CLOUDIAN HYPERSTORE

AN EDGENEXUS ADC DEPLOYMENT GUIDE

EDGE NEXUS

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

Cloudian HyperStore is one of the leading object-based storage solutions on the market that uses Amazon S3 as its specialist foundation. Cloudian's revolutionary technology means businesses small, large, and very large can take advantage of object-based storage in their data centers or cloud located S3 using the native Amazon S3-API.

High availability is supported in Cloudian 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 Cloudian HyperStore, and this guide explains how to set this up.

Document Intention

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

The quickest way to do this is to use the Cloudian HyperStore jetPACK, in which we have done all the work for you. However, we will also show each item that is configured, so you have a better understanding.

VIPs, Ports, and Other Bits

When load balancing Cloudian HyperStore, the following VIPs will be needed for Cloudian operations.

HTTP VIP Services

- S3 (HTTP) for handling HTTP requests from S3 client applications
- IAM (HTTP) for the identity and access management
- CMC (HTTP) for Cloudian management console requests

HTTPS VIP Services

- S3 (HTTPS) for handling HTTPS requests from S3 client applications
- IAM (HTTPS) for secure identity and access management
- CMC (HTTPS) for secure Cloudian management console requests
- API (HTTPS) for all API requests

Note: The IAM VIP services outlined above are optional for Cloudian HyperStore v7.1x or earlier but are mandatory for later versions (v7.2 and above).

Port Requirements

The following are the port requirements for the Cloudian HyperStore platform.

Port	Protocol	Service Type	Explanation
80	TCP	L4-TCP or L7 HTTP	This port is used to handle all HTTP requests from S3 client applications. You can use Layer 4 TCP with SSL Passthrough or Layer 7 with SSL Offload or SSL Bridging.
8888	TCP	L4-TCP or L7 HTTP	Port used to handle un-secured requests from clients (CMC). You can use Layer 4 TCP with SSL Passthrough or Layer 7 with SSL Offload or SSL Bridging.
16080	TCP	L4-TCP or L7 HTTP	Port used to handle unsecured IAM services traffic. 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 S3 client applications. You can use Layer 4 TCP with SSL Passthrough or Layer 7 with SSL Offload or SSL Bridging.
8443	TCP	L4-TCP or L7 HTTPS	It is used to handle SSL secured requests from clients (CMC). You can use Layer 4 TCP with SSL Passthrough or Layer 7 with SSL Offload or SSL Bridging.
16443	TCP	L4-TCP or L7 HTTPS	Port used to handle secured SSL IAM service traffic. You can use Layer 4 TCP with SSL Passthrough or Layer 7 with SSL Offload or SSL Bridging.
19443	TCP	L4-TCP or L7 HTTPS	This port is used to handle the admin requests to the Cloudian API. You can use Layer 4 TCP with SSL Passthrough or Layer 7 with SSL Offload or SSL Bridging.

Sizing the EdgeADC for Cloudian

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.

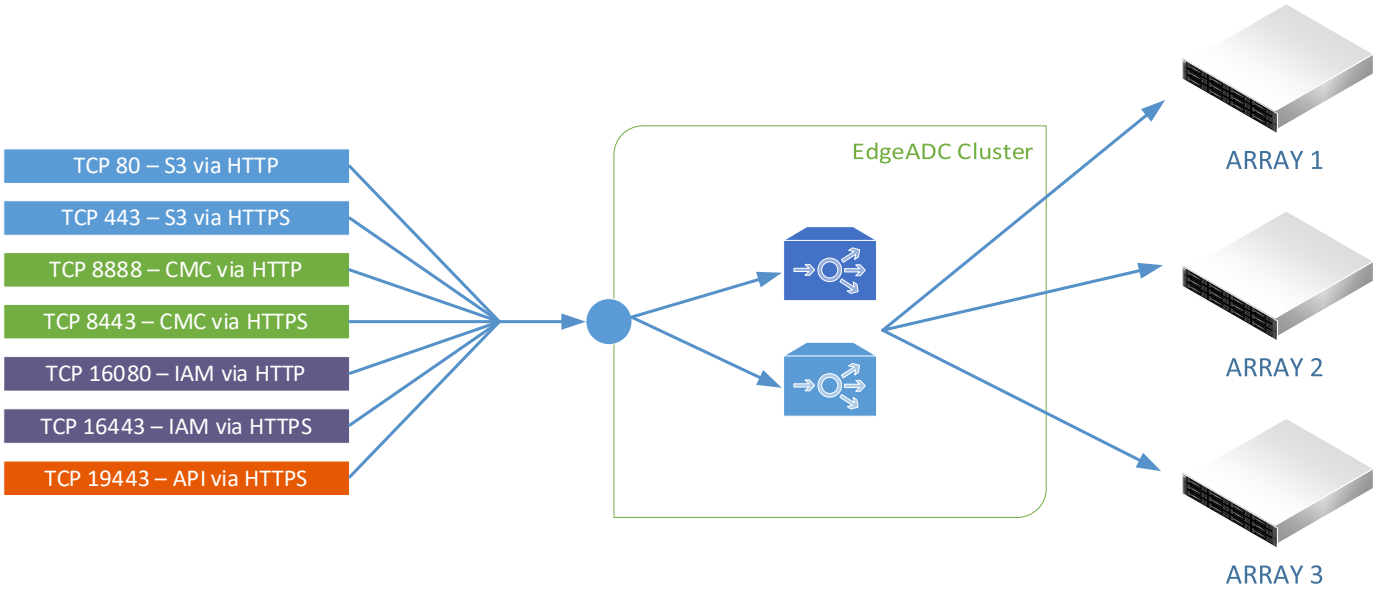
In virtualized environments, we recommend that you set the ADC to 4 vCPU with 8GB RAM, to begin with, and scale up when you need to.

