EPIC EHR

AN EDGENEXUS ADC DEPLOYMENT GUIDE

EDGE NEXUS

Contents

Document Properties

Document Number: 2.0.6.23.21.19.06

Document Creation Date: June 3, 2021

Document Last Edited: June 23, 2021

Document Author: Jay Savoor

Document Last Edited by:

Document Referral: EdgeADC - Version All

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. However, 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

Information in this document is subject to change without prior notice and does not represent a commitment on the manufacturer's part. No part of this guide may be reproduced or transmitted in any form or means, electronic or mechanical, including photocopying and recording, for any purpose, without the express written permission of the manufacturer. Registered trademarks are properties of their respective owners. Every effort is made to make this guide as complete and as accurate as possible, but no warranty of fitness is implied. The authors and the publisher shall have neither responsibility nor liability to any person or entity for loss or damages arising from using the information contained in this guide.

Trademarks

The Edgenexus logo, Edgenexus, EdgeADC, EdgWAF, EdgeGSLB, EdgeDNS are all trademarks or registered trademarks of Edgenexus Limited. All other trademarks are the properties of their respective owners and are acknowledged.

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 EPIC EHR system and its load balancing. This document contains specific general suggestions and guidance, which may or may not be relevant for use within your organization.

What is EPIC EHR?

Epic is a web-based EHR solution used in community hospitals, independent practices and hospital groups, and hospices.

Epic offers the known and accepted EHR features, and organizations can add modules depending on their specialty. Epic focuses on patient engagement and enabling remote care. Epic is equipped with an extensive browser-accessed patient portal, also available as a native app on Android and iOS operating systems, allowing patients more flexibility in managing their healthcare requirements. Additionally, Epic offers many 'tele-health' options ranging from video visits and post-procedure follow-ups to patient monitoring.

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 EPIC EHR, and this guide explains how to set this up.

Acronyms used

VIP – Virtual IP

VS – Virtual Service

ADC – Edgenexus Application Delivery Controller

VIPs, Ports, and Other Bits

Load balancing the EPIC EHR system is pretty straightforward. We will be providing two load balancing methods in this document, but depending on your infrastructure, other ways of load balancing the system may be possible.

VIP, VS, and Port Requirements

The following are the VS and Port requirements for the EPIC EHR platform. Although you will get better performance using a Layer 4 TCP service type, there may be advantages in using a Layer 7 HTTP service type in conjunction with flightPATH rules that will filter requests based on their origin or URL path.

Port	Protocol	Service Type	Explanation
443	TCP	L7 HTTP	This port is used to handle all HTTPS requests from client applications. You can use Layer 7 with SSL Offload or SSL Bridging.

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.

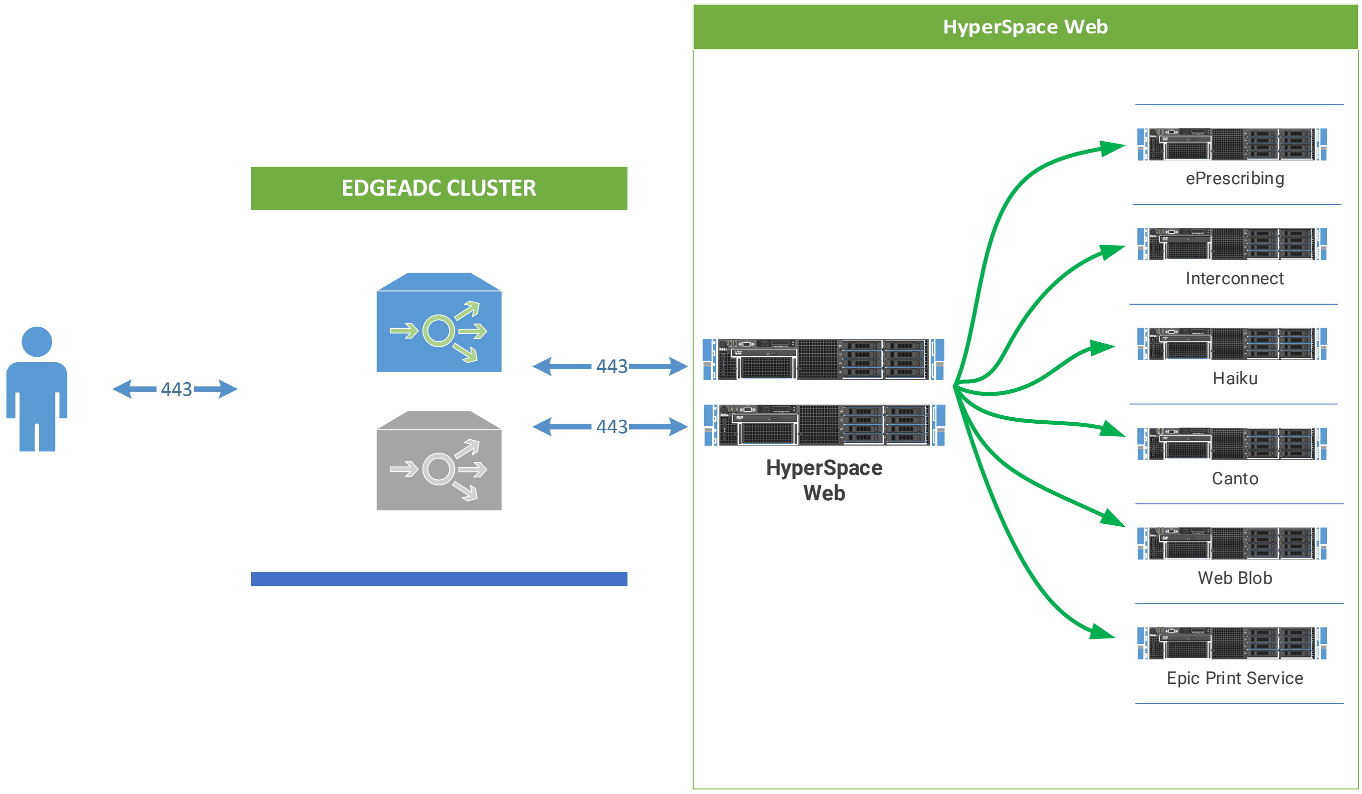
In virtualized environments, we recommend that you set the ADC to 4 vCPU with 8GB RAM, to begin with, and scale up when you need to.

