NETAPP STORAGEGRID

AN EDGENEXUS ADC DEPLOYMENT GUIDE

EDGE NEXUS

Contents

Document Properties

Document Number: 2.0.6.24.21.12.06

Document Creation Date: June 11, 2021

Document Last Edited: June 24, 2021

Document Author: Jay Savoor

Document Last Edited by:

Document Referral: EdgeADC - Version 4.2.7.x and higher

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

Trademarks

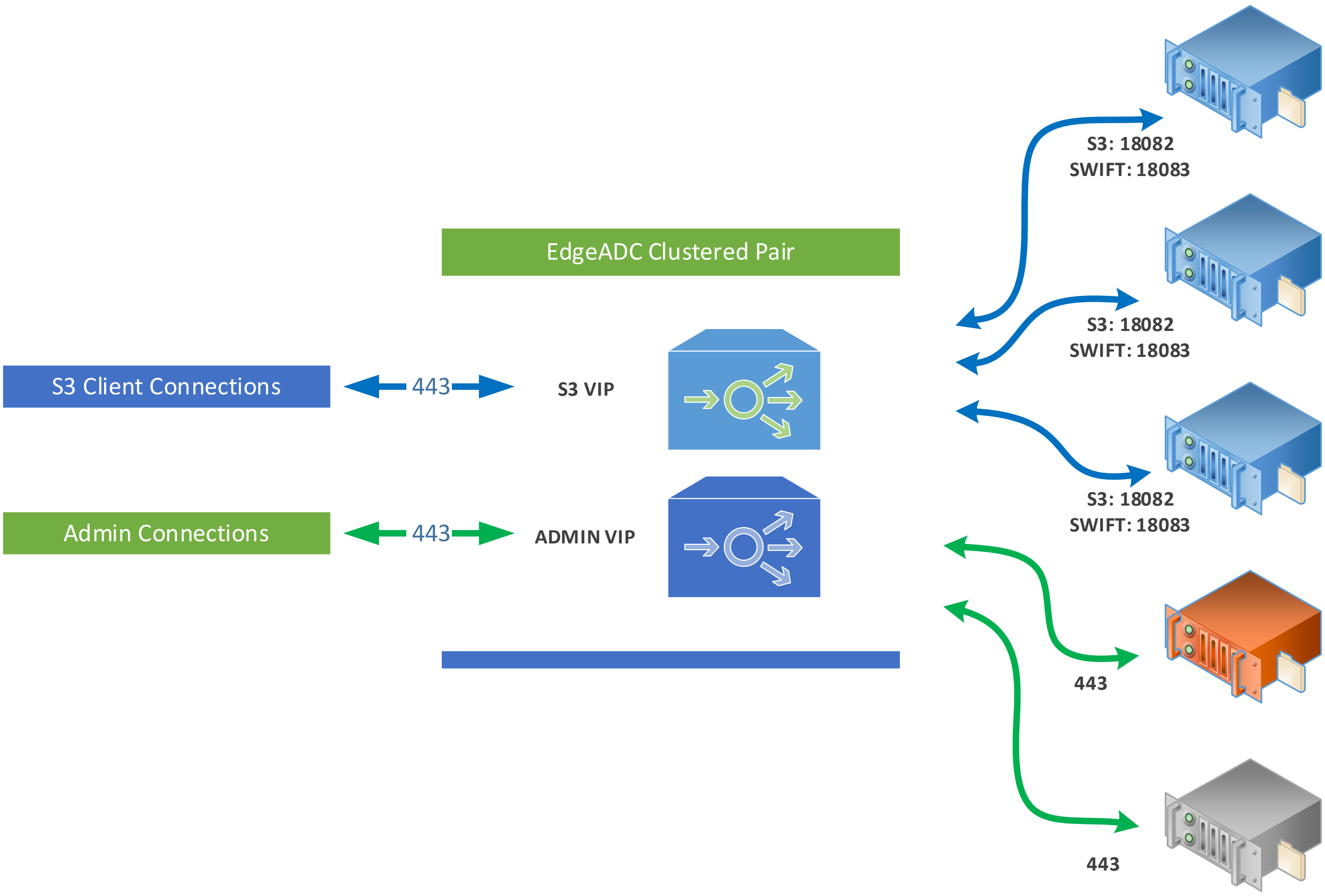
The Edgenexus logo, Edgenexus, EdgeADC, EdgWAF, EdgeGSLB, EdgeDNS are all trademarks or registered trademarks of Edgenexus Limited. All other trademarks are the properties of their respective owners and are acknowledged.

