NFMS Server And Network Standard Operating Procedure

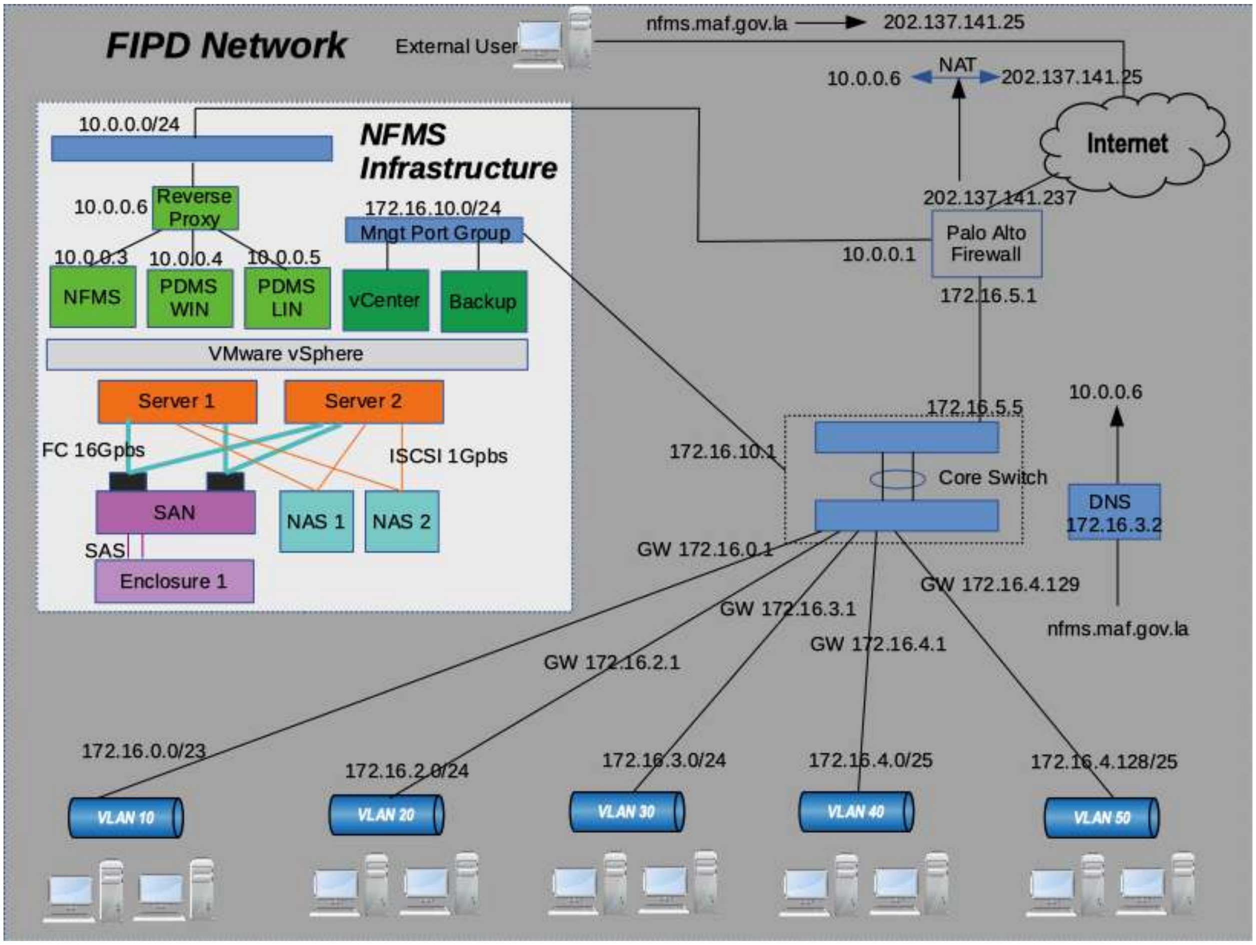
Table of Contents

1 Infrastructure Overview

NFMS infrastructure is hosted inside FIPD network, various network equipment and technologies have been implemented to secure and enhance capabilities of the infrastructure, which will be explained later in the following articles in this document.

1.1 FIPD Network

Diagram below illustrates overall picture of FIPD Network:



- Data flow – External users requesting nfms.maf.gov.la:
  1. External users open their browser and request for nfms.maf.gov.la
  2. Domain registrar translate nfms.maf.gov.la to IP 202.137.141.25
  3. ISPs route traffic looking for 202.137.141.25
  4. Request reach our Palo Alto Firewall
  5. Our firewall translate 202.137.141.25 to 192.168.155.3
  6. Request traffic looking for 192.168.155.3
  7. Request reach WAF

8. WAF translate 192.168.155.3 to 10.0.0.6 (Reverse proxy)
9. Request traffic looking for 10.0.0.6
10. Request reach Reverse proxy
11. Finally reverse proxy forward the traffic to NFMS servers (based on URL/Serveice requested)
12. NFMS servers return response

- Data flow – Users in FIPD Network requesting nfms.maf.gov.la:
  1. Internal users open their browser and request for nfms.maf.gov.la
  2. FIPD Internal DNS translate nfms.maf.gov.la to IP 192.168.155.3
  3. Request traffic looking for 192.168.155.3
  4. Request reach WAF
  5. WAF translate 192.168.155.3 to 10.0.0.6 (Reverse proxy)
  6. Request traffic looking for 10.0.0.6
  7. Request reach Reverse proxy
  8. Finally reverse proxy forward the traffic to NFMS servers (based on URL/Serveice requested)
  9. NFMS servers return response

1.2 NFMS Servers and Network Infrastructure

As illustrated in the diagram above, NFMS servers and network infrastructure is now a virtual machine infrastructure powered by VMware vSphere and the underlying hardware.

- Hardware Layer:
  - Servers:
    2 Servers acts as a cluster providing high availability services and serves as compute resources (CPU and Memory) for virtual machines, each server providing 16 physical CPU cores or 32 logical CPU cores and 128GB of RAM.

  - SAN Storage:
    SAN Storage serves as a main data storage for virtual machines and their data, this storage is block level storage and supports 15Krpm HDDs and the connection to servers is Fiber Channel 16Gbps, the storage in our setup (colored purple in the diagram) consists of one main unit and one enclosure unit, total usable capacity of 15TB (after raid configuration) detailed configurations will be explained in 4.1 (SAN Configurations).

  - NAS Storage:
    2 x NAS Storage servers as a secondary storage used for backup and archive purpose, this storage support 7.2Krpm HDD and connection to servers is iSCSI 1Gpbs per network port, the storage in our setup (colored light blue in the diagram) consists of two NAS units, total usable capacity of 40TB (after raid configuration) detailed configurations will be explained in 4.2 (NAS configurations).

For detailed information about hardware specification see article “3 NFMS Hardware”

- Software/Hypervisor Layer:
  VMware vSphere or ESXi is selected as hypervisor layer, works as a conjunction point between Virtual Machines and Hardware resources. Virtual Machine requesting for resources from hardware through hypervisor layer.
- Virtual Machine Layer:
  Virtual Machine (VM) is a virtual computer or server, guess operating system of your choice is installed and providing services to end users. Making it’s possible to create multiple VMs running on single physical server and possible to move VMs across multiple ESXi hosts, providing flexibility and high-availability.

2 NFMS Hardware Monitoring

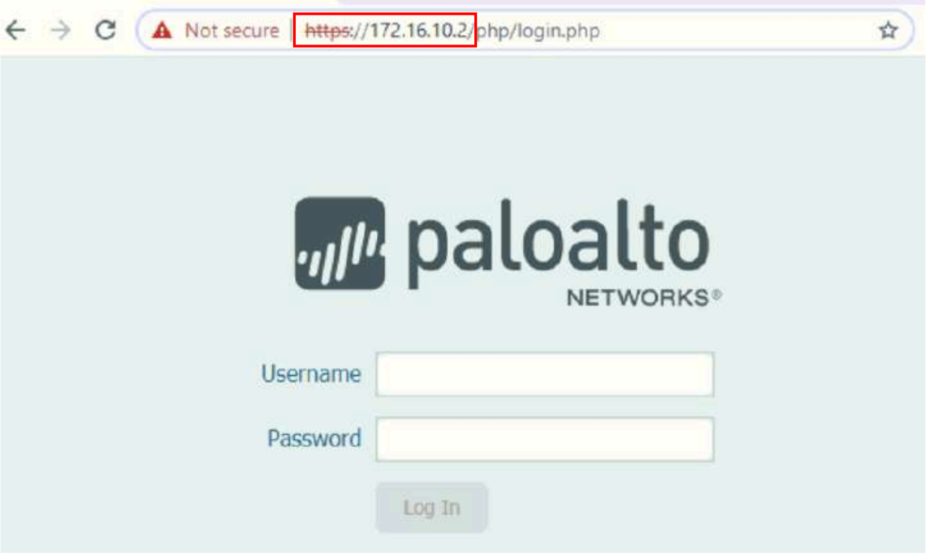
2.1 Physical Monitoring

- Observe physical condition and check for led/error indicator of servers, storage, firewall, switches, hard disks, power supply, power connectors, UPS…
  If hardware error found arrange for replacement with spare parts or contact vendors for support. (daily or at least weekly).
- vacuum cleaning server room and outside of all equipment (Monthly)

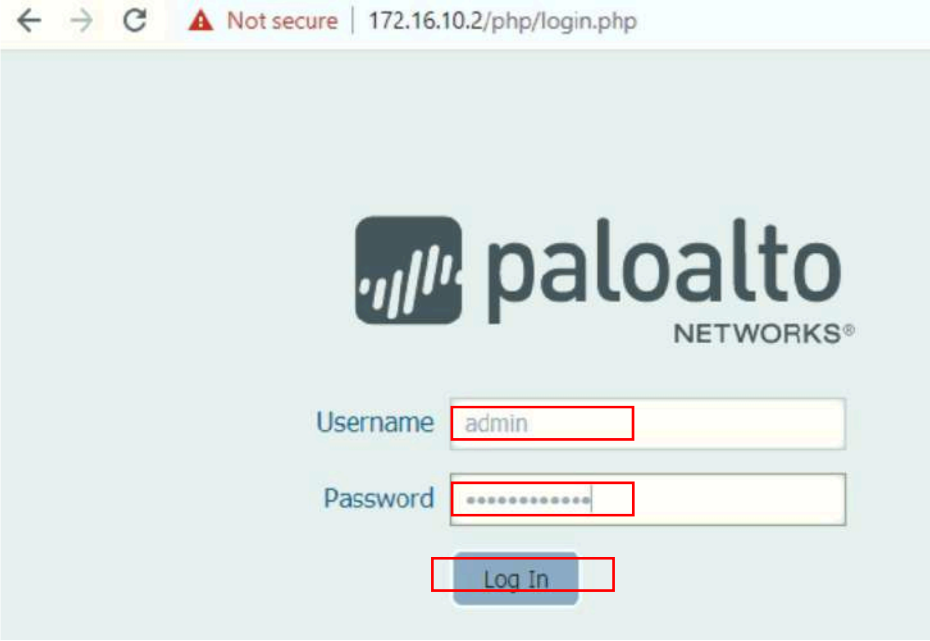
3 NFMS Network

3.1 Firewall Palo Alto PA-2200

- Monitor Firewall (Weekly)
  The firewall is configured to allow access only on management interface, meaning access request must be initiated only from FIPD Vlans (DMZ and Outside networks are not allow). To access web interface of the firewall first you need to login to a computer inside FIPD Vlans then open your web browser and fill in the address bar with this link https://172.16.10.2 you’ll be redirected to login page as below:



Fill in login credentials and click login

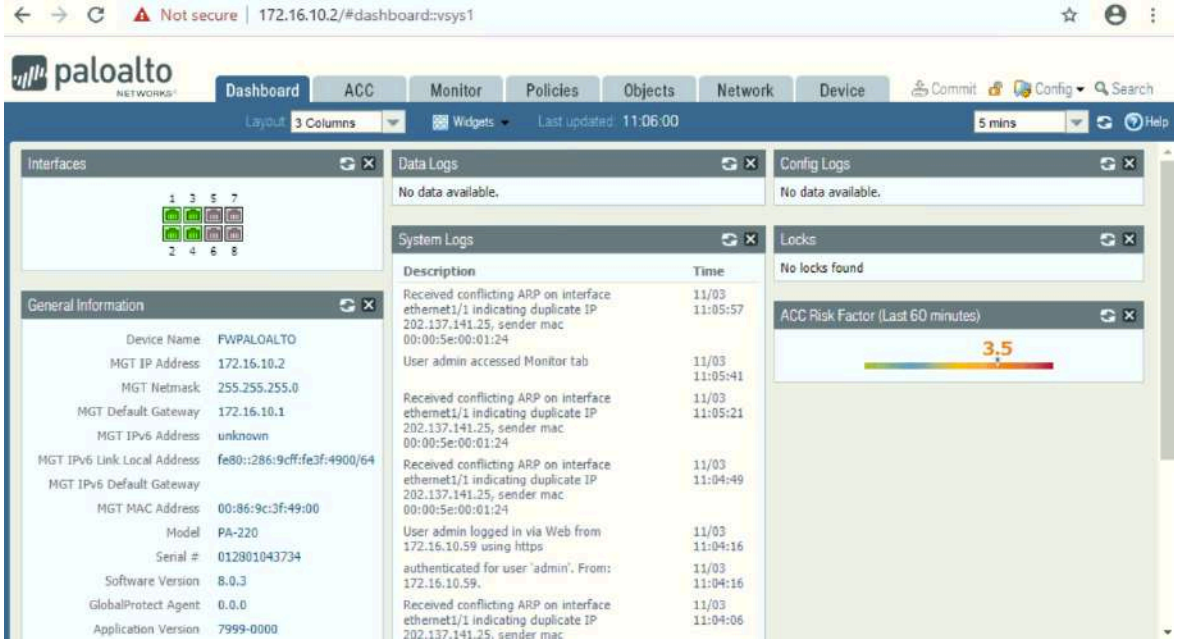


Not secure | 172.16.10.2/php/login.php

Username: admin

Password: ••••••••••••

That’s all, you’re now inside the web management interface as below:



Not secure | 172.16.10.2/#dashboard::vsys1

Layout: 3 Columns

Last updated: 11:06:00

5 mins

General Information

Device Name	FWPALOALTO
MGT IP Address	172.16.10.2
MGT Netmask	255.255.255.0
MGT Default Gateway	172.16.10.1
MGT IPv6 Address	unknown
MGT IPv6 Link Local Address	fe80::286:9cff:fe3f:4900/64
MGT IPv6 Default Gateway	
MGT MAC Address	00:86:9c:3f:49:00
Model	PA-220
Serial #	012801043734
Software Version	8.0.3
GlobalProtect Agent	0.0.0
Application Version	7999-0000

Data Logs

No data available.

System Logs

Description	Time
Received conflicting ARP on interface ethernet1/1 indicating duplicate IP 202.137.141.25, sender mac 00:00:5e:00:01:24	11/03 11:05:57
User admin accessed Monitor tab	11/03 11:05:41
Received conflicting ARP on interface ethernet1/1 indicating duplicate IP 202.137.141.25, sender mac 00:00:5e:00:01:24	11/03 11:05:21
Received conflicting ARP on interface ethernet1/1 indicating duplicate IP 202.137.141.25, sender mac 00:00:5e:00:01:24	11/03 11:04:49
User admin logged in via Web from 172.16.10.59 using https	11/03 11:04:16
authenticated for user 'admin'. From: 172.16.10.59.	11/03 11:04:16
Received conflicting ARP on interface ethernet1/1 indicating duplicate IP 202.137.141.25, sender mac	11/03 11:04:06

Config Logs

No data available.

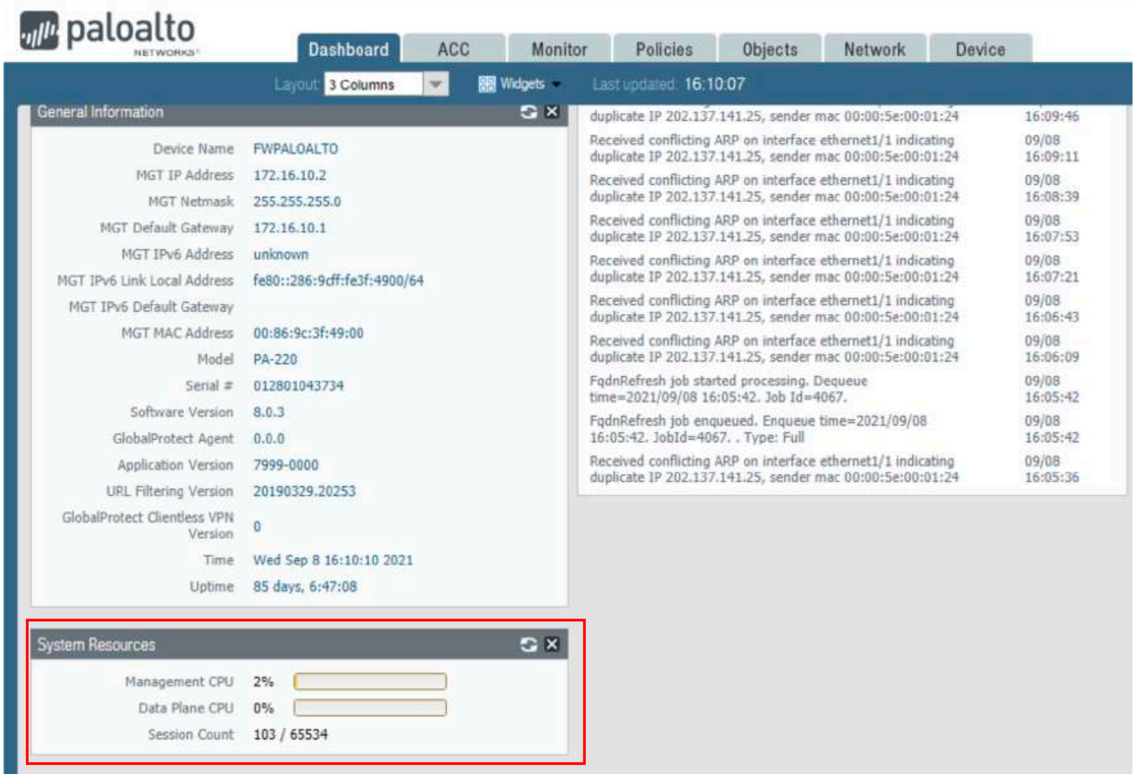
Locks

No locks found

ACC Risk Factor (Last 60 minutes)

3.5

Dashboard tab you can monitor many aspects including system resources of the firewall



General Information

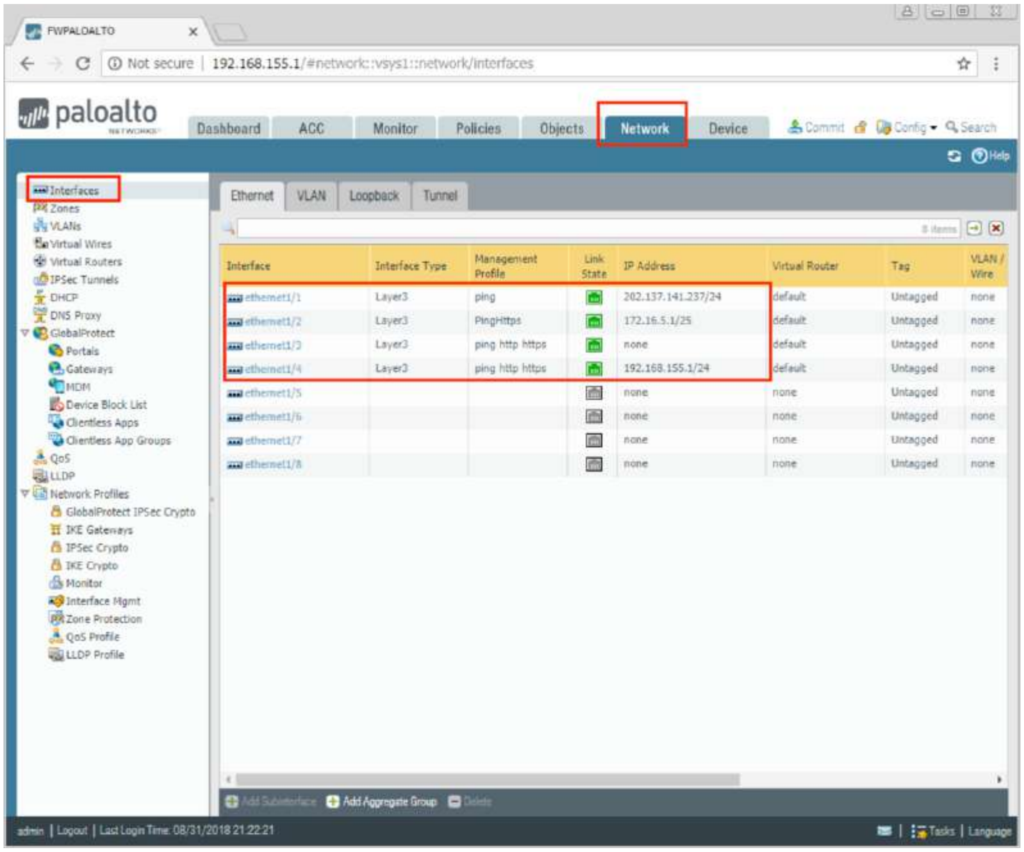
Device Name	FWPALOALTO
MGT IP Address	172.16.10.2
MGT Netmask	255.255.255.0
MGT Default Gateway	172.16.10.1
MGT IPv6 Address	unknown
MGT IPv6 Link Local Address	fe80::286:9cff:fe3f:4900/64
MGT IPv6 Default Gateway	
MGT MAC Address	00:86:9c:3f:49:00
Model	PA-220
Serial #	012801043734
Software Version	8.0.3
GlobalProtect Agent	0.0.0
Application Version	7999-0000
URL Filtering Version	20190329.20253
GlobalProtect Clientless VPN Version	0
Time	Wed Sep 8 16:10:10 2021
Uptime	85 days, 6:47:08

System Resources

Management CPU	2%
Data Plane CPU	0%
Session Count	103 / 65534

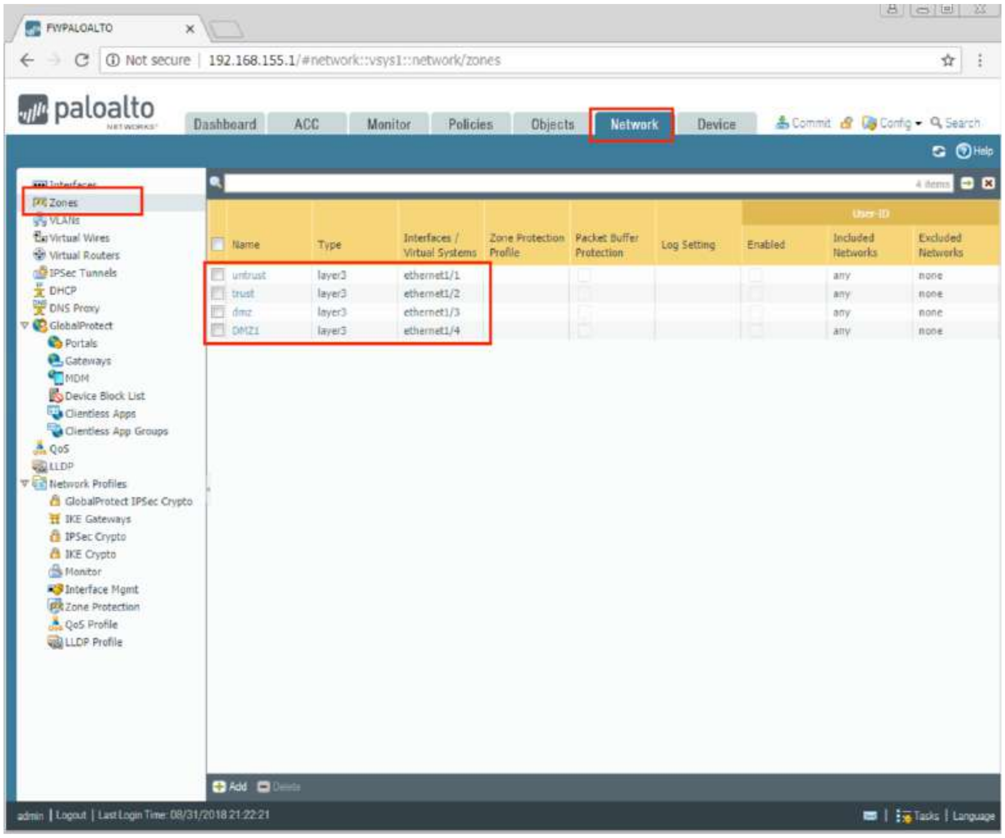
```
duplicate IP 202.137.141.25, sender mac 00:00:5e:00:01:24      16:09:46
Received conflicting ARP on interface ethernet1/1 indicating   09/08
duplicate IP 202.137.141.25, sender mac 00:00:5e:00:01:24      16:09:11
Received conflicting ARP on interface ethernet1/1 indicating   09/08
duplicate IP 202.137.141.25, sender mac 00:00:5e:00:01:24      16:08:39
Received conflicting ARP on interface ethernet1/1 indicating   09/08
duplicate IP 202.137.141.25, sender mac 00:00:5e:00:01:24      16:07:53
Received conflicting ARP on interface ethernet1/1 indicating   09/08
duplicate IP 202.137.141.25, sender mac 00:00:5e:00:01:24      16:07:21
Received conflicting ARP on interface ethernet1/1 indicating   09/08
duplicate IP 202.137.141.25, sender mac 00:00:5e:00:01:24      16:06:43
Received conflicting ARP on interface ethernet1/1 indicating   09/08
duplicate IP 202.137.141.25, sender mac 00:00:5e:00:01:24      16:06:09
FqdnRefresh job started processing. Dequeue                    09/08
time=2021/09/08 16:05:42. Job Id=4067.                         16:05:42
FqdnRefresh job enqueued. Enqueue time=2021/09/08              09/08
16:05:42. JobId=4067. . Type: Full                             16:05:42
Received conflicting ARP on interface ethernet1/1 indicating   09/08
duplicate IP 202.137.141.25, sender mac 00:00:5e:00:01:24      16:05:36
```