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 EPIC EHR 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. An example diagram is shown below.



Virtual Service Methods

Below are the suggested methods of configuring the ADC for use with EPIC EHR.

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. The ADC service type HTTP is used in this mode.
SSL Offload	This mode allows SSL traffic to be received by the ADC, which then terminates the SSL encryption internally before passing it to the nodes using unencrypted SSL. This mode may not be the desired choice for security reasons. The ADC service type HTTP is used in this mode.

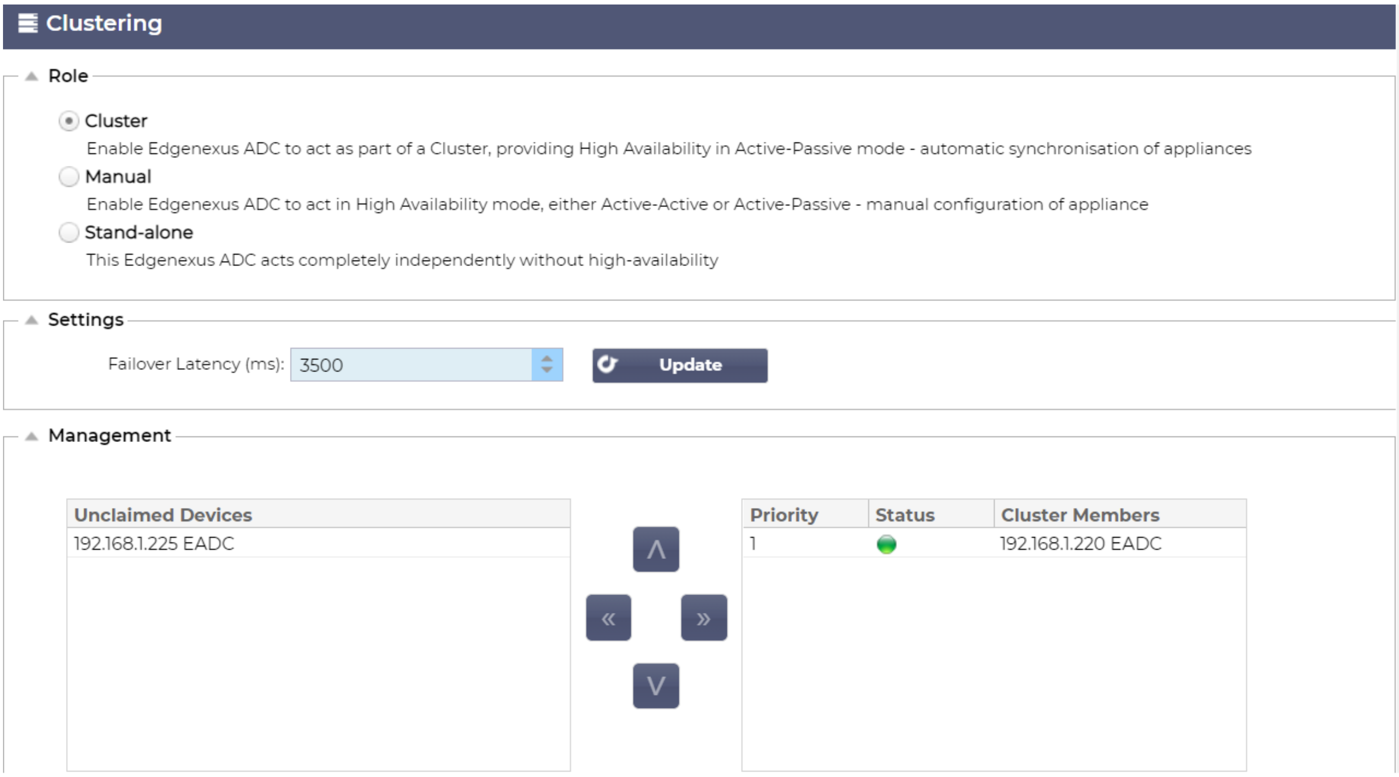
You may wish to use Layer 4 TCP and SSL Passthrough to attain the highest possible throughput speeds. However, if you use L4 TCP, then you will not be able to use the HTTP -> HTTPS redirect we have specified in the VIP examples.

