CEPH OBJECTS

AN EDGENEXUS ADC DEPLOYMENT GUIDE

Contents

Document Properties

Document Number: 2.0.6.24.21.12.06

Document Creation Date: May 20, 2021

Document Last Edited: June 24, 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. 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

Ceph is provided through the open-source market and is a free-of-cost, object-based storage solution.

High availability is supported in Ceph architecture using load balancers that are placed in advanced positions. The EdgeADC, with its advanced health monitoring and flightpath rules technology, makes the availability of the storage infrastructure assured.

The EdgeADC is capable of load-balancing Ceph, and this guide explains how to set this up. We do recommend that you have a working Ceph solution before load balancing using this guide.

Document Intention

This document is aimed at administrators who need to load-balance their Ceph storage nodes efficiently and quickly.

VIPs, Ports, and Other Bits

When load balancing Ceph, the following ports will be used. Ceph, however, is a very flexible system and can be configured to use ports you wish. So the following pages with their port requirements are guides, and you will need to replace the stated ports with the ports you decide are right for your environment.

Port Requirements

The following are the port requirements for the Ceph Objects platform.

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 for access over port 80, but we do not recommend this as it is unsecured. Using Layer 7 will also allow for flightPATH rules to be used.
443	TCP	L4-TCP or L7 HTTP	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. Using Layer 7 will also allow for flightPATH rules to be used
8080	TCP	L4-TCP	It is used to handle HTTP requests for Ceph Dashboard. You can use Layer 4 TCP for access over port 80, but we do not recommend this as it is unsecured. Using Layer 7 will also allow for flightPATH rules to be used.
8443	TCP	L4-TCP or L7 HTTP	It is used to handle SSL secured requests for Ceph Dashboard. You can use Layer 4 TCP with SSL Passthrough or Layer 7 with SSL Offload or SSL Bridging. Using Layer 7 will also allow for flightPATH rules to be used

Sizing the EdgeADC for Ceph Objects

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.

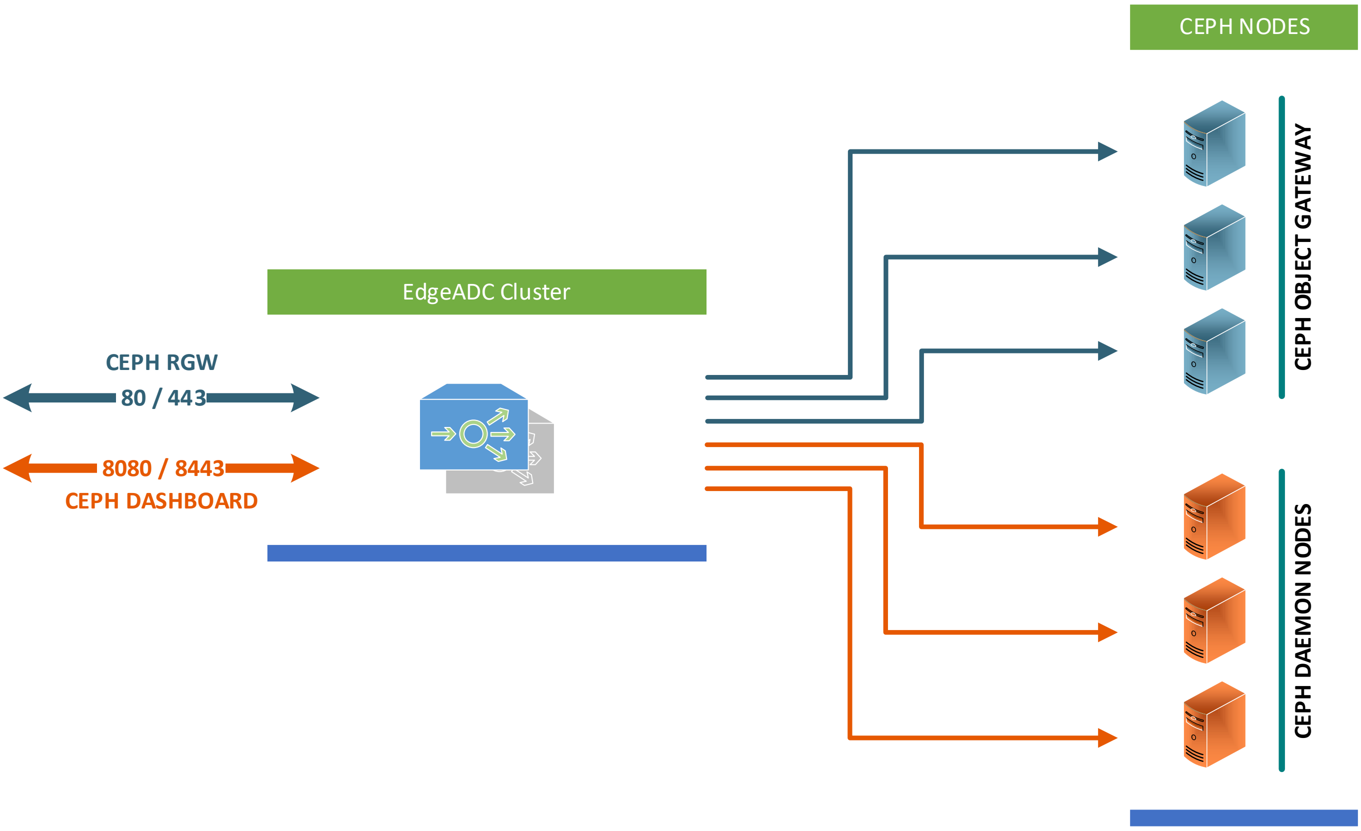
In virtualized environments, we recommend that you set the ADC to 4 vCPU with 8GB RAM, to begin with, and scale up when you need to.