- Common configuration tasks (On Demand)
  - **<u>Configure Firewall Interfaces:</u>**
    Start configuring the firewall by assigning IP to its interfaces: ***Network > Interfaces > ethernet1/x***



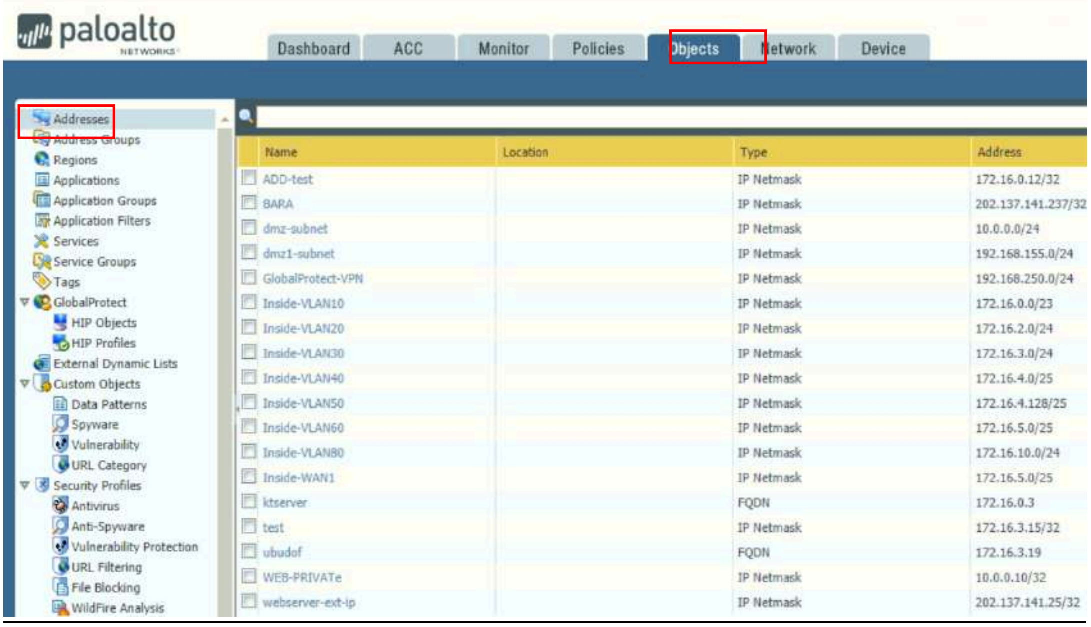
Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Wire
ethernet1/1	Layer3	ping	🟩	202.137.141.237/24	default	Untagged	none
ethernet1/2	Layer3	PingHttps	🟩	172.16.5.1/25	default	Untagged	none
ethernet1/3	Layer3	ping http https	🟩	none	default	Untagged	none
ethernet1/4	Layer3	ping http https	🟩	192.168.155.1/24	default	Untagged	none
ethernet1/5			▨	none	none	Untagged	none
ethernet1/6			▨	none	none	Untagged	none
ethernet1/7			▨	none	none	Untagged	none
ethernet1/8			▨	none	none	Untagged	none

- **<u>Configure Security Zone:</u>**
  Create security zones to be used when configuring policies: ***Network > Zones***



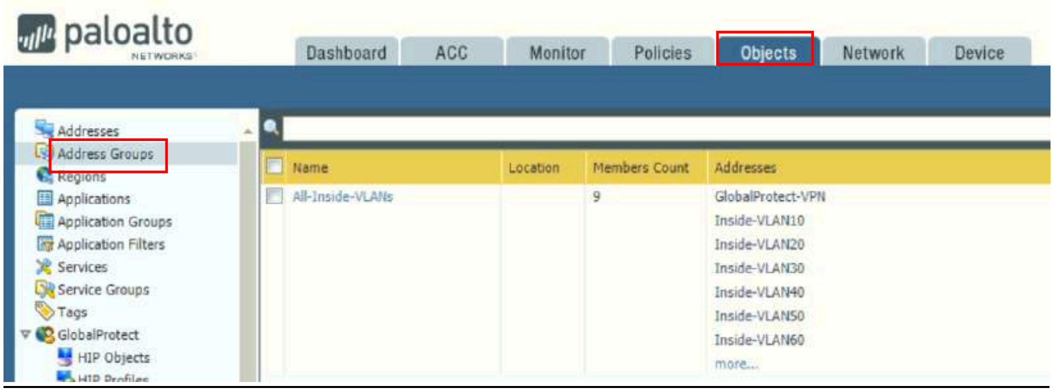
						User-ID		
Name	Type	Interfaces / Virtual Systems	Zone Protection Profile	Packet Buffer Protection	Log Setting	Enabled	Included Networks	Excluded Networks
untrust	layer3	ethernet1/1		□		□	any	none
trust	layer3	ethernet1/2		□		□	any	none
dmz	layer3	ethernet1/3		□		□	any	none
DMZ1	layer3	ethernet1/4		□		□	any	none

- **<u>Configure Network Objects:</u>**
  Create network objects: ***Objects > Addresses***



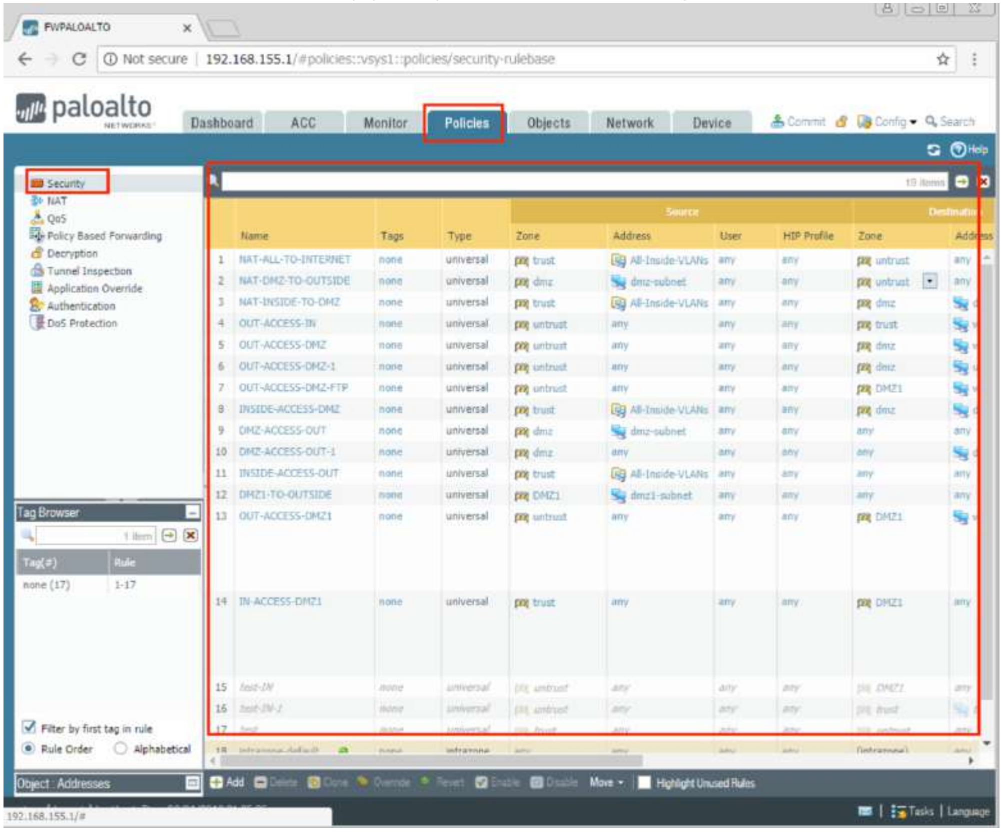
Name	Location	Type	Address
ADD-test		IP Netmask	172.16.0.12/32
BARA		IP Netmask	202.137.141.237/32
dmz-subnet		IP Netmask	10.0.0.0/24
dmz1-subnet		IP Netmask	192.168.155.0/24
GlobalProtect-VPN		IP Netmask	192.168.250.0/24
Inside-VLAN10		IP Netmask	172.16.0.0/23
Inside-VLAN20		IP Netmask	172.16.2.0/24
Inside-VLAN30		IP Netmask	172.16.3.0/24
Inside-VLAN40		IP Netmask	172.16.4.0/25
Inside-VLAN50		IP Netmask	172.16.4.128/25
Inside-VLAN60		IP Netmask	172.16.5.0/25
Inside-VLAN80		IP Netmask	172.16.10.0/24
Inside-WAN1		IP Netmask	172.16.5.0/25
ktserver		FQDN	172.16.0.3
test		IP Netmask	172.16.3.15/32
ubudof		FQDN	172.16.3.19
WEB-PRIVATe		IP Netmask	10.0.0.10/32
webserver-ext-ip		IP Netmask	202.137.141.25/32

- **<u>Configure Address Group:</u>**
  Create Address Groups: ***Objects > Address Groups***



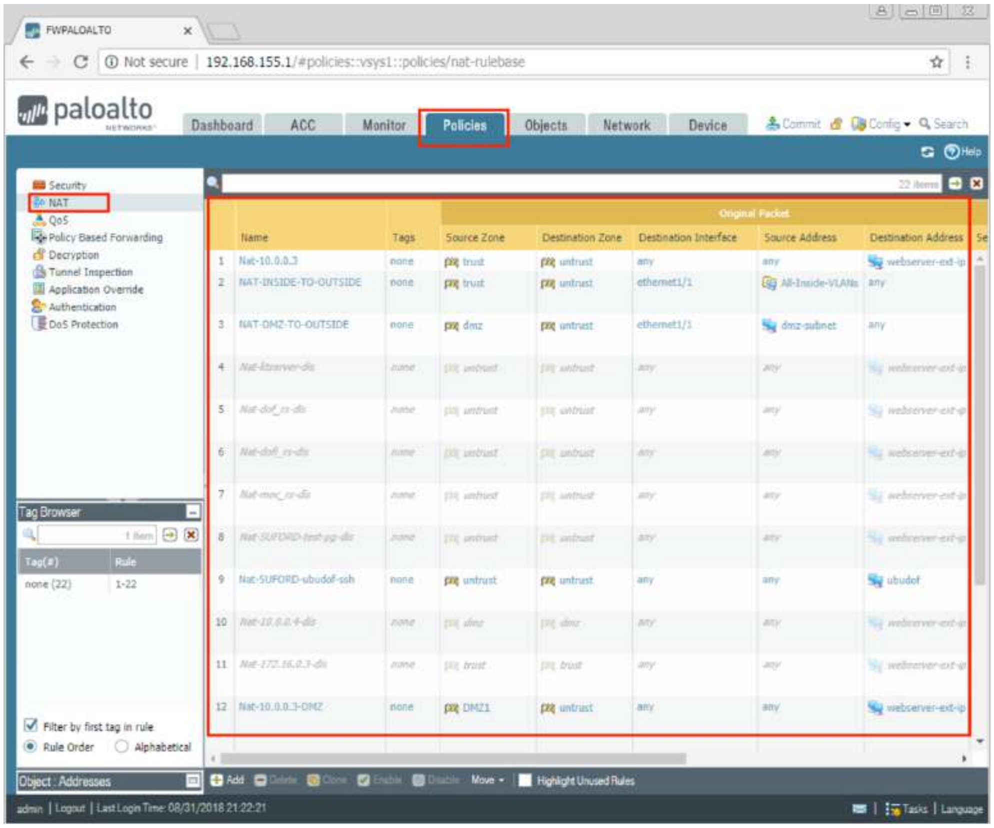
Name	Location	Members Count	Addresses
All-Inside-VLANs		9	GlobalProtect-VPN Inside-VLAN10 Inside-VLAN20 Inside-VLAN30 Inside-VLAN40 Inside-VLAN50 Inside-VLAN60 more...

- **Configure Security Policy:**
  Now we can create security policy: ***Policies > Security***



				Source				Destination	
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address
1	NAT-ALL-TO-INTERNET	none	universal	trust	All-Inside-VLANs	any	any	untrust	any
2	NAT-DMZ-TO-OUTSIDE	none	universal	dmz	dmz-subnet	any	any	untrust	any
3	NAT-INSIDE-TO-DMZ	none	universal	trust	All-Inside-VLANs	any	any	dmz	
4	OUT-ACCESS-IN	none	universal	untrust	any	any	any	trust	
5	OUT-ACCESS-DMZ	none	universal	untrust	any	any	any	dmz	
6	OUT-ACCESS-DMZ-1	none	universal	untrust	any	any	any	dmz	
7	OUT-ACCESS-DMZ-FTP	none	universal	untrust	any	any	any	DMZ1	
8	INSIDE-ACCESS-DMZ	none	universal	trust	All-Inside-VLANs	any	any	dmz	
9	DMZ-ACCESS-OUT	none	universal	dmz	dmz-subnet	any	any	any	any
10	DMZ-ACCESS-OUT-1	none	universal	dmz	any	any	any	any	
11	INSIDE-ACCESS-OUT	none	universal	trust	All-Inside-VLANs	any	any	any	any
12	DMZ1-TO-OUTSIDE	none	universal	DMZ1	dmz1-subnet	any	any	any	any
13	OUT-ACCESS-DMZ1	none	universal	untrust	any	any	any	DMZ1	
14	IN-ACCESS-DMZ1	none	universal	trust	any	any	any	DMZ1	any
15	test-IN	none	universal	untrust	any	any	any	DMZ1	any
16	test-IN-1	none	universal	untrust	any	any	any	trust	
17	test	none	universal	trust	any	any	any	untrust	any
18	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any

- **Configure NAT Policy:**
  Create NAT policies: ***Policies > NAT***



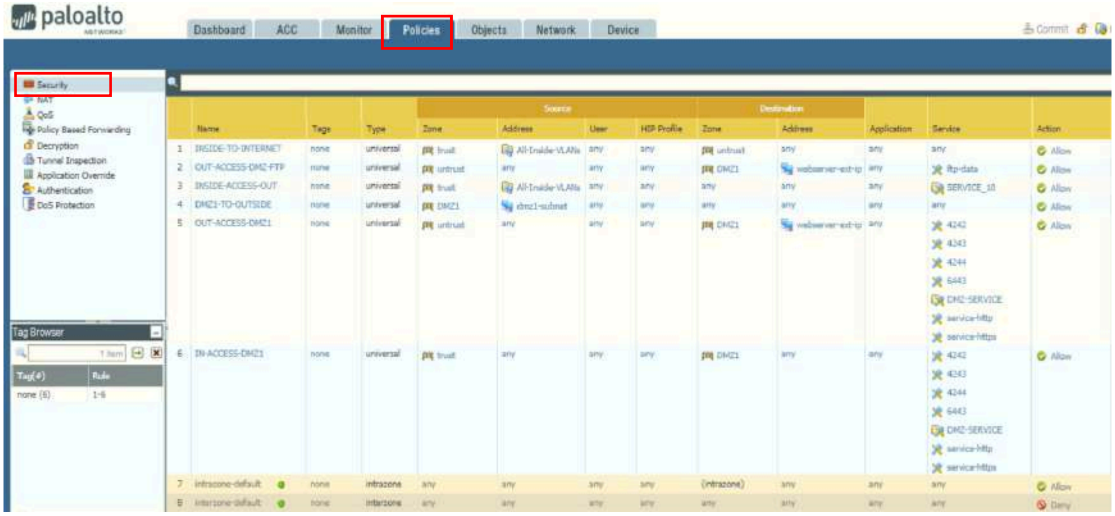
22 items

			Original Packet				
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address
1	Nat-10.0.0.3	none	trust	untrust	any	any	webserver-ext-ip
2	NAT-INSIDE-TO-OUTSIDE	none	trust	untrust	ethernet1/1	All-Inside-VLANs	any
3	NAT-DMZ-TO-OUTSIDE	none	dmz	untrust	ethernet1/1	dmz-subnet	any
4	*Nat-ktserver-dis*	*none*	*untrust*	*untrust*	*any*	*any*	*webserver-ext-ip*
5	*Nat-dof_rs-dis*	*none*	*untrust*	*untrust*	*any*	*any*	*webserver-ext-ip*
6	*Nat-dofi_rs-dis*	*none*	*untrust*	*untrust*	*any*	*any*	*webserver-ext-ip*
7	*Nat-mec_rs-dis*	*none*	*untrust*	*untrust*	*any*	*any*	*webserver-ext-ip*
8	*Nat-SUFORD-test-pg-dis*	*none*	*untrust*	*untrust*	*any*	*any*	*webserver-ext-ip*
9	Nat-SUFORD-ubudof-ssh	none	untrust	untrust	any	any	ubudof
10	*Nat-10.0.0.4-dis*	*none*	*dmz*	*dmz*	*any*	*any*	*webserver-ext-ip*
11	*Nat-172.16.0.3-dis*	*none*	*trust*	*trust*	*any*	*any*	*webserver-ext-ip*
12	Nat-10.0.0.3-DMZ	none	DMZ1	untrust	any	any	webserver-ext-ip

Tag(#)	Rule
none (22)	1-22

- Configurations related to NFMS
  - **Security Policy related to NFMS:**

    Navigate to ***Policies > Security***, the list of configured security policies is displayed.

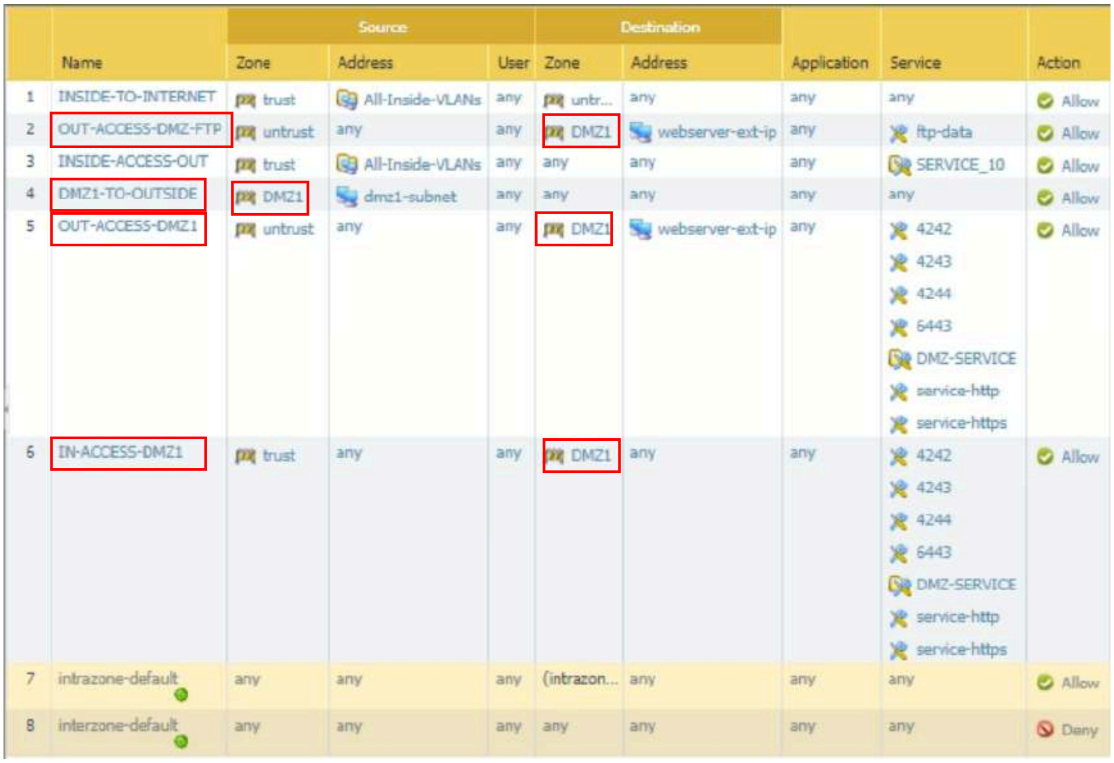


				Source				Destination				
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	INSIDE-TO-INTERNET	none	universal	trust	All-Inside-VLANs	any	any	untrust	any	any	any	Allow
2	OUT-ACCESS-DMZ-FTP	none	universal	untrust	any	any	any	DMZ1	webserver-ext-ip	any	ftp-data	Allow
3	INSIDE-ACCESS-OUT	none	universal	trust	All-Inside-VLANs	any	any	any	any	any	SERVICE_10	Allow
4	DMZ1-TO-OUTSIDE	none	universal	DMZ1	dmz1-subnet	any	any	any	any	any	any	Allow
5	OUT-ACCESS-DMZ1	none	universal	untrust	any	any	any	DMZ1	webserver-ext-ip	any	4242 4243 4244 6443 DMZ-SERVICE service-http service-https	Allow
6	IN-ACCESS-DMZ1	none	universal	trust	any	any	any	DMZ1	any	any	4242 4243 4244 6443 DMZ-SERVICE service-http service-https	Allow
7	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow
8	interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny

Tag(#)	Rule
none (6)	1-6

To identify policies related to NFMS we look get field Source->Zone and Destination->Zone, if one of the mentioned field contain DMZ1 meaning that the policies related to NFMS (Because DMZ1 is the zone name configured for NFMS's VM connections)

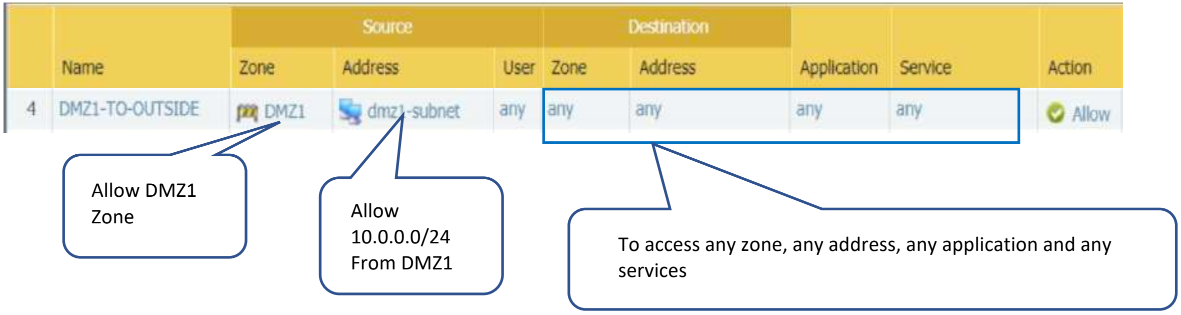
Zoom in:



		Source			Destination				
	Name	Zone	Address	User	Zone	Address	Application	Service	Action
1	INSIDE-TO-INTERNET	trust	All-Inside-VLANs	any	untr...	any	any	any	Allow
2	OUT-ACCESS-DMZ-FTP	untrust	any	any	DMZ1	webserver-ext-ip	any	ftp-data	Allow
3	INSIDE-ACCESS-OUT	trust	All-Inside-VLANs	any	any	any	any	SERVICE_10	Allow
4	DMZ1-TO-OUTSIDE	DMZ1	dmz1-subnet	any	any	any	any	any	Allow
5	OUT-ACCESS-DMZ1	untrust	any	any	DMZ1	webserver-ext-ip	any	4242 4243 4244 6443 DMZ-SERVICE service-http service-https	Allow
6	IN-ACCESS-DMZ1	trust	any	any	DMZ1	any	any	4242 4243 4244 6443 DMZ-SERVICE service-http service-https	Allow
7	intrazone-default	any	any	any	(intrazon...	any	any	any	Allow
8	interzone-default	any	any	any	any	any	any	any	Deny

