NFMS Server And Network Standard Operating Procedure

Table of Contents

1	Infr	astructure Overview	2
	1.1	FIPD Network	. 2
	1.2	NFMS Servers and Network Infrastructure	. 3
2	NFN	1S Hardware Monitoring	4
	2.1	Physical Monitoring	. 4
3	NFN	15 Network	4
	3.1	Firewall Palo Alto PA-2200	. 4
	3.2	Core Switch	14
4	Virt	ual Machine Administration	19
5	Мог	nitor Backup (Daily)	29
6	Oth	er Systems Administration	31
	6.1	DNS Configuration	31
	6.2	Reverse Proxy Configuration	33
7	Stor	age Administration	35
	7.1	SAN Configuration	35
	7.2	NAS Configuration	37

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:

←→	C A Not sec	ure https://17	72.16.10.2/php/login.php	¢
			paloalto	
			NETWORKS®	
		Username		
		Password		
			Log In	

Fill in login credentials and click login

\leftrightarrow \rightarrow G	A Not secure 172.16.10.2/php/login.php
	m paloalto
	NETWORKS®
	Username admin
	Password
	Log In

That's all, you're now inside the web management interface as below: $\leftarrow \rightarrow \mathbb{C}$ A Not secure | 172.16.10.2/#dashboard:vsys1

☆ **0** :

paloalto	Dashboard ACC	Monitor Policies Obje	ects Network	k Device & Commit & Q	Config - Q Search
	Layout 3 Columns	👻 📓 Widgets 🔹 Last updated 11:0	6.00	5 mins	💌 😋 🕥 Help
Interfaces	S X	Data Logs	S X	Config Logs	S X
13	5 7	No data available.		No data available.	
		System Logs	S ×	Locks	S × C
2.4	0.0	Description	Time	No locks found	
General Information	S ×	Received conflicting ARP on interface ethernet1/1 indicating duplicate IP 202 137 141 25 cender mar	11/03 11:05:57	ACC Risk Factor (Last 60 minutes)	S ×
Device Name	FWPALOALTO	00:00:5e:00:01:24		35	
MGT IP Address	172.16.10.2	User admin accessed Monitor tab	11/03	3.5	_
MGT Netmask	255.255.255.0	Received conflicting ARP on interface	11/03		
MGT Default Gateway	172.16.10.1	ethemet1/1 indicating duplicate IP	11:05:21		
MGT IPv6 Address	unknown	202.137.141.25, sender mac 00:00:5e:00:01:24			
MGT IPv6 Link Local Address	fe80::286:9cff:fe3f:4900/64	Received conflicting ARP on interface	11/03		
MGT IPv6 Default Gateway		ethemet1/1 indicating duplicate IP	11:04:49		
MGT MAC Address	00:86:9c:3f:49:00	00:00:5e:00:01:24			
Model	PA-220	User admin logged in via Web from	11/03		
Serial #	012801043734	172.16.10.59 using https	11:04:16		
Software Version	8.0.3	172.16.10.59.	11:04:16		
GlobalProtect Agent	0.0.0	Received conflicting ARP on interface	11/03		
Application Version	7999-0000	ethernet1/1 indicating duplicate IP 202.137.141.25, sender mac	11:04:06		

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

HEI WORKS		- Last united 15-10.07	
eneral Information	Layout 3 Columns	Last optialed. 16.10.07	
		duplicate IP 202.137.141.25, sender mac 00:00:5e:00:01:24	16:09:46
Device Name	FWPALOALTO	Received conflicting ARP on interface ethernet1/1 indicating duplicate IP 202.137.141.25, sender mac 00:00:5e:00:01:24	09/08
MGT IP Address	172.16.10.2	Received conflicting ARP on interface ethernet1/1 indicating	09/08
MGT Netmask	255.255.255.0	duplicate IP 202.137.141.25, sender mac 00:00:5e:00:01:24	16:08:39
MGT Default Gateway	172.16.10.1	Received conflicting ARP on interface ethernet1/1 indicating duplicate IP 202.137.141.25, sender mac 00:00:5e:00:01:24	09/08 16:07:53
MGT IPv6 Address	unknown	Received conflicting ARP on interface ethernet1/1 indicating	09/08
MGT IPv6 Link Local Address	fe80::286:9cff:fe3f:4900/64	duplicate IP 202.137.141.25, sender mac 00:00:5e:00:01:24	16:07:21
MGT IPv6 Default Gateway		Received conflicting ARP on interface ethernet1/1 indicating duplicate IP 202.137.141.25, sender mac 00:00:5e:00:01:24	09/08
MGT MAC Address	00:86:9c:3f:49:00	Received conflicting ARP on interface ethernet1/1 indicating	09/08
Model	PA-220	duplicate IP 202.137.141.25, sender mac 00:00:5e:00:01:24	16:06:09
Serial #	012801043734	FqdnRefresh job started processing. Dequeue time=2021/09/08 16:05:42 Job Id=4067	09/08
Software Version	8.0.3	FadnRefresh job enqueued, Enqueue time=2021/09/08	09/08
GlobalProtect Agent	0.0.0	16:05:42. JobId=4067 Type: Full	16:05:42
Application Version	7999-0000	Received conflicting ARP on interface ethernet1/1 indicating dualization 18,202,132,141,25, condex may 00/00/5a/00/01/124	09/08
URL Filtering Version	20190329.20253	Supreste 17 202.137.141.23, Sender mat 00.00.36.00.01.24	10.05.50
GlobalProtect Clientless VPN Version	0		
Time	Wed Sep 8 16:10:10 2021		
Uptime	85 days, 6:47:08		
ystern Resources	S	×	
Management CPU	2%		
Data Plane CPU	0%		
Session Count	103 / 65534		