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.

Layer 7 Deployment Scenario

Connections to the Ceph Objects 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 Ceph Objects nodes configured within the ADC and linked to the VIP. An example diagram is shown below.



We will be creating individual VIPs for the different service types as best practices.

The following pages will take you through each of the VIP configurations. Please take care to configure each one correctly to avoid issues in operations.

VIP – Ceph Objects Dashboard

The first VIP and VS we are going to create is the one that handles the Dashboard 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 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
10.10.10.222	255.255.0.0	8443	Ceph Objects Dashboard	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	Weight	Calculated Weight	Notes	ID
10.10.11.100	8443	100	100	Ceph Dashboard 1	1

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

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.11.102	8443	100	100	Ceph Dashboard 2	2

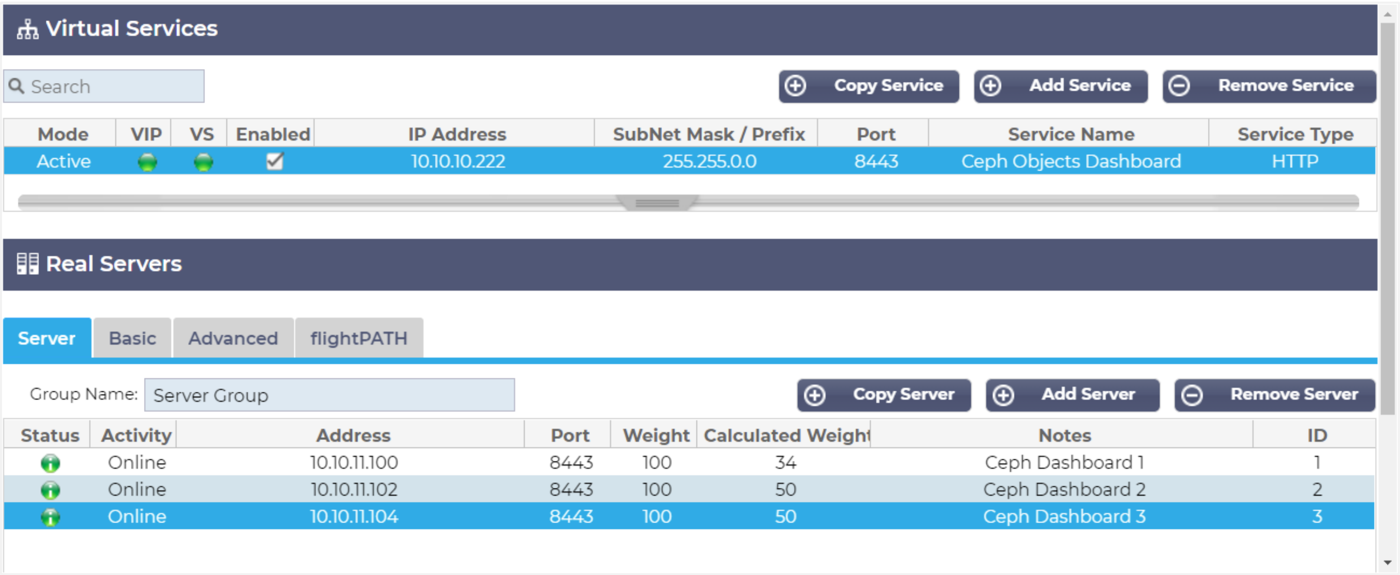
- Click Update to save.
- Click the Copy Server button and make changes for the third node.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.11.104	8443	100	100	Ceph Dashboard 3	3