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

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

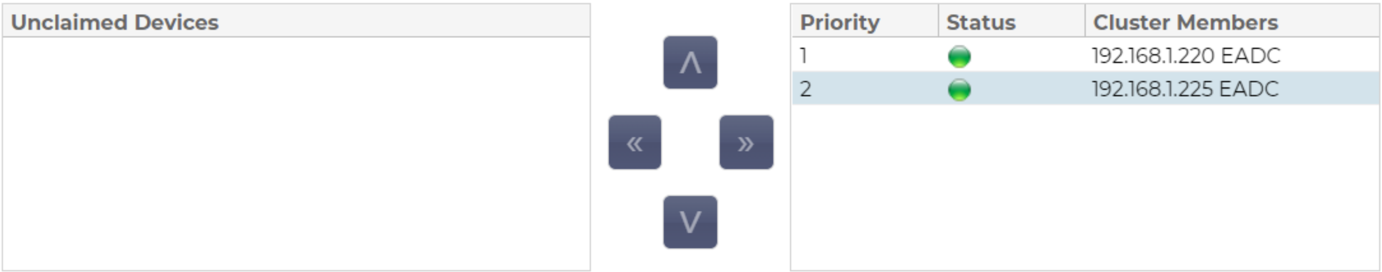
Failover Latency (ms): 3500

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.

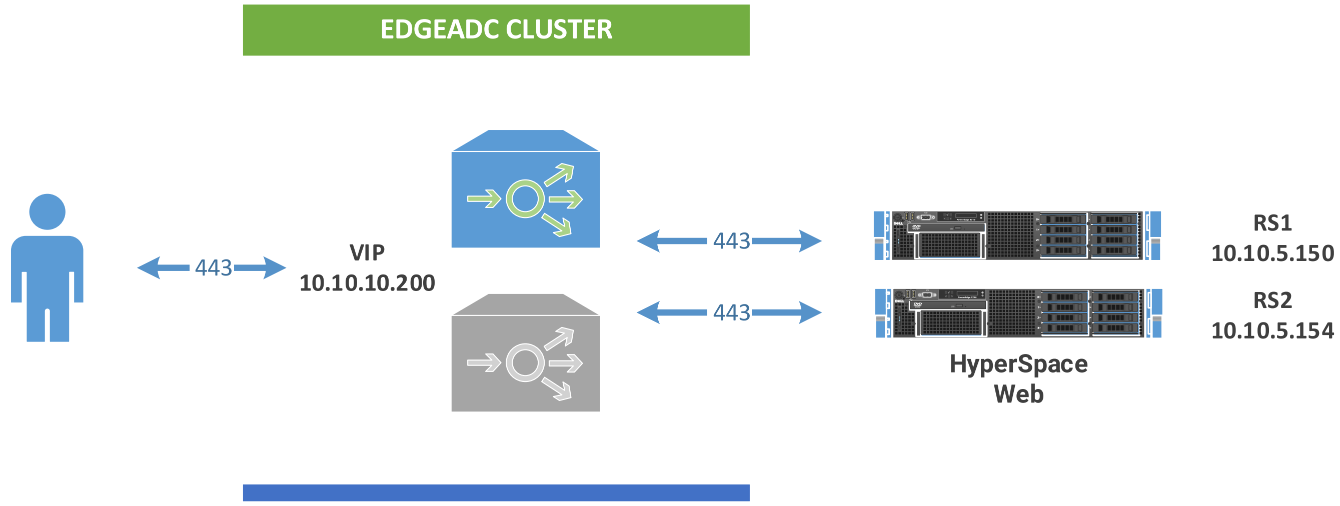


Priority	Status	Cluster Members
1	🟢	192.168.1.220 EADC
2	🟢	192.168.1.225 EADC

EPIC EHR Load Balancing using SSL Bridging

The VIP we are going to create will handle all traffic into the HyperSpace server. The VIP will be linked to a set of Real Servers (RS) and will use SSL Bridging (aka SSL offload and re-encryption). It means that traffic entering the VIP will be decrypted using the organization's SSL certificate and then inspected if required, after which it will be re-encrypted and sent onto the Real Servers.

