Deployable Defensive Cyber Operations (DCO) System – Modular (DDS-M) Installation/User/Admin Guide

Prepared By:
Cyber Platforms and Systems (CPS)
9625 Middleton Road, Bldg. 1189 B
Ft. Belvoir, VA 22060

Table of Contents

Version History

Date	Changes	Revision
May 2024	Document Creation	1

1. User Manual

1.1 Foreword

This document details the steps required to build and deploy a DDS-Mv1E or DDS-Mv2. The wiring for DDS-Mv1E can be found here and DDS-Mv2 can be found in here.

1.1.1 Resources

For installation or operation support of this hardware please contact the **Tobyhanna Army Depot - Fort Gordon (Armory)** via one of the following methods:

Email: usarmy.gordon.tyad.list.armory-civ@army.mil

Phone: 1-570-615-4DCO (4326)

1.2 VMware Overview

VMware vSphere is VMware's virtualization platform, which transforms data centers into aggregated computing infrastructures that include CPU, storage, and networking resources. vSphere manages these infrastructures as a unified operating environment and provides you with the tools to administer the data centers that participate in that environment.

The two core components of vSphere are ESXi and vCenter Server. ESXi is the virtualization platform where you create and run virtual machines and virtual appliances. vCenter Server is the service through which you manage multiple hosts connected in a network and pool host resources.

vSphere

The core ability of vSphere is the centralized management of your virtual machines and virtual environment.

vCenter Server

As a component of vSphere, vCenter is designed to allow server management capabilities through a centralized platform. It enables visibility across the environment, while automating and delivering virtual infrastructure. It allows you to manage ESXi hosts and virtual machines.

ESXi

ESXi is the other main component of vSphere. It is a bare-metal hypervisor, which means it is installed directly on the hardware of the machine, between the hardware and the operating system. Because the bare-metal hypervisor separates the Operating System from the underlying hardware, the software no longer relies on, or is limited to, specific hardware devices or drivers. This allows us to run multiple Operating Systems and virtual machines on the same physical machine and they can more easily shift and reallocate resources, as needed.

1.3 Node deployment procedures

1.3.1 Node BIOS settings

When using SN3000 nodes that were not previously being used for a DDS-Mv1E, it may be necessary to adjust the BIOS to the following configurations:

✎ **Note:** These steps will need to be repeated for each node. Take note of IPMI differences between nodes.

1. Configure EFI
    a. **Setup Menu** ([**DEL**] during boot) -> **Advanced** tab -> **PCIe/PCI/PnP Configuration**
        i. Set **CPU SLOTS6 PCI-E 3.0 X16 OPROM** to **EFI**
        ii. Set **CPU SLOTS7 PCI-E 3.0 X8 OPROM** to **EFI**
        iii. Set **JMD1:M.2-HC PCI-E 3.0 X4 OPROM** to **EFI**
        iv. Set **JMD2:M.2-H PCI-E 3.0 X2 OPROM** to **EFI**
        v. Set **PCI-E 3.0 X1 OPROM** to **EFI**
        vi. Set **Onboard LAN Option ROM** Type to **EFI**
        vii. Set **Onboard Video Option ROM** to **EFI**

✎ **Note:** If the node has been reset to factory default, you may also need to change the following:

        i. Set **SR-IOV** to **Enabled**.
        ii. Set **NVMe Firmware Source** is set to **AMI Native Support**

2. Setup IPMI
    a. **Setup Menu** -> **IPMI** tab -> **BMC Network Configuration**
        i. Set **Update IPMI LAN Configuration** to **yes**
        ii. Set **Configuration Address Source** to **Static**
        iii. Set **Static IP Address** to appropriate address
            - Bastion Node is 192.168.0.2
                - Set Subnet Mask to 255.255.255.0
                  Set Gateway IP Address to 192.168.0.1
            - The last octet of standard non-Bastion nodes will increment in order by 1 starting at 192.168.0.20 (192.168.0.21, 192.168.0.22, etc…)
                - Set Subnet Mask to 255.255.255.0
                  Set Gateway IP Address to 192.168.0.1

3. Set Boot to UEFI
    a. Setup Menu -> Boot tab
    b. Set **Boot mode** to **UEFI**
    c. Set **Legacy to EFI support** to **Disabled**

4. Save Changes and Exit (**F4**).

✎ Note: You must Save & Exit (F4) after Step 3 in order to see the necessary options for step 5.

5. Set Boot Priorities
    a. Setup Menu -> Boot tab
    b. UEFI NETWORK Drive BBS Priorities
    c. Boot Option #1
        i. Select **(B181/D0/F3) UEFI: PXE IPv4 10GbE SFP+**
        ii. ESC out of the current Menu
    d. UEFI Boot Option #1
        i. Select **UEFI Hard Disk**
    e. UEFI Boot Option #2
        i. Select **UEFI Network: (B181/D0/F3) UEFI: PXE IPv4 10GbE SFP+**

6. Save Changes and exit (**F4**).

1.3.2 Bastion Build

This section assumes that the kit has been cabled properly.

This step should typically be done through IPMI from the Admin Laptop. You can access this by going to 'https://192.168.0.2' in a web browser, logging in and clicking the "**remote console preview**". Ensure that you have an ethernet cable going from the IPMI port of the Admin Laptop to the Bastion node.

1. Plug the Bastion USB Drive into the designated Bastion node.

2. Reboot the device.

3. Click [**f11**] to enter the boot menu.

4. Select the USB device used in the first step for UEFI boot.

5. Enter the following information, when prompted:
    a. Wipe Drives? :
        i. Type '**y**'
        ii. To confirm, type **'y'**
    b. Enter your kit number: **<kit #>**
    c. Enter your DDSM Hardware Version: **<Select appropriate version.>**
    d. Please select your drive number for the installation(1-5): **nvme0n1 <usually 5>**
    e. Confirm (y/n):
        i. Type '**y**'

6. After the node reboots (~20min). log in to the GUI.
    a. You will be required to unlock the drives because they are encrypted.
    b. Log in as defender with the new default password.
    c. open a terminal and escalate to root

```
$ sudo su (or sudo -i)
```

    d. Attach to the install tmux session and watch until it is done.

```
# tmux a
```

✎ **Note:** This will take at least 3hrs from this step. Do not interrupt the process.

1.3.3 Deploy Laptop

1. Plug the laptop into **Port 12** of the **T-switch**.

2. Power on the laptop and press [**f12**] to PXE boot.

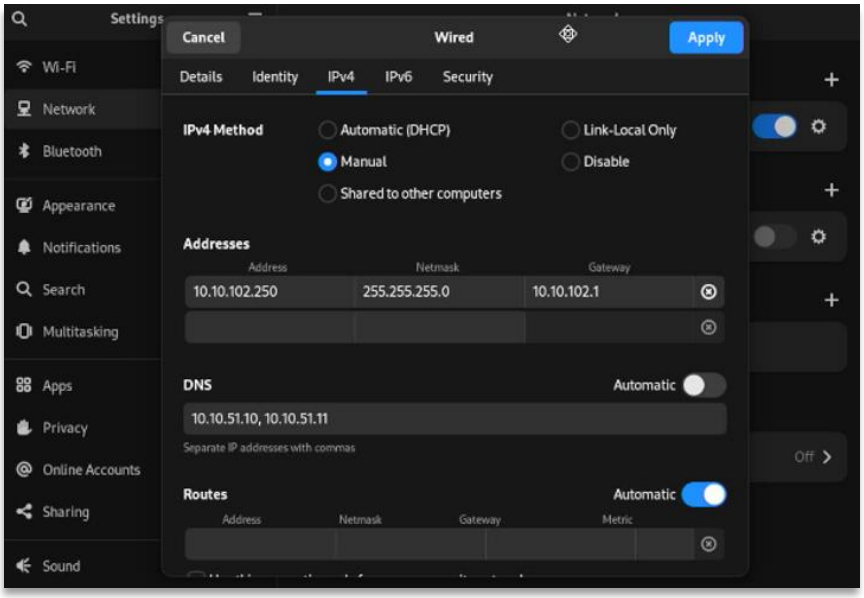
3. When prompted, enter a secure password for the laptop.

4. When prompted, unlock the vault with the vault password.

5. The Admin Laptop can be accessed using the username defender.

6. After the install is finished, set a static IP address.

    a. Open the network GUI and edit the wired interface to set the following:
        - IPV4 Method: Manual
        - Address: 10.<kit#>.102.250
        - Netmask: 255.255.255.0
        - Gateway: 10.<kit#>.102.1
        - DNS: 10.<kit#>.51.10, 10.<kit#>.51.11
        - Routes: Automatic



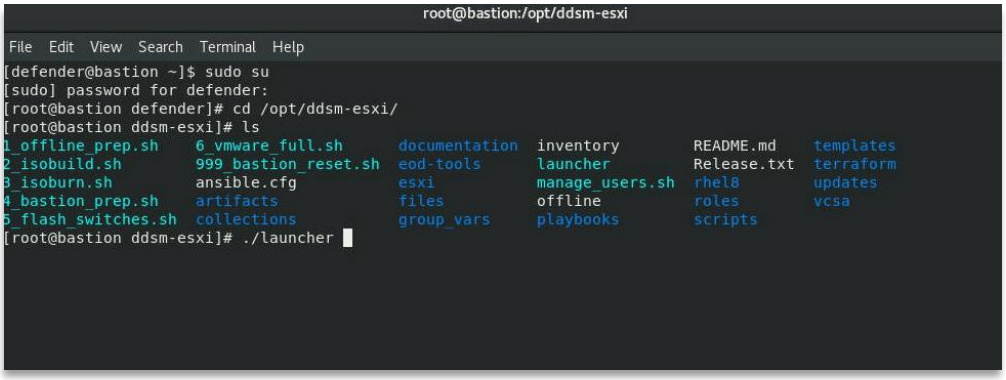
1.3.4 Deploy switch operational configurations

✎ **Note:** Successful deployment requires the switches to either be in a factory default state (See here for instructions on resetting the various switches) or previously used on the same type of kit (v1E or v2) currently being deployed on.

✎ **Note:** TFTP should be enabled by default, but ensure that it is or the switches will fail to deploy.- The status can be verified by the command 'sudo systemctl status tftp'. If tftp is disabled, type 'sudo systemctl start tftp'. You can also temporarily enable TFTP from the launcher, under Admin Menu.

1. Open a terminal on the bastion (either via ssh or IPMI) and navigate to the ddsm-esxi directory.

```
# cd /opt/ddsm-esxi
```

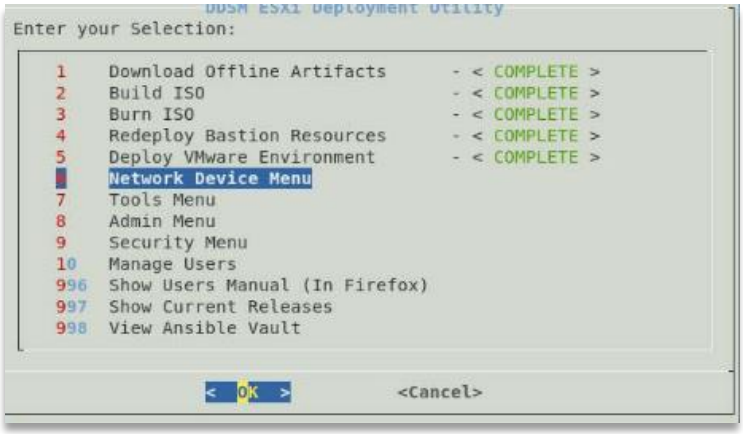


2. Start the launcher

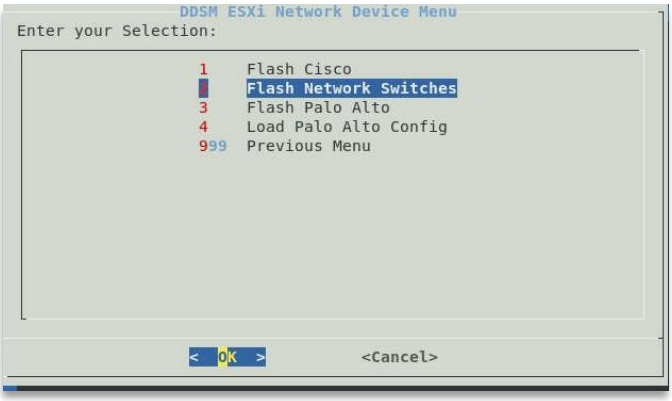
```
# ./launcher
```

3. Click [**enter**] to **unseal vault**.

4. Select **Network Device Menu**.



5. Select **Flash Network Switches**

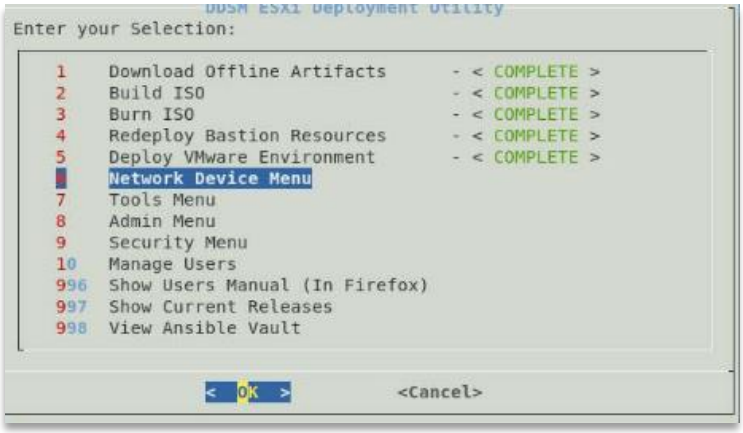


1.3.5 Deploy Cisco switch

✎ **Note:** Ensure that the Cisco has been reset to factory default settings prior to attempting these steps.

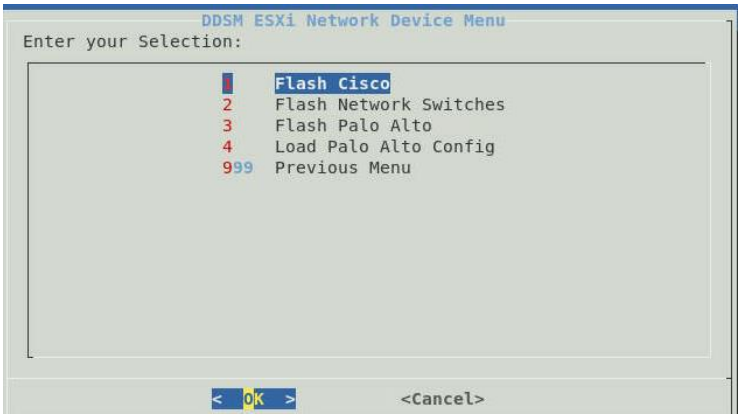
1. From the Bastion, go to the launcher menu.

2. Choose **Network Devices Menu**.



✎ **Note:** Ensure that only the cable from the bastion to the Cisco is plugged in during the following step.

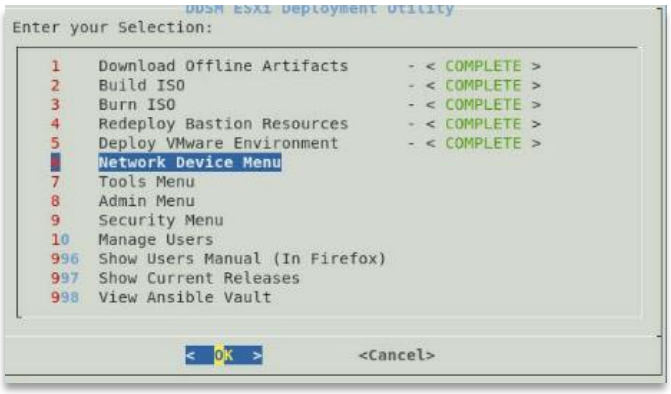
3. Choose **Flash Cisco**.



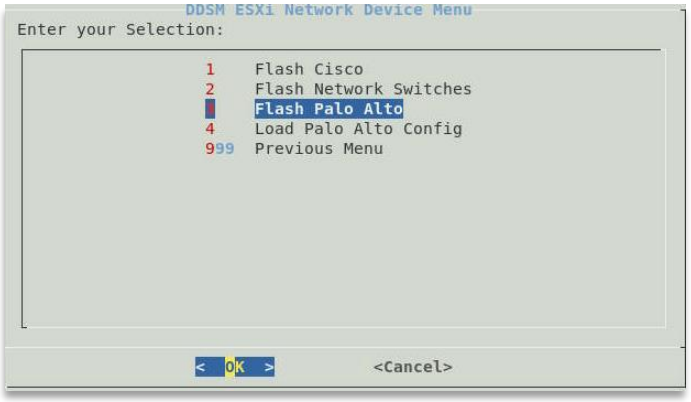
After some time, the cisco will be successfully flashed and upon reboot, it should DHCP from the Bastion and configure itself. This process takes around 40 minutes and should not be interrupted.

1.3.6 Deploy Palo Alto

1. From the Bastion, go to the launcher menu and select **Network Devices Menu**.

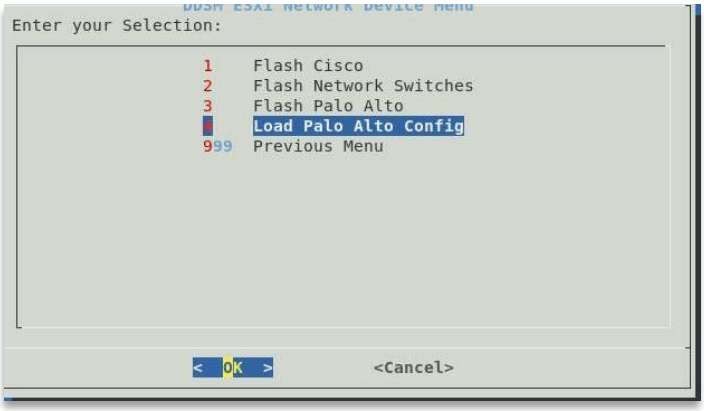


2. Select **Flash Palo Alto**.



✎ **Note:** This step takes a few minutes to complete. Allow at least 5 minutes before moving to step 3.

3. After the Palo Alto has been successfully flashed, select **Load Palo Alto Config**.

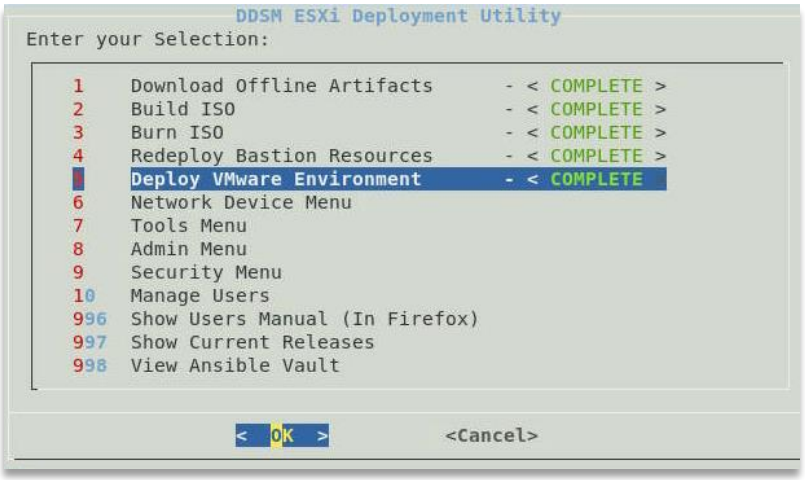


1.3.7 Deploy VMware

1. From **/opt/ddsm-esxi** on the bastion, start the launcher

```
# ./launcher
```

2. Select **Deploy VMWare Environment**.



3. When prompted, enter the number of nodes.

After completion of this step, there are some additional steps that should be completed to properly utilize the system. These include creating the vSAN cluster, enabling cluster DRS, and enabling CAC authentication.

1.3.8 Reporting issues with node deployments

The bastion host is a log server.

All of the logs for the kit builds are in “/var/log/rsyslog/<host>”

For installation or operation support of this hardware please contact the **Tobyhanna Army Depot - Fort Gordon (Armory)** via one of the following methods:

Email: usarmy.gordon.tyad.list.armory-civ@army.mil

Phone: 1-570-615-4DCO (4326)

1.3.9 Kit authentication and passwords

When the kit is initially deployed, passwords can be viewed in the “/opt/ddsm-esxi” directory and using the launcher. To view passwords, do the following:

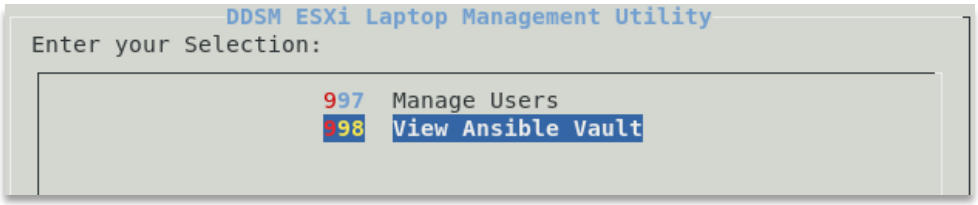
1. Open a terminal on the Admin Laptop and navigate to the ddsm-esxi directory.

```
$ cd /opt/ddsm-esxi
```

2. Start the launcher

```
$ ./launcher
```

3. Click enter to **unseal vault**.
4. Enter the vault password
5. Select View Ansible Vault



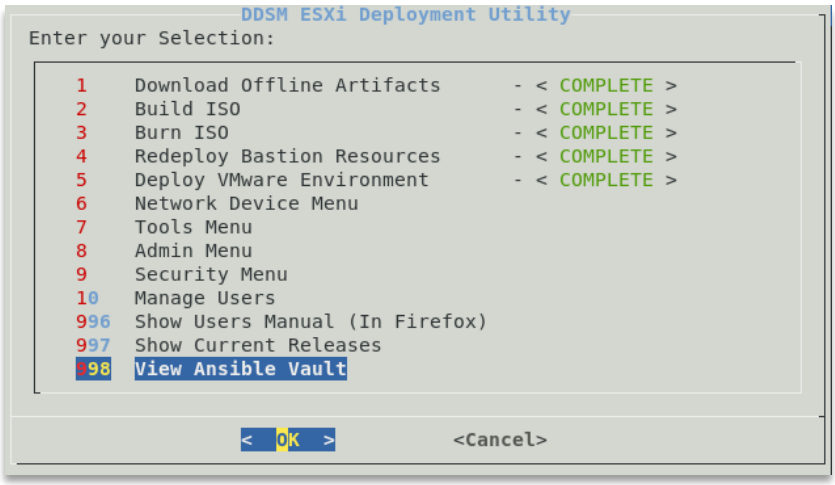
Relevant usernames can be found in “/opt/ddsm-esxi/group_vars/all” in the file “users.yml”.

Deploy Tools

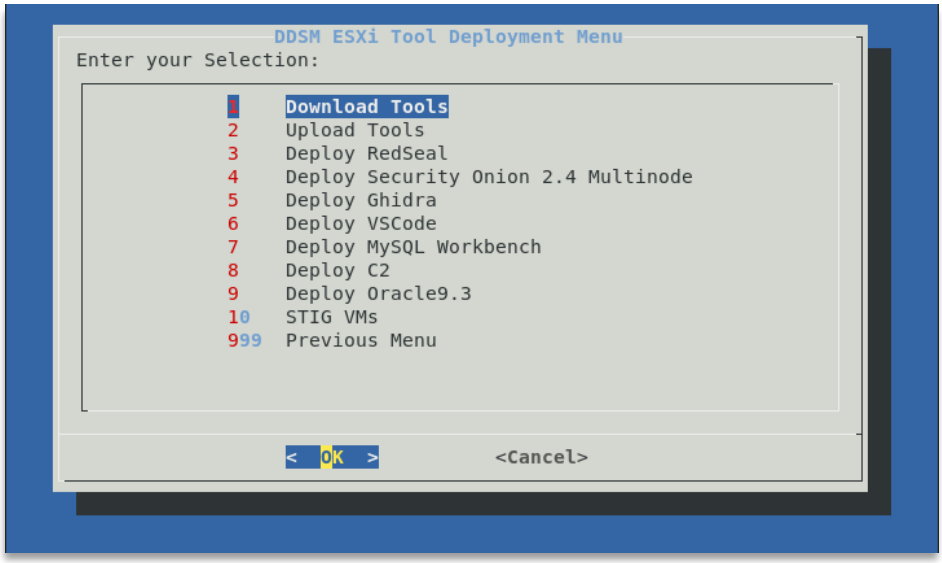
1. From **/opt/ddsm-esxi** on the bastion, start the launcher

```
# ./launcher
```

2. Select Tools Menu.



3. Select upload tools.



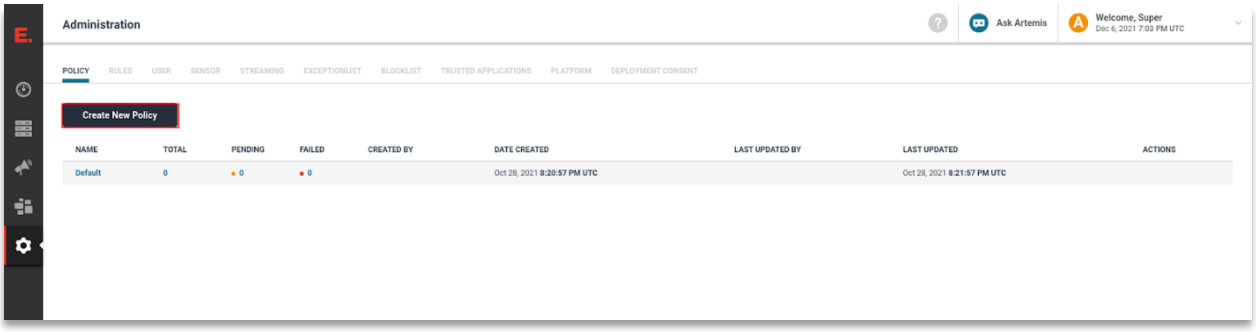
4. After the tools have been uploaded, return to the Tools Menu and select the tool you wish to deploy.

If deploying Redseal or endgame, there are some extra configuration steps required that are detailed below.

1.3.9.1 Endgame configuration

1. Login to the Endgame WebUI
   https://endgame.{{ kit_num }}cpt.cpb.mil/login

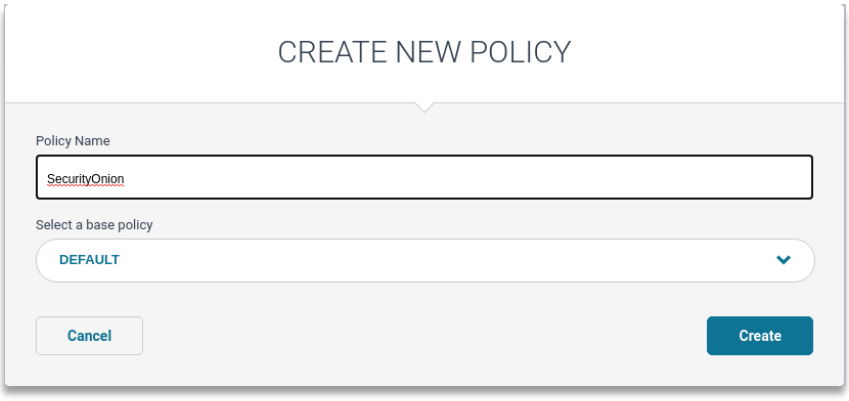
2. Navigate to **Administration** and click on **Policy** and then "**Create New Policy**."



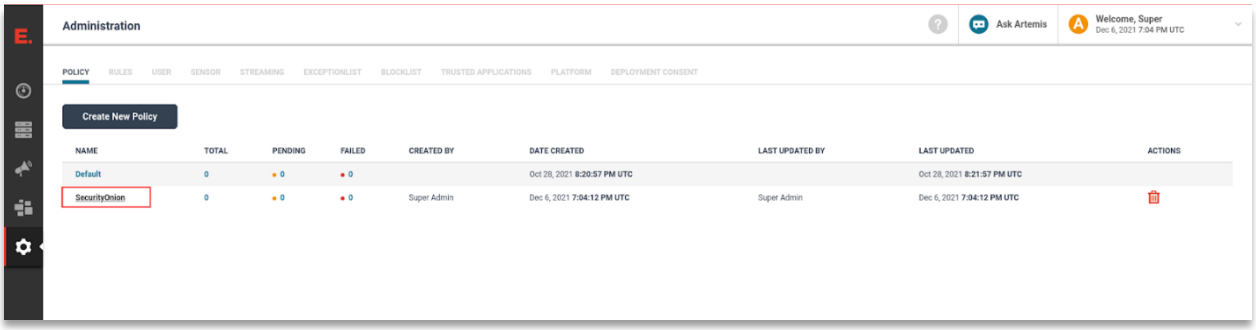
3. Create the policy for security onion using the following:

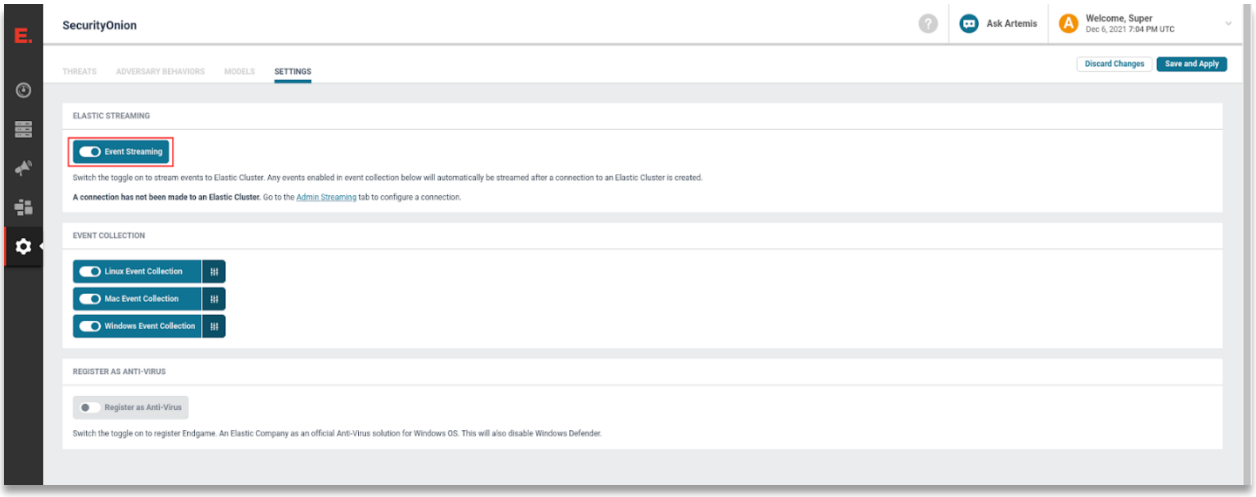
   Name: SecurityOnion

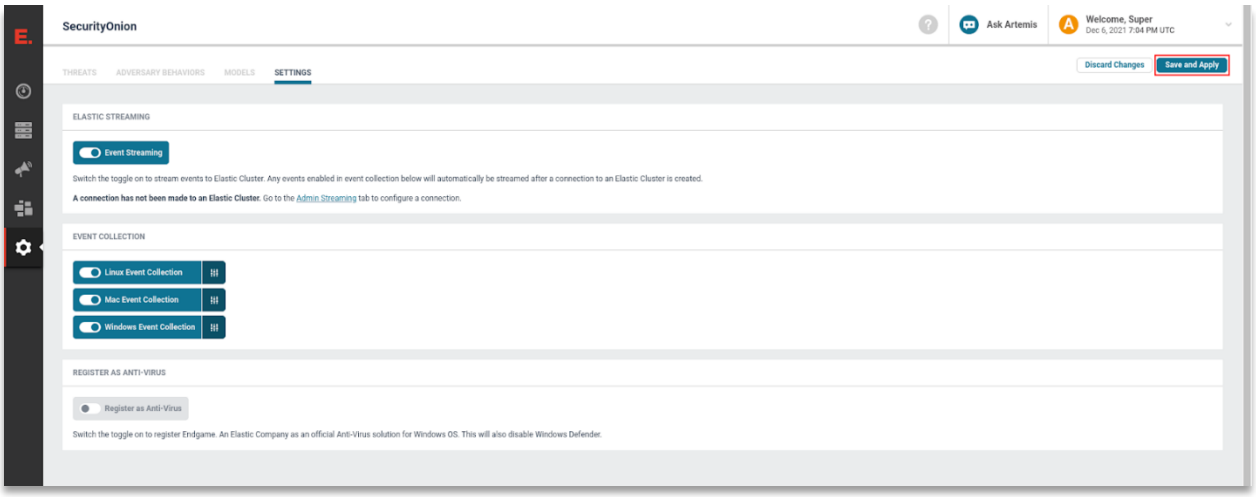
   Base Policy: Default



4. Click on the newly created policy and navigate to the **Settings** tab; toggle **enable event streaming** then click "**save and apply**", "**save changes**," and "**finish**."

