNA UI APP23	
172.16.109.24	8443	100	100	VNA UI APP24	
172.16.109.25	8443	100	100	VNA UI APP25	
172.16.109.26	8443	100	100	VNA UI APP26	

At this stage, you should have a Real Servers section that looks like this.



Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
●	Online	172.19.109.22	8443	100	100	VNA UI APP22	
●	Online	172.19.109.23	8443	100	100	VNA UI APP23	
●	Online	172.19.109.24	8443	100	100	VNA UI APP24	
●	Online	172.19.109.25	8443	100	100	VNA UI APP25	
●	Online	172.19.109.26	8443	100	100	VNA UI APP26	

The next stage is to configure the Basic tab.

- Click on the Basic tab within the Real Servers section.
- Make changes as follows:

Field	Value
Load Balancing Policy	IP List Based
Server Monitoring	TCP Connect
Caching Strategy	Off
Acceleration	Off
Virtual Service SSL Cert	No SSL
Real Server SSL Cert	No SSL

- Click Update when done.

The next section that needs configuring is the Advanced tab.

Field	Value
Connectivity	Reverse Proxy
Cipher Options	Defaults
Client SSL Renegotiation	Enabled
Client SSL Resumption	Enabled
SNI Default Cert	None
Security Log	On
Connection Timeout (sec)	1800
Monitoring Interval (sec)	10
Monitoring Timeout (sec)	10
Monitoring In Count	2
Monitoring Out Count	2
Max Connections (per RS)	(leave blank)

Virtual Service for VNA DICOM using SSL

We will now create a Virtual Service (VS) using the previously configured VS.

- Click on the VNA REST VIP you just created
- Click Copy Service
- You will see a copy of the service. Change the values to reflect the ones below. The field values we provide are examples for your reference.

IP Address	Subnet Mask	Port	Service Name	Service Type
172.16.97.51	255.255.255.0	104	*VNA DICOM*	Layer 4 TCP

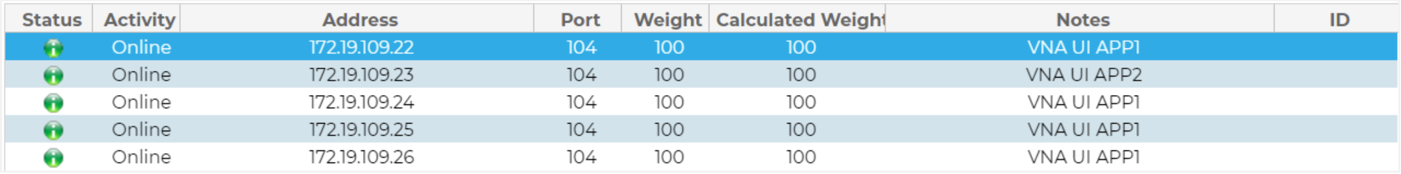
- Click Update

There is no need to define the Real Servers as we copied the VIP. But we do need to make changes to the Real Servers to reflect the port, and the Basic and Advanced tabs, as shown below.

- Click on the Servers tab to display the Real Servers listing.
- Please click and edit each Real Server and make the changes highlighted in RED.

Address	Port	Weight	Calculated Weight	Notes	ID
172.16.109.22	104	100	100	VNA UI APP22	
172.16.109.23	104	100	100	VNA UI APP23	
172.16.109.24	104	100	100	VNA UI APP24	
172.16.109.25	104	100	100	VNA UI APP25	
172.16.109.26	104	100	100	VNA UI APP26	

At this stage, you should have a Real Servers section that looks like this.



Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
●	Online	172.19.109.22	104	100	100	VNA UI APP1	
●	Online	172.19.109.23	104	100	100	VNA UI APP2	
●	Online	172.19.109.24	104	100	100	VNA UI APP1	
●	Online	172.19.109.25	104	100	100	VNA UI APP1	
●	Online	172.19.109.26	104	100	100	VNA UI APP1	

The next stage is to configure the Basic tab.

- Click on the Basic tab within the Real Servers section.
- Make changes as follows:

Field	Value
Load Balancing Policy	Least Connections
Server Monitoring	TCP Connect
Caching Strategy	Off
Acceleration	Off
Virtual Service SSL Cert	No SSL
Real Server SSL Cert	No SSL

- Click Update when done.

The next section that needs configuring is the Advanced tab.