- 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, and you should see something like this:



Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active	●	●	☑	10.10.10.222	255.255.0.0	8443	Ceph Objects Dashboard	HTTP

Group Name: Server Group

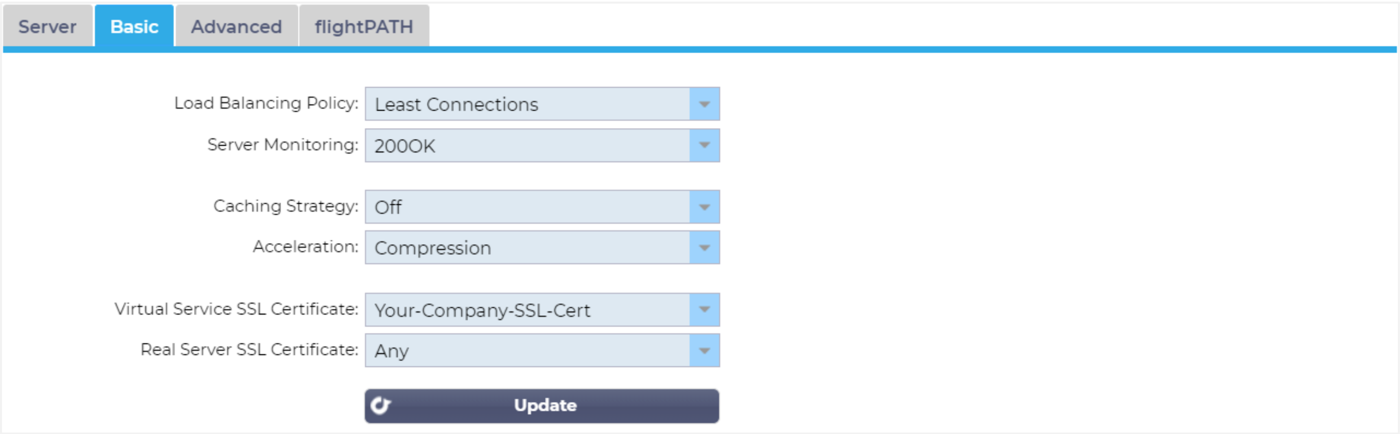
Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
●	Online	10.10.11.100	8443	100	34	Ceph Dashboard 1	1
●	Online	10.10.11.102	8443	100	50	Ceph Dashboard 2	2
●	Online	10.10.11.104	8443	100	50	Ceph Dashboard 3	3

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

You should see something like this:



Load Balancing Policy: Least Connections

Server Monitoring: 200OK

Caching Strategy: Off

Acceleration: Compression

Virtual Service SSL Certificate: Your-Company-SSL-Cert

Real Server SSL Certificate: Any

The above configuration will ensure SSL offload and re-encryption. Should you not require this, we would suggest as follows:

- Use Layer 4 TCP to provide SSL Passthrough. Doing this negates the traffic from being inspected for any security purposes and makes for faster throughput.

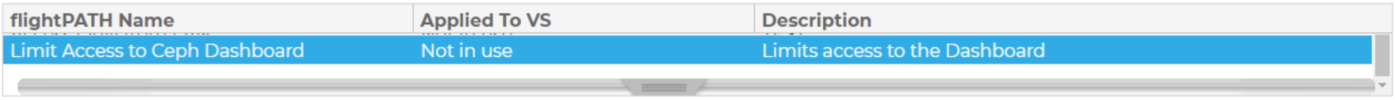
  - Use SSL offload and have your storage nodes use HTTP. To do this, you will need to set the Real Server SSL certificate to NONE.
- Click Update when done.

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

Limiting Access to the Ceph Dashboard

We would advise that you utilize the flightPATH system to limit access to the Ceph Dashboard. It's straightforward to create the flightPATH rule to filter and allow packets depending on the source IP or subnet, or even country, etc.

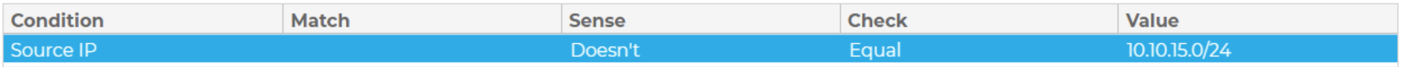
- Click on Library > flightPATH in the Navigation panel
- Click on the Add New button to create a new rule
- In the flightPATH Name field, enter something like Limit Access to Ceph Dashboard.
- In the description field, enter a suitable description.
- Click Update to create the new rule.
- You will see from the "Applied To VS" column that it is not currently in use. When the rule is in use, you will see the VIP details here.



flightPATH Name	Applied To VS	Description
Limit Access to Ceph Dashboard	Not in use	Limits access to the Dashboard

We will now create the condition for the new rule. Here we will specify the Source IP address from where the access is allowed.