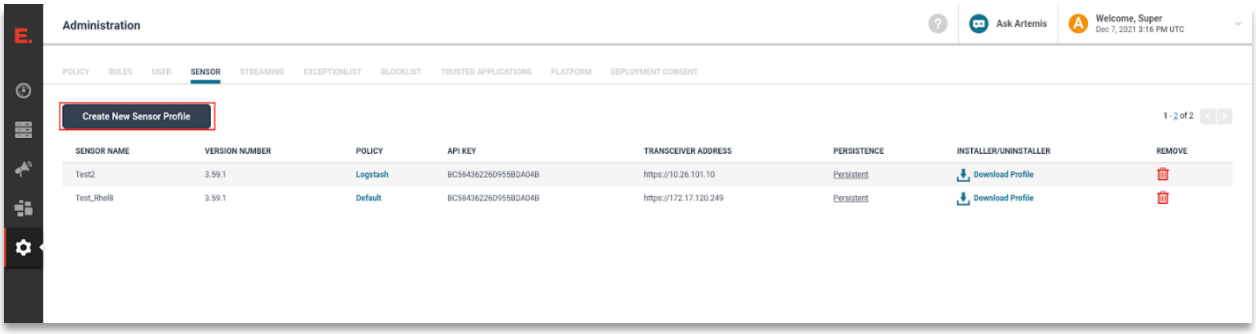






1.3.9.2 Configure Endgame Sensor Profile

1. Navigate to the Administration tab and click on Sensor then “Create New Sensor Profile”



2. Create the Sensor profile with the following information:

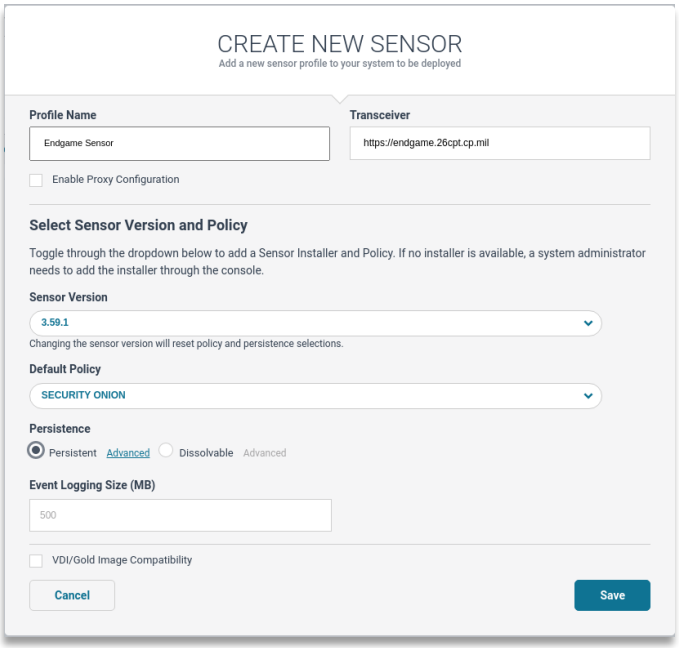
   Name: Endgame sensor

   Transceiver: https:// {endgame url} (you can use the ip or the hostname)

   Default policy: security onion policy

   Persistence: persistent

   Save



1.3.9.3 Redseal Configuration

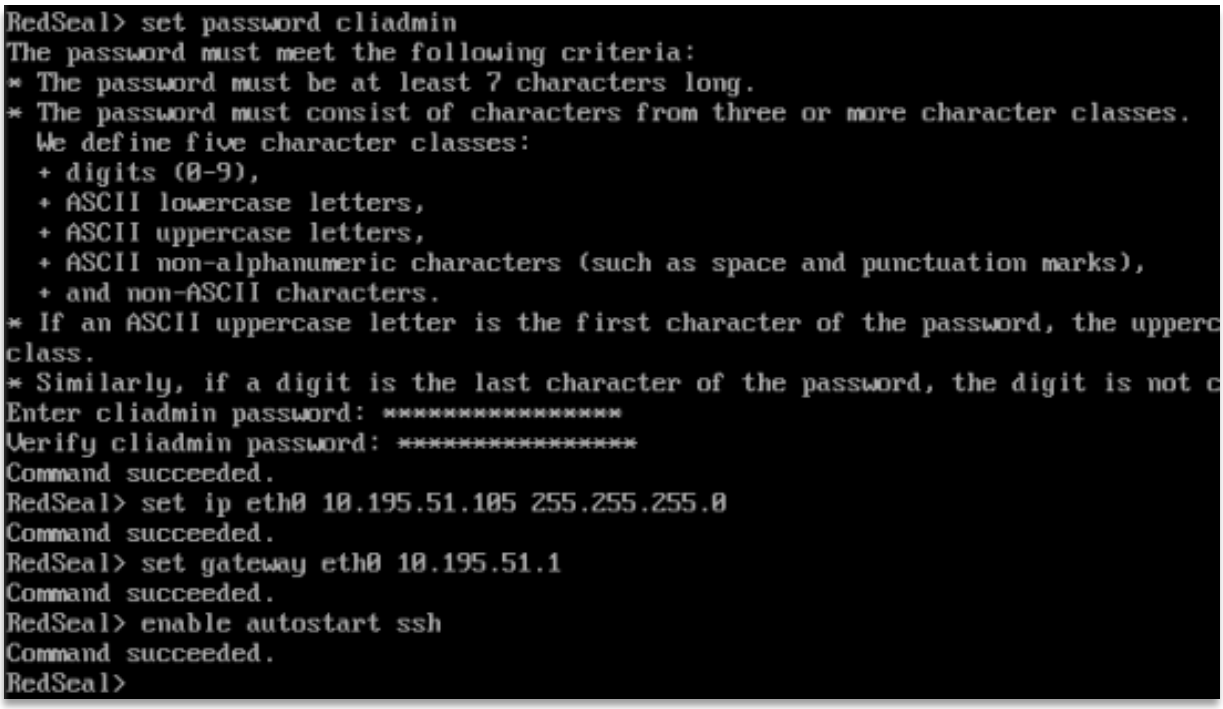
1. Power on the VM and access the console.

2. Type set password cliadmin

3. Type set ip eth0 10.<kit#>.101.110 255.255.255.0

4. Type set gateway eth0 10. <kit#>.101.1

5. Type enable autostart ssh



6. SSH to the RedSeal VM IP

7. Type set license

```
RedSeal> set license
Paste the license information that was received, including the envelope
(the 'begin' and 'end' lines before and after the text).
Hit Control-D after the license has been pasted.
--begin license--
AANTUk0AAAAAP+07zr9JCokf6ty5qG/BHroXw98sJ0/vCBf4/EzUdQQm1d+2dfNncytHvT0bjnjj
EdUTU94dA6yNfRrPFVjFjtxUKcNI0N8WhX0Ree4esC1kkfs1O/mVobUzv5UktQGVJlGP5vwJxIaN
eKTJuOoeUwRy58jnDaFBfgLawtklBJbXhPSer5C5qadANrvukDj+paCrlQxCWOGllBMwfuzics9t
7vhDjV8hGUTd8fFhmte33+TNljw2LWRdWi/1ydllgaC6VX91wvEtyHz/1JBx/MZiG5tcMdFMnxe2
EI2tYSnAcYH3yf09Pi0qJobKIIaxX9/bHG+cKrjilwxizingzckIWOo3OZQiBxaQ/TM3hupN/eJg
JPE0KqZrxyDyB6Wm9ys7CR5+nMIuW32OfFYgiB/AjXtFTQ4hBH01ZH2LMz8CHqvTO5mvGE/O/4V0
ri2Eb0ZDAJrEkRrR15wB9s8pNAaR5+u5Q/aSvr5pBgj+f/oBCTDbJvjGAjBSyaJVg6sZ/XMN3Zb9
l4tN/Z/f/3/TiFVujjHKTsRo/Qol44GdWFj8xj3sGLfk+LupJPrgwXOu5b8qdPnB2XL5jJ69EVsP
Q0deDsPBXpAgc40XVdmv2iks0WvTQTiMwJ5pqGv4QYHBsKIgPzEcdwq/Zis4g5siKoB8qY7ldDht
```

8. Copy/paste the entire contents of the license file

9. Prese “Ctrl-D” once complete

```
RedSeal> show license
License Status                          = Valid
License Expires On                      = Apr 19, 2023
Maintenance Expires On                  = Apr 19, 2023
License Model                           = Device Limit
Node Locked                             = Unlocked
Number of L3 Devices                    = 0/10000 (in use/licensed)
Total Number of Routing Tables          = 0
Routing Tables Requiring License        = 0
```

10. Type **show license** (validate license)

11. Type startup server

```
RedSeal> startup server

You must first set the data password.
The password must meet the following criteria:
* The password must be at least 7 characters long.
* The password must consist of characters from three or more character classes.
  We define five character classes:
  + digits (0-9),
  + ASCII lowercase letters,
  + ASCII uppercase letters,
  + ASCII non-alphanumeric characters (such as space and punctuation marks),
  + and non-ASCII characters.
* If an ASCII uppercase letter is the first character of the password, the uppercase letter
d toward its character class.
* Similarly, if a digit is the last character of the password, the digit is not counted tow
ter class.
Data password should not contain the following restricted characters: + \ , : " < > #
Enter data password: ****************
Verify data password: ****************
```

12. Set data and uiadmin passwords

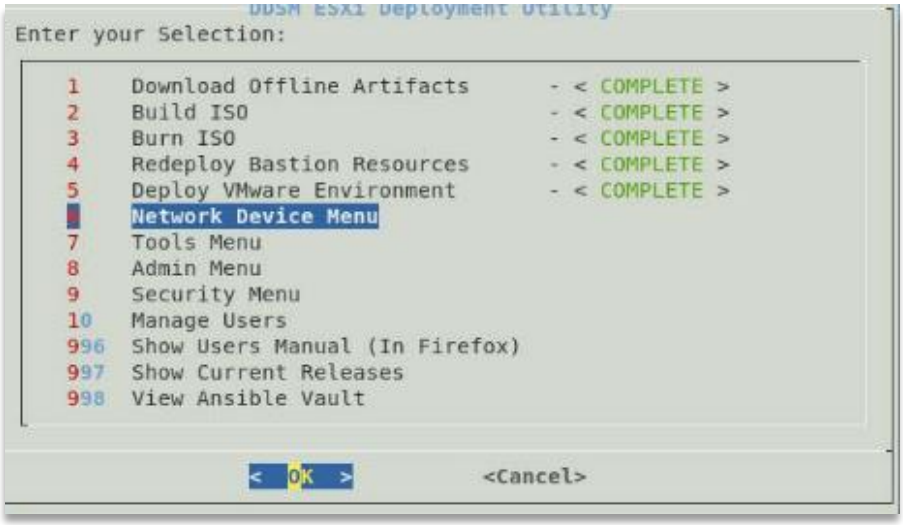
```
You must also first set the uiadmin password to allow for uiadmin GUI
The password must meet the following criteria:
* The password must be at least 7 characters long.
* The password must consist of characters from three or more characte
  We define five character classes:
  + digits (0-9),
  + ASCII lowercase letters,
  + ASCII uppercase letters,
  + ASCII non-alphanumeric characters (such as space and punctuation
  + and non-ASCII characters.
* If an ASCII uppercase letter is the first character of the password
d toward its character class.
* Similarly, if a digit is the last character of the password, the di
ter class.
Enter uiadmin password: ***************
Verify uiadmin password: ***************
```

13. Use the command **status all** to monitor server startup (Validate server-https is auto enabled and running)

14. Use Firefox to access the RedSeal WebUI

1.4 Launcher Menu

The “launcher” located in “/opt/ddsm-esxi/” has been created to automate as much of the kit deployment tasks as possible. However, there are other options available for users with specific use cases. This section details the options listed in the launcher menu and a brief explanation of what their function is.



Download Offline Artifacts

This option will create new directories containing the artifacts and tools required to build the iso and the kit. Most users should not have to select this option since the drive sent to mission teams will already have this done.

Build ISO

This creates “/var/iso”, extracts the contents of the RHEL8 CD-ROM to “/var/iso”, put's a copy of this GitLab project (with downloaded artifacts) into “/var/iso/ddsm-esxi”, and then creates an iso from the resultant folder.

Burn ISO

Assembles the contents of the ISO onto the drive, making it “boot-ready”

Redeploy Bastion Resources

Rebuilds the Bastion and all its resources from scratch. Used primarily as a last case scenario if everything is broken and the user wants to start over.

Deploy VMWare Environment

Deploys 1-9 ESXi hosts, Deploys vCenter, Configures Datacenter (Datacenter/Cluster/Networking/etc.), Uploads ISOs (LTAC, SecOnion, RHEL8, etc.), Deploys OVAs (VSAN Witness/PA VM-500), Uploads Tool OVFs, Applies STIG to ESXi Hosts, Applies STIG to vCenter Appliance, Joins vCenter to the Windows Domain, Enables MFA for VMware environment

Network Device Menu

Menu containing various options for flashing and configuring the network devices. This includes the dell switches, Cisco switch, and the Palo Alto.

Tools Menu

Contains submenu for:

- Upload Tools
- Deploy RedSeal
- Deploy Security Onion 2.4 Multinode

Admin Menu

Contains submenu for:

- Flash/Configure SuperMicro BIOS
- Run Wipefs Automation
- Enable TFTP for 2 hours
- Reset Bastion Host

Security Menu

Contains submenu for:

- Run Nessus Scan on kit
- Re-Run Evaluate STIG

Manage Users

Contains submenu for:

- Add Standard Users
- Add Admin Users
- Delete Users

Show Users Manual (In Firefox)

Brings up relevant documentation in a Firefox browser.

Show Current Releases

Shows version number of various kit resources, such as ESXi on DDS-M (EOD) version number and Tools version number.

View Ansible Vault

Opens the vault that contains all relevant default passwords for the kit.

2. Installation Manual

2.1 DDS-Mv1E

Introduction

The Deployable Defensive Cyber Operations (DCO) System – Modular version 1 Enhanced, or Echo (DDS-Mv1E) is a modular fly-away computing cluster that is purpose-built for conducting Defensive Cyber Operations (DCO) missions. This kit was built to provide an easily deployable hardware platform for the US Army and their DoD mission partners. The flagship DDS-Mv1E kit consists of 1 backpack and 3 protective cases containing multiple server nodes, switches, a network tap, a hardware firewall, and the required cables and accessories.

Additionally, the kit has been constructed to be transportable in the overhead compartment of an airplane and configured in under an hour at the designated customer location.

Document Conventions
Text in **bold** represents text to be typed or an action to be taken.
Graphics are only for illustration. They should contain no required technical content.

Contact

For installation or operation support of this hardware please contact the **Tobyhanna Army Depot - Fort Gordon (Armory)** via one of the following methods:

Email: usarmy.gordon.tyad.list.armory-civ@army.mil

Phone: 1-570-615-4DCO (4326)

Safety Summary

The following are general safety precautions and instructions not related to any specific procedure and, therefore, do not appear elsewhere in this manual. These are recommended precautions and procedures that personnel must understand and apply during many phases of operation and maintenance.

Overall Precautions

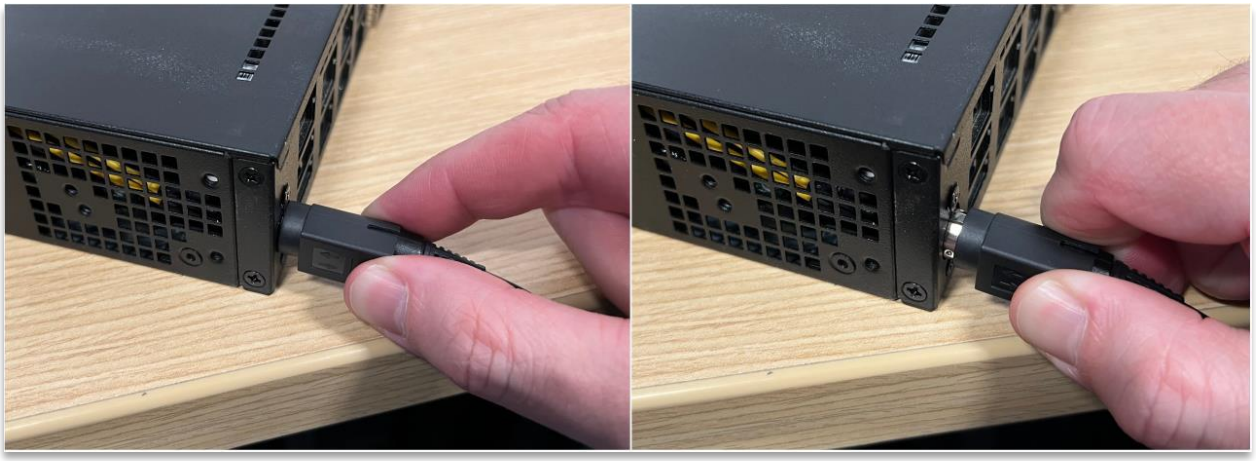
- Become familiar with the documentation safety sections.
- Do not make any unauthorized alterations to the equipment.
- Do not reconfigure while the set is powered up.
- Do not power off the kit without following the startup/shutdown procedures.
- Do not pull cables by the cord.
- Do determine the appropriate power requirements for the operating location and use a power strip that is rated for that environment.

- Installers should prepare a cable plan for routing all cables over a common path away from high-traffic areas.

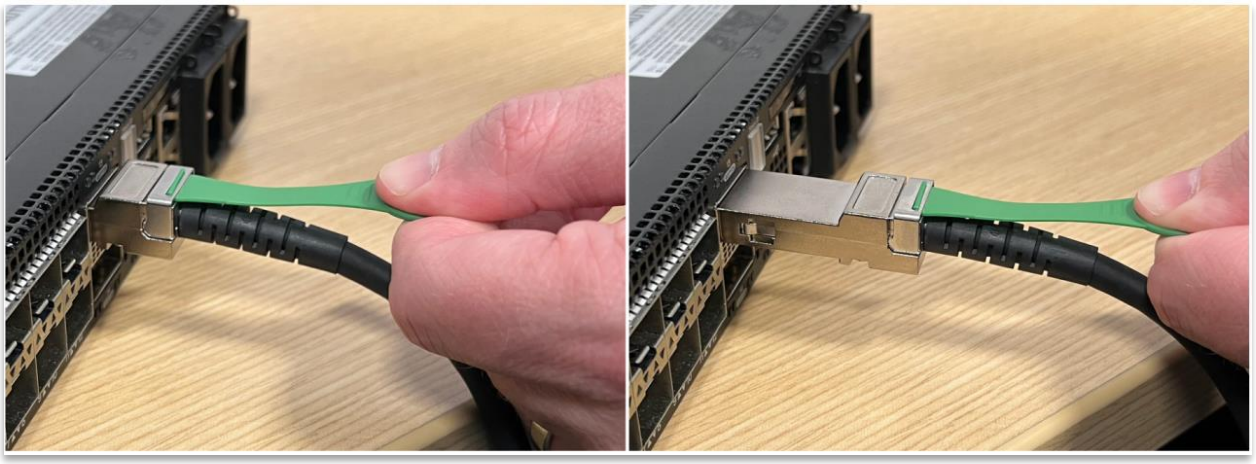
✎ Note: DO NOT UNPLUG CABLES BY PULLING ON THE CORD

Ensure you are following the proper procedures for unplugging cables from the kit.

To unplug power from the nodes, pull the power cable by the spring-tensioned release mechanism.



To unplug the QSFP or DAC cables, including the 100G stacking cable between the switches and the 40G breakout cables, pull on the release mechanism on both ends.



2.1.1 System Overview

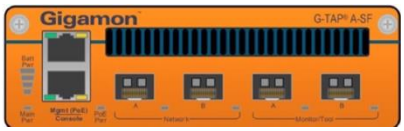
2.1.1.1 Functional description

DDS-Mv1E is a comprehensive, lightweight, and rapidly mobilized system that allows for users to perform a wide range of cyber defensive mission activities. The overall system is transported in 1 backpack and 3 carry-on compliant cases. Its modular design allows a team to deploy a virtualized environment being run on anywhere from 1-7 servers, and its portability allows teams to maintain positive control of the system while traveling.

2.1.2 Visual components breakdown

This section serves to provide illustrative reference for the physical components included in DDS-Mv1E. This kit should not be used for conducting kit inventory. It is simply a reference. Refer to the inventory list received at checkout of the kit and the component cards contained in each case of the kit for exact components of your specific kit.

Component	Image	Quantity
Dell Laptop		1
Laptop Power Supply		1
Tripp Lite 6-Port Surge Protector		1
APC 8-Port Surge Protector		1

Server Nodes		8
Server AC/DC Power Adapter		8
Dell S4112-F Switch		1
Dell S4112-T Switch		1
Palo Alto Networks PA-440		1
Dell Power Cable (C13 to 5-15P)		2
Micro-USB Console Cable (Dell Switch)		2
Gigamon A-Tap		1
Cisco Catalyst Operator Switch		1

Cisco Power Cable (C15 to 5-15P)		1
Mini-USB Console Cable (Cisco Switch)		1
Startech Mobile Console Adapter		1
0.5m SFP+ Direct Connect (DELL)		8
1.0m SFP+ Direct Connect (DELL)		8
3.0m SFP+ Direct Connect (DELL)		2
1.0m QSFP Breakout Cable (DELL)		4
RJ45 SFP+ Module (Gigamon)		2

LR-Fiber SFP+ Module (Gigamon)		2
SR-Fiber SFP+ Module (Gigamon)		2
LR-Fiber SFP+ Module (Intel)		4
SR-Fiber SFP+ Module (Intel)		4
RJ45 SFP+ Module (DELL)		4
LR-Fiber SFP+ Module (DELL)		4
SR-Fiber SFP+ Module (DELL)		4
3.0 ft CAT 6e (Black)		9

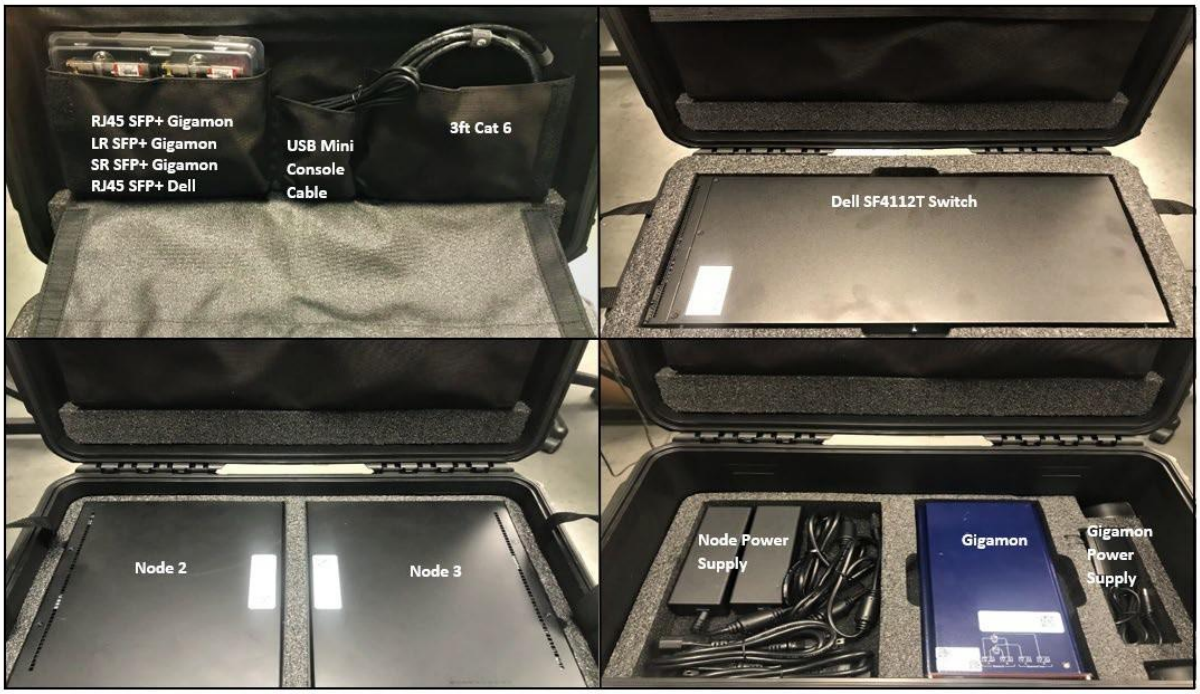
6.0 ft CAT 6e (Black)		3
2.0m Ruggedized SM Fiber Cable		3
1.0m Ruggedized MM Fiber Cable		3
Dell 100G QSFP28 Cable		1
Sonnet 10Gbps SFP+ Thunderbolt Adapter		1

Backpack		1
SKB Fly Away Case		3

2.1.3 DDS-Mv1 layout

This section is only to be used as a reference. Each kit will include layout sheets similar to the images provided below. Refer to the inventory sheet received at kit check-out and the layout sheets included with the kit when completing re-packing.

Case 1



Case 1	Qty
Dell EMC Switch S4112T	1
Server Node Chassis w/ Magnet	2
192w 16A AC/DC External Power Supply for Server	2
Gigamon G-TAP A Series TAP	1
Gigamon G-TAP A Series TAP Power Adapter	1
RJ45 SFP+ Module (Gigamon)	2
LR-Fiber SFP+ Module (Gigamon)	2
SR-Fiber SFP+ Module (Gigamon)	2
RJ45 SFP+ Module (DELL)	4
USB Mini Console Cable for Dell Switches	1
3.0 ft CAT 6e (Black)	3

Case 2

Case 2	Qty
Dell EMC Switch S4112F	1
Server Node Chassis w/ Magnet	2
192w 16A AC/DC External Power Supply for Server	2
0.5m SFP+ Direct Connect (DELL)	8
LR-Fiber SFP+ Module (Intel)	4
SR-Fiber SFP+ Module (Intel)	4
USB Mini Console Cable for Dell Switches	1
3.0 ft CAT 6e (Black)	3

Case 3

Case 3	Qty
Server Node Chassis w/ Magnet	3
192w 16A AC/DC External Power Supply for Server	3
USB Mini Console Cable for Cisco Switch	1
Cisco Switch	1
1.0m SFP+ Direct Connect (DELL)	8
LR-Fiber SFP+ Module (DELL)	4
SR-Fiber SFP+ Module (DELL)	4
3.0 ft CAT 6e (Black)	3

Backpack

Case 3	Qty
Dell Precision 7540 Laptop	1
Dell Precision 7540 Laptop Power Adapter	1
Server Node Chassis w/ Slip Case and Magnet	1
192w 16A AC/DC External Power Supply for Server	1
8 Outlet Power Strip	1
6 Outlet Power Strip	1
Ruggedized 2M SM Fiber Cable	3
Ruggedized 1M MM Fiber Cable	3
3.0m SFP+ Direct Connect (DELL)	2
1.0m QSFP Breakout Cable (DELL)	4
100GQSFP28 Passive	1
Cisco Switch Power Cable	1
Dell EMC Switch Power Cords	2
Solo10G™ SFP+ Thunderbolt™ 3 Network Adapter	1
USB Laptop Console Crash Cart Adapter	1
6.0 ft CAT 6e (Black)	3
Velcro Straps	12

2.1.4 Power Information

2.1.4.1 Power Requirements

All electronic components listed in this section are rated for operation at **100-240V** and **50-60 Hz**. When operating outside of the United States select a power strip that is rated for voltage, frequency, and plug type at that specific location.

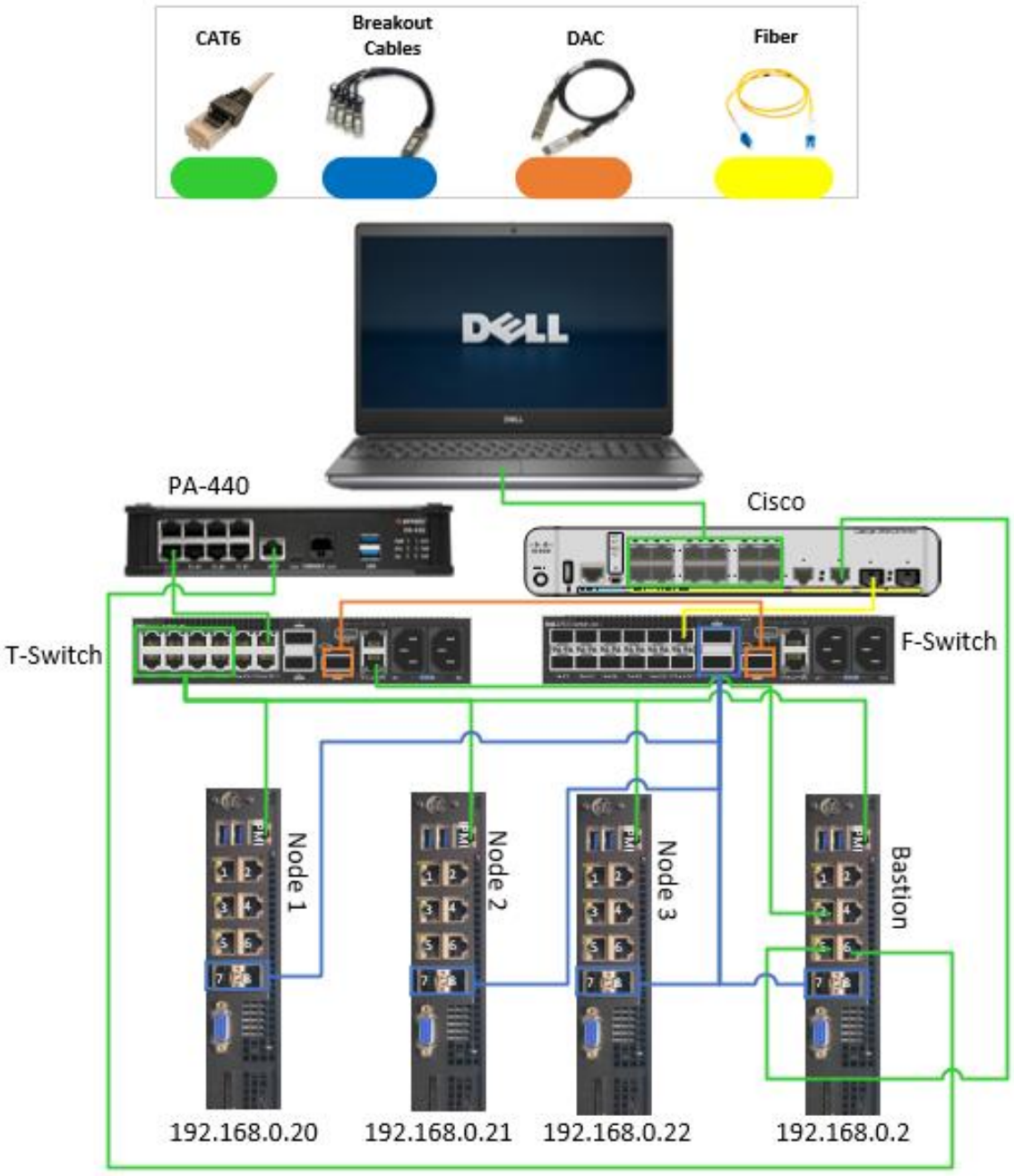
2.1.4.2 Power Consumption

Hardware without nodes

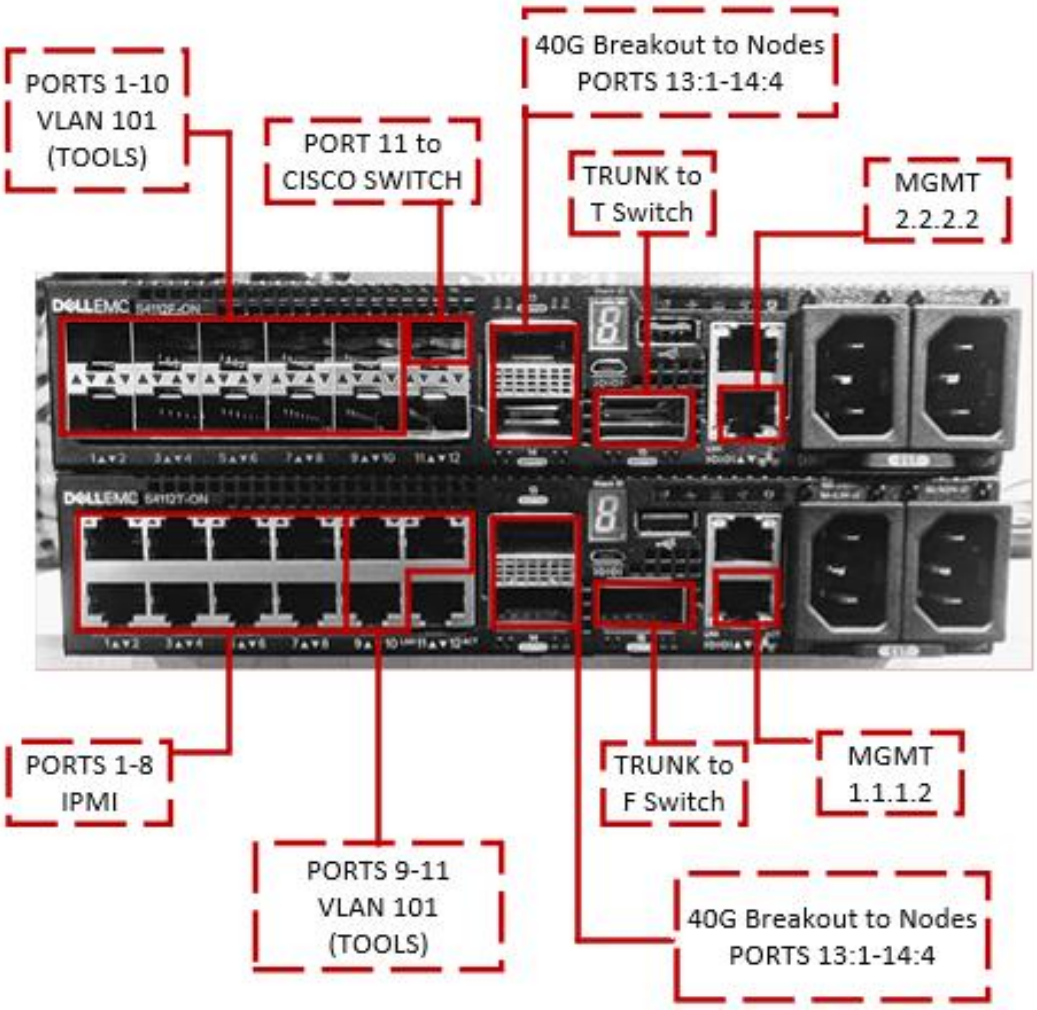
DDS-Mv1E Component	Typical Power Consumption	Maximum Power Consumption
S4112F-ON	90W	180W
S4112T-ON	120W	200W
Cisco Catalyst 3560	30W	270W (Full PoE Load)
Dell Precision 7540/7550/7560	90W	130W
Individual SN3000 Node	130W	160W
Gigamon A-TAP	15W	15W
PA-440	29W	34W

2.1.5 Cabling Instructions and Wiring Diagrams

2.1.5.1 DDS-Mv1E overview

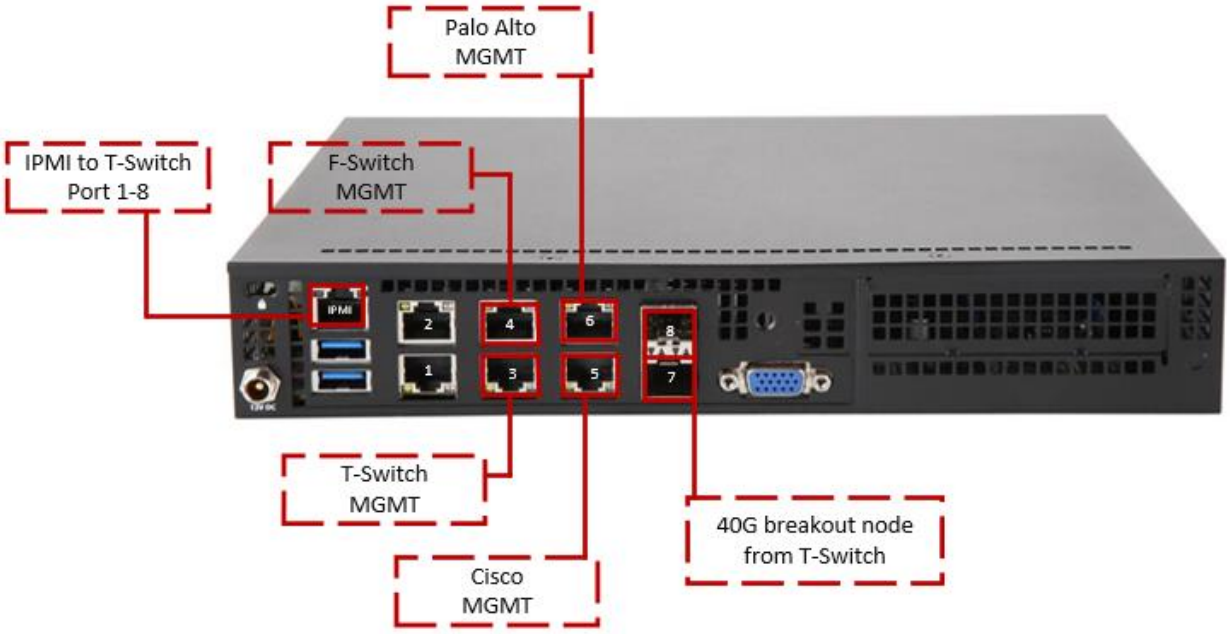


2.1.5.2 Dell S4112-ON series Switches

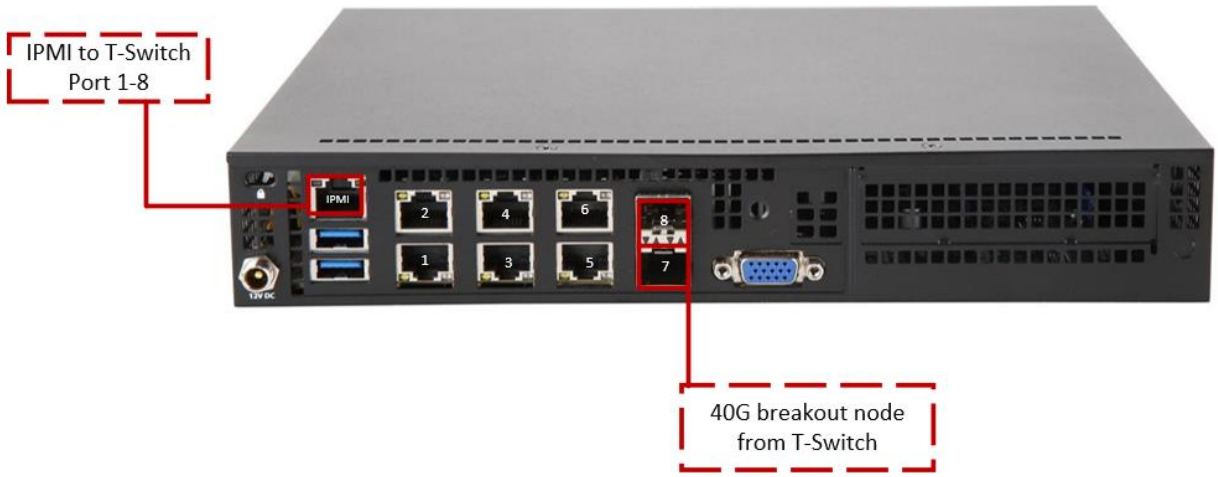


✎ **Note**: Ensure that the SFP+ module is appropriate for the type of cable you are using. For example, if using single-mode fiber (SMF), use an SFP+ SMF module.