We'll look at policy number 4 as an example for allowing outgoing requests from NFMS VMs and policy number 5 as an example for allowing incoming requests to NFMS VMs as below:

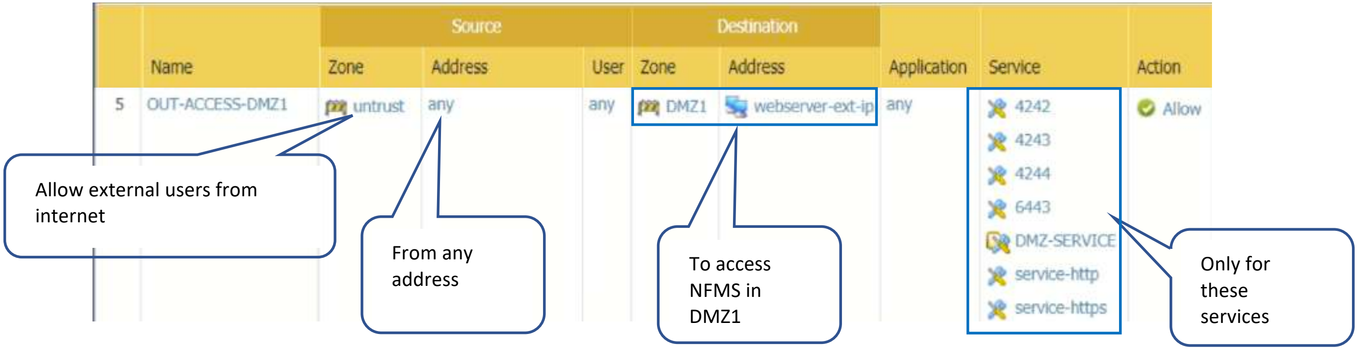
Policy number 4:



		Source			Destination				
	Name	Zone	Address	User	Zone	Address	Application	Service	Action
4	DMZ1-TO-OUTSIDE	DMZ1	dmz1-subnet	any	any	any	any	any	Allow

Allow DMZ1 Zone
Allow 10.0.0.0/24 From DMZ1
To access any zone, any address, any application and any services

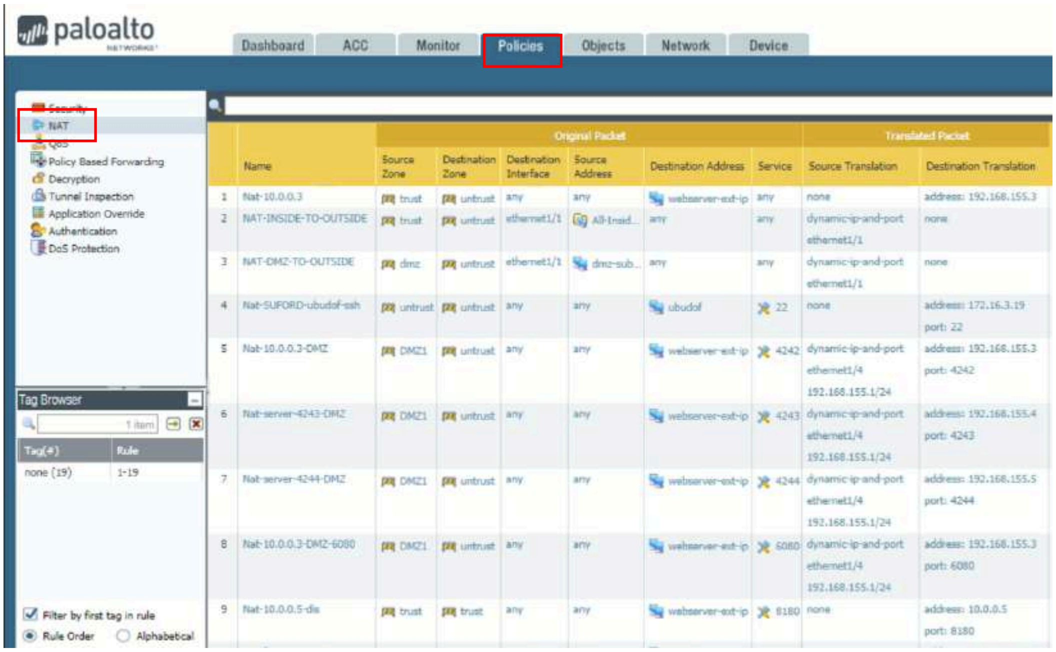
Policy Number 5:



		Source			Destination				
	Name	Zone	Address	User	Zone	Address	Application	Service	Action
5	OUT-ACCESS-DMZ1	untrust	any	any	DMZ1	webserver-ext-ip	any	4242 4243 4244 6443 DMZ-SERVICE service-http service-https	Allow

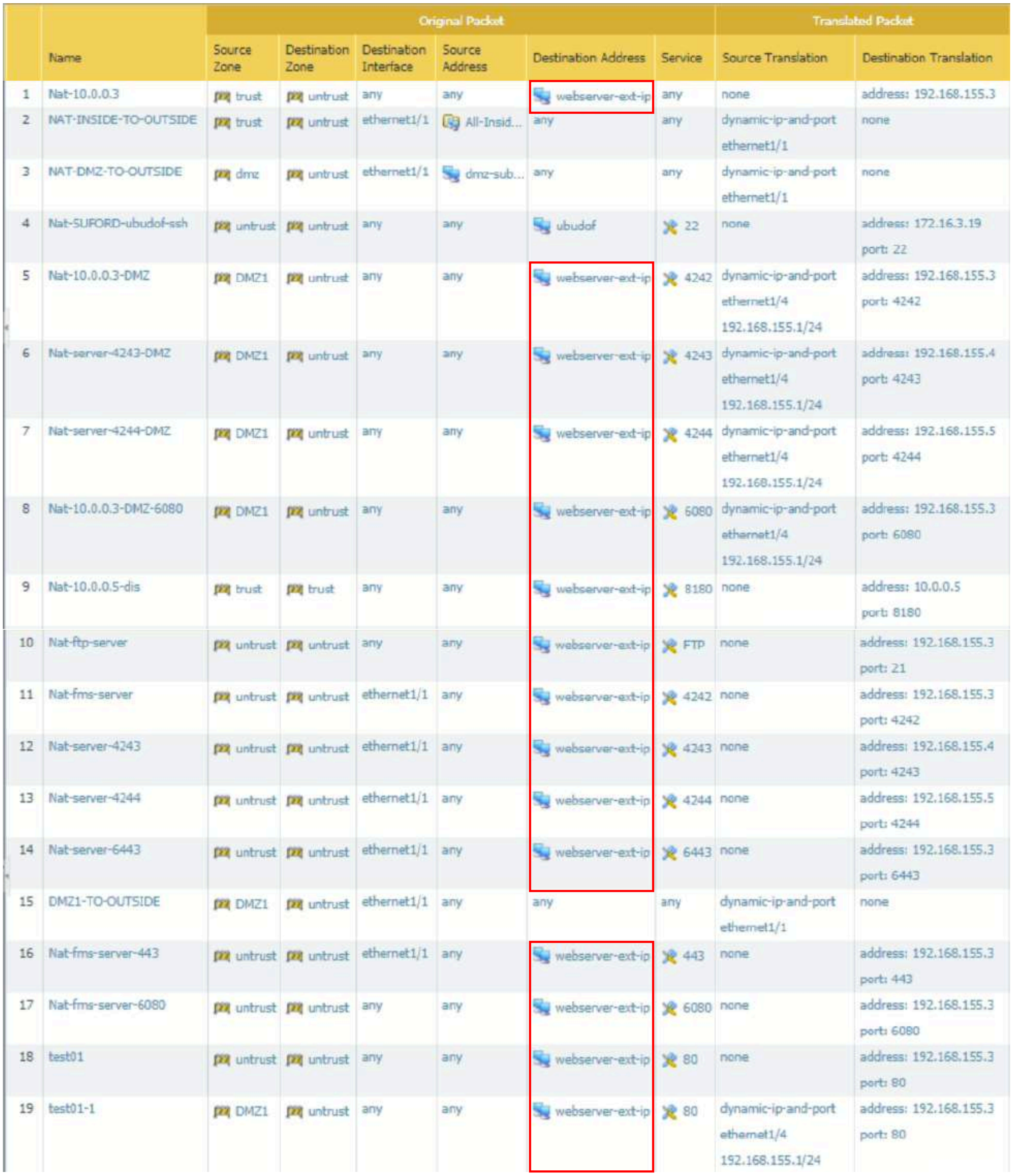
- **<u>NAT Policy related to NFMS:</u>**

Navigate to ***Policies > NAT,*** the list of configured NAT policies is displayed



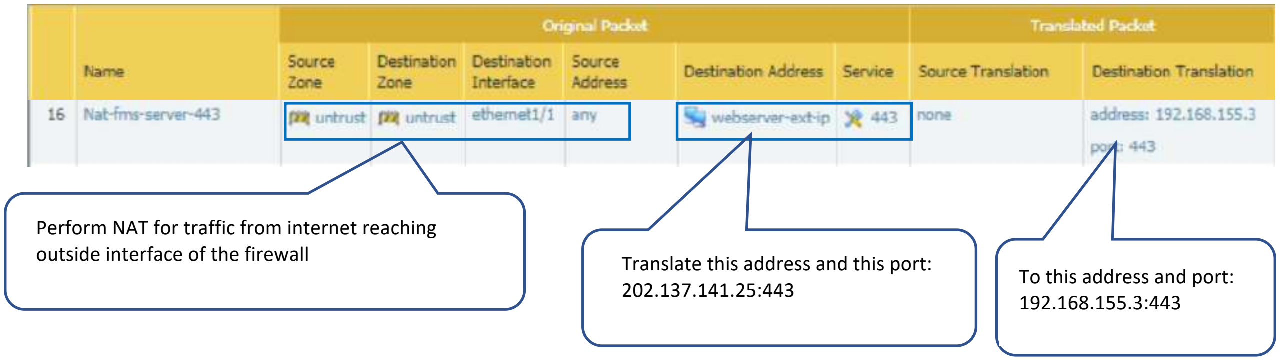
		Original Packet						Translated Packet	
	Name	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	Nat-10.0.0.3	trust	untrust	any	any	webserver-ext-ip	any	none	address: 192.168.155.3
2	NAT-INSIDE-TO-OUTSIDE	trust	untrust	ethernet1/1	All-Insid...	any	any	dynamic-ip-and-port ethernet1/1	none
3	NAT-DMZ-TO-OUTSIDE	dmz	untrust	ethernet1/1	dmz-sub...	any	any	dynamic-ip-and-port ethernet1/1	none
4	Nat-SUFORD-ubudof-ssh	untrust	untrust	any	any	ubudof	22	none	address: 172.16.3.19 port: 22
5	Nat-10.0.0.3-DMZ	DMZ1	untrust	any	any	webserver-ext-ip	4242	dynamic-ip-and-port ethernet1/4 192.168.155.1/24	address: 192.168.155.3 port: 4242
6	Nat-server-4243-DMZ	DMZ1	untrust	any	any	webserver-ext-ip	4243	dynamic-ip-and-port ethernet1/4 192.168.155.1/24	address: 192.168.155.4 port: 4243
7	Nat-server-4244-DMZ	DMZ1	untrust	any	any	webserver-ext-ip	4244	dynamic-ip-and-port ethernet1/4 192.168.155.1/24	address: 192.168.155.5 port: 4244
8	Nat-10.0.0.3-DMZ-6080	DMZ1	untrust	any	any	webserver-ext-ip	6080	dynamic-ip-and-port ethernet1/4 192.168.155.1/24	address: 192.168.155.3 port: 6080
9	Nat-10.0.0.5-dis	trust	trust	any	any	webserver-ext-ip	8180	none	address: 10.0.0.5 port: 8180

To identify policies related to NFMS we look get field Destination Address, if the mentioned field contain webserver-ext-ip meaning that the policies related to NFMS (Because webserver-ext-ip is the public used for NFMS's NAT (202.137.141.25))



		Original Packet						Translated Packet	
	Name	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	Nat-10.0.0.3	trust	untrust	any	any	webserver-ext-ip	any	none	address: 192.168.155.3
2	NAT-INSIDE-TO-OUTSIDE	trust	untrust	ethernet1/1	All-Insid...	any	any	dynamic-ip-and-port ethernet1/1	none
3	NAT-DMZ-TO-OUTSIDE	dmz	untrust	ethernet1/1	dmz-sub...	any	any	dynamic-ip-and-port ethernet1/1	none
4	Nat-SUFORD-ubudof-ssh	untrust	untrust	any	any	ubudof	22	none	address: 172.16.3.19 port: 22
5	Nat-10.0.0.3-DMZ	DMZ1	untrust	any	any	webserver-ext-ip	4242	dynamic-ip-and-port ethernet1/4 192.168.155.1/24	address: 192.168.155.3 port: 4242
6	Nat-server-4243-DMZ	DMZ1	untrust	any	any	webserver-ext-ip	4243	dynamic-ip-and-port ethernet1/4 192.168.155.1/24	address: 192.168.155.4 port: 4243
7	Nat-server-4244-DMZ	DMZ1	untrust	any	any	webserver-ext-ip	4244	dynamic-ip-and-port ethernet1/4 192.168.155.1/24	address: 192.168.155.5 port: 4244
8	Nat-10.0.0.3-DMZ-6080	DMZ1	untrust	any	any	webserver-ext-ip	6080	dynamic-ip-and-port ethernet1/4 192.168.155.1/24	address: 192.168.155.3 port: 6080
9	Nat-10.0.0.5-dis	trust	trust	any	any	webserver-ext-ip	8180	none	address: 10.0.0.5 port: 8180
10	Nat-ftp-server	untrust	untrust	any	any	webserver-ext-ip	FTP	none	address: 192.168.155.3 port: 21
11	Nat-fms-server	untrust	untrust	ethernet1/1	any	webserver-ext-ip	4242	none	address: 192.168.155.3 port: 4242
12	Nat-server-4243	untrust	untrust	ethernet1/1	any	webserver-ext-ip	4243	none	address: 192.168.155.4 port: 4243
13	Nat-server-4244	untrust	untrust	ethernet1/1	any	webserver-ext-ip	4244	none	address: 192.168.155.5 port: 4244
14	Nat-server-6443	untrust	untrust	ethernet1/1	any	webserver-ext-ip	6443	none	address: 192.168.155.3 port: 6443
15	DMZ1-TO-OUTSIDE	DMZ1	untrust	ethernet1/1	any	any	any	dynamic-ip-and-port ethernet1/1	none
16	Nat-fms-server-443	untrust	untrust	ethernet1/1	any	webserver-ext-ip	443	none	address: 192.168.155.3 port: 443
17	Nat-fms-server-6080	untrust	untrust	any	any	webserver-ext-ip	6080	none	address: 192.168.155.3 port: 6080
18	test01	untrust	untrust	any	any	webserver-ext-ip	80	none	address: 192.168.155.3 port: 80
19	test01-1	DMZ1	untrust	any	any	webserver-ext-ip	80	dynamic-ip-and-port ethernet1/4 192.168.155.1/24	address: 192.168.155.3 port: 80

Explained example of a NAT Policy:



		Original Packet						Translated Packet	
	Name	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
16	Nat-fms-server-443	untrust	untrust	ethernet1/1	any	webserver-ext-ip	443	none	address: 192.168.155.3 port: 443

Perform NAT for traffic from internet reaching outside interface of the firewall

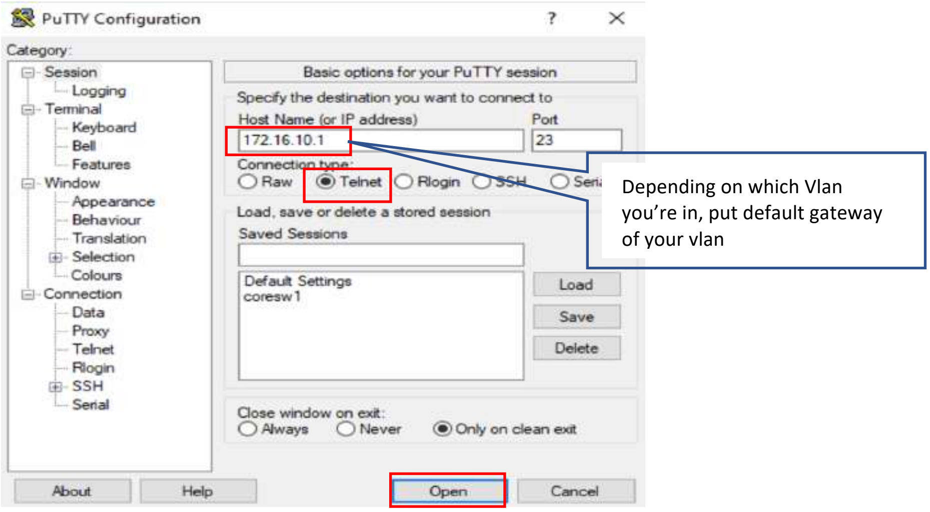
Translate this address and this port: 202.137.141.25:443

To this address and port: 192.168.155.3:443

3.2 Core Switch

- Core Switch Configuration (On Demand)

You need to be inside FIPD network or login to a computer inside FIPD network. Using Putty to access FIPD core switch, fill in access information as below:



Host Name (or IP address): 172.16.10.1

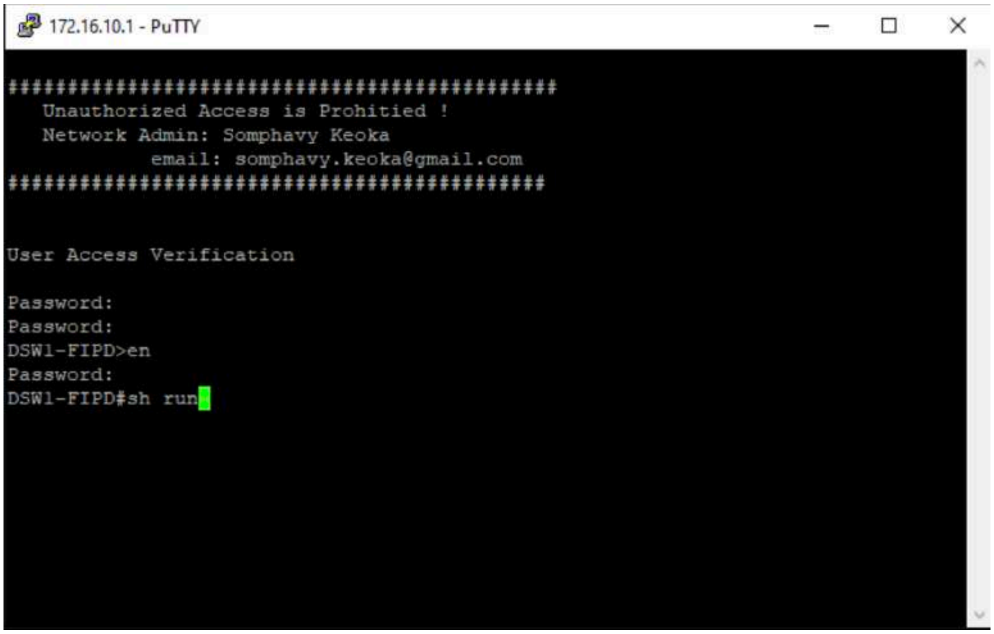
Port: 23

Connection type: ○ Raw ● Telnet ○ Rlogin ○ SSH ○ Serial

Saved Sessions: Default Settings, coresw1

Close window on exit: ○ Always ○ Never ● Only on clean exit

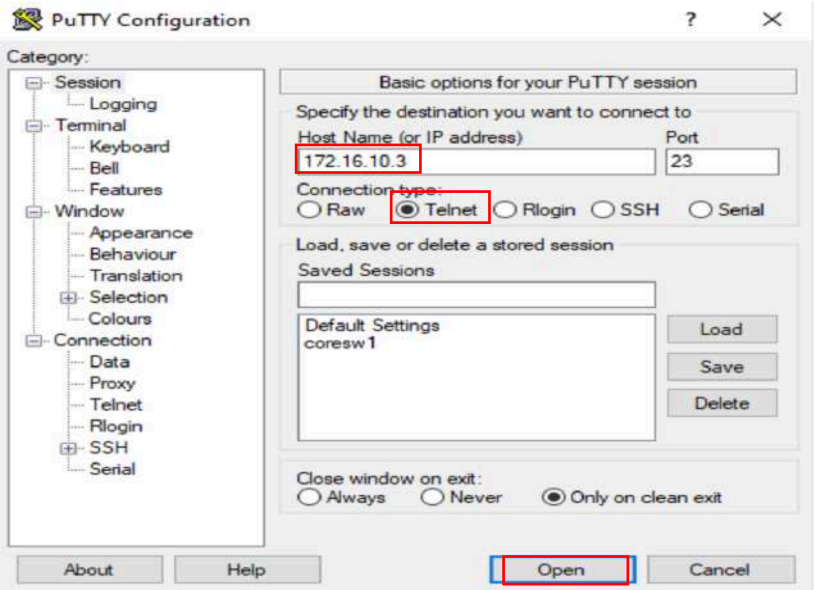
Depending on which Vlan you're in, put default gateway of your vlan



```
##############################################
   Unauthorized Access is Prohitied !
   Network Admin: Somphavy Keoka
            email: somphavy.keoka@gmail.com
#############################################


User Access Verification

Password:
Password:
DSW1-FIPD>en
Password:
DSW1-FIPD#sh run
```

- Accessing NFMS Switch:
-

You need to be inside FIPD network or login to a computer inside FIPD network. Using Putty to access NFMS switch, fill in access information as below:



Specify the destination you want to connect to

Host Name (or IP address): 172.16.10.3 Port: 23

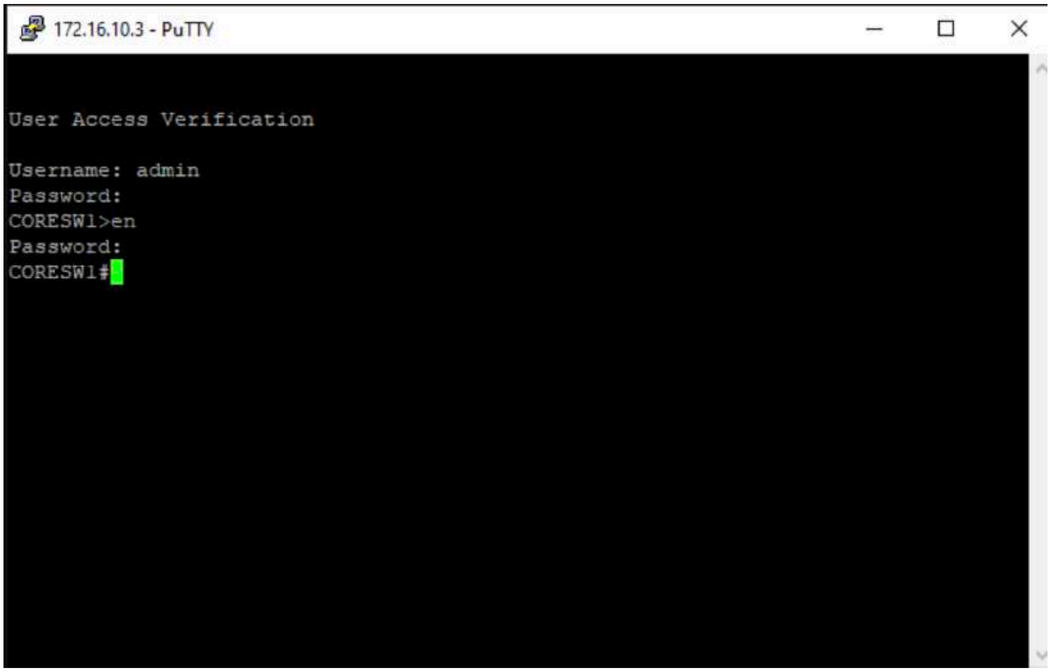
Connection type: ○ Raw ● Telnet ○ Rlogin ○ SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