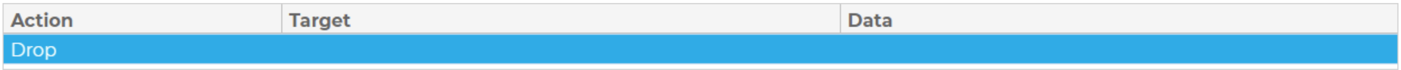
- In the Condition section, click on Add New.
- In the Condition field, select Source IP from the dropdown.
- In the Sense field, select the Doesn't option.
- In the Check field, select Equal.
- In the Value field, specify the Source IP/Subnet from where your access to the Dashboard originates.
- Click Update.



Condition	Match	Sense	Check	Value
Source IP		Doesn't	Equal	10.10.15.0/24

Finally, we will create the Action to be used should the Condition be met.

- In the Action area, click the Add New button
- From the Action field, select Drop.
- Click Update.



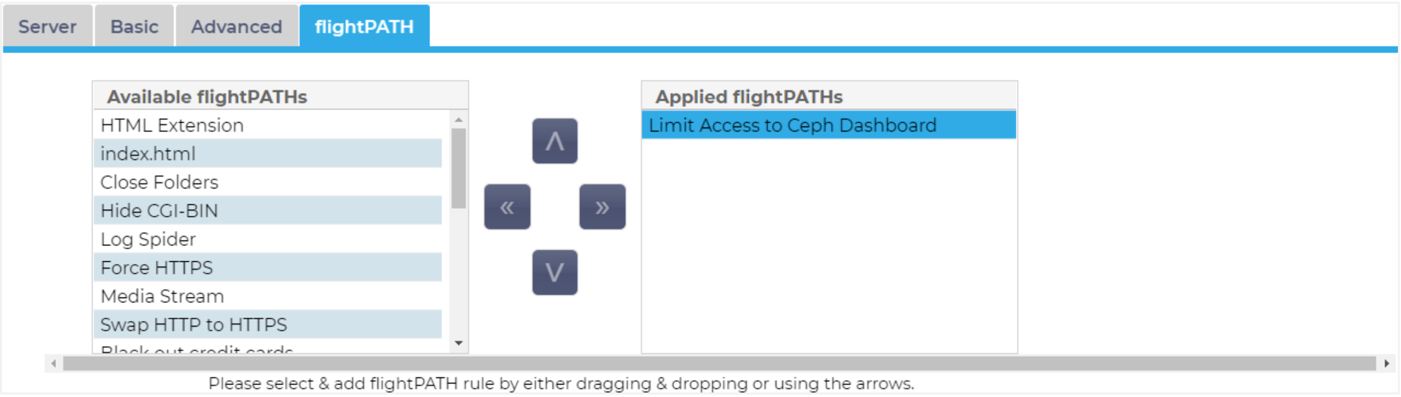
Action	Target	Data
Drop		

The flightPATH rule has been created.

Deploying the flightPATH Rule

To deploy the newly created flightPATH rule, follow the steps below.

- Click on the Ceph Objects Dashboard VIP you created.
- Proceed to the flightPATH tab in the Real Servers section.
- Select *Limit Access to Ceph Dashboard* from the Available flightPATHs section, and click the Right-Arrow button in the central cluster.



- The flightPATH rule is now activated.

Traffic arriving from any IP address other than that specified in the rule will be dropped.

VIP – Ceph RGW

The VIP we are going to create now will handle the client application traffic to the storage nodes. We will be showing the creation of an HTTPS VIP, but the detail for making the HTTP VIP/VS is almost the same.

- 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
10.10.10.122	255.255.0.0	443	Ceph Objects RGW	HTTP

So this has now created the initial VIP with the entry IP address of 10.10.10.122. 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	Weight	Calculated Weight	Notes	ID
10.10.12.100	443	100	100	Ceph RGW 1	1

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

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.12.102	443	100	100	Ceph RGW 2	2

