DDS-M Manuals

For

Defensive Cyber Operations

Prepared for:
Department of the Army
Program Executive Office (PEO)
Enterprise Information Systems
9350 Hall Road, Bldg. 1445
Fort Belvoir, VA 22060

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

May 2023 **Revision 19**

Version History

Date	Description	Revision
October 2019	- Initial Release	R00
January 2020	- Project CURE Updates	R01
May 2020	- Merged CURE Installation, CURE Administration manuals	R02
September 2020	- Addition of Table of Contents - Significant revision to wire diagram layout and visual quality to match updated PLACT deployment instructions. - Removal of Thunderbolt adapter as primary connectivity for Deployment Laptop. - Addition of significant operator instructions in Section 2. - Revision of startup, shutdown, and kit redeployment procedures in Section 4. - Additional procedures added to appendix.	R03
November 2020	- CURE was renamed to DDT	R04
February 2021	- Replace screenshots with updated GUIs from Satellite, IdM, and play.py - Update Table of Contents to include hyperlinks.	R05
July 2021	- User Manual, Software Manual, and Troubleshooting Manual combined to one manual and broken into 3 sections. - Formatting overhaul, update to images, section headers, and many others. - Software sections updated to RHEL 8. - Section added on how to use Minicom.	R06
November 2021	- Centered and captioned all images. - Clarified code blocks. - Clarified text in Software and Troubleshooting guides.	R07
February 2022	- Updated play.py, Satellite, IdM, Engine, and Palo Alto images for DDT 1.5.3 release. - Clarified System Power Up and Shutdown Sequence (Section 4.4.1 & 4.4.2). - Revised Dell S4112 Factory Reset Procedures (Section 4.7.2). - Revised BIOS Optimized Configuration (Section 21.2). - Changed paths from /opt/cure/ to /opt/ddt/ in Version 1.5.3.	R08
March 2022	- Updated play.py images for DDT 1.6.0 release. - Clarified system power requirements (Section 2 & 4.1). - Added COPE and Short Circuit guides (Section 5).	R09

Version History (Continued)

Date	Description	Revision
April 2022	- Updated play.py images for DDT 1.6.1 release. - Added Host-based Error Retrieval Platform (HERP) instructions (Section 4.6.5). - Updated Palo Alto images (Section 10.1). - Updated Illustrated Reference / DDS-M Layout (Section 5.1). - Updated BIOS Optimized Configuration (Section 21.2).	R10
May 2022	- Updated Inventories to reflect multiple kit versions (Section 4.2.1 and 4.2.2). - Updated Minicom instructions to include cisco, dell0, and dell1 profiles (Section 11.1.4)	R11
June 2022	- Updated inventory references in all Section 2 diagrams. - Removed all references to the obsolete 'shared_storage' gluster volume. - Updated play.py images for DDT v1.6.3 release.	R12
July 2022	- Updated play.py, Satellite, Engine, and Palo Alto images for DDT 1.7.0 release. - Clarified cabling instructions in all Section 2 scenarios. - Revised 'virsh' syntax for readability in Section 4.	R13
August 2022	- Updated Satellite images in sections 4.6.1, 8.2.2, and 8.2.3 for DDT v1.8.0 release.	R14
September 2022	- Updated Identity Management, Satellite, Engine, and Palo Alto procedures for DDT 1.8.1 release. - Updated DDS-M Transit Case Overview (Section 1.2) - Included steps for manual HERP diagnostic procedures. (Section 4.6.4) - Referenced updated minicom profiles. (Section 5.4.9) - Updated Red Hat Identity Management images and clarified instruction. (Section 8.1.3) - Updated Red Hat Satellite common administration task readability. (Section 8.2.4) - Updated syntax for Red Hat Virtualization domains; removed SR-IOV instructions. (Section 9.1.4) - Clarified VNC console instructions. (Section 9.1.5) - Updated Palo Alto administration syntax. (Section 10.2.8) - Updated network naming references. (Section 11.1.1)	R15
December 2022	- Added instructions for managing repos via Satellite. (Section 5.4.12) - Added instructions for FML build process. (Section 5.4.13) - Updated Bios Optimized configurations. (Section 21.2) - Updated Ft. Gordon Armory email info (Foreword sections)	R16

Version History (Continued)

Date	Description	Revision
February 2023	- Updated instructions for configuring time protocol. (Section 5.4.6) - Clarified note verbiage in Gluster Volume Information. (Section 9.2.3)	R17
April 2023	- Integrated DOPE manual at the end of this document. - Updated logos and formatting due to change in responsibility of document maintenance. - Corrected information regarding cabling when provisioning nodes with RHVH. (Section 4.6.4) - Added note indicating that certain steps should only be done by armory personnel. (Section 13.8)	R18
May 2023	- Updated Dell S4112 series switch configuration info and screenshots. (Section 11.1.5)	R19

Table of Contents

DDS-M Kit
Operator's User Manual

May 2023 Revision 19

Foreword

Introduction

The Deployable Defensive Cyber Operations (DCO) System - Modular (DDS-M) 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-M kit consists of 1 backpack and 3 protective cases containing 8 servers, 3 switches, a network tap, 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

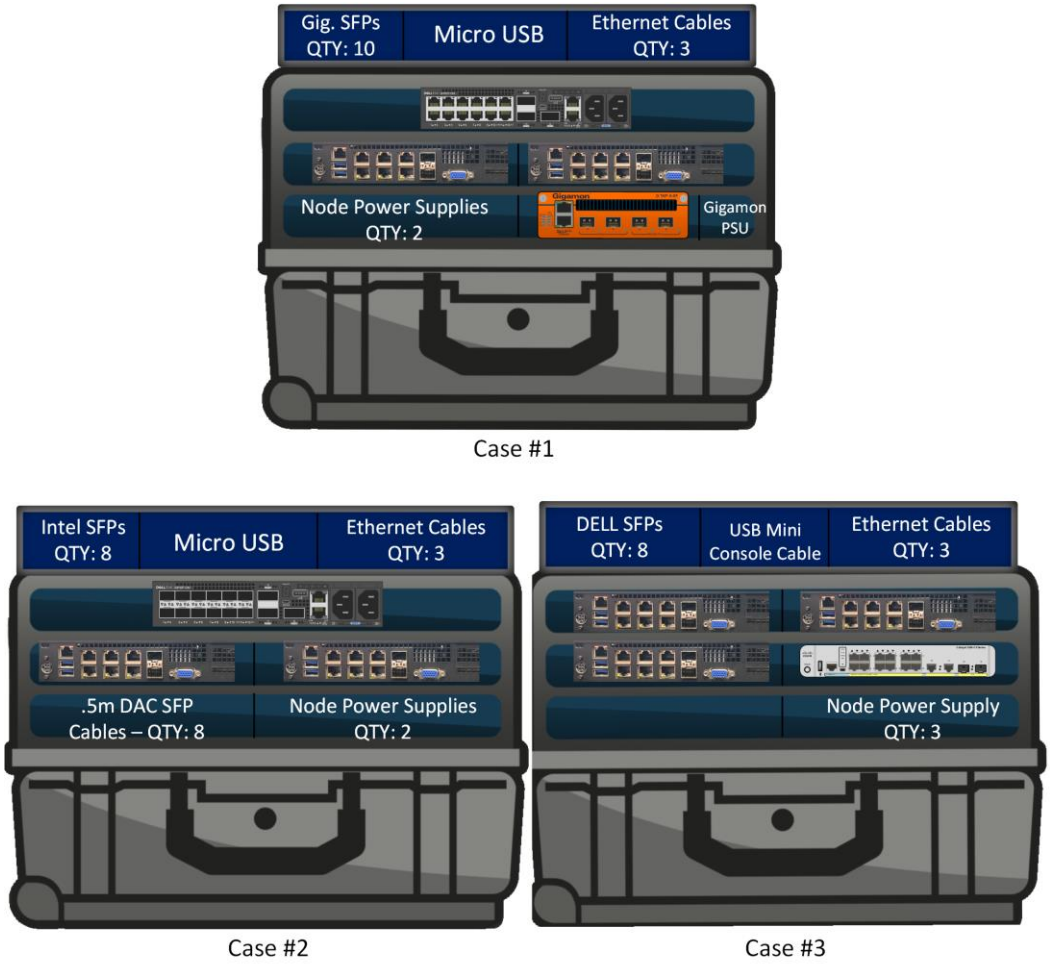
- Become familiar with the documentation safety sections.
- **Do not** make any unauthorized alterations to the equipment.
- **Do not** reconfigure while the set is powered up.
- **Do not** power off the kit without following the startup/shutdown procedures.
- **Do not** pull cables by the cord.
- **Do** determine the appropriate power requirements for the operating location and use a power strip that is rated for that environment (See **Section 4.1** for more information).
- Installers should prepare a cable plan for routing all cables over a common path away from high-traffic areas.

1 System Overview

1.1 Functional Description

DDS-M 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 1-8 servers, and its portability allows teams to maintain positive control of the system while traveling.

1.2 Transit Case Overview



1.2-DDS-M Cases

2 Cabling Diagrams

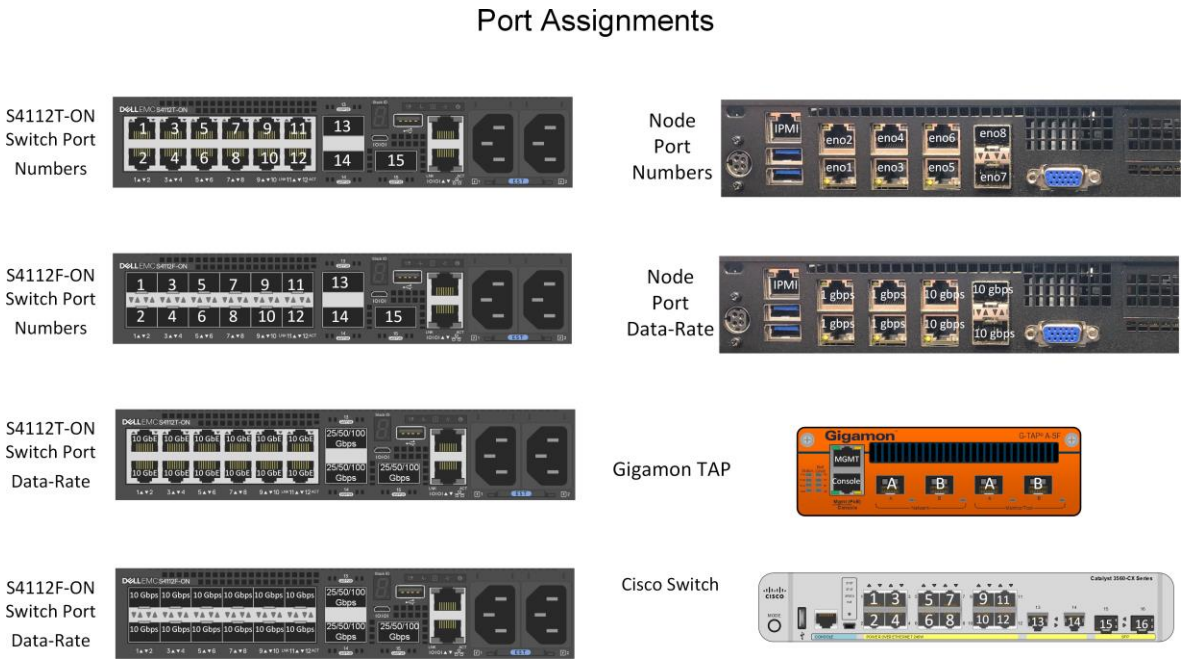
The cabling diagrams are shown in relation to the following deployment use cases:

2.1 : Port Assignments
2.2 : 6 RHEV Servers and 2 Bare-Metal Servers
2.3 : 3 RHEV Servers and 5 Bare-Metal Servers
2.4 : 3 RHEV Servers and 1-5 Bare-Metal Servers
2.5 : 8 Bare-Metal Servers
2.6 : Switchports and Logical Diagram Network Flow

Ensure to follow all cabling recommendations across all appropriate examples.

✎ **Note:** Each numbered section is represented by multiple diagrams explaining required interfaces. Connections to the nodes (servers) should be associated as shown. The nodes may be situationally connected to the switches either through ethernet or Direct Attach Cables.

2.1 Port Assignments

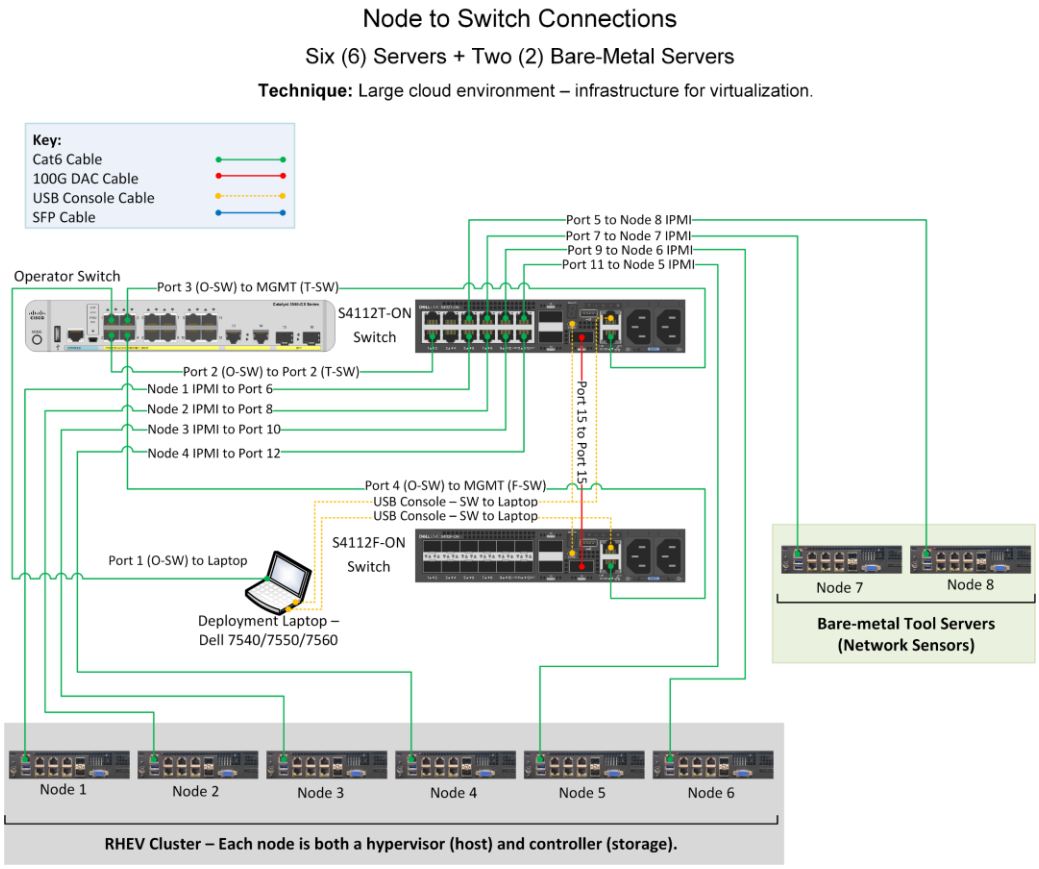


2.1 Port Assignments

2.2 6 RHEV Servers + 2 Bare-Metal Servers

Technique: This configuration is suitable for Large Hyper-converged cloud virtualization environments and provides a long-term data storage platform.

2.2.1 Switch to IPMI Connections:



2.2.1 Switch to IPMI Connections

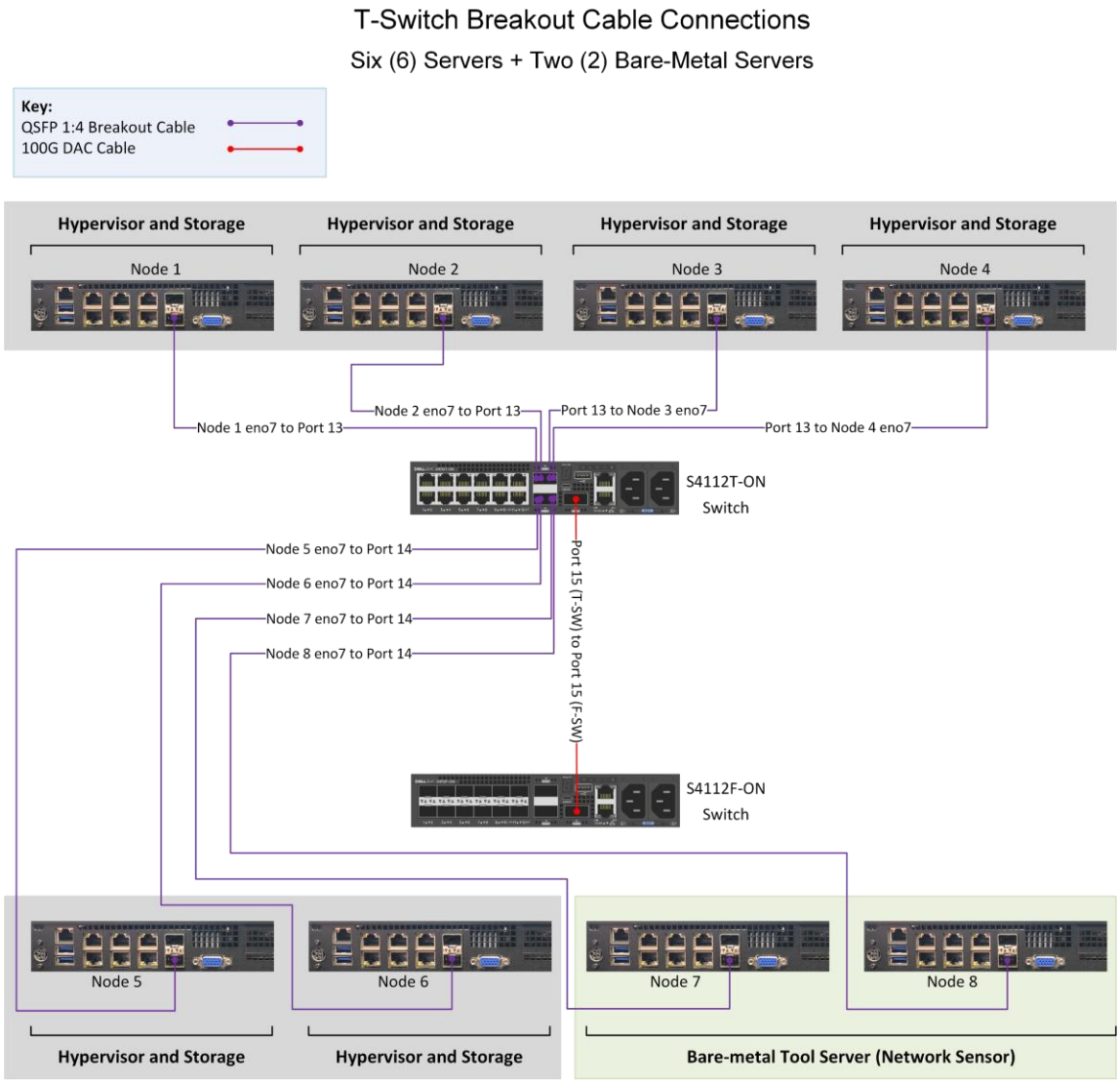
Situation: Required

Instructions:

1. Connect the **Deployment Laptop** to the Operator switch by using a CAT6e cable.
2. Connect the **Operator Switch** to **Port 2** on **the Dell S4112T Switch** by using a CAT6e cable.
3. Connect required nodes at the interface designated as **IP Management Interface (IPMI)** (VLAN 53) to **Ports 5-12** on the **S4112T** switch.
4. Proceed to **Task 2.2.2** to complete cabling procedures.