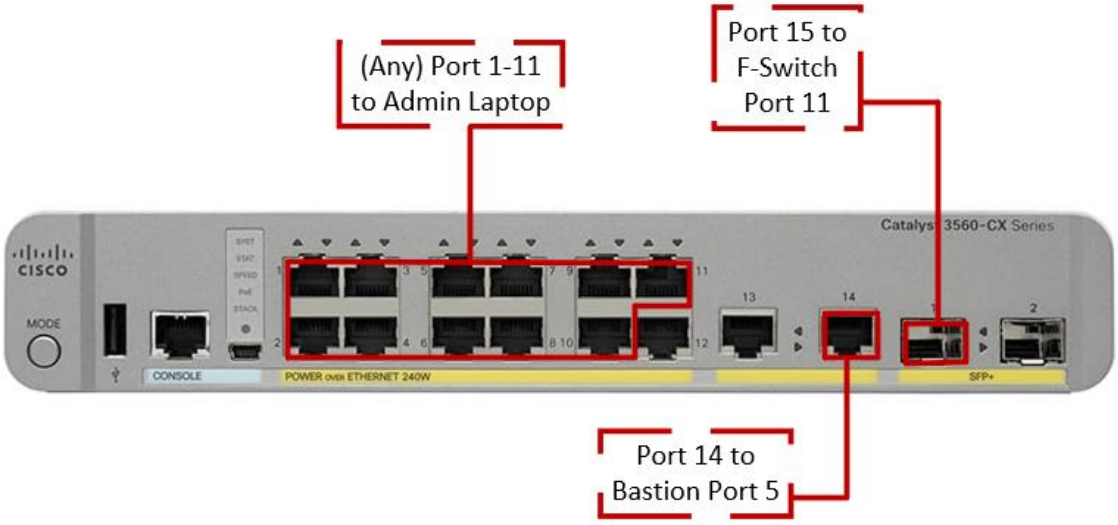
Bastion node



SN3000 node



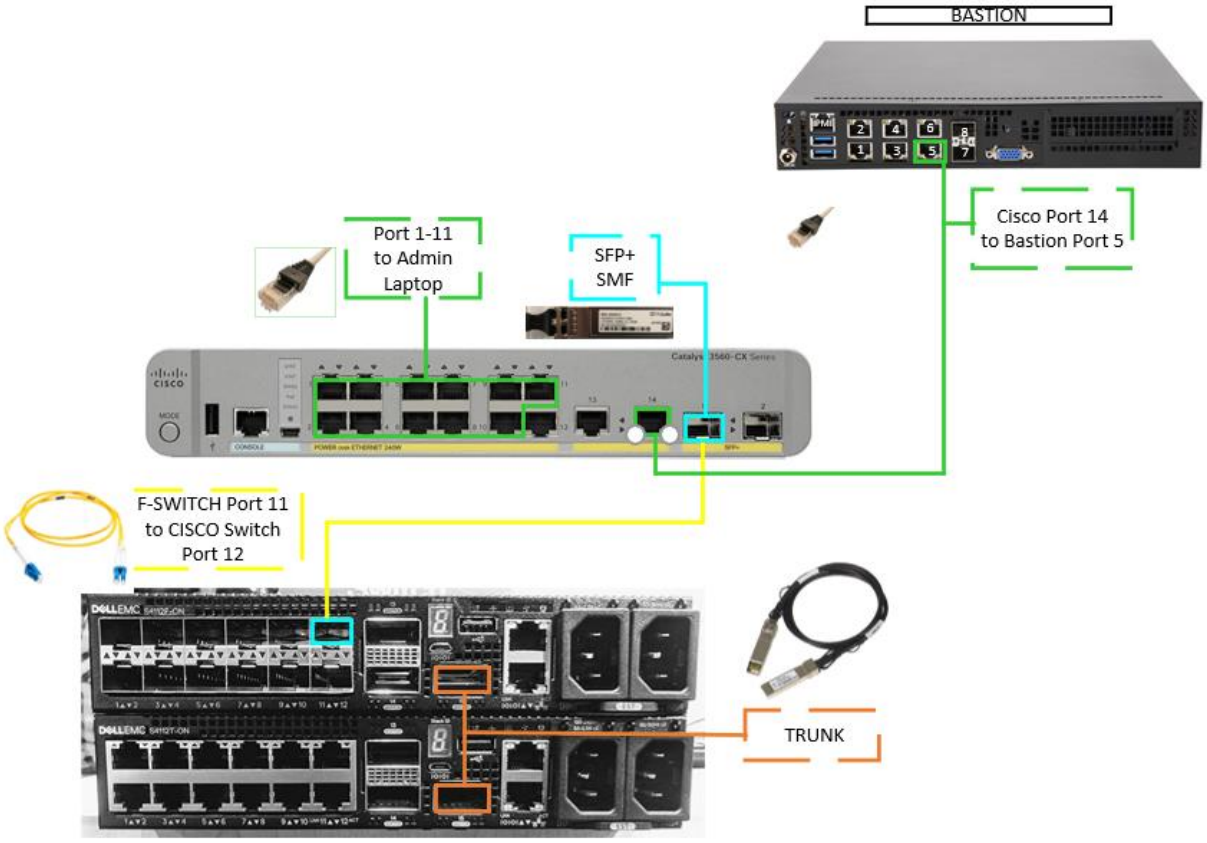
Cisco Switch



PA-440

2.1.5.3 Detailed Cabling Instructions

Dell Switches connections and Port Assignments



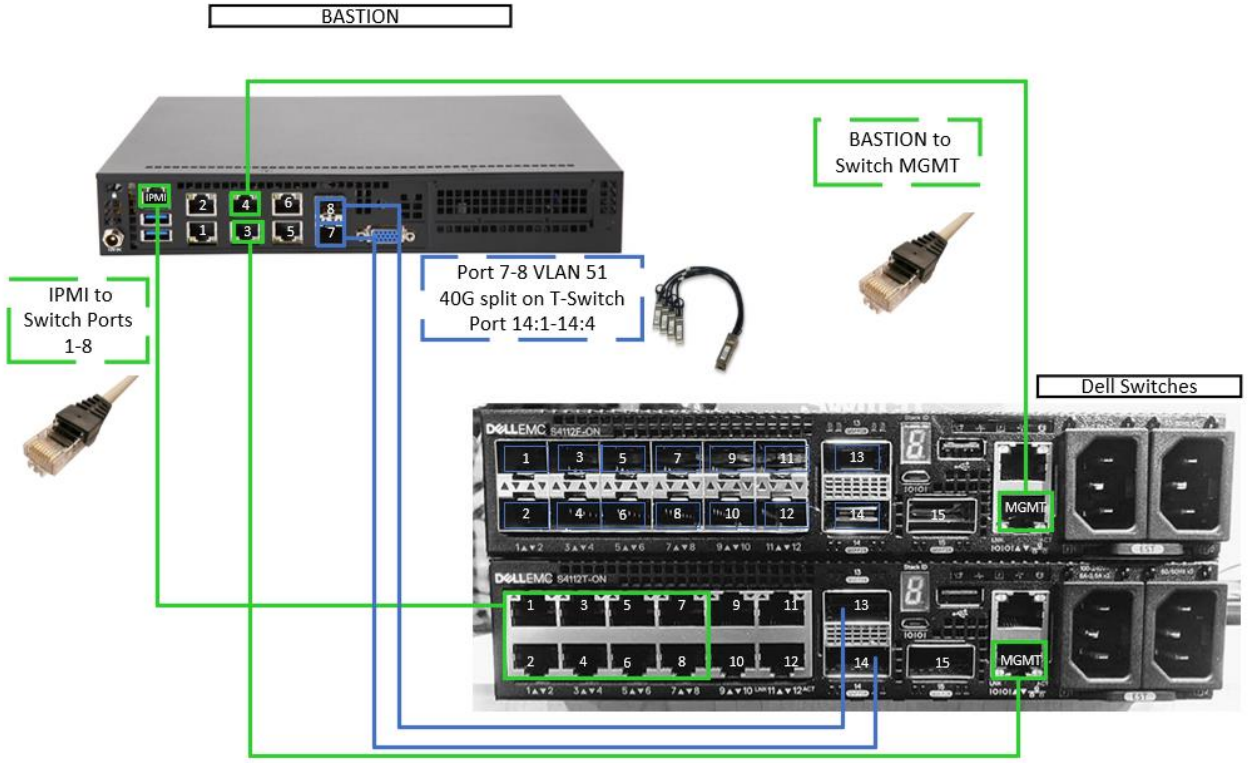
1. (TRUNK) Connect **port 15** of the **S4112T-ON switch** to **port 15** of the **S4112F-ON switch** using the 100G DAC cable.

2. (CISCO) Connect **port 11** of the **S4112F-ON switch** to **port 15** of the **Cisco switch** using the yellow Single-Mode Fiber (SMF) cable with the appropriate SFP+ module.

3. (ADMIN LAPTOP) Connect the **Admin Laptop** to the **Cisco switch** using any port between **ports 1-11**.

4. (BASTION) Connect the Bastion's **Port 5** to the Cisco's **Port 14**.

Bastion to Dell Switches connections



5. (IPMI) Connect the **IPMI Port** on the **BASTION** to a port between **Ports 1-8** on the **S4112T-ON switch** using an appropriate CAT6 cable.

6. (VLAN 51) Connect the large end of a breakout cable to **Port 13** of the **S4112T-ON switch.**

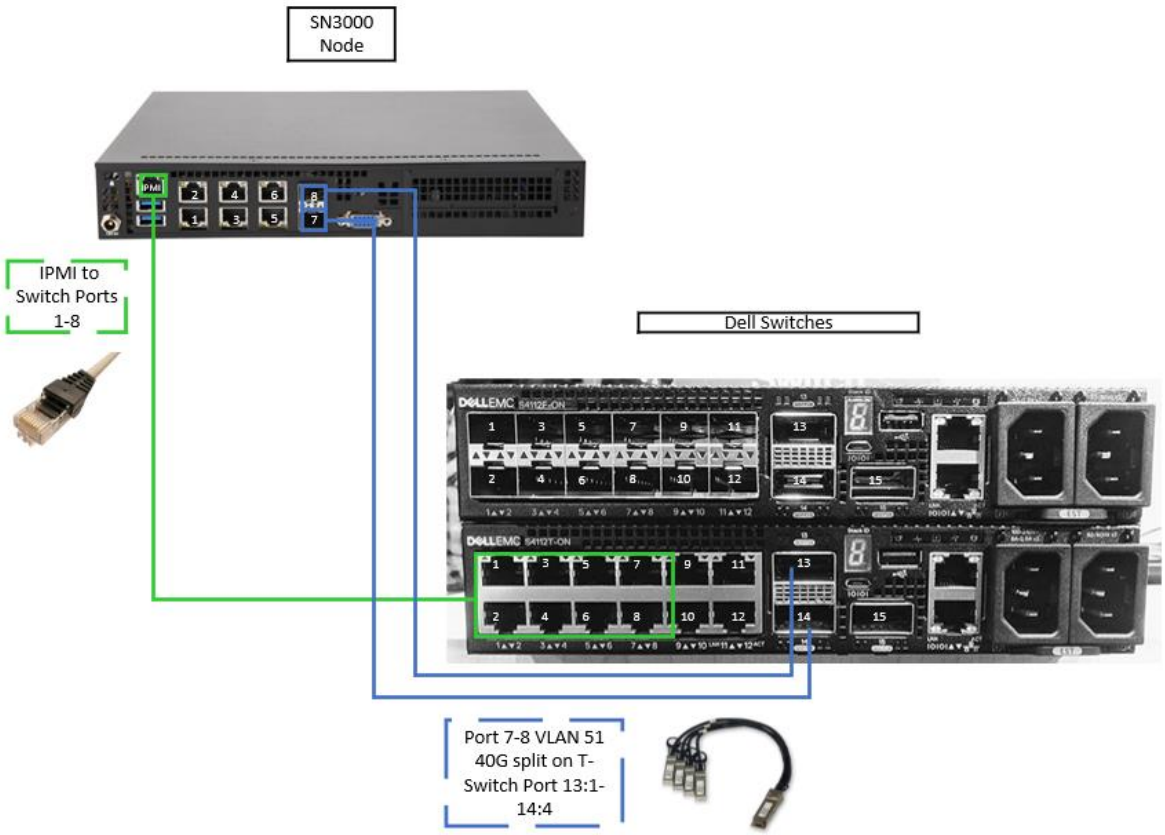
7. (VLAN 51) Connect the large end of a breakout cable to **Port 14** of the **S4112T-ON switch.**

8. (VLAN 51) Connect any one of the small ends of the breakout cable to **Port 7** of the **Bastion**.

9. (VLAN 51) Connect any one of the small ends of the breakout cable to **Port 8** of the **Bastion**.

10. (MGMT) Connect the lower **MGMT port** of the **S4112T-ON switch** to **Port 3** on the **SN3000** and the lower **MGMT port** on the **S4122F-ON switch** to **Port 4** of the **SN3000**.

Dell Switches to nodes connections



11. (IPMI) Connect the designated IPMI port on the **SN3000 node** to a port between **Ports 1-8** on the **S4112T-ON switch** by using an appropriate CAT6 cable.

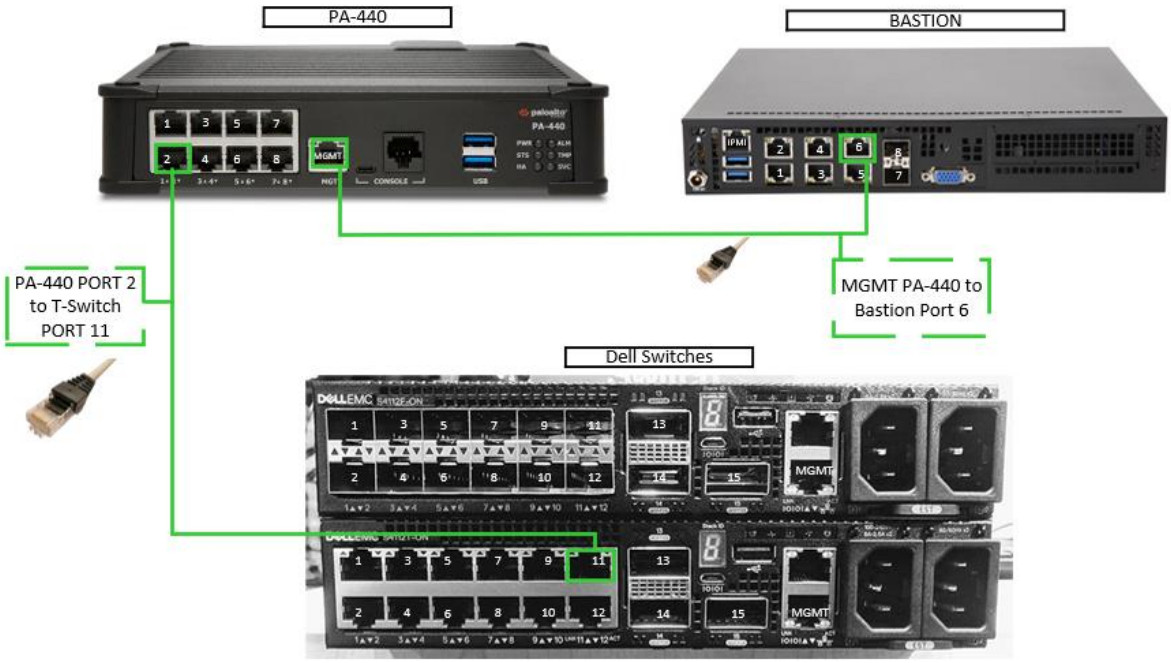
12. (VLAN 51) Using the breakout cable plugged into **Port 13** of the **S4112T-ON switch** used in step 6, connect one of the remaining modules to **Port 8** of the **SN3000 node**.

13. (VLAN 51) Using the breakout cable plugged into **Port 14** of the **S4112T-ON switch** used in step 8, connect one of the remaining modules to **Port 7** of the **SN3000 node**.

14. Repeat steps 13-14 for all standard (i.e. Not Bastion) SN3000 nodes.

Note: If there are no additional connections available via the breakout cables on the T-Switch, Ports 13 and 14 of the F-Switch may also be used.

PA-440 connections



15. (PA-440) Connect **Port 2** of the **PA-440** to **Port 11** of the **S4112T-ON switch** using an appropriate CAT6 cable.

16. (BASTION) Connect the **MGMT Port** of the **PA-440** to **Port 6** of the **Bastion**.

17. Plug in the appropriate power cables into the kit-provided power strips.

✎ **Note**: The Bastion should be powered on before the other nodes to avoid any potential issues.

After completing the cabling instructions, you should continue to the node deployment section of this document, located here.

2.2 Equipment check-out procedures

✎ Note: This step requires the presence of someone with a valid DA1687 “NOTICE OF DELEGATION OF AUTHORITY - RECEIPT FOR SUPPLIES:” from the gaining unit. This person will inventory and sign a DA3161 for all equipment, temporarily taking the items into their unit Property Book.

1. An approved Form 5 (Armory Request Form), approved by all required entities (BN S3, BDE S3, NERD, ARCYBER, ACM, etc.).

2. Transfer all equipment, software, firmware, and VM serial numbers, version numbers, and patch levels in the tracking database. This is for software asset management and ensures DCO, Armory, Forge, and CPT personnel, are clear on exactly what is in the assigned kit.

3. The CPT member and designated Armory personnel will test DDS-M to ensure proper functionality per section 9 of the Armory SOP.

4. Inventory the kit(s) with the CPT Personnel that are arriving to retrieve the kit.

5. Once kit inventory is 100%, sign the kit over to CPT Personnel using appropriate document i.e., DA 3161, DA 2062, and/or DDSM Kit component list.

3. Admin Manual

3.1 VMWare vSphere Management

3.1.1 Node power procedures

While the nodes are fairly resilient and *should* not have issues if suddenly powered off, it is always good practice to gracefully shut everything down and bring everything up. Standard procedures for powering the nodes on and off are listed below.

✎ **Note:** Powering on the nodes and switches in the following steps takes around 5 minutes. Be patient and allow them to power on before moving on to any next steps.

3.1.1.1 Power on procedures

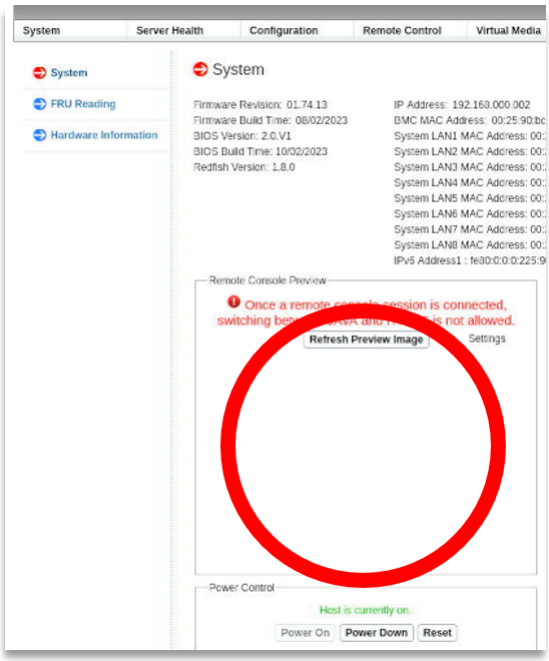
1. Power up the switches.

2. Power on the Admin Laptop

3. Turn on the Bastion-designated node by pressing the power button on the device.

    a. Open the IPMI web GUI for the Bastion on the Admin Laptop by typing in the IPMI address into the web browser. This should be https://192.168.0.2.

    b. Open the console window in the IPMI web GUI.



c. Type in the LUKS passphrase for the Bastion when prompted.

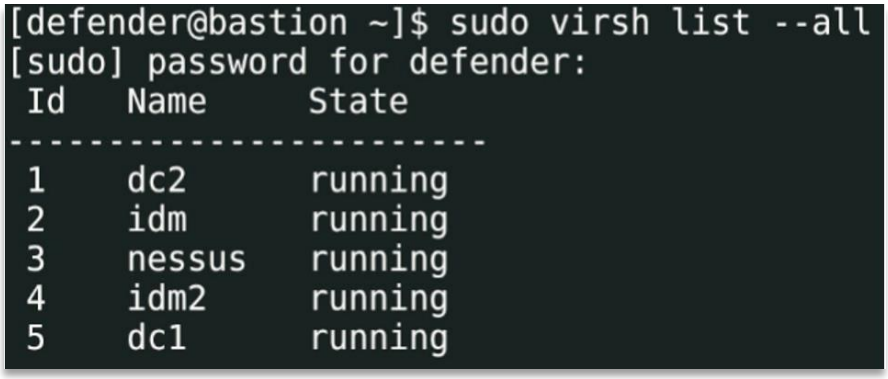
d. Ping the Bastion from the Admin Laptop until you receive a response from the Bastion to ensure that the Bastion is fully up and running.

4. SSH into the Bastion from a terminal on the Admin Laptop.
   ✎ Note: Open a terminal from the Admin Laptop, not from the web GUI used in step 3.

```
$ ssh bastion
```

5. From the SSH terminal, ensure that the virtual machines on the Bastion are running.

```
$ sudo virsh list --all
```



6. Power on the ESXi host nodes.

7. Ping the first node's IPMI until you have a connection.

```
$ ping 10.<kit#>.51.20
```

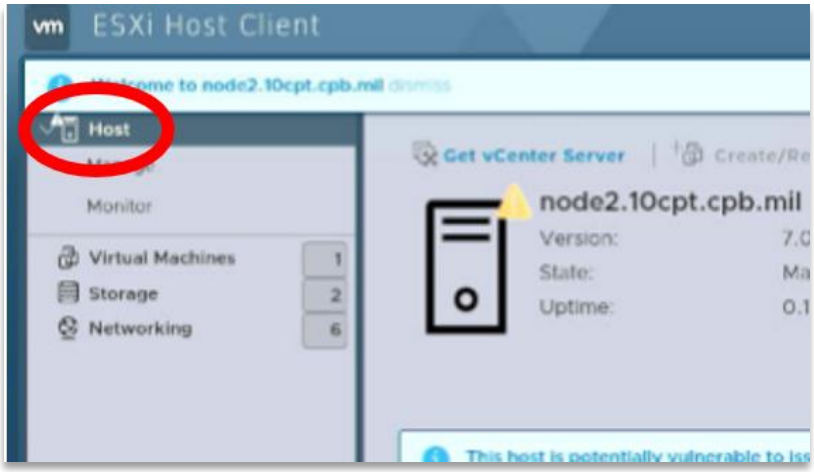
8. Navigate to the ESXi web page for each host.

   a. https://node#.<kit#>cpt.cpb.mil

9. Log in to the web page

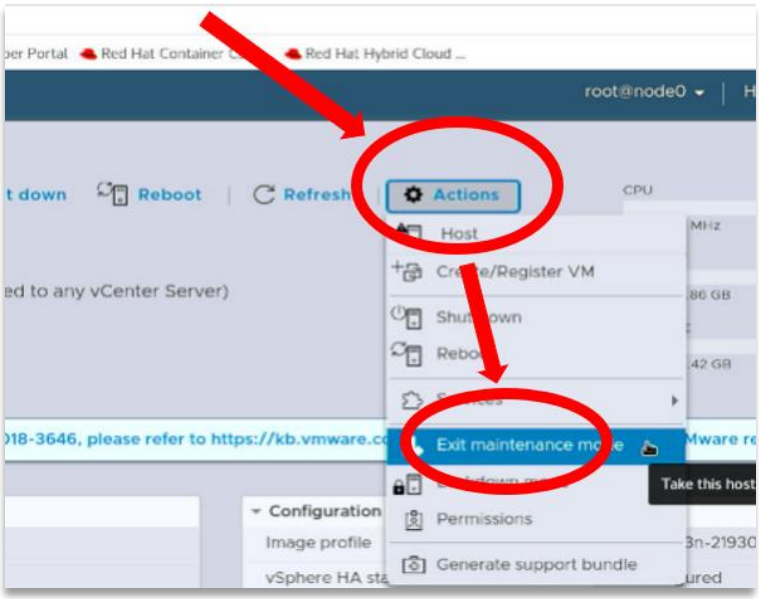
10. Take each host out of maintenance mode.

    a. From the Navigator pane, select **Host**.



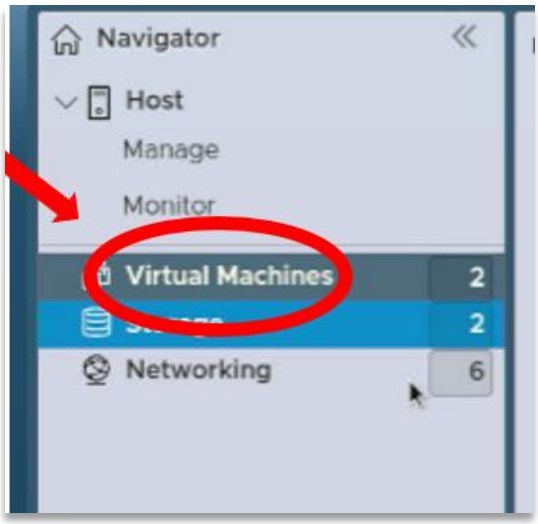
    b. Click on the **Actions** dropdown from the toolbar.

    c. Select **Exit Maintenance Mode**.



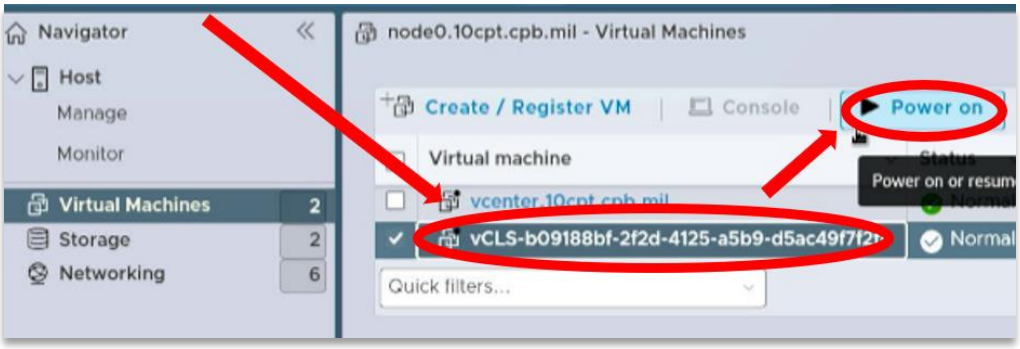
11. Power on the vSphere cluster services on each host.

    a. From the **Navigator** pane, select **Virtual Machines**.



    b. Click on the **vCLS - ####** virtual machine.

    c. Click the **Power On** button of the toolbar.

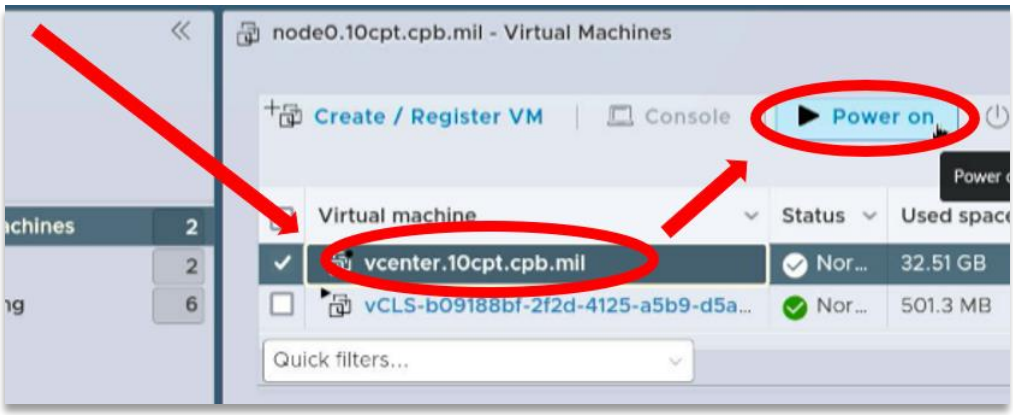


12. Power on the vCenter Server on ONE of the hosts.

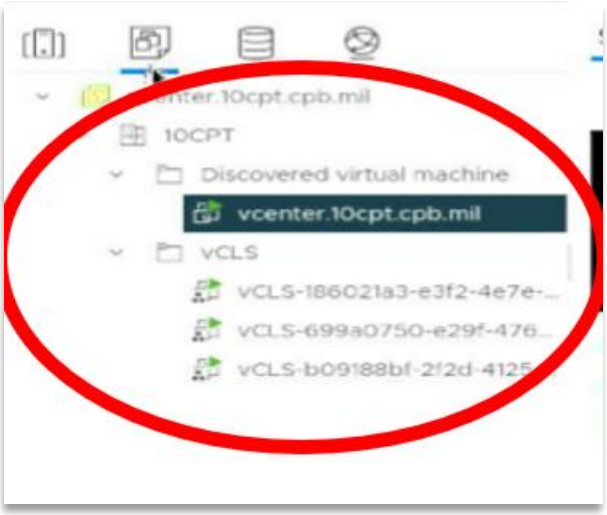
    a. From the **Navigator** pane, select **Virtual Machines**.

    b. Click on the **vCenter-Server** virtual machine.

    c. Click the **Power On** `button of the toolbar.