We will be creating two VIPs, one for the HTTPS entry point and another as a redirector from HTTP to HTTPS, for which will utilize a flightPATH rule.



- The first step is to create the VIP and initial VS
- 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
10.10.10.200	255.255.255.0	443	EPIC HYPERSPACE	HTTP

So this has now created the initial VIP with the entry IP address of 10.10.10.200. In this example, we show a NAT IP address, and the assumption is that there is a firewall between the ADC and the public Internet. You can, of course, have a public IP address as the VIP entry point.

- 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 two nodes, but you may have more.

Address	Port	Weigh t	Calculated Weight	Notes	ID
10.10.5.150	443	100	100	HyperSpace RS1	

- Click Update to save.

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

Address	Port	Weigh t	Calculated Weight	Notes	ID
10.10.5.154	443	100	100	HyperSpace RS2	

- Click Update to save.

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

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

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	200OK
Caching Strategy	By Host
Acceleration	Compression
Virtual Service SSL Cert	Your SSL certificate
Real Server SSL Cert	Any

- Click Update when done.
- Click the Advanced Tab
- Make changes as follows:

Field	Value
Connectivity	Reverse Proxy
Cipher Options	Defaults
Client SSL Renegotiation	Checked
Client SSL Resumption	Checked
SNI Default Certificate	None
Security Log	On
Connection Timeout (sec)	600
Monitoring Interval (sec)	1
Monitoring Timeout (sec)	10
Monitoring In Count	2
Monitoring Out Count	3

Max Connections (per RS)	Blank

Note: To add your SSL certificate, please consult the EdgeADC Administration Guide

Creating the HTTP to HTTPS Redirector VIP

Although we want users to use HTTPS as their entry method, we may get users using HTTP, and we need to move them to HTTPS transparently. To do this, create a second VIP and then utilize one of the built-in flightPATH rules to automate the redirection.

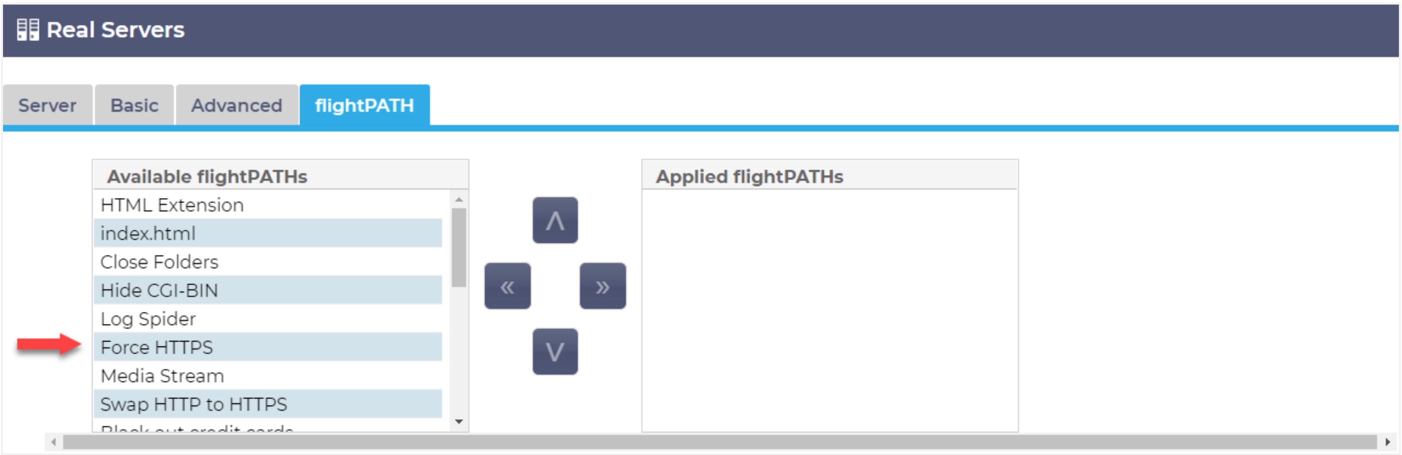
- Click on the first VIP we created.
- Click on Copy Service.
- The VIP and its Real Servers will be copied.
- Change the VIP details as below:

IP Address	Subnet Mask	Port	Service Name	Service Type
10.10.10.200	255.255.255.0	80	EPIC 443 Redirect	HTTP