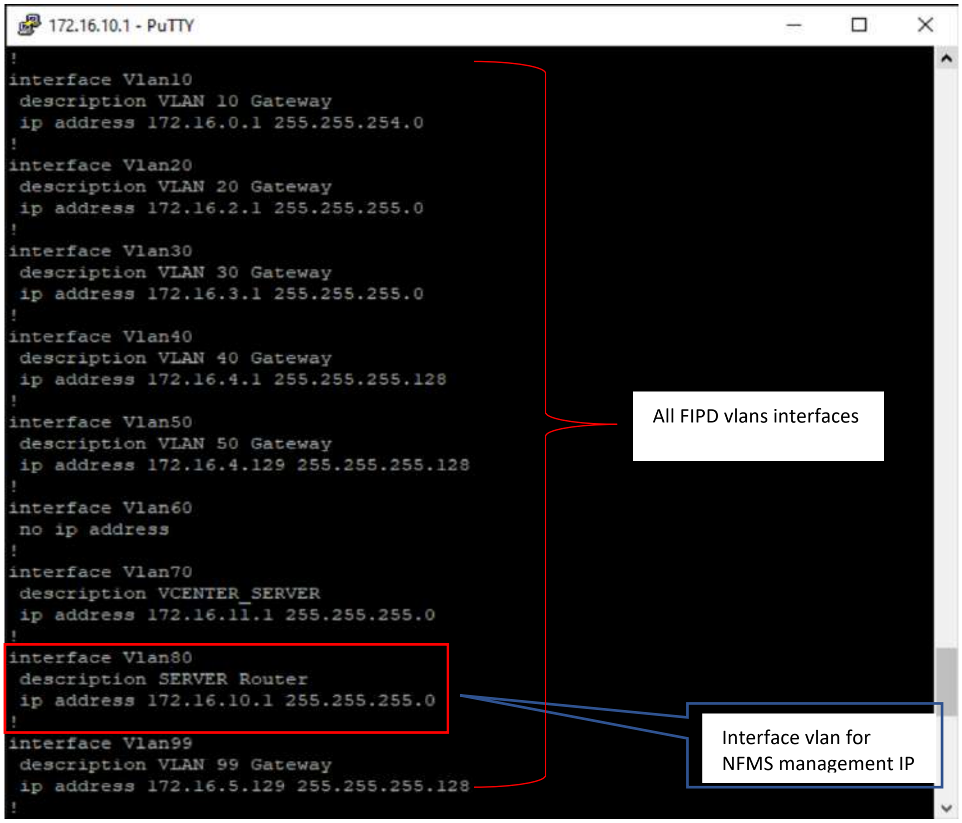
Default Settings
coresw1

Close window on exit: ○ Always ○ Never ● Only on clean exit



```
User Access Verification

Username: admin
Password:
CORESW1>en
Password:
CORESW1#
```

- Configurations related to NFMS
    - Configurations in FIPD core switch

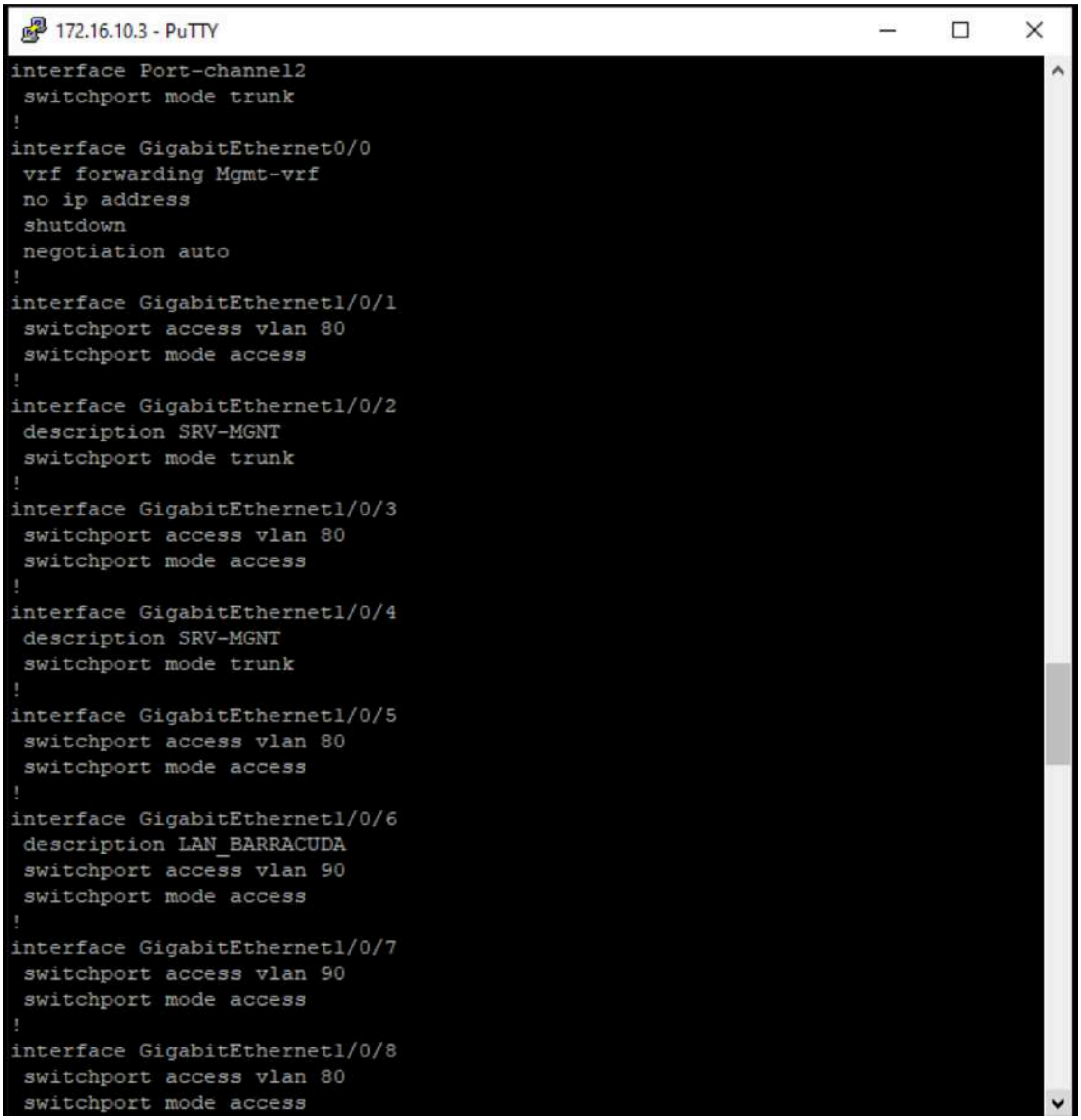


```
!
interface Vlan10
 description VLAN 10 Gateway
 ip address 172.16.0.1 255.255.254.0
!
interface Vlan20
 description VLAN 20 Gateway
 ip address 172.16.2.1 255.255.255.0
!
interface Vlan30
 description VLAN 30 Gateway
 ip address 172.16.3.1 255.255.255.0
!
interface Vlan40
 description VLAN 40 Gateway
 ip address 172.16.4.1 255.255.255.128
!
interface Vlan50
 description VLAN 50 Gateway
 ip address 172.16.4.129 255.255.255.128
!
interface Vlan60
 no ip address
!
interface Vlan70
 description VCENTER_SERVER
 ip address 172.16.11.1 255.255.255.0
!
interface Vlan80
 description SERVER Router
 ip address 172.16.10.1 255.255.255.0
!
interface Vlan99
 description VLAN 99 Gateway
 ip address 172.16.5.129 255.255.255.128
!
```

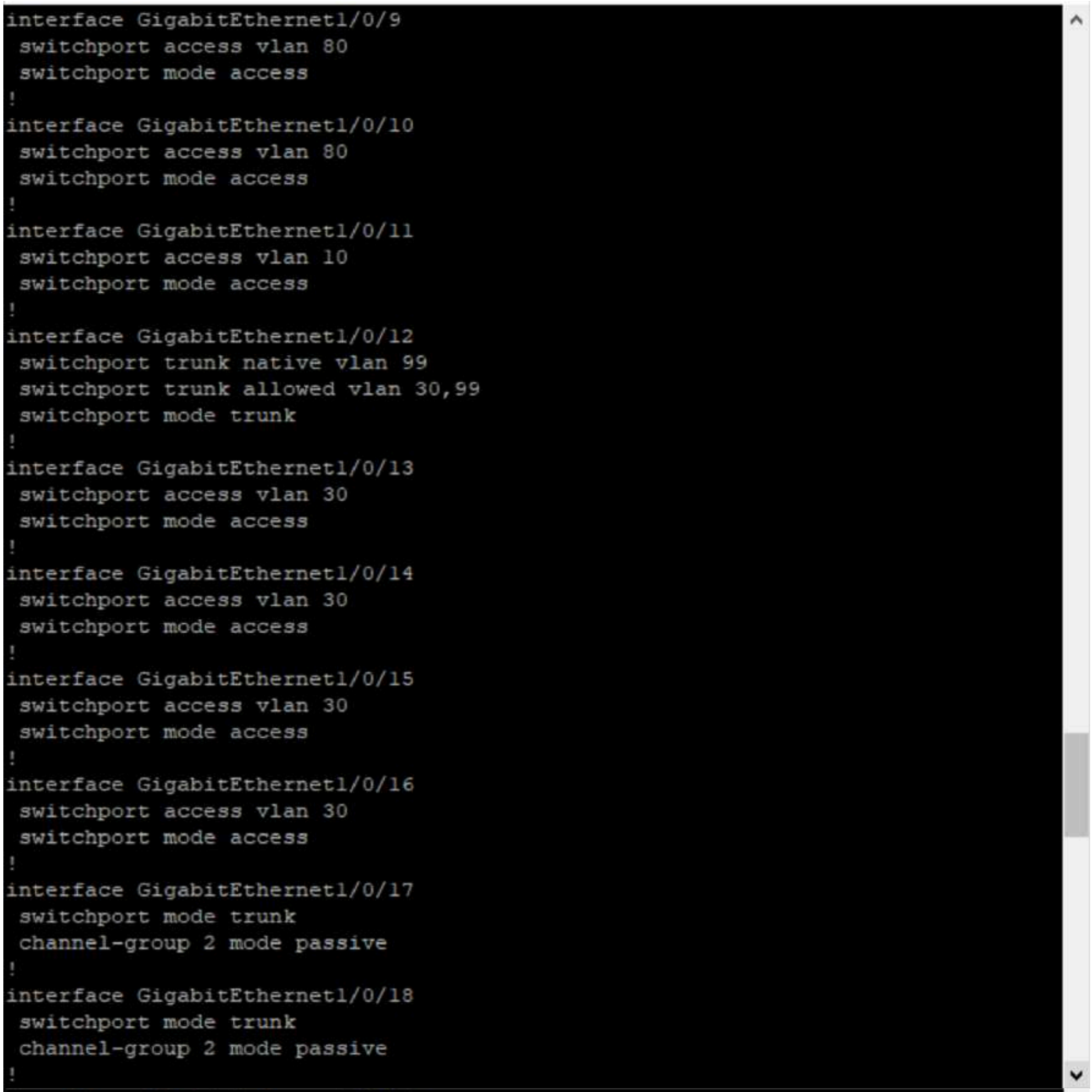
All FIPD vlans interfaces

Interface vlan for NFMS management IP

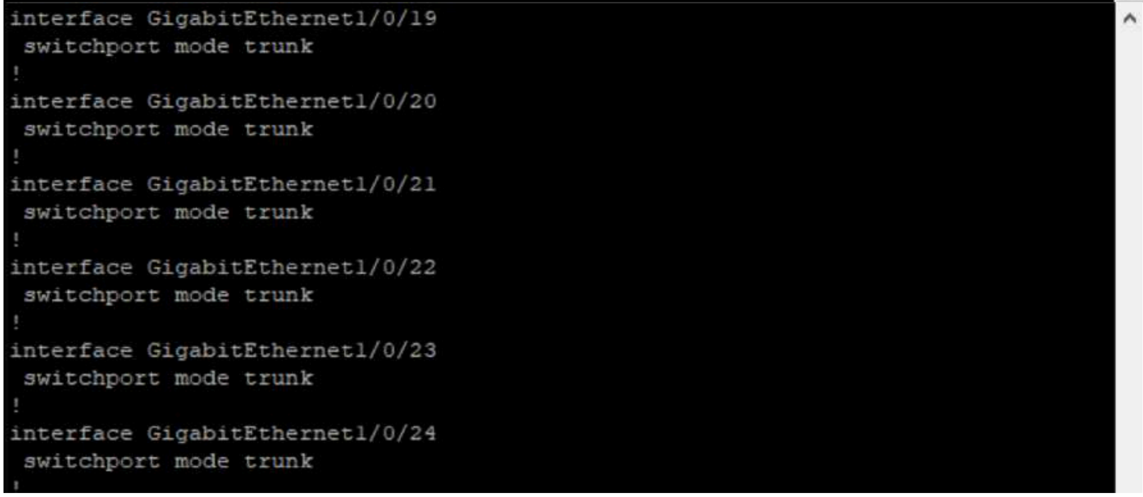
- Configurations in NFMS switch



```
interface Port-channel2
 switchport mode trunk
!
interface GigabitEthernet0/0
 vrf forwarding Mgmt-vrf
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet1/0/1
 switchport access vlan 80
 switchport mode access
!
interface GigabitEthernet1/0/2
 description SRV-MGNT
 switchport mode trunk
!
interface GigabitEthernet1/0/3
 switchport access vlan 80
 switchport mode access
!
interface GigabitEthernet1/0/4
 description SRV-MGNT
 switchport mode trunk
!
interface GigabitEthernet1/0/5
 switchport access vlan 80
 switchport mode access
!
interface GigabitEthernet1/0/6
 description LAN_BARRACUDA
 switchport access vlan 90
 switchport mode access
!
interface GigabitEthernet1/0/7
 switchport access vlan 90
 switchport mode access
!
interface GigabitEthernet1/0/8
 switchport access vlan 80
 switchport mode access
```



```
interface GigabitEthernet1/0/9
 switchport access vlan 80
 switchport mode access
!
interface GigabitEthernet1/0/10
 switchport access vlan 80
 switchport mode access
!
interface GigabitEthernet1/0/11
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/12
 switchport trunk native vlan 99
 switchport trunk allowed vlan 30,99
 switchport mode trunk
!
interface GigabitEthernet1/0/13
 switchport access vlan 30
 switchport mode access
!
interface GigabitEthernet1/0/14
 switchport access vlan 30
 switchport mode access
!
interface GigabitEthernet1/0/15
 switchport access vlan 30
 switchport mode access
!
interface GigabitEthernet1/0/16
 switchport access vlan 30
 switchport mode access
!
interface GigabitEthernet1/0/17
 switchport mode trunk
 channel-group 2 mode passive
!
interface GigabitEthernet1/0/18
 switchport mode trunk
 channel-group 2 mode passive
!
```

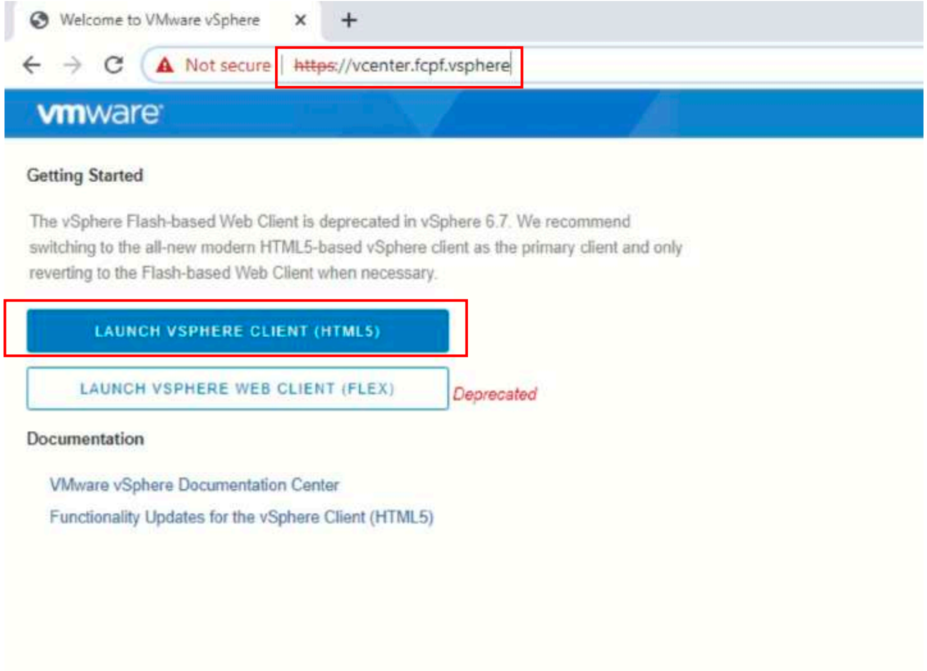


```
interface GigabitEthernet1/0/19
 switchport mode trunk
!
interface GigabitEthernet1/0/20
 switchport mode trunk
!
interface GigabitEthernet1/0/21
 switchport mode trunk
!
interface GigabitEthernet1/0/22
 switchport mode trunk
!
interface GigabitEthernet1/0/23
 switchport mode trunk
!
interface GigabitEthernet1/0/24
 switchport mode trunk
!
```

4 Virtual Machine Administration

- VM Infrastructure Monitoring (Weekly)
  - Accessing from vCenter Web Interface

  You need to be inside FIPD vlans or login to a computer inside FIPD vlans, open your web browser and fill in the address bar with https://vcenter.fcpf.vsphere then click on "LAUNCH VSPHERE CLIENT (HTML5)"



Welcome to VMware vSphere
Not secure
~~https~~://vcenter.fcpf.vsphere
vmware
LAUNCH VSPHERE CLIENT (HTML5)
LAUNCH VSPHERE WEB CLIENT (FLEX)
Deprecated

Getting Started

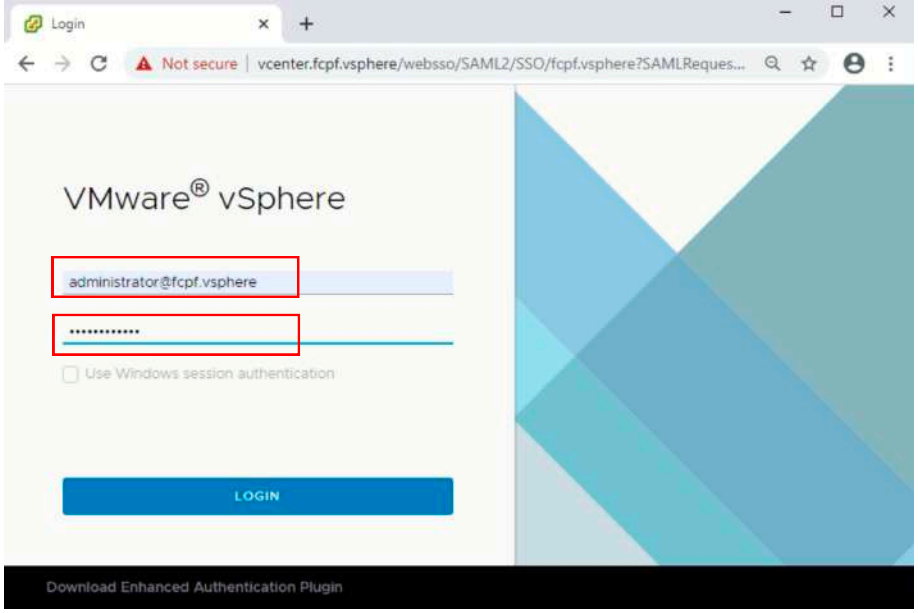
The vSphere Flash-based Web Client is deprecated in vSphere 6.7. We recommend switching to the all-new modern HTML5-based vSphere client as the primary client and only reverting to the Flash-based Web Client when necessary.

Documentation

VMware vSphere Documentation Center

Functionality Updates for the vSphere Client (HTML5)

Fill in login credentials then click LOGIN



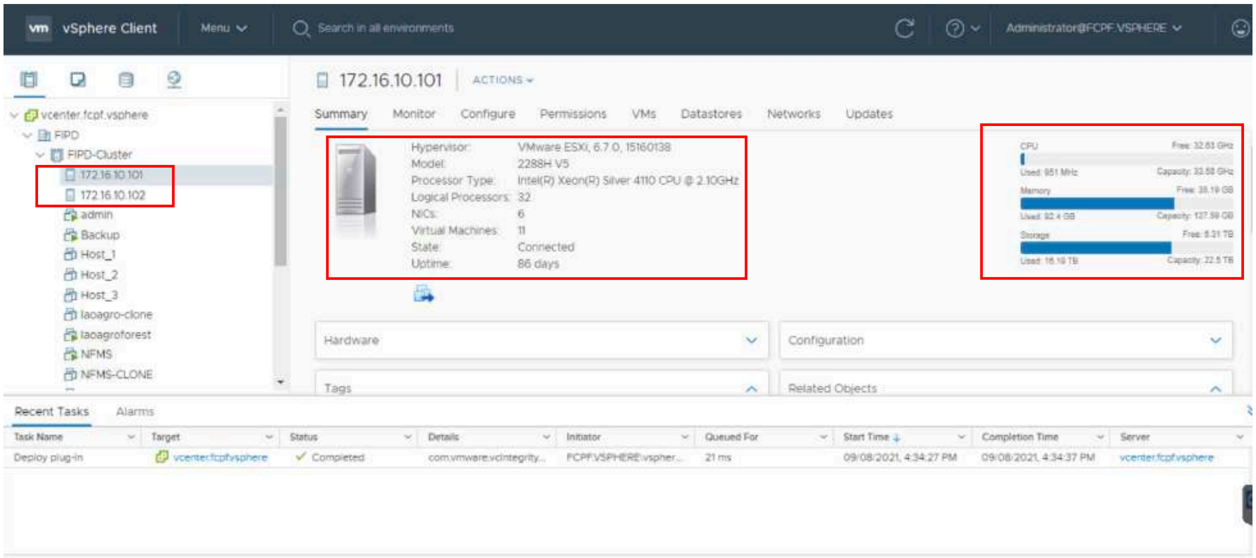
Login
Not secure
vcenter.fcpf.vsphere/websso/SAML2/SSO/fcpf.vsphere?SAMLReques...
VMware® vSphere
LOGIN
Download Enhanced Authentication Plugin

administrator@fcpf.vsphere

••••••••••••

□ Use Windows session authentication

Monitor system resources of ESXi hosts:

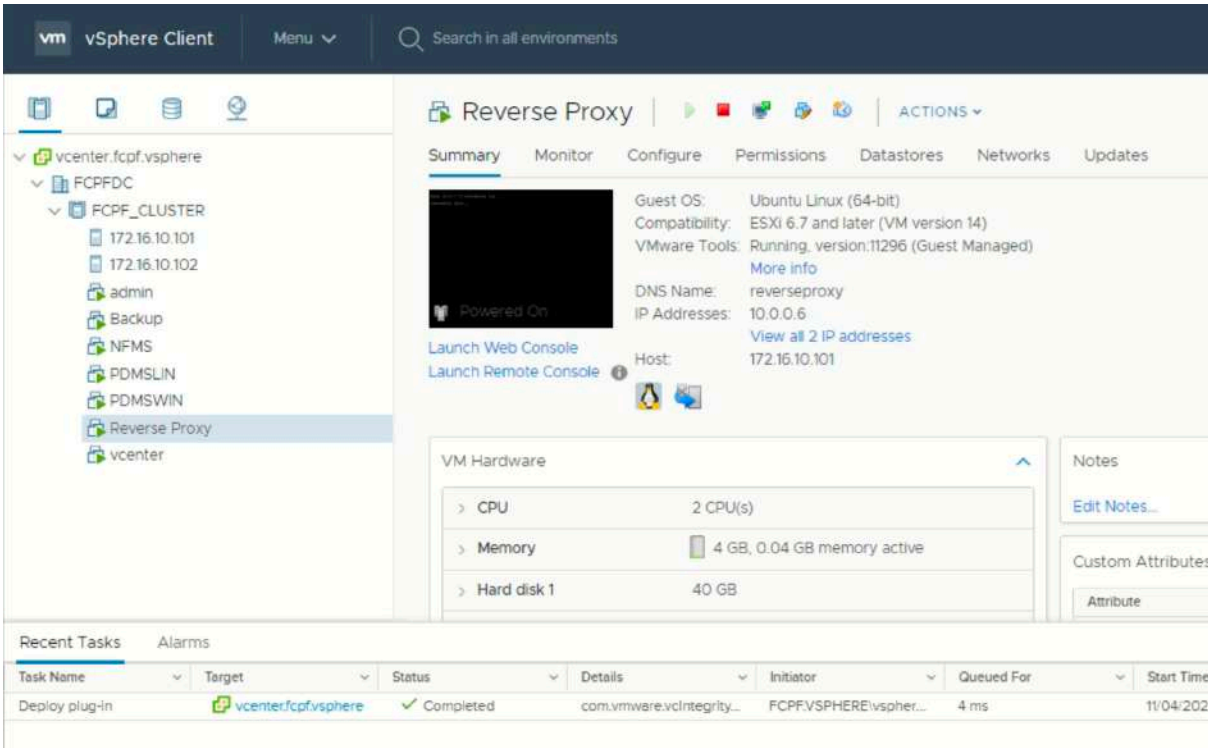


Hypervisor: VMware ESXi, 6.7.0, 15160138
Model: 2288H V5
Processor Type: Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz
Logical Processors: 32
NICs: 6
Virtual Machines: 11
State: Connected
Uptime: 86 days