13. Navigate to the vCenter web GUI (https://vcenter.<kit#>cpt.cpb.mil) to turn on any other required virtual machines.



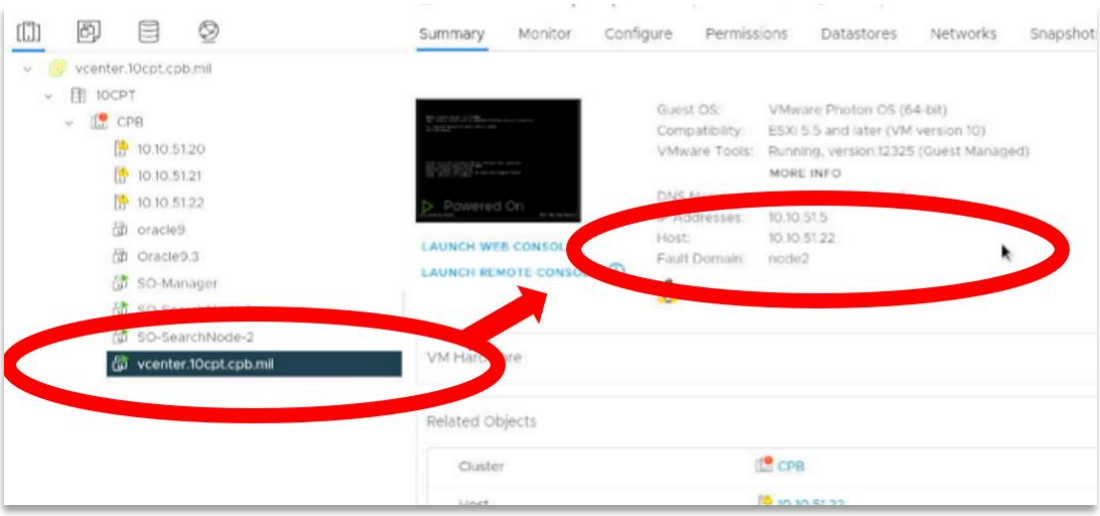
3.1.1.2 Power off procedures

1. Navigate to the vCenter Web GUI (https://vcenter.<kit#>cpt.cpb.mil) and log in.

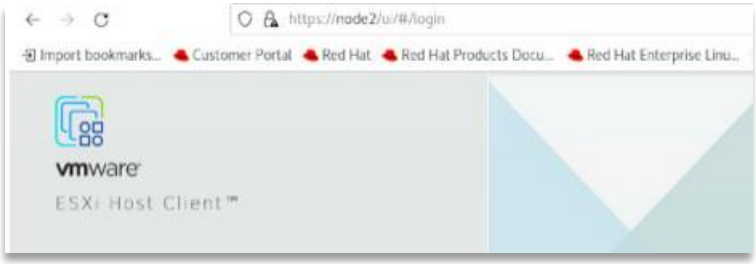
2. Navigate to the virtual machines or Hosts tab to turn off any remaining virtual machines.

✎ **Note:** Do NOT power off vCenter or any vCLS

3. Take note of which host vCenter is on. (Do not power it off at this time).



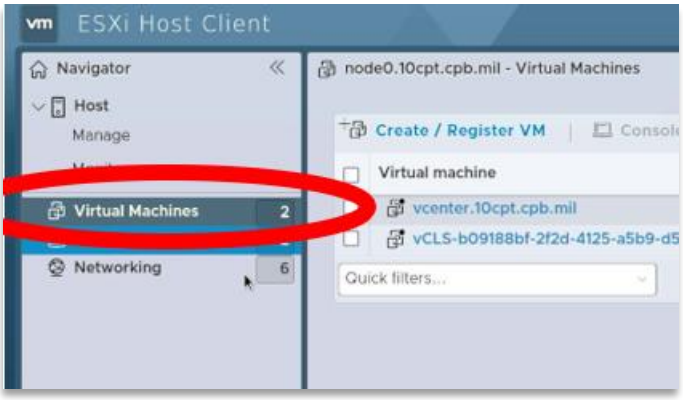
4. Navigate to the ESXI Web Page for each host with the username ‘root’ and the password from the vault. **(https://node#.<kit#>cpt.cpb.mil) or 10.<kit#>.51.20 - 10.<kit#>.51.23**.



5. Log in to the web page.

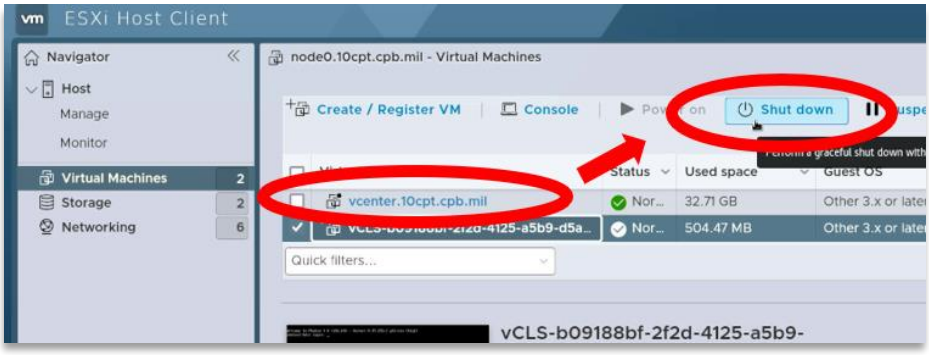
6. Power off the vCenter Server on ONE of the hosts by doing the following:

   a. On the **Navigator Pane** select **Virtual Machines**.



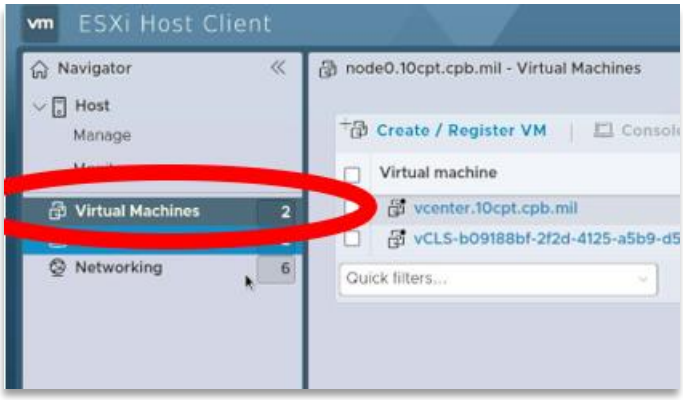
   b. Click on the **vCenter-Server** virtual machine.

   c. Click the **Power Off** button on the tool bar.



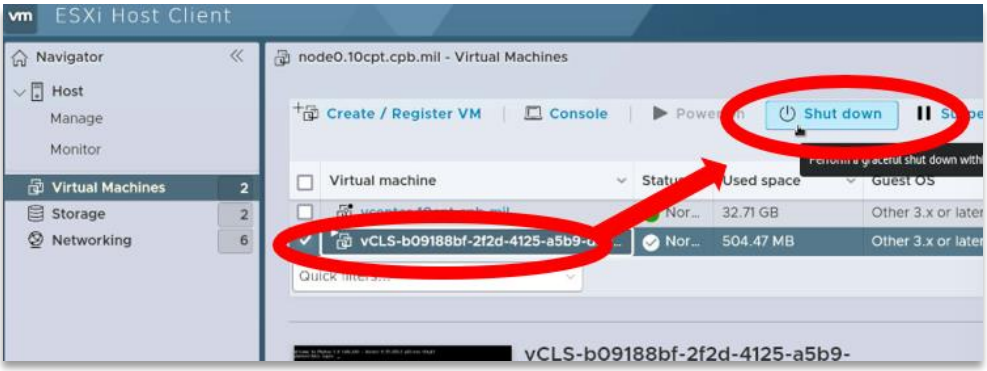
7. Power off the vSphere Cluster Services on each host.

    a. On the **Navigator Pane** select **Virtual Machines**.



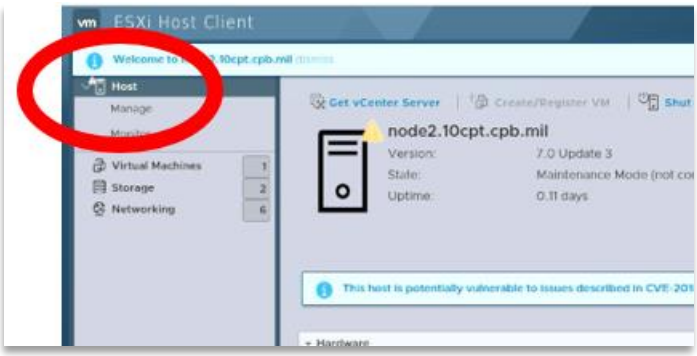
    b. Click on the **vCLS - ####** virtual machine.

    c. Click the **Power Off** button on the tool bar.



8. Put each host into maintenance mode.

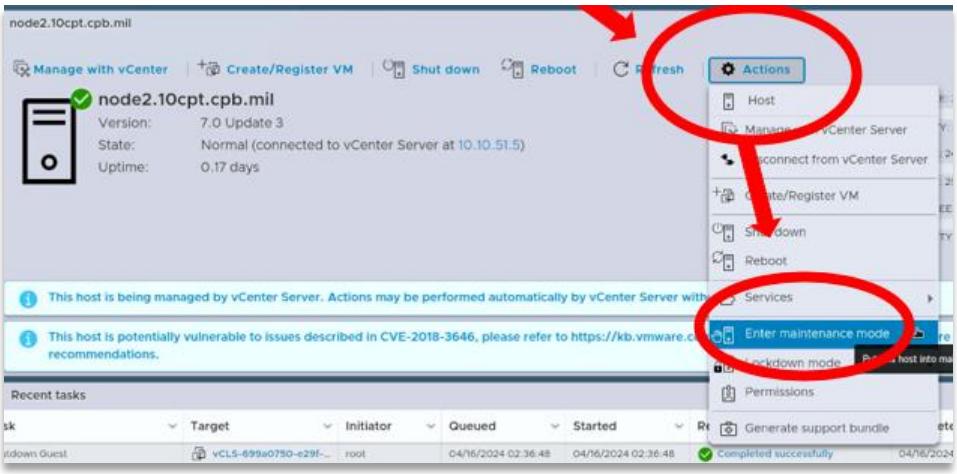
    a. On the **Navigator Pane** select **Host**.



b. Click on the **Actions** dropdown on the tool bar.

c. Select **Enter Maintenance Mode** and confirm the change in the pop up.

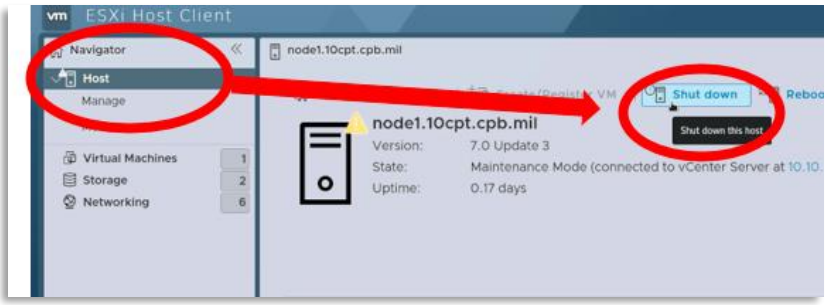
✎ **Note:** In the pop-up menu, leave “vSAN Data Migration” set to “No Data Migration.”



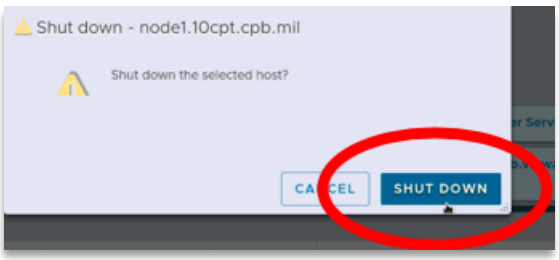
9. Power off the ESXi Hosts.

a. On the **Navigator** pane, select **Host**.

b. In the toolbar, click **Shutdown**.



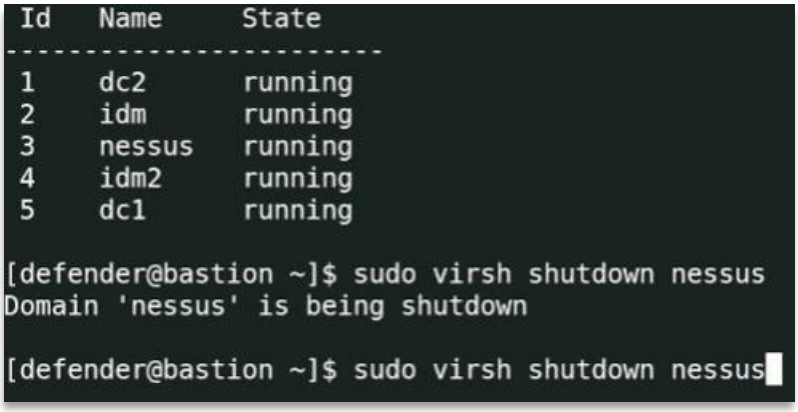
c. In the pop-up, click **Shutdown**.



10. Connect to the Bastion from the Admin laptop through SSH

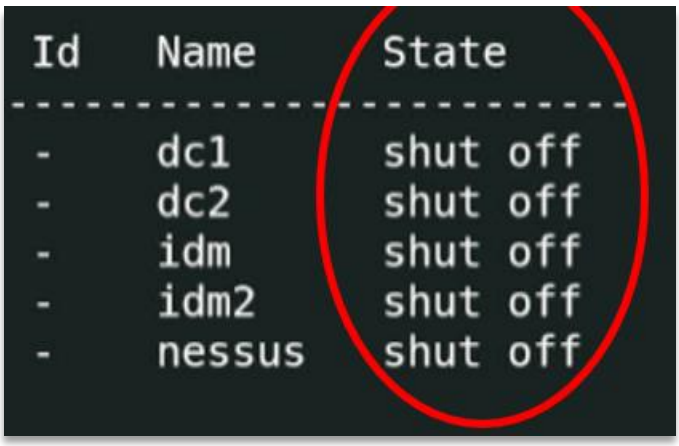
```
$ ssh defender@bastion
```

11. Make sure the virtual machines on the Bastion are “POWERED OFF”




```
$ sudo virsh list –all
$ sudo virsh shutdown <VM name>
$ sudo virsh list --all
```

✎ **Note:** Ensure that all VMs on the list say shutdown



12. Power off the Bastion (Node8)

From the SSH session, type:

```
$ poweroff
```

✎ **Note:** Alternatively, you should be able to press the power button on the

13. Power off the Admin Laptop

14. Power off the switches by removing the power cable

15. If packing up the kit, ensure you pack everything in the appropriate container using the provided inventory cards in each case and backpack.

3.1.2 User management

User and password management is critical for maintaining kit operations and access to all infrastructure, services, and tools. Passwords for all infrastructure and services deployed by EOD automation are available in the vault, which can be found in **/opt/ddsm-esxi**. Once in the correct folder launch the vault by typing **./launcher**. Some additional user management tasks not included with the launcher are detailed below.

3.1.2.1 Default Usernames

Bastion: defender

Laptop: cpsadmin

IPMI: ADMIN

ESXi: root

vCenter: administrator@vsphere.local

Palo Alto: EOD_PA_ADMIN

Dell switches: EOD_DELL_ADMIN

Cisco switches: EOD_CISCO_ADMIN

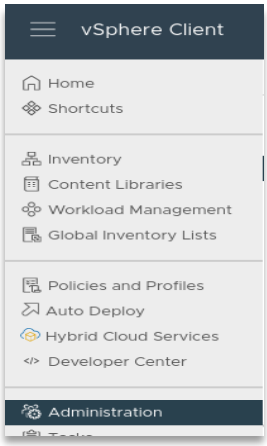
3.1.2.2 CAC authentication setup

The following steps are pre-requisites to enabling CAC authentication and adding CAC-enabled users on the kit.

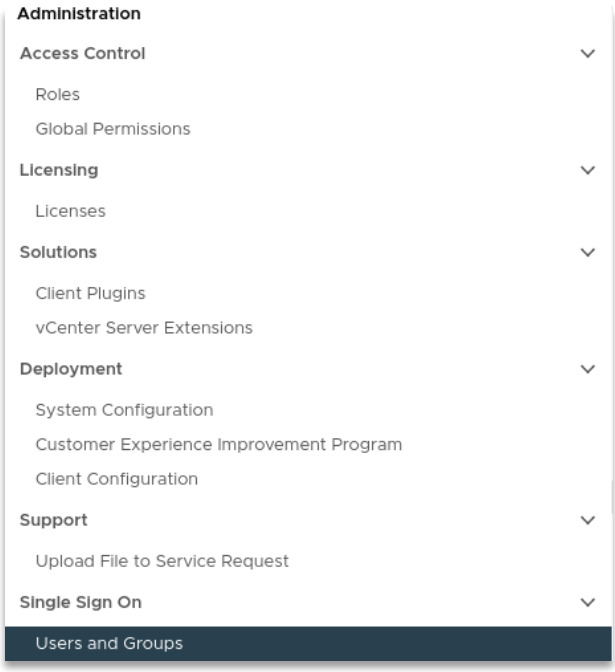
✎ **Note:** Do not select TPM (Trusted Platform Module). The kit does not have TPM.

1. Log in to vcenter, by going to https://vcenter.<kit#>cpt.cpb.mil with the username “administrator@vsphere.local and the password stored in the vault.

2. Navigate to **administration** from the hamburger menu in the top left.



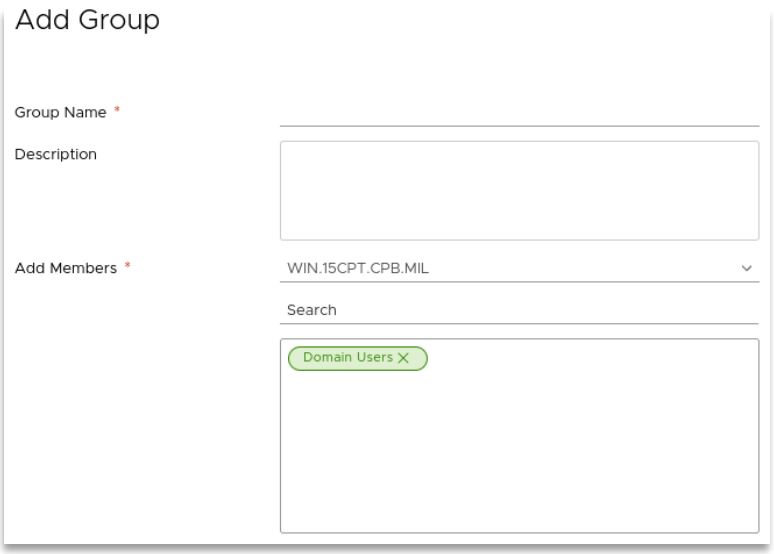
3. Navigate to **users/groups** > **Groups**



4. Click **Add**.

5. Set the Add Members drop down to WIN.<kit#>CPT.CPB.MIL.

6. Search for Domain Users and click **Add**.



3.1.2.3 Add new user

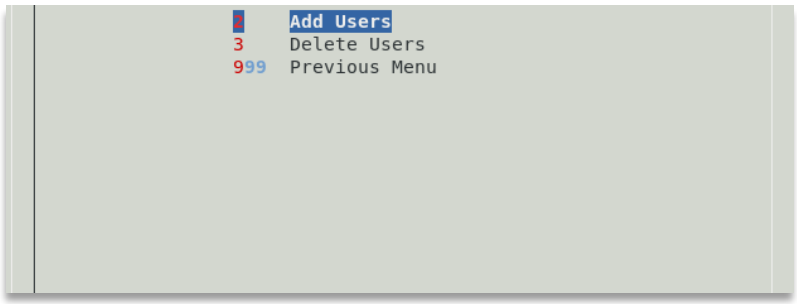
Adding a new CAC-enabled user is most easily done through the launcher GUI on the Admin Laptop.

1. On the Admin Laptop, navigate to **/opt/ddsm-esxi**.

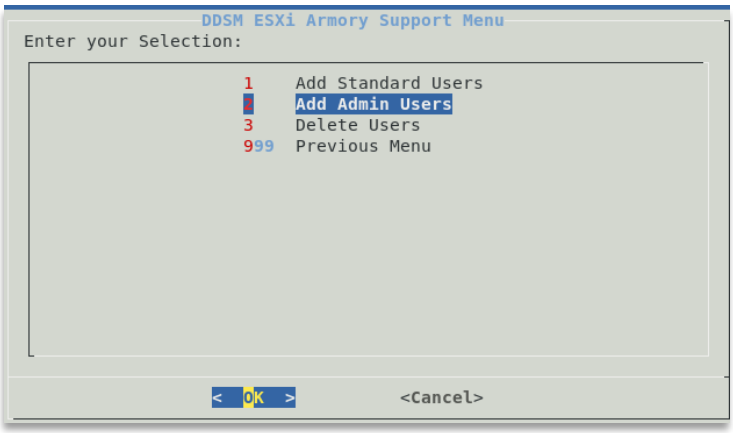
2. Start **./launcher**.

3. Enter the vault password.

4. Select the **Add Users** option.

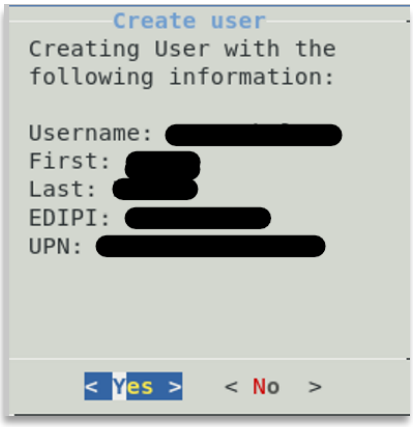


5. You will see several options for types of users that can be added. Select the appropriate user type for your needs.



6. You will be prompted to insert the CAC of the user you would like to add.

7. When asked if you would like to create the user, ensure that the information is correct and select **Yes**.



3.1.2.4 Change Administrator Account password

1. From the direct console, select **Configure Password**.
2. Type the current password in the Old Password line and press Enter.
3. In the New Password line, type a new password and press Enter.
4. Retype the new password and press Enter.

3.1.2.5 Reset ESXi root password with Host Profile

1. Login to the vCenter WebClient.
2. Go to **Home** and then choose **Host Profiles** from Operations and Policies Section.
3. Choose **Extract profile from a host**.
4. In the Extract Host Profile menu wizard, select the host you want to update the password for.
5. Name the Host Profile and click **Next** and then **Finish** to complete the capture of the host profile template. The new host profile should appear on the Host Profile Objects Field.
6. Right Click the new Host Profile or using the Actions menu and choose **Edit Settings**.

7. In the 'Edit Host Profile' Wizard. Uncheck all boxes.

8. Then using the search filter search for root.

9. Highlight and then select the check box for **root**.

10. A configurable window will display the root User configuration.

11. At the Password subsection, choose **Fixed password configuration**.

12. Here you will fill in the new password and confirm it before proceeding.

13. Double check that all other non-applicable boxes have no check marks and proceed to Finish.

14. Once the Task Completes highlight the new host profile and from the **Actions** drop down menu and choose **Attach Detach Hosts and Clusters** then Select the host in the wizard.

15. From the Action Menu select **Check Host Compliance**.

16. From the Action Menu select **Remediate**.

17. Then Check **Host Compliance**.

18. Remove the Host Profile from the Host. At this time the host password should be successfully upgraded.

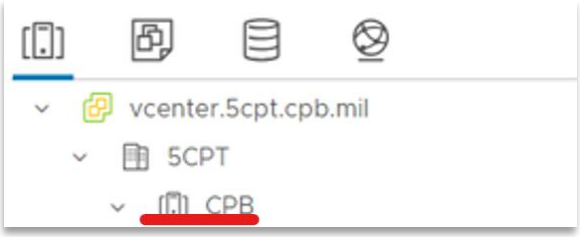
3.1.3 Creating a vSAN cluster

VMware vSAN uses a software-defined approach that creates shared storage for virtual machines. It virtualizes the local physical storage resources of ESXi hosts and turns them into pools of storage that can be divided and assigned to virtual machines and applications according to their quality-of-service requirements. vSAN is implemented directly in the ESXi hypervisor. vSAN aggregates all local capacity devices into a single datastore shared by all hosts in the vSAN cluster.

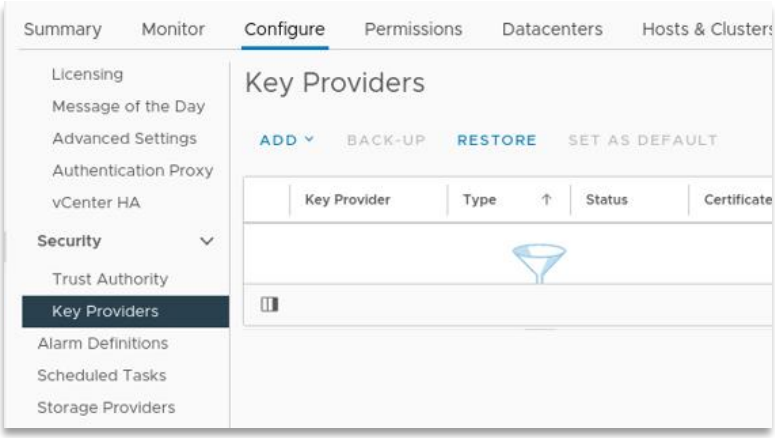
1. Type https://vcenter.<kit#>cpt.cpb.mil in the web browser and **Launch Vsphere client**.

2. Login with the username 'administrator@vsphere.local' and the password from the vault.

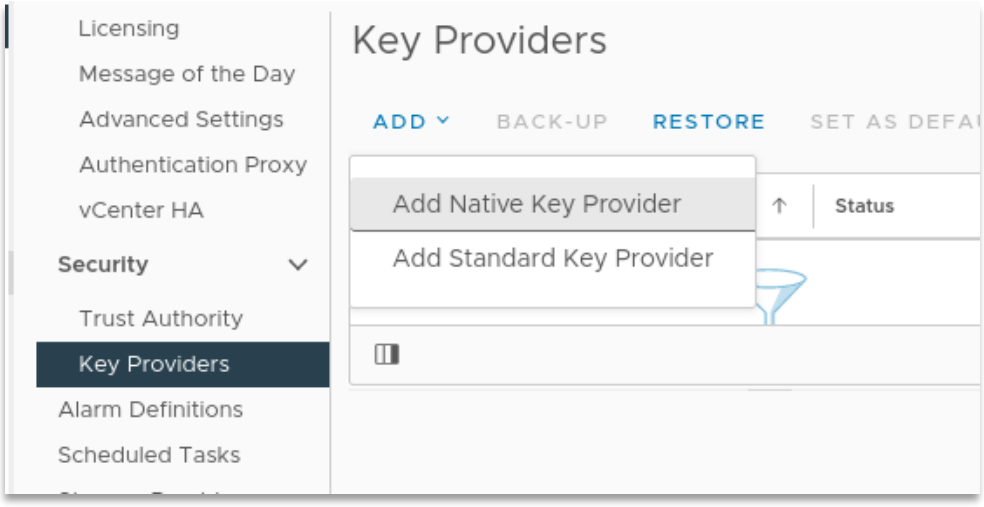
3. Navigate to the cluster.



4. Select Configure > **Key Providers**.

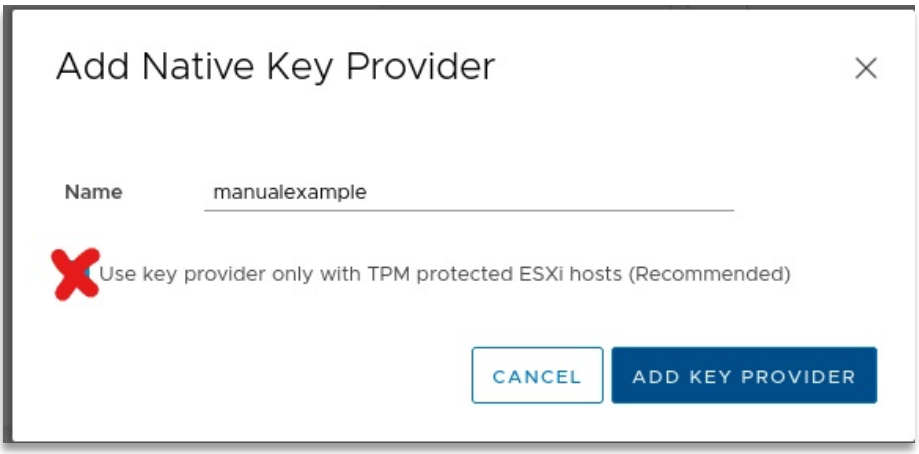


5. Select **ADD +** > **Add Native Key Provider**.

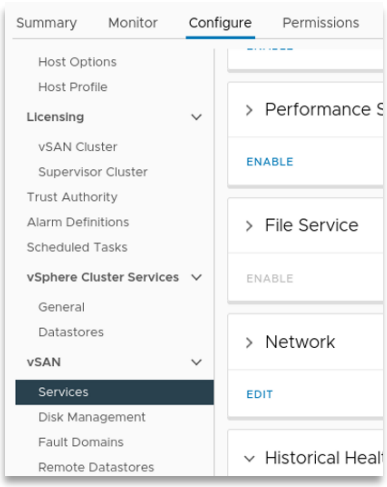


6. Give a name to the provider and ensure that “Use key provider only with TPM protected ESXi hosts” is NOT checked.

7. Click **Add Key Provider**.



8. Navigate to **cluster** > **configure** > **vsan** > **Services** > **Data Services > Edit**.



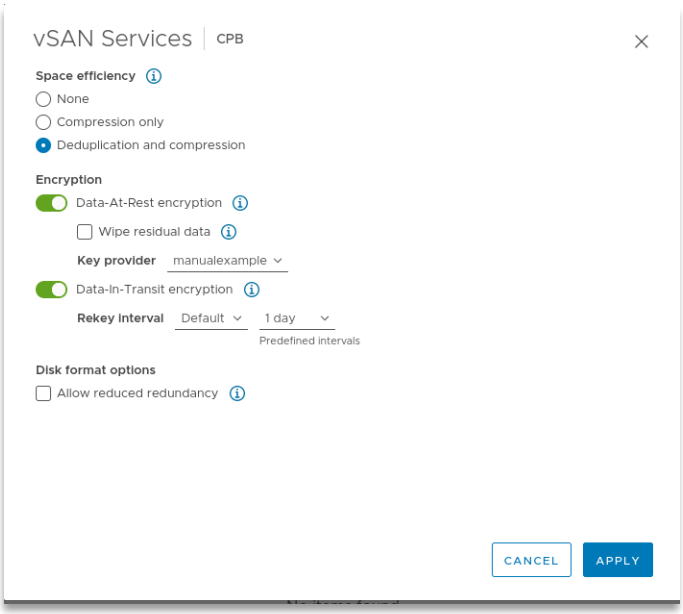
9. Select **Deduplication and compression**.

10. Turn on **Data-At-Rest encryption**.

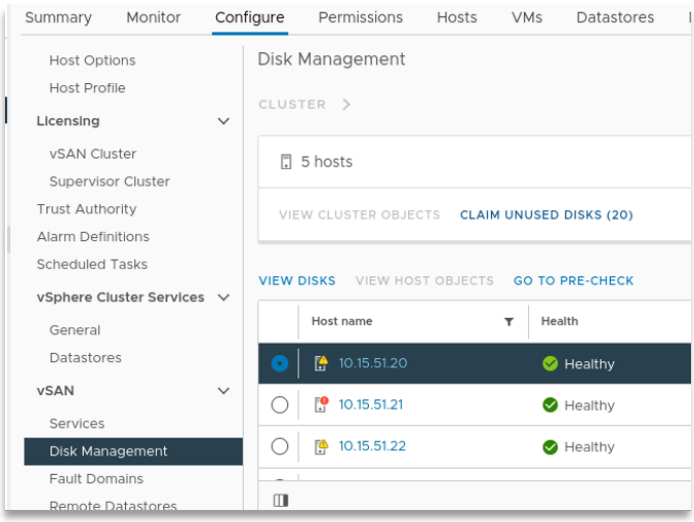
✎ **Note:** Ensure that the Key provider is the one that we created and named in the previous steps.

11. Turn on **Data-in-Transit encryption**.

12. Click **Apply**.

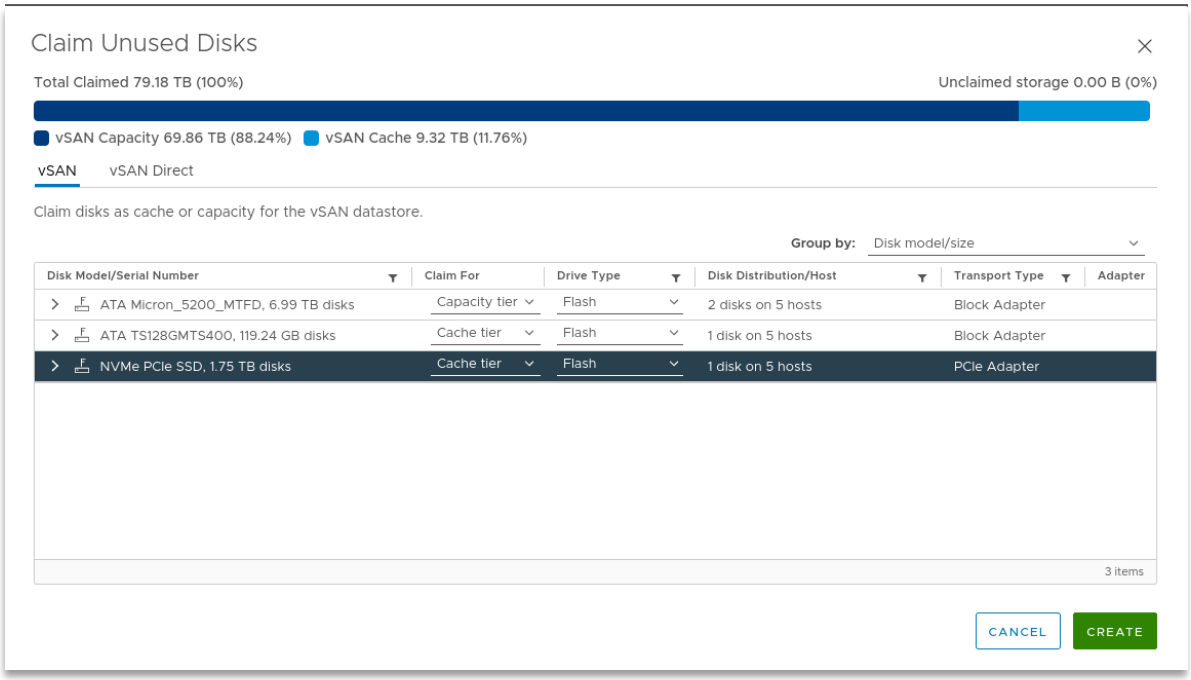


13. Navigate to **cluster** > **configure** > **vsan** > **Disk Management**.



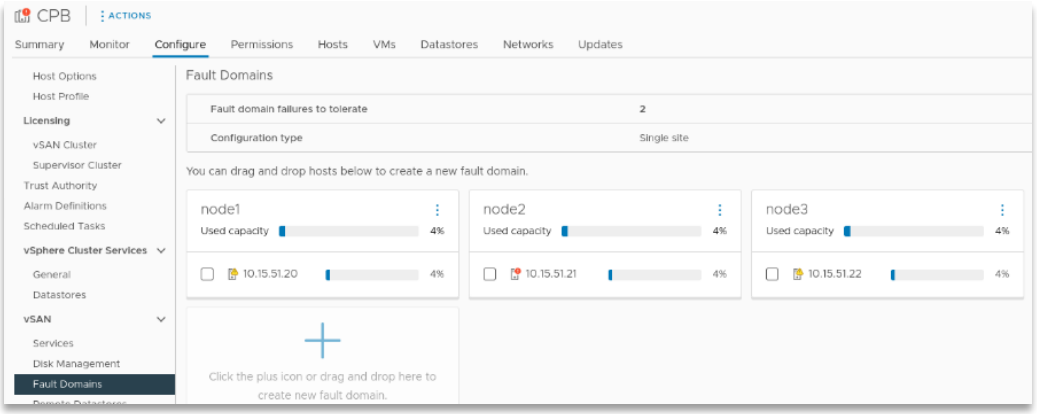
14. Click **Claim Unused Disks**.