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 Cloudian HyperStore 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 Cloudian 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.

Creating the Cloudian Real Server Monitors

A vital requirement within the ADC infrastructure for Cloudian, and indeed for many other installations, is the definition of real server monitors that will check on the back-end nodes' health and then use the data to determine if traffic should be sent to them.

- Navigate to Library > Real Server Monitors using the navigation pane.
- Click Add Monitor.
- A new blank entry will be created.
- Create the monitors using the guides below.

Cloudian Management Console (CMC)

Name	Description	Monitoring Method	Page Location	Required Content	User	Password
Cloudian-CMC	As needed	HTTP 200OK	/Cloudian/login.html	200 OK	Username	Password

Cloudian S3

Name	Description	Monitoring Method	Page Location	Required Content	User	Password
Cloudian-S3	As needed	HTTP 200OK	/.healthcheck	200 OK	Username	Password

Cloudian API

IMPORTANT

For Cloudian HyperStore systems starting from version 7.22 and later, the ***sysadmin*** password is randomly generated, and you will need to perform the following steps to obtain it.

a. Connect to the HyperStore Puppet Master node as ***root*** or ***sa_admin*** if the root access is disabled.
b. Execute the following commands to retrieve the password for ***sysadmin***.

```
[root@hs1 7.2.x]# hsctl config get admin.auth
{
"base64": "c3lzYWRtaW46SWxp4yeg7jFtaW5nb3MuVGhleSdyZV9uJ8tF5yu=",
"password": "CQA4xFerdMUn8lvoZrbBC6HZ5[D=",
"password": "H8GHY9he7knYHJuohtyen[bleie8 =",
"username": "sysadmin"
}
```

c. Copy the password as you will need to enter it into the monitor you will create for the API VS.

Name	Description	Monitoring Method	Page Location	Required Content	User	Password
Cloudian-API	As needed	HTTP 200OK	/.healthcheck	200 OK	sysadmin	Password

Cloudian IAM *

The monitor for the Cloudian IAM service does not need to be created as it is already defined in the Server Monitoring field of the Basic tab for that service.

Name	Description	Monitoring Method	Page Location	Required Content	User	Password
Cloudian-IAM	As needed	TCP Connect *				

* You can find this in IP Services > Basic Tab > Server Monitoring

VIP – Cloudian Management Console (CMC)

The first VIP and VS we are going to create is the one that handles the CMC 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
192.168.1.222	255.255.255.0	8443	CMC Cloudian	HTTP

So this has now created the initial VIP with the entry IP address of 192.168.1.222. 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 two array nodes, but you may have more.

Address	Port	Weight	Calculated Weight	Notes	ID
192.168.1.201	8443	100	100	Array Node 1	

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

Address	Port	Weight	Calculated Weight	Notes	ID
192.168.1.202	8443	100	100	Array Node 2	

- 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 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	Cloudian-CMC
Caching Strategy	Off
Acceleration	Compression
Virtual Service SSL Cert	Your SSL certificate
Real Server SSL Cert	Your SSL Certificate

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 reasons.
  - Use SSL offload and have your storage nodes use HTTP. To do this, you will need to set the Real Server SSL certificate to ANY.
- Click Update when done.