✎ **Warning**: For Node Redeployment purposes, connect only the specific **(6) SIX** nodes for discovery and provisioning. RHVH nodes receive a DHCP issued IP address and remain accessible by web console at **`https://10.[kit number].53.[200-205]`**.

2.2.2 Dell 4112T Switch Breakout Cable Connections:



2.2.2 Dell 4112T Switch Breakout Cable Connections

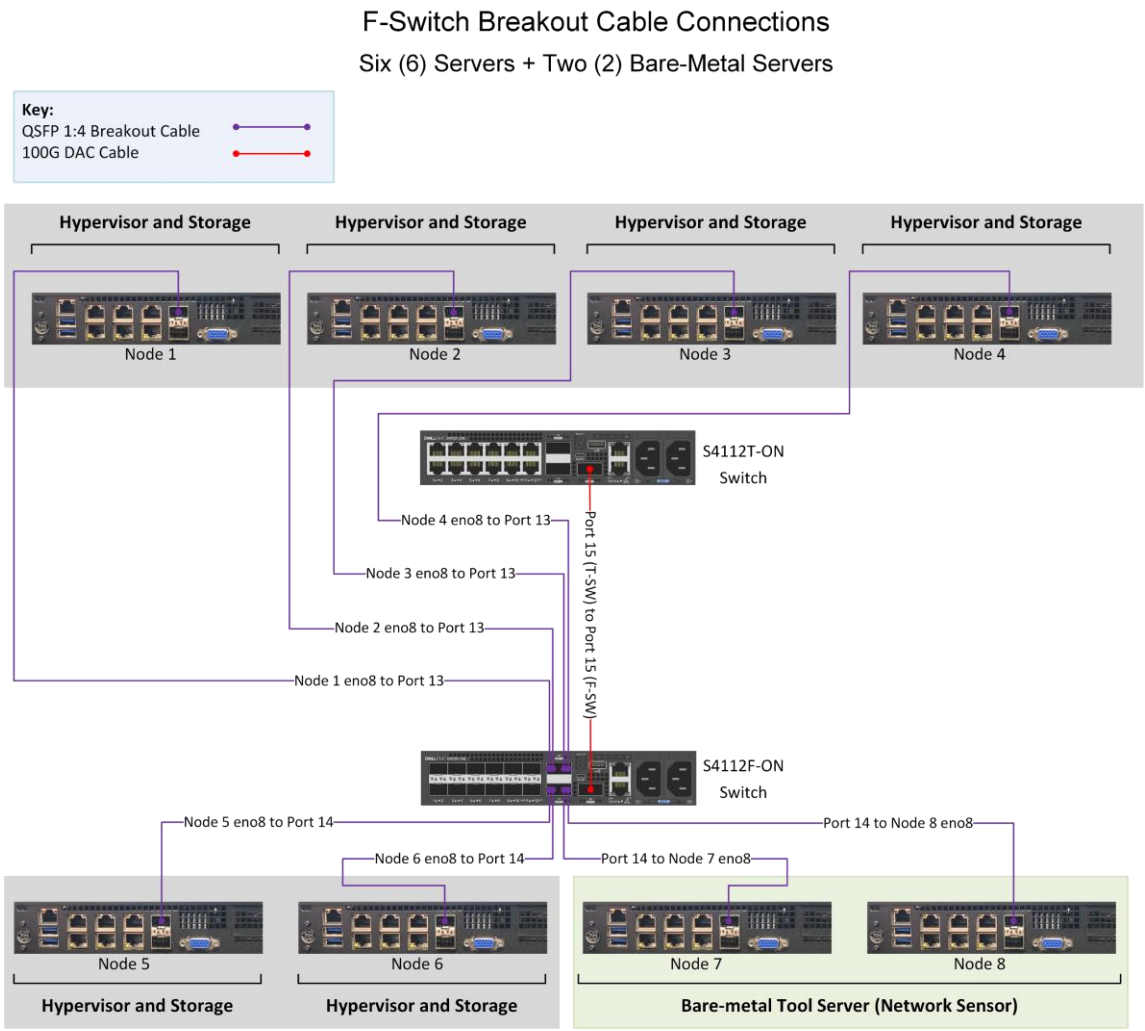
Situation: Required

Instructions:

1. Connect required nodes at the interface designated **eno7** (`VLAN 51` and `oVIRT Networks`) to the **QSFP 1-to-4 Breakout** cable seated in **Port 13** or **Port 14** on the **S411T** switch.
2. Proceed to **Task 2.2.3** to complete cabling procedures.

✎ **Note**: After deployment, RHVH nodes will use this interface for management and will be issued a static IP address of **`10.[kit number].51.[20-25].`** Bare-metal nodes on this network receive a DHCP assigned address of **`10.[kit number].51.[200-250].`**

2.2.3 Dell 4112F Switch Breakout Cable Connections:



2.2.3 Dell 4112F Switch Breakout Cable Connections

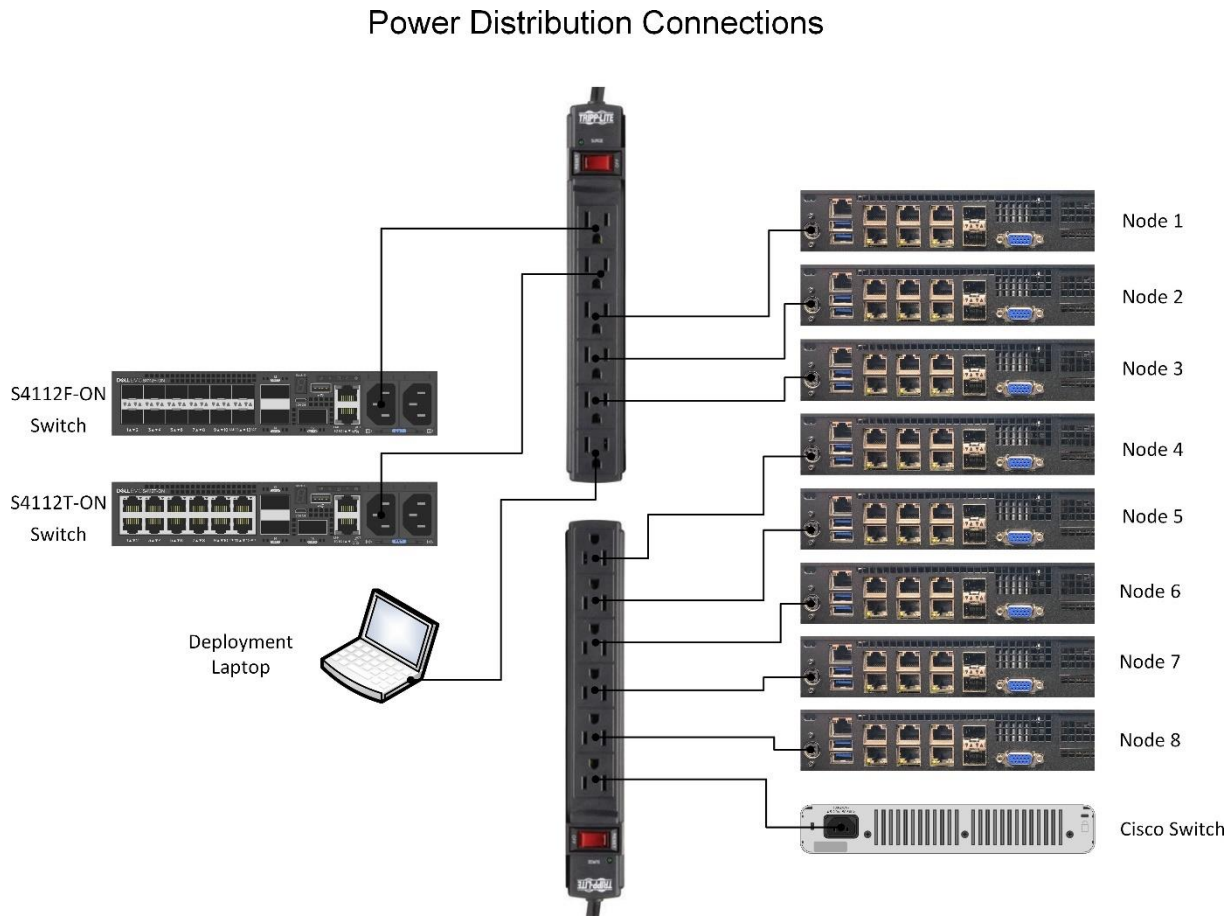
Situation: Required

Instructions:

1. Connect required nodes at the interface designated **eno8** (VLAN 52) to the **QSFP 1-to-4 Breakout** cable seated in **Port 13** or **Port 14** on the **S4112F** switch.
2. Proceed to **Task 2.2.4** to complete cabling procedures.

✎ **Note**: After deployment, RHVH nodes will use this interface for GlusterFS Storage synchronization and will be issued a static IP address of **`10.[kit number].52.[20-25].`** Bare-metal nodes on this network receive a DHCP assigned address of **`10.[kit number].52.[200-250].`**

2.2.4 Power Distribution Connections:



2.2.4 Power Distribution Connections

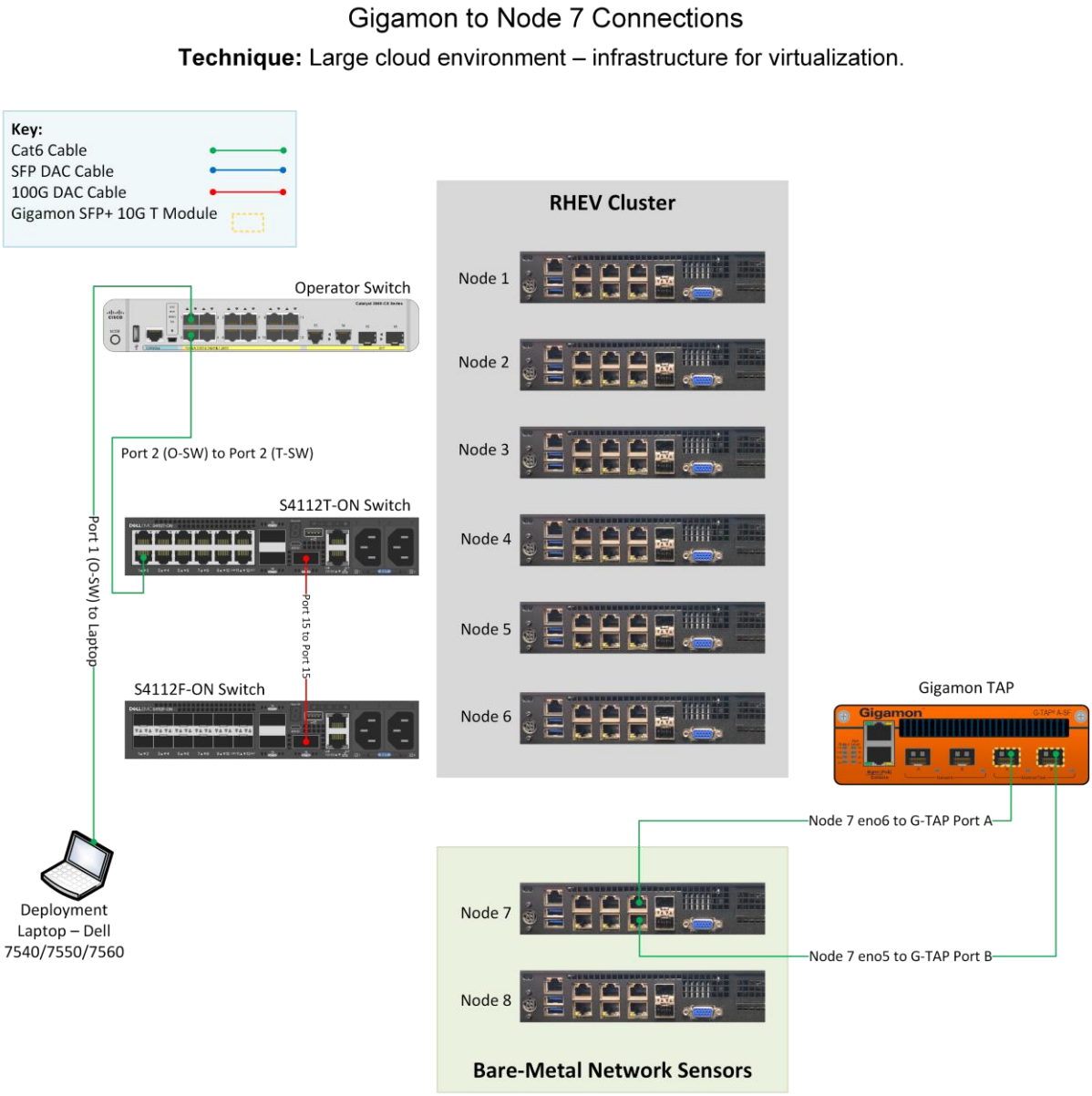
Situation: Required

Instructions:

1. Ensure the power strip is **NOT** energized while connecting equipment.
2. Plug in any required nodes, switches, and devices and then apply power by activating the rocker switch located on each power strip.
3. Proceed to **Task 2.2.5** to complete cabling procedures.

✎ **Note**: The power strips included with the DDS-M Kit are rated for **`120V, 60 Hz`** operation in the United States. Use an appropriate power strip for locations where voltage and frequency are different.

2.2.5 Gigamon to Bare-Metal Node Connections:



2.2.5 Gigamon to Bare-Metal Node Connections

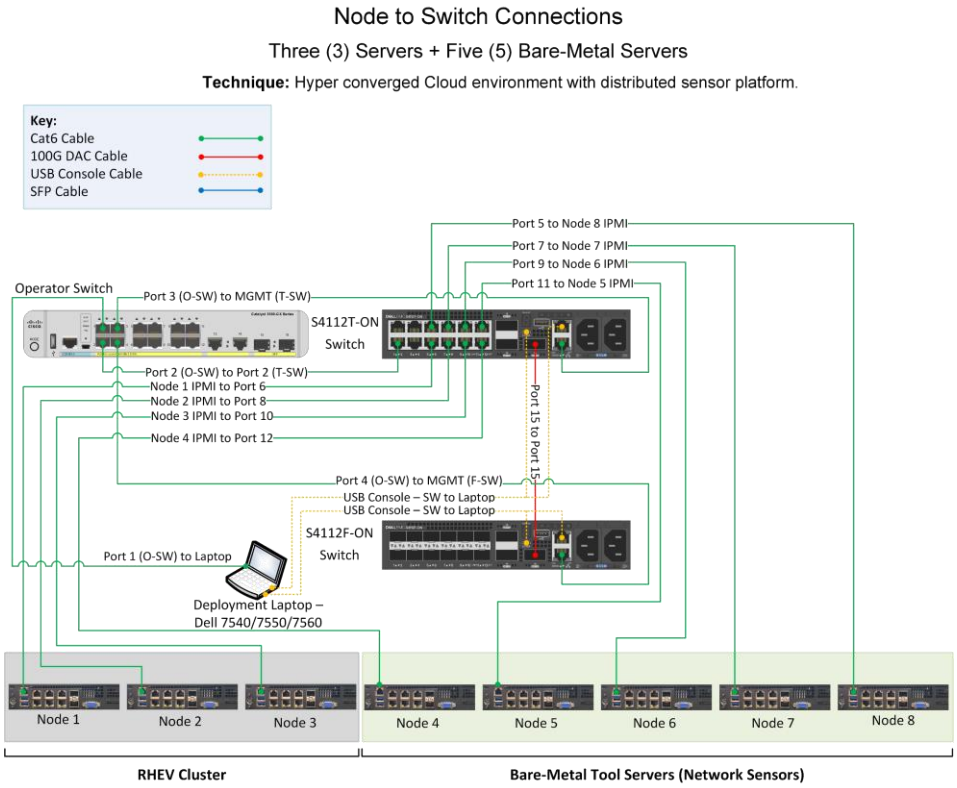
Situation: Optional

Instructions: Connect a sensor to the Gigamon G-TAP as specified in the diagram above.

2.3 3 RHEV Servers + 5 Bare-Metal Servers

Technique: This configuration provides both a Hyper-converged medium density cloud environment and distributed bare-metal sensor platforms.

2.3.1 Switch to IPMI Connections:



2.3.1. Switch to IPMI Connections

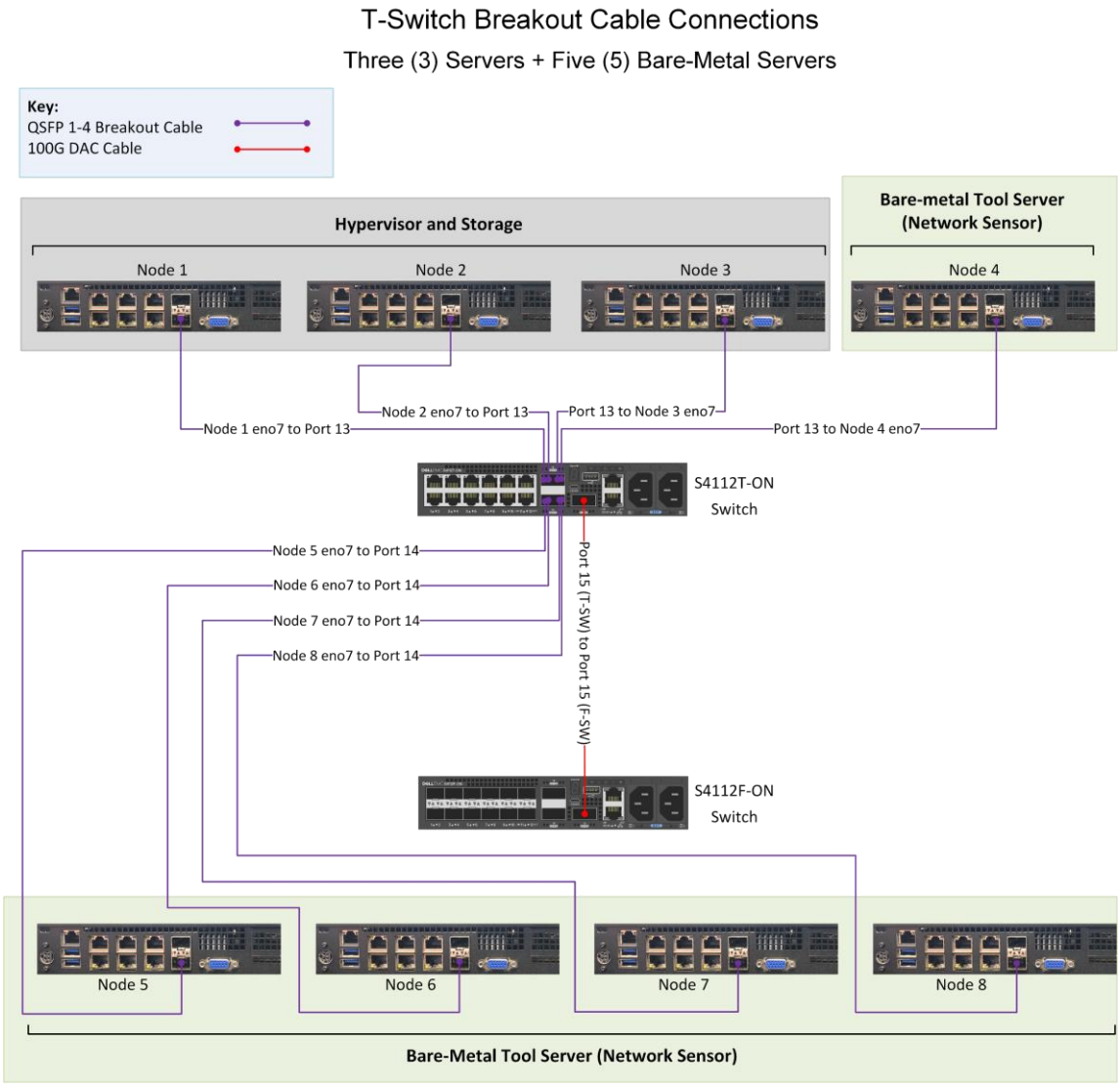
Situation: Required

Instructions:

1. Connect the **Deployment Laptop** to the Operator switch by using a CAT6e cable.
2. Connect the **Operator Switch** to **Port 2** on **the Dell S4112T Switch** by using a CAT6e cable.
3. Connect required nodes at the interface designated as **IP Management Interface (IPMI)** (VLAN 53) to **Ports 5-12** on the **S4112T** switch.
4. Proceed to **Task 2.3.2** to complete cabling procedures.