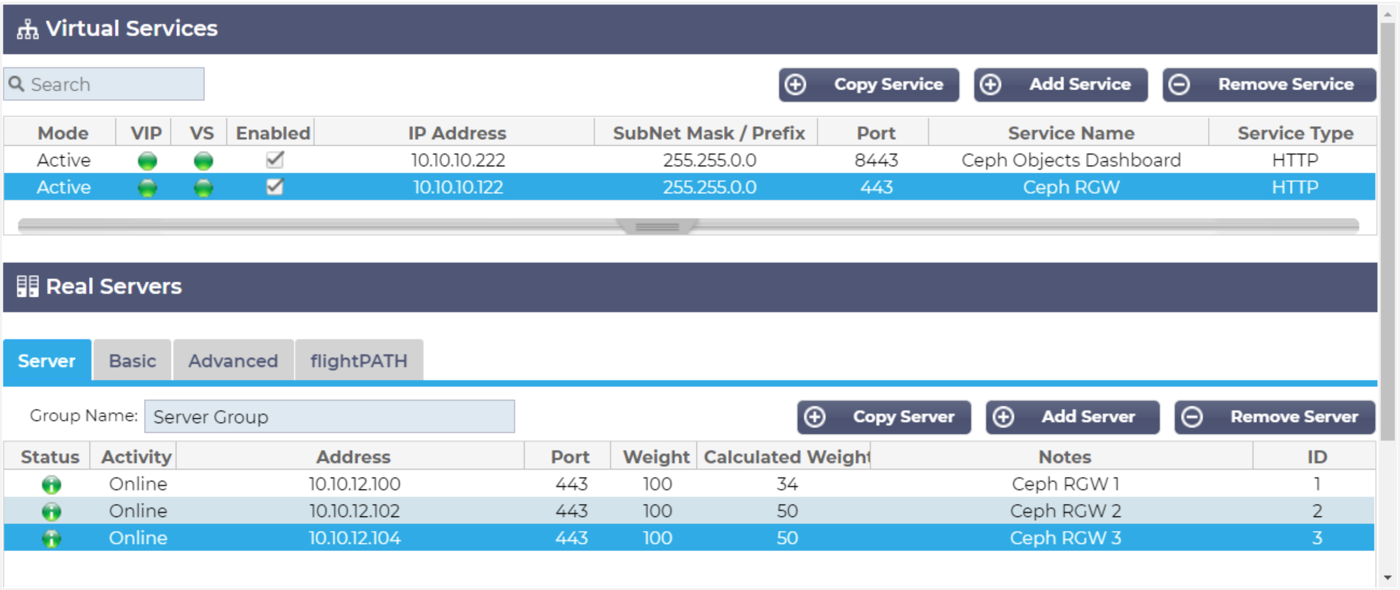
- Click Update to save.
- Click the Copy Server button and make changes for the third node.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.12.104	443	100	100	Ceph RGW 3	3

- 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, and you should see something like this:



Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active	●	●	☑	10.10.10.222	255.255.0.0	8443	Ceph Objects Dashboard	HTTP
Active	●	●	☑	10.10.10.122	255.255.0.0	443	Ceph RGW	HTTP

Group Name: Server Group

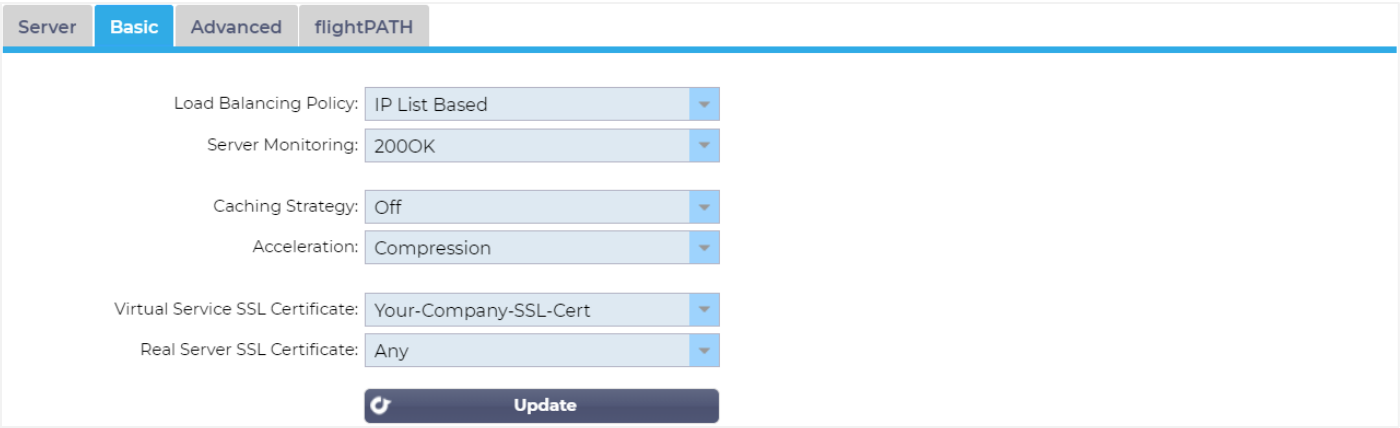
Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
●	Online	10.10.12.100	443	100	34	Ceph RGW 1	1
●	Online	10.10.12.102	443	100	50	Ceph RGW 2	2
●	Online	10.10.12.104	443	100	50	Ceph RGW 3	3