15. Ensure that the “Claim For” drop down is set to Capacity tier for the Larger Micron disk and set to Cache tier for the other smaller disks. (See picture below)



16. Navigate to **cluster** > **configure** > **vsan** > **fault domains**.

17. Create one fault domain per host (name disks and drag to plus sign).

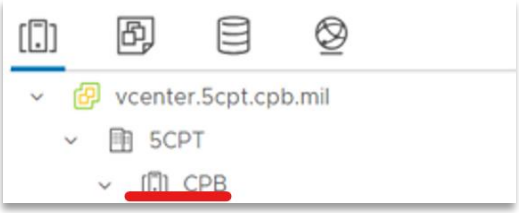


3.1.4 Enable Cluster DRS & HA

A cluster is a group of hosts. When a host is added to a cluster, the host's resources become part of the cluster's resources. The cluster manages the resources of all hosts within it. Clusters enable the vSphere High Availability (HA) and vSphere Distributed Resource Scheduler (DRS) solutions.

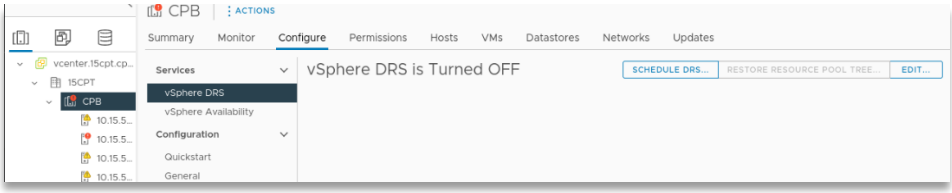
✎ **Note:** Users should be careful if the cluster is under load. This will cause VMs to migrate and create more load.

1. Navigate to the cluster (CPB).

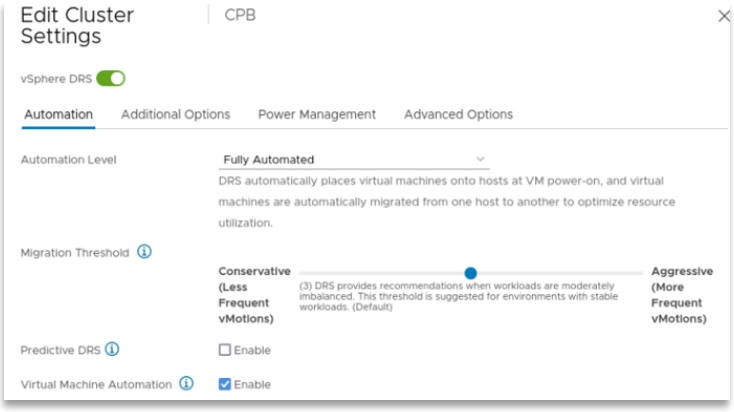


2. Go to **Configure** > **Services** > **vSphere DRS**.

3. Select **Edit…**

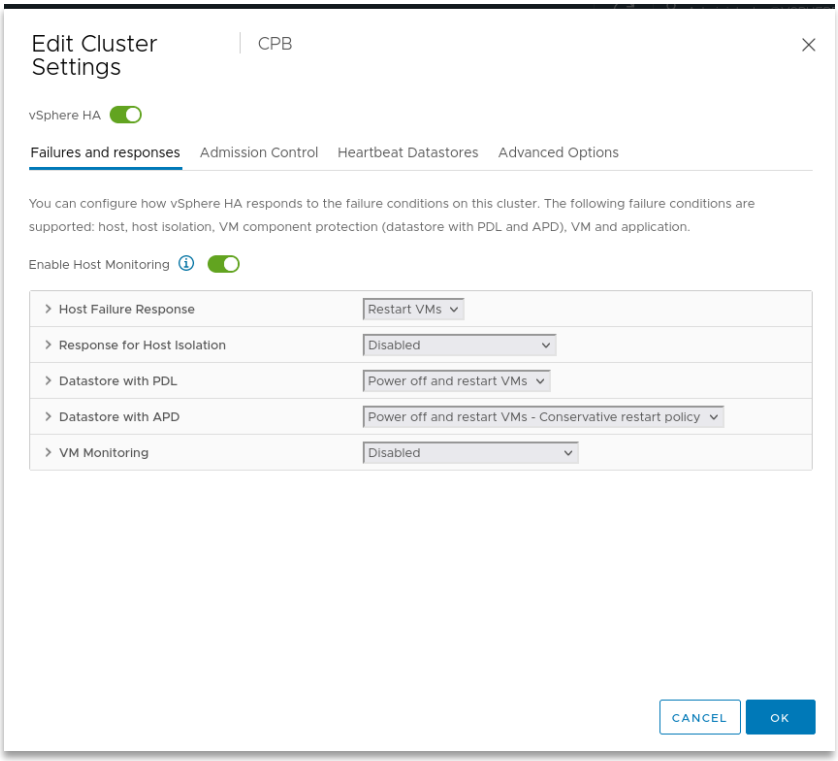


4. Toggle on **vSphere DRS** and click **OK.**



5. Return to **Configure** > **Services** and select **vSphere Availability**.

6. Toggle on v**Sphere HA** and click **OK**.



3.1.4.1 Identity Management Server

IdM is running as a virtual machine on the Bastion. IdM provides DNS, Secondary NTP, future capabilities for Remote Authentication Dial-In User Service (RADIUS), and Account Management.

You can reach IdM by going to:

https://idm.<kit#>.51.10

OR

https://idm.<kit#>.51.11

3.1.4.2 Windows Domain Controller

The windows domain controller is running as a virtual machine on the bastion. It has been replicated into dc1.win and dc2.win. It primarily provides CAC authentication for VMware.

The dc1.win and dc2.win currently only support command line interaction.

3.1.5 Network management

3.1.5.1 view ip address information

1. To view current network configuration, for all interfaces, use the following command:

```
[user@host ~]$ ip addr
```

2. To find information regarding a specific interface, add the interface name after the command, example:

```
[user@host ~]$ ip addr show dev br-ex
```

3.1.5.2 Configuring Network Interfaces

In RHEL, network address configuration is stored within the following directory:

```
/etc/sysconfig/network-scripts/
```

Each interface should have its own **ifcfg-<interface>** file that stores all relevant configuration persistent across reboots. After editing this file, restart the network for the changes to take effect. Below is an example file for an interface named **eth0** with a static IP address of **10.1.51.50**:

```
DEVICE=eth0
BOOTPROTO=static
ONBOOT=yes
IPADDR=10.1.51.50
NETMASK=255.255.255.0
GATEWAY=10.1.51.1
DNS1=10.1.51.10
```

✎ **Note**: the **ONBOOT=yes** option must be included if the interface should be activated after a reboot or network restart. If set to '**no**', the interface will not automatically display!

3.1.6 Partitions and Filesystems

3.1.6.1 ESXI

With ESXi 7.0, partitions are consolidated into fewer, larger partitions that are expandable, depending on the used boot media and its capacity.

The ESXi 7.0 system storage layout consists of four partitions:

Partition	Use	Type
System Boot	Stores boot loader and EFI modules	FAT16
Boot-bank 0	System space to store ESXi boot modules	FAT16
Boot-bank 1	System space to store ESXi boot modules	FAT16
ESX-OSData	Acts as the unified location to store additional modules. Not used for booting and virtual machines. Consolidates the legacy /scratch partition, locker partition for VMware Tools, and core dump destinations Caution: Always create ESX-OSData partitions on persistent storage devices that are not shared between ESXi hosts. Use USB, SD, and non-USB flash media devices only boot bank partitions.	VMFS-L

Partition sizes, except for the system boot partition, can vary depending on the size of the boot media used. If the boot media is a high-endurance one with capacity larger than 142 GB, a VMFS datastore is created automatically to store virtual machine data.

You can review the boot media capacity and the automatic sizing as configured by the ESXi installer by using the vSphere Client and navigating to the Partition Details view. Alternatively, you can use ESXCLI, for example the "`esxcli storage filesystem list`" command.

The ESX-OSData volume is divided into two high-level categories of data, persistent and non-persistent data. Persistent data contains of data written infrequently, for example, VMware Tools ISOs, configurations, and core dumps.

Non-persistent data consists of frequently written data, for example, logs, VMFS global traces, vSAN Entry Persistence Daemon (EPD) data, vSAN traces, and real-time databases.

System Storage Volume	Symbolic Link
Boot-bank 0	/bootbank
Boot-bank 1	/altbootbank
Persistent data	/product locker /locker /var/core /usr/lib/vmware/isoimages /usr/lib/vmware/floppies
Non-persistent data	/var/run /var/log /var/vmware /var/tmp /scratch

3.1.6.2 Red Hat Enterprise Linux

Partitions, hard drives, and file systems are essential to managing storage and keeping data separated logically and physically. The Solid State Drives (SSDs) installed inside of DDT nodes vary in form-factor, speed, and storage capacity. Each drive must be used for a specific purpose. Drives can be separated into partitions for filesystems and other bulk storage

1. In RHEL, drive and file system information can be viewed with the parted command **parted –l**:

```
[user@host ~]$ sudo parted -l
```

```
Model: NVMe Device (nvme)
Disk /dev/nvme0n1: 2048GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start   End     Size    File system  Name                  Flags
 1      1049kB  1075MB  1074MB  fat32        EFI System Partition  boot
 2      1075MB  2149MB  1074MB  xfs
 3      2149MB  2048GB  2046GB                                     lvm
```

2. Beyond the basic drive information, the partition name, volume name, mount location, and capacity can be viewed with the **lsblk** command.

```
[user@host ~]$ lsblk
```

```
NAME                  MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sda                     8:0    1 119.3G  0 disk
nvme0n1               259:0    0   1.9T  0 disk
├─nvme0n1p1           259:1    0     1G  0 part /boot/efi
├─nvme0n1p2           259:2    0     1G  0 part /boot
└─nvme0n1p3           259:3    0   1.9T  0 part
  ├─rootvg01-lv_root  253:0    0 377.4G  0 lvm  /
  ├─rootvg01-lv_swap  253:1    0  15.6G  0 lvm  [SWAP]
  ├─rootvg01-lv_audit 253:2    0     1G  0 lvm  /var/log/audit
  ├─rootvg01-lv_tmp   253:3    0  94.4G  0 lvm  /tmp
  ├─rootvg01-lv_var   253:4    0   1.4T  0 lvm  /var
  └─rootvg01-lv_log   253:5    0     2G  0 lvm  /var/log
```

3. The **lsblk** command shows what drives, partitions, or volumes are mounted or unmounted. In the example output above, the **sda** drive is not mounted, but could be mounted to a directory. To mount an unmounted drive or partition, use the mount command while supplying a drive location and directory to mount to. Drive/partition locations default to **/dev/<device>**.

```
[user@host ~]$ sudo mkdir /mnt/device
[user@host ~]$ sudo mount /dev/sda /mnt/device
   mount: /dev/sda is write-protected, mounting read-only
[user@host ~]$ lsblk
```

4. To **unmount** a drive, partition, or volume that is no longer needed, use the **umount** command with the mount location as an argument.

```
[user@host ~]$ sudo umount /mnt/device
```

✎ **Note**: Drives currently in use by any system process cannot be unmounted. This can occur if the path and location is open in another terminal or held by another process. If the drive is in use, the following error is shown: **umount: <mount_directory>: target is busy**.

3.1.7 Kerberos Tickets

Kerberos is a computer-network authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. It provides mutual authentication—both the user and the server verify each other's identity.

The DDS-M utilizes Kerberos tickets for navigation around the kit. In practice, this means that while logging in as yourself with a smartcard, you will be able to SSH to the bastion or IdM or wherever else you may need to go with your Kerberos ticket instead of keys.

3.1.8 SSH

The Secure Shell (SSH) protocol is essential to securing, installing, and managing the DDS-M cluster. It allows access to text-based terminals on remote hosts by creating encrypted sessions. When connected via SSH, commands entered into the terminal are encrypted, sent, and then executed on the remote host.

When connecting to a host via SSH, authentication is handled with either passwords or SSH keys. Passwords are used in conjunction with usernames to give the operator a one-time session. However, this method carries the risk of brute-force attack attempts and the potential for password sniffing. SSH keys provide additional security by introducing the concept of a set of matching cryptographic key pairs - one public, one private.

Public keys can be distributed freely while private keys should never be shared. They are copied to remote servers and stored within the home directory of a user (generally within ~/.ssh/authorized_keys) to keep track of which system(s) are authorized to connect. During connection, clients will send their public key to the host and the host will generate a randomized string, encrypting it with the public key. This string can only be decrypted by the associated private key, which should reside on the client system. The encrypted string is sent back to the client for decryption to test if the client has the associated private key. Finally, the client will decrypt the message with the private key (if available) and send back a response. If the response matches, an encrypted SSH session is created. Please see below on how to create, share, and manage SSH keys.

The SSH public keys reside at the following location:

/etc/ssh/ssh_host_rsa_key.pub

The SSH private keys reside at the following location:

/etc/ssh/ssh_host_rsa_key

3.1.8.1 create new pair

1. To being, create a new key pair value on the client using the following command.

```
[user@host ~]# ssh-keygen
```

This command will ask for a location for the private key (**/etc/ssh/ssh_host_rsa_key**) and passphrase to create the keys. The passphrase will need to be entered for every use of the private key. Please store it in a secure location.

This command generates the private key (**/etc/ssh/ssh_host_rsa_key**) and public key (**/etc/ssh/ssh_host_rsa_key.pub**).

3.1.8.2 sharing public keys with remote hosts

If you decide that you want to use authorized keys to log in to a host with SSH, you can upload authorized keys with a vifs command.

✎ **Note:** Because authorized keys allow SSH access without requiring user authentication, consider carefully whether you want to use SSH keys in your environment.

Authorized keys allow you to authenticate remote access to a host. When users or scripts try to access a host with SSH, the key provides authentication without a password. With authorized keys, you can automate authentication, which is useful when you write scripts to perform routine tasks.

You can upload the following types of SSH keys to a host:

- Authorized keys file for the root user
  /host/ssh_root_authorized_keys
- RSA key
  /host/ssh_host_rsa_key
- RSA public key
  /host/ssh_host_rsa_key_pub

1. At the command line or an administration server, use the ‘vifs’ command to upload the SSH key to an appropriate location on the ESXi host.

```
# vifs --server hostname --username username --put filename <key type>
```

✎ **Note:** The <key type> should be filled in with the appropriate location shown above. For example, to upload an RSA public key, replace <key type> with ‘/host/ssh_rsa_key_pub’.

3.1.8.3 managing the passphrase of a private key

If for any reason the paraphrase of a private key should be changed or removed, enter the following command:

```
[user@host ~]$ sudo ssh-keygen -p
```

This command will ask for the location of the private key, the old passphrase, and the new passphrase (leave empty for no passphrase).

3.1.8.4 Accessing resources from SSH

From the admin laptop or the Bastion, you can SSH into various locations using the following commands:

The passwords for each are located in the vault.

T-Switch:

```
$ ssh-EOD_DELL_ADMIN@10.<kit#>.102.1
```

F-Switch:

```
$ ssh-EOD_DELL_ADMIN@10.<kit#>.102.252
```

Cisco Switch:

```
$ ssh-EOD_CISCO_ADMIN@10.<kit#>.102.253
```

Bastion:

```
$ ssh-defender@bastion
         OR
$ ssh defender@10.<kit#>.51.2
```

3.1.9 Palo Alto Firewall

Palo Alto Firewalls are stateful firewalls used to filter network traffic based on an implicit deny structure through zone-based filtering. Palo Alto Firewalls also feature Site to Site VPN over IPSec and static routing. Palo Alto Firewalls are needed in DDT to deny unauthorized traffic from reaching the kit network. It is also used to provide Site to Site access to the kit network for operators and provide static routes to them. This allows for remote connections to be made over IPSec.

The Palo Alto web interface provides operators a well-organized view of tasks that can be performed such as creating policy rules, managing interfaces, monitoring traffic, setting up VPNs and routes. The web interface is available at **`https://10.{kit#}.101.254`** with the following default credentials:

Username: EOD_PA_ADMIN

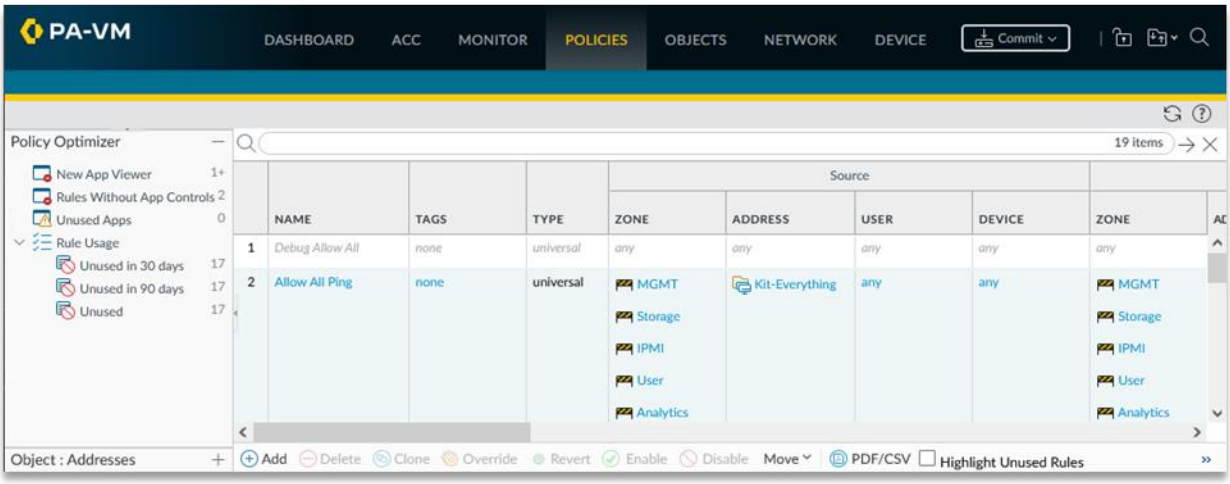
Password: [password from vault]

The following picture shows the primary navigation pane for changing various settings on the firewall.

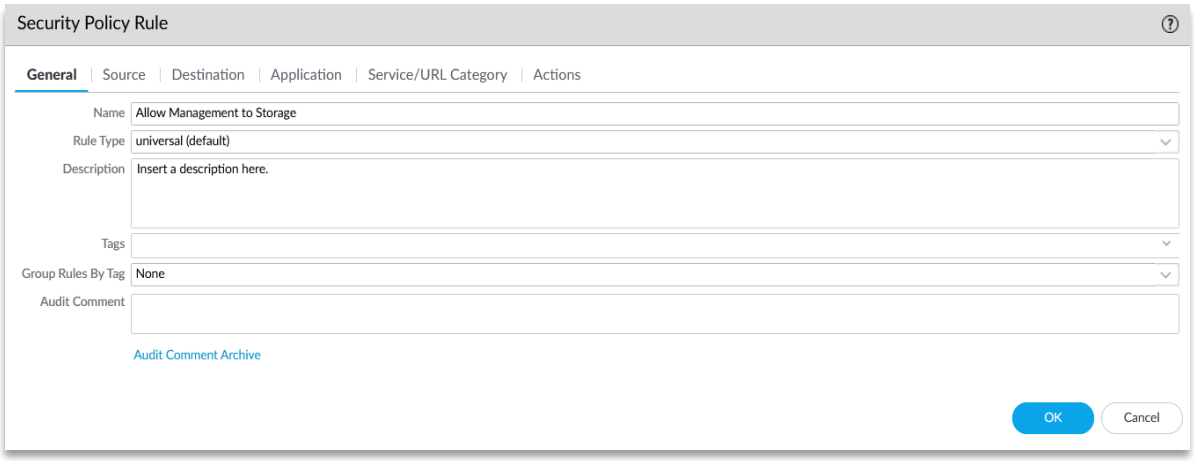
3.1.9.1 Creating Security Policy Rules

1. Select the **Policies** tab at the top of the webpage.

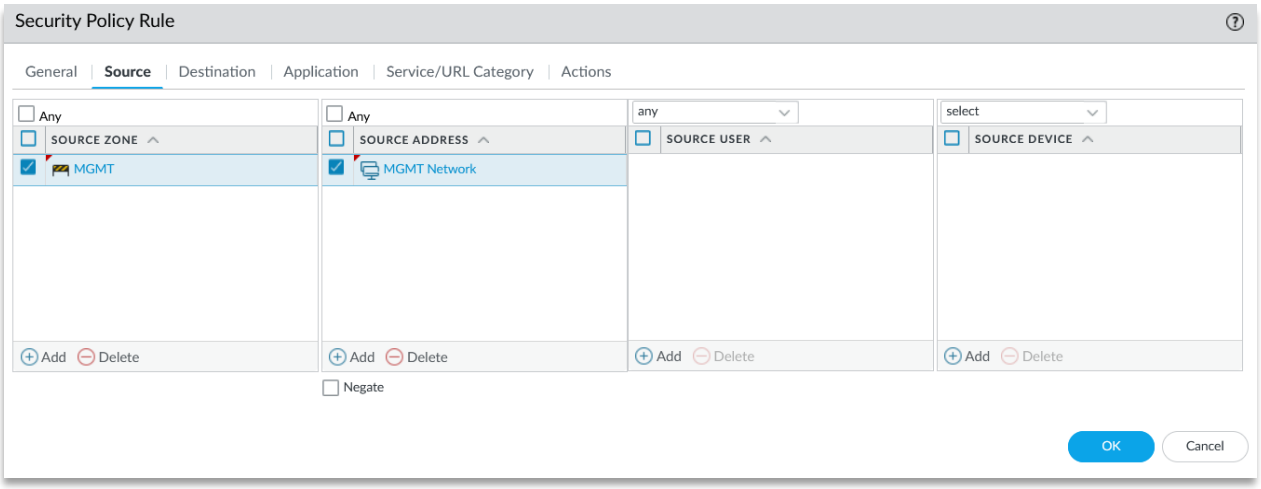
2. From within, click **Add** (at the bottom of the window with the + symbol) to create a new policy.



3. Fill in the following required settings within the General tab (the rest are optional):
   - **Name:** Select an appropriate description.
   - **Rule Type:** Universal, intrazone or interzone. Interzone is traffic between zones, intrazone is traffic within a zone and universal is both interzone and intrazone traffic.

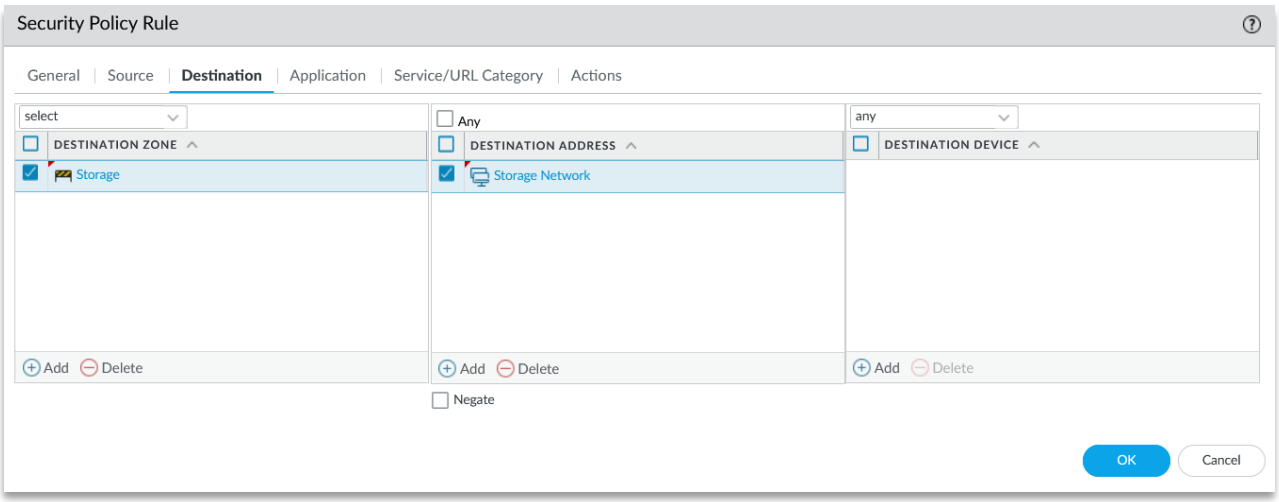


4. Switch to the **Source** tab. Add the desired source zone and source address range.

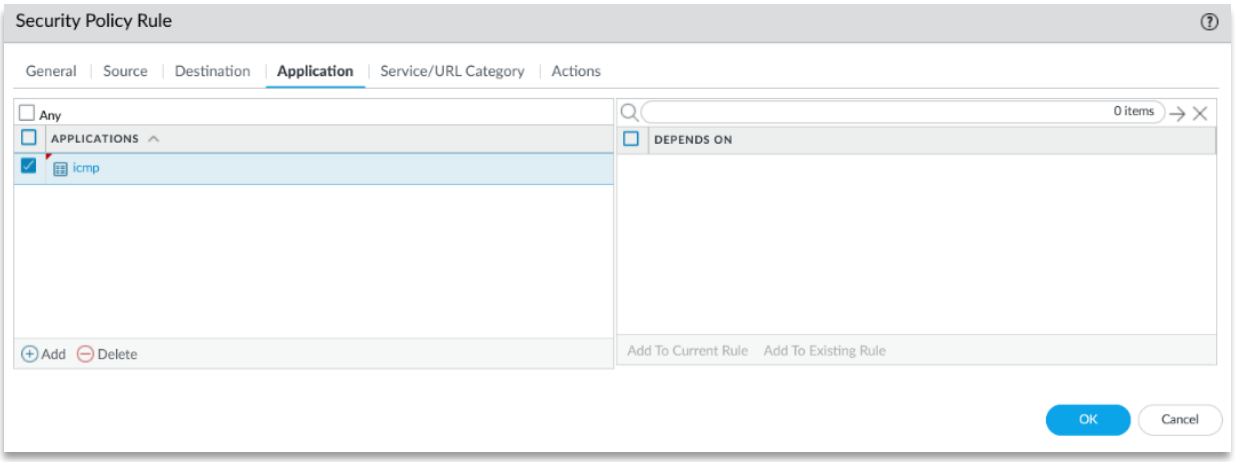


✎ **Note**: The **User** tab is not typically used but can add a user and HIP Profile to this policy if desired.

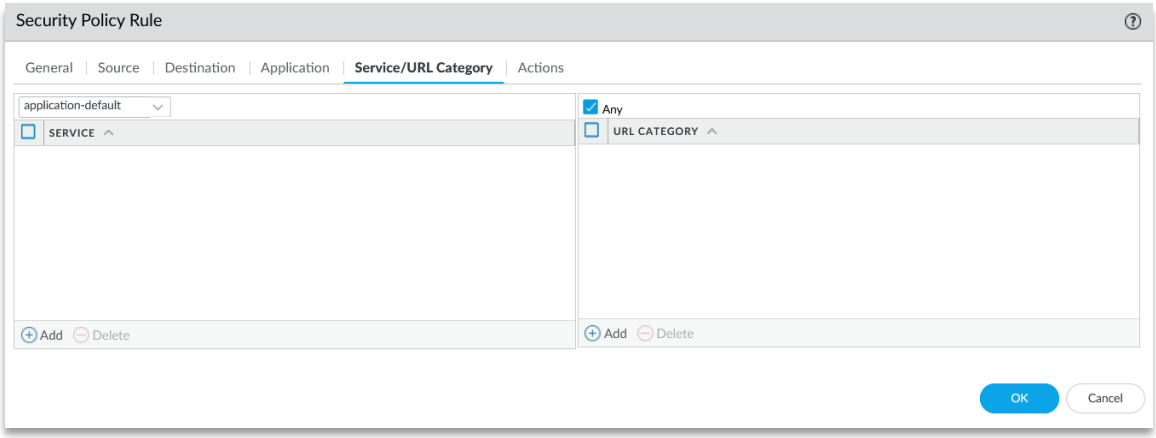
5. Switch to the **Destination** tab and add the Destination Zone and Destination IP range.



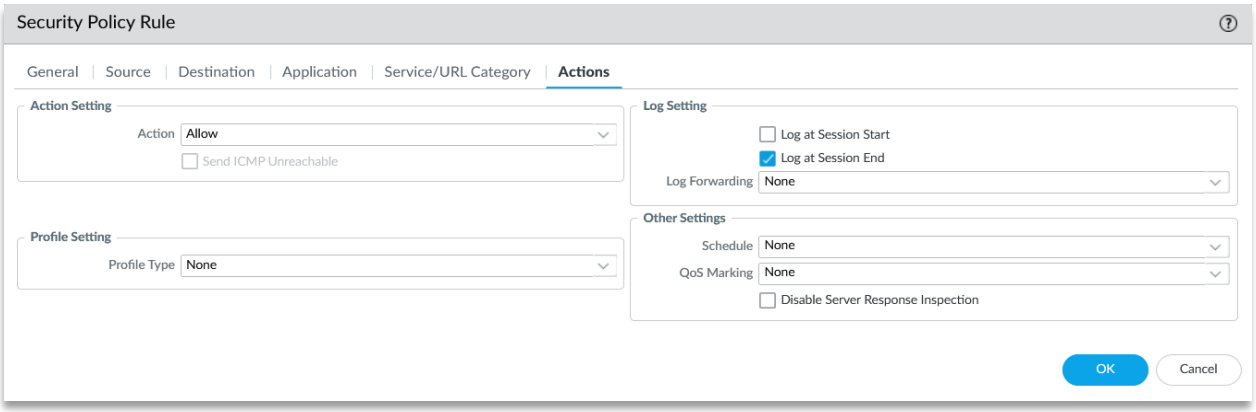
6. Switch to the **Application** tab. Set applications to the rule to allow or block as needed.



7. Select the **Service/URL** Category tab. Add services/URL categories to allow or block accordingly.



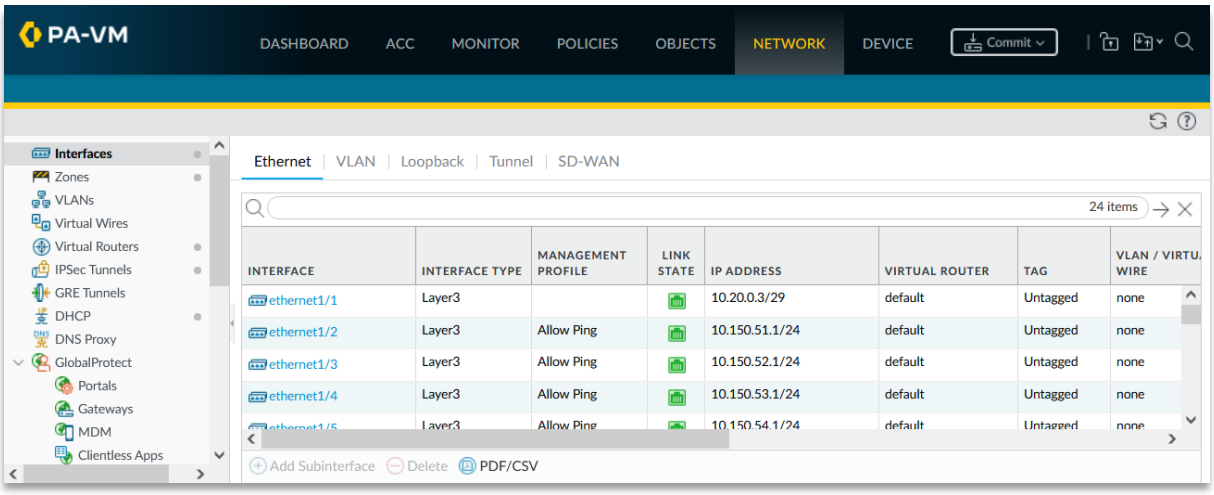
8. Switch to the **Actions** tab and fill in the settings as desired and click **OK** when finished.