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



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 NetApp StorageGRID, and this guide explains how to set this up.

About NetApp StorageGRID

A software-defined, object-based storage system, NetApp is one of the pioneers in the storage world. The system uses industry-standard object APIs like Swift and Amazon S3, allowing single namespaces to build across multiple sites.

The NetApp StorageGRID system has its proprietory load balancing methodology built witin the Admin Nodes, but third-party ADC technology such as EdgeADC has proven far more effective.

The nodes that we will be looking to load balance in this document will be the Admin and Storage nodes.

Application versions supported

This document supports the following NetApp StorageGRID versions:

- NetApp StorageGrid 11.3 and later

Acronyms used

VIP – Virtual IP

VS – Virtual Service

ADC – Edgenexus Application Delivery Controller

VIPs, Ports, and Other Bits

When load balancing NetApp StorageGRID, the following VIPs will be needed for operations.

- HTTPS VIP for Grid/Tenant Admin Connections
- HTTPS VIP for S3 Client Connections

Port Requirements

The following are the port requirements for the NetApp StorageGRID platform. The ingress ports will be 443 for both VIPS, but the egress ports from the ADC to the Storage nodes will depend on the protocol in use. For example, the S3 protocol uses 18082, while the Swift protocol uses 18083.

Port	Protocol	Service Type	Explanation
80	TCP	L4-TCP or L7 HTTP	This port is used to handle all HTTP requests from client applications. You can use Layer 4 TCP with SSL Passthrough or Layer 7 with SSL Offload or SSL Bridging.
443	TCP	L4-TCP or L7 HTTPS	This port is used to handle all HTTPS requests from client applications. You can use Layer 4 TCP with SSL Passthrough or 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.

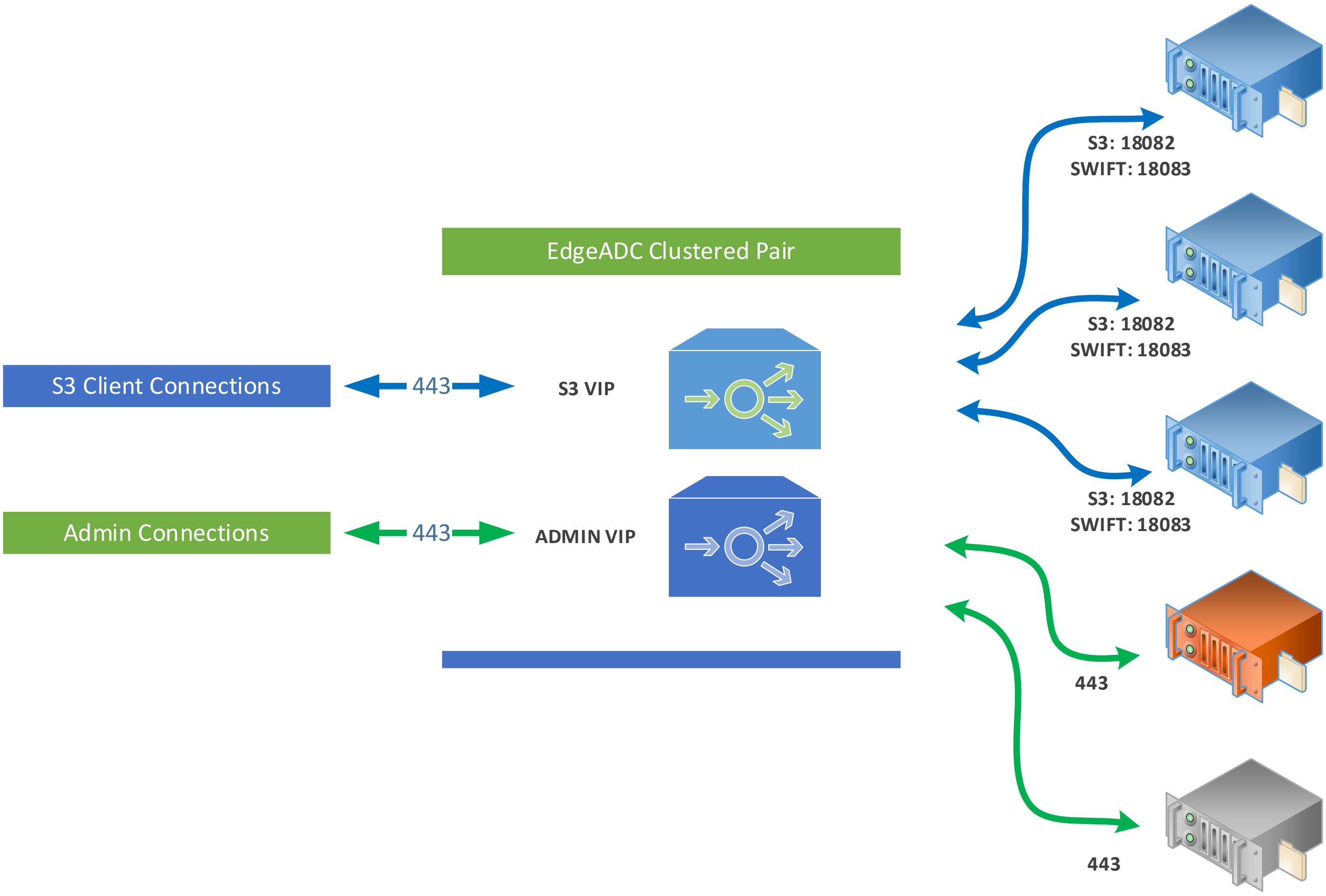
In virtualized environments, we recommend that you set the ADC to 4 vCPU with 8GB RAM, to begin with, and scale up when you need to.