✎ **Warning**: For Node Redeployment purposes, connect only the specific **(3) THREE** nodes for discovery and provisioning. RHVH nodes receive a DHCP issued IP address and remain accessible by web console at **`https://10.[kit number].53.[200-202]`**.

2.3.2 Dell 4112T Switch Breakout Cable Connections:



2.3.2 Dell 4112T Switch Breakout Cable Connections

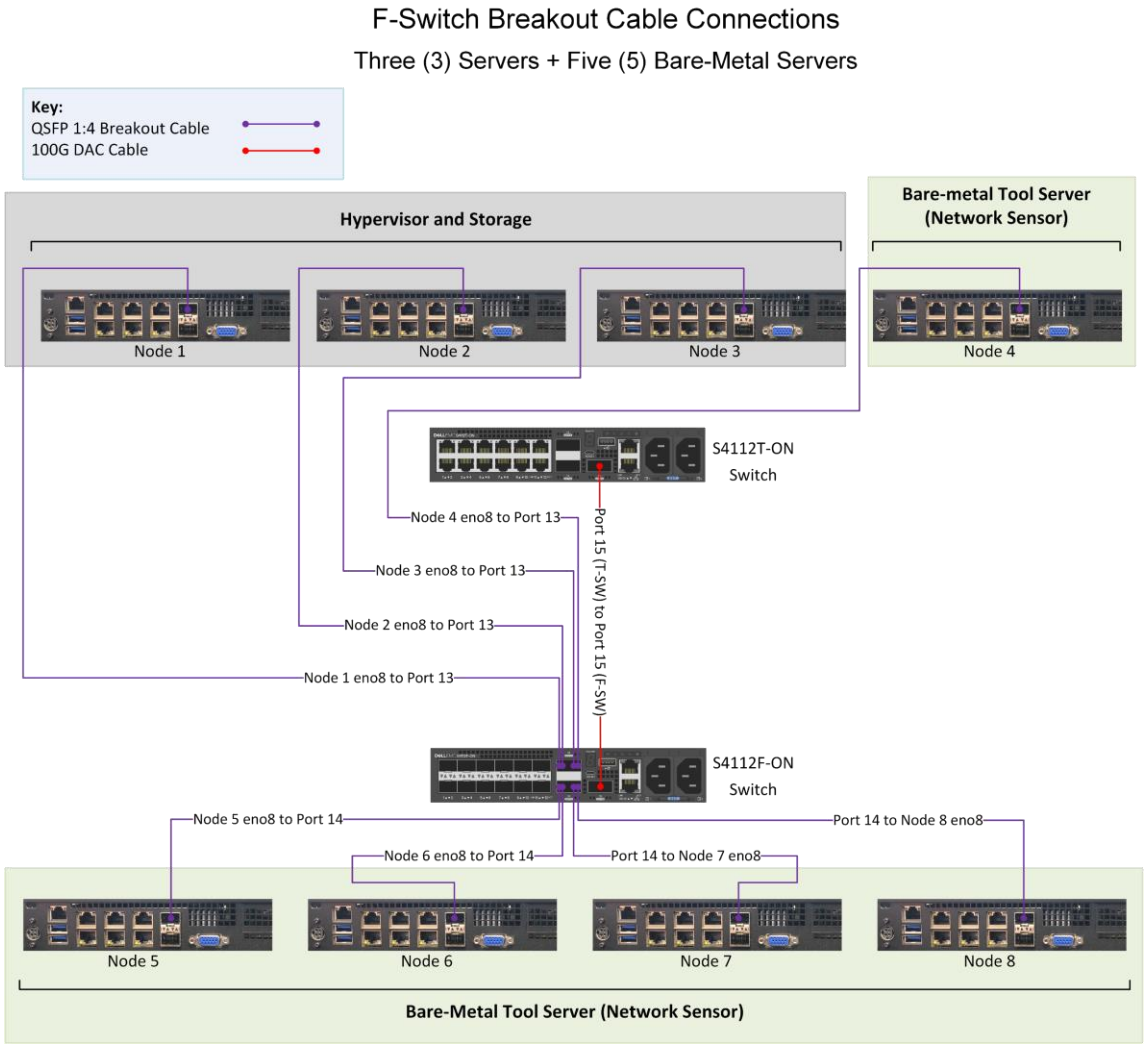
Situation: Required

Instructions:

1. Connect required nodes at the interface designated **eno7** (`VLAN 51` and `oVIRT Networks`) to the **QSFP 1-to-4 Breakout** cable seated in **Port 13** or **Port 14** on the **S411T** switch.
2. Proceed to **Task 2.3.3** to complete cabling procedures.

✎ **Note**: After deployment, RHVH nodes will use this interface for management and will be issued a static IP address of **`10.[kit number].51.[20-22].`** Bare-metal nodes on this network receive a DHCP assigned address of **`10.[kit number].51.[200-250].`**

2.3.3 Dell 4112F Switch Breakout Cable Connections:



2.3.3 Dell 4112F Switch Breakout Cable Connections

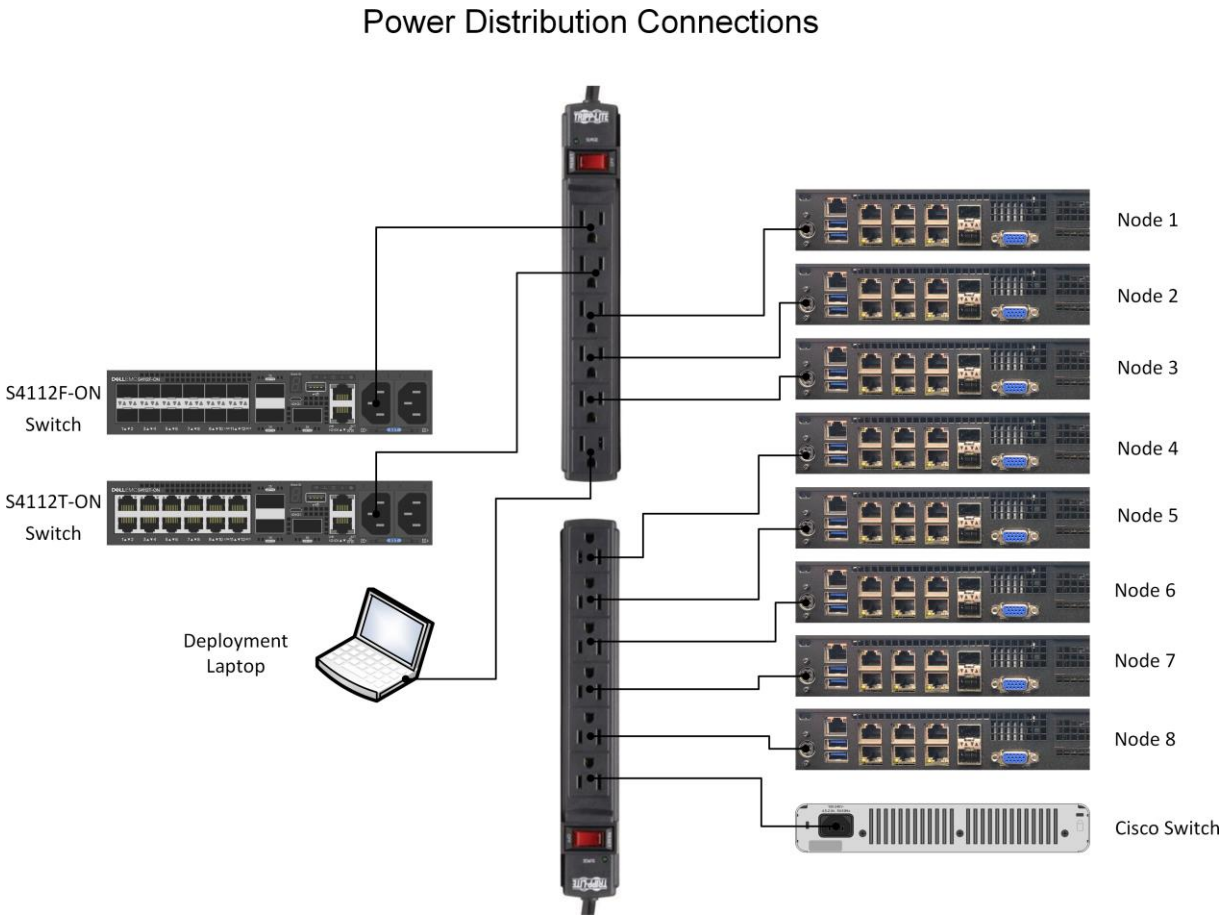
Situation: Required

Instructions:

1. Connect required nodes at the interface designated **eno8** (VLAN 52) to the **QSFP 1-to-4 Breakout** cable seated in **Port 13** or **Port 14** on the **S4112F** switch.
2. Proceed to **Task 2.3.4** to complete cabling procedures.

✎ **Note**: After deployment, RHVH nodes will use this interface for GlusterFS Storage synchronization and will be issued a static IP address of **`10.[kit number].52.[20-22].`** Bare-metal nodes on this network receive a DHCP assigned address of **`10.[kit number].52.[200-250].`**

2.3.4 Power Distribution Connections:



2.3.4 Power Distribution Connections

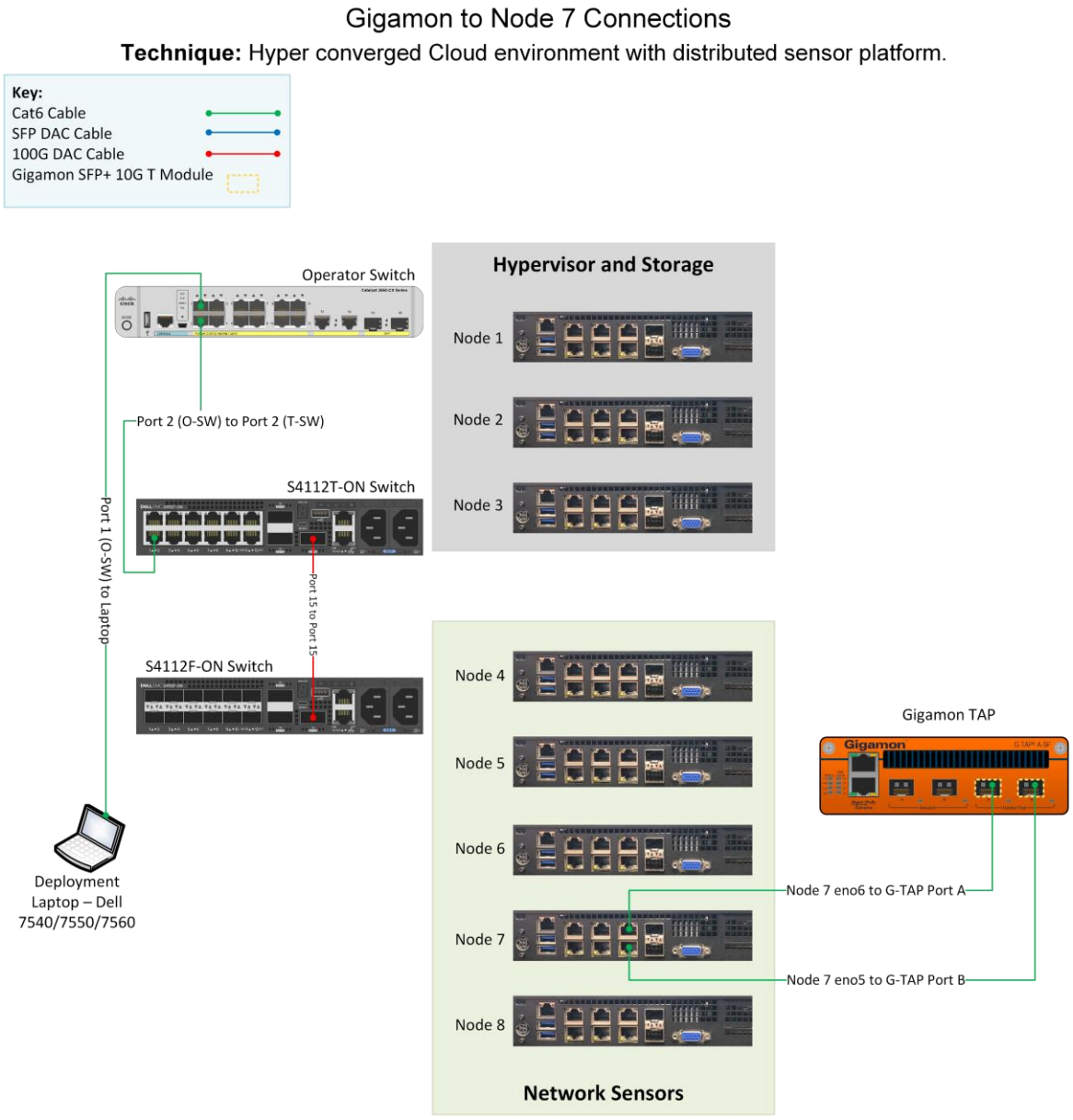
Situation: Required

Instructions:

1. Ensure the power strip is **NOT** energized while connecting equipment.
2. Plug in any required nodes, switches, and devices and then apply power by activating the rocker switch located on each power strip.
3. Proceed to **Task 2.3.5** to complete cabling procedures.

✎ **Note**: The power strips included with the DDS-M Kit are rated for **`120V, 60 Hz`** operation in the United States. Use an appropriate power strip for locations where voltage and frequency are different.

2.3.5 Gigamon to Bare-Metal Node Connections:



2.3.5 Gigamon to Bare-Metal Node Connections

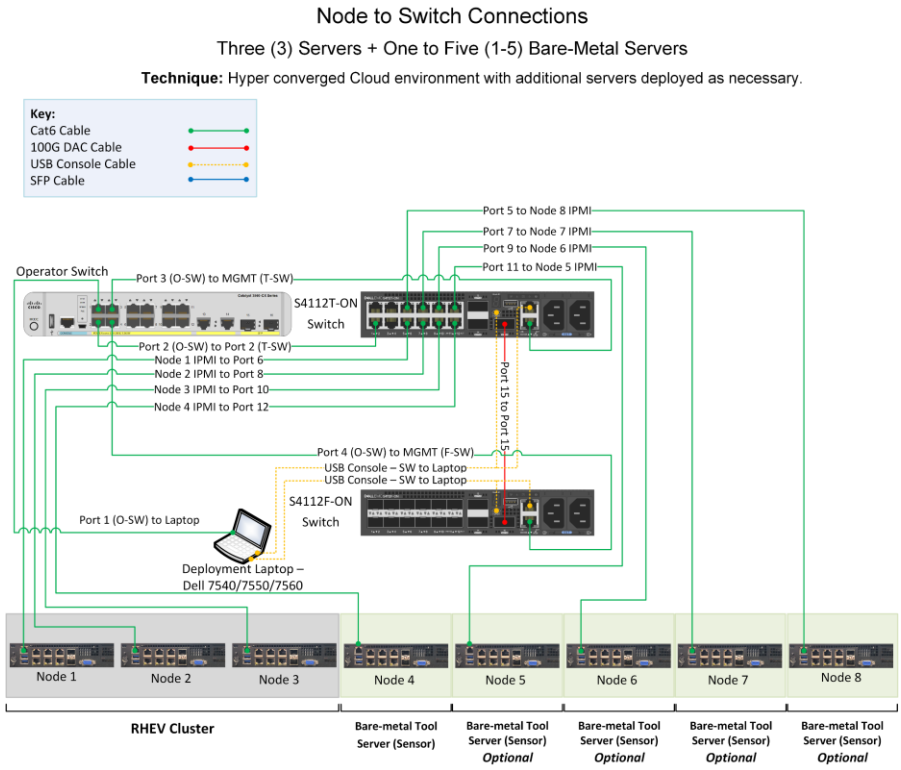
Situation: Optional

Instructions: Connect a sensor to the Gigamon G-TAP as specified in the diagram above.

2.4 3 RHEV Servers + 1-5 Bare-Metal Servers

Technique: This configuration is appropriate for small cloud environments and for low bandwidth networks.

2.4.1 Switch to IPMI Connections:



2.4.1 Switch to IPMI Connections

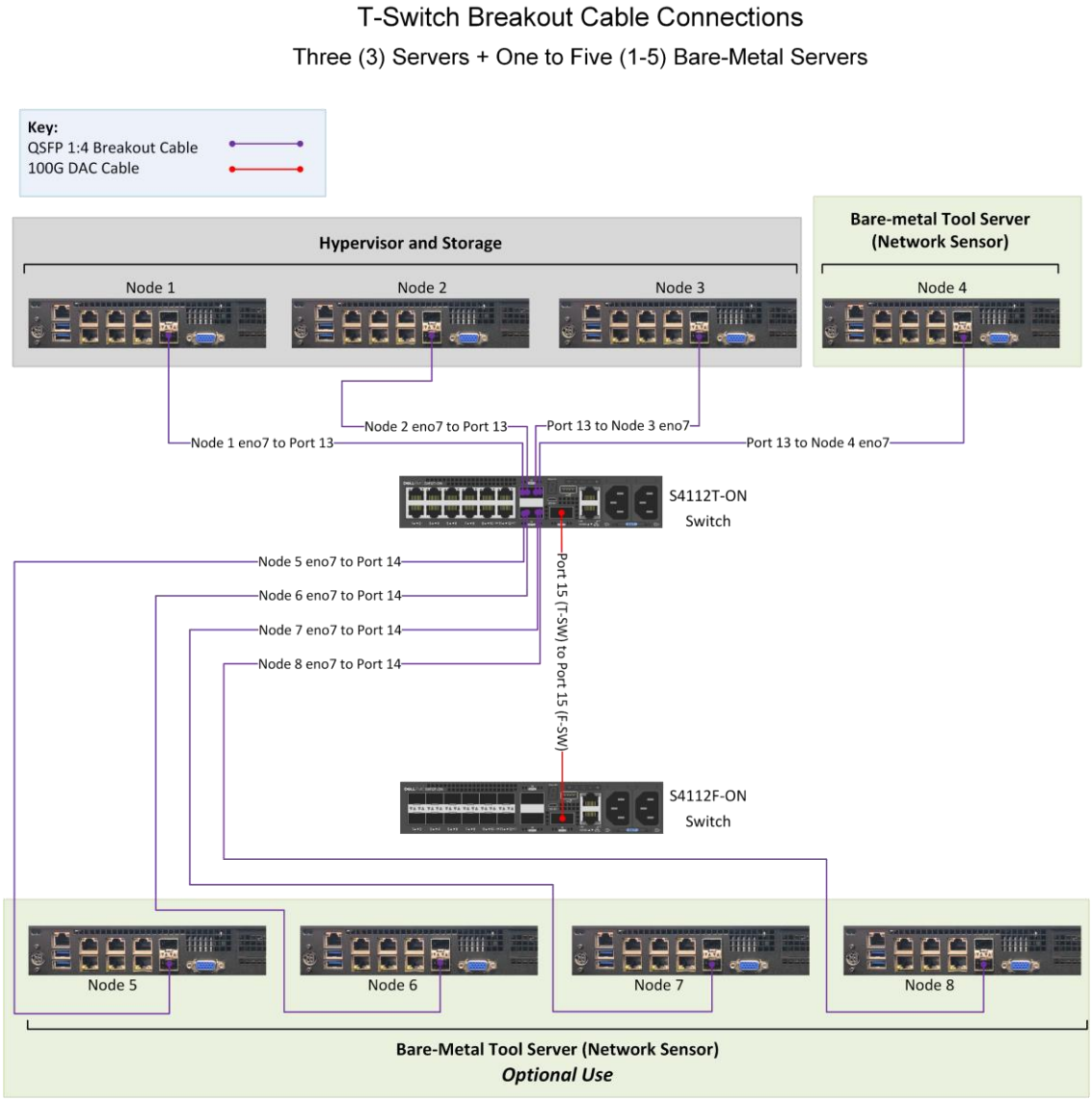
Situation: Required

Instructions:

1. Connect the **Deployment Laptop** to the Operator switch by using a CAT6e cable.
2. Connect the **Operator Switch** to **Port 2** on **the Dell S4112T Switch** by using a CAT6e cable.
3. Connect required nodes at the interface designated as **IP Management Interface (IPMI)** (`VLAN 53`) to **Ports 5-12** on the **S4112T** switch.
4. Proceed to **Task 2.4.2** to complete cabling procedures.