Field	Value
Connectivity	Reverse Proxy
Cipher Options	Defaults
Client SSL Renegotiation	Enabled
Client SSL Resumption	Enabled
SNI Default Cert	None
Security Log	On
Connection Timeout (sec)	1800
Monitoring Interval (sec)	10
Monitoring Timeout (sec)	10
Monitoring In Count	2
Monitoring Out Count	2
Max Connections (per RS)	(leave blank)

Virtual Service for VNA HL7 using SSL

Before we detail the procedure for the HL7 service creation, we want to explain the difference between DICOM and HL7.

There are two options for a modality vendor to implement an IS interface: the Health Level (HL7) or Digital Imaging Communication in Medicine (DICOM) communication standard. HL7 is often customized on-site, while DICOM is much more rigid. HL7 files are somewhat larger sizewise because of character-based encoding, implying conversion of pixel data to characters. Thanks to MPPS, the DICOM protocol can provide more timely and precise information about performed diagnostic studies.

We will now create a Virtual Service (VS) for VNA HL7 using the previously configured VS.

- Click on the VNA DICOM VIP you just created
- Click Copy Service
- You will see a copy of the service. Change the values to reflect the ones below. The field values we provide are examples for your reference.

IP Address	Subnet Mask	Port	Service Name	Service Type
172.16.97.51	255.255.255.0	12124	*VNA HL7*	Layer 4 TCP

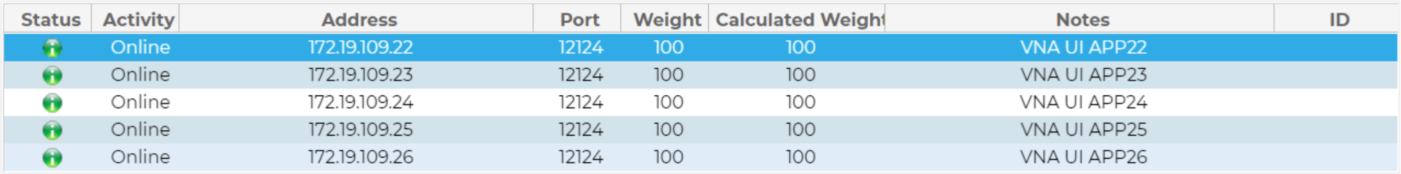
- Click Update

There is no need to define the Real Servers as we copied the VIP. But we do need to make changes to the Real Servers to reflect the port, and the Basic and Advanced tabs, as shown below.

- Click on the Servers tab to display the Real Servers listing.
- Please click and edit each Real Server and make the changes highlighted in RED.

Address	Port	Weight	Calculated Weight	Notes	ID
172.16.109.22	12124	100	100	VNA UI APP22	
172.16.109.23	12124	100	100	VNA UI APP23	
172.16.109.24	12124	100	100	VNA UI APP24	
172.16.109.25	12124	100	100	VNA UI APP25	
172.16.109.26	12124	100	100	VNA UI APP26	

At this stage, you should have a Real Servers section that looks like this.



Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
●	Online	172.19.109.22	12124	100	100	VNA UI APP22	
●	Online	172.19.109.23	12124	100	100	VNA UI APP23	
●	Online	172.19.109.24	12124	100	100	VNA UI APP24	
●	Online	172.19.109.25	12124	100	100	VNA UI APP25	
●	Online	172.19.109.26	12124	100	100	VNA UI APP26	

The next stage is to configure the Basic tab.

- Click on the Basic tab within the Real Servers section.
- Make changes as follows:

Field	Value
Load Balancing Policy	Least Connections
Server Monitoring	TCP Connect
Caching Strategy	Off
Acceleration	Off
Virtual Service SSL Cert	No SSL
Real Server SSL Cert	No SSL

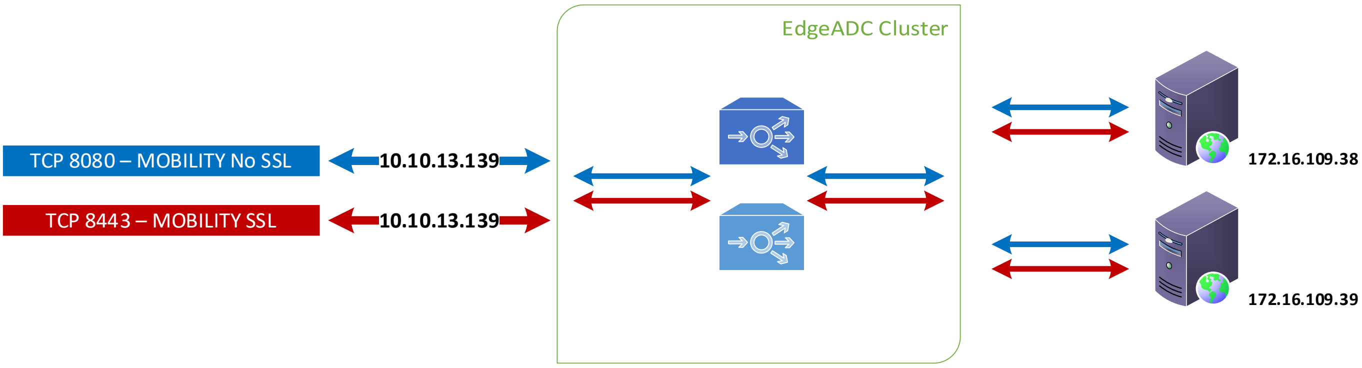
- Click Update when done.