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

VS – S3 Client Application (S3)

The VS we are going to create is the one that handles the S3 client application traffic. We will be showing the creation of an HTTPS VIP, but the detail for making the HTTP VIP/VS is almost the same.

- Click on the CMC VIP you had created earlier.
- Click Copy Service
- A new VS row will be created, and the Real Servers (RS) copied for this new VS. The field values we provide are examples for your guidance.

IP Address	Subnet Mask	Port	Service Name	Service Type
192.168.1.222	255.255.255.0	443	Cloudian S3 C-APP	HTTP

Now that you have created the new VS, you will need to alter the Real Servers allocated to this service.

- Click on the Servers tab to display the Real Servers listing.
- The previously created servers are there, but their port entries will be wrong and must be changed.

Address	Port	Weight	Calculated Weight	Notes	ID
192.168.1.201	443	100	100	Array Node 1	
192.168.1.202	443	100	100	Array Node 2	

- Click Update to save.

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	Cloudian-S3
Caching Strategy	Off
Acceleration	Compression
Virtual Service SSL Cert	Your SSL certificate
Real Server SSL Cert	Your SSL Certificate

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 reasons.
    - Use SSL offload and have your storage nodes use HTTP. To do this, you will need to set the Real Server SSL certificate to ANY.
- Click Update when done.

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

VS – Administration API Requests (API)

The VS we are going to create is the one that handles the API administration traffic requests. We will be showing the creation of an HTTPS VIP, but the detail for making the HTTP VIP/VS is almost the same.

- Click on the S3 VIP you had created earlier.
- Click Copy Service
- A new VS row will be created, and the Real Servers (RS) copied for this new VS. The field values we provide are examples for your guidance.

IP Address	Subnet Mask	Port	Service Name	Service Type
192.168.1.222	255.255.255.0	19443	Cloudian API	HTTP

Now that you have created the new VS, you will need to alter the Real Servers allocated to this service.

- Click on the Servers tab to display the Real Servers listing.
- The previously created servers are there, but their port entries will be wrong and must be changed.

Address	Port	Weight	Calculated Weight	Notes	ID
192.168.1.201	19443	100	100	Array Node 1	
192.168.1.202	19443	100	100	Array Node 2	

- Click Update to save.

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	Cloudian-API
Caching Strategy	Off
Acceleration	Compression
Virtual Service SSL Cert	Your SSL certificate
Real Server SSL Cert	Your SSL Certificate

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 reasons.
    - Use SSL offload and have your storage nodes use HTTP. To do this, you will need to set the Real Server SSL certificate to ANY.
- Click Update when done.

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

VS – Identity and Access Management (IAM)

The VS we are going to create is the one that handles the API administration traffic requests. We will be showing the creation of an HTTPS VIP, but the detail for making the HTTP VIP/VS is almost the same.

*IMPORTANT – This VIP/VS is optional for Cloudian HyperStore versions 7.1.x and earlier. It is **mandatory** for versions 7.2x and later.*

- Click on the S3 VIP you had created earlier.
- Click Copy Service
- A new VS row will be created, and the Real Servers (RS) copied for this new VS. The field values we provide are examples for your guidance.

IP Address	Subnet Mask	Port	Service Name	Service Type
192.168.1.222	255.255.255.0	16443	Cloudian IAM	HTTP

Now that you have created the new VS, you will need to alter the Real Servers allocated to this service.

- Click on the Servers tab to display the Real Servers listing.
- The previously created servers are there, but their port entries will be wrong and must be changed.

Address	Port	Weight	Calculated Weight	Notes	ID
192.168.1.201	16443	100	100	Array Node 1	
192.168.1.202	16443	100	100	Array Node 2	

- Click Update to save.