✎ **Warning**: For Node Redeployment purposes, connect only the specific **(3) THREE** nodes for discovery and provisioning. RHVH nodes receive a DHCP issued IP address and remain accessible by web console at **`https://10.[kit number].53.[200-202]`**.

2.4.2 Dell 4112T Switch Breakout Cable Connections:



2.4.2 Dell 4112T Switch Breakout Cable Connections

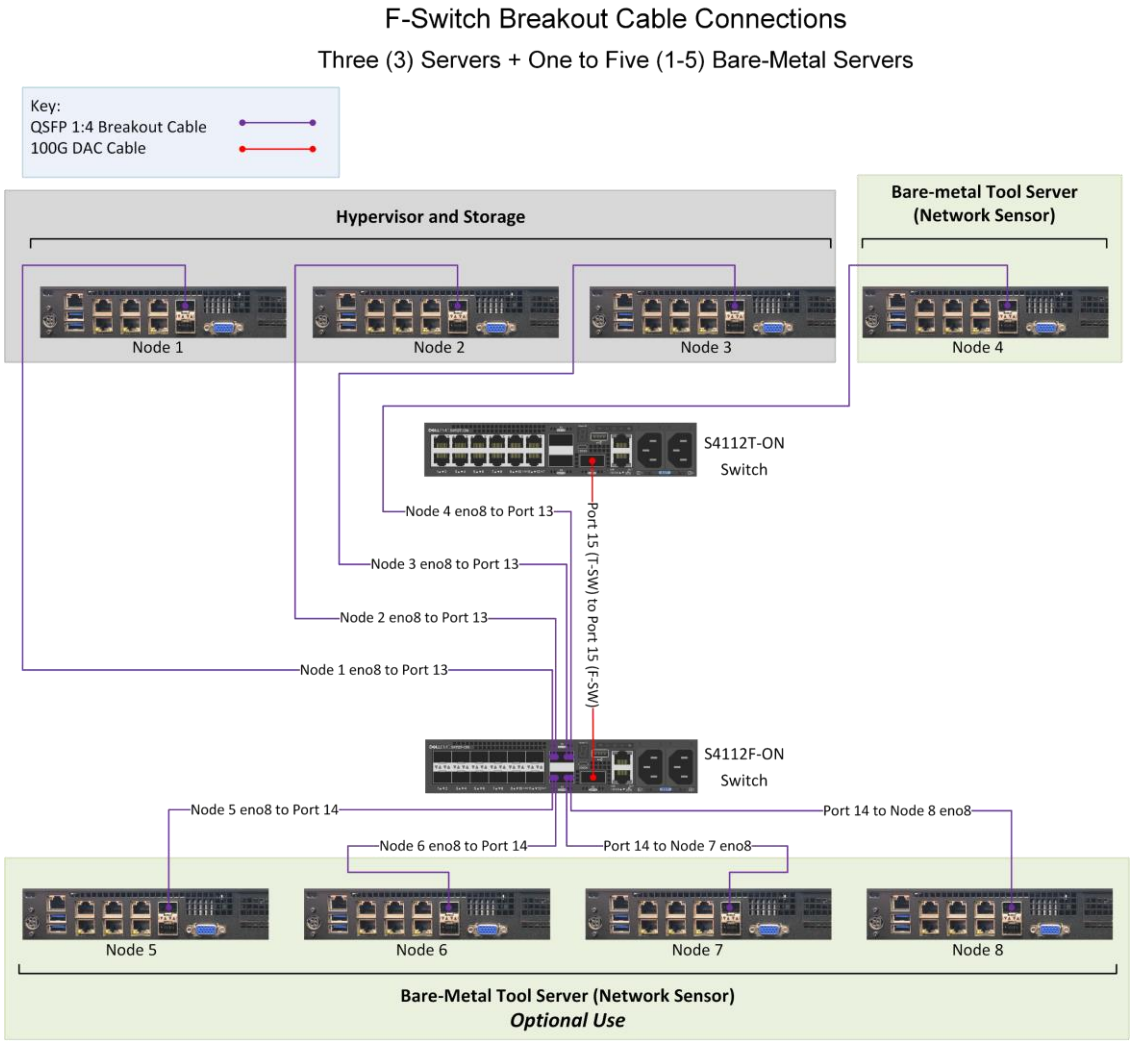
Situation: Required

Instructions:

1. Connect required nodes at the interface designated **eno7** (`VLAN 51` and `oVIRT Networks`) to the **QSFP 1-to-4 Breakout** cable seated in **Port 13** or **Port 14** on the **S411T** switch.
2. Proceed to **Task 2.4.3** to complete cabling procedures.

✎ **Note**: After deployment, RHVH nodes will use this interface for management and will be issued a static IP address of **`10.[kit number].51.[20-22].`** Bare-metal nodes on this network receive a DHCP assigned address of **`10.[kit number].51.[200-250].`**

2.4.3 Dell 4112F Switch Breakout Cable Connections:



2.3.3 Dell 4112F Switch Breakout Cable Connections

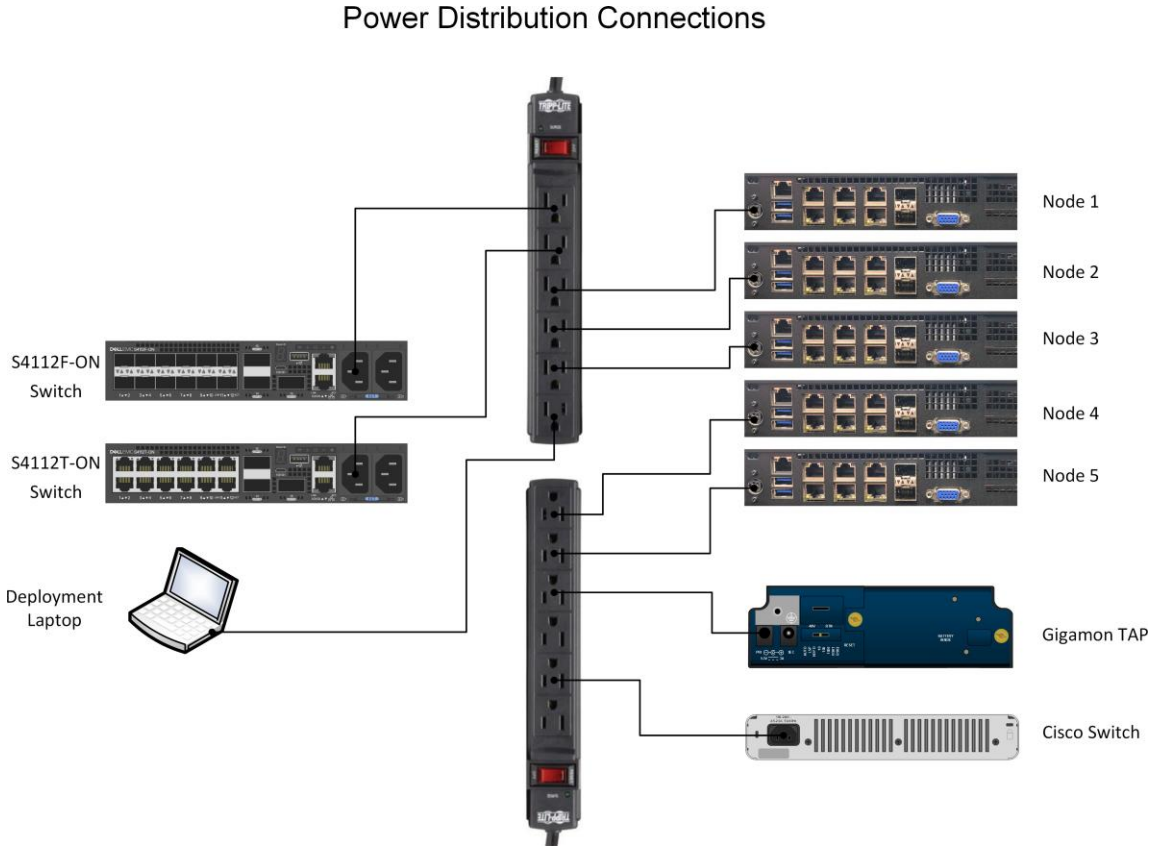
Situation: Required

Instructions:

1. Connect required nodes at the interface designated **eno8** (VLAN 52) to the **QSFP 1-to-4 Breakout** cable seated in **Port 13** or **Port 14** on the **S4112F** switch.
2. Proceed to **Task 2.4.4** to complete cabling procedures.

✎ **Note**: After deployment, RHVH nodes will use this interface for GlusterFS Storage synchronization and will be issued a static IP address of **`10.[kit number].52. [20-22].`** Bare-metal nodes on this network receive a DHCP assigned address of **`10.[kit number].52. [200-250].`**

2.4.4 Power Distribution Connections:



2.4.3 Power Distribution Connections

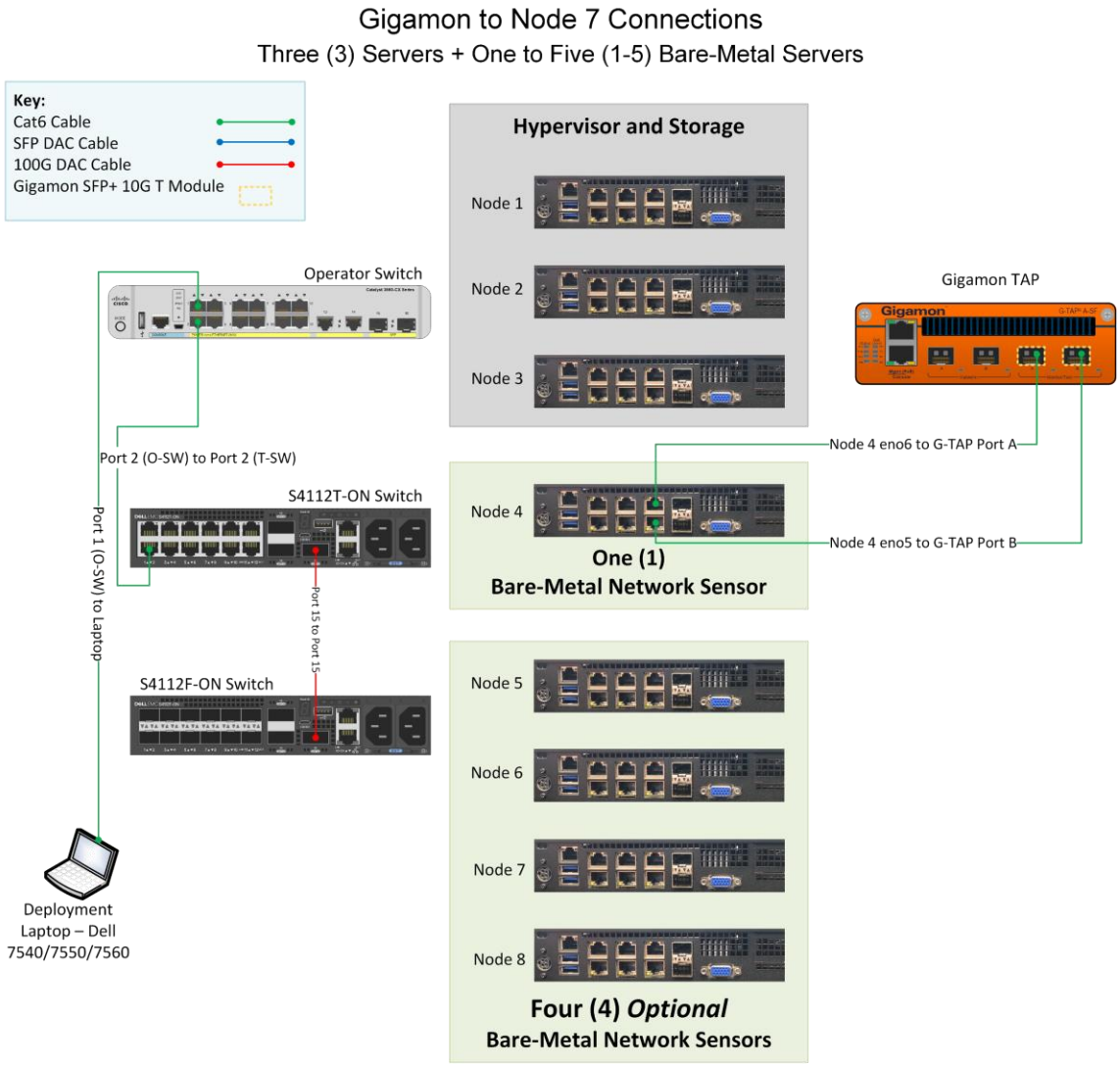
Situation: Required

Instructions:

1. Ensure the power strip is **NOT** energized while connecting equipment.
2. Plug in any required nodes, switches, and devices and then apply power by activating the rocker switch located on each power strip.
3. Proceed to **Task 2.4.5** to complete cabling procedures.

✎ **Note**: The power strips included with the DDS-M Kit are rated for **`120V, 60 Hz`** operation in the United States. Use an appropriate power strip for locations where voltage and frequency are different.

2.4.5 Gigamon to Bare-Metal Node Connections:



2.4.4 Gigamon to Bare-Metal Node Connections

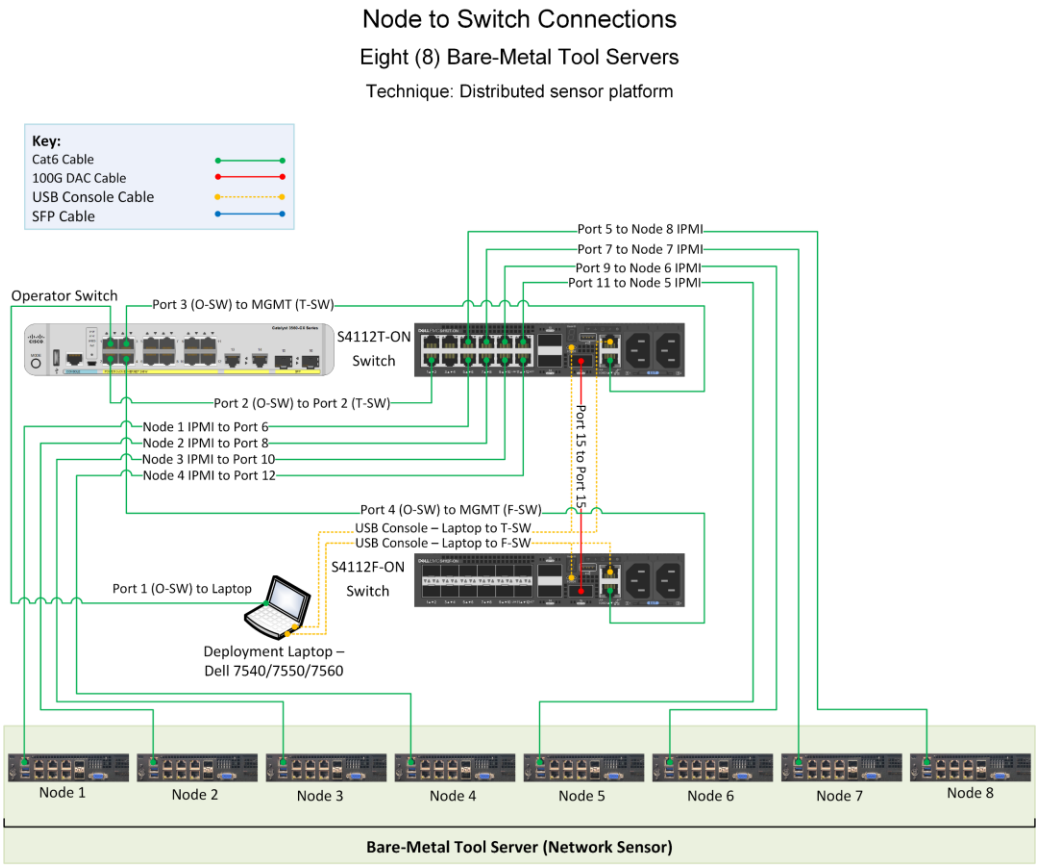
Situation: Optional

Instructions: Connect a sensor to the Gigamon G-TAP as specified in the diagram above.

2.5 8 Bare-Metal Servers

Technique: This configuration is recommended for distributed sensor platforms.