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

Interfaces Ethernet VLAN Loopback Tunnel M Zones W.V.Mis Interface Type Management Link IP Address Virtual Router Tag M Postula DHCP District Interface Type Management Link IP Address Virtual Router Tag M Postula DHCP District Interface Type Management Link IP Address Virtual Router Tag M District DHCP District Interface Type Management Link IP Address Virtual Router Tag M District District Interface Type Management Link IP Address Virtual Router Tag M District District Layer3 Ping IP Address Virtual Router Untaged M State Layer3 Ping http https Interface none none Untaged M District Gateways Interface Router Interface Interface Interface Untaged M District Profile Interface Router Interface Intaged Intaged	Q Sear	🕞 Contig 🗸 🔾	🔒 Commit 💰	Network Device	cts	Policies Obje	Monitor	ashboard ACC	paloalto
Within Sources Interface Interface Type Management Profile State Virtual Routers Virtual Routers Virtual Routers Virtual Routers Virtual Routers Interface Interface Type Management Profile State State Virtual Routers Tag DHCP DHCP DHCP Globalizotact Globalizot	50	e				1	oopback Tunnel	Ethernet VLAN L	Interfaces 194 Zones
With Routers Interface In	-	3 Herris			Link	Municipaniant		4	Ry VLANs Be Virtual Wires
DHCP Layer3 ping 20.2.137.141.237/24 default Untagged DNS Proxy GobalProtect im ethemet1/2 Layer3 Pinghttps im 172.16.5.1/25 default Untagged GobalProtect im ethemet1/2 Layer3 ping http https im 172.16.5.1/25 default Untagged GobalProtect im ethemet1/2 Layer3 ping http https im none default Untagged MGM Device Block List im ethemet1/3 im im ethemet1/3 im none none Untagged GobalProtect Block List im ethemet1/7 im im none none Untagged GobalProtect Block List im ethemet1/7 im im none none Untagged Mitter Staps im ethemet1/6 im im none none Untagged Mitter Staps im ethemet1/6 im im none none Untagged Mitter Staps im im im im none none Untagged Mitter Staps im	Wit	Tag	Virtual Router	IP Address	State	Profile	Interface Type	Interface	Ø Virtual Routers Ø IPSec Tunnels
Chose Prozy Immethane Layer3 Panghittps Immethane 172.16.5.1/25 Sefault Untagged GlobalProtect Protision Immethane Layer3 ping http https Immone default Untagged GlobalProtect Immethane Layer3 ping http https Immone none default Untagged GlobalProtect Immethane Immethane Immethane Immethane Immethane Untagged GlobalProtect Immethane Immethane Immethane Immethane Immethane Untagged GlobalProtect Immethane Immethane <td>nor</td> <td>Untagged</td> <td>default</td> <td>202.137.141.237/24</td> <td></td> <td>ping</td> <td>Layer3</td> <td>themet1/1</td> <td>DHCP</td>	nor	Untagged	default	202.137.141.237/24		ping	Layer3	themet1/1	DHCP
Substant votect m ethemet1/2 Layer3 ping http https m none default Untagged Contains m ethemet1/4 Layer3 ping http https m none 192.168.155.1/24 default Untagged Detrice Block List m ethemet1/4 Layer3 ping http https m none none Untagged Optionetess Apps m ethemet1/4 Layer3 ping http https m none none Untagged Contentess Apps m ethemet1/7 m none none Untagged Contentess Apps m ethemet1/7 m none none Untagged LiUP methemet1/8 m none none Untagged KEConpto methemet1/8 m none none Untagged Mitter Statemarys m none none Untagged Mitter Statemarys Mitter Statemarys <	nor	Untagged	default	172.16.5.1/25		PingHttps	Layer3	and etherwet1/2	DNS Proxy
Gateways im ethemet1/4 Layer3 ping http https im 192.168.155.1/24 default Untagged Denice Block List im ethemet1/% im none none Untagged Oterritess Apps im ethemet1/% im im none none Untagged Oterritess Apps im ethemet1/% im im none none Untagged Gateways im ethemet1/% im im none none Untagged Gateways im ethemet1/% im im im none im im Gateways im im im im none im im im im Gateways im im<	nor	Untagged	default	none		ping http https	Layer3	and ethemet1/0	Portais
Indext Support Image: Indext Support Device Block Litt Image: Indext Support Indext Support Image: Indext Support Offenties App Groups Image: Indext Support ILDP Image: Indext Support A GlobalProtect IPSec Crypto Image: Indext Support A GlobalProtection Image: Indext Support A Ministrice Mignt Image: Indext Support Image: Indext Support Image: Indext Support Image: In	noi	Untagged	default	192.168.155.1/24		ping http https	Layer3	and ethemet1/4	Cateways
Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substrate Bioloc List: Image: Substr	nor	Untagged	none	none	1			and ethemet1/5	MDM
Otentiess App Groups millione none Intragged QoS millione none untagged Methorsk Profiles mone internet1/A mone Untagged Methorsk Profiles mone internet1/A mone Untagged Methorsk Profiles mone internet1/A mone Untagged Montar mone mone internet internet Montar mone Protection mone internet internet	no	Untagged	none	none				and ethemet1/6	Cientiess Apps
QOS water themet 1/h im none none Untagged Situation Situation Situation Situation Situation Situation Situation Monitor Situation Situation Situation Situation Situation Situation Situation Situation Situation Situation Situat	nor	Untagged	none	none	1			and ethemet1/7	Clientless App Groups
Bickbork Profiles Bickbork Profiles Bickbork Profiles Diffectorysto Diff	nor	Untagged	none	none				and ethernet1/8	QoS
A QoS Profile									Globolintotect Irise Crypto TVE Getenarys TVE Getenarys TVE Tete Crypto Monitor Monitor Monitor Qos Profile LLDP Profile

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

1 10 10 10 10 10 10 10 10 10 10 10 10 10	192.168.155.	L/#network::v	sys1::network/zoi	165					\$
paloalto	ashboard	ACC N	Ionitor Policie	ns Object	s Netwo	rk Device	\$ Co	mmit 🔏 🗔 Con	fg • 9, Searc
									S ()
Zones	•	_	_				_		4 items
VEANs Virtual Wires Virtual Routers	🔲 Name	Туре	Interfaces / Virtual Systems	Zone Protection Profile	Packet Buffer Protection	Log Setting	Enabled	Included Networks	Excluded Networks
IPSec Tunnels	untrust	layer3	ethernet1/1	1				any	none
DHCP	T trust	layer3	ethemet1/2					any.	none
DNS Praxy	III dma	layer3	ethernet1/3					any	none
GlobalProtect	E CMZ1	layer5	ethernet1/4					any	none
LLDP									
LLDP Network Profiles									
CLUP Hetwork Profiles GlobalProtect IPSec Crypto HE Cateways HE Cateways HE Crypto HE Crypto HE Crypto HE Crypto HE Crypto Componentiate LLCP Profile LLCP Profile									

• Configure Network Objects:

Create network objects: *Objects > Addresses*

paloalto	Dashboard ACC	Monitor Policies	Diects Letwork Devi	ce
Addresses	~ Q			
Address Groups	Name	Location	Type	Address
S. Regions	IT ADD Aven		75 10-10-10	172.16.0.12/22
Applications	III ADD-test		IP Netmask	1/2.16.0.12/32
Application Groups	EI BARA		IP Netmask	202.137.141.237/3
Services	dmz-subnet		IP Netmask	10.0.0/24
Service Groups	mil dmz1-subnet		IP Netmask	192.168.155.0/24
Tags	GlobalProtect-VPN		IP Netmask	192.168.250.0/24
V 😨 GlobalProtect	Inside-VLAN10		IP Netmask	172.16.0.0/23
HIP Objects	Inside-VLAN20		IP Netmask	172.16.2.0/24
HIP Profiles	In and A ANTO		10 Nates arts	173 16 2 0/34
External Dynamic Lists	In inside victorso		IP Welmidsk.	1/2-16-3-0/24
V 🔂 Custom Objects	Inside-VLAN40		IP Netmask	172.16.4.0/25
Data Patterns	, El Inside-VLAN50		IP Netmask	172.16.4.128/25
Spyware	Inside-VLAN60		IP Netmask	172.16.5.0/25
Vulnerability	Inside-VLANB0		IP Netmask	172.16.10.0/24
G URL Category	Inside-WAN1		IP Netmask	172.16.5.0/25
Security Profiles	T kteanor		FOON	172 16 0 3
Antivirus	The second secon		10 Materials	173 16 3 18/33
Vulnerability Protection			1P Welmask	1/2.10.3.15/32
URI Filtering	Li ubudot		FQDN	1/2.16.3.19
File Blocking	WEB-PRIVATE		IP Netmask	10.0.0.10/32
WildFire Analysis	webserver-ext-ip		IP Netmask	202.137.141.25/32