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	Compression
Virtual Service SSL Cert	Your SSL certificate
Real Server SSL Cert	Your SSL Certificate

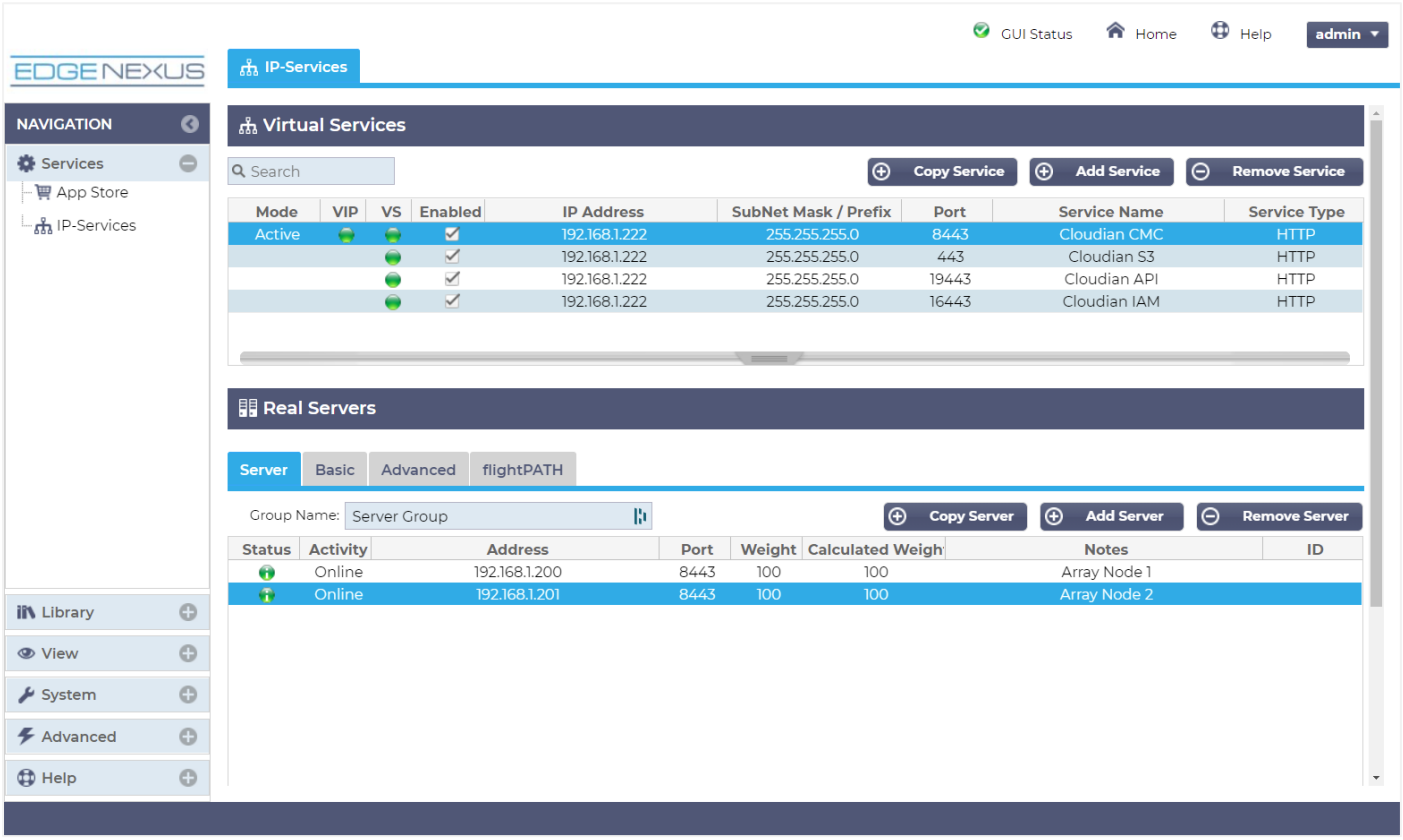
The above configuration will ensure SSL offload and re-encryption. Should you not require this, we would suggest as follows:

    - Use Layer 4 TCP to provide SSL Passthrough. Doing this negates the traffic from being inspected for any security reasons.
    - Use SSL offload and have your storage nodes use HTTP. To do this, you will need to set the Real Server SSL certificate to ANY.
- Click Update when done.