CPU Free: 32.63 GHz
Used: 951 MHz Capacity: 33.58 GHz
Memory Free: 35.19 GB
Used: 92.4 GB Capacity: 127.59 GB
Storage Free: 6.31 TB
Used: 16.19 TB Capacity: 22.5 TB

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time	Server
Deploy plug-in	vcenter.fcpf.vsphere	✓ Completed	com.vmware.vcIntegrity...	FCPF.VSPHERE\vspher...	21 ms	09/08/2021, 4:34:27 PM	09/08/2021, 4:34:37 PM	vcenter.fcpf.vsphere

Monitor system resources of VM:



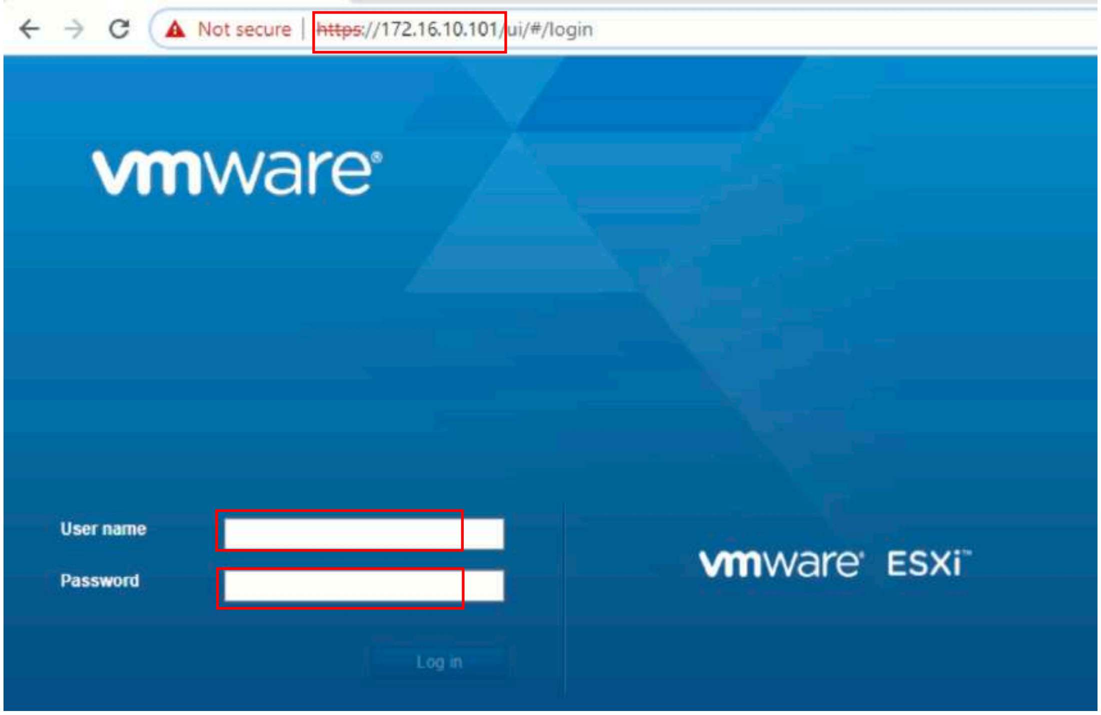
Guest OS: Ubuntu Linux (64-bit)
Compatibility: ESXi 6.7 and later (VM version 14)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: reverseproxy
IP Addresses: 10.0.0.6
Host: 172.16.10.101

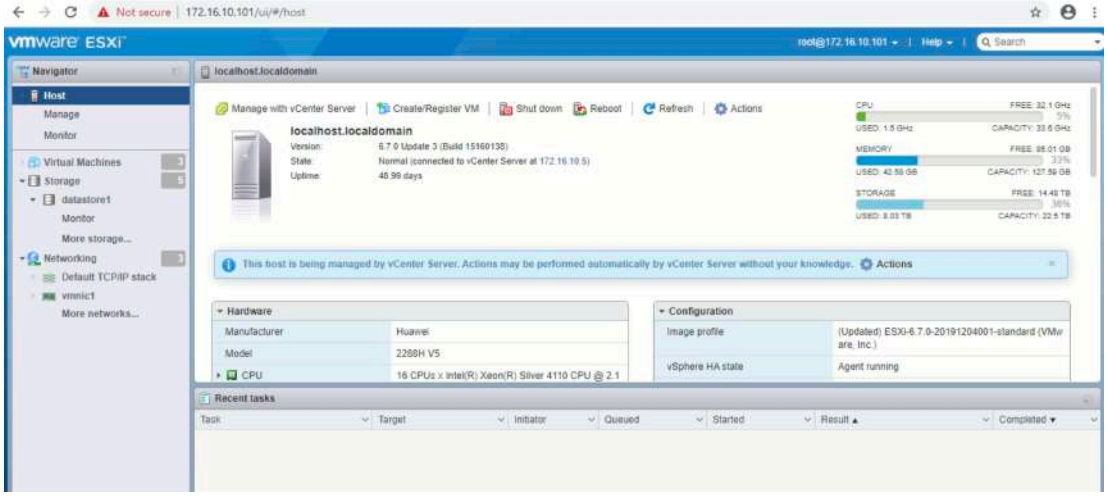
CPU	2 CPU(s)
Memory	4 GB, 0.04 GB memory active
Hard disk 1	40 GB

Task Name	Target	Status	Details	Initiator	Queued For	Start Time
Deploy plug-in	vcenter.fcpf.vsphere	✓ Completed	com.vmware.vcIntegrity...	FCPF.VSPHERE\vspher...	4 ms	11/04/202

- Accessing from ESXi Web Interface

You need to be inside FIPD vlans or login to a computer inside FIPD vlans, open your web browser and fill in the address bar with https://172.16.10.101 for ESXi1 or https://172.16.10.102 for ESXi2 then fill in login credentials and click Log in.





localhost.localdomain

Version:	6.7.0 Update 3 (Build 15160138)
State:	Normal (connected to vCenter Server at 172.16.10.5)
Uptime:	46.99 days

CPU FREE: 32.1 GHz 5% USED: 1.5 GHz CAPACITY: 33.6 GHz

MEMORY FREE: 85.01 GB 33% USED: 42.58 GB CAPACITY: 127.59 GB

STORAGE FREE: 14.48 TB 36% USED: 8.03 TB CAPACITY: 22.5 TB

This host is being managed by vCenter Server. Actions may be performed automatically by vCenter Server without your knowledge. Actions

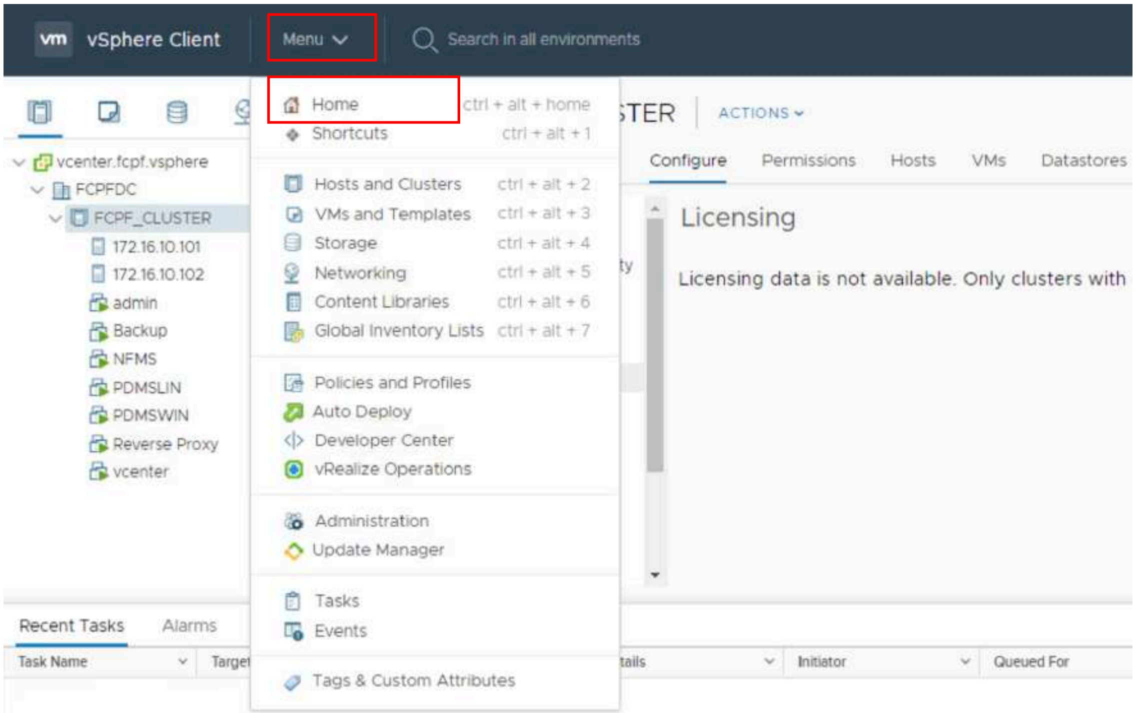
Hardware	
Manufacturer	Huawei
Model	2288H V5
CPU	16 CPUs x Intel(R) Xeon(R) Silver 4110 CPU @ 2.1

Configuration	
Image profile	(Updated) ESXi-6.7.0-20191204001-standard (VMware, Inc.)
vSphere HA state	Agent running

Task	Target	Initiator	Queued	Started	Result ▲	Completed ▼

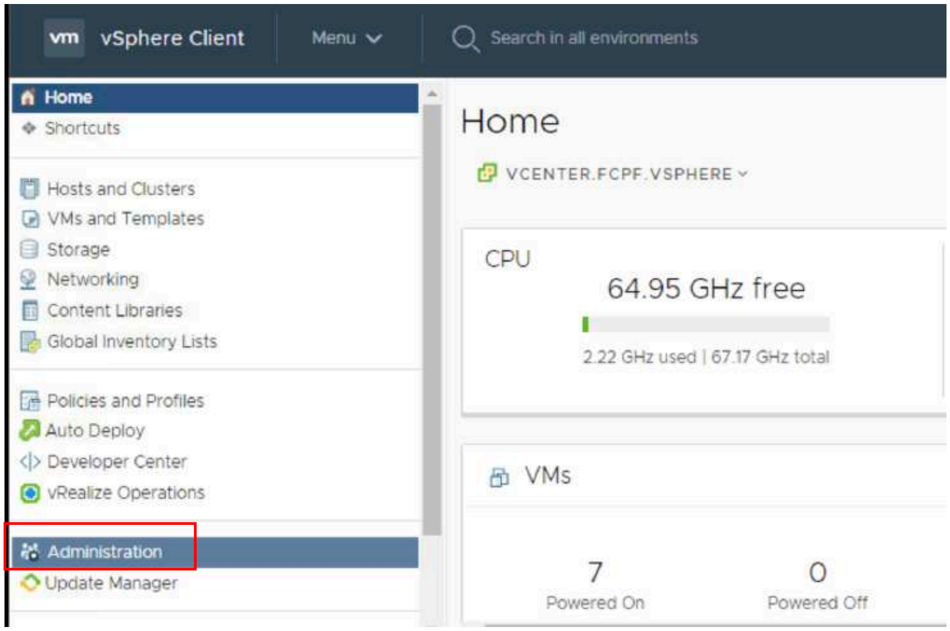
- Licenseing

To access license configuration page, first return to home page by clicking Menu button then select Home:

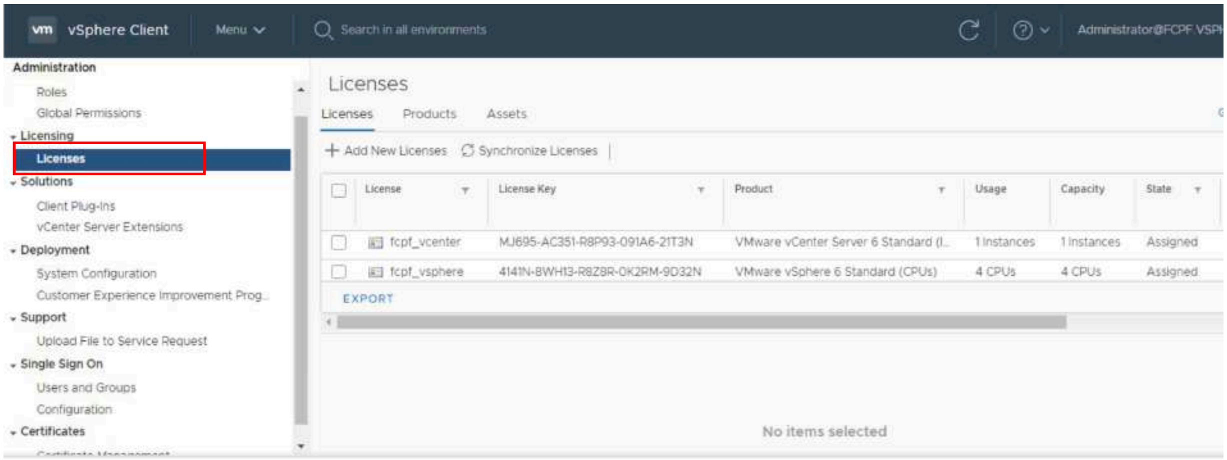


Licensing data is not available. Only clusters with

After that click on Administration:



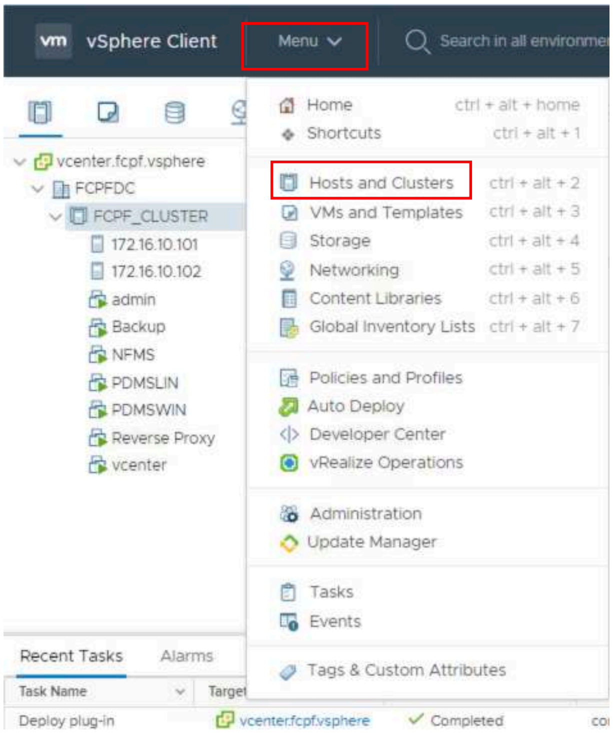
Then click on Licenses under Licensing, this page we can view, add or remove licenses.



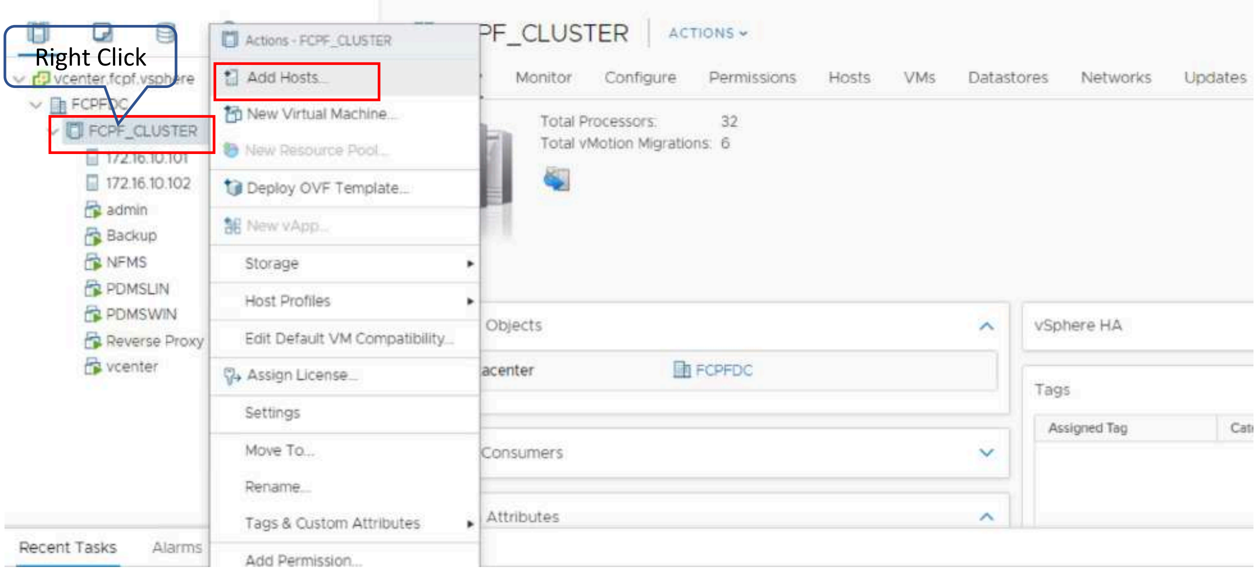
License	License Key	Product	Usage	Capacity	State
fcpf_vcenter	MJ695-AC351-R8P93-091A6-21T3N	VMware vCenter Server 6 Standard (I...	1 Instances	1 Instances	Assigned
fcpf_vsphere	4141N-8WH13-R8Z8R-0K2RM-9D32N	VMware vSphere 6 Standard (CPUs)	4 CPUs	4 CPUs	Assigned

- Cluster Configurations
  - Adding Hosts to cluster

Click on the main Menu then click “Hosts and Clusters”



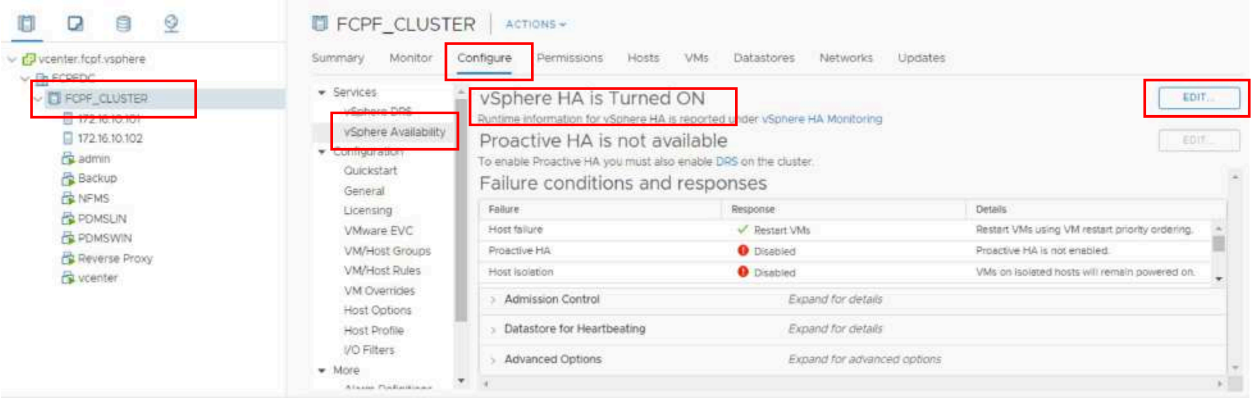
Right click on Cluster name which you want to add host to, then click on Add Hosts, then follow the instruction window.



Total Processors: 32
Total vMotion Migrations: 6

- High-Availability (HA) Configuration

VMware HA is configured to protect VMs from host failure, if system detect no response from a host, vSphere will automatically move VMs of the host to another host. To view or modify HA configuration click on the cluster, then click Configure, then vSphere Availability, then you'll see vSphere HA is Turned ON or Off, to modify its state click on Edit button.



vSphere HA is Turned ON

Runtime information for vSphere HA is reported under vSphere HA Monitoring

Proactive HA is not available

To enable Proactive HA you must also enable DRS on the cluster.

Failure conditions and responses

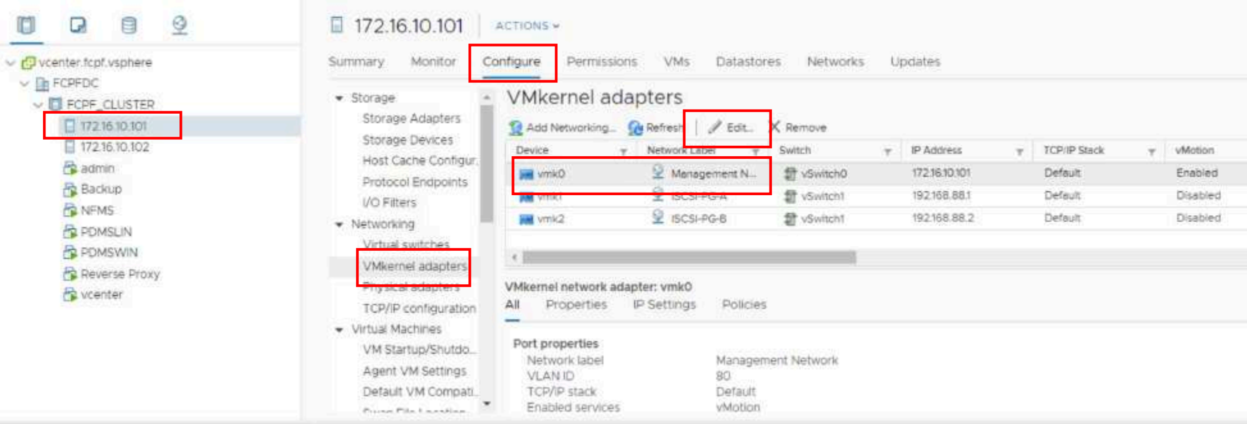
Failure	Response	Details
Host failure	✓ Restart VMs	Restart VMs using VM restart priority ordering.
Proactive HA	● Disabled	Proactive HA is not enabled.
Host isolation	● Disabled	VMs on isolated hosts will remain powered on.

Admission Control	*Expand for details*
Datastore for Heartbeating	*Expand for details*
Advanced Options	*Expand for advanced options*

- Host Configurations
  - Configure vMotion

vMtion is the key feature making it's possible to automate/move VMs across ESXi hosts, to enable vMotion make sure appropriate VMkernel Adapter is configured to enable vMotion traffic:

To view or modify vMotion configuration, click on ESXi host you which to view, then click configure, then click VMkernel Adapters, then select VMkernal you wish to check, then click Edit, Edit setting window appeared, check to enable vmotion, uncheck to disable it.