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

	Dashboard	ACC Monito	or Policies	Objects	Network Devic
Addresses				1.772	
Regions Applications Applications Application Groups Application Filters Services	All-Inside-VLANs	Location	9	GlobalProtect-VPN Inside-VLAN10 Inside-VLAN20 Inside-VLAN30	
Service Groups Tags GlobalProtect HIP Objects HIP Defice				Inside-VLAN40 Inside-VLAN50 Inside-VLAN60 more	

• <u>Configure Security Policy:</u>

Now we can create security policy: *Policies > Security*

paloalto	Dashbo	ard ACC	Monitor	Policies	Objects	Network Dev	lice	📥 Commit 👩	Config -	Q , Searc
										s ()
Security									19 it	ania 🖨
NAT						Stores				Destina
Policy Based Forwarding		Name	Tags	Туре	Zone	Address	User	HIP Profile	Zone	A
Decryption	1	NAT-ALL-TO-INTERNET	none	universal	for trust	EB All-Inside-VLANs	any	any	seg untrust	ar
Tunnel Inspection	2	NAT-DHZ-TO-OUTSIDE	none	universal	pag danz	Se dmz-subnet	any	any	pog untrust	-
Application Overnoe	3	NAT-INSIDE-TO-OMZ	none	universal	(III) trust	Al-Inside-VLANs	any.	any	pag dmz	5
DoS Protection	4	OUT-ACCESS-IN	none	universal	pag untrust	any	any	any	pre trust	5
	5	OUT-ACCESS-DMZ	none	universal	(10) untrust	anhy	any :	any,	pre deuz	5
	6	OUT-ACCESS-DHZ-1	norie	universal	prog unitruent	any	atry.	any	fill desz	5
	7	OUT-ACCESS-DM2-FTP	none	universal	(R) untruist	arry	any	any.	PR DHEL	5
	8	INSIDE-ACCESS-DM2	none	universal	pag trust	Al-Inside-VLANs	any	any	pre deuz	15
	9	OMZ-ACCESS-OUT	none	universal	(22) dmz	dmz-subnet	any	any	any'	
	10	DMZ-ACCESS-DUT-1	none	universal	pro dmz	arry	any	any	any	5
	11	INSIDE-ACCESS-OUT	none	universal	(m) trust	Al-Inside-VLANs	atty	any	any	1
	12	DH21-TO-OUTSIDE	0.00110	universal	ITTHE PAR	Se dm21-subnet	any	any	any	
Frowser E	13	OUT-ACCESS-OMZ1	none	universal	(FFR) suntrust	any	апу	any	FOR DM21	5
e(<i>u</i>) <i>vv</i>	14	IN-ACCESS-DM21	none	universal	proj trust	any	any	any	PRI DHIZE	
	15	Inst-IN	none	Linversal	(R), untrust	day.	any	MY	phg 204272	
	15	Inst-IN-1	admir	universal	(#1) ambract	2017	229	Bly	pit hust	
Filter by first tag in rule	17	hed	and the	iniumal	and friend	ANY	100	200	TEL approach	
Rule Order O Alphabetical	18	Intramona dallardi 28	panel.	Inframme	and the	-	(and and its a		(intrames)	1.44

<u>Configure NAT Policy:</u>

Create NAT policies: *Policies > NAT*

paloalto	Dashboard AC	C Monitor	Policies	Objects Nets	vork Device	🐣 Commit 👩 😡	Config + Q Sean
							G 🖸
Security	٩						22 Atoms
Qo5					Origin		
Policy Based Forwarding	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Addres
Tunnel Inspection	1 Nat-10.0.0.3 2 NAT-INSIDE-T	D-OUTSIDE none	pag trust	(22) untrust	ethemet1/1	any	Si webserver-ext- any
DoS Protection	3 NAT-DMZ-TO-0	DUTSIDE none	pag denz	(20) untrust	ethemet1/3	Sy doz-subnet	any (
	4 Nat-Atranyer-d	e: aune),	provident -	(m) solitaint	207	any -	Networker-and
	5 Nat-dof_ra-da	2002	(10) intrint	pay untriat	any	any.	🤤 webserver eit
	6 Nat-dol_co-do	enne	Di unbust	PR unbust	any.	ary .	Sg webcerver-en
Browser	7 Nat-more to-da	rane	(2), untrust	pil untrust	<i></i>	417	Si webserver est
t Karn 🤕	8 Netscriptore	et ge de 🛛 sere	III indust	DR without	any	Alty.	Sq andresser est
e (22) 1-22	9 Nat-SUFORD-u	budof-sch nane	FR untrust	(22) untrust	any	any	😽 ubudof
	10 Not-10.0.0.4-d	is none	tal qua	pre dine	MV.	ATK.	Ne melanner en
	11 Net-172.16.0.3	di eme ;	(II) brist	pag trust	any	жy	Se webserver ext
Filter by first tag in rule Rule Order O Alphabeti	12 Nat-10.0.0.1-0	MZ sione	PRE DMZ1	(22) untrast	any	any	Sy webserver-ext

- Configurations related to NFMS
 - <u>Security Policy related to NFMS:</u>

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

NAT OoS													
Policy Based Forwarding		Name	Tege	Турн	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
Decryption	1	INSIDE TO INTERNET	none	universal	(PR break	Al-Inside VLANs	anv	sev	(R) unitsuit	sny	sny	any	C Alon
Tunnel Inspection Amiliation Overside	2	OUT-ACCESS-OM2-FTP	mane	uriversal	pre untrust	any	arty	servy	FIRE OWER	Sa webaarver-ext-ip	iarry	R Rp-data	O Alton
Authentication	3	INSIDE-ACCESS-OUT	none	universal	pit tout	Al-Inside VLAtis	any	any	any	any	any	SERVICE_10	O Allow
Da5 Protection	4	DH21-TO-OUTSIDE	none	universal	POR LINEZ L	😽 ehmz1-submet	#19y	any	any	any	any	any	O Allow
3rowaer E					proven				pre unita			 4343 4343 4244 6443 CMC-SERVICE service-fitty service-fitty service-fitty 	Alon
(5) 1-5	6	IN-ACCESS-ONE)	none	uriversal	pag trust	any	9119	PAA	tel pict	arry'	any .	** 42.42 ** 42.43 ** 42.44 ** 54.63 *** 0.042-5ERV/ICE *** service-Mttp *** service-Mttp	© Allow
	7	intracone-default	nonie	intrazone	304	any	any	349	(intrazone)	any	ani	any	O Nov
	5	Antersone-Default	none	interzone	any !	ary	111	MTY .	any.	ally.	177	ATT	O Dany

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:

						Destination			
	Name	Zone	Address	User	Zone	Address	Application	Service	Action
1	INSIDE-TO-INTERNET	(22) trust	All-Inside-VLANs	any	pag untr	any	any	any	O Allow
Z	OUT-ACCESS-DMZ-FTP	🕅 untrust	any	any	DMZ1	😼 webserver-ext-ip	any	🗶 ftp-data	O Allow
З	INSIDE-ACCESS-OUT	122 trust	All-Inside-VLANs	any	any	any	any	SERVICE_10	O Allow
4	DMZ1-TO-OUTSIDE	DM21	Sy dmz1-subnet	any	any	any	any	any	O Allow
5	OUT-ACCESS-DMZ1	12 untrust	any	any	R DMZ1	😼 webserver-ext-ip	any	 ¥ 4242 ¥ 4243 ¥ 4244 ¥ 6443 DMZ-SERVICE × service-https 	S Allow
6	IN-ACCESS-DMZ1	(M) trust	any	any	NQ DMZ1	any	any	 24242 4243 4244 6443 DMZ-SERVICE service-http service-https 	O Allow
7	intrazone-default	any	any	any	(intrazon	any	any	any	O Allow
8	interzone-default	any	any	any	any	any	any	any	O 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:



Policy Number 5:



• NAT Policy related to NFMS:

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

Sourty	•		_							
SP NAT										
Policy Based Forwarding		Name	Source Zone	Destination Zone	Destruction Interface	Source Address	Destination Address	Service	Source Translation	Destination Translatio
🙆 Tunnel Inspection	1	Nat-10.0.0.3	(## trust	F22 untrust	any	any	Sa webserver-ext-ip	алу	none	address: 192.168.151
Application Override Authentication Configuration	72	NAT-INSIDE-TO-OUTSIDE	proj trust	PR untrust	ethervet1/1	69 All-Insid	aty.	апу	dynamic-ip-and-port ethemet1/1	name
C Cos Prosecutiv	н	NAT-DM2-TO-OUTSIDE	proj dime	(PR untrust	ethernet1/1	😼 dmz-sub .	алу	згү	dynamic-ip-and-port ethemet1/1	nane
	-4	Nat-SUFORD-ubudof-ssh	(22) untrust	(PR) untrust	any	any	lobudu 👺	X 22	none	address) 172.16.3.19 port: 22
na Drawine	N.	Nat-10.0.0.3-DMZ	ted DW21	pag untrust	any	any	Si webserver estrip	X 4242	dynamic-ip-and-port ethemett/4 192.168.155.1/24	address: 192,166,151 port: 4242
ag(+)	6	Natiserver 4243-OM2	PR DMZ1	PR untrust	апу	any	😼 webserver-extrip	X 4243	dynamic ip and port athemet1/4 192.168.155.1/24	address: 192.168.15 port: 4243
one (19) 1-19	7	Not-server-4244-DMZ	(M) DMZ1	pat untrust	any,	any	Sy webserver-ext-ip	X 4244	dynamic ip and port ethernet1/4 192.168.155.1/24	address: 192,168,15 port: 4244
	8	Nat-10.0.0.3-DM2-6050	FAR DWGT	(R) untrust	any	апу	Sy vebaror est-p	X 5080	dynamic-ip-and-port ethemet1/4	address: 192.168.15 port: 6080
Filter by first tag in rule Rule Order O Alphabetical	9	Nat-10.0.0.5-dis	(R) trust	pag trust	any	any	😼 webserver-ext-ip	2 8180	none	address: 10.0.0.5 port: 8380

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))

				Ori	iginal Packet			Transla	ted Packet
	Name	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	Nat-10.0.0.3	100 trust	(22) untrust	any	any	😼 webserver-ext-ip	any	none	address: 192.168.155.3
z	NAT-INSIDE-TO-OUTSIDE	[22] trust	(R) untrust	ethernet1/1	All-Insid	any	any	dynamic-ip-and-port ethernet1/1	none
3	NAT-DMZ-TO-OUTSIDE	proj dime	🕅 untrust	ethernet1/1	😼 dmz-sub	any	any	dynamic-ip-and-port ethemet1/1	none
4	Nat-SUFORD-ubudof-ssh	122 untrust	(#2) untrust	any	any	Sg ubudof	X 22	none	address: 172.16.3.19 port: 22
5	Nat-10.0.0.3-DMZ	(##) DMZ1	122 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	PRI DMZ1	1991 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	1991 DMZ1	🕅 untrust	any	any	😼 webserver-ext-ip	X 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	(PR) DMZ1	🕅 untrust	any	any	😪 webserver-ext-ip	2 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	(22) brust	(PP) trust	алу	any	😼 webserver-ext-ip	× 8180	none	address: 10.0.0.5 port: 8180
10	Nat-ftp-server	(P2) untrust	(22) untrust	any	алу	😼 webserver-ext-ip	X FTP	none	address: 192.168.155.3 port: 21
11	Nat-fms-server	Pl untrust	1991 untrust	ethernet1/1	any	😼 webserver-ext-ip	X 4242	none	address: 192.168.155.3 port: 4242
12	Nat-server-4243	122 untrust	M untrust	ethernet1/1	any	Sig webserver-ext-ip	X 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	M untrust	ethernet1/1	any	😼 webserver-ext-ip	× 6443	none	address: 192.168.155.3 port: 6443
15	DMZ1-TO-OUTSIDE	DMZ1	M untrust	ethernet1/1	any	any	any	dynamic-ip-and-port ethemet1/1	none
16	Nat-fms-server-443	🕅 untrust	🕅 untrust	ethernet1/1	any	😼 webserver-ext-ip	X 443	none	address: 192.168.155.3 port: 443
17	Nat-fms-server-6080	121 untrust	M untrust	any	any	😼 webserver-ext-ip	× 6080	none	address: 192.168.155.3 port: 6080
18	test01	(PR) untrust	121 untrust	any	any	😼 webserver-ext-ip	28 👷	none	address: 192.168.155.3 port: 80
19	test01-1	Pa DMZ1	🕅 untrust	any	any	😽 webserver-ext-ip	2 80	dynamic-ip-and-port ethemet1/4 192.168.155.1/24	address: 192.168.155.3 port: 80

Explained example of a NAT Policy:



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:

Real PuTTY Configuration		?	\times	
ategory:				
Session Logging Terminal Keyboard Bell	Basic options for your Pu Specify the destination you want to Host Name (or IP address)	TTY session connect to Port 23		
Features For early for the second s	Connection type: Raw Telnet Riogin (Load, save or delete a stored sessi Saved Sessions	on Set	Depe you'r of yo	ending on which Vlan re in, put default gateway pur vlan
Colours Connection Data Proxy Telnet	Default Settings coresw1	Load Save Delete	2	
i - Riogin ⊞- SSH - Serial	Close window on exit: Always Never On	lly on clean exit		
About Help	Open	Cance	4	



• 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:

- Session	Basic options for your P	uTTY session
 Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telept 	Specify the destination you want the Host Name (or IP address) 172.16.10.3 Connection type: Raw Telnet Rlogin Load, save or delete a stored sess Saved Sessions Default Settings coresw1	o connect to Port 23 O SSH O Serial sion Load Save Delete
⊷ Rlogin ⊕ SSH Serial	Close window on exit: Always Never I C	Only on clean exit



- Configurations related to NFMS
 - Configurations in FIPD core switch



• Configurations in NFMS switch

Putry 172.16.10.3 - Putry		×
interface Port-channel2		^
switchport mode trunk		
1		
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		
:		
Interiace Gigapitethernet1/0/4		
description Sky-meni		
switchport mode train		
: interface CigabitEthernet1/0/5		
switchnort access when 80		
switchport mode access		
I I I I I I I I I I I I I I I I I I I		
interface GigabitEthernet1/0/6		
description LAN BARRACUDA		
switchport access vian 90		
switchport mode access		
I		
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 <u>https://vcenter.fcpf.vsphere</u> then click on "LAUNCH VSPHERE CLIENT (HTML5)"