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	Off
Acceleration	Compression
Virtual Service SSL Cert	Your SSL certificate
Real Server SSL Cert	Any

You should see something like this:



Load Balancing Policy: IP List Based
Server Monitoring: 200OK
Caching Strategy: Off
Acceleration: Compression
Virtual Service SSL Certificate: Your-Company-SSL-Cert
Real Server SSL Certificate: Any

The above configuration will ensure SSL offload and re-encryption. Should you not require this, we would suggest as follows:

- Use Layer 4 TCP to provide SSL Passthrough. Doing this negates the traffic from being inspected for any security purposes and makes for faster throughput.

   - Use SSL offload and have your storage nodes use HTTP. To do this, you will need to set the Real Server SSL certificate to NONE.
- Click Update when done.

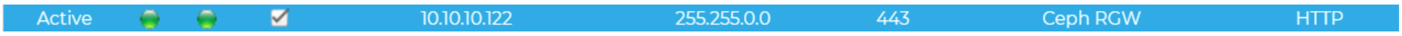
There are no configurations to be done within the Advanced tab.

We will now create a rule to move traffic from HTTP (80) to HTTPS (443) automatically using flightPATH.

Creating the HTTP Redirector VIP

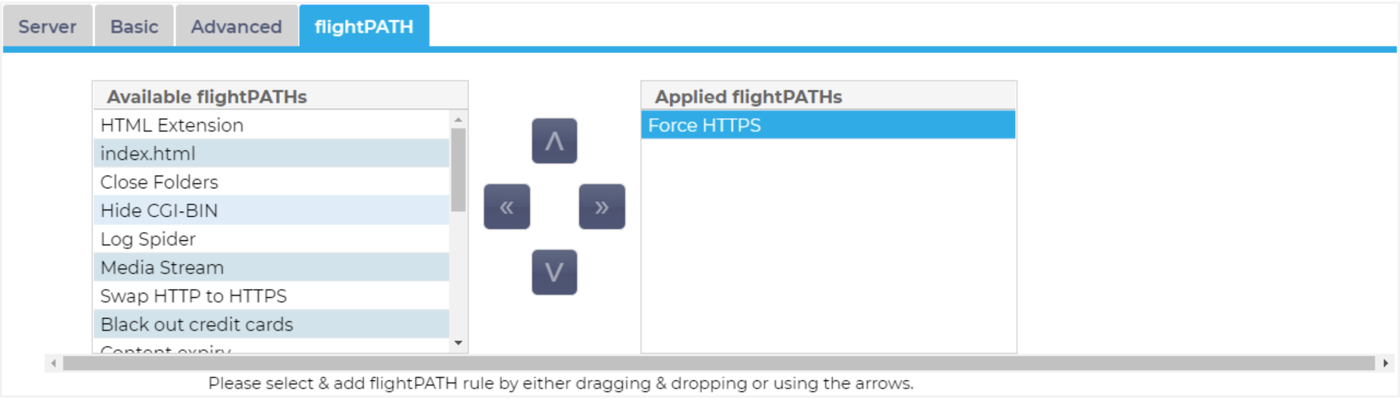
If your corporate IT rules dictate that all connections must be secure, you will need to create a redirector VIP. To do this, follow the procedure below:

- Click on the Ceph RGW VIP you just created



Active	●	●	☑	10.10.10.122	255.255.0.0	443	Ceph RGW	HTTP

- Click the Copy Service button
- A copy of the service is created, and you will be placed in edit mode.
- Change the port to 80, change the Service Name to 80 to 443 Redirector, and click Update
- Now go to the flightPATH tab in the Real Servers section.
- Select Force HTTPS and click the Right-Arrow button in the central cluster.