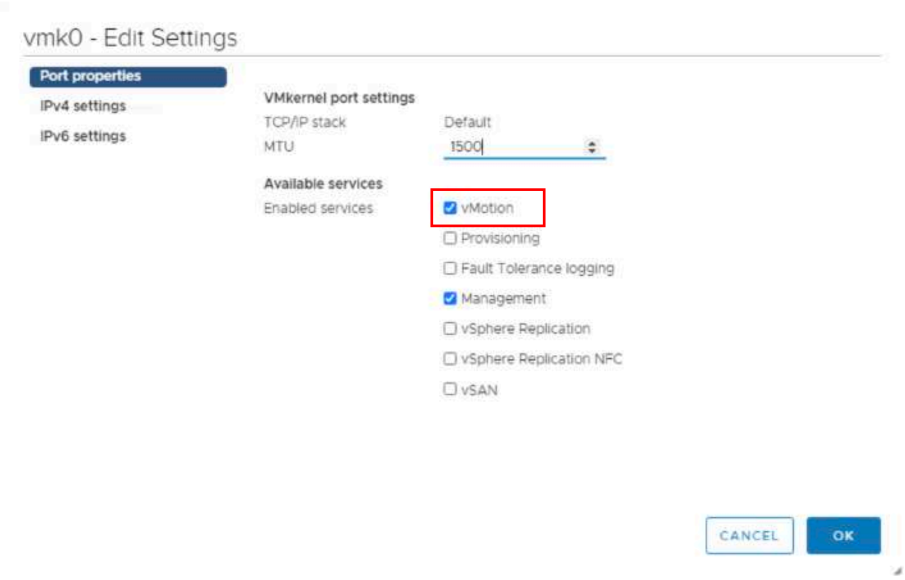
VMkernel adapters

Device	Network Label	Switch	IP Address	TCP/IP Stack	vMotion
vmk0	Management N...	vSwitch0	172.16.10.101	Default	Enabled
vmk1	ISCSI-PG-A	vSwitch1	192.168.88.1	Default	Disabled
vmk2	ISCSI-PG-B	vSwitch1	192.168.88.2	Default	Disabled

VMkernel network adapter: vmk0

Port properties

Network label	Management Network
VLAN ID	80
TCP/IP stack	Default
Enabled services	vMotion



vmk0 - Edit Settings

VMkernel port settings

TCP/IP stack Default

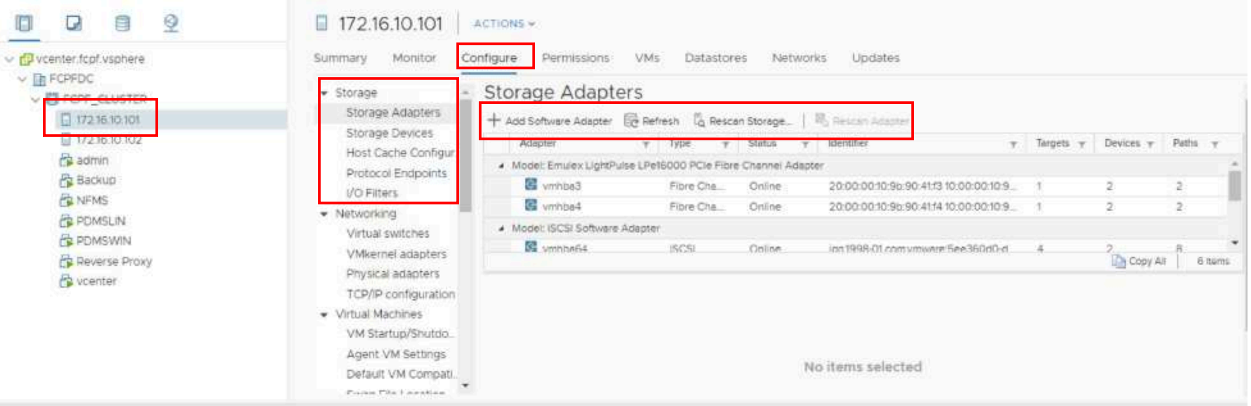
MTU 1500

Available services

Enabled services
☑ vMotion
☐ Provisioning
☐ Fault Tolerance logging
☑ Management
☐ vSphere Replication
☐ vSphere Replication NFC
☐ vSAN

- Host Storage Configurations

To view or modify storage configuration for ESXi host, click on the host you wish to view, click on configure, then click on a task under Storage.

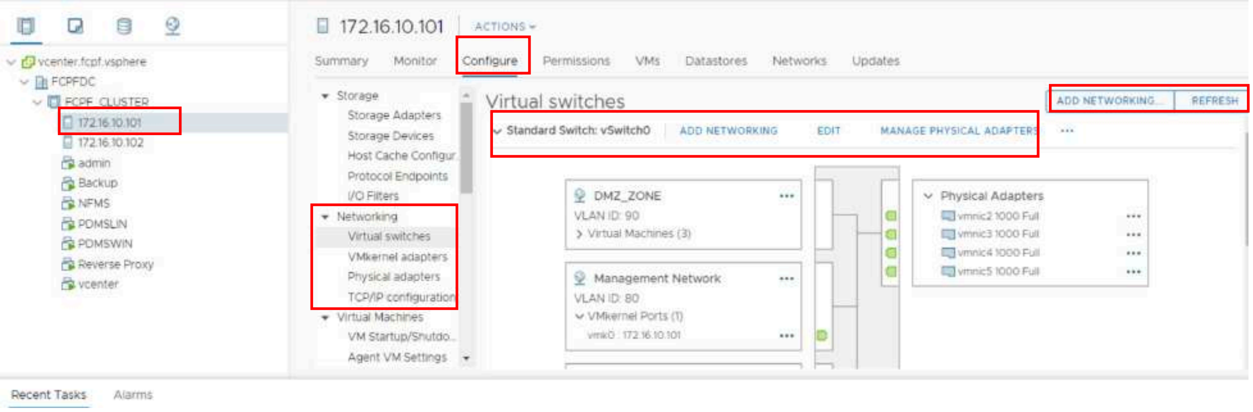


Storage Adapters

Adapter	Type	Status	Identifier	Targets	Devices	Paths
Model: Emulex LightPulse LPe16000 PCIe Fibre Channel Adapter						
vmhba3	Fibre Cha...	Online	20:00:00:10:9b:90:41:f3 10:00:00:10:9...	1	2	2
vmhba4	Fibre Cha...	Online	20:00:00:10:9b:90:41:f4 10:00:00:10:9...	1	2	2
Model: iSCSI Software Adapter						
vmhba64	iSCSI	Online	iqn.1998-01.com.vmware:5ee360d0-d...	4	2	8

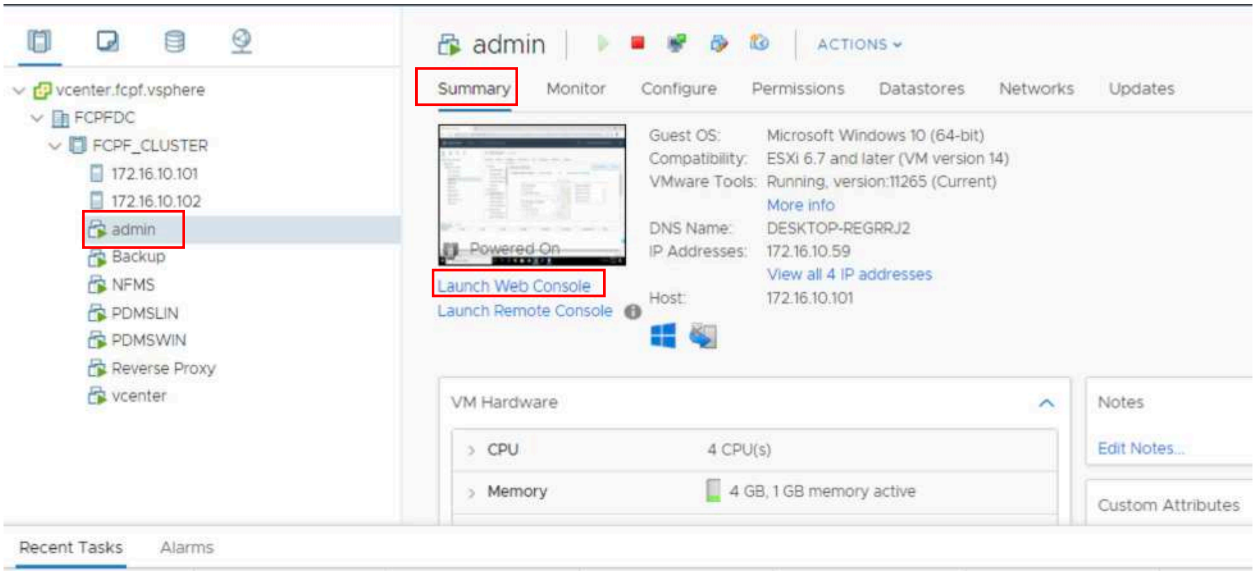
- Host Network Configurations

To view or modify network configuration for ESXi host, click on the host you wish to view, click on configure, then click on a task under Networking.



- VM Operations
  - Accessing VM

    We can access a VM by clicking the on the VM, then Summary, then Launch Web Console

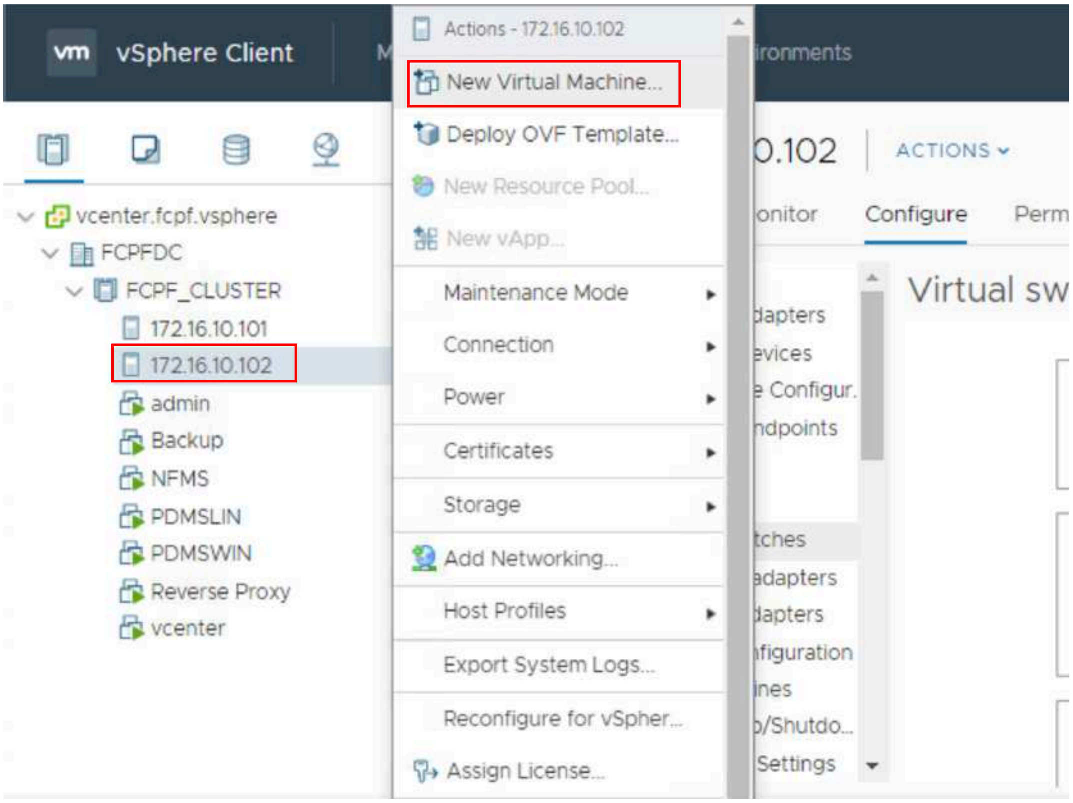


Guest OS: Microsoft Windows 10 (64-bit)
Compatibility: ESXi 6.7 and later (VM version 14)
VMware Tools: Running, version:11265 (Current)
DNS Name: DESKTOP-REGRRJ2
IP Addresses: 172.16.10.59
Host: 172.16.10.101

CPU 4 CPU(s)
Memory 4 GB, 1 GB memory active

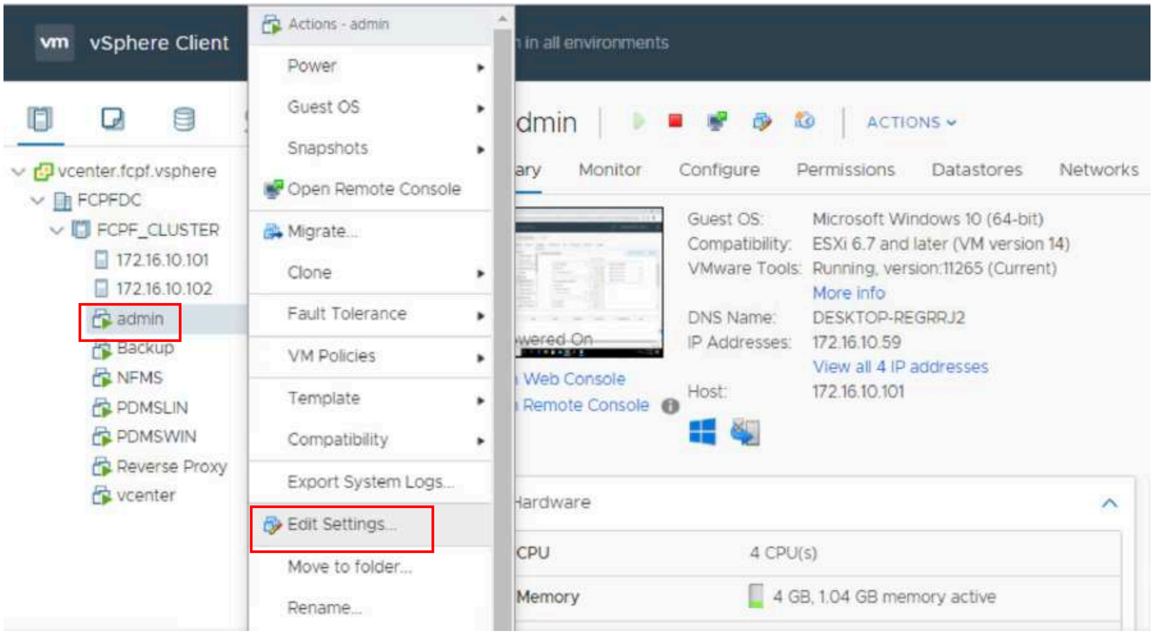
  - Create New VM

    To create new VM, right click on the host you wish to create new VM on, then click New Virtual Machine, then follow instruction window to complete VM creation.



- Edit VM Settings

To edit VM's settings, right click on the VM you wish to edit, then click Edit settings

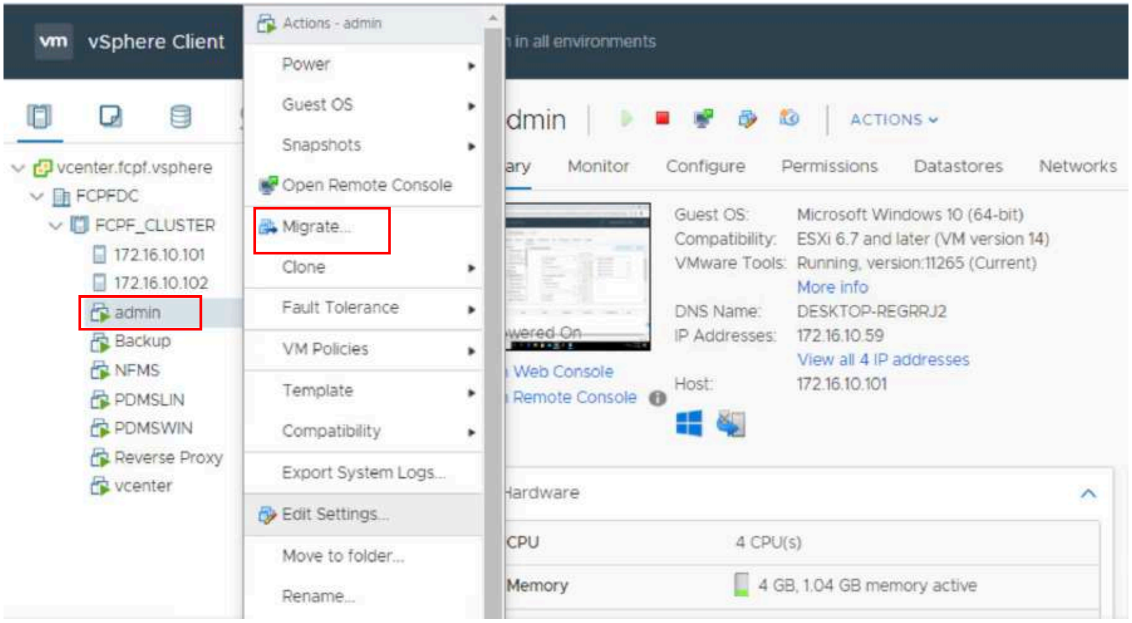


Guest OS: Microsoft Windows 10 (64-bit)
Compatibility: ESXi 6.7 and later (VM version 14)
VMware Tools: Running, version:11265 (Current)
DNS Name: DESKTOP-REGRRJ2
IP Addresses: 172.16.10.59
Host: 172.16.10.101

CPU 4 CPU(s)
Memory 4 GB, 1.04 GB memory active

- Migrate VM

To migrate VM from one host to the other, right click on the VM you wish to move, then click Migrate, select appropriate host then click on to complete the movement.

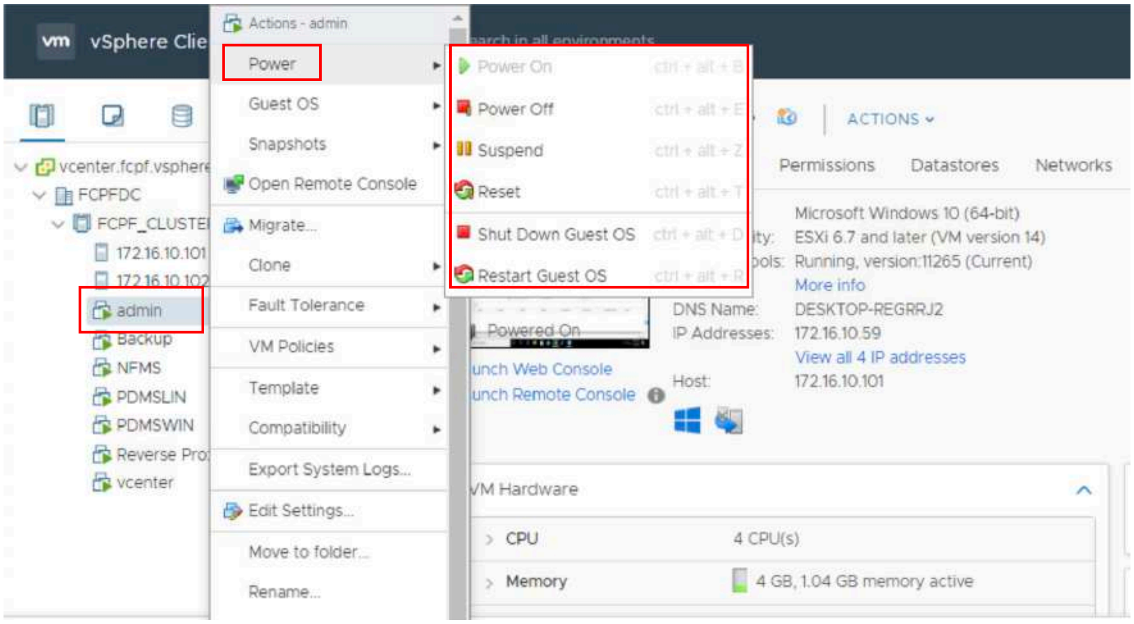


Guest OS: Microsoft Windows 10 (64-bit)
Compatibility: ESXi 6.7 and later (VM version 14)
VMware Tools: Running, version:11265 (Current)
DNS Name: DESKTOP-REGRRJ2
IP Addresses: 172.16.10.59
Host: 172.16.10.101

CPU	4 CPU(s)
Memory	4 GB, 1.04 GB memory active

- Power On/Off the VM

To power on/off VM, right click on the VM, then select Power, then select appropriate action you wish to perform.



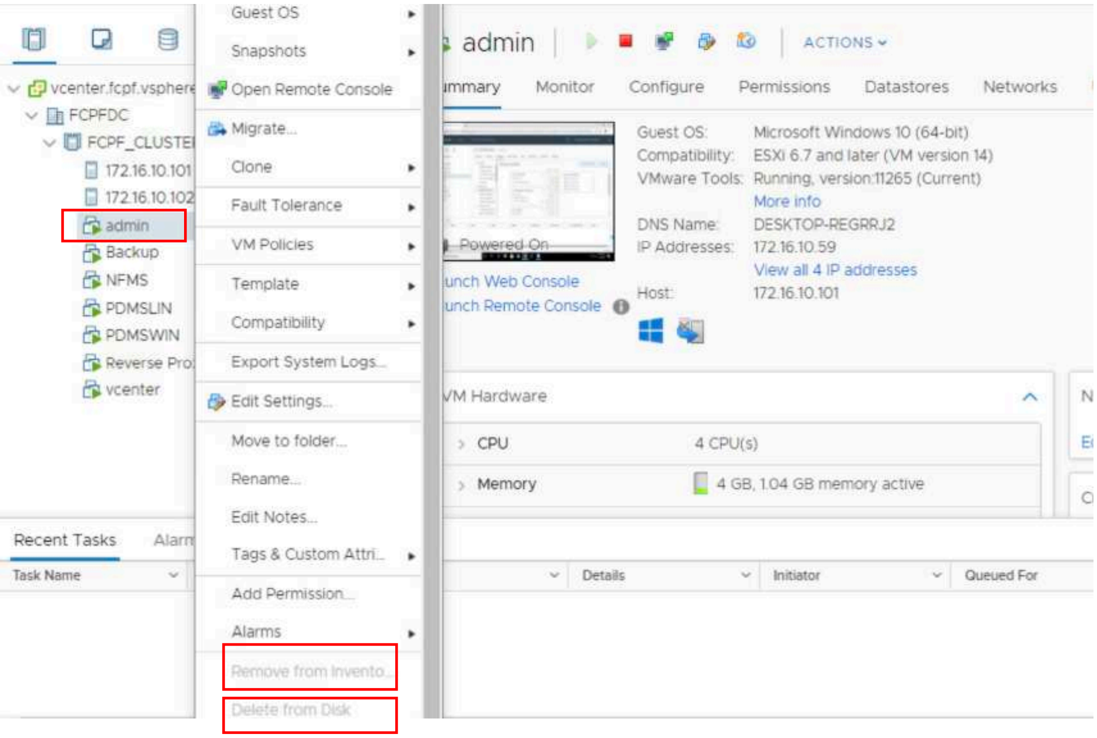
ity: ESXi 6.7 and later (VM version 14)
ools: Running, version:11265 (Current)
Microsoft Windows 10 (64-bit)
DNS Name: DESKTOP-REGRRJ2
IP Addresses: 172.16.10.59
Host: 172.16.10.101

CPU	4 CPU(s)
Memory	4 GB, 1.04 GB memory active

- Delete/Remove VM

To remove VM from management interface but keep its files in the storage, right click on the VM, then click on Remove from Inventory.