2.5.1 Switch to IPMI Connections:



2.5.1 Switch to IPMI Connections

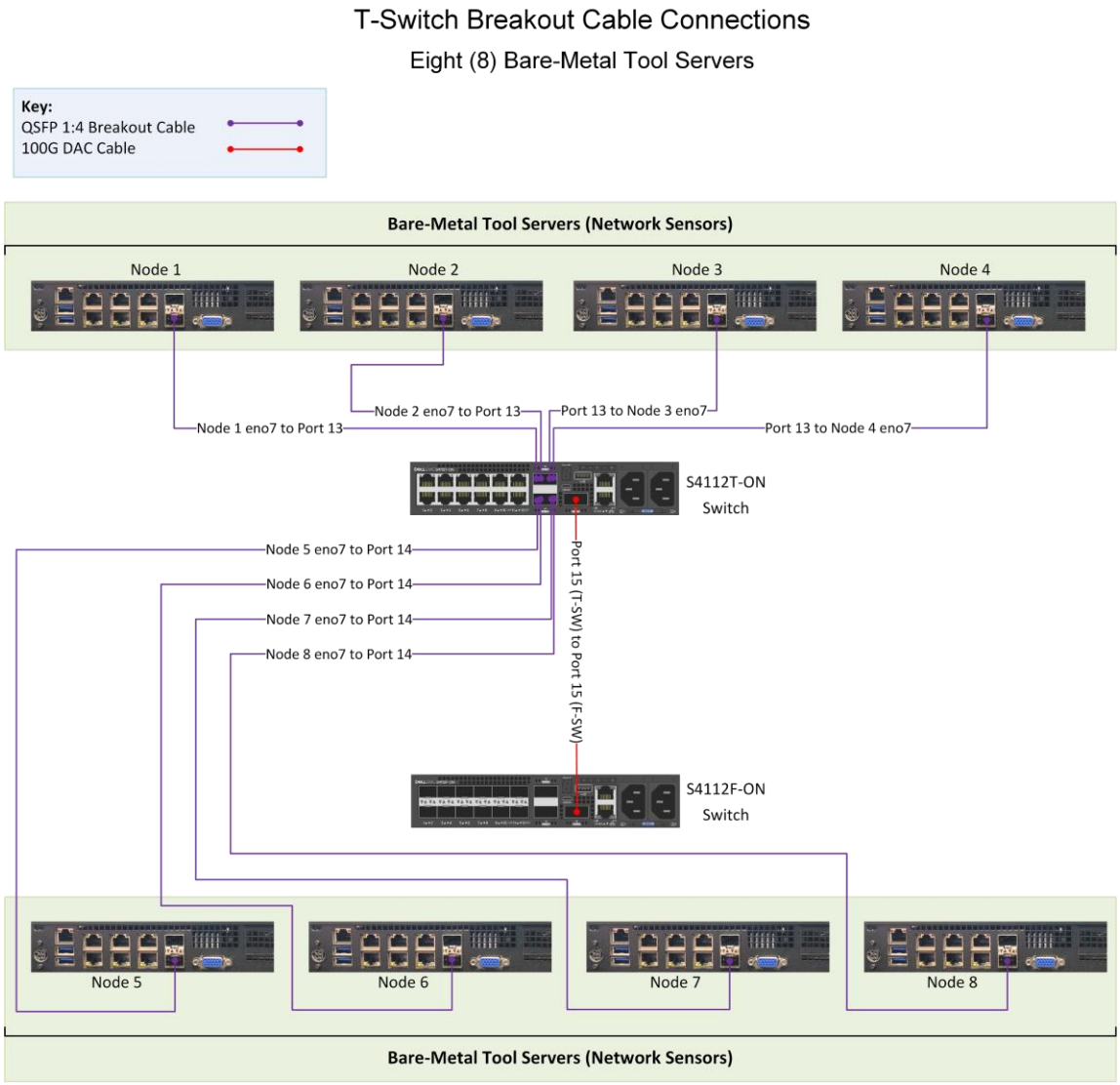
Situation: Required

Instructions:

1. Connect the **Deployment Laptop** to the Operator switch by using a CAT6e cable.
2. Connect the **Operator Switch** to **Port 2** on **the Dell S4112T Switch** by using a CAT6e cable.
3. Connect required nodes at the interface designated as **IP Management Interface (IPMI)** (VLAN 53) to **Ports 5-12** on the **S4112T** switch.
4. Proceed to **Task 2.5.2** to complete cabling procedures.

✎ **Warning**: Bare-Metal Nodes receive a DHCP issued IP address and remain accessible by web console at **`https://10.[kit number].53.[200-250]`**.

2.5.2 Dell 4112T Switch Breakout Cable Connections:



2.5.2 Dell 4112T Switch Breakout Cable Connections

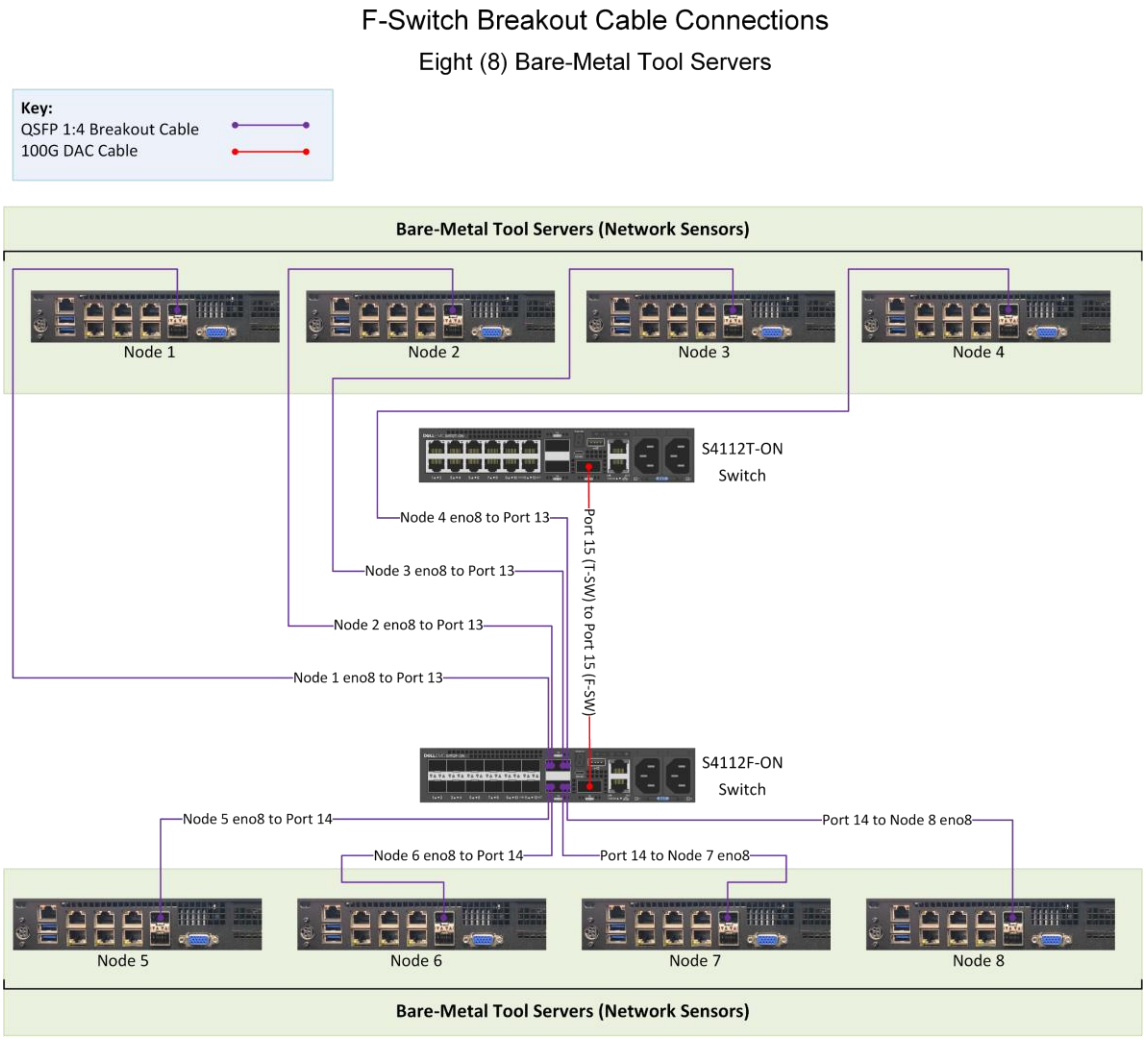
Situation: Required

Instructions:

1. Connect required nodes at the interface designated **eno7** to the QSFP 1-to-4 Breakout cable seated **in Port 13** or **Port 14** on the **S4112T switch**.
2. Proceed to **Task 2.5.3** to complete cabling procedures.

✎ **Note:** Bare-Metal Servers should be used to support operational configurations using **10Gbe** and connected to `VLAN 100, 101, or 102` as needed. Connect interfaces **eno1** to **eno6** as required.

2.5.3 Dell 4112F Switch Breakout Cable Connections:



2.5.3 Dell 4112F Switch Breakout Cable Connections

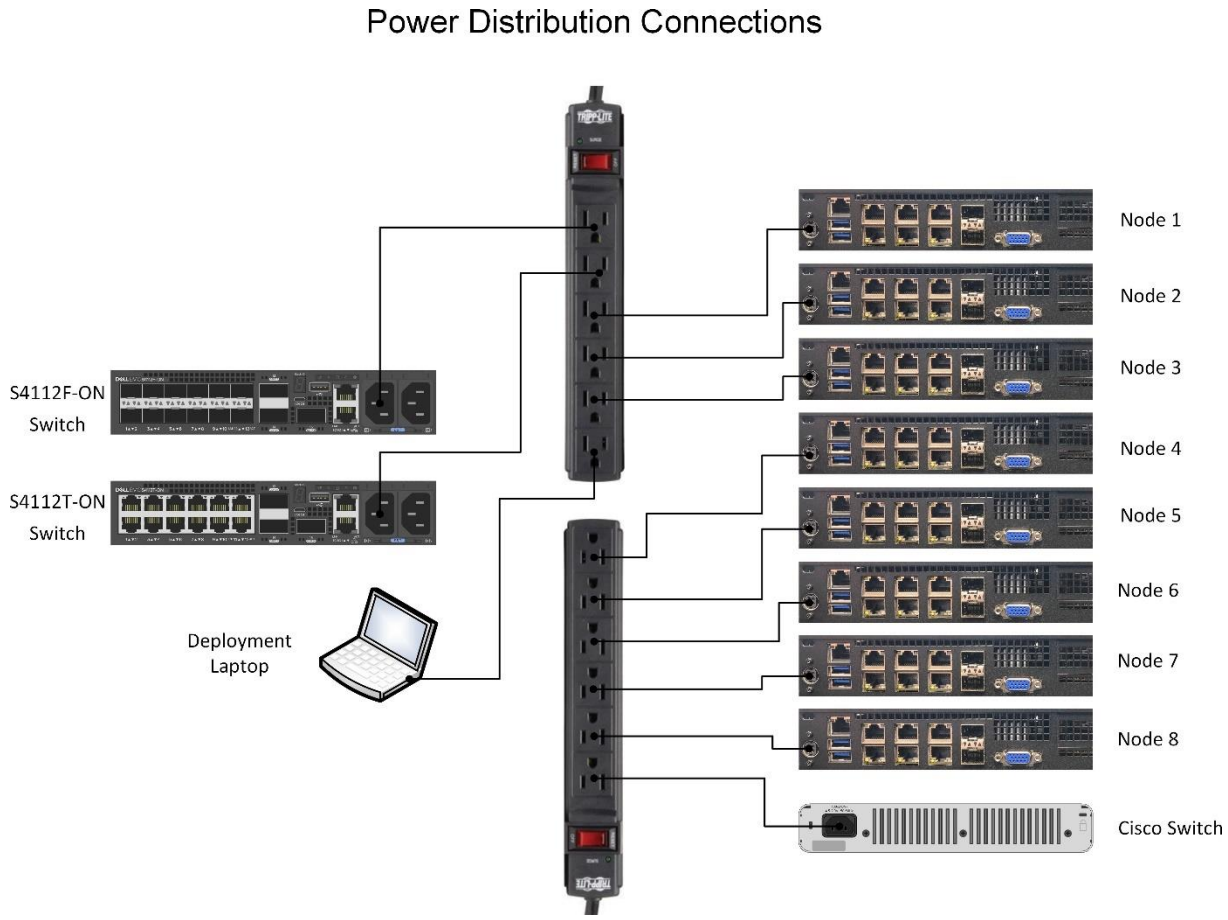
Situation: Required

Instructions:

1. Connect required nodes at the interface designated **eno8** to the **QSFP 1-to-4 Breakout Cable** seated **in Port 13** or **Port 14** on the **S4112F switch**.
2. Proceed to **Task 2.5.4** to complete cabling procedures.

✎ **Note:** Bare-Metal Servers should be used to support operational configurations using **10Gbe** and connected to `VLAN 100, 101, or 102` as needed. Connect interfaces **eno1** to **eno6** as required.

2.5.4 Power Distribution Connections:



2.5.4 Power Distribution Connections

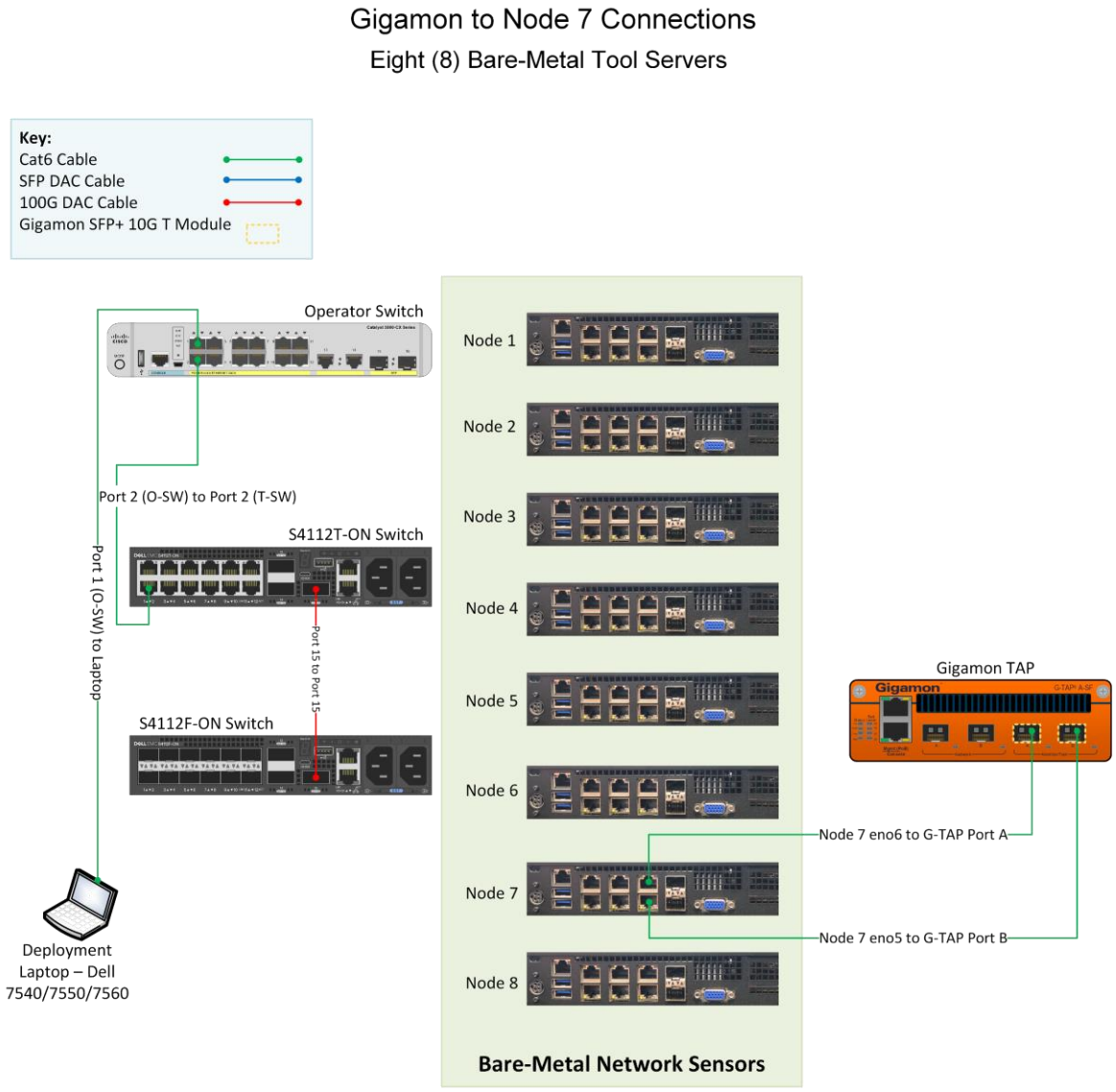
Situation: Required

Instructions:

1. Ensure the power strip is **NOT** energized while connecting equipment.
2. Plug in any required nodes, switches, and devices and then apply power by activating the rocker switch located on each power strip.
3. Proceed to **Task 2.5.5** to complete cabling procedures.

✎ **Note**: The power strips included with the DDS-M Kit are rated for **`120V, 60 Hz`** operation in the United States. Use an appropriate power strip for locations where voltage and frequency are different.

2.5.5 Gigamon to Bare-Metal Connections:

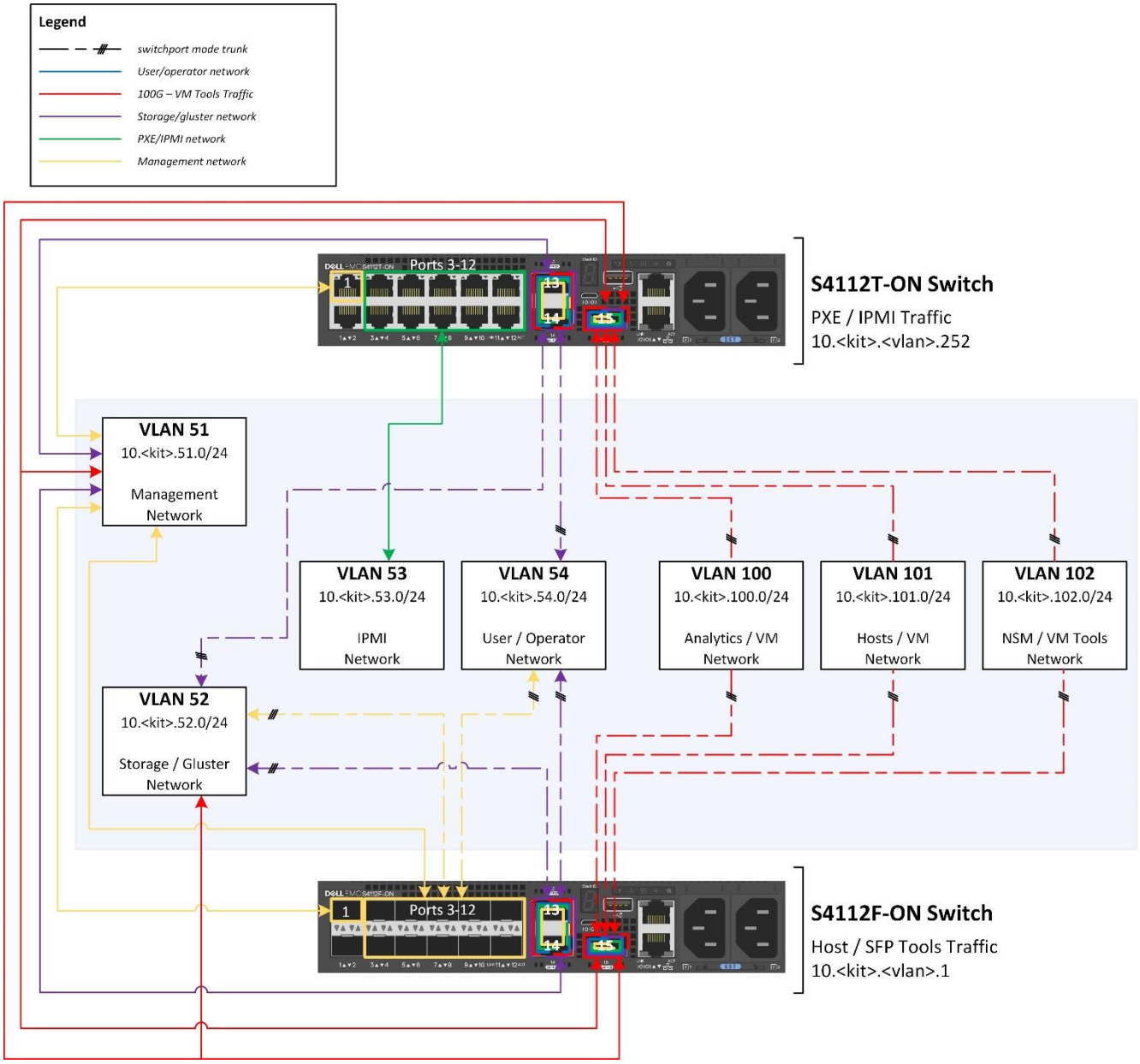


2.5.5 Gigamon to Bare-Metal Connections

Situation: Optional

Instructions: Connect a sensor to the Gigamon G-TAP as specified in the diagram above.