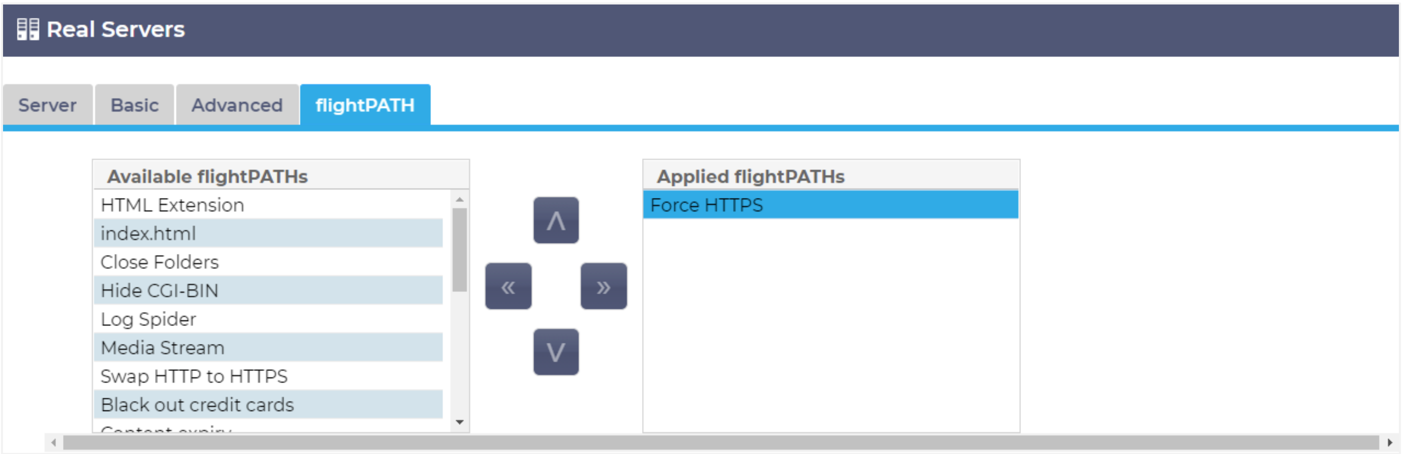
- You will notice that the Real Servers remain with their ports showing 443. The port value does not matter, as we are only going to use this as a redirector.
- Click on the Basic tab within the Real Servers section.
- Make changes as follows:

Field	Value
Load Balancing Policy	Least Connections
Server Monitoring	None
Caching Strategy	By Host
Acceleration	Compression
Virtual Service SSL Cert	Your SSL certificate
Real Server SSL Cert	None

- Click Update when done.
- Click on the flightPATH tab.
- You will see the tab showing the following contents (or similar).



- Click on the Force HTTPS entry in the Available flightPATHs panel on the left.
- Drag the entry to the Applied flightPATHs panel, or use the right arrow button.
- The display should now show as follows:



Available flightPATHs

- HTML Extension
- index.html
- Close Folders
- Hide CGI-BIN
- Log Spider
- Media Stream
- Swap HTTP to HTTPS
- Black out credit cards
- Content expiry