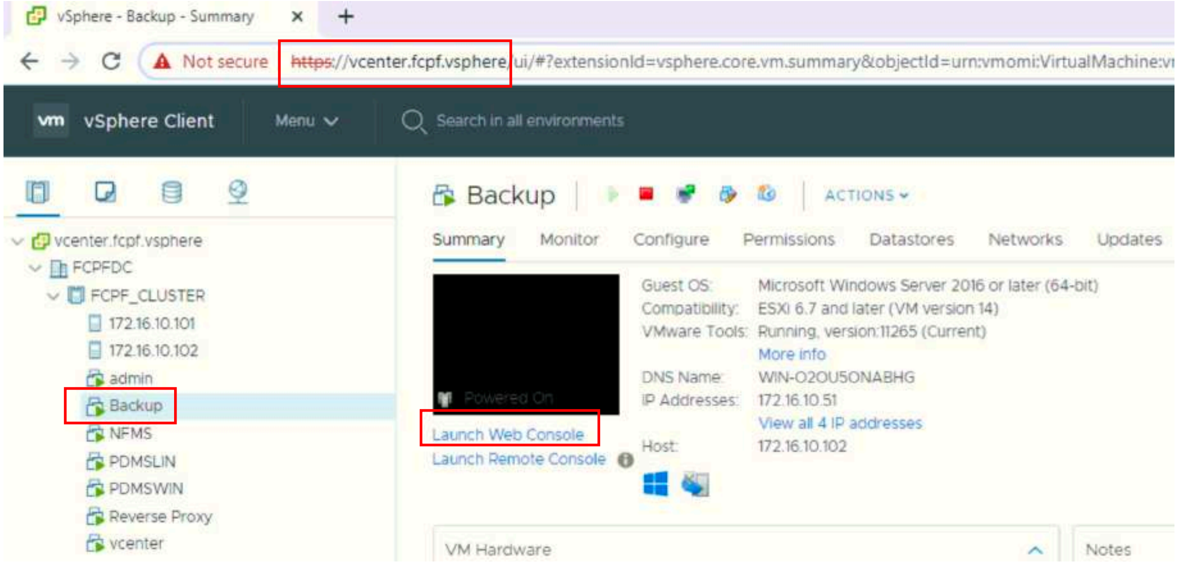
To permanently delete VM from management interface and delete its files from storage, right click on the VM, then click on Delete from disk



5 Monitor Backup (Daily)

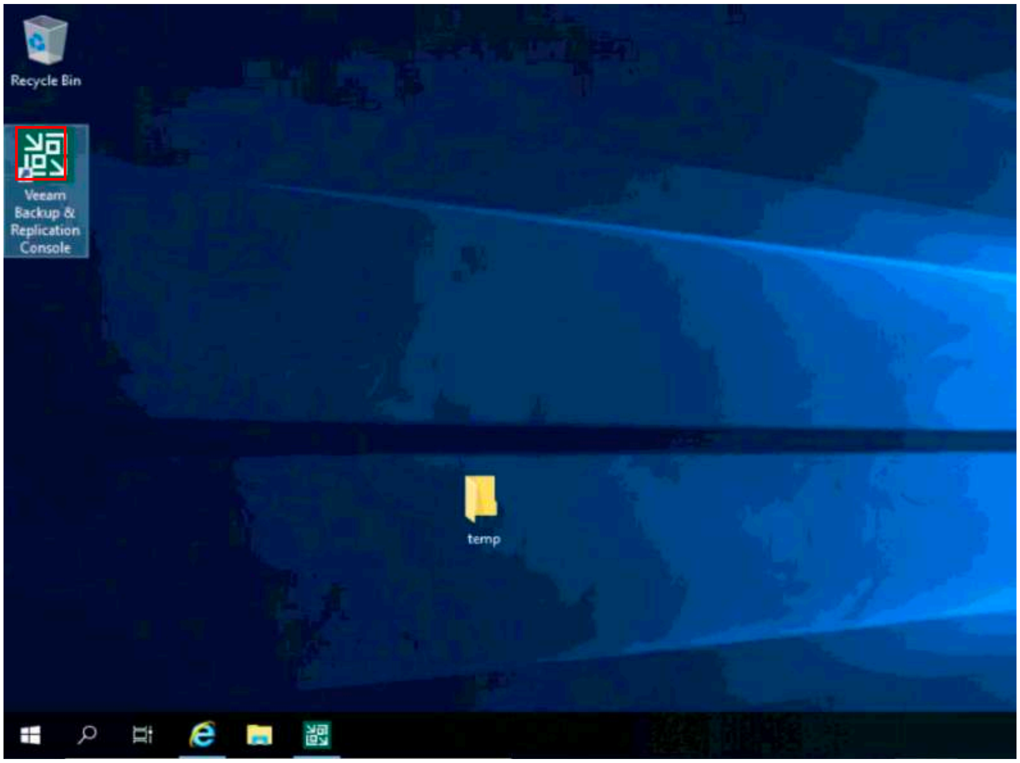
Backup server is a Virtual Machine created in FCPF_CLUSTER, but the backup server is only hosting backup software/application, backup data store in a shared folder in 2 x NAS storage.

we can access the backup server from vCenter Web interface, first you need to be in FIPD vlans to login to a computer in FIPD vlans, then open your web browser and fill the address bar with https://vcenter.fcpf.vsphere fill login credential and click login. Click Menu->Hosts and Clusters, the click VM named “Backup” then click on “Launch Web Console”

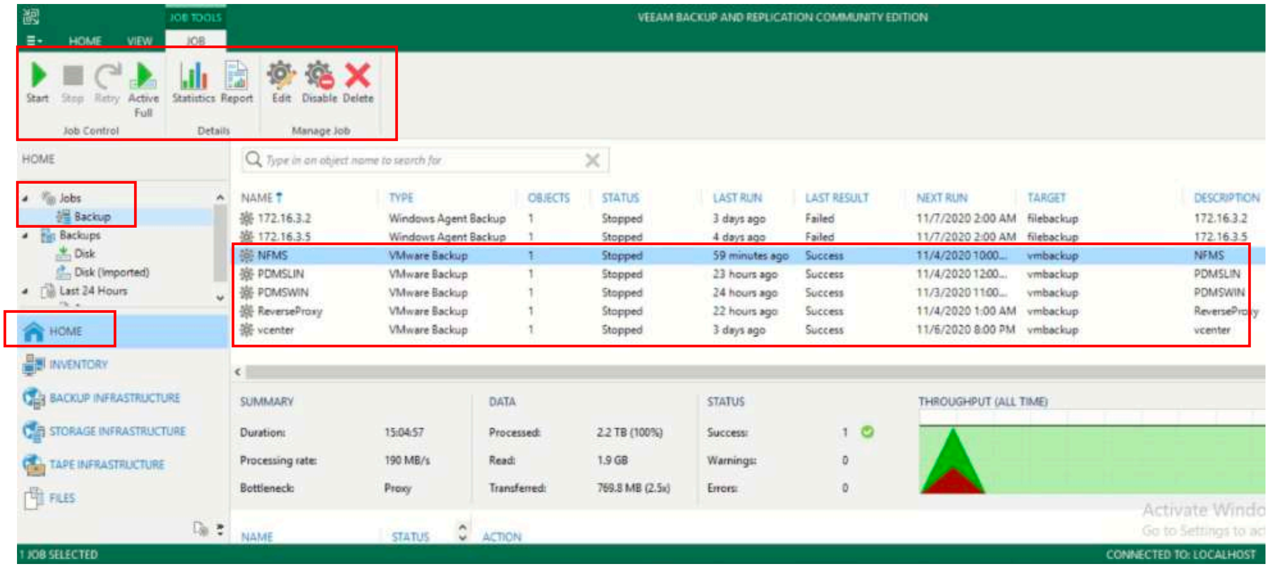


Guest OS: Microsoft Windows Server 2016 or later (64-bit)
Compatibility: ESXi 6.7 and later (VM version 14)
VMware Tools: Running, version:11265 (Current)
DNS Name: WIN-O2OU5ONABHG
IP Addresses: 172.16.10.51
Host: 172.16.10.102

Login to windows below screen is displayed, open Veeam Backup and Replication.



To view, modify or create new backup job, navigate to Home->Jobs->Backup, then on the right hand window displayed list of existing backup jobs, click on a job and choose preferred action from menu above:

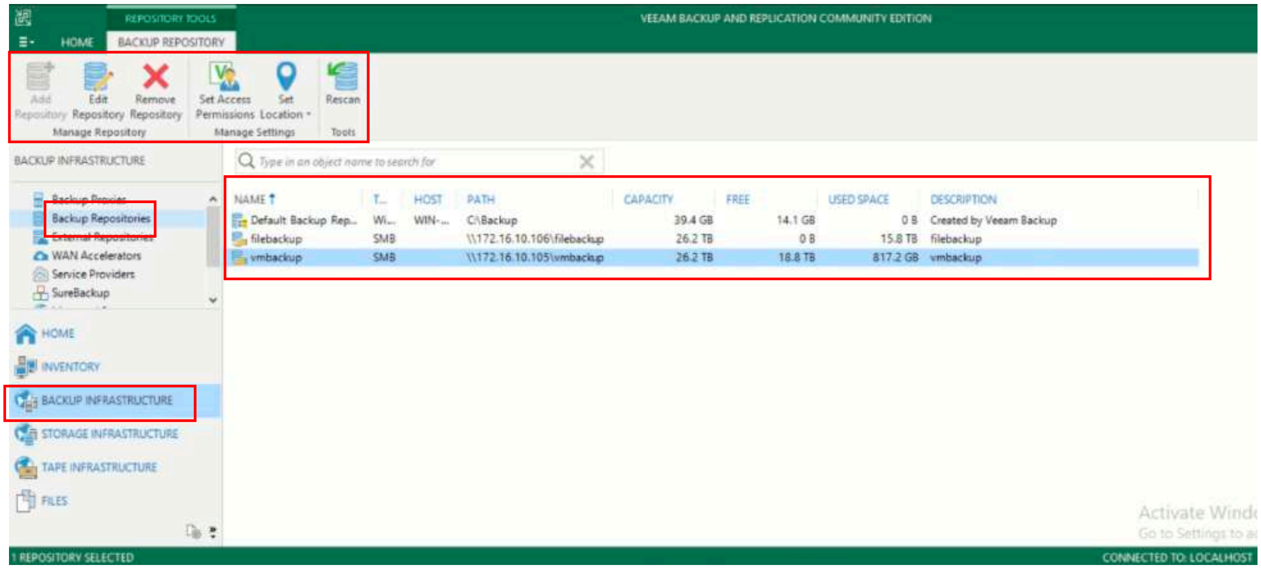


NAME	TYPE	OBJECTS	STATUS	LAST RUN	LAST RESULT	NEXT RUN	TARGET	DESCRIPTION
172.16.3.2	Windows Agent Backup	1	Stopped	3 days ago	Failed	11/7/2020 2:00 AM	filebackup	172.16.3.2
172.16.3.5	Windows Agent Backup	1	Stopped	4 days ago	Failed	11/7/2020 2:00 AM	filebackup	172.16.3.5
NFMS	VMware Backup	1	Stopped	59 minutes ago	Success	11/4/2020 10:00...	vmbackup	NFMS
PDMSLIN	VMware Backup	1	Stopped	23 hours ago	Success	11/4/2020 12:00...	vmbackup	PDMSLIN
PDMSWIN	VMware Backup	1	Stopped	24 hours ago	Success	11/3/2020 11:00...	vmbackup	PDMSWIN
ReverseProxy	VMware Backup	1	Stopped	22 hours ago	Success	11/4/2020 1:00 AM	vmbackup	ReverseProxy
vcenter	VMware Backup	1	Stopped	3 days ago	Success	11/6/2020 8:00 PM	vmbackup	vcenter

SUMMARY		DATA		STATUS	
Duration:	15:04:57	Processed:	2.2 TB (100%)	Success:	1 ✓
Processing rate:	190 MB/s	Read:	1.9 GB	Warnings:	0
Bottleneck:	Proxy	Transferred:	769.8 MB (2.5x)	Errors:	0

NAME	STATUS	ACTION

To view, modify or create new backup destination (backup data storage), click on BACKUP INFRASTRUCTURE, then click Backup Repositories, then on the right hand window displayed list of existing backup repositories, click on a repository and choose your preferred action from menu above:

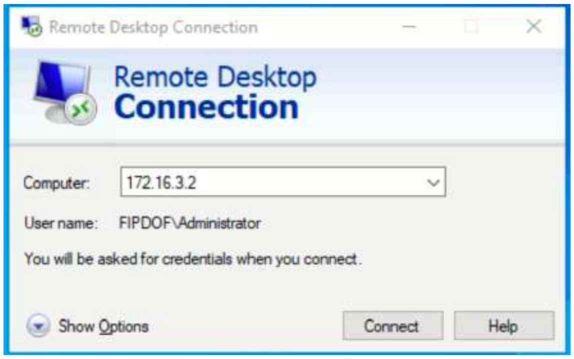


NAME	T...	HOST	PATH	CAPACITY	FREE	USED SPACE	DESCRIPTION
Default Backup Rep...	Wi...	WIN-...	C:\Backup	39.4 GB	14.1 GB	0 B	Created by Veeam Backup
filebackup	SMB		\\172.16.10.106\filebackup	26.2 TB	0 B	15.8 TB	filebackup
vmbackup	SMB		\\172.16.10.105\vmbackup	26.2 TB	18.8 TB	817.2 GB	vmbackup

6 Other Systems Administration

6.1 DNS Configuration

Accessing FIPD DNS server, first you'll need to be in FIPD vlans or login to a computer in FIPD vlans, then using MS remote desktop to login to DNS server.



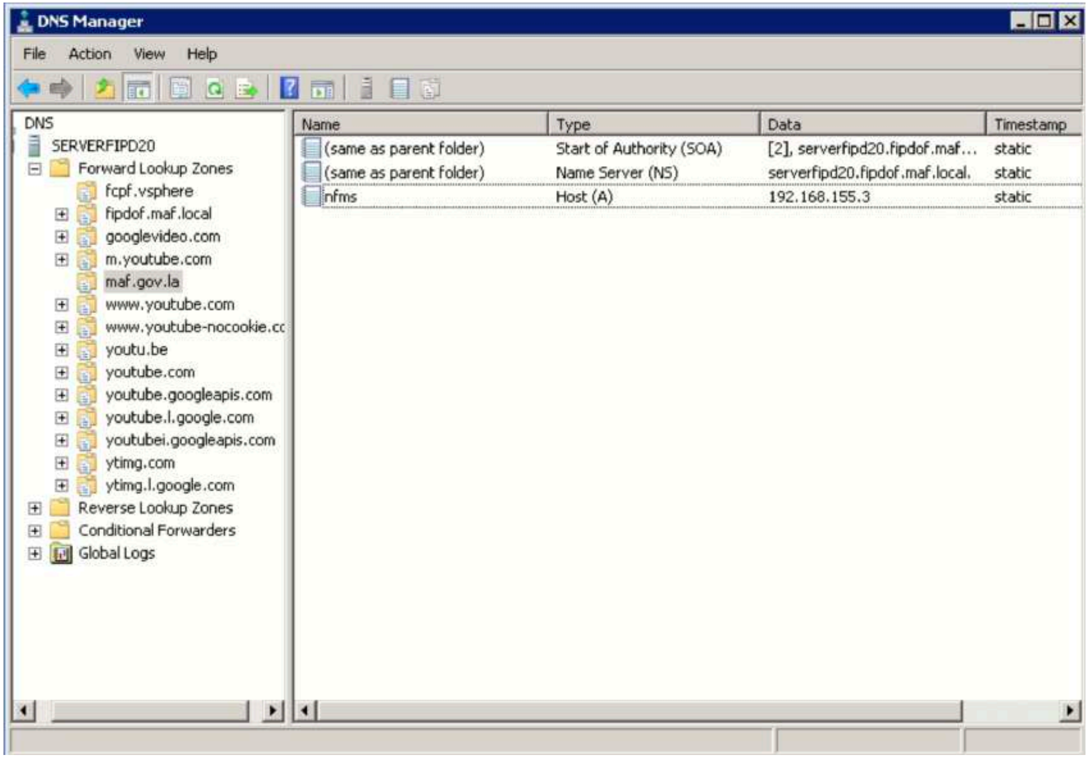
Computer: 172.16.3.2

User name: FIPDOF\Administrator

You will be asked for credentials when you connect.

- Local DNS configuration for nfms.maf.gov.la

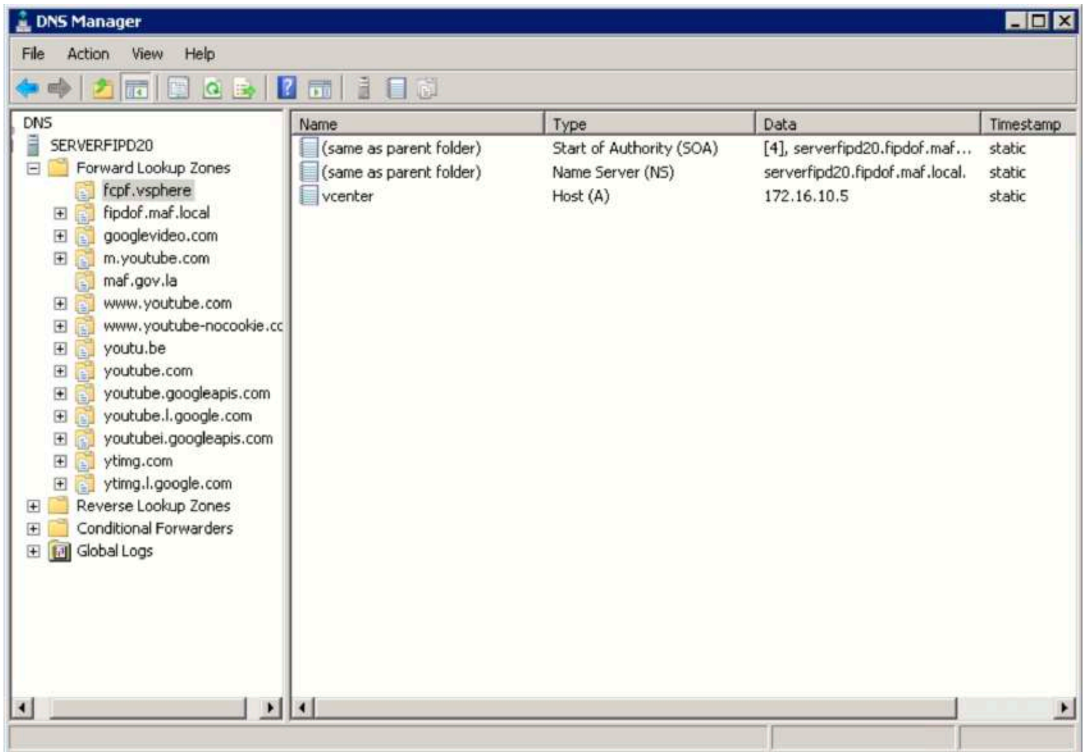
When logged in to DNS server, open DNS management console, then locate Forward Lookup zone, then look for maf.gov.la and click on it, on the right hand window you'll see nfms, currently it's pointing to 192.168.155.3



Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[2], serverfipd20.fipdof.maf...	static
(same as parent folder)	Name Server (NS)	serverfipd20.fipdof.maf.local.	static
nfms	Host (A)	192.168.155.3	static

- Local DNS configuration for vCenter

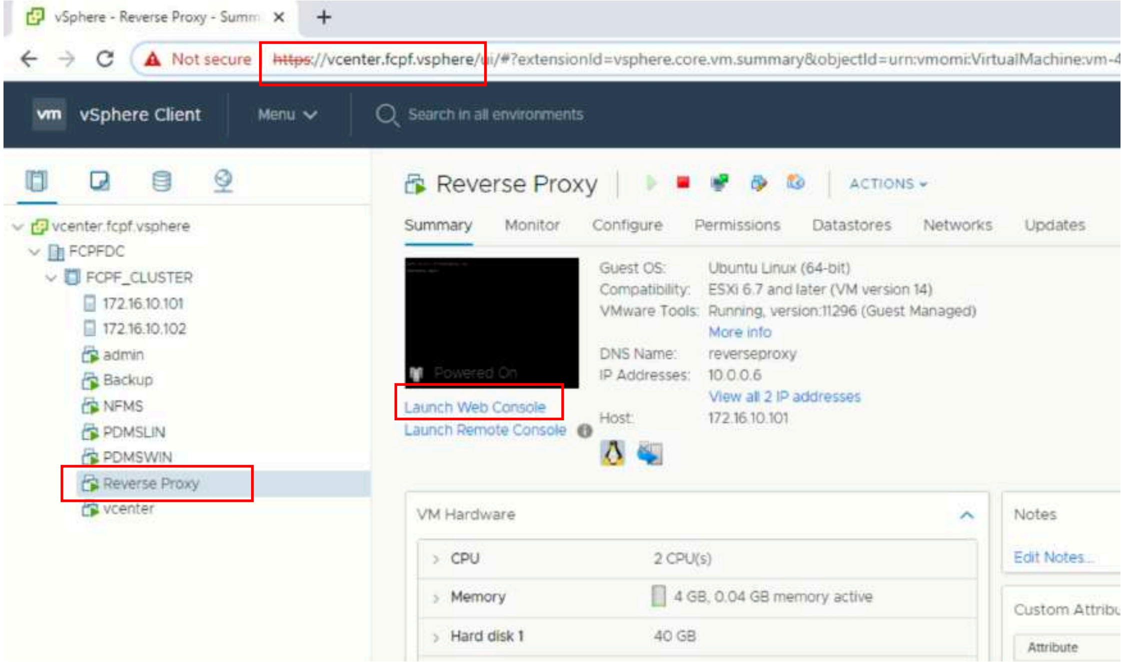
When logged in to DNS server, open DNS management console, then locate Forward Lookup zone, then look for fcpf.vsphere and click on it, on the right hand window you'll see nfms, currently it's pointing to 172.16.10.5



Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[4], serverfipd20.fipdof.maf...	static
(same as parent folder)	Name Server (NS)	serverfipd20.fipdof.maf.local.	static
vcenter	Host (A)	172.16.10.5	static

6.2 Reverse Proxy Configuration

Reverse proxy server is a Virtual Machine created in FCPF_CLUSTER, we can access the reverse proxy server from vCenter Web interface

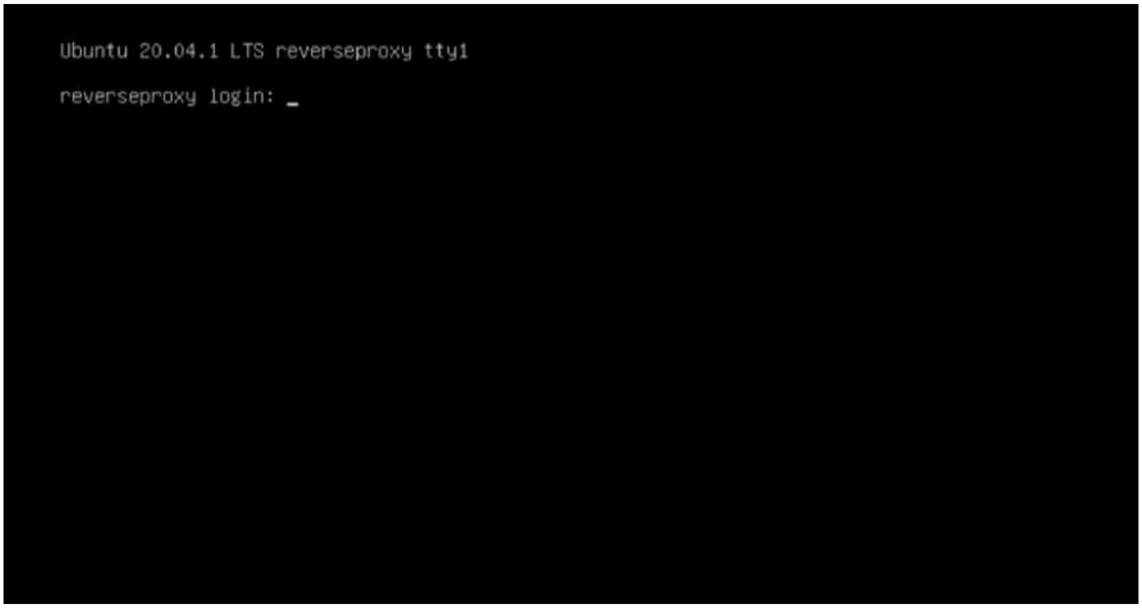


https://vcenter.fcpf.vsphere/ui/#?extensionId=vsphere.core.vm.summary&objectId=urn:vmomi:VirtualMachine:vm-4

Guest OS: Ubuntu Linux (64-bit)
Compatibility: ESXi 6.7 and later (VM version 14)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: reverseproxy
IP Addresses: 10.0.0.6
Host: 172.16.10.101

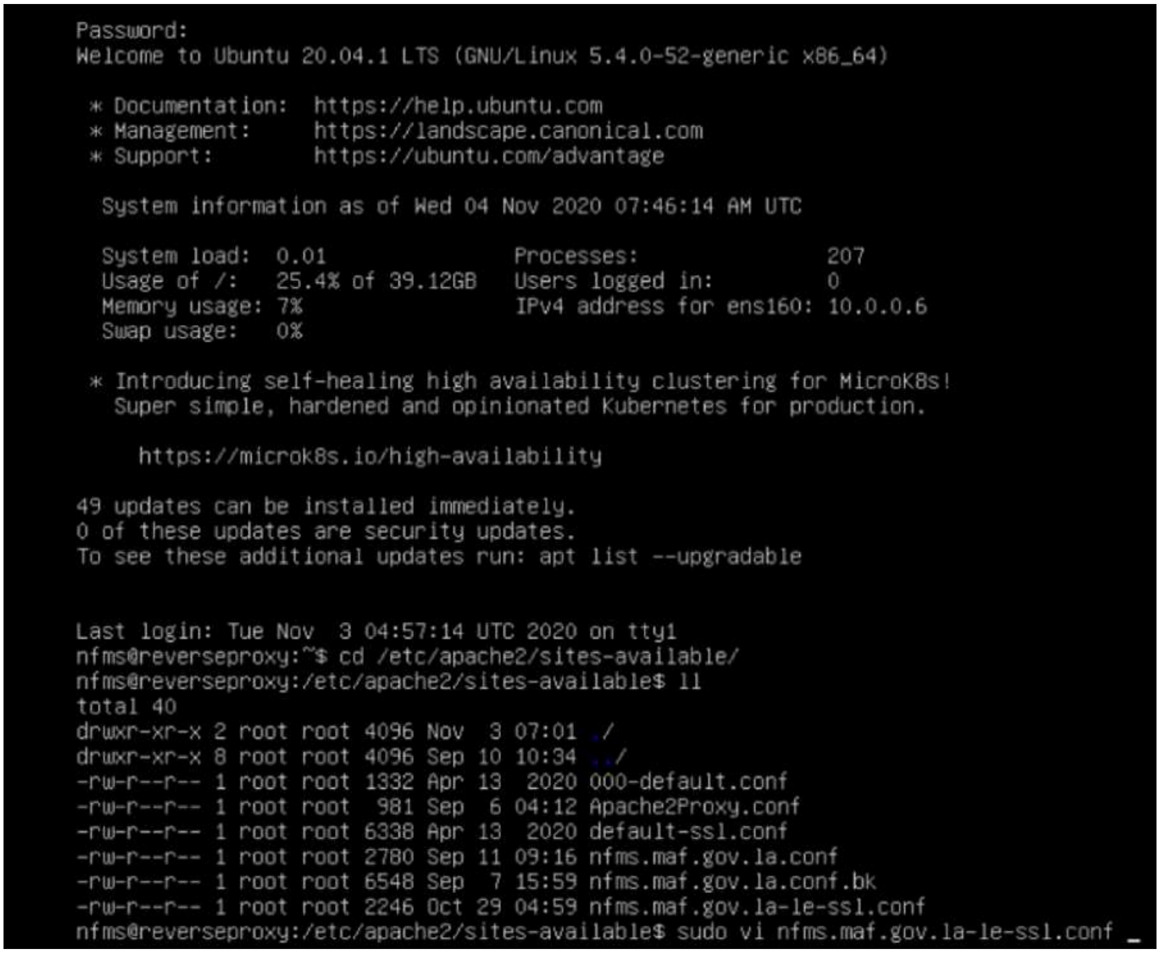
CPU	2 CPU(s)
Memory	4 GB, 0.04 GB memory active
Hard disk 1	40 GB