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

Layer 7 Summary

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

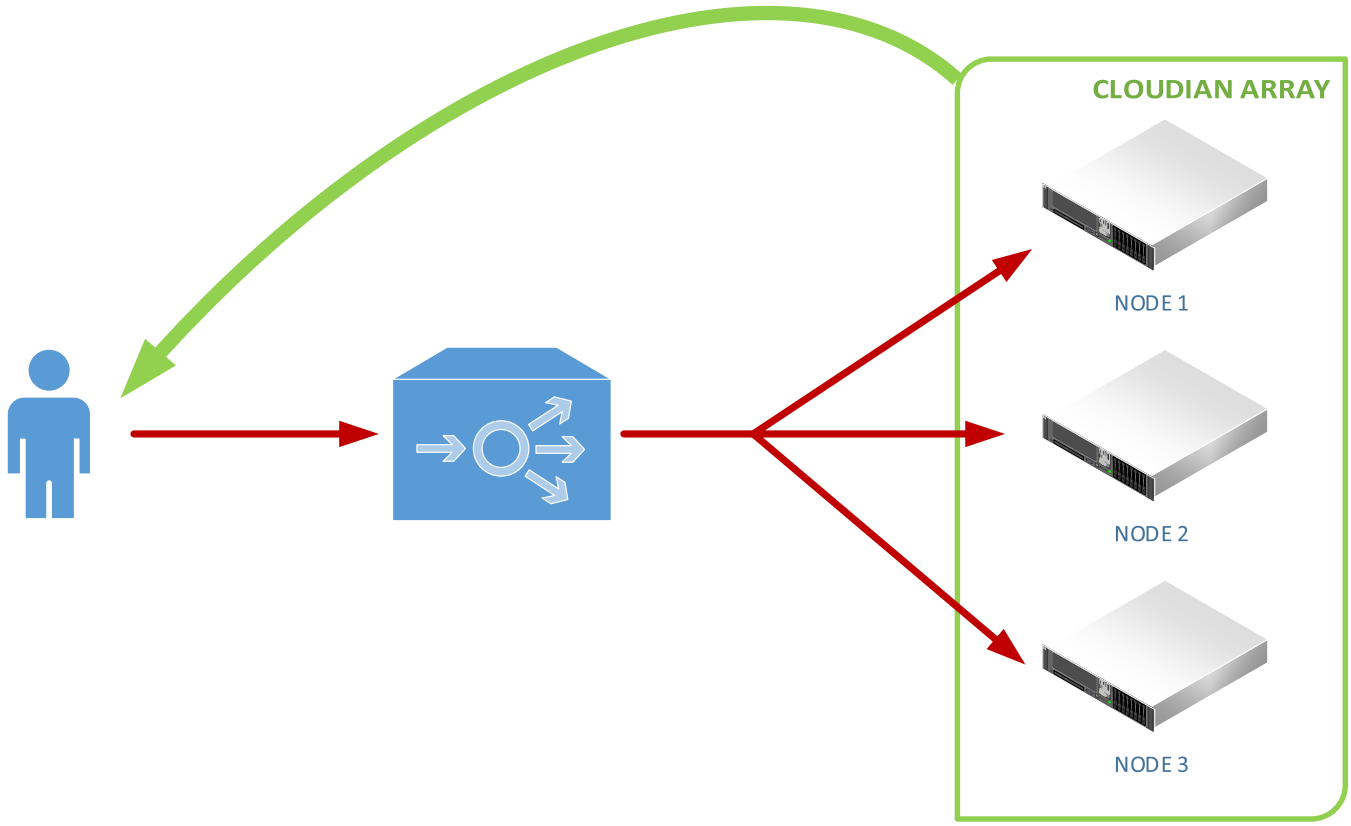


High-Speed Transactions and Layer 4 with DSR

The reverse proxy within the EdgeADC is an exceptionally high speed and has been built for high-speed transactional environments. However, there may be occasions when your needs demand even higher throughputs, and in such cases, we would recommend you switch to Layer 4 TCP load balancing, with Direct Server Return rather than Reverse Proxy.

DSR or Direct Server Return is often used when the Request is small, but the Request-Reply is large. Examples could include large image files, video playback and streaming, and large data file retrieval. In such cases, the traversal of data through the Reverse Proxy would probably delay its return to the originator, and passing it directly to the source is highly advantageous.

An example of DSR is shown in the illustration below.



In the example shown, the Request traverses through the EdgeADC and is distributed to the Cloudian nodes using the load balancing policy.