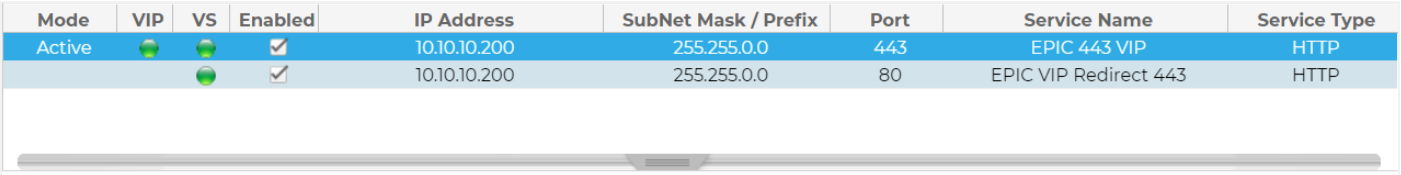
Applied flightPATHs

- Force HTTPS

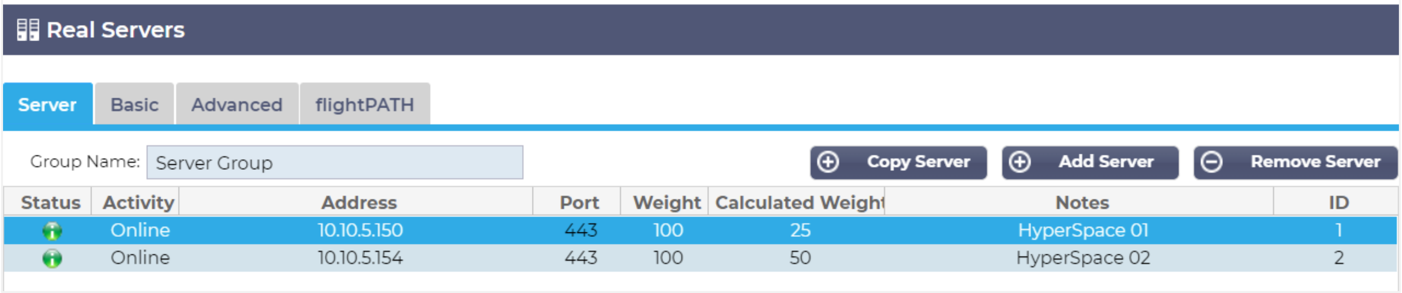
- You can now see the flightPATH has directly been applied.

Traffic now entering the VIP on port 80 will automatically be forced to use HTTPS.

The working solution should look like this:



Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active	●	●	☑	10.10.10.200	255.255.0.0	443	EPIC 443 VIP	HTTP
		●	☑	10.10.10.200	255.255.0.0	80	EPIC VIP Redirect 443	HTTP

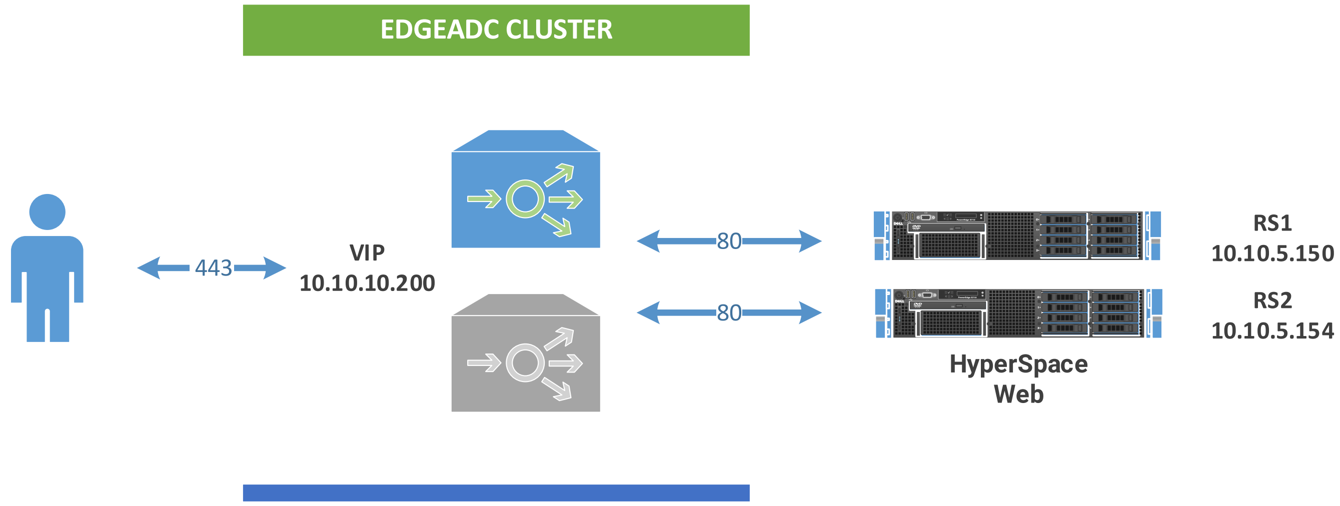


Group Name: Server Group

Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
●	Online	10.10.5.150	443	100	25	HyperSpace 01	1
●	Online	10.10.5.154	443	100	50	HyperSpace 02	2

EPIC EHR Load Balancing using SSL Offload

This VIP is slightly different from the previous one that uses SSL Bridging. We are instead going to create an SSL Offload method for all traffic entering the HyperSpace server. It means that traffic entering the VIP will be decrypted using the organization's SSL certificate and then inspected if required, after which it will be passed onto the Real Servers using HTTP 80.



- The first step is to create the VIP and initial VS
- 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
10.10.10.200	255.255.255.0	443	EPIC OFFLOAD	HTTP

So this has now created the initial VIP with the entry IP address of 10.10.10.200. In this example, we show a NAT IP address, and the assumption is that there is a firewall between the ADC and the public Internet. You can, of course, have a public IP address as the VIP entry point.

- 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 two nodes, but you may have more.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.5.150	80	100	100	HyperSpace RS1	

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

Address	Port	Weigh t	Calculated Weight	Notes	ID
10.10.5.154	80	100	100	HyperSpace RS2	

- Click Update to save.