Then login with the credentials:



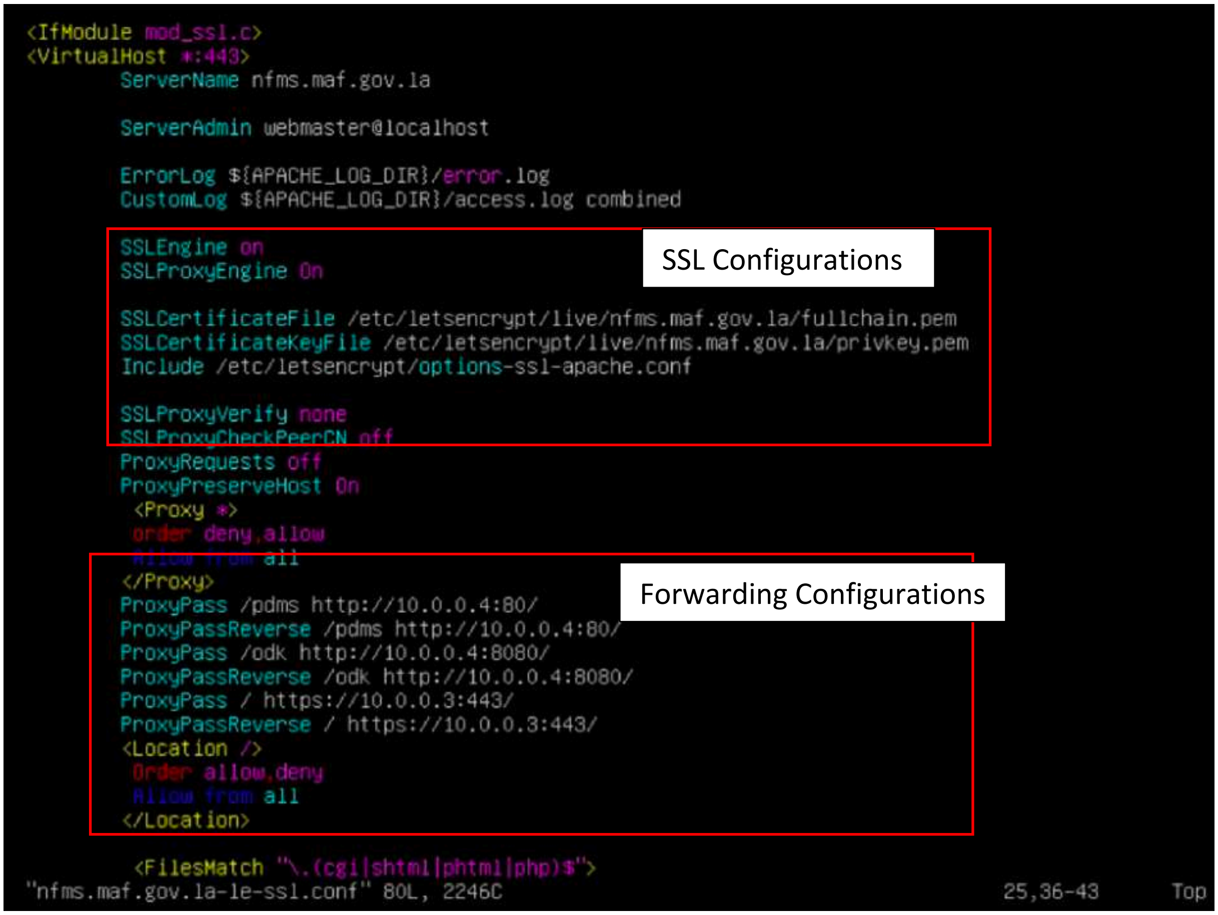
```
Ubuntu 20.04.1 LTS reverseproxy tty1

reverseproxy login: _
```

After logged in cd to: ***//etc/apache2/sites-availables/***
Then open a configuration file using command: ***sudo vi nfms.maf.gov.la-le-ssl.conf***



```
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-52-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed 04 Nov 2020 07:46:14 AM UTC

  System load:  0.01              Processes:              207
  Usage of /:   25.4% of 39.12GB  Users logged in:        0
  Memory usage: 7%                IPv4 address for ens160: 10.0.0.6
  Swap usage:   0%

 * Introducing self-healing high availability clustering for MicroK8s!
   Super simple, hardened and opinionated Kubernetes for production.

     https://microk8s.io/high-availability

49 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable


Last login: Tue Nov  3 04:57:14 UTC 2020 on tty1
nfms@reverseproxy:~$ cd /etc/apache2/sites-available/
nfms@reverseproxy:/etc/apache2/sites-available$ ll
total 40
drwxr-xr-x 2 root root 4096 Nov  3 07:01 ./
drwxr-xr-x 8 root root 4096 Sep 10 10:34 ../
-rw-r--r-- 1 root root 1332 Apr 13  2020 000-default.conf
-rw-r--r-- 1 root root  981 Sep  6 04:12 Apache2Proxy.conf
-rw-r--r-- 1 root root 6338 Apr 13  2020 default-ssl.conf
-rw-r--r-- 1 root root 2780 Sep 11 09:16 nfms.maf.gov.la.conf
-rw-r--r-- 1 root root 6548 Sep  7 15:59 nfms.maf.gov.la.conf.bk
-rw-r--r-- 1 root root 2246 Oct 29 04:59 nfms.maf.gov.la-le-ssl.conf
nfms@reverseproxy:/etc/apache2/sites-available$ sudo vi nfms.maf.gov.la-le-ssl.conf _
```

Ssl configrations and forwarding configurations are in this file



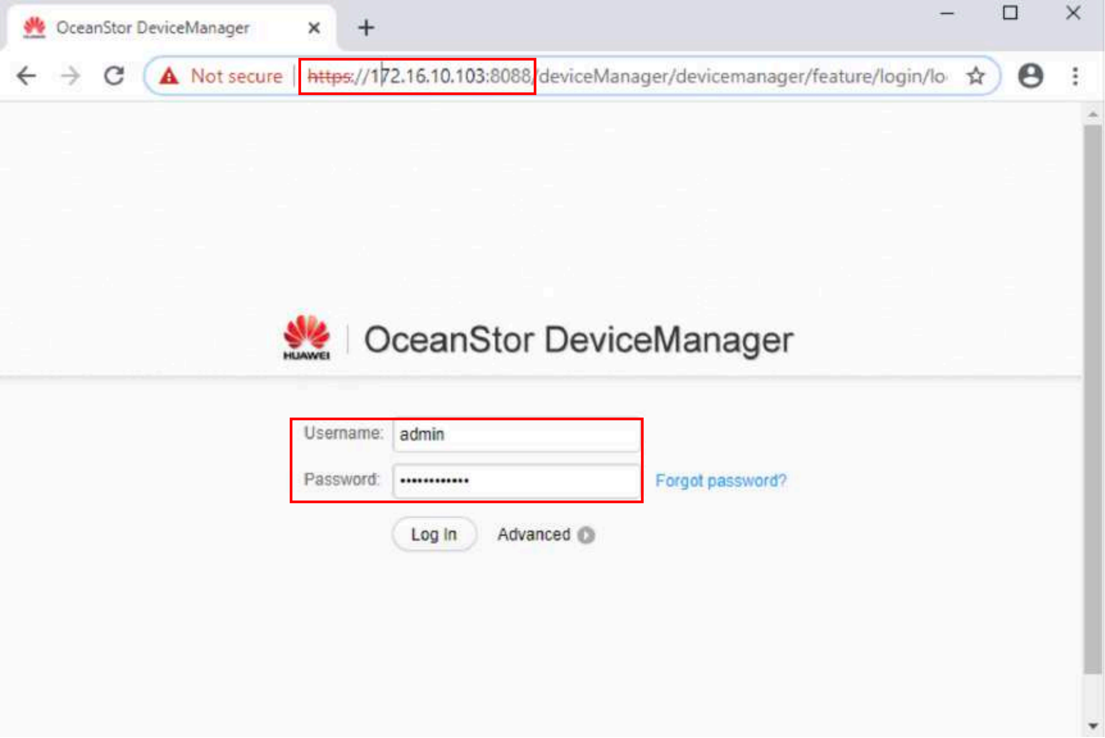
```
<IfModule mod_ssl.c>
<VirtualHost *:443>
        ServerName nfms.maf.gov.la

        ServerAdmin webmaster@localhost

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        SSLEngine on
        SSLProxyEngine On

        SSLCertificateFile /etc/letsencrypt/live/nfms.maf.gov.la/fullchain.pem
        SSLCertificateKeyFile /etc/letsencrypt/live/nfms.maf.gov.la/privkey.pem
        Include /etc/letsencrypt/options-ssl-apache.conf

        SSLProxyVerify none
        SSLProxyCheckPeerCN off
        ProxyRequests off
        ProxyPreserveHost On
         <Proxy *>
         order deny,allow
         Allow from all
        </Proxy>
        ProxyPass /pdms http://10.0.0.4:80/
        ProxyPassReverse /pdms http://10.0.0.4:80/
        ProxyPass /odk http://10.0.0.4:8080/
        ProxyPassReverse /odk http://10.0.0.4:8080/
        ProxyPass / https://10.0.0.3:443/
        ProxyPassReverse / https://10.0.0.3:443/
        <Location />
         Order allow,deny
         Allow from all
        </Location>

         <FilesMatch "\.(cgi|shtml|phtml|php)$">
"nfms.maf.gov.la-le-ssl.conf" 80L, 2246C                          25,36-43      Top
```

7 Storage Administration

7.1 SAN Configuration

- Accessing SAN

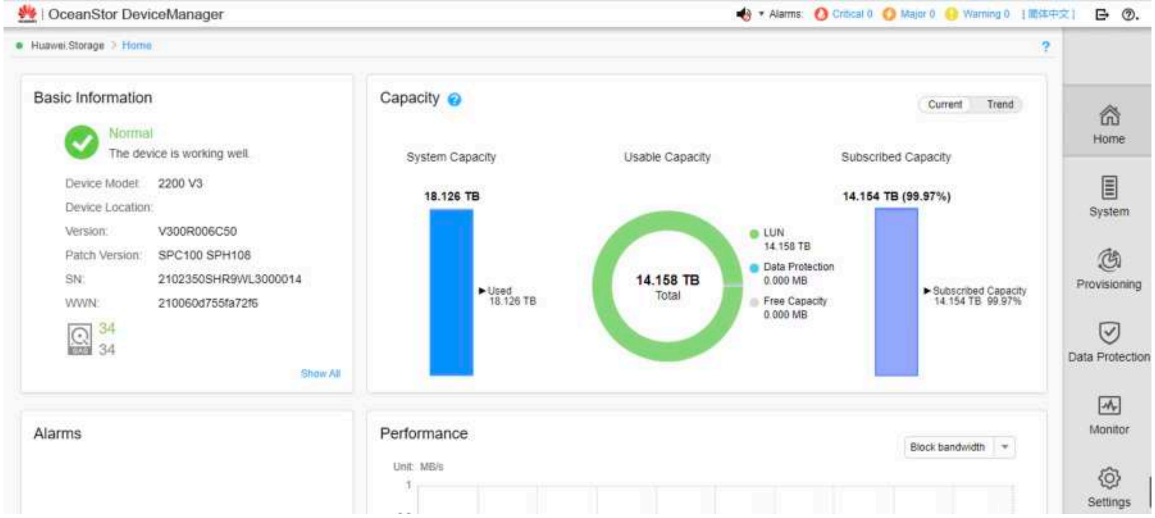
First you'll need to be in FIPD vlans or login to a computer in FIPD vlans, then open your web browser, fill in the address bar with https://172.16.10.103:8088, then fill in login credentials:



~~https~~://172.16.10.103:8088/deviceManager/devicemanager/feature/login/lo

Username: admin

Password: •••••••••••••

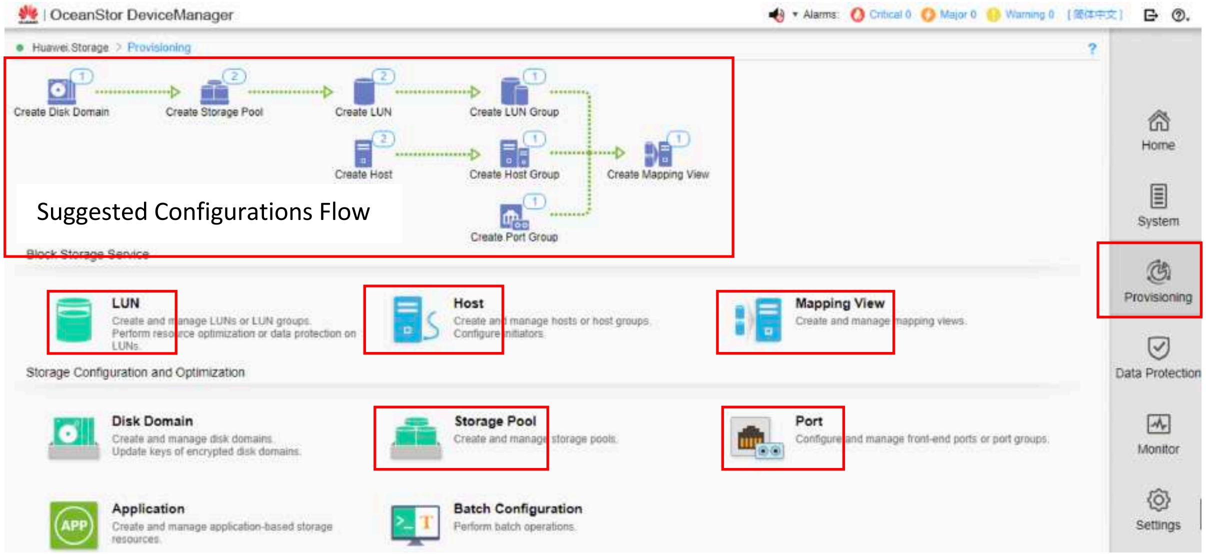


Basic Information

Normal
The device is working well.

Device Model: 2200 V3
Device Location:
Version: V300R006C50
Patch Version: SPC100 SPH108
SN: 2102350SHR9WL3000014
WWN: 210060d755fa72f6

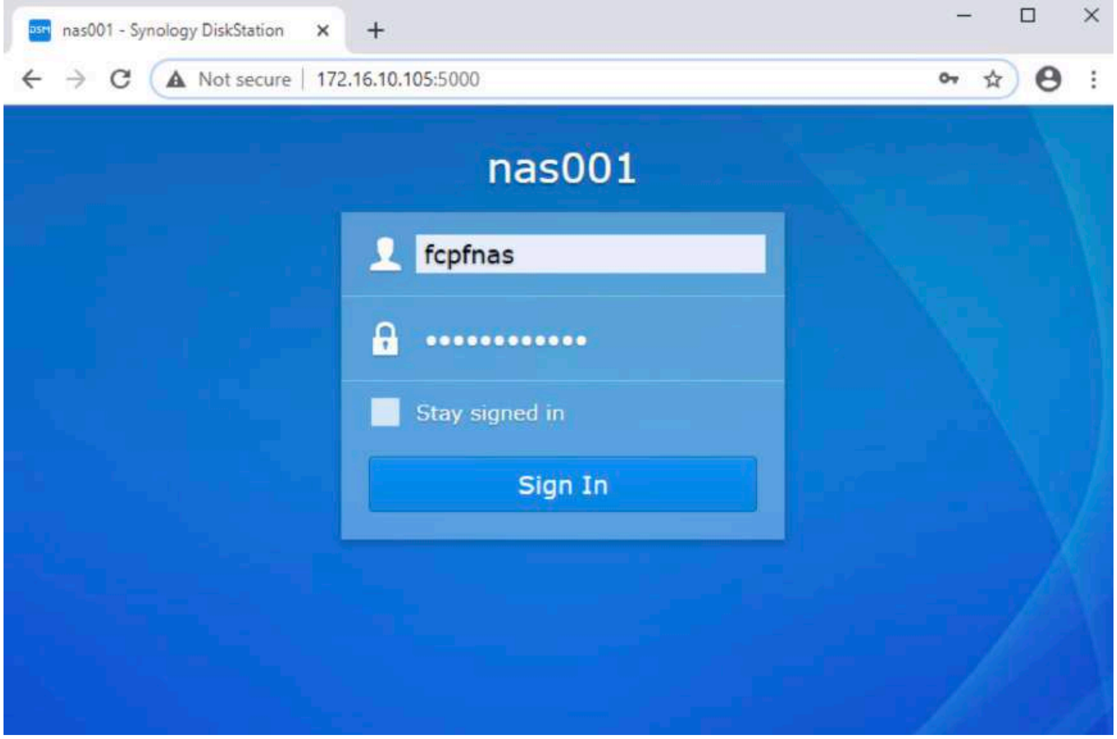
After logged in, click on Provisioning, most relevant configurations are in this page.


OceanStor DeviceManager
Alarms: Critical 0 Major 0 Warning 0 [简体中文]
Huawei Storage > Provisioning
Create Disk Domain
Create Storage Pool
Create LUN
Create LUN Group
Create Host
Create Host Group
Create Mapping View
Create Port Group
Block Storage Service
LUN
Create and manage LUNs or LUN groups. Perform resource optimization or data protection on LUNs.
Host
Create and manage hosts or host groups. Configure initiators.
Mapping View
Create and manage mapping views.
Storage Configuration and Optimization
Disk Domain
Create and manage disk domains. Update keys of encrypted disk domains.
Storage Pool
Create and manage storage pools.
Port
Configure and manage front-end ports or port groups.
Application
Create and manage application-based storage resources.
Batch Configuration
Perform batch operations.
Home
System
Provisioning
Data Protection
Monitor
Settings

Suggested Configurations Flow

7.2 NAS Configuration

Accessing NAS storage, first you'll need to be in FIPD vlans or login to a computer in FIPD vlans, then open your web browser and fill in the address bar with http://172.16.10.105:5000 for NAS1 and http://172.16.10.106:5000 for NAS2, then fill in the login credentials:



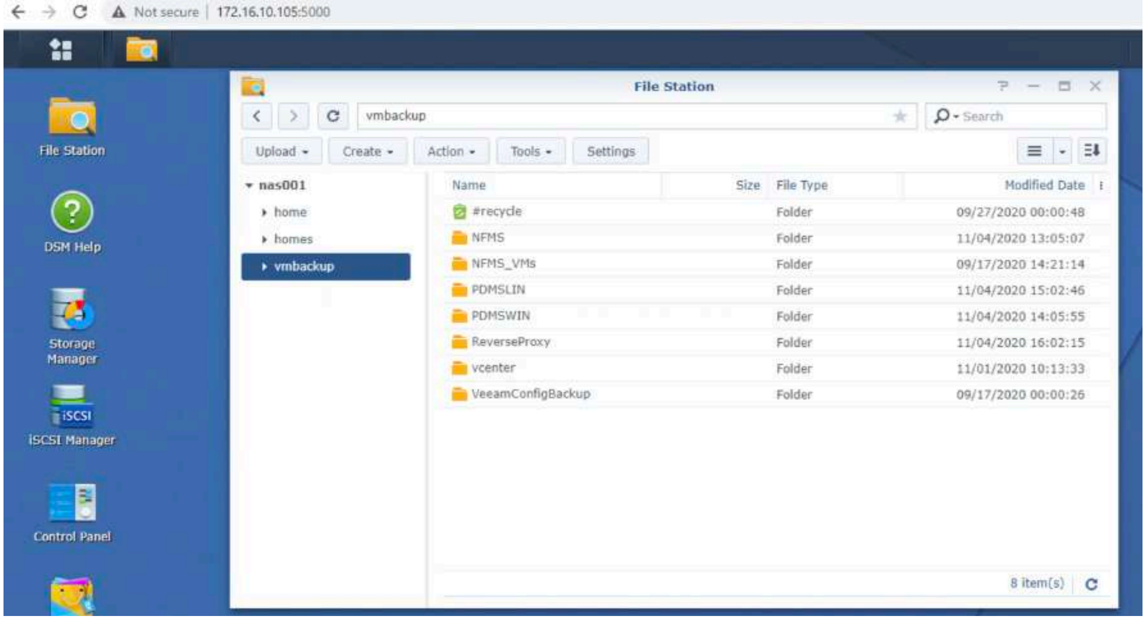
172.16.10.105:5000

fcpfnas

●●●●●●●●●●●●

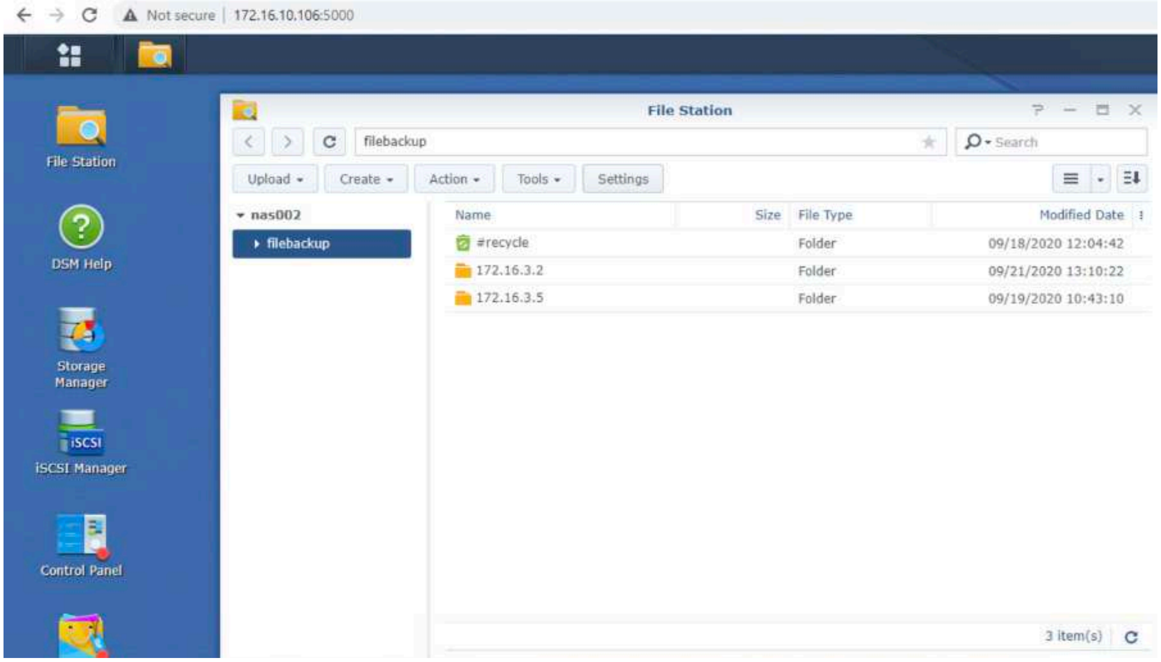
Since NAS is only configured as shared folder to store backup date, therefore relevant configuration is only creation of shared folder

Shared folder in NAS1, click on File Station and you'll see vmbackup, it's a shared folder created to store backup data of Virtual Machines in side NFMS Virtual Infrastructure.



Name	Size	File Type	Modified Date
#recycle		Folder	09/27/2020 00:00:48
NFMS		Folder	11/04/2020 13:05:07
NFMS_VMs		Folder	09/17/2020 14:21:14
PDMSLIN		Folder	11/04/2020 15:02:46
PDMSWIN		Folder	11/04/2020 14:05:55
ReverseProxy		Folder	11/04/2020 16:02:15
vcenter		Folder	11/01/2020 10:13:33
VeeamConfigBackup		Folder	09/17/2020 00:00:26

Shared folder in NAS2, click on File Station and you'll see filebackup, it's a shared folder created to store backup data of FIPD servers.



Name	Size	File Type	Modified Date
#recycle		Folder	09/18/2020 12:04:42
172.16.3.2		Folder	09/21/2020 13:10:22
172.16.3.5		Folder	09/19/2020 10:43:10