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

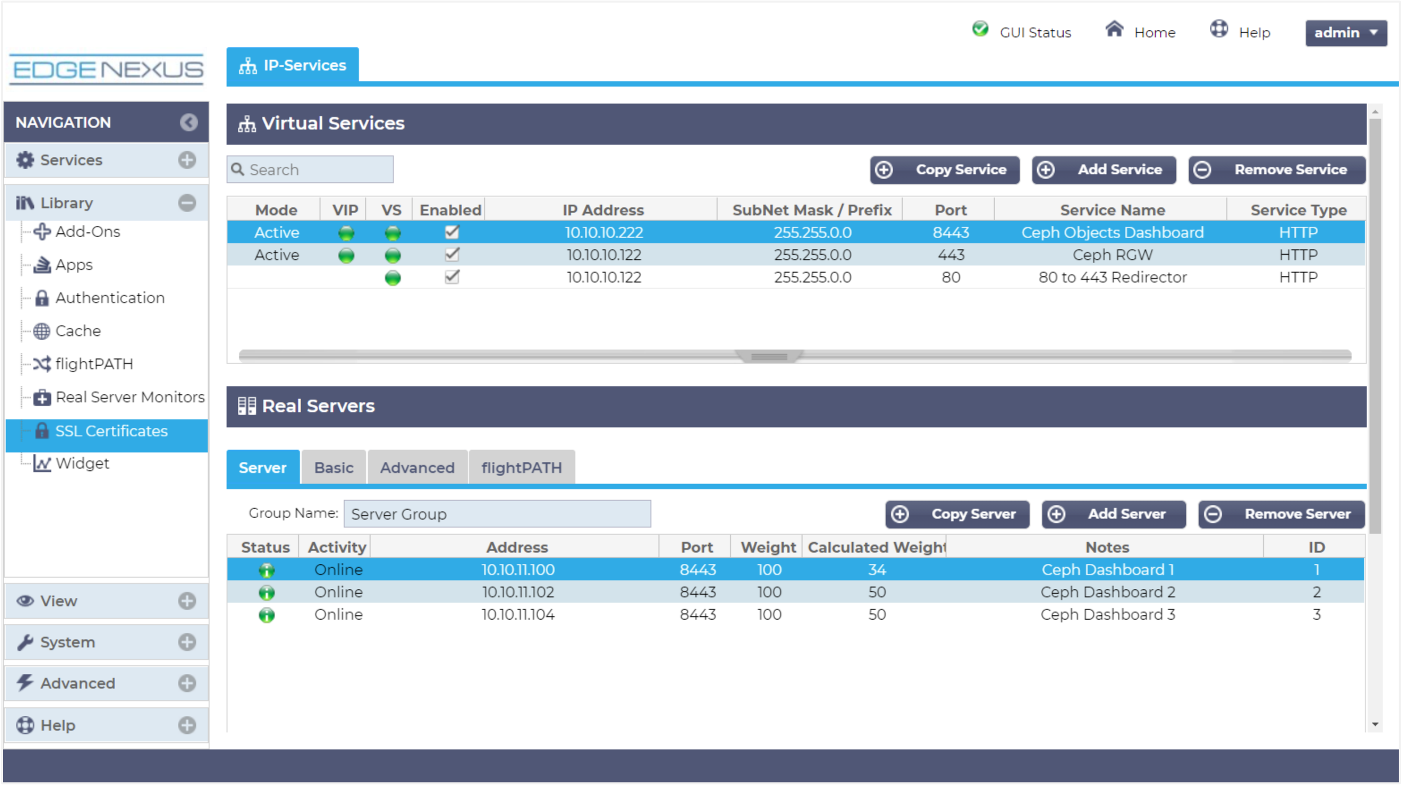
Applied flightPATHs
- Force HTTPS

Please select & add flightPATH rule by either dragging & dropping or using the arrows.

The flightPATH rule is now activated, and all traffic entering the VIP on port 80 will be switched to use the 443 based VIP.

Ceph Objects Layer 7 Summary

The Layer 7 traffic load balancing configurations are now complete, and the ADC should look something like the example below.



Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active	●	●	☑	10.10.10.222	255.255.0.0	8443	Ceph Objects Dashboard	HTTP
Active	●	●	☑	10.10.10.122	255.255.0.0	443	Ceph RGW	HTTP
		●	☑	10.10.10.122	255.255.0.0	80	80 to 443 Redirector	HTTP

Group Name: Server Group

Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
●	Online	10.10.11.100	8443	100	34	Ceph Dashboard 1	1
●	Online	10.10.11.102	8443	100	50	Ceph Dashboard 2	2
●	Online	10.10.11.104	8443	100	50	Ceph Dashboard 3	3