2.6 Switchports: Logical Diagram Network Flow



2.6 Switchports: Logical Diagram Network Flow

3 General Information

DDS-M is designed to be easily re-deployable in any of the supported configurations to prepare for a mission. DDS-M uses Red Hat's automation suite, Ansible, to configure Red Hat Virtualization on the nodes. Ansible deploys IDM and Satellite as virtual machines on the master laptop. Satellite is pre-loaded with all required software repositories for the kit to function in an air-gapped environment.

The Dell S4112 switch ports are configured to use breakout cables and provide both storage and management networks to the nodes. Red Hat Satellite can then be used to automatically provision Red Hat Virtualization or other Operating Systems to the nodes, enabling operators to deploy virtual machines as required.

3.1 Theory of Operations

3.1.1 Scenario 1

In a scenario that a DCO Force is assigned a mission in which they feel minimal resources and personnel are required, it is possible to utilize only the backpack. Inside the backpack there is:

DDS-M Components for Minimal Resource Operations (Backpack Only)

Item	Quantity
Dell Precision 7500-series laptop with six core Intel i7, 64GB RAM, 2TB NVMe	1
10Gbe Thunderbolt SFP+ adapter	1
DDS-M Server with 16 cores, 256GB RAM, 26TB Storage	1
Assorted Direct Connect Cables, CAT6e cable, power strips, KVM crash cart adapter	1

✎ **Note:** The crash cart adapter turns the laptop into a portable console for accessing servers. It allows for transferring files from the laptop to the server, capturing screenshots of server configurations, error messages, and activity for faster troubleshooting.

3.1.2 Scenario 2

If a DCO Force is assigned a mission in which additional resources are needed but not all the resources of a full kit, it is recommended to utilize the backpack and case 1. This configuration will enable the deployment of multiple sensors.

DDS-M Components for Additional Resources (Backpack + 1 Case)

Item	Quantity
Dell Precision 7500-series laptop with six core Intel i7, 64GB RAM, 2TB NVMe	1
Dell EMC S4112-T, 12 10G	1
10Gbe Thunderbolt SFP+ adapter	1
DDS-M Server with 16 cores, 256GB RAM, 26TB Storage	3
Assorted Direct Connect Cables, CAT6e cable, power strips, KVM crash cart adapter	1

3.1.3 Scenario 3

In a scenario that a DCO Force is assigned a mission in which high availability, load balancing, or aggregate compute power is required, it is recommended to utilize a 6-node clustered deployment. This provides an additional switch that can be used either as a tap aggregator/load balancer or as an additional switch for high availability and multiple sensors.

✎ **Note**: If additional equipment is needed, coordinate with the Armory for acquisition.

4 Operation and Configuration Procedures

This section provides an overview of the physical setup and interconnection of each component for DDS-M.

✎ **Warning:** DDS-M cases are designated as a one-person lift. Use the handles on the top and sides of the cases when lifting.

✎ **Warning:** Failure to adhere to the below power consumption tables may result in personal injury.

4.1 Power Information

4.1.1 Power Requirements

All electronic components listed in **Section 4.1.2** 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.

4.1.2 Power Consumption

Hardware without nodes

DDS-M 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 DDS-M Node	130W	160W
Gigamon A-TAP	15W	15W

Full Kit with RHV and Bare-Metal Sensors

Node Deployment	Typical	Maximum	Recommended Breaker
6 servers RHEV, and 2 Bare-Metal servers, Dell S4112-F, Dell S4112-T, Gigamon A-TAP	1385W	1835W	Dedicated 20amp or spread over (2) 15amp breakers
3 servers and 2 Bare-Metal servers, Dell S4112-F, Dell S4112-T, Gigamon A-TAP	995W	1355W	Dedicated 15amp

4.2 Unpacking and Inspection

Compare the contents of each case against the lists provided in the following tables. Inspect all equipment for issues which may cause failure during operational deployments.

✎ **Note**: Refer to Section 5.1 or the laminated inventory sheets provided in each transit case and backpack for re-packing and QA/QC processes.

4.2.1 Differential List of DDS-M Physical Components

Kit Modifications	Kits	Outlying Differences	Storage Location
Dell Precision 7540 Laptop	1 - 49	1 Each	Backpack
Dell Precision 7550 Laptop	50 - 109	1 Each	Backpack
Dell Precision 7560 Laptop	110+	1 Each	Backpack
Tripp Lite 6-Port Power Strip	1 - 89	2 Each in Kits 1 - 49 1 Each in Kits 50 - 89	Backpack
APC 8-Port Power Strip	50+	1 Each in Kits 50 - 89 2 Each in Kits 90+	Backpack
Fiberstore (FS) Branded Cables	1 - 89	All Direct Attach and Fiber Cables	Cases 1 – 3, Backpack
ProLabs Branded Cables	90+	All Direct Attach and Fiber Cables	Cases 1 – 3, Backpack

4.2.2 List of DDS-M Physical Components per Case

Case Number 1

Items	Quantity
Case Number 1	
Dell EMC Switch S4112T	1
Server Node Chassis	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
Micro-USB Console Cable (Dell Switch)	1
3.0 ft CAT 6e (Black)	3

Case Number 2

Items	Quantity
Case Number 2	
Dell EMC Switch S4112F	1
Server Node Chassis	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
Micro-USB Console Cable (Dell Switch)	1
3.0 ft CAT 6e (Black)	3

Case Number 3

Items	Quantity
Case Number 3	
Server Node Chassis	3
192w 16A AC/DC External Power Supply for Server	3
12-Port Cisco Catalyst 3560 Switch	1
Mini-USB Console Cable (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

Items	Quantity
Backpack	
Dell Precision 7500-Series Laptop	1
Server Node Chassis	1
Slip Case for Server Node	1
192w 16A AC/DC External Power Supply for Server	1
Power Strips	2
2.0m Ruggedized SM Fiber Cable	3
1.0m Ruggedized MM Fiber Cable	3
3.0m SFP+ Direct Connect (Dell)	2
1.0m QSFP Breakout Cable (Dell)	4
100G QSFP28 Passive Cable	1
Dell EMC Switch Power Cords	2
Cisco Switch Power Cord	1
Dell Precision 7500-series Laptop Power Adapter	1
Solo10G™ SFP+ Thunderbolt™ 3 Network Adapter	1
USB Laptop Console Crash Cart Adapter	1
6.0 ft CAT 6e (Black)	3

4.3 Operation and Configuration

The DDS-M solution provides a compute and storage environment for handling traffic via distributed collection and analysis. Using a total of eight nodes, it is designed to aggregate network traffic in excess of 15 Gbps. It can also be broken into smaller, powerful sensors distributed to separate collection points across one or more networks.

4.3.1 Kit Authentication and Passwords

When the kit is initially deployed the **passwords.yml** file is created which contains all usernames and passwords for the deployed Red Hat Enterprise Virtualization (RHEV) environment. The passwords.yml file is located in the **/opt/ddt/ansible_main/** directory.

✎ **Note**: Passwords must be changed every 60 days.

✎ **Note**: For versions prior to DDT Release Version 1.5.3, the path location is **/opt/cure/ansible_main**.

Red Hat Satellite, Red Hat Identity Management (IdM), and Red Hat Virtualization Hosted Engine will use the ***admin*** username as named in the credential scheme as ***[host]_admin_pass***.
OS level credentials will use the **root** user as named in the credential scheme as ***[host]_root_pass***.

✎ **Note**: The **Deployment Laptop** root level SSH identity is imported as an authorized key for DDS-M internal systems. When initiating SSH connections ensure to elevate using the '**sudo'** command.

```
[defender@master ~]$ sudo ssh node0
[root@node0 ~]# gluster volume list
```

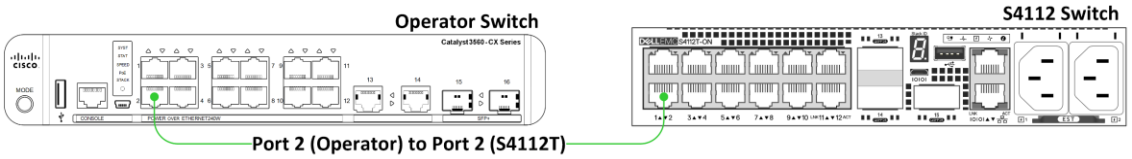
Significant Information

The **Red Hat Virtualization Host (RHV-H)**, and the **Red Hat Virtualization Hosted Engine** systems are appliances and do not function as typical operating systems normally do. Refrain from executing OS level configuration tasks without requesting developer support or referencing the correct Red Hat provided administration guide.

4.3.2 Connecting to the S4112-T Switch

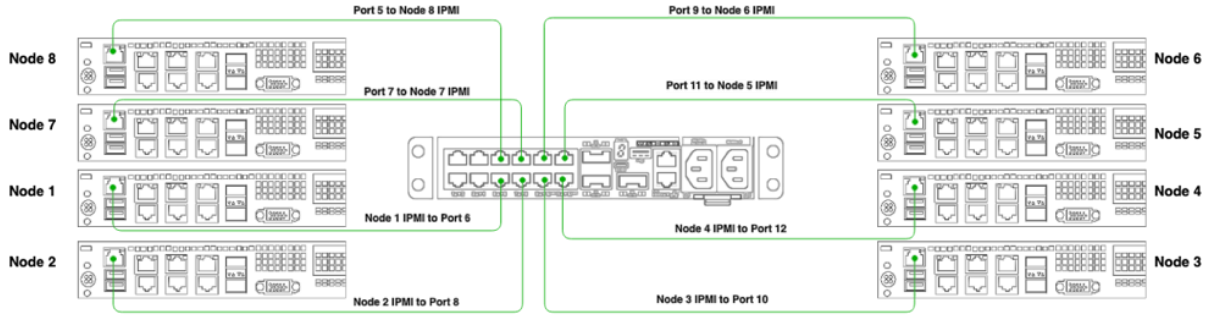
Cables Needed for T-Switch Connections
(9) CAT 6 Cables - Indicated by green line
(2) QSFP Breakout Cables - Indicated by purple line

1 Begin by plugging a **CAT6** cable into **Port 2** on the **S4112-T** switch and the other end into the **Operator Switch**.



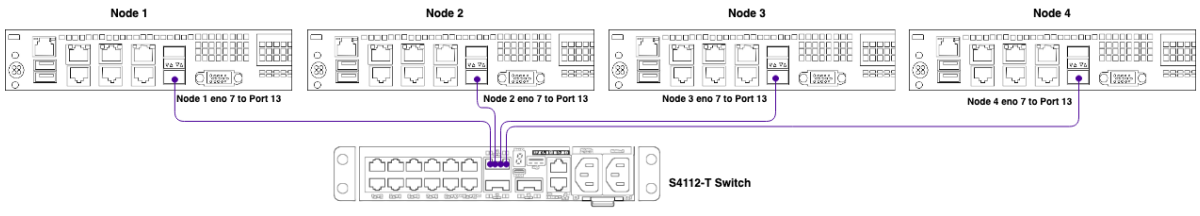
4.3.2(a) Operator Uplink to Dell 4112T

2 Using a **CAT6** cable, connect **Nodes 1-8 IPMI** into **Ports 5-12** on the **T** switch.



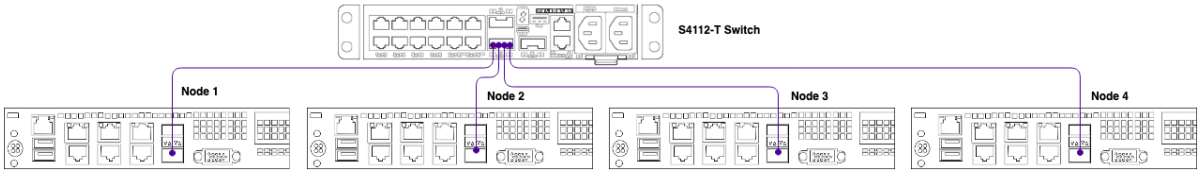
4.3.2(b) Dell 4112T IPMI to Nodes

3 Using **QSFP Breakout cable**, connect **Nodes 1-4 eno 7** into **Port 13** on the **T** Switch.



4.3.2(c) Dell 4112T eno13 Breakout to eno7 on Nodes

4 Using a **QSFP Breakout cable**, connect **Nodes 5-8 eno 7** into **Port 14**



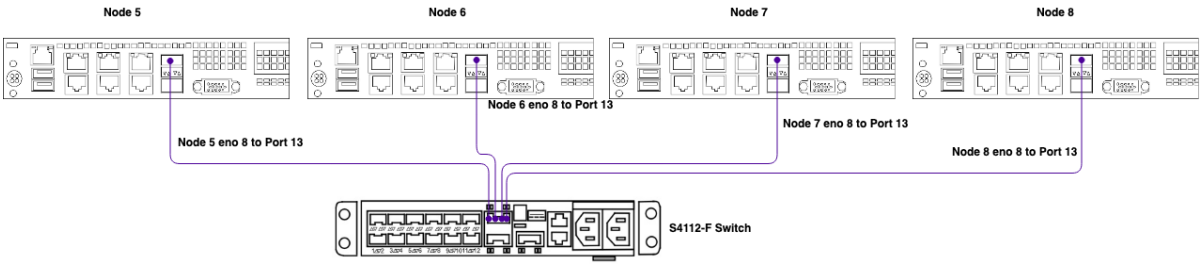
4.3.2(d) Dell 4112T eno14 Breakout to eno7 on Nodes

4.3.3 Connecting to the S4112-F Switch

Cables Needed for F-Switch Connections

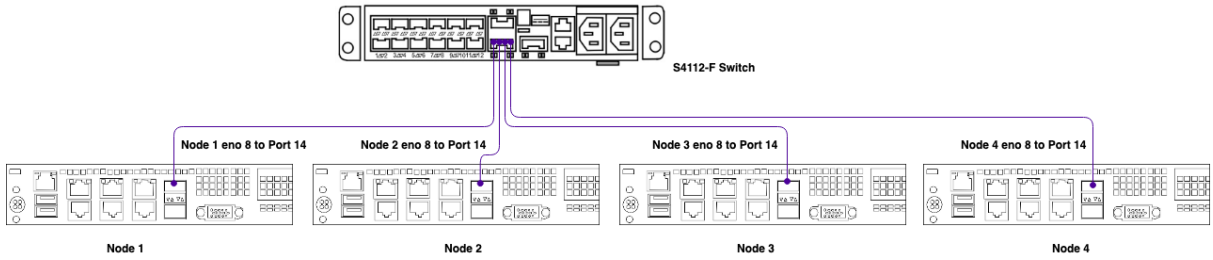
(2) QSFP Breakout Cables - Indicated by purple line

1 Using a **QSFP Breakout cable**, connect **Nodes 5-8 eno 8** into **Port 13**



4.3.3(a) Dell 4112T eno14 Breakout to eno8 on Nodes

2 Using a **QSFP Breakout cable**, connect **Nodes 1- 4 eno 8** into **Port 14**



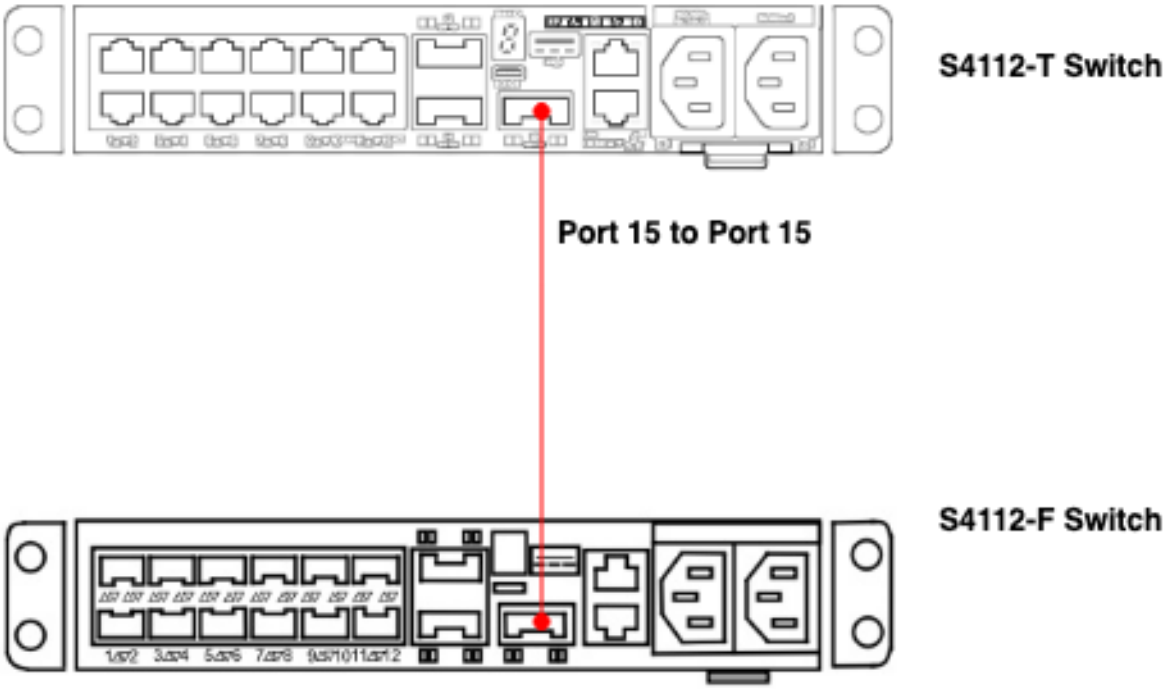
4.3.3(b) Dell 4112T eno14 Breakout to eno8 on Nodes

4.3.4 Connecting Both Switches

Cable Needed for S4112-T to S4112-F Connection

(1) 100G Cable - Indicated by red line

1 Using a **100G** cable, connect the **S4112-T** switch, **Port 15** to the **S4112-F** switch, **Port 15**.



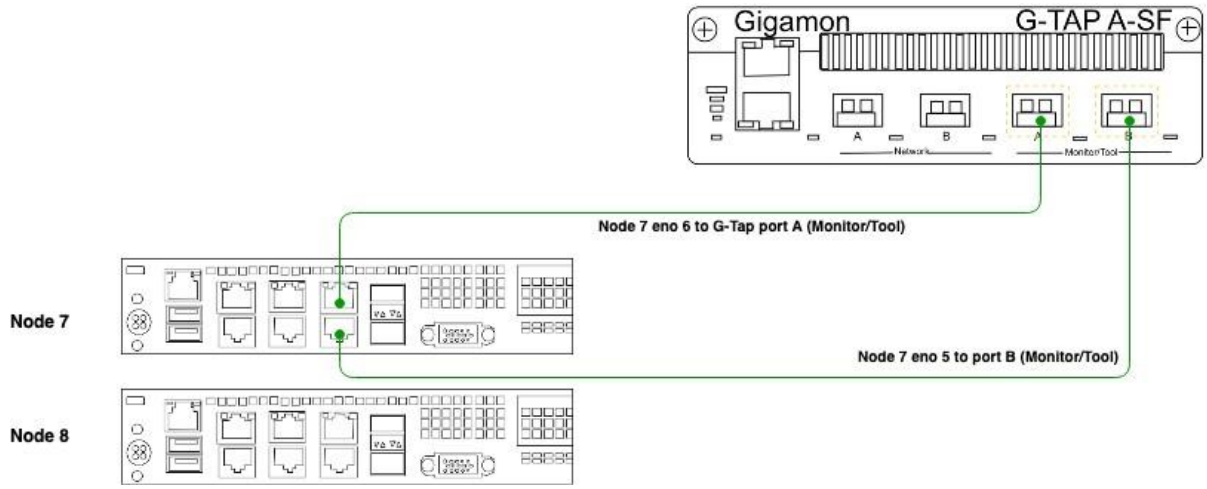
4.3.4 Dell 4112T to Dell 4112F 100g Link

4.3.5 Connecting to the Gigamon Network Tap

Cable and SFP Module Needed for Gigamon Connection
(2) CAT 6 Cables - Indicated by green line
(2) Gigamon SFP+ 10G T Modules – Indicated by gold dash box

1 Connect 2 **Gigamon SFP+ 10G T Modules** to **Gigamon Tap Port A Monitor/Tool** and **Port B- Monitor/Tool**
2 Using a **CAT6** cable, connect **Node 7 eno 6** to the **Gigamon Tap Port A Monitor/Tool**. Next, using a **CAT6** cable, connect **Node 7 eno 5** to **Port B-Monitor/Tool**

✎ **Note**: Depending on deployment scenario, this could be Node 4 with the same port and module connections.