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 NetApp StorageGRID 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

There are several methods of configuring the ADC for use with NetApp StorageGRID.

SSL Passthrough If you do not require to inspect and manage the traffic coming to the Admin nodes, then this is the mode that we will use. First, the traffic enters the ADC on port 443 using SSL. Then, the traffic is sent onto the Admin nodes without inspection.
ADC service type Layer 4 TCP is used.

SSL Bridging We would suggest that you use Layer 7 for the Admin nodes. In this mode, you can then use flightPATH to inspect and manage the traffic. For example, you may wish to limit access to the Admin system from specific IP addresses or subnets, which is only possible using Layer 7 and flightPATH. 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.

SSL Termination We will be using this mode for the Storage nodes. Traffic will enter the ADC using 443 and exit using the appropriate port depending on whether we use S3 or Swift. In this mode, SSL traffic will be received by the ADC, which then terminates the SSL encryption internally before passing it to the Storage nodes unencrypted.
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.

ADMIN VIP – Using SSL Bridging

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 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
10.10.10.100	255.255.255.0	443	*NetApp Admin*	HTTP

So this has now created the initial VIP with the entry IP address of 10.10.10.222. 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 three array nodes, but you may have more.

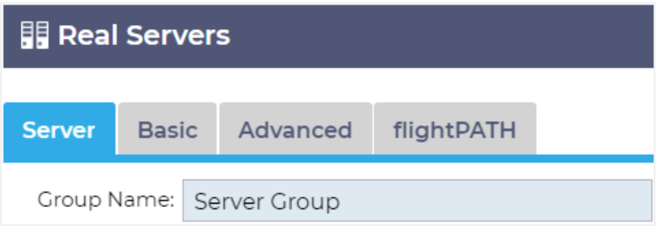
Address	Port	Weigh t	Calculated Weight	Notes	ID
10.10.10.201	443	100	100	Node 1	

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

Address	Port	Weigh t	Calculated Weight	Notes	ID
10.10.10.202	443	100	100	Node 2	

- Click Update to save.

You can 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.

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

- Click Update when done.

There are no configurations to be done within the Advanced tab.

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.