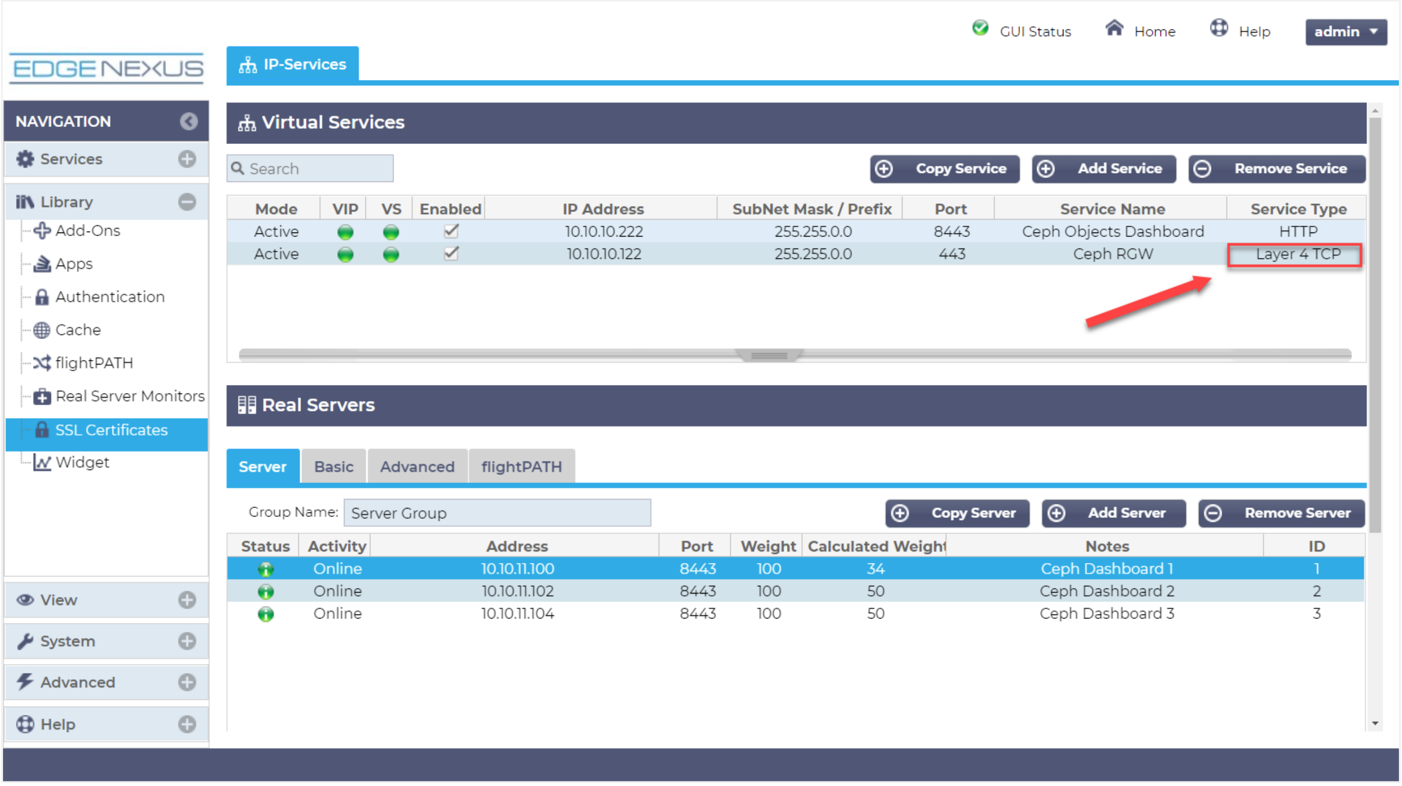
Using TCP Layer 4 Passthrough

The reverse proxy engine within the EdgeADC is an exceptionally high-speed solution built for high-speed transactional environments. However, you may not want to decrypt, inspect and then re-encrypt the SSL data stream. We would recommend you switch to Layer 4 TCP load balancing with Reverse Proxy in such cases.

The configuration of the EdgeADC for Layer 4 Passthrough is very similar to the Layer 7 method. There are essentially one field that needs changing.

- Service Type – for each virtual service defined, and should be changed to Layer 4 TCP.
- 80 to 443 Redirector Service – is no longer required as you cannot use flightPATH with Layer 4 TCP load balancing.
- flightPATH - rule does not need to be configured.

Please see the screenshots below.



Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active	●	●	✓	10.10.10.222	255.255.0.0	8443	Ceph Objects Dashboard	HTTP
Active	●	●	✓	10.10.10.122	255.255.0.0	443	Ceph RGW	Layer 4 TCP

Group Name: Server Group

Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
●	Online	10.10.11.100	8443	100	34	Ceph Dashboard 1	1
●	Online	10.10.11.102	8443	100	50	Ceph Dashboard 2	2
●	Online	10.10.11.104	8443	100	50	Ceph Dashboard 3	3

You will note that we have kept the Dashboard VIP on Layer 7 HTTP. The reason for this is that you may wish to use flightPATH based filtering to limit access to the VIP by country, or Source IP, or even a series of subnets based using RegEx.