4.3.5 Gigamon to Bare-Metal Sensor

4.4 Power Procedures

4.4.1 System Power Up Sequence

To power up the system, begin by cabling to switches and nodes first. Next, power on the switches, followed by the laptop. Lastly, power on servers. Perform the steps below.

1 Verify the virtual machines are running on the master laptop.

```
[defender@master ~]$ sudo virsh list --all
 Id Name                           State

 -  IDM                            running
 -  IDM_replica                    running
 -  satellite                      running
```

✎ **Note**: If the virtual machines are not running, manually start them by performing the following command. For example: to start the IDM virtual machine: **sudo virsh start IDM**

2 Power on all nodes and wait approximately 5 minutes for them to power up.
3 SSH into one of the nodes, enter the *gluster* cli, and start each volume.

```
[defender@master ~]$ sudo ssh node1
[root@node1 ~]# gluster

gluster> volume list
data
engine
isostore
vmstore
gluster> volume start <volume name>
```

✎ **Note**: This next step needs to be completed on EACH node before proceeding to the next step.

4 SSH into **EACH** node, in separate sessions, and verify that the **ovirt-ha-broker** and the **ovirt-ha-agent** services are listed as **active (running)**. If the service has stopped, request assistance and verify the system is correctly configured.

```
[defender@master ~]$ sudo ssh node0
[root@node0 ~]# systemctl status ovirt-ha-broker ovirt-ha-agent
```

✎ **Note**: Steps 4-5 must be completed only on **ONE** node before proceeding to step 6.

5 Exit maintenance mode of the hosted engine.

```
[defender@master ~]$ sudo ssh node0
[root@node0 ~]# hosted-engine --set-maintenance --mode=none
```

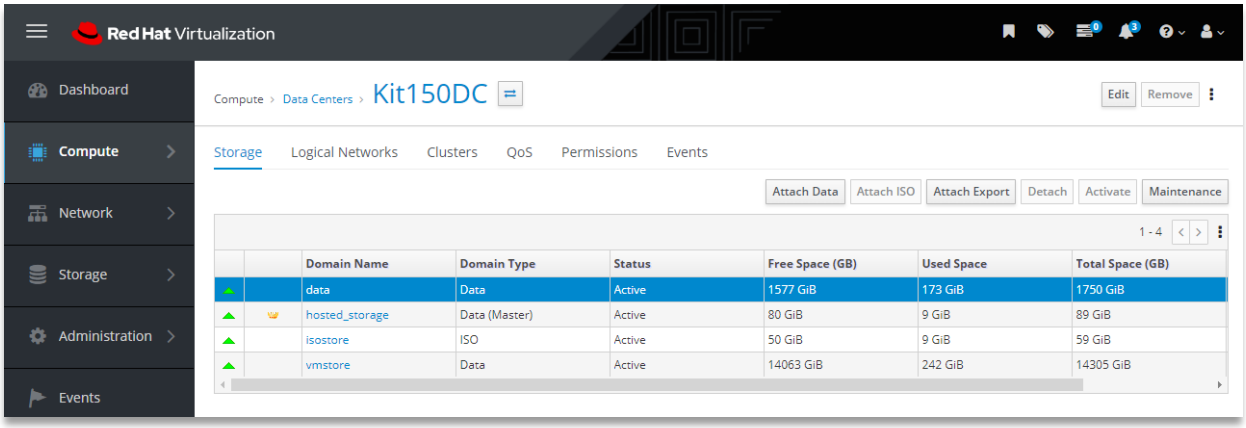
6 The hosted engine VM can take some time to boot up. Verify the process by entering and repeating the following command until Hosted Engine is in an Up and Good state:

```
[root@node0 ~]# hosted-engine --vm-status | grep status
```

With a web browser, use the **engine_admin_pass** in **passwords.yml** and log onto the hosted engine by navigating to the following website and selecting **Administration Portal**:

`https://engine.[kit number]cpt.cpb.mil/`

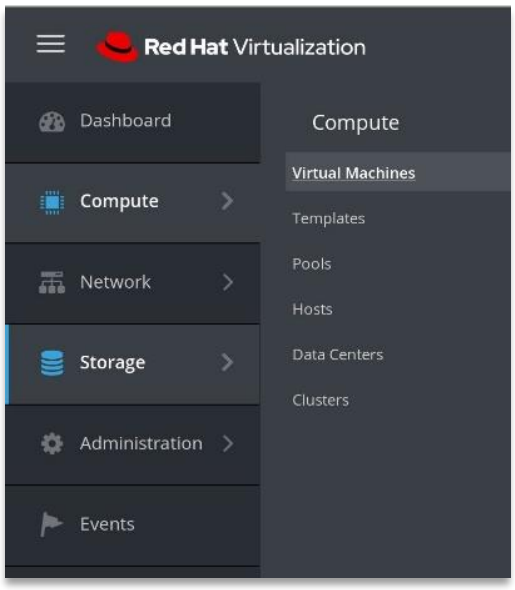
7 On the left-hand panel, navigate to **Compute > Data Centers->Kit#DC.**



4.4.1(a) Engine: Storage -> Domains

8 Click on a row to select a storage domain. For each domain, click the **Activate** button. Refresh the page to confirm each domain has successfully completed activation.

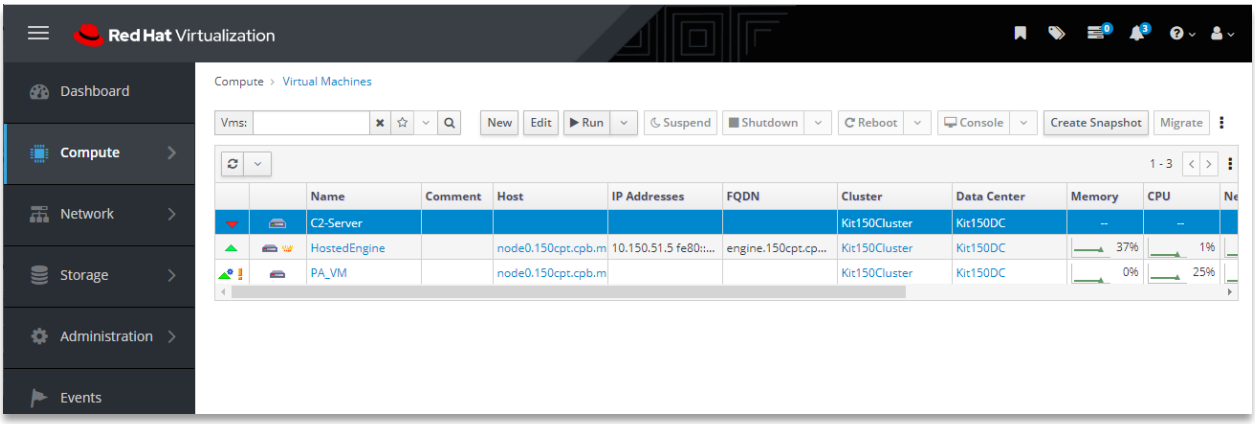
9 On the left-hand panel, navigate to **Compute > Virtual Machines**



4.4.1(c) Engine: Compute -> Virtual Machines

10 Start each virtual machine by selecting it and clicking the **Run** button in the top right. Wait until all virtual machines are turned on to continue any operational procedures.

✎ **Note**: Clicking the drop-down selection menu on the **Run** button enables additional task execution for a single boot event.



4.4.1(d) Engine: Starting Virtual Machines

4.4.2 System Power Down Sequence

The power down sequence is dependent upon what operating system and platform is deployed. For purpose of this document, it is assumed that the DDT software is deployed and providing a hyperconverged RHEV platform. Proper startup/shutdown procedures must always be followed to prevent the loss of data.

✎ **Note**: Determine which node is running Hosted Engine. Use this node during step 6.

1 With a web browser, use the **engine_admin_pass** in **passwords.yml** and log onto the hosted engine by navigating to the following website and selecting **Administration Portal**:

`https://engine.[kit number]cpt.cpb.mil/`

2 On the left-hand panel, navigate to **Compute > Virtual Machines**
3 Gracefully stop each virtual machine except Hosted Engine by selecting it and clicking the **Shutdown** button in the top right toolbar. Wait until all virtual machines are turned off. Some virtual machines can require up to ten minutes to stop.

✎ **Note**: To force a virtual machine to immediately power off, use the drop-down menu for the **Shutdown** button and select **Power Off**. This will kill the machine as if the power was cut. Do not force virtual machines to stop unless **Shutdown** fails to execute as described above.

4 On the left-hand panel, navigate to **Compute > Data Centers** and select **Kit[#]DC**

✎ **Note**: Do NOT move the Hosted Engine domain "**hosted_storage**" into maintenance mode. Hosted engine will no longer be available through the GUI. Step 6 describes the process to stop Hosted Engine.

5 Click the white space in each domain to select it. Click on the **Maintenance** button the top right for every storage domain except **hosted_storage**.
6 SSH into the node that is running Hosted Engine and run the following commands to enter maintenance mode and shutdown the hosted engine.

✎ **Note**: Running **hosted-engine --vm-status** on any node running RHEV will identify which node is running hosted-engine.

```
[defender@master ~]$ sudo ssh node0
[root@node0 ~]# hosted-engine --set-maintenance --mode=global
[root@node0 ~]# hosted-engine --vm-shutdown
```

7 Confirm the hosted engine is shut down by entering the following command and reviewing each node's hosted engine status.

```
[root@node0 ~]# hosted-engine --vm-status | grep status
```

8 SSH into **EACH** node, in separate sessions, and stop the **ovirt-ha-broker** and **ovirt-ha-agent** services, then disconnect the gluster storage.

```
[defender@master ~]$ sudo ssh node0

[root@node0 ~]# systemctl stop ovirt-ha-broker ovirt-ha-agent

[root@node0 ~]# hosted-engine --disconnect-storage
```

9 From **ONE** of the nodes, open the gluster cli and run **volume list** to show a list of the storage volumes. Stop each of these volumes with the following commands:

```
[defender@master ~]$ sudo ssh node1
[root@node1 ~]# gluster

gluster> volume list
data
engine
isostore
vmstore
gluster> volume stop <volume name>
```

10 Ensure **EACH** node is powered off, in separate sessions, by issuing the following commands:

```
[defender@master ~]$ sudo ssh node0
[root@node0 ~]# poweroff
```

11 On the **Deployment Laptop**, ensure the three virtual machines of **Satellite**, **IDM**, and **IDM2** are powered off.

```
[defender@master ~]$ sudo ssh satellite "poweroff"
[defender@master ~]$ sudo ssh idm2 "poweroff"
[defender@master ~]$ sudo ssh idm "poweroff"
```

12 Confirm each virtual machine is powered off by issuing the following commands:

```
[defender@master ~]$ sudo virsh list --all
 Id Name                           State

 -  IDM                            Shut Off
 -  IDM_replica                    Shut Off
 -  satellite                      Shut Off
```

13 Power off the **Deployment Laptop**.

4.5 Unplugging Nodes and Switches

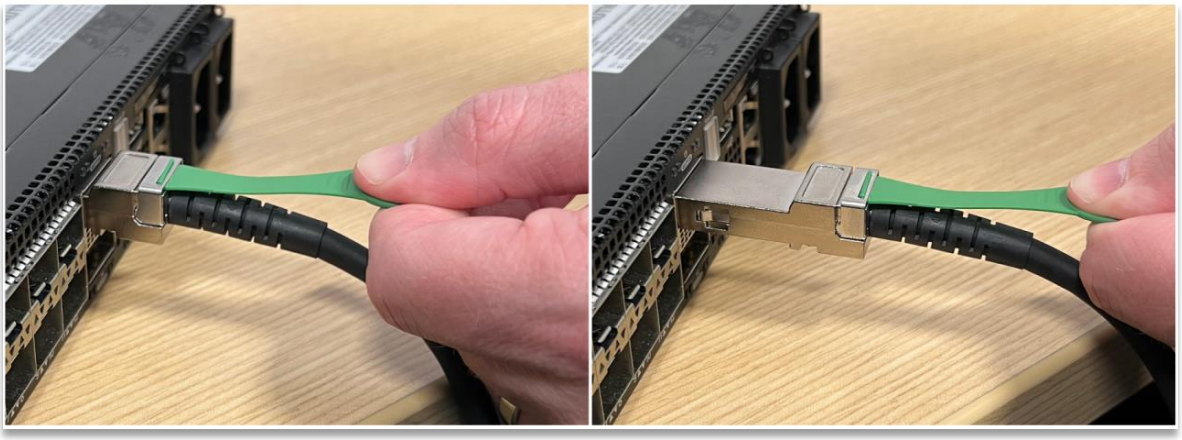
✎ **Note**: DO NOT UNPLUG CABLES BY PULLING ON THE CORD

Ensure proper breakdown of the kit by following the proper procedures to unplug the cables from the kit.

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

4.5(a) Unplugging Node Power Cable

2 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.



4.5(b) Unplugging DAC and QSFP Cables

4.6 Node Redeployment Procedures

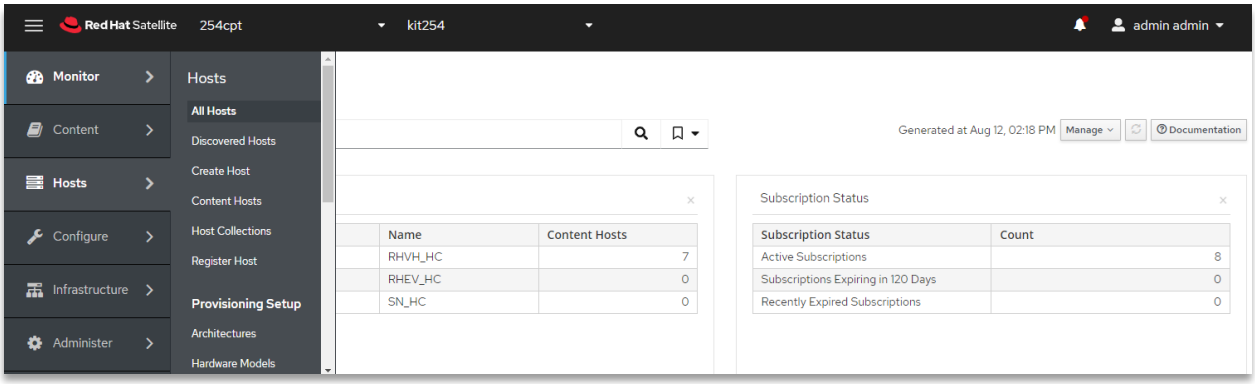
4.6.1 Removing Nodes from Hosted Engine and Satellite

After a mission, there may be a requirement to wipe a deployed kit so that it is ready to be re-deployed in another capacity. For purpose of this document, it is assumed the DDT software is deployed and providing a hyperconverged RHEV platform. Please take the following actions to ensure a successful wipe:

1 With a web browser, use the ***sat_admin_pass*** in ***passwords.yml*** and log into Satellite by navigating to:

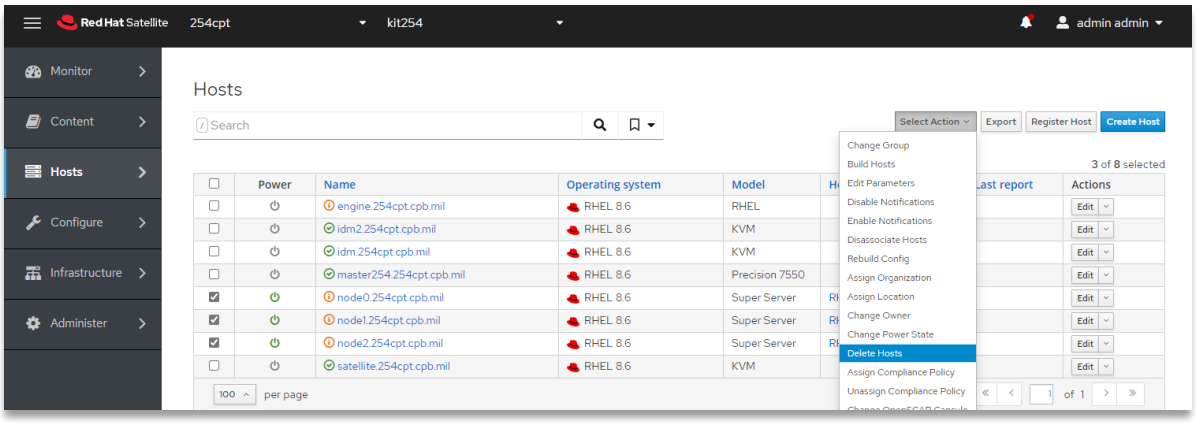
`https://satellite.[kit number]cpt.cpb.mil`

2 On the left-hand panel, navigate to **Hosts > All Hosts**



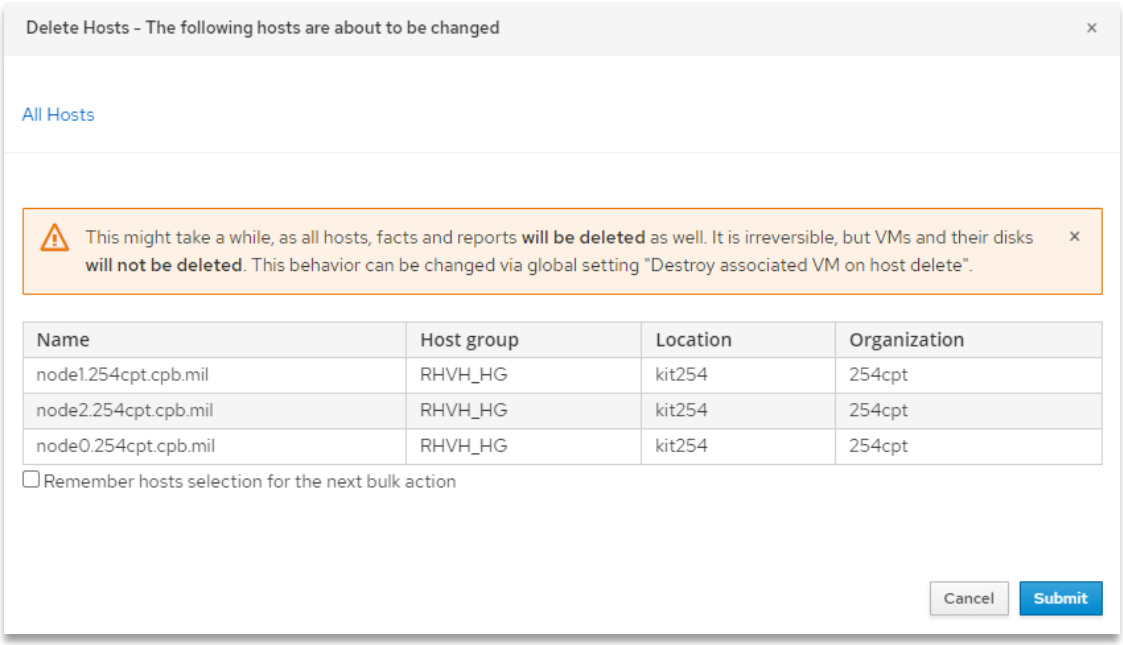
4.6.1(a) Satellite: Hosts > All Hosts

3 Click the checkboxes for each of the nodes to be wiped. Use the drop-down menu **Select Action** to click **Delete Hosts**