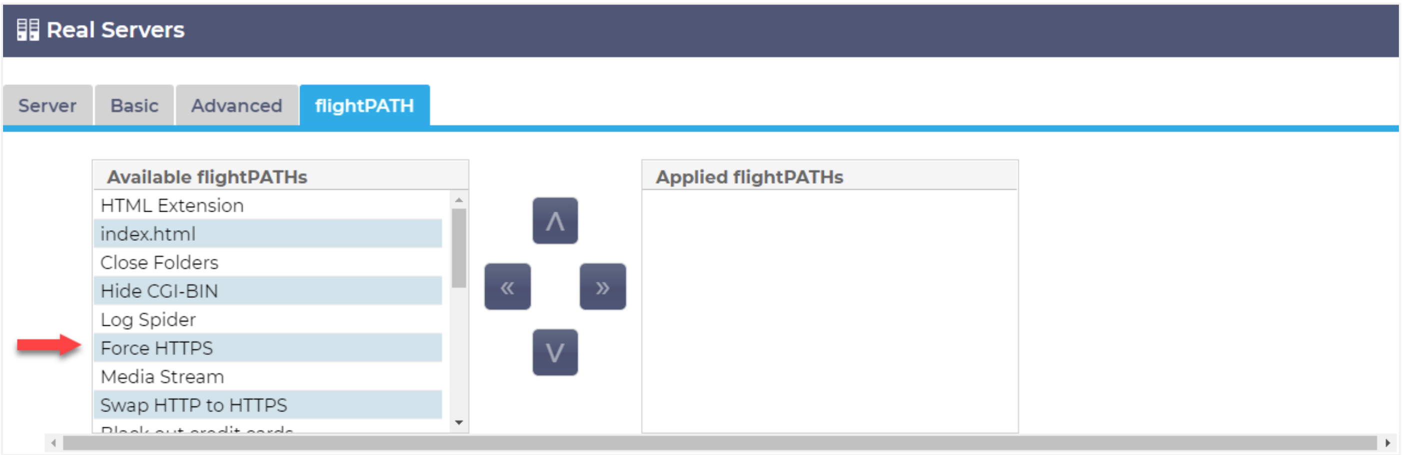
- Click on the first VIP we created.
- Click on Copy Service.
- The VIP and its Real Servers will be copied.
- Change the VIP details as below:

IP Address	Subnet Mask	Port	Service Name	Service Type
10.10.10.222	255.255.255.0	80	NetApp 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:

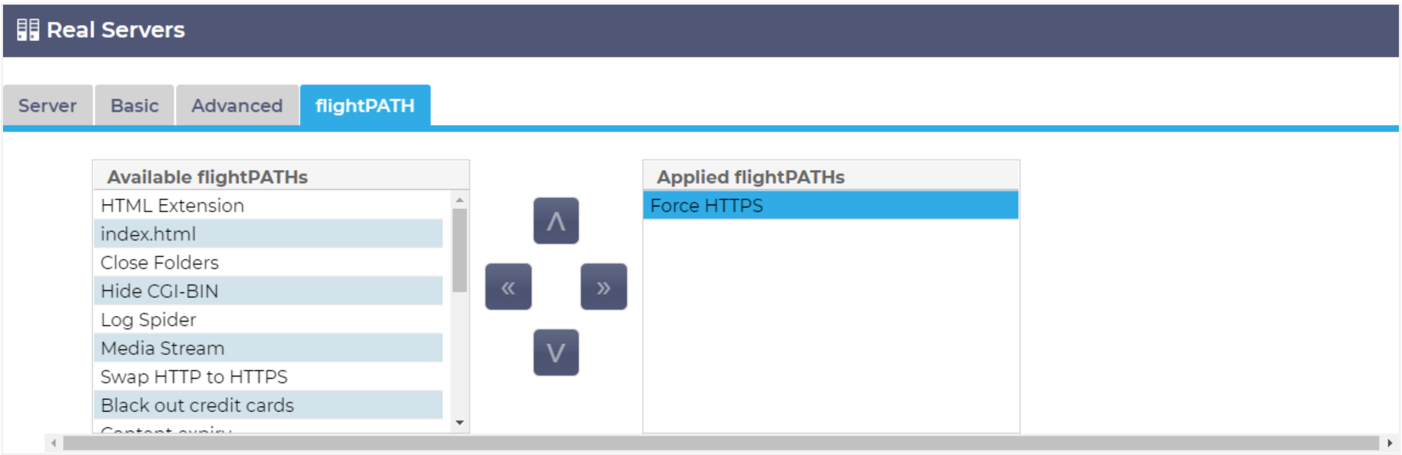
Field	Value
Load Balancing Policy	Least Connections
Server Monitoring	None
Caching Strategy	By Host
Acceleration	Compression
Virtual Service SSL Cert	Your SSL certificate
Real Server SSL Cert	None