The next section that needs configuring is the Advanced tab.

Field	Value
Connectivity	Reverse Proxy
Cipher Options	Defaults
Client SSL Renegotiation	Enabled
Client SSL Resumption	Enabled
SNI Default Cert	None
Security Log	On
Connection Timeout (sec)	1800
Monitoring Interval (sec)	10
Monitoring Timeout (sec)	10
Monitoring In Count	2
Monitoring Out Count	2
Max Connections (per RS)	(leave blank)

Configuring the VIP for Synapse Mobility

The VIP and VS we are going to create in this example is the one that handles the Mobility traffic. We will be showing the creation of an HTTPS VIP, but the detail for making the HTTP VIP/VS is almost the same. The method being used here is SSL Bridging. In this method, the SSL traffic enters the ADC, is then terminated internally, any inspection required is carried out, and the traffic is then re-encrypted and sent to the nodes.



- The first step is to create the VIP and VS
- Click Add Service
- You will see an empty row into which you will add values similar to the one below. The field values we provide are examples for your reference.

IP Address	Subnet Mask	Port	Service Name	Service Type
10.10.13.139	255.255.255.0	8443	*Mobility VIP SSL*	HTTP

So this has now created the initial VIP with the entry IP address of 10.10.13.139.

We will also be using HTTP Service Type to perform traffic inspection and initiate a flightPATH rule.

- Now we will define the Real Servers (RS) section.
- Click on the Servers tab to display the Real Servers listing.
- There is a ready-created blank entry to aid you in adding the RS entries.
- Please enter the details relevant to your infrastructure following the examples we have provided below. In our case, we have three array nodes, but you may have more.

Address	Port	Weigh t	Calculated Weight	Notes	ID
172.16.96.38	8443	100	100	Mobility Server 1	1

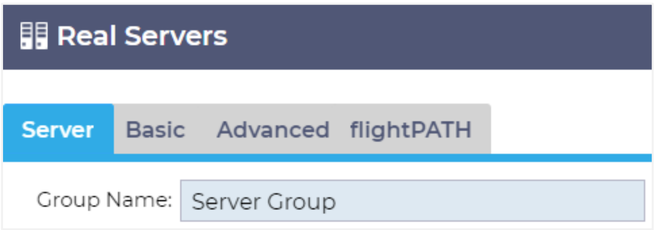
- Click Update to save.
- Click the Copy Server button and make changes for the second node.

Address	Port	Weigh t	Calculated Weight	Notes	ID
172.16.96.39	8443	100	100	Mobility Server 2	2

- Click Update to save.

- Repeat this process until you have created your Real Server set, ensuring you increment the ID field appropriately.
- The ID fields are going to be used in the flightPATH to ensure persistence.
- Click Update to save after each entry.

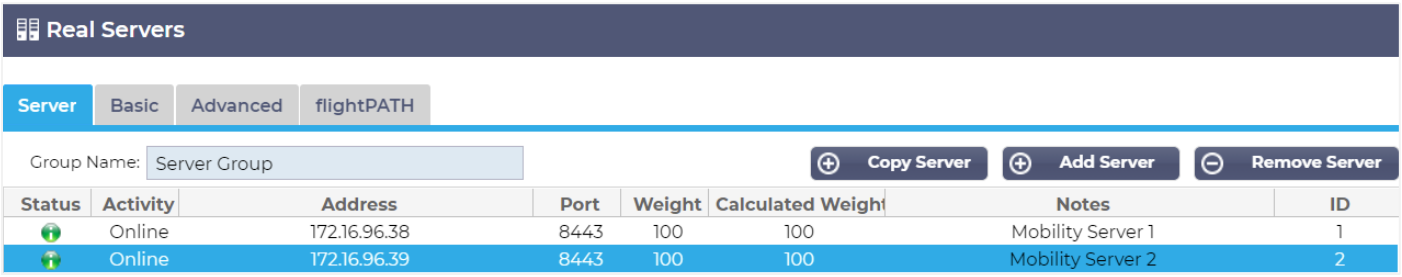
You can also add a name for the server group if you wish.