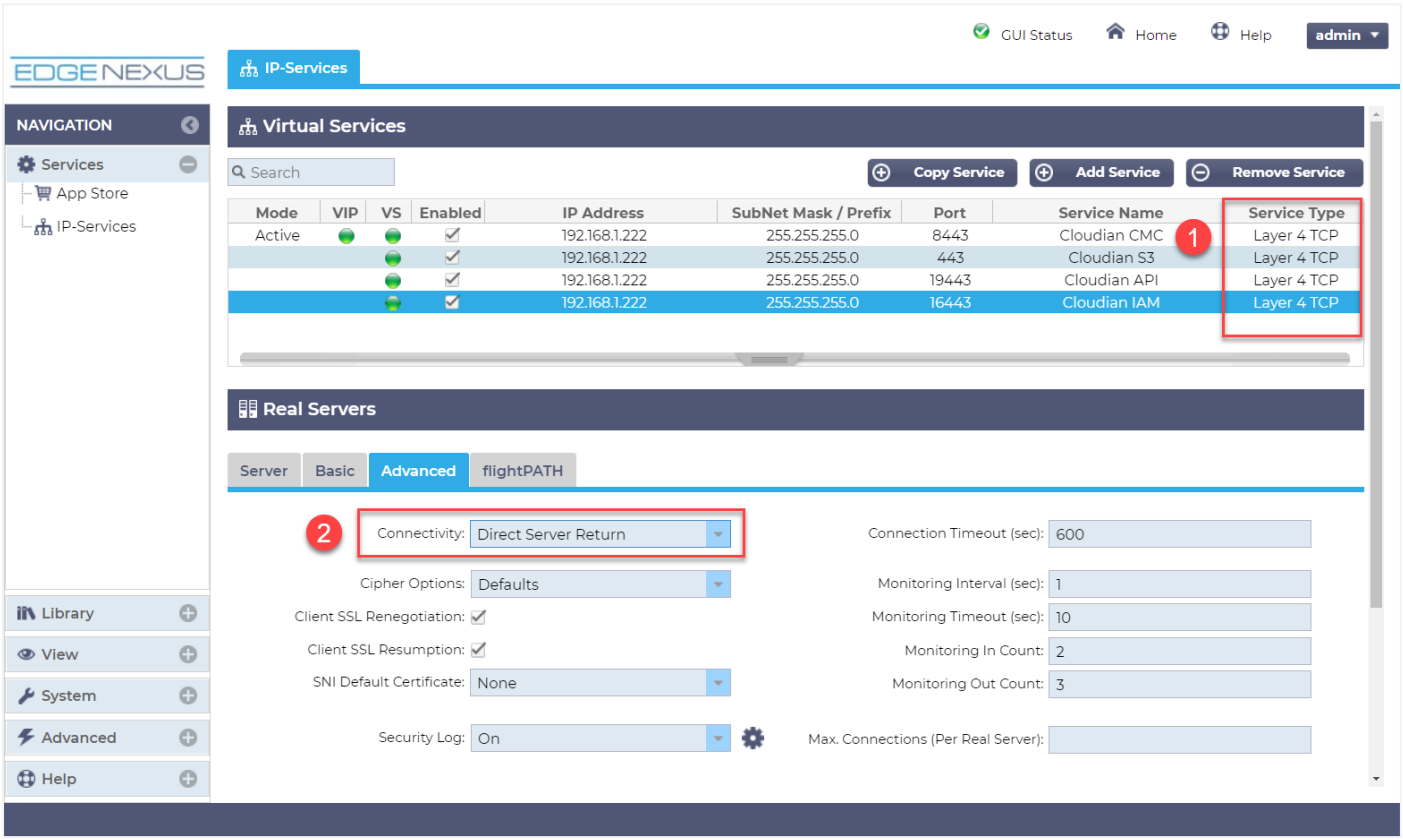
When the Request-Reply is sent back to the user, it bypasses the EdgeADC and is returned directly to the user, a Direct Server Return, or DSR.

Configuring the EdgeADC Layer 4 DSR for Cloudian

The configuration of the EdgeADC for Layer 4 and Direct Server Return is very similar to the Layer 7 method. There are essentially two fields that need changing.

- Service Type – for each virtual service defined, and should be changed to Layer 4 TCP.
- Connectivity – This is found under Real Servers > Advanced > Connectivity and should be changed to Direct Server Return. This change needs to be done for EACH VIP.

Please see the screenshots below.



VERY IMPORTANT

For Direct Server Return to work, the following **mandatory conditions must be met.**

a. The EdgeADC and the Cloudian Nodes must be on the same network segment / switching fabric. This requirement is due to the load balancing method working by rewriting MAC ID by operating at Layer 2 of OSI.
b. Each Cloudian HyperStore node must take ownership of the VIP address so they can all accept requests and send back responses. The address will need to be assigned to a loopback adapter.
c. Each Cloudian HyperStore node must be configured to not respond to ARP requests for the VIP address or advertise they own the VIP address.