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



Real Servers

- 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:

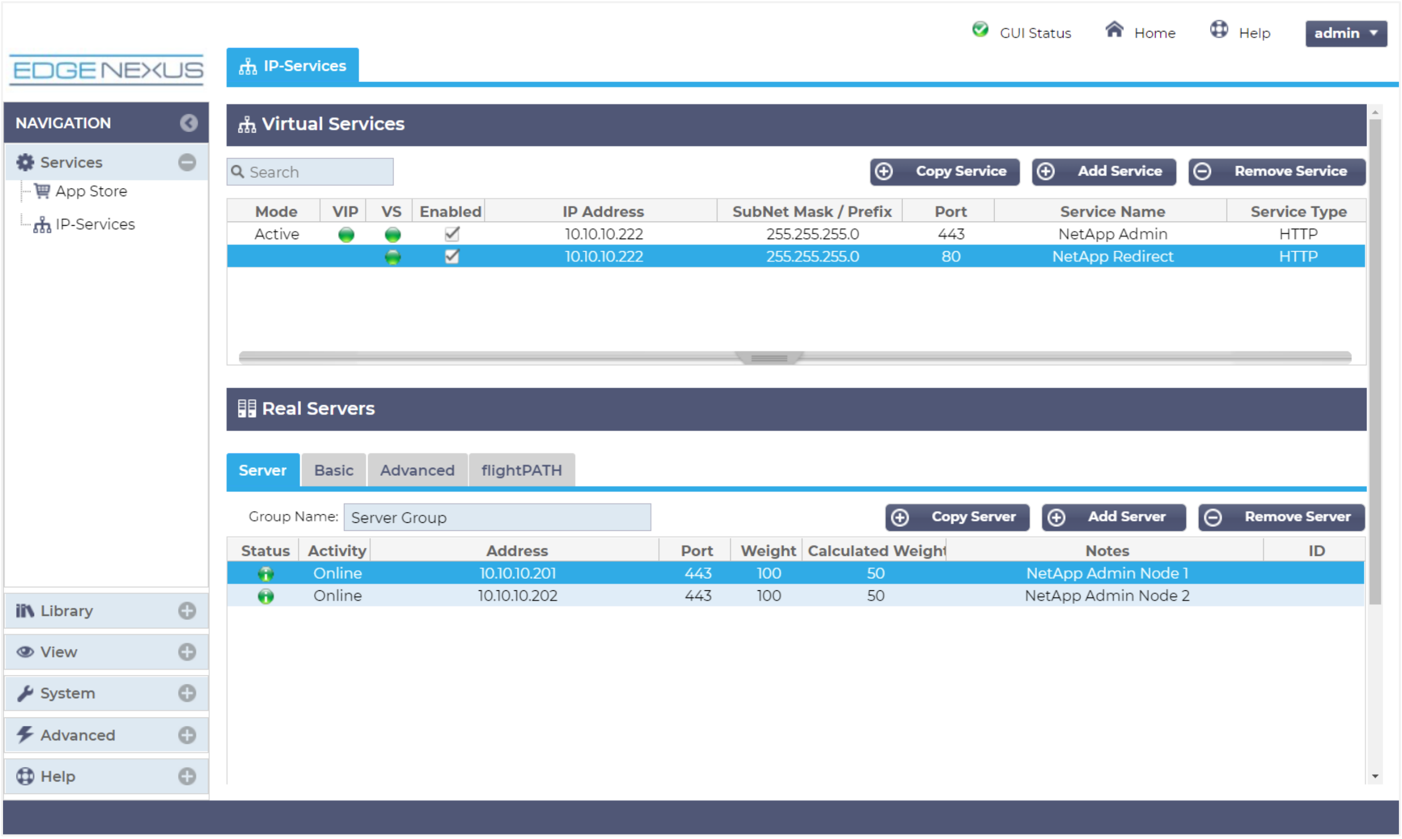


Real Servers

- 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 to protect the Admin nodes should look like this:



Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active	●	●	☑	10.10.10.222	255.255.255.0	443	NetApp Admin	HTTP
		●	☑	10.10.10.222	255.255.255.0	80	NetApp Redirect	HTTP

Group Name: Server Group

Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
●	Online	10.10.10.201	443	100	50	NetApp Admin Node 1	
●	Online	10.10.10.202	443	100	50	NetApp Admin Node 2	

Using flightPATH to restrict Admin Node access

When using Layer 7, the ADC allows you to use the flightPATH technology to inspect and manage the encrypted SSL traffic.

Several pre-defined flightPATH rules are included with the ADC, which can be found under Library > flightPATH.

You can also define your own rules using the provided methods or using RegEX.

NetApp Node VIP – Using SSL Offload

Unlike the SSL Bridging method used in the previous VIP, we will now be creating an SSL Offload, aka SSL Termination. In this mode, traffic will enter the VIP on Port 443 using SSL. It will then be decrypted and sent to the nodes using the appropriate target ports: 18082 for S3 traffic or 18083 for Swift.

- 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
10.10.10.223	255.255.255.0	443	*NetApp Storage Nodes*	HTTP

So this has now created the initial VIP with the entry IP address of 10.10.10.223. 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 three array nodes, but you may have more.

Address	Port	Weigh t	Calculated Weight	Notes	ID
10.10.5.101	18082*	100	100	Array Node 1	

* For S3 connections, use 18082, and for Swift connections, use 18083

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

Address	Port	Weigh t	Calculated Weight	Notes	ID
10.10.5.102	18082*	100	100	Array Node 2	

* For S3 connections, use 18082, and for Swift connections, use 18083

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

Address	Port	Weigh t	Calculated Weight	Notes	ID
10.10.5.103	18082*	100	100	Array Node 2	

* For S3 connections, use 18082, and for Swift connections, use 18083

- 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 connected Real Server nodes. We have to do some 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	TCP Connect
Caching Strategy	Off
Acceleration	Compression
Virtual Service SSL Cert	Your SSL certificate
Real Server SSL Cert	None**

** The value of None specifies that there is SSL Offload/Termination being performed.

The above configuration will ensure SSL termination/offload.

- Click Update when done.

There are no configurations to be done within the Advanced tab.

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.

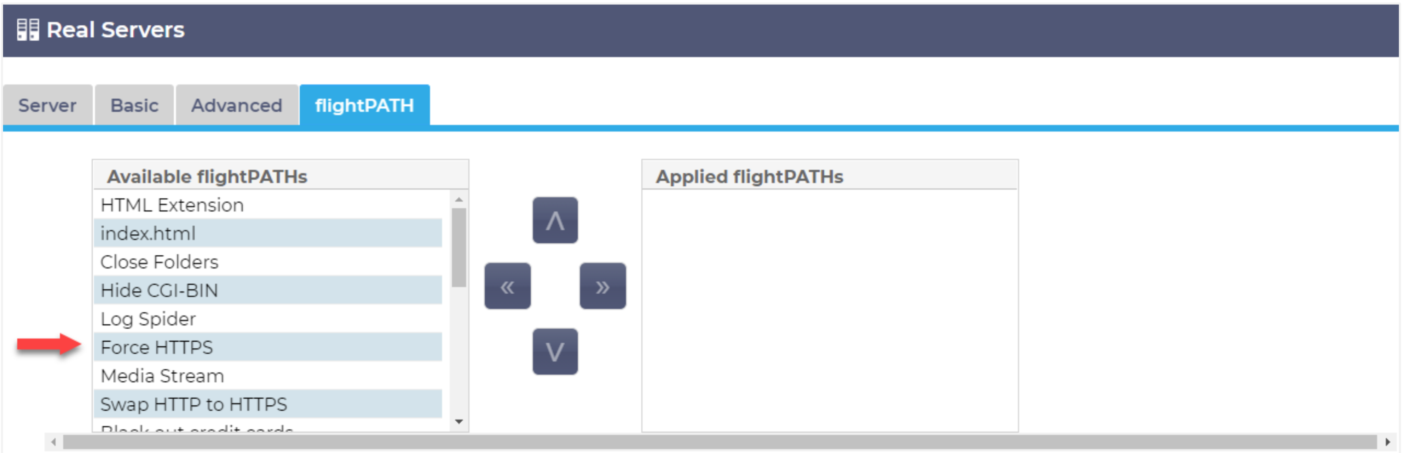
- Click on the first VIP we created.
- Click on Copy Service.
- The VIP and its Real Servers will be copied.
- Change the VIP details as below:

IP Address	Subnet Mask	Port	Service Name	Service Type
10.10.10.222	255.255.255.0	80	NetApp Redirect	HTTP

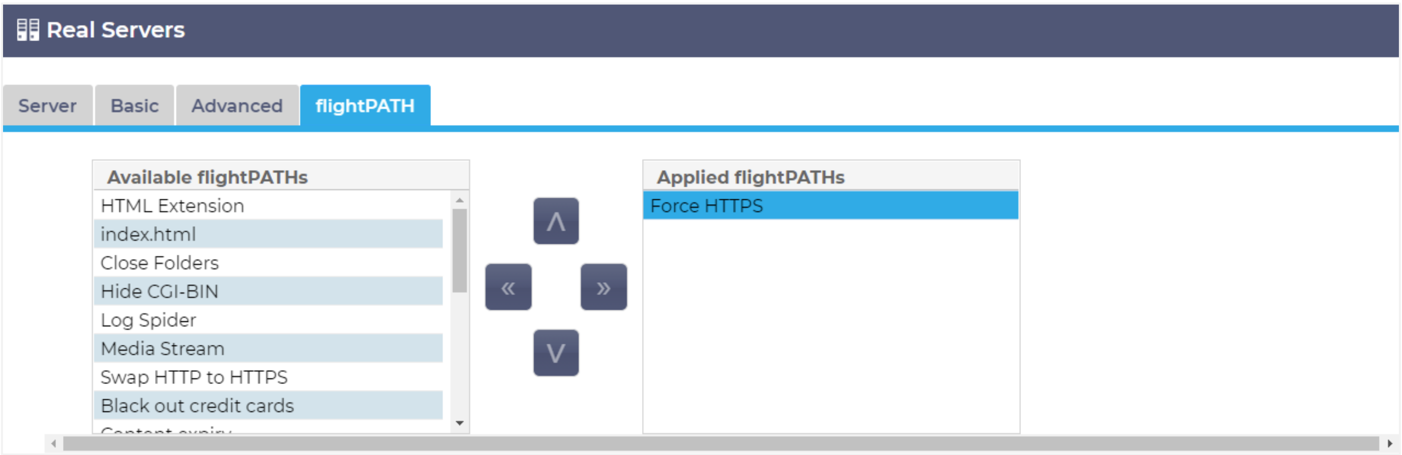
- You will notice that the Real Servers remain with their ports showing 443. The port value does not matter, as we are only going to use this as a redirector.
- Click on the Basic tab within the Real Servers section.
- Make changes as follows:

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).