Group Name: Server Group

We have now defined our first VIP, and its two connected Real Server nodes. We have to do some more work yet to do.

At this stage, you should have a Real Servers section that looks like this.



Group Name: Server Group

Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
●	Online	172.16.96.38	8443	100	100	Mobility Server 1	1
●	Online	172.16.96.39	8443	100	100	Mobility Server 2	2

The next stage is to configure the Basic tab.

- Click on the Basic tab within the Real Servers section.
- Make changes as follows:

Field	Value
Load Balancing Policy	Cookie ID Based
Server Monitoring	TCP Connect
Caching Strategy	Off
Acceleration	Off
Virtual Service SSL Cert	Your SSL Certificate
Real Server SSL Cert	Any

- Note that the Cookie ID Based load balancing ensures that persistence is performed to the mobility server.
- Click Update when done.

The next section that needs configuring is the Advanced tab.

Field	Value
Connectivity	Reverse Proxy
Cipher Options	Defaults
Client SSL Renegotiation	Enabled
Client SSL Resumption	Enabled
SNI Default Cert	None
Security Log	On
Connection Timeout (sec)	1800
Monitoring Interval (sec)	10
Monitoring Timeout (sec)	10
Monitoring In Count	2
Monitoring Out Count	2
Max Connections (per RS)	(leave blank)

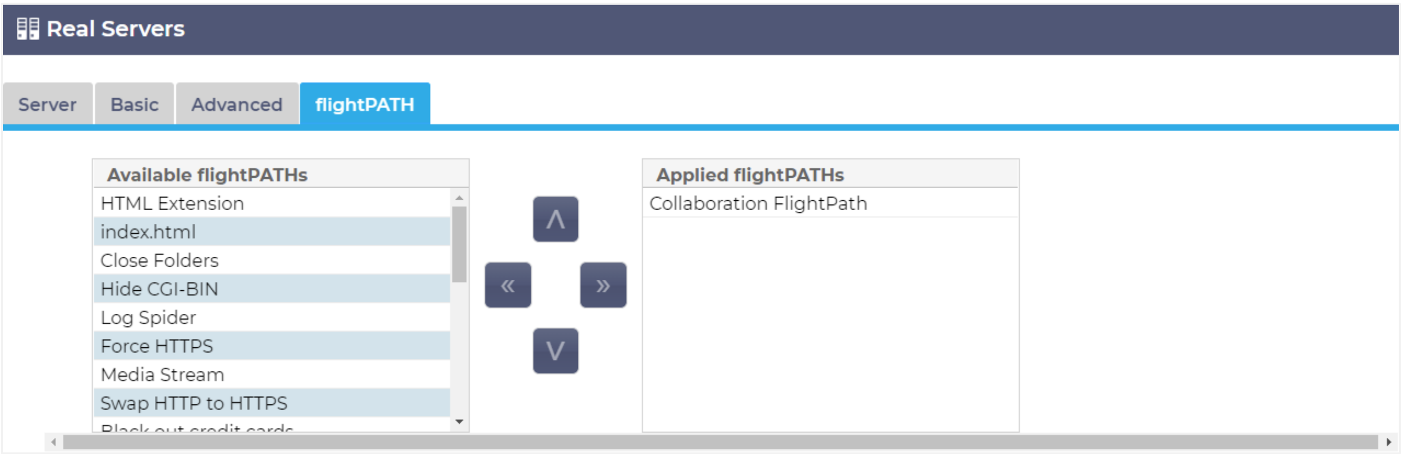
Finally, we have to create the flightPATH entry and allocate it to the VIP.

Adding the flightPATH to the Mobility Virtual Service

The Synapse Mobility server requires a flightPATH rule to ensure that users connecting are automatically redirected to the correct Mobility server on a persistent basis. Details of the flightPATH rule and how to create it are in the section following this one.

We will now assume that you have created the flightPATH rule and are ready to add it to the Mobility VS.

- Click on the IP Services tab, or select IP Services from the Services section in the Navigation panel.
- Click on the Mobility VIP SSL entry in the Virtual Services section
- Click on the flightPATH tab in the Real Servers section
- You will see something like the below image



- Scroll down the list shown in Available flightPATHs and find the flightPATH rule you created.
- Click the right arrow key in the central cluster or drag and drop the flightPATH rule to the Applied flightPATHs section.
- The flightPATH is added and is automatically activated on the service.