3.1.9.2 Interface Management

1. Log in to the Palo Alto web interface.

2. Navigate to the **Network** tab at the top of the webpage.

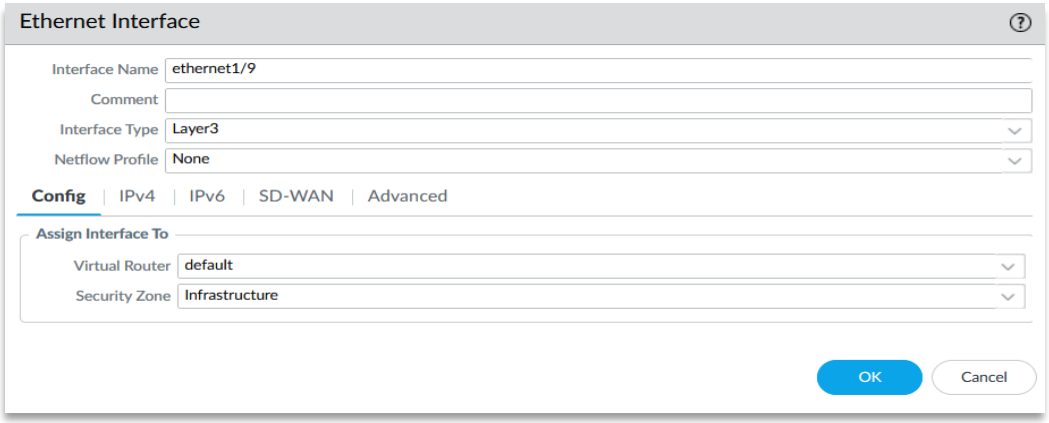


3. Within the **Ethernet** tab, click the desired interface.

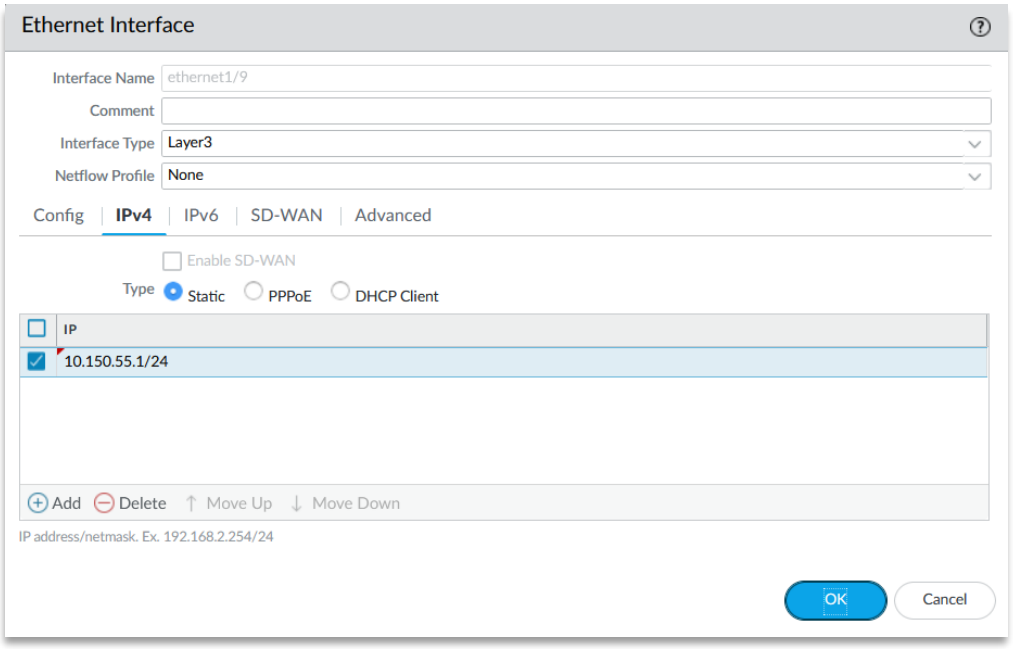
4. Fill out the **Interface Type:** Choose between Layer2, Layer3, Virtual Wire, TAP and HA.

✎ **Note**: Configuration options below are dependent on the selected interface type. The next steps will go over the configuration for a layer 3 interface.

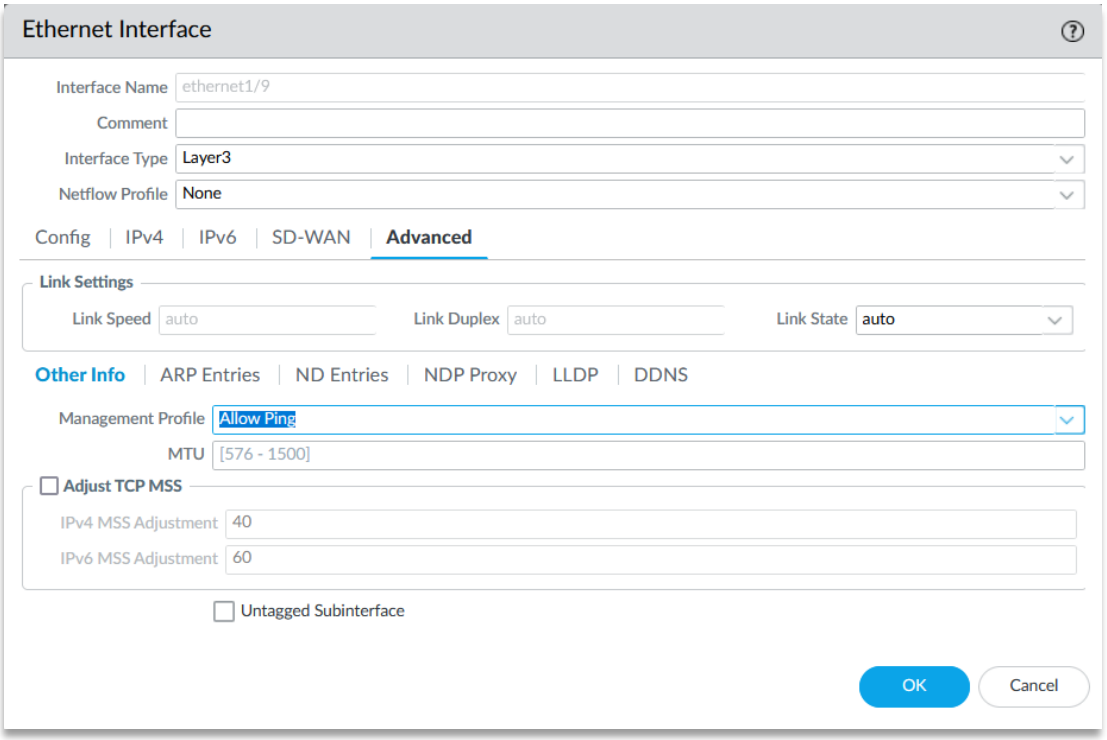
5. Set the Virtual Router and choose a Security Zone.



6. Click **IPv4** and add the designated IP address.



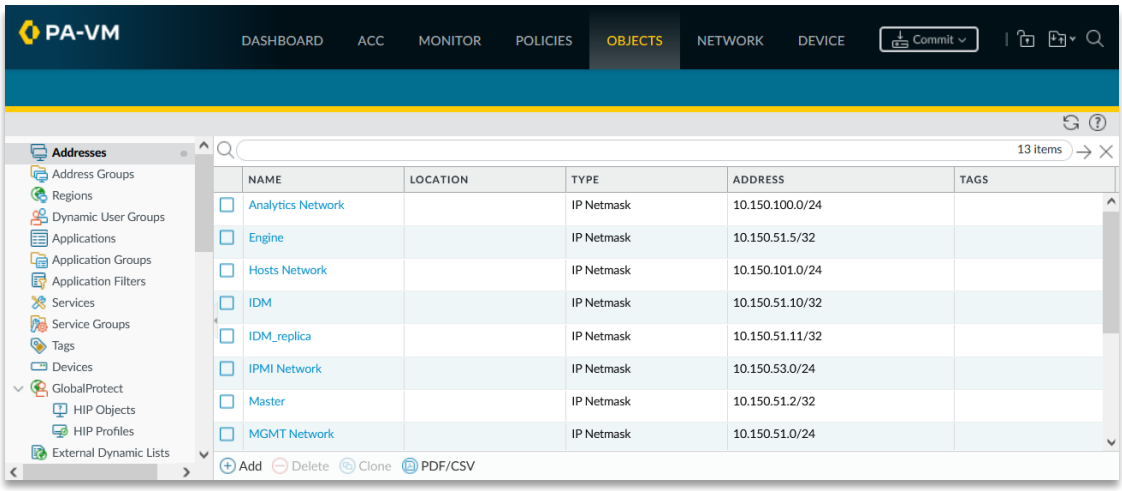
7. Click **Advanced** and populate additional fields as needed. Important fields to consider are MTU, Management profiles and LLDP. The “Allow Ping” profile is selected below.



3.1.9.3 Objects

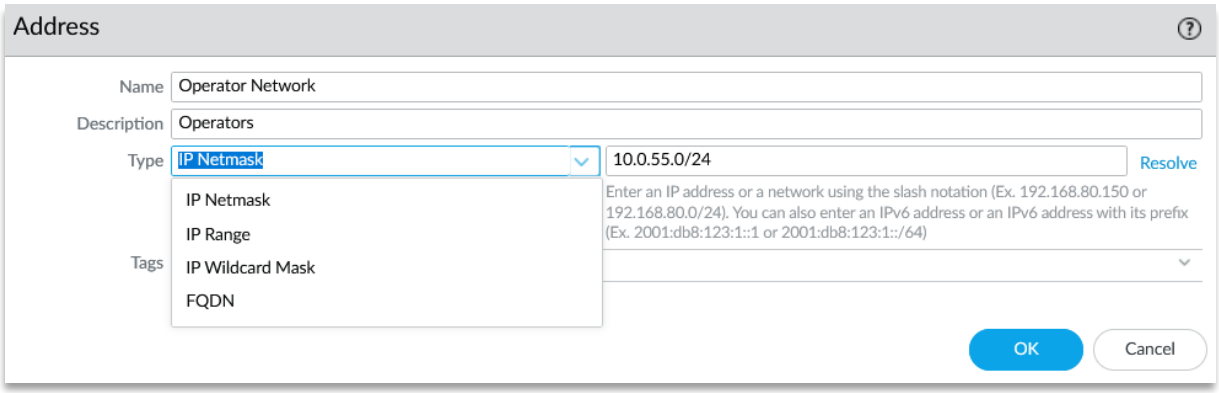
1. Click **Objects** on the top of the webpage.

2. Click **Add** at the bottom of the webpage.



3. Set a **Name** for the object and **Description**.

4. Choose a **Type** for the object which could be IP Netmask, IP Range, IP Wildcard Mask or FQDN. Then enter the required **Value**. Tags are optional.

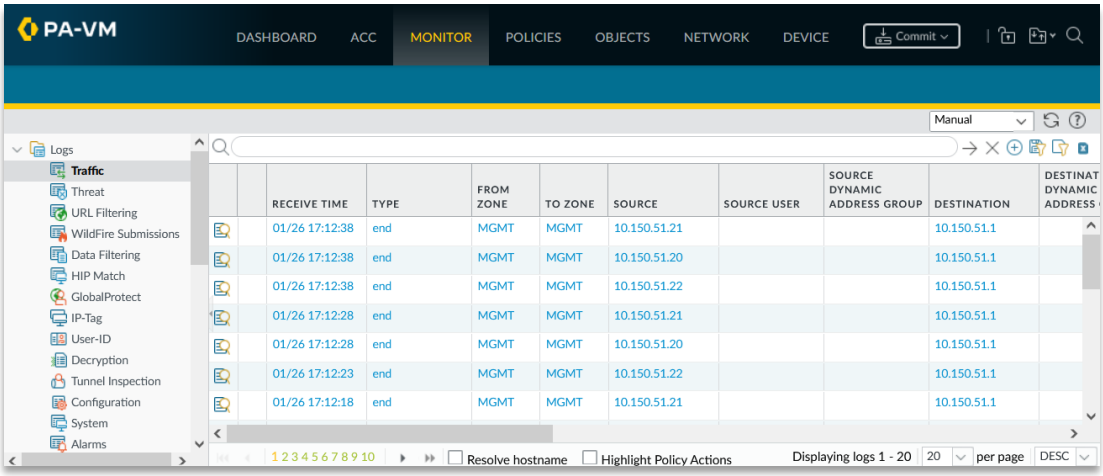


3.1.9.4 Monitor Traffic

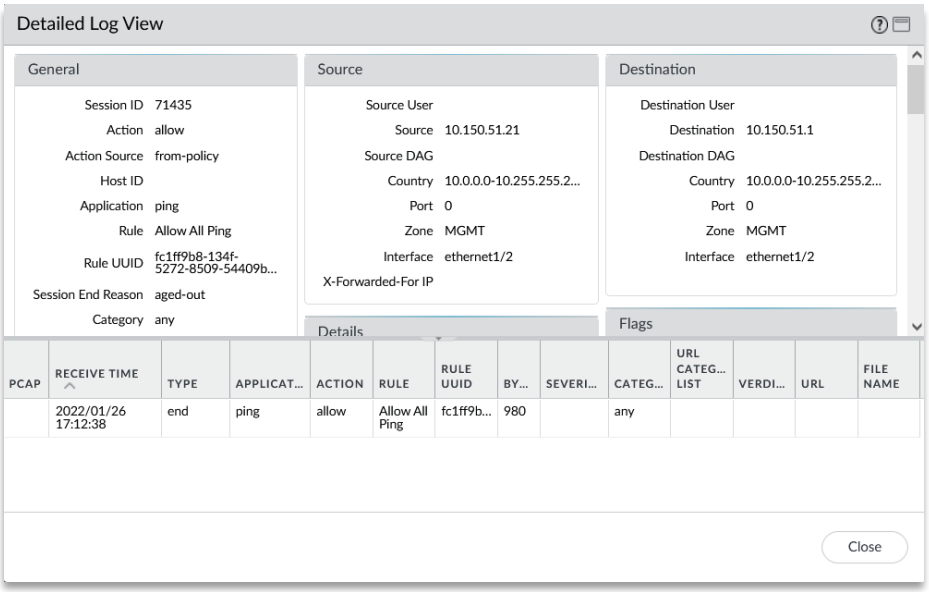
Palo Alto firewalls can also monitor traffic going through the network.

1. Navigate to the **Monitor** tab at the top.
2. Click **Traffic** in the **Logs** category tree to the left.

The traffic logs will display. It shows useful data such as source, destination, IP, port, etc.

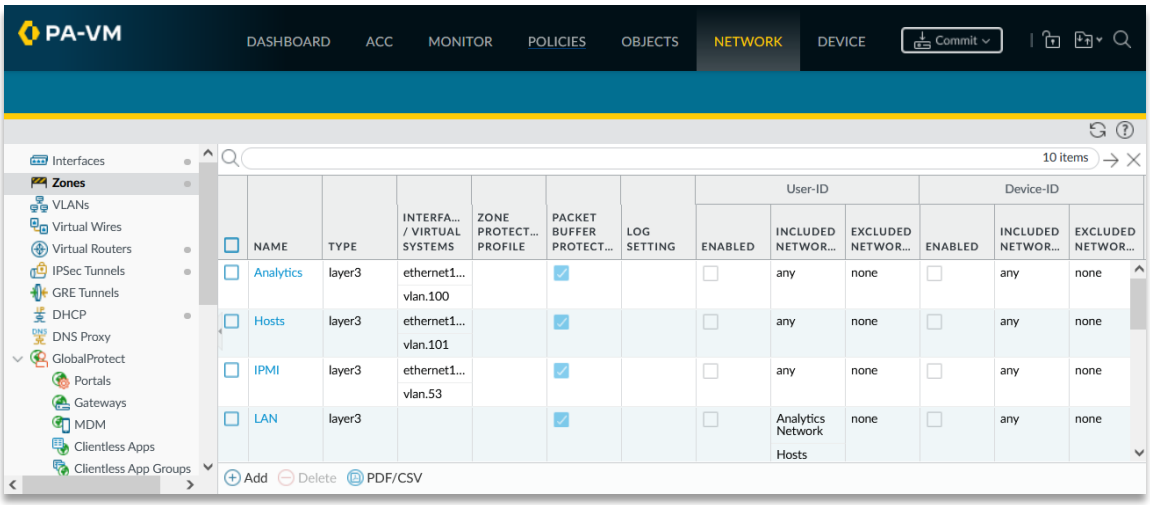


3. Click on the magnifying glass to view more details.



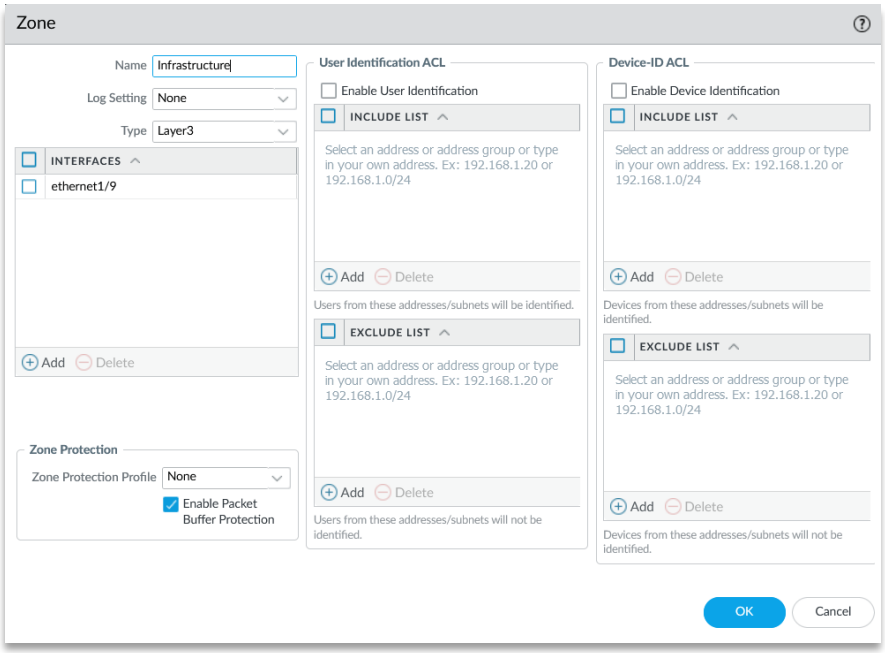
3.1.9.5 Zones

1. Select the **Network** tab and click **Zones**.



2. Towards the bottom of the page, click **Add**.

3. In the name section, choose a relevant name and set the type to Layer 3.



3.1.9.6 Management Profiles

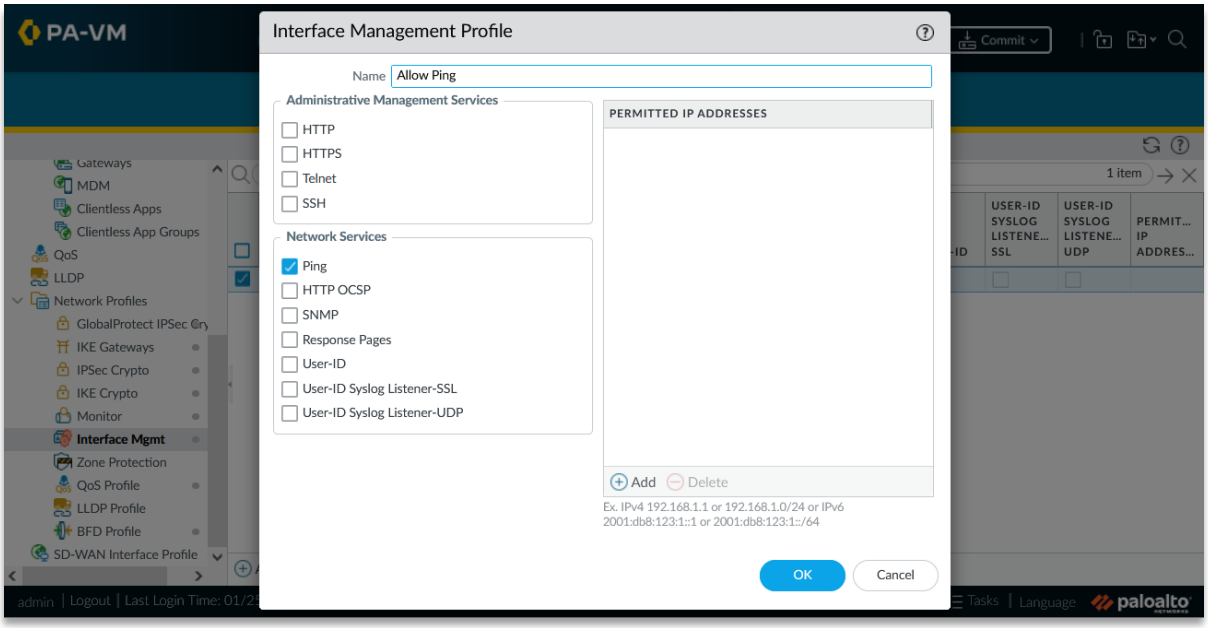
Management profiles are used by Palo Alto to allow for certain protocols to be allowed

1. Click **Network** from the top menu bar, then select **Interface Mgmt** on the side bar

2. Click **Add** near the bottom of the page.

3. Set a relevant name.

4. Place a checkmark next to any desired network services.



5. Press **OK** once finished.

3.1.9.7 Routes

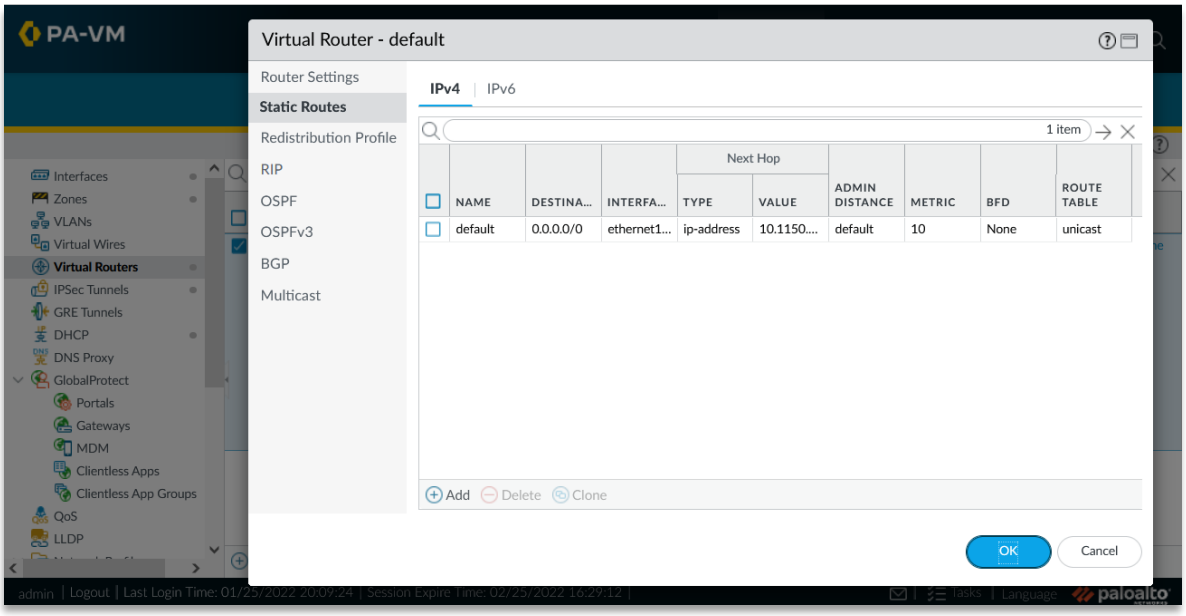
1. Click **Network** at the top of the web interface.

2. Select **Virtual Routers**.

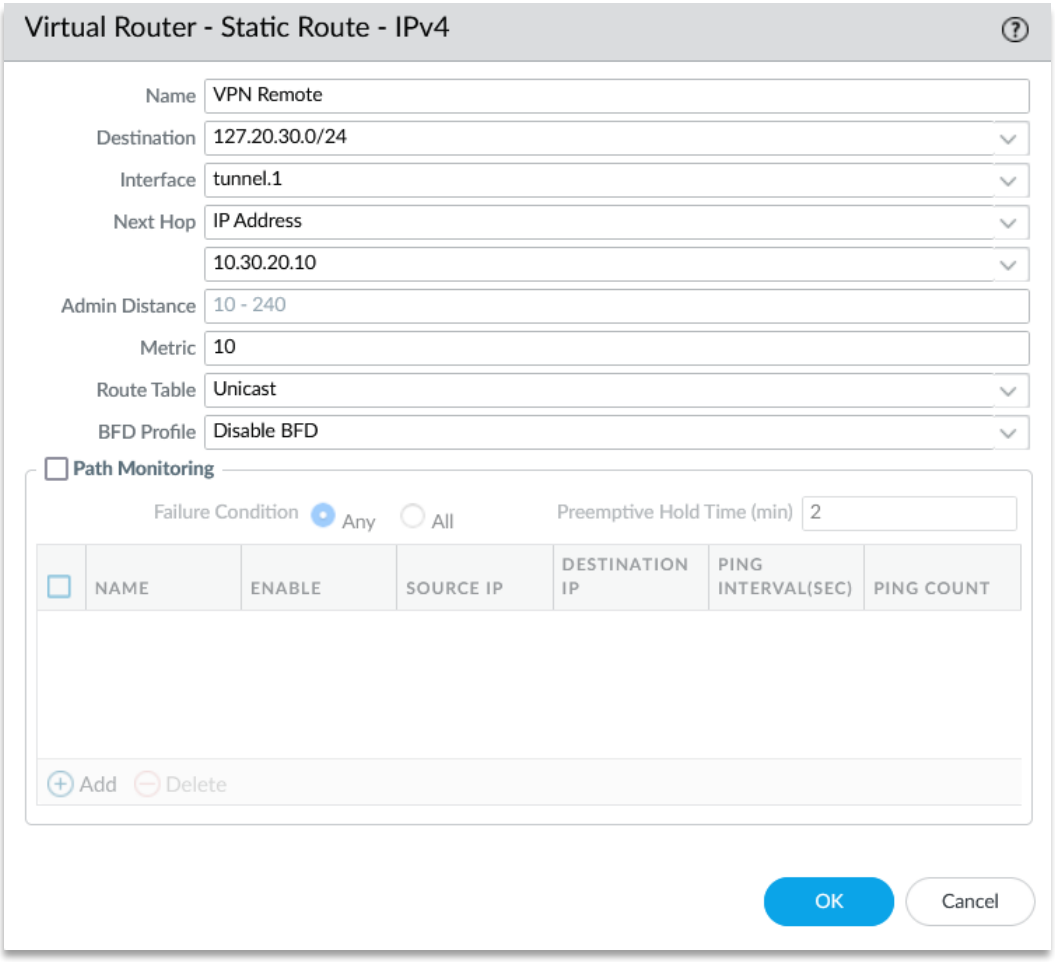
3. Choose and edit the default or preferred virtual router.

4. Click **Static Routes** on the left.

5. Click **Add** towards the bottom of the page.



6. Complete the following steps:
    - Set a **name**
    - Choose a **destination**
    - Select an **interface**
    - Give a desired **Next Hop** as an IP Address.
    - Other fields such as Admin Distance, metric and route table / BFD and path monitoring are optional settings.

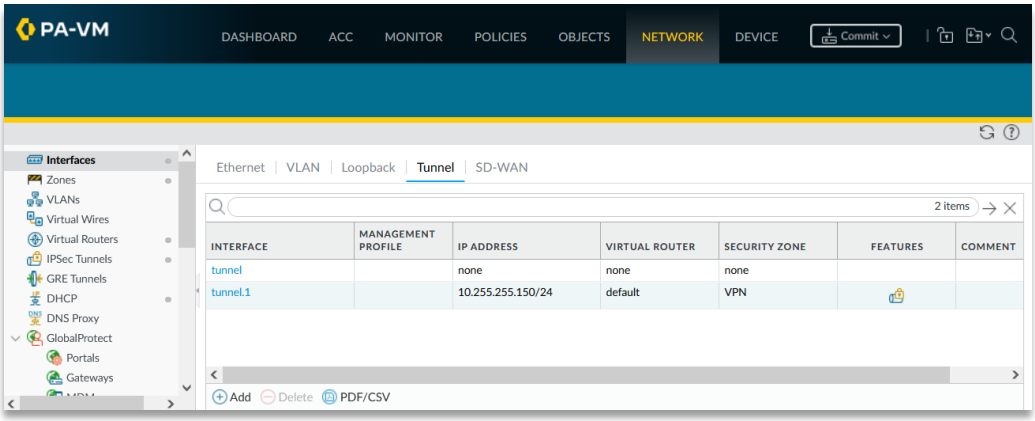


3.1.9.8 Site to Site VPNs

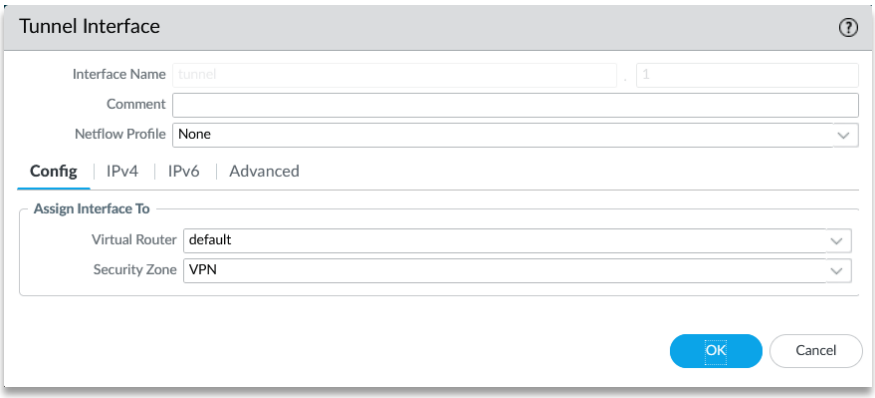
Site to Site VPNs can be implemented using IPSec to allow communication between 2 LANs. First, a static route to the internet must be established. Then, IKE crypto profiles and an IKE gateway must be selected. Finally, an IPSec crypto profile and IPSec tunnel can be configured.

Create a Tunnel

1. Click **Network** at the top of the web interface.
2. Choose **Interfaces** within the sidebar to the left.
3. Switch to **Tunnel** tab.
4. Select **Add.**

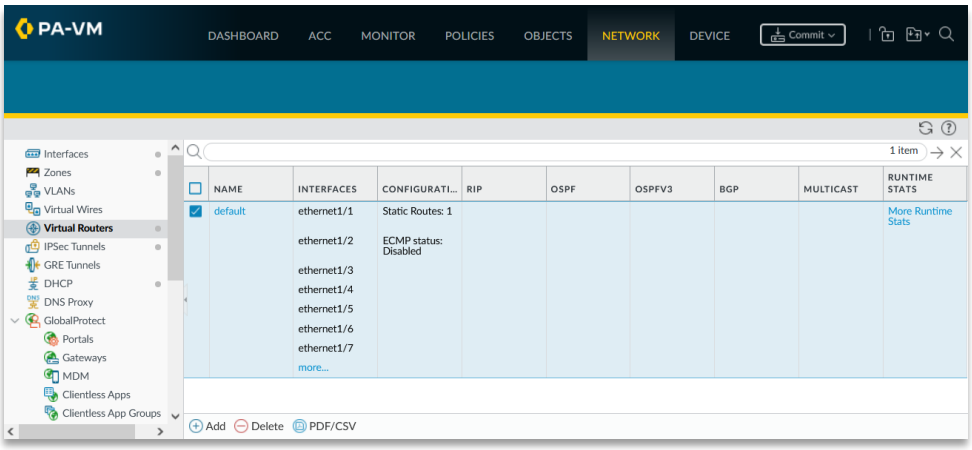


5. Populate the following settings:
    - Provide an **Interface Number ID** (eg. tunnel.1)
    - Set the **Virtual Router** to default
    - Set the **Security Zone** according to traffic then press **OK**.

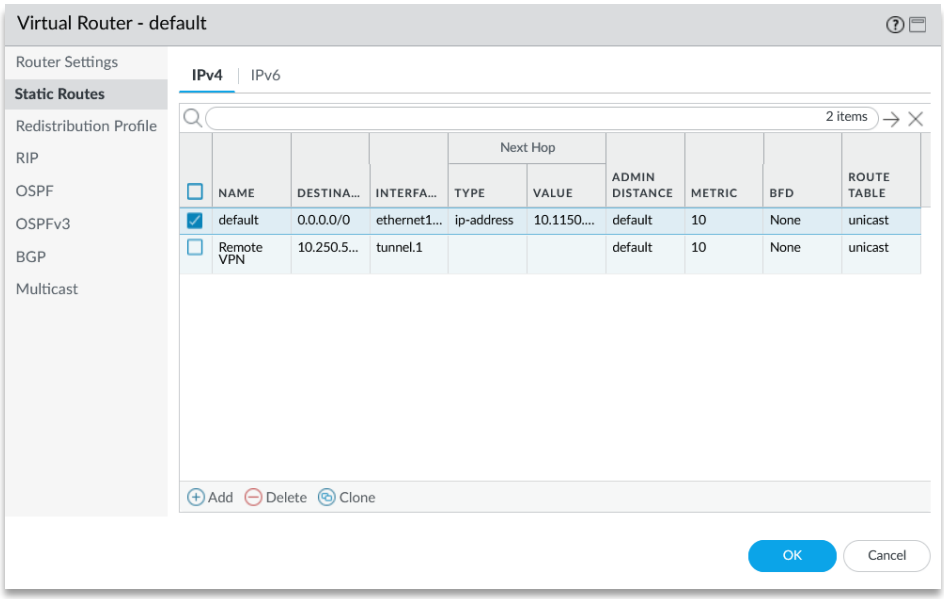


Add a Static Route

1. Click **Network** at the top of the web interface.
2. Select **Virtual Routers**.

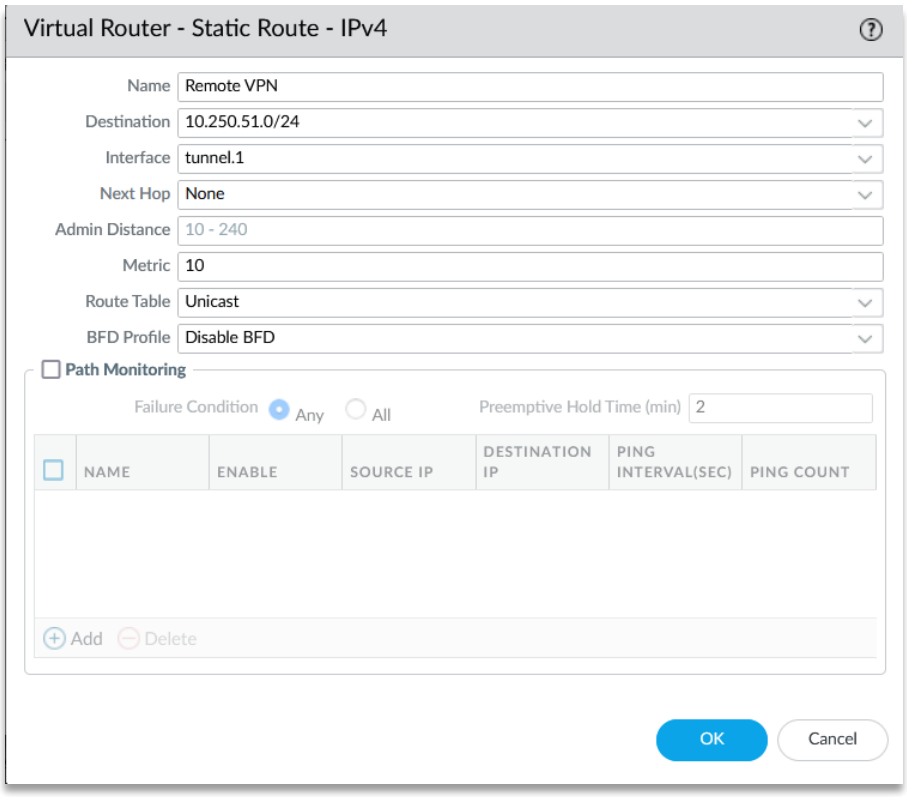


3. Click **Default**.
4. Click **Static Routes.**



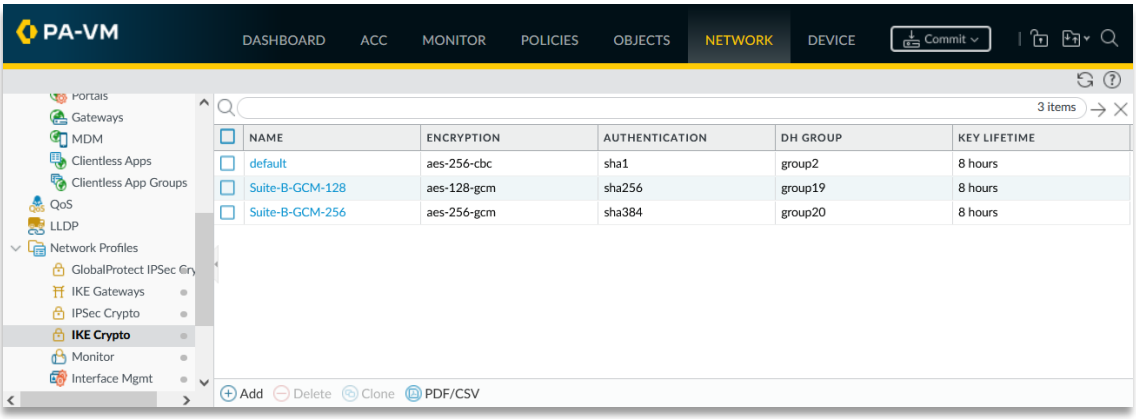
5. Click **Add** towards the bottom of the page.