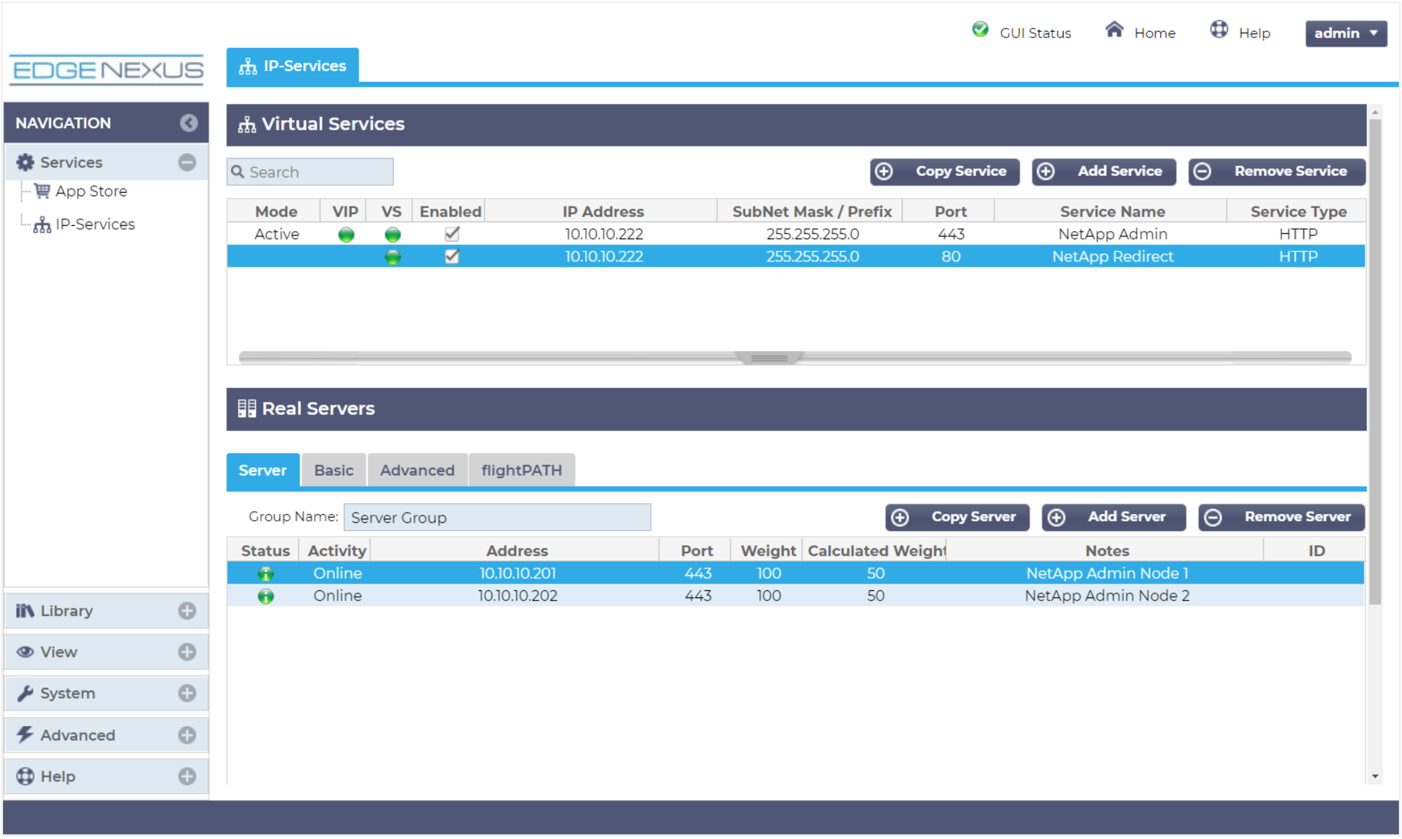
- Click on the Force HTTPS entry in the Available flightPATHs panel on the left.
- Drag the entry to the Applied flightPATHs panel, or use the right arrow button.
- The display should now show as follows:



- 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 to protect the Admin nodes should look like this:



Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active	●	●	☑	10.10.10.222	255.255.255.0	443	NetApp Admin	HTTP
		●	☑	10.10.10.222	255.255.255.0	80	NetApp Redirect	HTTP

Group Name: Server Group

Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
●	Online	10.10.10.201	443	100	50	NetApp Admin Node 1	
●	Online	10.10.10.202	443	100	50	NetApp Admin Node 2	

Using flightPATH to restrict Admin Node access

When using Layer 7, the ADC allows you to use the flightPATH technology to inspect and manage the encrypted SSL traffic.

Several pre-defined flightPATH rules are included with the ADC, which can be found under Library > flightPATH.

You can also define your own rules using the provided methods or using RegEX.