S Welcome to VMv	vare vSphere × +				
< → C (▲	Not secure https://vcenter.fcpf.vsphere				
vm ware [.]					
Getting Started					
The vSphere Flash- switching to the all-n reverting to the Flash	based Web Client is deprecated in vSphere 6.7. We recom ew modern HTML5-based vSphere client as the primary on h-based Web Client when necessary.	mend lient and only			
LAUNCH V	SPHERE CLIENT (HTML5)				
LAUNCH VS	PHERE WEB CLIENT (FLEX) Deprecated				
Documentation					
VMware vSphere	Documentation Center				
Functionality Upd	ates for the vSphere Client (HTML5)				
ill in login cr	edentials then click LOGIN		-		×
ill in login cr Ø Login ← → ℃ ▲ N	edentials then click LOGIN	sphere?SAMLReque	- s Q	□ ☆ 8	×
ill in login cr ❷ Login ← → C ▲ N VMware	edentials then click LOGIN × + ot secure vcenter.fcpf.vsphere/websso/SAML2/SSO/fcpf.v e [®] vSphere	sphere?SAMLReque	5.m Q	□ ★ 8	×
ill in login cr Ø Login ← → C ▲ N VMward administrator@t	edentials then click LOGIN × + pt secure vcenter.fcpf.vsphere/websso/SAML2/SSO/fcpf.v e [®] vSphere cpf.vsphere	sphere?SAMLReque	- 5 Q	□ ★ 8	×
ill in login cr ^{⊘ Login} ← → C ▲ N VMware administrator@l	edentials then click LOGIN + ot secure vcenter.fcpf.vsphere/websso/SAML2/SSO/fcpf.v e [®] vSphere cpf.vsphere	sphere?SAMLReque	- 5 Q	□ ★ 8	×
ill in login cr	edentials then click LOGIN × + ot secure vcenter.fcpf.vsphere/websso/SAML2/SSO/fcpf.v e [®] vSphere	sphere?SAMLReque	s Q	□ ★ 8	×
ill in login cr Login ← → C ▲ N VMWare administrator@l	edentials then click LOGIN × + ot secure vcenter.fcpf.vsphere/websso/SAML2/SSO/fcpf.v e [®] vSphere	sphere?SAMLReque	5 Q	□ ★ 8	X II
ill in login cr <pre> Login ← → C ▲ N </pre> VMware administrator@t	edentials then click LOGIN x + ot secure vcenter.fcpf.vsphere/websso/SAML2/SSO/fcpf.v e [®] vSphere	sphere?SAMLReque	5 Q	□ ★ 8	× I

Monitor system resources of ESXi hosts:

vm vSphere Client Menu v	Q	Search in all environments 172.16.10.101 Actions -		C @·	✓ Administrator@FCPF_VSPHERE ✓	6
		Summary Monitor Configure Permissions VMs Datastores Hypervisor VMware ESX, 6.7.0, 15160138 Modet 2288H V5 Processor Type: Intel(P) Xeon(R) Silver 4110 CPU (# 2.105Hz) Logical Processors 32 NCK 6 VMMare ESX, 6.7.0, 15160138 Silver 4110 CPU (# 2.105Hz) Silver 4110 CPU (# 2.10	Pé	etworks Updates	CPU Prec 32.93 0 Und 651 Mile Capacity: 33.55 0 Marriary Prec 33.19 Used 32.4 08 Capacity: 127.56 Bronge Frie 5.31 Used 16.16 15 Capacity: 22.5	340 342 38 38 108
급 laoagroforest 윤 NFMS 윤 NFMS-CLONE		Hardware	~	Configuration	Ŷ]
		Tags	^	Related Objects	^	6
Recent Tasks Alarms						
Task Nome - Target -	State	- V Details V Initiator V Queued For	For	✓ Start Time ↓ ✓	Completion Time - Server	12
Deploy plug-in Ø voentectoptysphere	4	Completed comvimware.vcintegrity PCPFVSPHERE/vspher 21 ms		09/08/2021, 4:34:27 PM	09/08/2021, 4:34:37 PM vcenter.fcpf.vsphere	
						1

Monitor system resources of VM:

	🖧 Reverse Proxy 🗼 📕 🦉 🧔 🛛 Actions -	
 FCPFDC FCPF_CLUSTER 172.16.10.101 172.16.10.102 admin Backup NFMS PDMSLIN PDMSVIN 	Guest OS: Ubuntu Linux (64-bit) Compatibility: ESXi 6.7 and later (VM version 14) VMware Tools: Running, version:11296 (Guest Managed) More info DNS Name: reverseproxy IP Addresses: 10.0.06 Launch Web Console Launch Remote Console US: Ubuntu Linux (64-bit) Compatibility: ESXi 6.7 and later (VM version 14) VMware Tools: Running, version:11296 (Guest Managed) More info DNS Name: reverseproxy IP Addresses: 10.0.06 View all 2 IP addresses Host: 172:16:10.101	opueses
C Reverse Proxy	VM Hardware	Notes
	> CPU 2 CPU(s)	Edit Notes
	> Memory 4 GB, 0.04 GB memory active	Custom Attribute
	> Hard disk 1 40 GB	Attribute
Recent Tasks Alarms		
The second se	Catus Dataile u Initiator u Ousuad Ear	Crart Time

• 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 <u>https://172.16.10.101</u> for ESXi1 or <u>https://172.16.10.102</u> for ESXi2 then fill in login credentials and click Log in.



ware esxi				root@172.16.10.101 + Help +	Q Search
Navigator	localhost.localdomain				
i Host Monage Monitor Virtual Machines Storage Gatastore1 Montor More storage	Anage with vCanter Serve Serve Sate Uptime	e Struct Greate Register VM B Shut Grown B Reboot ccaldomain 6.7 0 Update 3 (Build 15160130) Normal (connected to vCenter Server at 172.16.10.5) 48.99 days	C Refresh 🛛 🗛 Actions	CPU USED: 15 GHz MENORY USED: 42 36 GE 31004AGE USED: 2.03 78	FREE 12.1 GHU 5% CAPACITY 23.6 GHU 2400 3.30% CAPACITY 127.59 GH FREE 14.46 TB 26% CAPACITY 22.5 TB
Networking Default TCP/IP stack	This fost is being mana	iged by vCenter Server. Actions may be performed automatica	nly by vCenter Server without you	r knowledge. 🔘 Actions	
Networking Default TCP/IP stack More networks	This bost is being mana Hardware	ged by vCenter Server. Actions may be performed automatica	Ry by vCenter Server without you	r knowledge. 🧔 Actions	-
Networking Default TCP/IP stack me vrmic1 More networks	This foot is being mana Hardware Manufacturer	iged by vCenter Server. Actions may be performed automatica	Ity by vCenter Server without you + Configuration Image profile	(Updated) ESXI-5.7.0-2019	e e e e e e e e e e e e e e e e e e e
 Networking Default TCP/IP stack wmnic1 More networks 	This host is being mana Hardware Manufacturer Model	god by vCenter Server. Actions may be performed automatica Huaves 2269H V5	Hy by vCenter Server without you	Knowledge: Actions	P1204001-standard (VMw
Networking Detault TCP/IP stack wrinic1 More networks	This bost is being manu Hardware Manufacturer Model Model M CPU	god by vCenter Server. Actions may be performed automatica Huanes 2268H V5 16 CPUs x Inte(R) Xeon(R) Silver 4110 CPU @ 2.1	tty by vConter Server without you - Configuration Image profile vSphere HA state	Knowledge: Actions Updated) ESXI-6.7.0-2011 are, Inc.) Agent running	1204001-slandard (VMw
Ketworking Ketworking Workautt CP/IP stack wrmic1 More networka	This host is being mana Hardware Marufacturer Model CPU Recent tasks	nged by vCenter Server. Actions may be performed automatica Huarnel 2280H VS 16 CPUe x Intel(R) Xeen(R) Silver 4110 CPU @ 2.1	Ity by vCenter Server without you • Configuration Image profile vSphere HA state	Anowledge. Actions (Updated) ESXI-6 7.0-2011 are, Inc.) Agent running	H1204001-standard (VMw