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

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

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	JSP Session Cookie
Server Monitoring	200OK
Caching Strategy	By Host
Acceleration	Compression
Virtual Service SSL Cert	Your SSL certificate
Real Server SSL Cert	None

- Click Update when done.
- Click the Advanced Tab
- Make changes as follows:

Field	Value
Connectivity	Reverse Proxy
Cipher Options	Defaults
Client SSL Renegotiation	Checked
Client SSL Resumption	Checked
SNI Default Certificate	None
Security Log	On
Connection Timeout (sec)	600
Monitoring Interval (sec)	1
Monitoring Timeout (sec)	10
Monitoring In Count	2
Monitoring Out Count	3

Max Connections (per RS)	Blank

Note: To add your SSL certificate, please consult the EdgeADC Administration Guide

Creating the HTTP to HTTPS Redirector VIP

Although we want users to use HTTPS as their entry method, we may get users using HTTP, and we need to move them to HTTPS transparently. To do this, create a second VIP and then utilize one of the built-in flightPATH rules to automate the redirection.

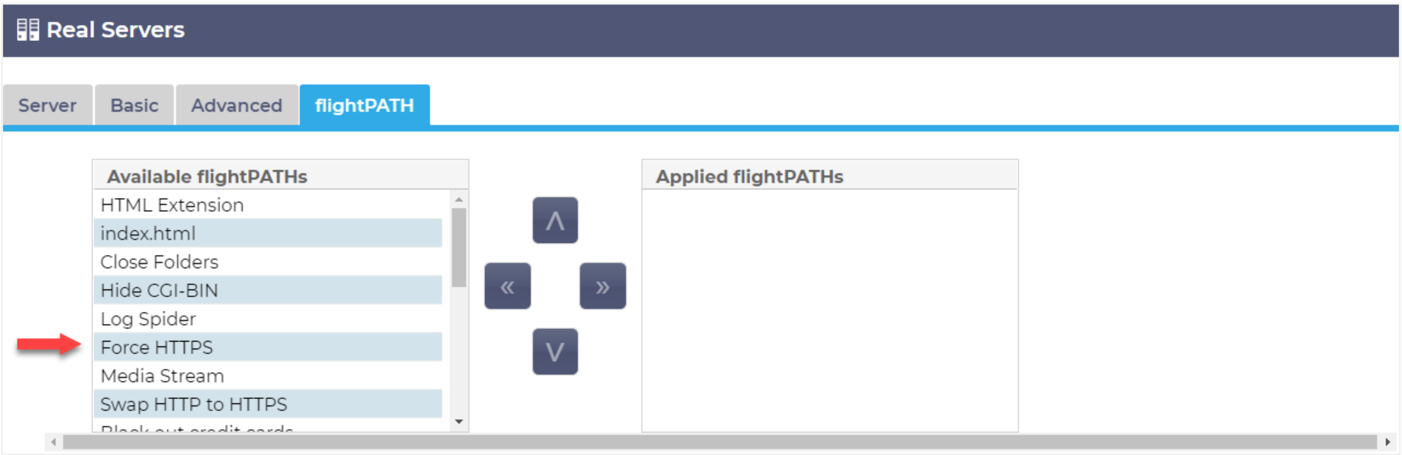
- Click on the first VIP we created.
- Click on Copy Service.
- The VIP and its Real Servers will be copied.
- Change the VIP details as below:

IP Address	Subnet Mask	Port	Service Name	Service Type
10.10.10.200	255.255.255.0	80	EPIC 443 Redirect	HTTP

- You will notice that the Real Servers remain with their ports showing 443. The port value does not matter, as we are only going to use this as a redirector.
- Click on the Basic tab within the Real Servers section.
- Make changes as follows:

Field	Value
Load Balancing Policy	Least Connections
Server Monitoring	None
Caching Strategy	By Host
Acceleration	Compression
Virtual Service SSL Cert	Your SSL certificate
Real Server SSL Cert	None

- Click Update when done.
- Click on the flightPATH tab.
- You will see the tab showing the following contents (or similar).