6. Next, complete the following tasks:
    - Set a **Name**.
    - Give a **Destination** IP as the IP address of the management interface on the other router.
    - Give an **Interface** of tunnel.1.
    - Give the **Next Hop** as none.
    - Other fields can be left blank. Click **OK** to save.

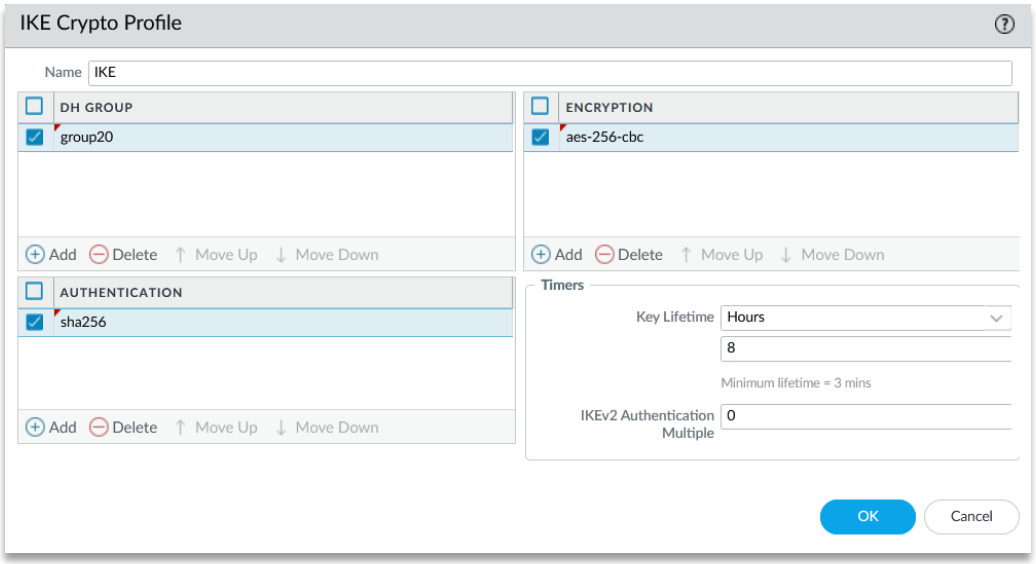


Create an IKE Crypto Profile

1. Select **Network** at the top of the webpage
2. Search for network profiles on the side and choose **IKE Crypto**.
3. Press **Add** towards the bottom of the page.

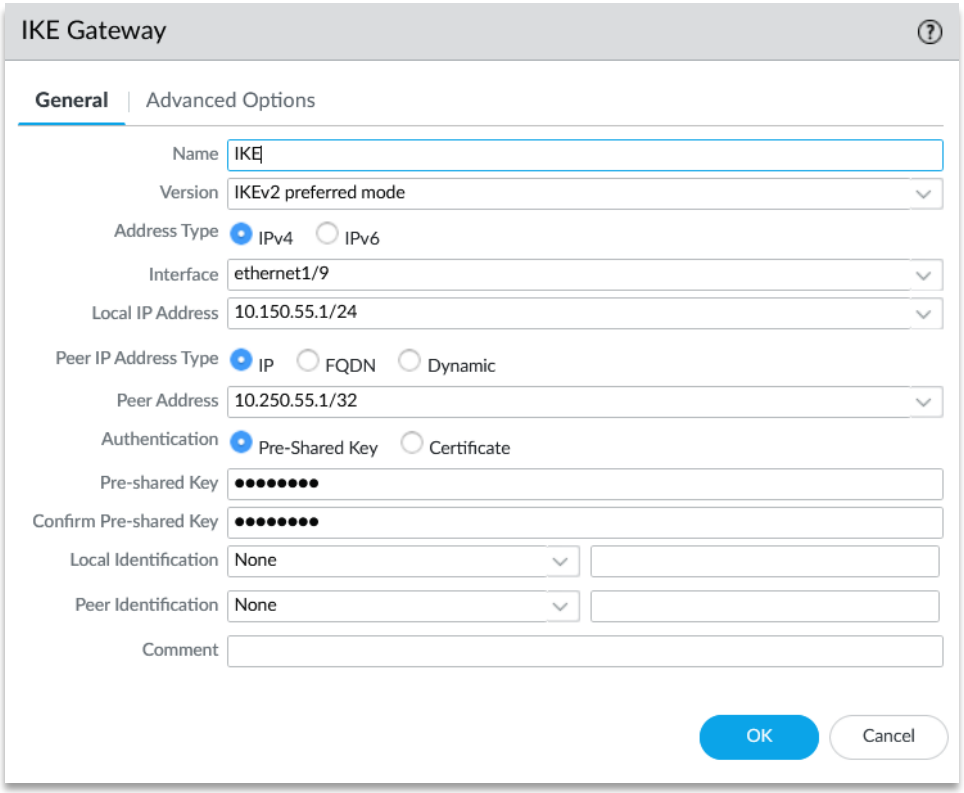


4. Complete the following tasks:
    - Set a desired **Name**
    - Set the **DH Group** to **group20**.
    - Set the **Encryption** to **aes-256-cbc**.
    - Set the **Authentication** to **sha256**.
    - Finally set **Key Lifetime** to 8.
    - Press **OK** to save and close.

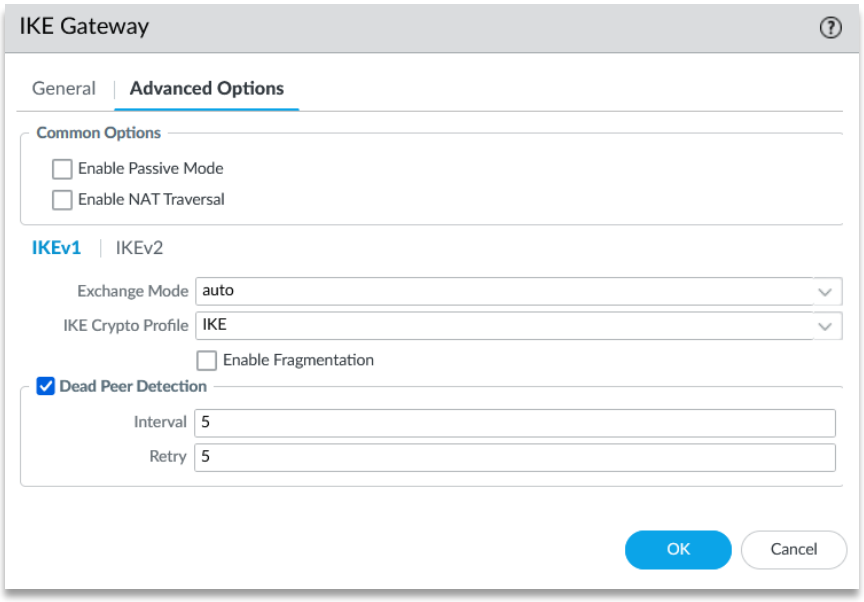


Create an IKE Gateway

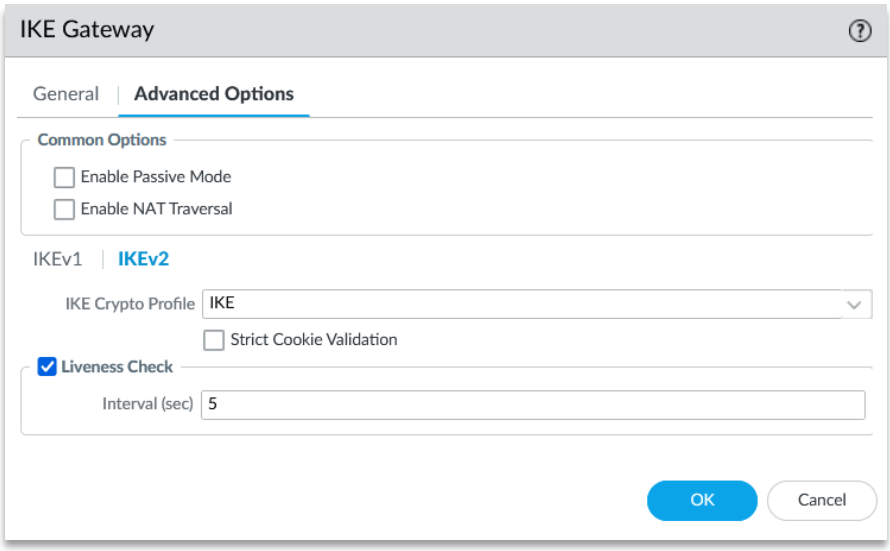
1. Select **Network**
2. Look for network profiles on the left and choose **IKE Gateways**.
3. Press **Add** and complete the following tasks:
    - Give a **Name**.
    - Set the **Version** to **IKEv2 preferred mode**.
    - Set the **Address Type** to **IPv4**.
    - Set the **Interface** to the **Internal Interface**, which connects to the other router.
    - Set the **Local IP Address** to the IP address on the internal interface. Include the subnet mask
    - For the **Peer Address**, put the IP address of the internal interface on the other firewall. Do not include the subnet mask.
    - For **Authentication**, use a pre shared key and choose the key shared with the other firewall.



4. Next, select **Advanced Options**. On IKEv1 exchange mode, click **Auto**.
    - **IKE Crypto Profile** set the name of the IKE profile previously configured
    - **Enable Dead Peer Detection**.

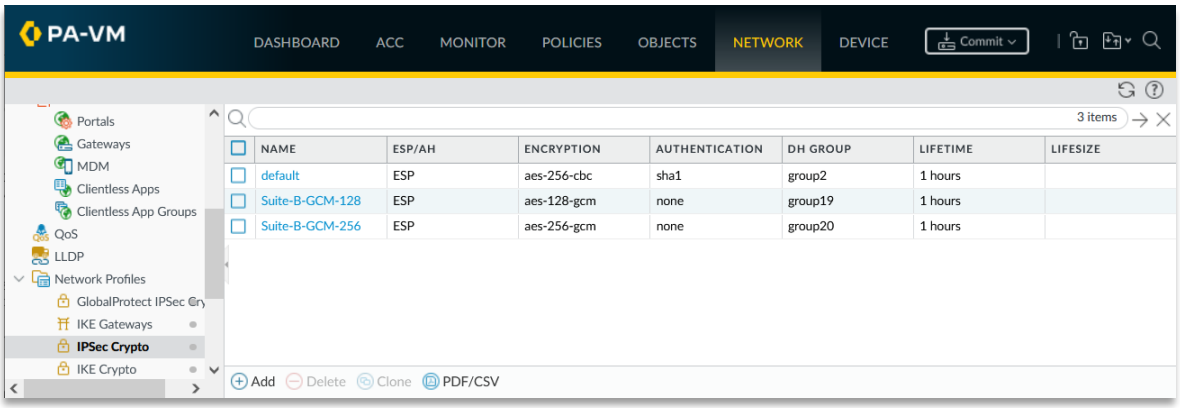


5. Within **Advanced Options**, switch to the **IKEv2** tab and select the **IKE Crypto Profile** previously created. Press **OK** to save and exit.

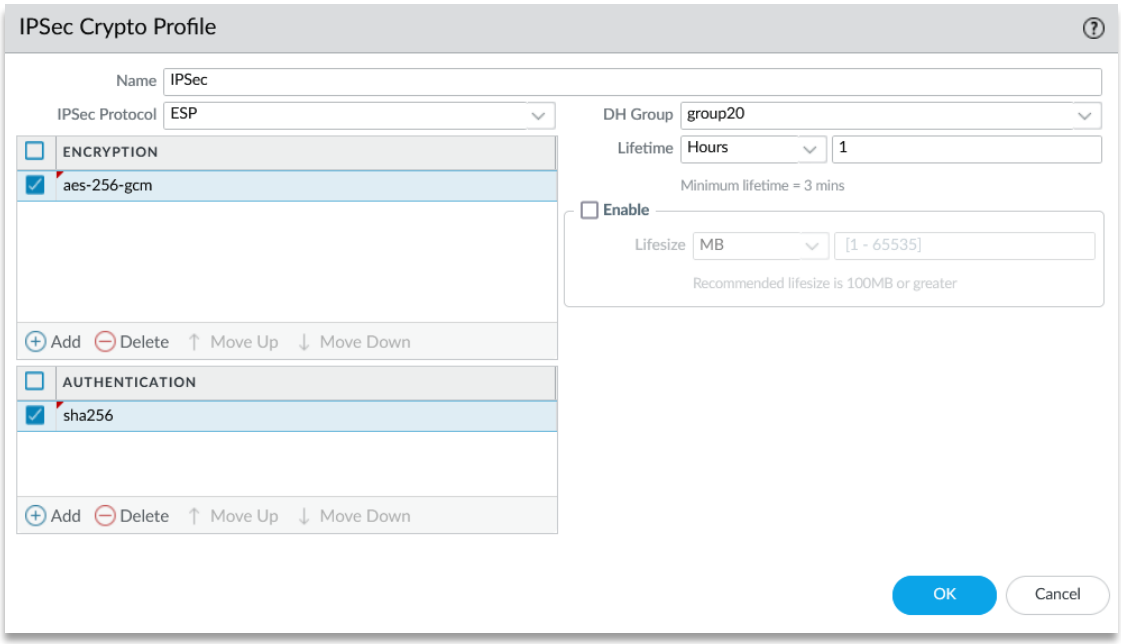


Create an IPSEC Crypto Profile

1. Choose **Network**, located at the top of the webpage.
2. Look for network profiles on the side and choose **IPSEC Crypto**.

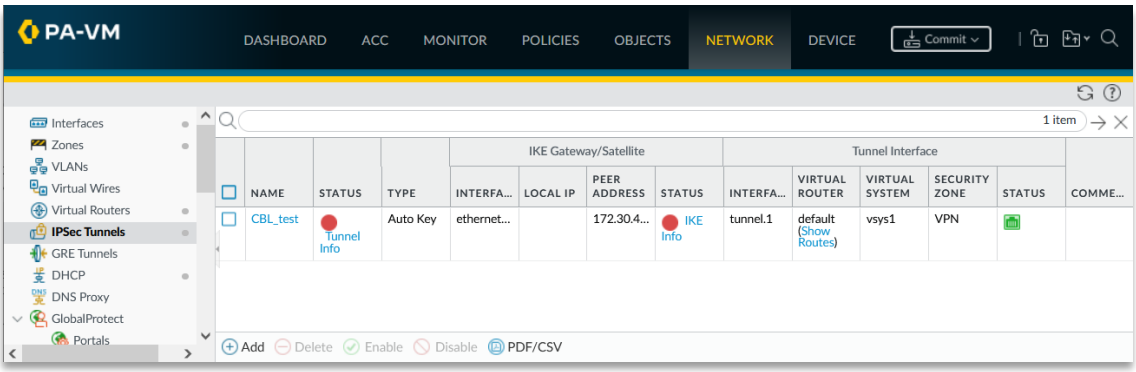


3. Press **Add** towards the bottom.
4. Complete the following tasks (the rest are optional):
    - Set a desired **Name**
    - Press **Add** and set the DH Group to **group20**.
    - Set the **Encryption** to **aes-256gcm** and the **Authentication** to **sha256**.

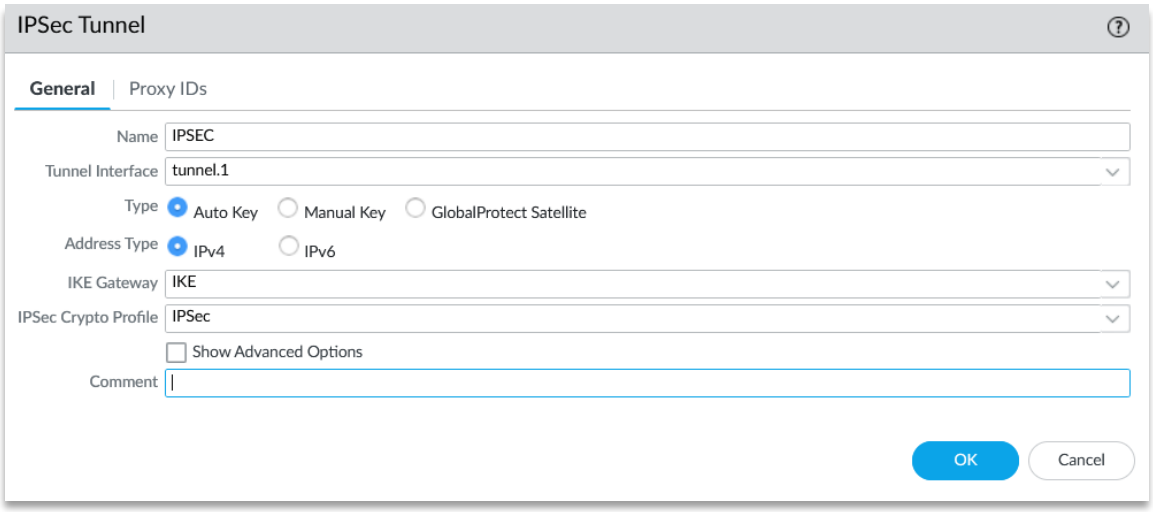


Create an IPSec Tunnel

1. Navigate to the **Network** tab, then choose **IPSec tunnels** on the left.



2. Click **Add** towards the bottom of the page and complete the following tasks:
    - Provide a **Name**.
    - Choose the **Tunnel Interface** previously configured.
    - Set the **Type** as **Auto Key.**
    - Put the **Address Type** as **IPv4**.
    - Set **IKE Gateway** to the name previously configured.
    - Set **IPSec Crypto Profile** to the name previously configured.

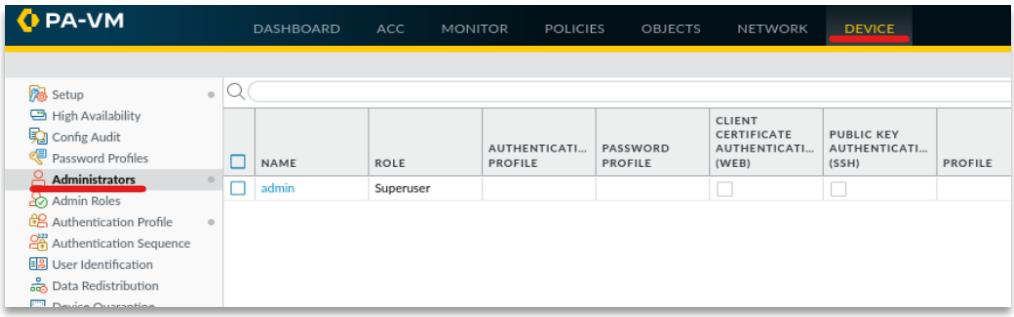


3. Press **OK** to save and close.

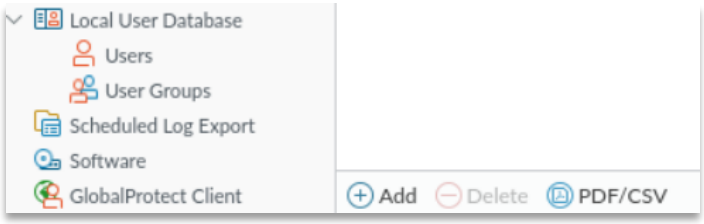
3.1.9.9 Creating a backup admin account in Palo Alto

Administrative accounts specify roles and authentication methods for firewall administrators. Perform the following steps to add an administrative account on the firewall.

1. Select **Device** > **Administrators**.



2. **Add** a new account.

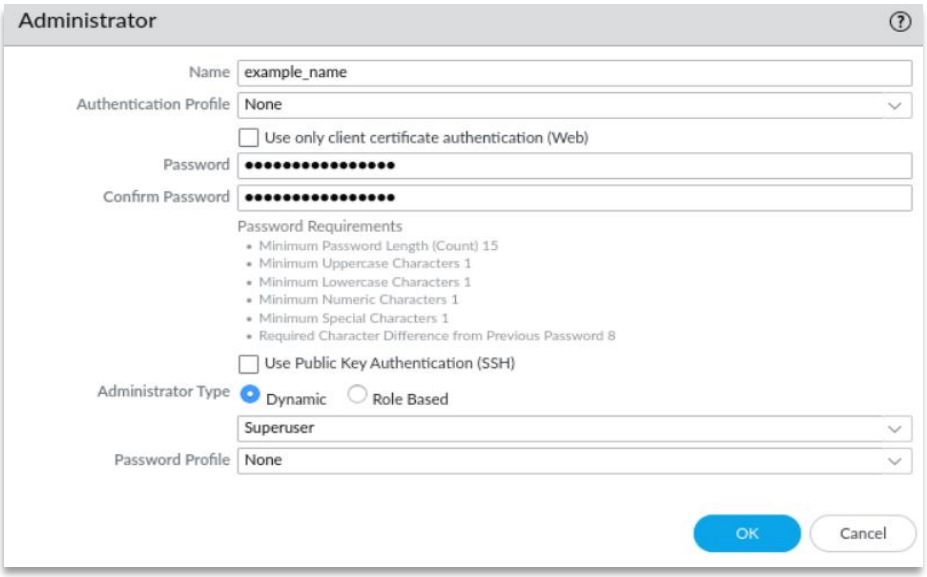


3. Enter a **Name** for the account.

4. Select an Authentication Profile or sequence, if you configured either, for the administrator.

5. Select the Administrator Type.

6. Select a **Password Profile** for administrators that the firewall authenticates locally without a local user database.

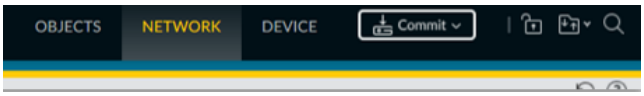


7. Click **OK** and **Commit.**

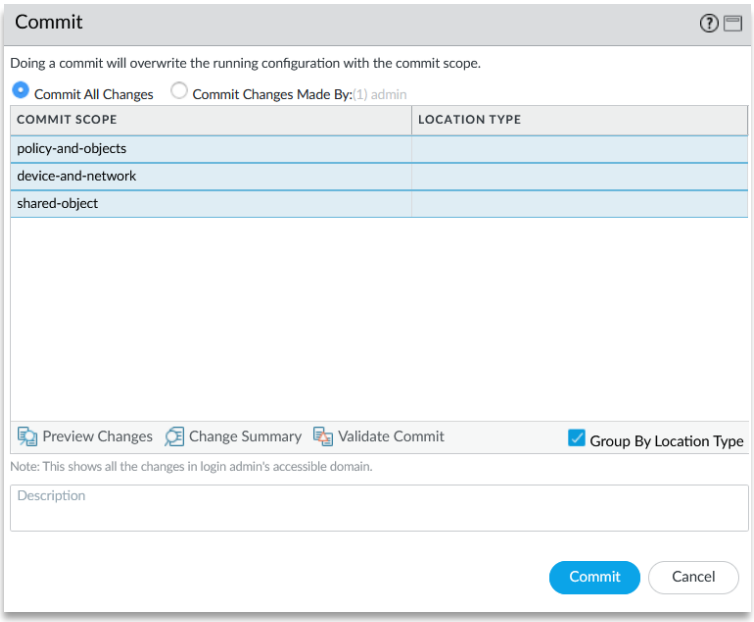
3.1.9.10 Committing changes

In Palo Alto it is important to frequently commit changes after modifying the configuration. Follow these steps to save all pending changes:

1. Click **Commit** at the top of the webpage.



2. Press **Commit** again when the window appears.



3.1.10 Configuration Overview

Managing proper network configuration of the DDS-M kit is vital to mission success. However, understanding details of DDS-M's network scheme and controlling network traffic can be very difficult without basic knowledge of physical and logical components of the network. This section is written to help users better understand the DDS-M's network and further configure the kit's network in accordance with the needs of any mission.

3.1.10.1 VLAN configuration

The deployed kit, both DDS-Mv1E and DDS-Mv2, will have 6 primary VLAN networks.

VLAN 51	10.<kit#>.**51**.0/24	Management Network
	10.<kit#>.51.2	Bastion
	10.<kit#>.51.5	vCenter
	10.<kit#>.51.10/11	IdM
	10.<kit#>.51.20-25	Nodes 0-5

VLAN 52	10.<kit#>.**52**.0/24	Storage Network
	10.<kit#>.52.20-25	vSAN

VLAN 53	10.<kit#>.**53**.0/24	vMotion Network
	10.<kit#>.53.20-25	vMotion

VLAN 101	10.<kit#>.**101**.0/24	Tools Network
	10.<kit#>.101.100	Sec Onion Manager
	10.<kit#>.101.101/102	Sec Onion Search
	10.<kit#>.101.254	Palo Alto

VLAN 102	10.<kit#>.102.0/24	User Network

VLAN 192	10.<kit#>.**52**.0/24	IPMI Network
	192.168.0.2	Bastion IPMI
	192.168.0.20-25	Nodes IPMI

Switch IPs		
1.1.1.2	-	T-switch MGMT
2.2.2.2	-	F-switch MGMT
3.3.3.2	-	Cisco MGMT

3.1.10.2 Switch Configuration

T-Switch VLAN map

F-Switch VLAN map

Common switch commands:

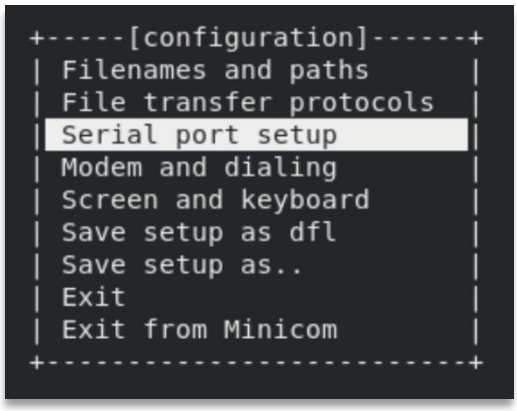
COMMAND	PURPOSE
show running-config	View fill running configuration
interface ethernet 1/1/x	Configure and individual interface
interface range ethernet 1/1/x-1/1/y	Select a range of interface
show config	Show running configuration on interface
interface vlan x	Configure a VLAN interface
ip address <ip> <netmask>	Configure an IP address on interface
switchport access vlan x	Assign an interface to a VLAN
switchport trunk allowed vlan x	Allow a VLAN on a trunk
copy running-configuration startup configuration	Persist changes between switch reboot
exit	Return to configuration mode, exec mode, or logout

3.1.10.3 Minicom

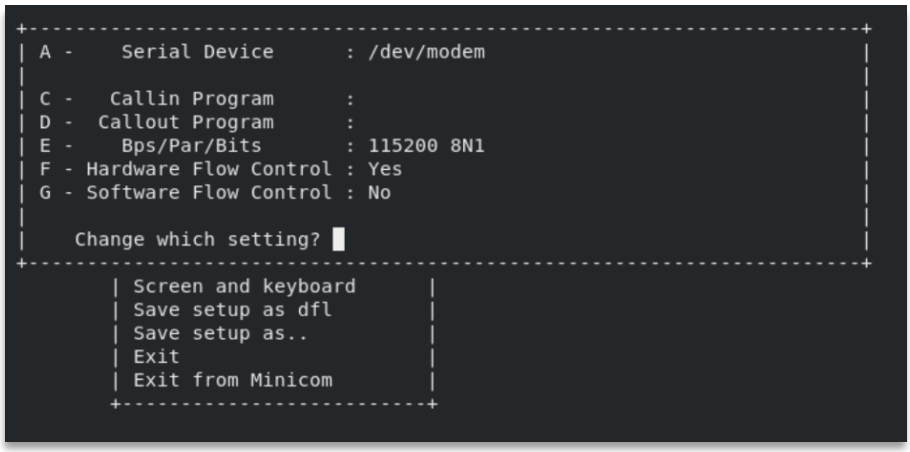
Minicom is a text-based interface that allows users to send and receive data, transfer files, run scripts, and emulate a terminal. It's easy to use and provides a friendly interface for configuring the serial port and selecting features like baud rate, flow control, and parity.

✎ **Note:** The following steps are for ttyUSB0, the steps will not change for ttyUSB1, other than replacing the number 0 with a 1.

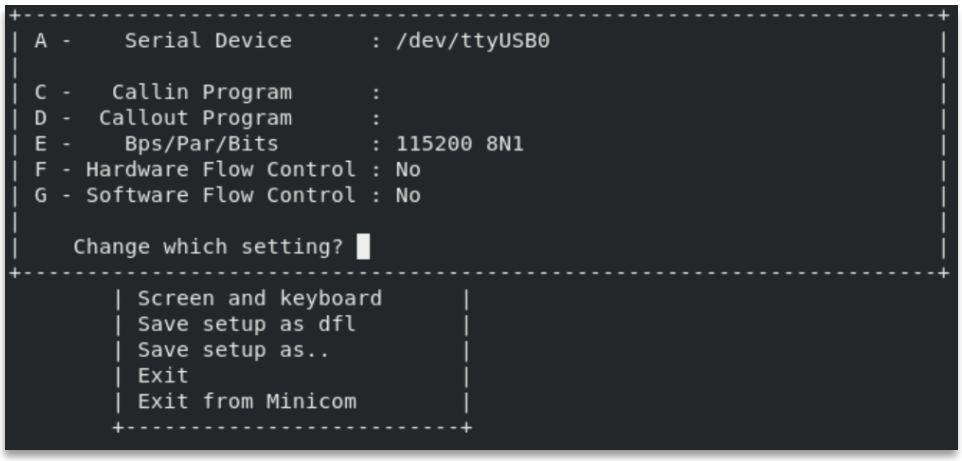
1. If a customized configuration is required, run **minicom -s** to access the setup menu and navigate down to Serial port setup.



2. Hit [**ENTER**] to perform setup.



1. Edit the Serial Device by entering [**A**] to modify the line and change the entry to **/dev/ttyUSB0**.



2. After editing the line, press [**ENTER**] to save this change.

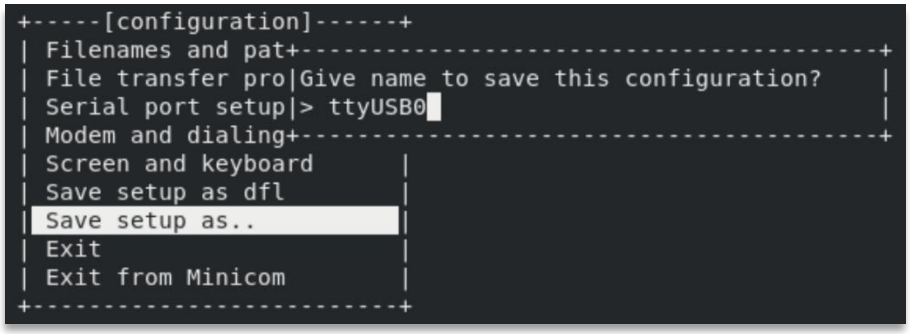
3. Press [**F**] to set **Hardware Flow Control** to **No**

✎ **Note:** The Baud rate in line E will be 9600 for the Cisco switch

4. then press [**ENTER**] to exit the setup configuration.

5. To save the configuration to a profile, navigate to '**Save setup as..**' and press [**ENTER**].

6. name this configuration **ttyUSB0**.



7. Press [**ENTER**] to save this configuration.

8. Navigate to '**Exit from Minicom**' and press 'enter' to exit the minicom configuration.

3.1.10.4 Switch configuration

The current DDS-M kit includes 3 switches: a Dell S4112F, a Dell S4112T, and the Cisco WS-C3560. The Dell switches are configuration managed enterprise level 1/10/100G switches that have many features including VLAN and IP routing whereas the Cisco switch is configured for plug-and-play user access. The Cisco Catalyst 3560CX has a total of 16 ports and is a mid-grade enterprise-level 1G switch.

✎ **Note:** SSH connection to switches from FIPS enabled systems will fail due to negotiation requirements.

Connecting to Dell switches (115200 default baud rate):

Using a serial USB port (recommended when applying changes):

```
[defender@master ~]$ sudo stty sane
[defender@master ~]$ sudo minicom ttyUSB0
[defender@master ~]$ sudo minicom ttyUSB1
```

Connecting to Cisco switches (9600 default baud rate):

Using a serial USB port (recommended when applying changes):

```
[defender@master ~]$ sudo stty sane
[defender@master ~]$ sudo minicom ttyACM0
```

✎ **Note**: "**#**" If the cisco profile does not exist, perform *Minicom Setup* in Section 11.1.4.