• Licenseing

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

vm vSphere Client	Menu V Q Search in all environments
v center.fcpf.vsphere	Home Ctrl + alt + home Shortcuts Ctrl + alt + 1 Configure Permissions Hosts VMs Datastore
 FCPFDC FCPF_CLUSTER 172.16.10.101 	Hosts and Clusters ctrl + alt + 2 VMs and Templates ctrl + alt + 3 Storage ctrl + alt + 4
 172.16.10.102 admin Backup 	Image: Second system <
PDMSLIN	Policies and Profiles Auto Deploy
Reverse Proxy	 Developer Center vRealize Operations
	Administration Opdate Manager
Recent Tasks Alarms	Tasks
Task Name V Targer	Tags & Custom Attributes

After that click on Administration:

Shortcuts	Home
Hosts and Clusters	VCENTER.FCPF.VSPHERE -
VMs and Templates	
Storage	CDU
Vetworking	64.95 GHz froo
Content Libraries	04.55 0H2 Tree
😼 Global Inventory Lists	2.22 GHz used 67.17 GHz total
Policies and Profiles	
🖉 Auto Deploy	
<>> Developer Center	
vRealize Operations	C) VINS
Administration	7 0

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

vm vSphere Client Menu v	Q. Search in all environments	CO	Administr	rator@FCPF.VSPI
Administration Roles Global Permissions • Licensing	Licenses Products Assets			×
Solutions Client Plug-Ins vCenter Server Extensions Deployment System Configuration Outdomer Experience Improvement Prog.	License VMware vCenter 5 Standard (I. Eftopf_vcenter MJ695-AC351-R8P93-091A6-21T3N VMware vCenter Server 6 Standard (I. Eftopf_vsphere 4141N-8WH13-R828R-0K2RM-9D32N VMware vSphere 6 Standard (CPUs) Evenor	Usage 1 Instances 4 CPUs	Capacity 1 instances 4 CPUs	State v Assigned Assigned
Support Upload File to Service Request Single Sign On Users and Groups Configuration Certificates	No items selected			

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.

Right Click	Actions - FCPF_CLUSTER	PF_CLUSTER ACTIONS ~ Monitor Configure Permissions Hosts VMs D	atastores Networks Updates
FCPFPC FCPF_CLUSTER T7216.10.101 172.16.10.102	New Virtual Machine New Resource Pool Deploy OVF Template	Total Processors: 32 Total vMotion Migrations: 6	
🔓 admin 🚰 Backup 🔂 NFMS	Storage		
C PDMSLIN	Host Profiles Edit Default VM Compatibility	Objects	∧ VSphere HA
🔓 vcenter	Settings	acenter FCPFDC	Tags
	Move To	Consumers	Assigned Tag Cate Cate
Recent Tasks Alarms	Tags & Custom Attributes	Attributes	~

• 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.

C vcenter.fcpf.vsphere	Summary Monitor C	onfigure Permissions Hosts	VMs Datastores Networks Updates		
Constant Constan	Services Victoria DOS Victo	VSphere HA is Turned C Puttime information for vSphere HA is no Proactive HA is not avai To enable Proactive HA you must also e Failure conditions and n	DN Isocred Linder vSphere HA Monitoring Iable Des on the cluster esponses		6.2) 6
C NFMS	Licensing	Failure	Response	Deteils	
E POMSUN	VMware EVC	Host failure	Restart VMs	Restart VMs using VM restart priority ordering.	*
	VM/Host Groups	Proactive HA	Disabled	Proactive HA is not enabled.	10
Chestan bar Linny	VM/Host Rules	Host isolation	Disabled	VMs on isolated hosts will remain powered on.	
Ca vcenter					
B vcenter	VM Overrides Host Ontions	> Admission Control	Expand for details		
B vcenter	VM Overrides Host Options Host Profile	Admission Control Datastore for Heartbeating	Expand for details Expand for details		
नि vcenter	VM Overrides Host Options Host Profile VO Filters	Admission Control Datastore for Heartbeating Advanced Options	Expand for details Expand for details 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.

vcenter.tcpf.vsphere	Summary Monitor Co	nfigure Permission	i VMs Datastor	es Networks	Updates		
✓ ☐ FCPEDC ✓ ☐ FCPE_CLUSTER ☐ 172.1610.101 ☐ 172.3610.102	Storage Storage Adapters Storage Devices	VMkernel ada	pters Refrest / Edit.	K Remove	ID Addition	- Yrdidb Genele	- Contractor
admin	Host Cache Configur.	Device T	Management N	∰ vSwitch/t	1721610101	Default	Fnabled
Backup	Protocol Endpoints	AN VIICI	SCSIPG-A	f vSwitch1	192,168,88.1	Default	Disabled
G NFMS G POMSUN G POMSWIN G Reverse Proxy G vcenter	Networking <u>Virtual switches</u> VMkernel adapters	vmk2	9 15CSI-PG-8	2 vSwitch1	192168.88.2	Default	Disabled
	TCP/IP configuration	VMkernel network adap All Properties	oter: vmk0 IP Settings Policies				
	VM Startup/Shutdo Agent VM Startup/Shutdo Default VM Compati	Port properties Network label VLAN ID TCP/IP stack Enabled services	Managen 80 Default vMotion	nent Network			

Port properties	VMkernel port settings		
Pv4 settings	TCP/IP stack	Default	
IPv6 settings	MTU	1500	
	Available services		
	Enabled services	🔁 vMation	
		Provisioning	
		Fault Tolerance logging	
		Management	
		vSphere Replication	
		vSphere Replication NFC	
		U VSAN	
		CANCEL	ок

• 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.

Content fcpf.vsphere Content fcpf.vsphere Content fcpf.vsphere Content fcpf.vsphere Content fcpf.vsphere	Summary Monitor Cor	Storage Adapters	s Datastori	es Netwo	orks Updates			
17216.10.101	Storage Adapters Storage Devices	+ Add Software Adapter 🕀 R	fresh 🛱 Resce	an Storage.	R ₂ Reson Adapter	Tarnets w	Devices -	Paths w
🔂 admin	Host Cache Configur	Model: Emulex LightPulse LP	16000 PCIe Fibre	e Channel Ada	pter y	migeo y	Devices 1	
Backup	VO Eltars	Carling and a state	Fibre Che	Online	20.00.00.10.96.90.41.13.10.00.00.10.9	1	2	2
INFMS	- Naturation	G vmhbe4	Fibre Cha	Online	20:00:00:10:95:90:41:14 10:00:00:10:9	1	2	2
PDMSLIN	Virtual switches	. Model: ISCSI Software Adapt	rt:					
읍 PDMSWIN G Reverse Proxy G vcenter	VMkernel adapters Physical adapters	52 ymnbe64	ISCSI	Online	ion1998-01.com/xmware/See360d0-d	4	2 Copy Al	t 6 nems
	TCP/IP configuration							
	 Virtual Machines 							
	VM Startup/Shutdo							
	Agent VM Settings				No items relacted			
	Default VM Compati.			16	No menta selected			
	Form Die Leveliee							

• 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.