Real Servers

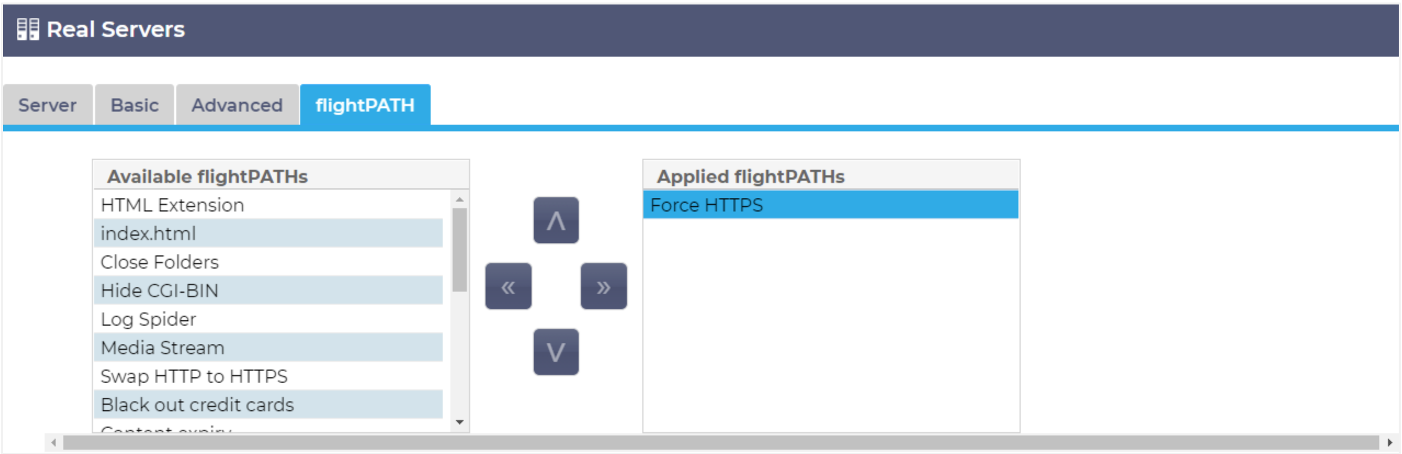
Server | Basic | Advanced | flightPATH

Available flightPATHs

HTML Extension
index.html
Close Folders
Hide CGI-BIN
Log Spider
Force HTTPS
Media Stream
Swap HTTP to HTTPS

Applied flightPATHs

- Click on the Force HTTPS entry in the Available flightPATHs panel on the left.
- Drag the entry to the Applied flightPATHs panel, or use the right arrow button.
- The display should now show as follows:



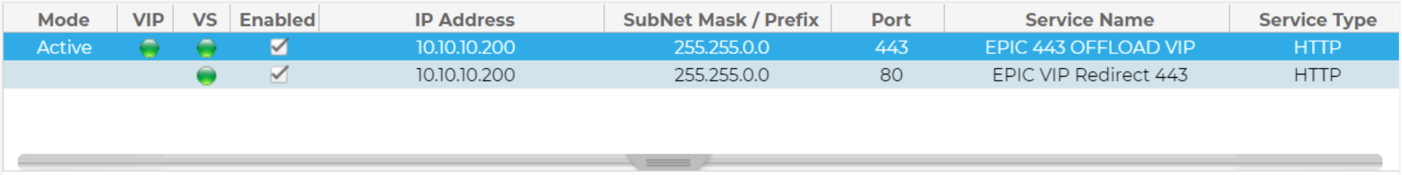
Available flightPATHs
- HTML Extension
- index.html
- Close Folders
- Hide CGI-BIN
- Log Spider
- Media Stream
- Swap HTTP to HTTPS
- Black out credit cards
- Content expiry

Applied flightPATHs
- Force HTTPS

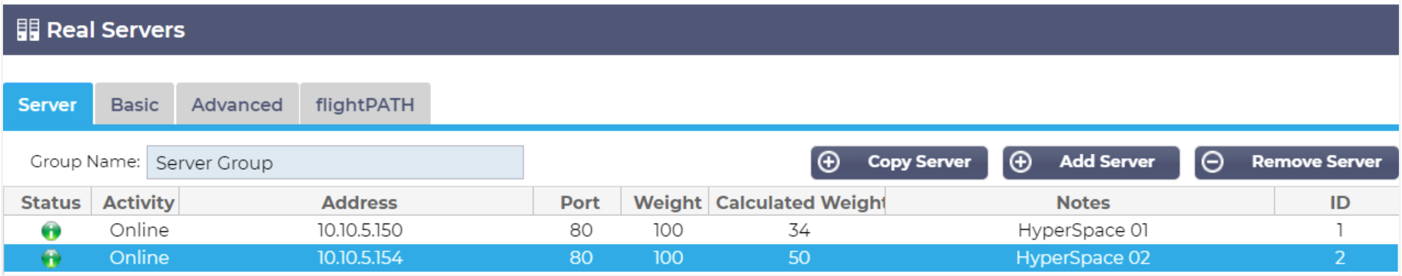
- You can now see the flightPATH has directly been applied.

Traffic now entering the VIP on port 80 will automatically be forced to use HTTPS.

The working solution should look like this:



Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active	●	●	☑	10.10.10.200	255.255.0.0	443	EPIC 443 OFFLOAD VIP	HTTP
		●	☑	10.10.10.200	255.255.0.0	80	EPIC VIP Redirect 443	HTTP



Group Name: Server Group

Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
●	Online	10.10.5.150	80	100	34	HyperSpace 01	1
●	Online	10.10.5.154	80	100	50	HyperSpace 02	2