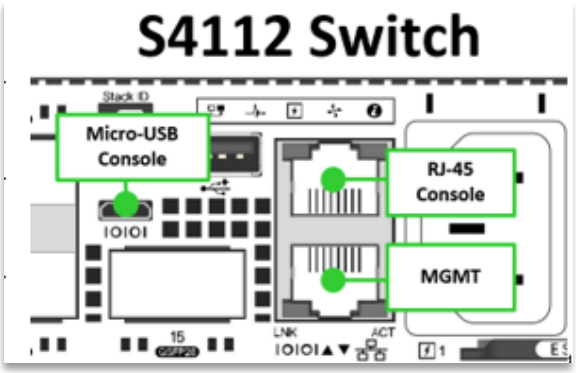
3.1.11 Resetting Switches

✎**Note:** Depending on circumstances, Users will either use vendor ZTP or manually reset with the following steps.

3.1.11.1 Dell S4112 Switches

The following scenario will return the included Dell S4112-series Switches to a factory default configuration.

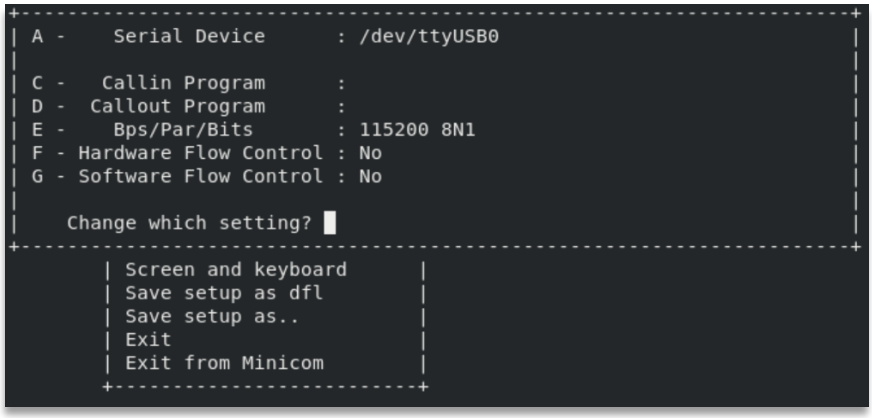
1. Connect the appropriate cable to the serial console port of the switch.



2. Open a terminal window on the **Admin Laptop** and type:

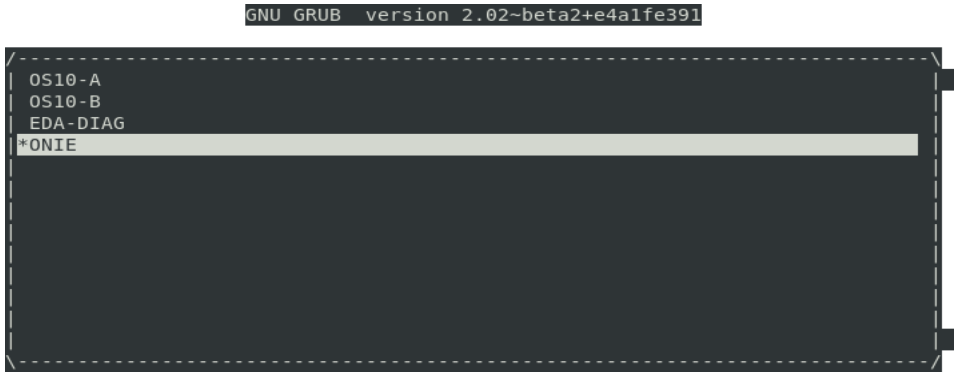
```
$ sudo minicom ttyUSB0
```

Your minicom menu should look like the following for the dell switches. If not, follow the instructions here to change them.



3. Power cycle the *Dell S4112* series switch by un-seating and re-seating the power cable.

4. Interrupt the Grub boot process by hitting the [**UP or DOWN**] key. Select the **ONIE** menu entry and from the submenu select **ONIE Install**.



✎ **Note:** The ONIE Installation process will automatically begin when a correct DHCP lease is acquired, from the Bastion node, by the management interface on each switch.

5. Exit the minicom session by pressing [**CTRL +A**] then [**Q**] and then selecting [**YES**] to exit.

3.1.11.2 Cisco Catalyst Switch

If you need to factory reset the Cisco switch for any reason, follow the below steps.

1. Minicom into the Cisco switch by connecting the kit provided console cable and typing '**sudo minicom -D ttyACM0**'.

```
# sudo minicom -D ttyACM0
```

2. Unplug the switch.

3. While holding the mode button, plug the switch back in.

4. Continue to hold down the mode button for approximately 1 minute. Several lights on the front will flash multiple times.

1. Type **flash_init**

2. Type **boot**

3. Type '**dir flash:**' . This should show you the files that exist on the switch. If you see config.text or vlan.dat, they must be deleted using the instructions below. If they do not exist, skip to step 8.

4. Type **del flash:config.text** and confirm deletion by typing '**y**' and pressing [**ENTER**].

```
switch: del flash:config.text
```

5. Type **del flash:vlan.dat** and confirm deletion by typing '**y**' and pressing [**ENTER**].

```
switch: del flash:vlan.dat
```

6. Type **boot**.

```
switch: boot
```

✎ **Note:** There may be a PnP error during this reboot. This is expected. DO NOT touch the mouse or keyboard during the reboot or you risk aborting the flash process.

3.1.11.3 Mellanox SW2050 Switch

To reset the switch back to factory settings, follow these steps.

1. Power the switch on and wait for the system to settle to an operational state.

2. For quick confirmation confirm the following lights are active and solid green.

3. Locate and press the reset button for 15 seconds using a paper clip or a similar item with a small end.

4. Upon release, the switch will reset.

WARNING: Do not use force to press the reset button as this will cause the button to break.

Once the switch resets it will be return to factory defaults.

3.2 Virtual Machine Administration

You can manage individual virtual machines or a group of virtual machines that belongs to a host or cluster.

From the virtual machine's console, you can change the guest operating system settings, use applications, browse the file system, monitor system performance, and so on. Use snapshots to capture the state of the virtual machine at the time you take the snapshot.

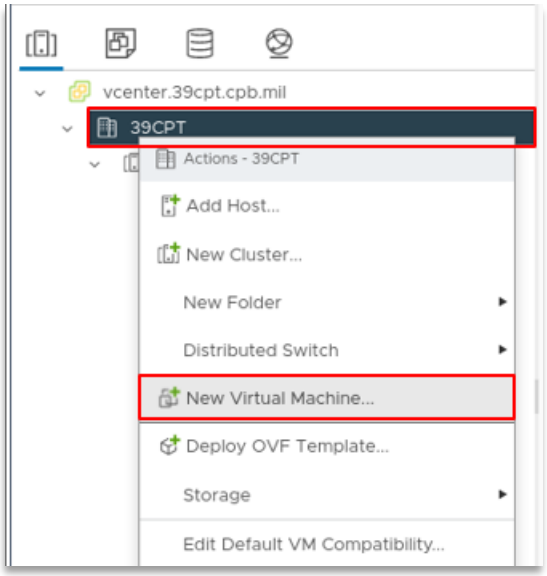
3.2.1 VM Creation

1. Login to the vSphere client at https://vcenter.<kit#>cpt.cpb.mil

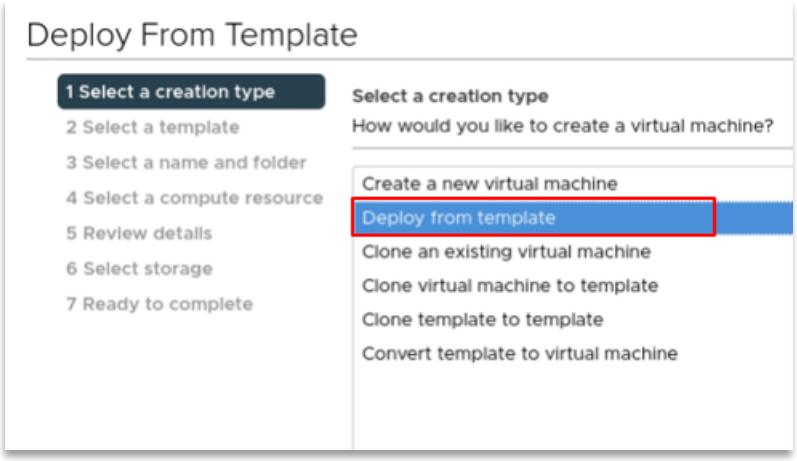
2. Click the kit section on the left-hand side

3. Once it is selected Right click

4. Select New Virtual Machine.



5. Once the Window opens select the “Deploy from template” section

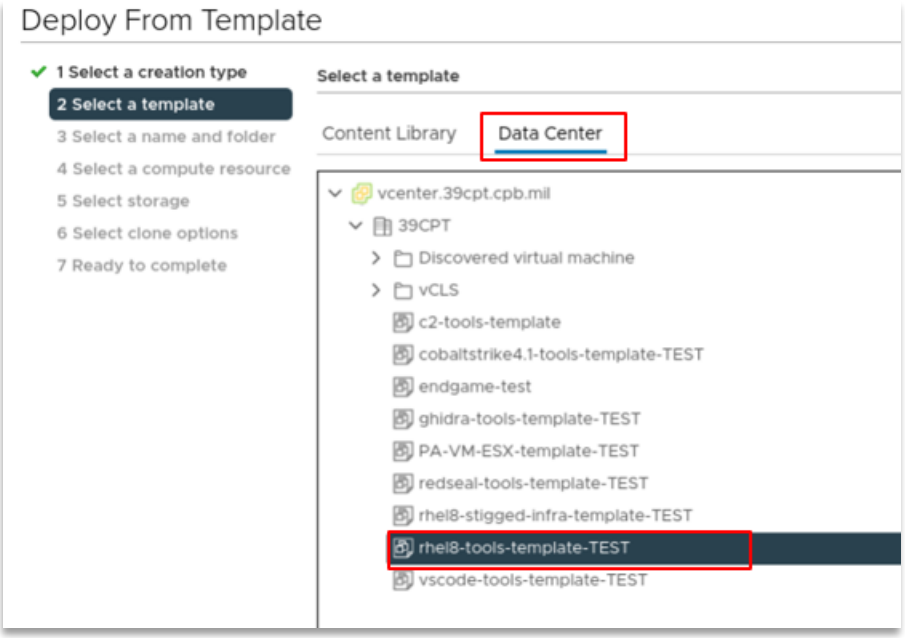


6. Click next

7. Click on the database cylinder

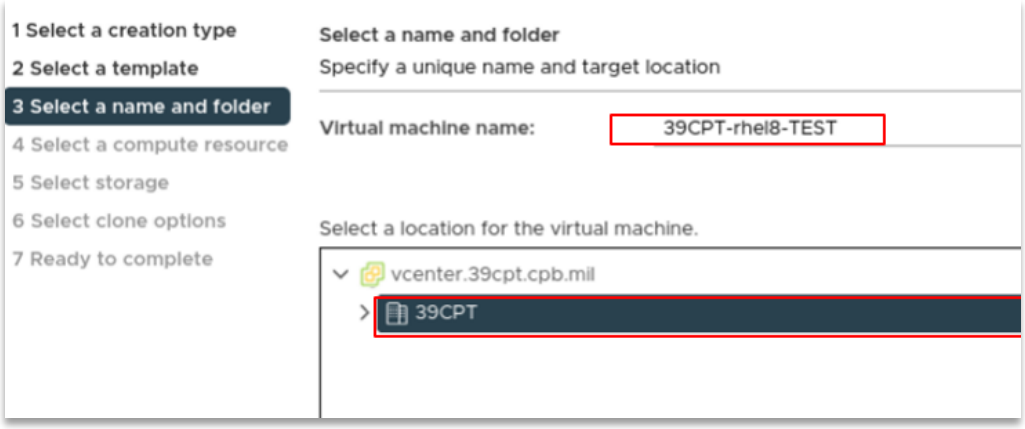
8. Click into the folders till you find the “ISO” folder

9. Select the template you wish to build from

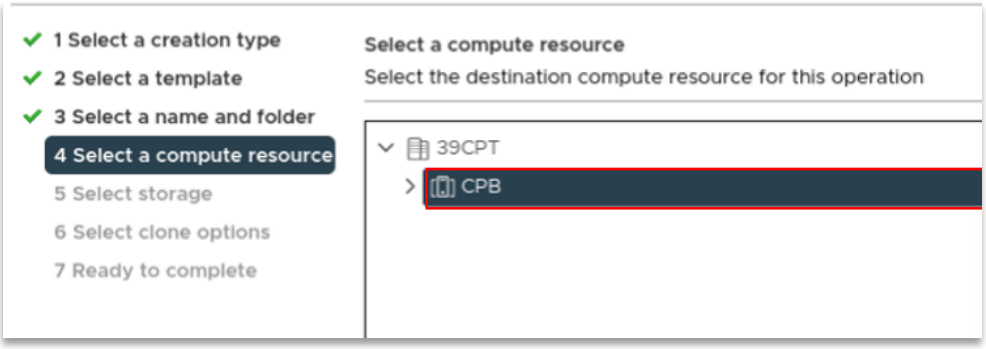


Click next

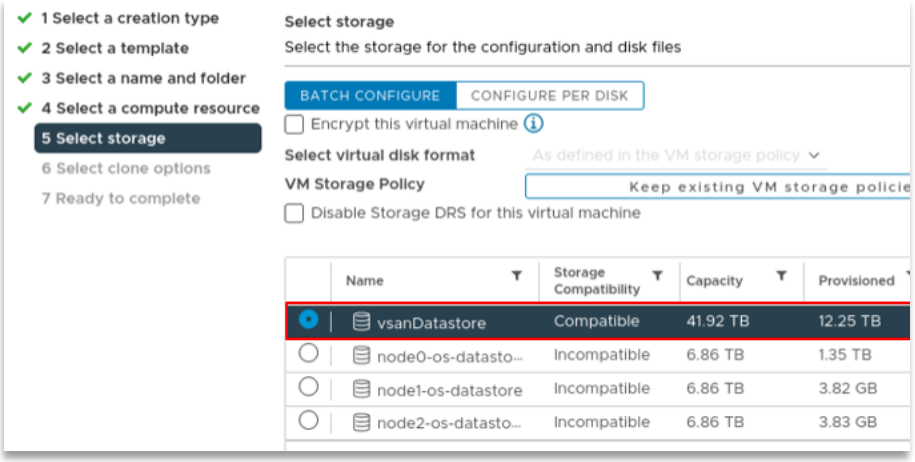
10. Name the VM and select the kit cluster or node that it will be deployed to.



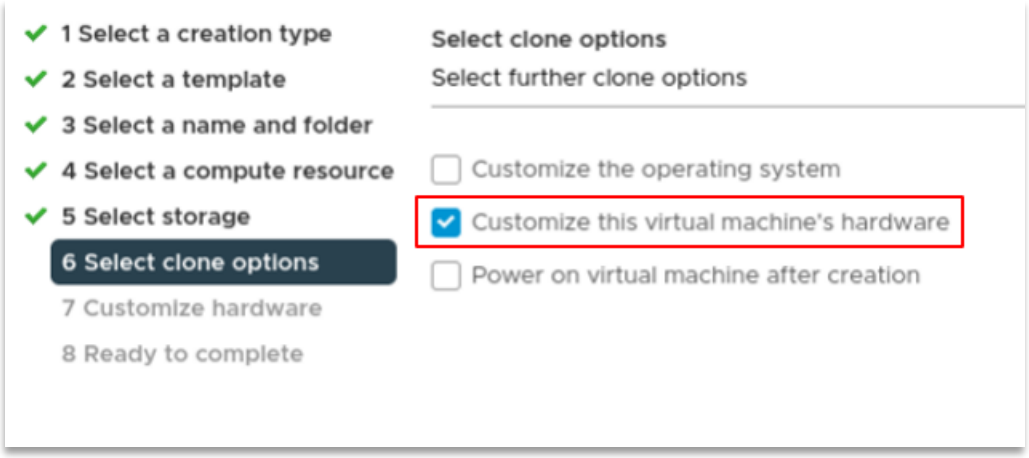
11. Select the resource pool that the VM will be operating from.



12. Select the storage pool the VM will pull from.

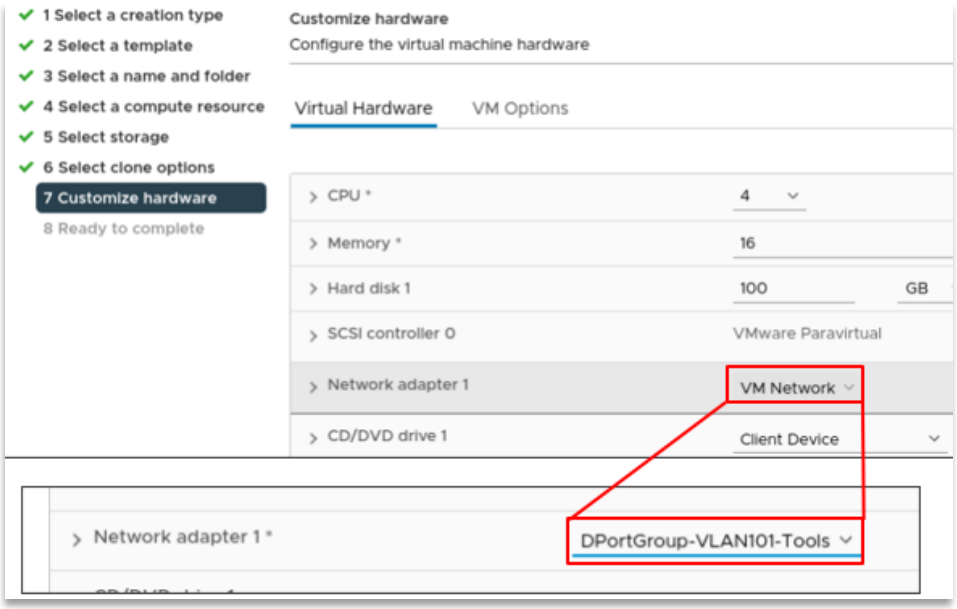


13. Select the option to customize the VMs hardware.

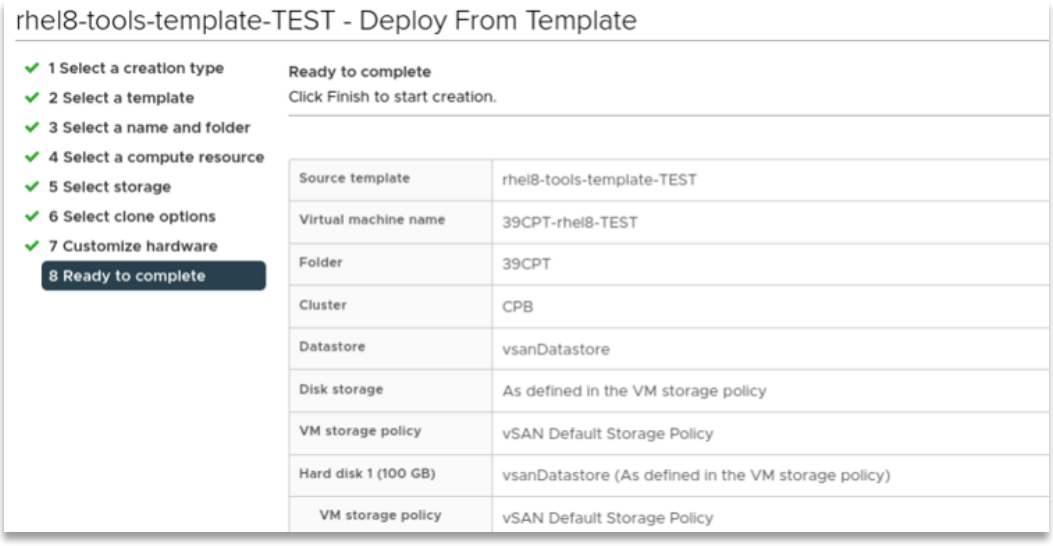


14. Customize hardware, as desired.

15. Ensure the Network Adapter 1 is set to the Tools VLAN.



16. Once you have customized the deployment, review the information and approve, when ready.



3.2.2 Managing Power States of a Virtual Machine

The basic power operations for a virtual machine include powering on, powering off, suspending, reset, and hard stop. These power options are analogous to the power operations on a physical computer.

1. Navigate to a virtual machine in the inventory.
2. Right-click the virtual machine or click **Actions**
3. Select **Power**.
4. Select a power operation:
    a. Power On: Powers on a virtual machine when the virtual machine is stopped.
    b. Power Off: Powers off a virtual machine. Powering off a virtual machine might cause loss of data within the guest operating system.
    c. Suspend: Suspends a running virtual machine and leaves it connected to the network. When you resume a suspended virtual machine, the virtual machine continues operating at the same point the virtual machine was at when it was suspended.
    d. Reset: Restarts the guest operating system. By using this operation, the virtual machine powers off and then powers on. By resetting a virtual machine, you might lose all unsaved information within a guest operating system.
    e. Hard Stop: You can use this operation only when you cannot power off a virtual machine or if a virtual machine becomes unresponsive. When you hard stop a virtual machine, all processes are ended, and the virtual machine is powered off. By using this operation, you may lose all unsaved information.

3.2.3 Edit Virtual Machine Startup and Shutdown Settings

You can configure virtual machines running on an ESXi host to start up and shut down with the host or after a delay. You can also set the default timing and startup order for virtual machines. This way, the operating system has enough time to save data when the host enters maintenance mode or is being powered off for another reason.

The Virtual Machine Startup and Shutdown (automatic startup) setting is deactivated for all virtual machines residing on hosts that are in a vSphere HA cluster. Automatic startup is not supported with vSphere HA.

1. In the vSphere Client, navigate to and select the host where the virtual machine is located.

2. Click the **Configure** tab.

3. Under **Virtual Machines**, select **VM Startup/Shutdown** and click **Edit**.
    a. The Edit VM Startup/Shutdown Configuration dialog box opens.

4. Select **Automatically start and stop the virtual machines with the system**.

5. (Optional) In the Default VM Settings pane, configure the default startup and shutdown behavior for all virtual machines on the host.

Setting	***Description***
Startup Delay	After you start the ESXi host, it starts powering on the virtual machines that are configured for automatic startup. After the ESXi host powers on the first virtual machine, the host waits for the specified delay time and then powers on the next virtual machine. The virtual machines are powered on in the startup order specified under the Default VM Settings pane.
Continue if VMware Tools is started	Shortens the startup delay of the virtual machine. If VMware Tools starts before the specified delay time passes, the ESXi host powers on the next virtual machine without waiting for the delay time to pass.
Shutdown Delay	Shutdown delay is the maximum time the ESXi host waits for a shutdown command to complete. When you power off the ESXi host, the autostart manager initiates the automatic shutdown on the first virtual machine and waits within the specific delay time for the virtual machine to complete the power action. The power action can be Power Off, Guest Shutdown, or Suspended. The order in which virtual machines are shut down is the reverse of their startup order. After the ESXi host shuts down the first virtual machine within the time that you specify, the host shuts down the next virtual machine. If a virtual machine does not shut down within the specified delay time, the host runs a power off command and then starts shutting down the next virtual machine. The ESXi host shuts down only after all virtual machines are shut down.
Shutdown Action	Select a shutdown action that is applicable to the virtual machines on the host when the host shuts down. • Guest Shutdown • Power Off • Suspend • None

6. (Optional) You can also configure the startup order and behavior for individual virtual machines. Use this option when you need the delay of the virtual machine to be different from the default delay for all machines. The settings that you configure for individual virtual machines override their default settings.
    a. To change the startup order of virtual machines, select a virtual machine from the **Manual Startup** category and use the up arrow to move it up to the **Automatic** or **Automatic Ordered** categories. Use the up and down arrows to change the startup order for virtual machines in the **Automatic** and **Manual Startup** categories. During shutdown, the virtual machines shut down in the reverse order.

    b. To edit the startup and shutdown behavior of a virtual machine, select a virtual machine, use the up arrow to move it, and click the **Edit** icon. The **Virtual Machine Startup/Shutdown** setting dialog box opens.

    c. In the **Startup Settings** pane, configure the startup behavior of the virtual machine. You can decide to use the default startup delay or you can specify a new one. If you select **Continue immediately if VMware Tools starts**, the ESXi host powers on the next virtual machine without waiting for the delay to pass.

    d. In the **Shutdown Settings** pane, configure the shutdown behavior of the virtual machine. You can use the default shutdown delay or specify a new one and select the shutdown action.

    e. Click **OK**.

7. Click **OK**.

3.2.4 Answer Virtual Machine Questions

Virtual machine questions are messages that are generated by vCenter Server. Virtual machine questions appear whenever the virtual machine needs user intervention to continue its operation. In most cases, virtual machine questions appear when you power on a virtual machine.

To save time and ensure the consistency of your virtual environment, you can apply the same answer to multiple or to all virtual machines that have the same pending question.

1. Navigate to a virtual machine with a question.
2. Right-click the virtual machine and select **Guest OS** > **Answer Question**.
    a. The **Answer Question** wizard opens.
3. In the **Answer Question** dialog box, select your answer.
4. (Optional) Apply the selected answer to other virtual machines that have the same pending question.

a. Click the **Select other virtual machines** hyperlink. A list of all virtual machines with the same pending question appears.
b. Select the virtual machines to which to apply the answer.

5 Click **OK**.

3.2.5 Adding Existing Virtual Machines to vCenter Server

When you add a host to vCenter Server, it discovers all the virtual machines on that managed host and adds them to the vCenter Server inventory.

If a managed host is disconnected, the already discovered virtual machines continue to be listed in the inventory.

If a managed host is disconnected and reconnected, any changes to the virtual machines on that managed host are identified, and the vSphere Client updates the list of virtual machines. For example, if node3 is removed and node4 is added, the new list of virtual machines adds node4 and shows node3 as orphaned.

3.2.6 Remove VMs or VM Templates from vCenter Server or from the Datastore

You can temporarily remove a virtual machine or a VM template from vCenter Server or you can permanently delete it from the datastore.

The process is the same for virtual machine or a VM template:

- When you remove a virtual machine from the inventory, you unregister it from the host and vCenter Server, you do not delete it from the datastore. Virtual machine files remain at the same storage location and you can later re-register the virtual machine by using the datastore browser. This helps if you want to edit the virtual machine configuration file. It is also useful to temporarily remove a virtual machine when you have reached the maximum number of virtual machines that your license or hardware allows.
- If you no longer need a virtual machine and want to free up space on the datastore, you can remove the virtual machine from vCenter Server and delete all virtual machine files from the datastore, including the configuration file and virtual disk files.

Log in to the vSphere Client and perform the task:

Option	***Description***
Temporarily remove the virtual machine or VM template	1. Right-click the virtual machine 2. Select **Remove From Inventory** and click **Yes**
Permanently delete the virtual machine or VM template	1. Right-click the virtual machine 2. Select **Delete from Disk** and click **Yes**

3.2.7 Register a VM or VM Template with vCenter Server

If you removed a VM or VM template from vCenter Server but did not delete it from disk, you can return it to the vCenter Server inventory by registering it with the vCenter Server.

1. In the vSphere Client inventory, right-click the datastore on which the virtual machine configuration file is stored and select **Register VM**.

2. Browse to, and select the virtual machine configuration (.vmx) file or the VM template configuration file (.vmtx) and click **OK**.
    a. The **Register Virtual Machines** wizard opens.

3. On the Select a name and folder page, use the existing name, or type a new name then select a datacenter or folder location and click **Next**.

4. Select a host or cluster on which to run a new virtual machine.

Option	*Action*
Run the virtual machine on a standalone host	Select the host and click **Next**.
Run the virtual machine in a cluster with DRS automatic placement	Select the cluster and click **Next**.
Run the virtual machine in a cluster without DRS automatic placement	1. Select the cluster and click **Next**. 2. Select a host within the cluster and click **Next**.

5. Select a resource pool in which to run the virtual machine and click **Next**.

6. On the Ready to complete page, review your selections and click **Finish**.

3.2.8 Change VM Template name

If you move a template to another host or datacenter folder, you can change the template name to make it unique in that folder.

1. Right-click the template and select Rename.
2. Enter a new name and click OK.

3.2.9 Deleting Templates

You can delete a template by removing it from the inventory or deleting the template from the disk. If you remove the template from the inventory, it remains on the disk and can be reregistered with vCenter Server to restore it to the inventory.

3.2.9.1 Remove Templates from Inventory

If a template has become outdated and you no longer use it in your environment, you can remove it from the inventory. Removing a template unregisters it from the vCenter Server inventory, but it is not removed from the datastore. The template remains at the same storage location, and you can use the datastore browser to re-register the template at a later time. You can later decide to update the template rather than create one.

1. Click the template and select **Remove from Inventory**.
2. Click **Yes** to confirm removing the template from the vCenter Server database.

3.2.9.2 Delete a Template from the Disk

If you no longer need a template or need to free up disk space, you can remove it from the disk. Templates that you delete are permanently removed from the system.

Important: You cannot recover a template that you delete from the disk.

1. Right-click the template and select **Delete from Disk**.
2. Click **Yes** to confirm removing the template from the datastore.

3.2.9.3 Reregister Templates

Templates can become unregistered from vCenter Server if they are removed from the inventory or if the hosts with which they are associated are removed from vCenter Server and then readded.

1. In the vSphere Client, navigate to the datastore that contains the template.
2. Select the datastore and click the **Files** tab.
3. Locate the template folder and click it to display the template files.
4. Select the .vmtx file and click the **Register VM** icon.
    a. The **Register VM Template** wizard opens.
5. On the Select a name and folder page, specify a name and location for the template and click **Next**.
6. On the Select a compute resource page, select a host or cluster on which to store the template and click **Next**.
7. On the Ready to complete page, review your selections and click **Finish**.

Inventory Object	*Steps*
Host	Browse to the host. On the **VMs** tab, click **VM Templates**.
Cluster	On the **VMs** tab, click **VM Templates**.

8. The template is registered to the host. You can view the template by clicking on the host's **VM Templates**.

3.2.10 Managing VMs with Snapshots

Snapshots preserve the state and data of a virtual machine at the time you take the snapshot. When you take a snapshot of a virtual machine, an image of the virtual machine in a given state is copied and stored. Snapshots are useful when you want to revert repeatedly to a virtual machine state, but you do not want to create multiple virtual machines.

You can take multiple snapshots of a virtual machine to create restoration positions in a linear process. With multiple snapshots, you can save many positions to accommodate many kinds of work processes. Snapshots operate on individual virtual machines. Taking snapshots of multiple virtual machines, for example, taking a snapshot of a VM for each member of a team, requires that you take a separate snapshot of each team member's virtual machine.

Snapshots are useful as a short term solution for testing software with unknown or potentially harmful effects. For example, you can use a snapshot as a restoration point during a linear or iterative process, such as installing update packages, or during a branching process, such as installing different versions of a program. Using snapshots ensures that each installation begins from an identical baseline.

With snapshots, you can preserve a baseline before you change a virtual machine.

Several operations for creating and managing virtual machine snapshots and snapshot trees are available in the vSphere Client. These operations enable you to create snapshots, revert any snapshot in the snapshot hierarchy, delete snapshots, and more. You can create snapshot trees where you save the virtual machine state at any specific time so that you can revert that virtual machine state later. Each branch in a snapshot tree can have up to 32 snapshots.

A snapshot preserves the following information:

- Virtual machine settings. The virtual machine directory, which includes the disks added or changed after you take the snapshot.
- Power state. The virtual machine can be powered on, powered off, or suspended.
- Disk state. State of all the virtual machine's virtual disks.
- (Optional) Memory state. The contents of the virtual machine's memory.
  Virtual Machines with Snapshots

3.3 Appendices

3.3.1 Common CLI commands

Command	Use
`ssh [ip or hostname].`	Secure shell, an encrypted network protocol allowing for remote login and command execution
`sudo [command]`	Run a command with root permissions
`sudo -s`	Switch to root user mode
`pwd`	Print working directory
`whoami`	Displays the logged in user id
`cd /cd [target]`	Change the directory to "target" directory
`cd /opt/ddt/ansible_main`	Change the directory to the root of the filesystem
`ls`	View list of files in directory
`clear`	Clears the terminal screen
`cat [filename]`	Displays the contents of filename to standard out
`cp [source_file] [target file]`	Creates a copy of the source file
`mkdir /path/to/[directory name]`	Create a specific directory
`rm [target file]`	Removes a specific file
`mv [source_file] [target_file]`	Moves a specific file
`ip a`	View all Internet Protocol (IP) information
`ifup [nic]; ifdown [nic]`	Bring a Network Interface Card (NIC) up / down
`find . -name [file / directory]`	Find file or directory by name
`systemctl start name.service`	Start a system service
`systemctl stop name.service`	Stop a system service
`systemctl enable name.service`	Enable a system service to start upon system startup
`systemctl disable name.service`	Disable a system service from starting upon system startup

3.3.2 Miscellaneous Admin Tasks

3.3.2.1 Enabling USB

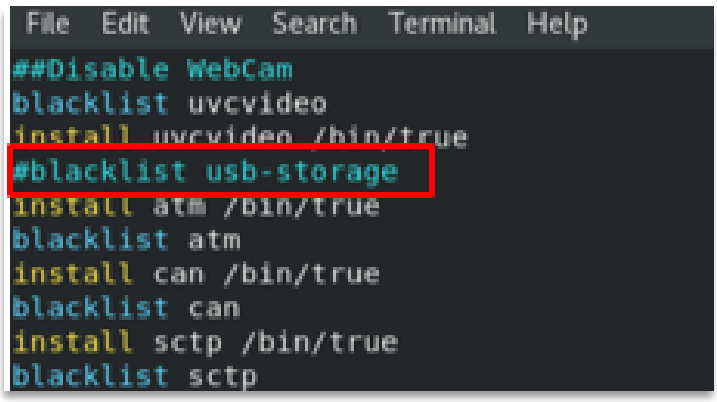
If you are having issues getting a USB device recognized, it may be necessary to edit two configuration files and remove the USB blacklist.

To do so:

1. Navigate to **/etc/modprobe.d**.

```
$ cd /etc/modprobe.d
```

2. Using vim, comment out the usb-storage line in blacklist.conf



3. Comment out install usb-storage /bin/true in **/etc/modprobe.d/usb-storage.conf**.