□ □ □ ≦ ≦ Ø vcenter.fcpt.vsphere □	Summary Monitor Configure	Permissions VMs Datastores Networks Updates	
COPOL COPOL CLUSTER COPOL CLUSTER COPOL CLUSTER COPOL CLUSTER COPOL CLUSTER COPOL CLUSTER CLU	Storage Adapters Storage Devices Host Cache Configur. Devices	IAI SWITCHES INDIARD NETWORKING EDIT MANAGE PHYSICAL ADAPTERS	ADD NETWORKING REFRES
 Backup NFMS PDMSLIN PDMSWIN 	VO Fites	DMZ_ZONE VLAN ID: 90 VIrtual Machines (3) Virtual Machines (3)	5
읍 Reverse Proxy 금말 vcenter	Physical adapters TCP/IP contiguration • Virtual Machines VM Startup/Shutdo Agent VM Settings •	Management Network •••• VLAN ID: 80 •••• • UMMerine Ports (1) •••• vmik0: 172.36.10.101 ••••	•••

```
Recent Tasks Alarms
```

- VM Operations
 - Accessing VM

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

vcenter.fcpf.vsphere	Summary Monitor Configure Permissions Datastores Networks	Updates
 FCPF_CLUSTER 172.16.10.101 172.16.10.102 admin Backup NFMS PDMSLIN PDMSWIN Reverse Proxy 	Guest OS: Microsoft Windows 10 (64-bit) Compatibility: ESXi 6.7 and later (VM version 14) VMware Tools: Running, version:11265 (Current) More info DNS Name: DESKTOP-REGRRJ2 IP Addresses: 172.16.10.59 View all 4 IP addresses Host: 172.16.10.101	
🕞 vcenter	VM Hardware	Notes
	> CPU 4 CPU(s)	Edit Notes
	> Memory 4 GB, 1 GB memory active	Custom Attribut

• 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

vm vSphere Client	Actions - admin	n in all environments
ropitere enerit	Power •	
	Guest OS Snapshots	dmin 🕨 🖷 😻 🕸 actions -
vcenter.fcpf.vsphere	Popen Remote Console	ary Monitor Configure Permissions Datastores Networks
V C FCPF_CLUSTER	Aligrate	Guest OS: Microsoft Windows 10 (64-bit) Compatibility: ESXi 6.7 and later (VM version 14)
172.16.10.101	Clone •	VMware Tools: Running, version:11265 (Current)
🛱 admin	Fault Tolerance	DNS Name: DESKTOP-REGRRJ2
Backup	VM Policies	View all 4 IP addresses
	Template +	Remote Console Host: 172.16.10.101
PDMSUN	Compatibility •	4
Reverse Proxy	Export System Logs	
	🔂 Edit Settings	hardware A
	Move to folder	CPU 4 CPU(s)
	Rename	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.

vm vSphere Client	Actions - admin	n in all environments
VM VSphere Client	Power Guest OS Snapshots Open Remote Console Open Remote Console Clone Fault Tolerance VM Policies Template	Image: Second system Image: Second system ACTIONS - ary Monitor Configure Permissions Datastores Networks Guest OS Microsoft Windows 10 (64-bit) Compatibility: ESXI 6.7 and later (VM version 14) VMware Tools: Running, version:11265 (Current) More info DNS Name: DESKTOP-REGRRJ2 IP Addresses: 172.16.10.59 View all 4 IP addresses Host: IP2.16.10.101 IP2.16.10.101
	Compatibility .	a 📲 💐
	Export System Logs	Hardware
	Bedit Settings	
	Move to folder Rename	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.

vm vSobere Cl	Actions - admin	asrch in all anuironments
viii vspilere ci	Power	Power On ctrl + alt + B
vcenter.fcpf.vsphe	Guest OS Snapshots	Power Off ctrl + alt + E ACTIONS ~ Il Suspend ctrl + alt + Z Permissions Datastores Networks
FCPF_CLUST	El 📇 Migrate 21 Clone	Shut Down Guest OS ctrl + alt + D ity: ESXi 6.7 and later (VM version 14) Sols: Running, version:11265 (Current) More info
🛱 admin	Fault Tolerance	DNS Name: DESKTOP-REGRRJ2
Backup	VM Policies	View all 4 IP addresses
	Template Compatibility	Unch Web Console Host: 172.16.10.101
Reverse P	Export System Logs	
	🛃 Edit Settings	VM Hardware
	Move to folder	> CPU 4 CPU(s)
	Rename	> 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"

🚱 vSphere - Backup - Summary 🗙 🕂	
← → C ▲ Not secure https://vcer	nter.fcpf.vsphere.ui/#?extensionId=vsphere.core.vm.summary&objectId=urn:vmomi:VirtualMachine:v
vm vSphere Client Menu v	Q Search in all environments
	🛱 Backup 📔 💌 🖉 🦻 🤷 🛛 Actions 🗸
 Conter.fcpf.vsphere FCPFDC FCPF_CLUSTER 172.16.10.101 172.16.10.102 admin Backup 	Summary Monitor Configure Permissions Datastores Networks Updates 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) More info More info DNS Name: WIN-02OUSONABHG IP Addresses: 172.16.10.51
NFMS PDMSLIN PDMSWIN Reverse Proxy	Launch Web Console Launch Remote Console 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:

3년 로- HOME VIEW	JOB				VEEAM BA	ICKUP AND REPLICAT	ION COMMUNITY E	NITION		
Start Step Retry Active	Statistics Re Details	eport Edit Disable De Manage Job	¢ ete							
HOME		Q. Type in an object in	ome to search for		×					
Jobs Backup	î	NAME 1 第 172.16.3.2	TYPE Windows Agent Backup Windows Agent Backup	OBJECTS	STATUS Stopped	LAST RUN 3 days ago	LAST RESULT Failed	NEXT RUN 11/7/2020 2:00 AM	TARGET filebackup	DESCRIPTION 172.16.3.2
Disk Disk Disk (imported) Disk (terminal Disk (te	v	蒙 NFMS 秦 PDMSLIN 秦 PDMSLIN 秦 ReverseProxy 秦 vcenter	VMware Backup VMware Backup VMware Backup VMware Backup VMware Backup VMware Backup	1 1 1 1 1	Stopped Stopped Stopped Stopped Stopped Stopped	59 minutes ago 23 hours ago 24 hours ago 22 hours ago 3 days ago	Success Success Success Success Success	11/4/2020 1000 11/4/2020 1200 11/4/2020 1200 11/3/2020 1100 11/4/2020 1:00 AM 11/6/2020 8:00 PM	vmbackup vmbackup vmbackup vmbackup vmbackup	NFMS PDMSLIN PDMSVIN Reverse ^p roly vcenter
BACKUP INFRASTRUCTUR	ie Re	C SUMMARY Duration: Processing rate:	DAT/ 15:04:57 Proc 190 MB/s Read	A essedt	2.2 TB (100%) 1.9 GB	STATUS Successi Warningsi	1 🖸	THROUGHPUT (ALL	TIME)	
	Dg 🛫	Bottleneck	Proxy Trans	sferred:	769.8 MB (2.5x)	Errors	0			Activate Windo Go to Settings to ac

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:

E- HOME BACKUP REPO	IDOLS IS/TORY					VEEAM BACKU	P AND RE	PLICATION	COMMUNITY EDITIO	N .=	
Add Edit Repository Repository Repository Manage Repository	Set A Permi M	scores Set ssions Location - anage Settings Tools									
BACKUP INFRASTRUCTURE		Q. Type in an object nan	ne to sea	rchi for	×						
Backup Denset Backup Repositories External Repositories WAN Accelerators Service Providers SureBackup HOME Fill ascentropy	Ŷ	NAME † Default Backup Rep Sitebackup wmbackup	T SMB SMB	HOST WIN	PATH C/Backup \\172.16.10.106\filebackup \\172.16.10.105\wnbackup	CAPACITY 39.4 GB 26.2 TB 26.2 TB	FREE	14.1 G8 0 8 18.8 TB	USED SPACE 08 15.8 TB 817.2 GB	DESCRIPTION Created by Vesam Backup Riebackup vmbackup	
[1] FILES	Cip 2										Activate Wind Go to Settings to

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.

Nemote	Desktop Connection	Ξ.	Ц	×
4	Remote Deskto Connection	p		
Computer:	172.16.3.2	~]	
You will be as	sked for credentials when you	connect.		
Show O	ptions	Connect	He	łp –

• 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

				-
SERVERFIPD20 Forward Lookup Zones fcpf.vsphere fipdof.maf.local googlevideo.com maf.gov.la www.youtube.com www.youtube.com youtube.com youtube.com youtube.com youtube.com youtube.com youtube.com youtube.com youtube.com youtube.googleapis.com youtube.l.google.com ytimg.l.google.com ytimg.l.google.com Global Logs	ame (same as parent folder) (same as parent folder) nfms	Type Start of Authority (SOA) Name Server (NS) Host (A)	Data [2], serverfipd20.fipdof.maf serverfipd20.fipdof.maf.local. 192.168.155.3	Timestarr static static 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

• 🔿 🔰 📰 🖾 🗟 🚺				
NS SERVERFIPD20 Forward Lookup Zones fcpf.vsphere fipdof.maf.local googlevideo.com maf.gov.la www.youtube.com youtube.com gyoutube.com gyoutube.com gyoutube.com gyoutube.lgoogleapis.com gyoutube.lgoogleapis.com gyutubel.googleapis.com gyutubel.googleapis.com gyutubel.googleapis.com gyutubel.googleapis.com gyutubel.googleapis.com gyutubel.googleapis.com gyutubel.googleapis.com gyutubel.googleapis.com gyutubel.googleapis.com gyutubel.googleapis.com gyutubel.googleapis.com gyutubel.googleapis.com gyutubel.googleapis.com gyutubel.googleapis.com gyutubel.googleapis.com gyutubel.googleapis.com gyutubel.googleapis.com gyutubel.googleapis.com	Name (same as parent folder) (same as parent folder) vcenter	Type Start of Authority (SOA) Name Server (NS) Host (A)	Data [4], serverfipd20.fipdof.maf serverfipd20.fipdof.maf.local. 172.16.10.5	Timestam static static 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

vm vSph	ere Client	Menu 🗸	Q Search in all environments	
	()	Q	Reverse Proxy P P P P P Actions	Unriates
 FCPFDC FCPF FCPF T72 T72<!--</td--><td>_CLUSTER .16.10.101 .16.10.102 min ckup MS MSLIN MSWIN</td><td></td><td>Guest OS: Ubuntu Linux (64-bit) Compatibility: ESXi 6.7 and later (VM version 14) VMware Tools: Running, version:11296 (Guest Managed) More info DNS Name: reverseproxy IP Addresses: 10.0.6 Launch Web Console Launch Remote Console Guest OS: Ubuntu Linux (64-bit) Running, version:11296 (Guest Managed) More info DNS Name: reverseproxy IP Addresses: 10.0.6 View all 2 IP addresses Host: 172.16.10.101</td><td></td>	_CLUSTER .16.10.101 .16.10.102 min ckup MS MSLIN MSWIN		Guest OS: Ubuntu Linux (64-bit) Compatibility: ESXi 6.7 and later (VM version 14) VMware Tools: Running, version:11296 (Guest Managed) More info DNS Name: reverseproxy IP Addresses: 10.0.6 Launch Web Console Launch Remote Console Guest OS: Ubuntu Linux (64-bit) Running, version:11296 (Guest Managed) More info DNS Name: reverseproxy IP Addresses: 10.0.6 View all 2 IP addresses Host: 172.16.10.101	
Rei Voe	verse Proxy inter		VM Hardware	Notes
			> CPU 2 CPU(s)	Edit Notes .
			> Memory 4 GB, 0.04 GB memory active	Custom At
			> Hard disk 1 40 GB	Attribute

Then login with the credentials:



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: Usage of /: 25.4% of 39.12GB Memory usage: 7% Users logged in: 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\$ 11 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



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 <u>https://172.16.10.103:8088</u>, then fill in login credentials:





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

 Huawei, Storage > Provisioning 	2	?
Create Disk Domain Create Storage Pool Create LUN Create LUN Group		Rine Home
Suggested Configurations Flow		System
Block Storage Service Host	Mapping View	(C) Provisioning
Create and runage LUNs or LUN groups. Perform resource optimization or data protection on LUNs. Storage Configuration and Optimization	Create and manage mapping views.	Data Protection
Disk Domain Create and manage disk domains. Update keys of encrypted disk domains.	Port Configure and manage front-end ports or port groups.	Monitor
Application Batch Configuration		0

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 <u>http://172.16.10.105:5000</u> for NAS1 and <u>http://172.16.10.106:5000</u> for NAS2, then fill in the login credentials:



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.

		File St	tation	7 - E X
	< > C vmbac	kup	-	P - Search
File Station	Upload • Create •	Action - Tools - Settings		≡ - ≣4
	▼ nas001	Name	Size File Type	Modified Date
	home	2 #recycle	Folder	09/27/2020 00:00:48
DSM Help	homes	E NFMS	Folder	11/04/2020 13:05:07
contractor.	▶ vmbackup	NFMS_VMs	Folder	09/17/2020 14:21:14
		PDMSLIN	Folder	11/04/2020 15:02:46
- 74		PDMSWIN	Folder	11/04/2020 14:05:55
Storage		ReverseProxy	Folder	11/04/2020 16:02:15
Manager		e vcenter	Folder	11/01/2020 10:13:33
		VeeamConfigBackup	Folder	09/17/2020 00:00:26
isesi				
SCSI Manager				
Control Panel				

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.

← → C ▲ Not secure	172.16.10.106:5000						
		File	Station		7	_	E X
	C fileback	up		*	₽ Search		
File Station	Upload • Create •	Action • Tools • Settings				=	+E4
	▼ nas002	Name	Size	File Type		Modified	Date 1
	▶ filebackup	🗑 #recycle		Folder	09/18/2	020 12:0	4:42
DSM Help		172.16.3.2		Folder	09/21/2	020 13:1	0:22
		<u> </u>		Folder	09/19/2	020 10:4	3:10
Storage Manager ISCSI ISCSI Manager Control Panel							
						3 item(s	c