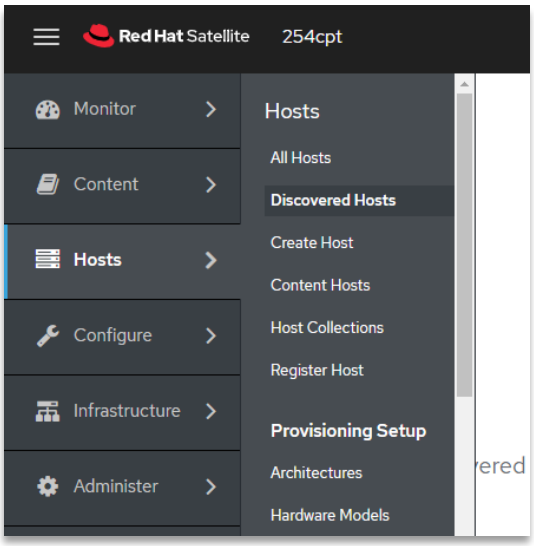
4.6.1(b) Satellite: Deleting Hosts

4 Click **Submit** on the confirmation window



4.6.1(c) Satellite: Delete Hosts Confirmation

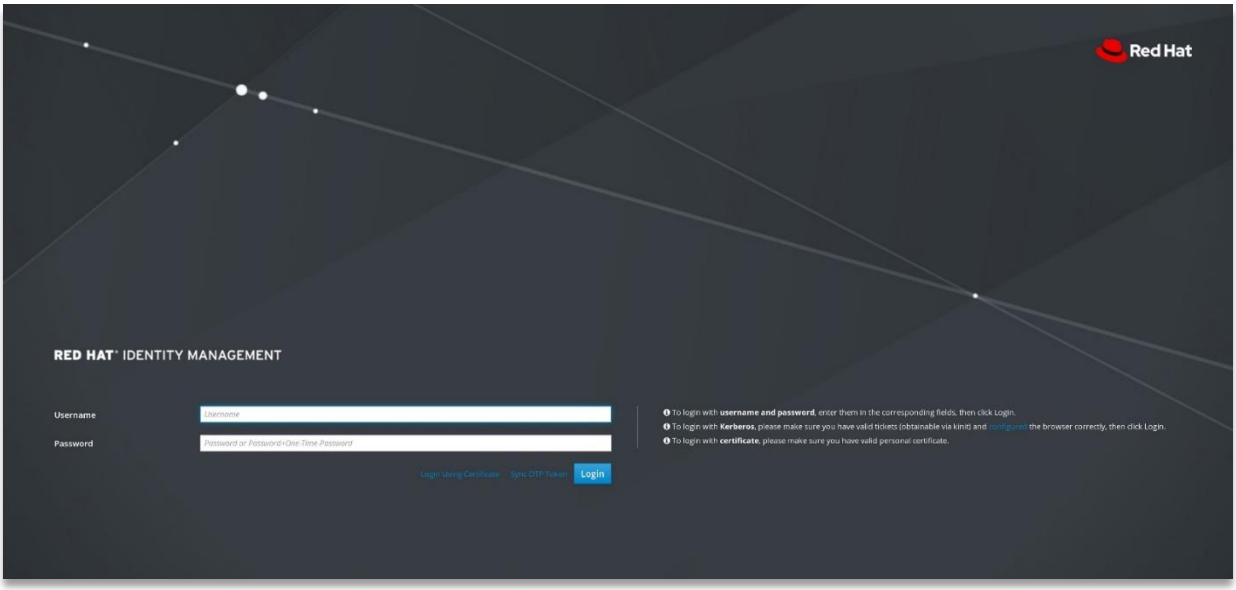
5 On the left-hand panel, navigate to **Hosts > Discovered Hosts**. Select and delete any hosts listed in this area.



4.6.1(d) Satellite: Hosts > Discovered Hosts

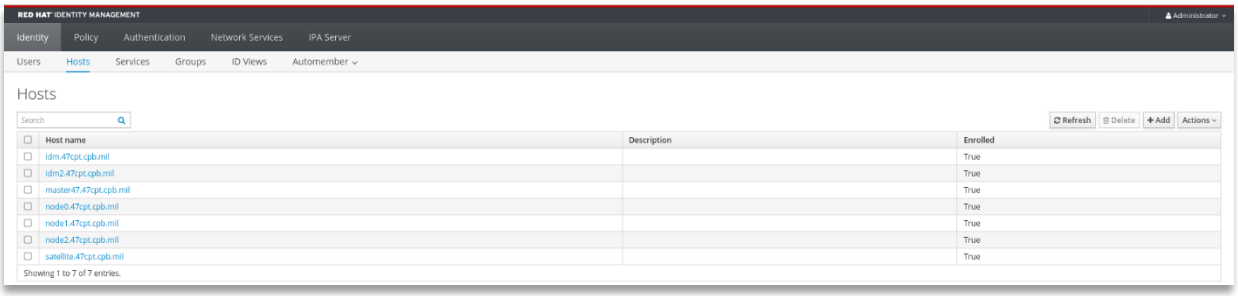
6 With a web browser, use the ***ipa_admin_pass*** in ***passwords.yml*** and log into IdM by navigating to:

`https://idm.[kit number]cpt.cpb.mil`



4.6.1(e) IdM: Web UI Login

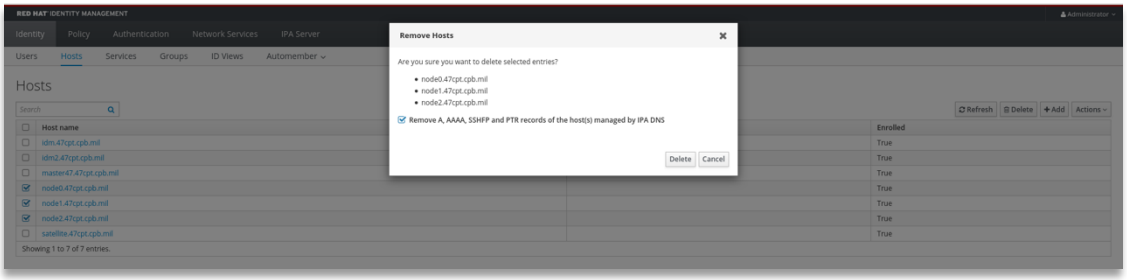
7 Navigate to the **Identity > Hosts** tab.



4.6.1(f) IdM: Identity > Hosts

8 Click the checkboxes to select each of the nodes. Click the **Delete** button in the top-right.

✎ **Note**: Click the checkbox for "Remove A, AAAA, SSHFP and PTR records of the host(s) managed by IPA DNS.



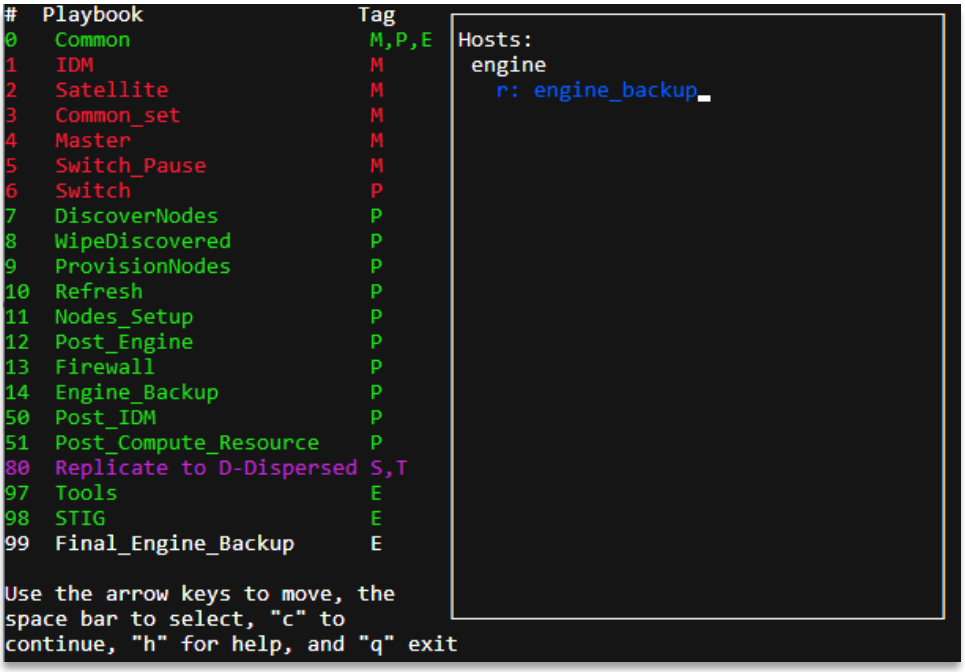
4.6.1(g) IdM: Deleting Hosts

9 Navigate to **/opt/ddt/ansible_main** and run **tmux**, then run play.py as sudo and specify the number of clustered nodes to deploy.

```
[defender@master ~]$ sudo tmux
[root@master ~]# cd /opt/ddt/ansible_main
[root@master ansible_main]# ./play.py -n #     (Replace # with cluster size)
```

10 Select the necessary operator playbooks by pressing [**SPACE**] to select playbooks **07 – DiscoverNodes** to **99 - Final_Engine_Backup**. Press [**c**] to continue.

✎ **Note**: Passwords must be changed every 60 days.



4.6.1(h) Play.py: Playbooks DiscoverNodes – Final_Engine_Backup

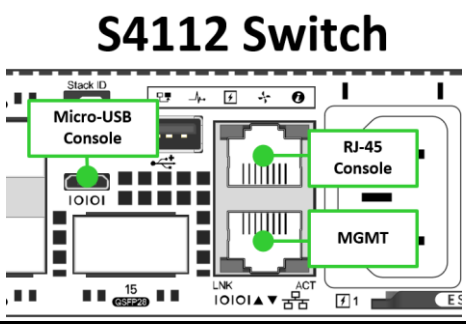
4.6.2 Factory Reset and Configure S4112 Switches

Task completed by: **Operator (Required During Kit Re-Deployment)**

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

Cables Needed for Switch Connections
(2) USB to RJ-45 Console Cables
(4) RJ-45 Cat6E Ethernet Cables

1. Using the included **Cisco WS-C3560 12 Port User Switch**, connect the following sequence:

From Port	To Port	Reference
User Switch **[Port 1]**	*Master Laptop* **[RJ-45 em1]**	
User Switch **[Port 2]**	*Dell S4112-T* **[Port 2]**	
User Switch **[Port 3]**	*Dell S4112-T* **[MGMT]**	
User Switch **[Port 4]**	*Dell S4112-F* **[MGMT]**	

2. Using a **USB to RJ-45** cable, connect the **RJ-45** adapter to the top-right Console interface on the front panel of the **S4112-F** switch. Connect the cable from the **USB** adapter to the first USB interface on the **Deployment Laptop**.
    - Alternatively, connect the **USB to Micro-USB** cable to the Console interface above Port 15 on the front panel of the **S4112-F** switch.
3. Using a **USB to RJ-45** cable, connect the **RJ-45** adapter to the top-right Console interface on the front panel of the **S4112-T** switch. Connect the cable from the **USB** adapter to the second USB interface on the **Deployment Laptop**.
    - Alternatively, connect the **USB to Micro-USB** cable to the Console interface above Port 15 on the front panel of the **S4112-T** switch.

Performing ONIE Install.

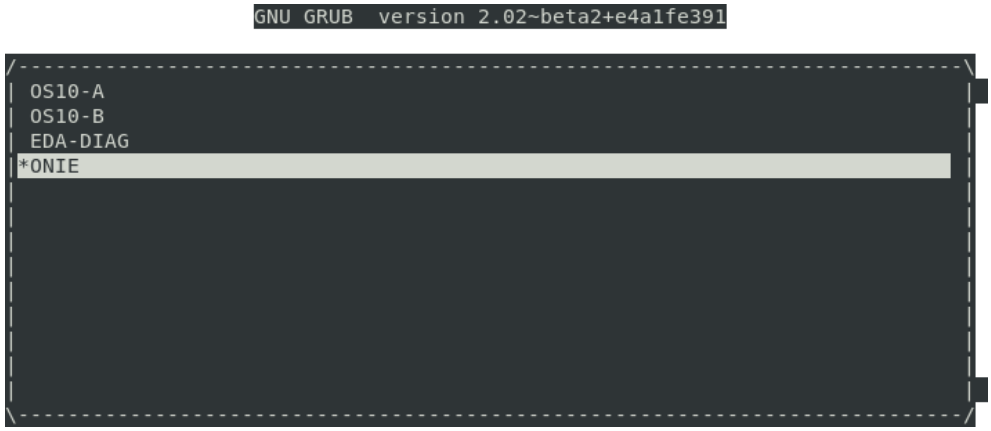
✎ **Note**: Adjust the minicom profile name from **dell0** to **dell1** if using the second USB cable connected to the Deployment Laptop.

- Open a terminal window on the **Deployment Laptop** and type:

```
[defender@master ~]$ sudo minicom dell0
```

✎ **Note**: If the dell0 or dell1 profiles do not exist, run the setup tasks described in **Section 11.1.4** and create profiles for use during this task.

- Power cycle the *Dell S4112* series switch by un-seating and re-seating the power cable.
- Interrupt the Grub boot process by hitting the [**UP or DOWN**] key. Select the **ONIE** menu entry and from the submenu select **ONIE Install**.



4.6.2(a) Dell S4112 ONIE Installation

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

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

4. Repeat the above process on the second switch before proceeding to the next step. The switch fans will run at 100% speed until the process is complete. Continue once the switches have resumed normal fan operation.
5. On the **deployment laptop**, run the following commands to remove the *network_setup* file and then proceed to the next task.

```
[defender@master ~]$ ls -lah /.network_setup
-rw-r—r--. 1 root root 0 Jan 1 16:00 /.network_setup
[defender@master ~]$ sudo rm /.network_setup
[defender@master ~]$
```

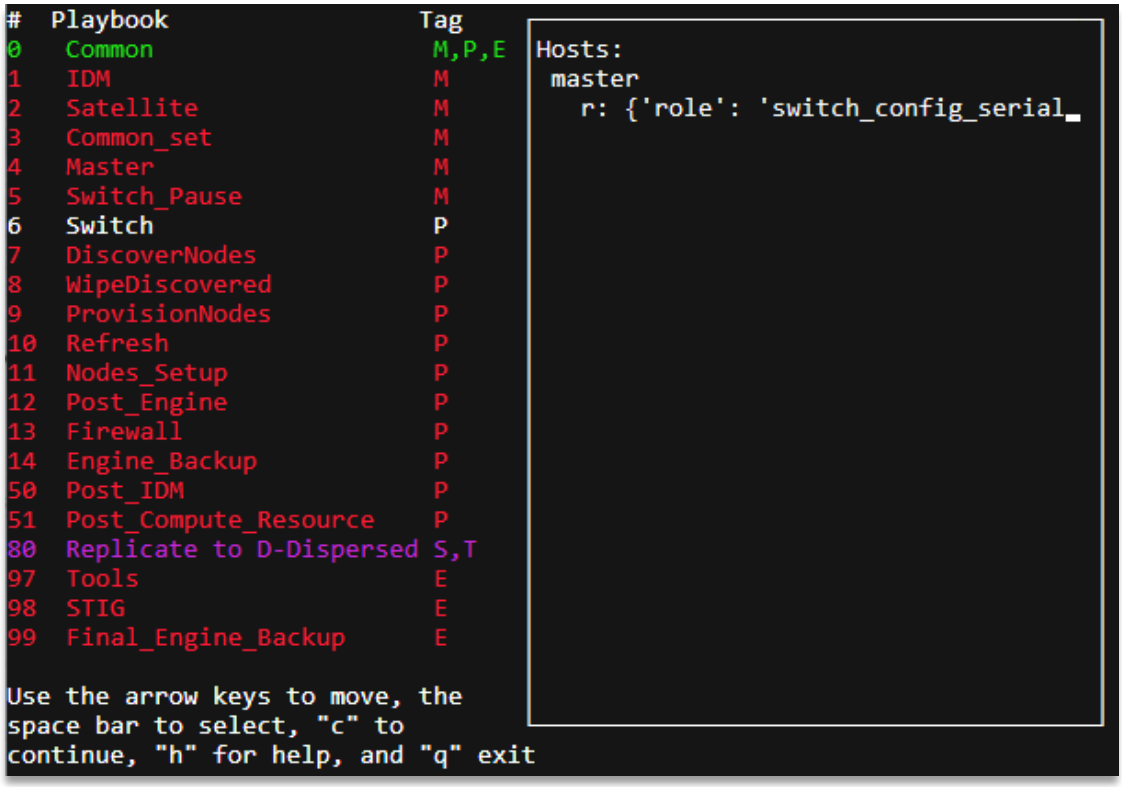
4.6.3 Deploy Switch Operational Configurations

1. Correctly cable the kit according to Cable Diagrams as specified in **Section 2** of this manual per node requirements. Exit any currently running minicom sessions by choosing the appropriate terminal and pressing [**CTRL +A**] then [**Q**] and then selecting [**YES**] to exit.
2. Navigate to **/opt/ddt/ansible_main** and run play.py as root level user within a tmux session.

✎ **Note**: Maximize the terminal window. Do not run the tmux command if tmux is already running (indicated by a green bar below the terminal window).

```
[defender@master ~]$ sudo tmux
[root@master ~]# cd /opt/ddt/ansible_main
[root@master ansible_main]# ./play.py
```

3. Select playbook **6-Switch.yml**, then press [**C**] to continue.



4.6.3 Play.py Switch Playbook

4.6.4 Provisioning Nodes with RHVH

Task completed by: **Operator (Required During Kit Re-Deployment)**

1. Pre-Requisite:
   - Move the cable connecting the master laptop to port 1 of the Cisco switch so that it is instead plugged into port 1 of the S4112-T switch.

✎ **Note**: This cabling change is temporary and should be moved back to port 1 of the Cisco switch after the following procedures are completed.

   - If previously unused or bare-metal hosts are being reconfigured as RHVH nodes, perform BIOS Factory Reset Procedures according to the **Troubleshooting manual, Appendix, Task 21.2.**
2. Open a terminal and run the following commands to run play.py as root level user within a tmux session:

✎ **Note**: Maximize the terminal window. Do not run the tmux command if tmux is already running (indicated by a green bar below the terminal window).

```
[defender@master ~]$ sudo tmux
[root@master ~]# cd /opt/ddt/ansible_main
```

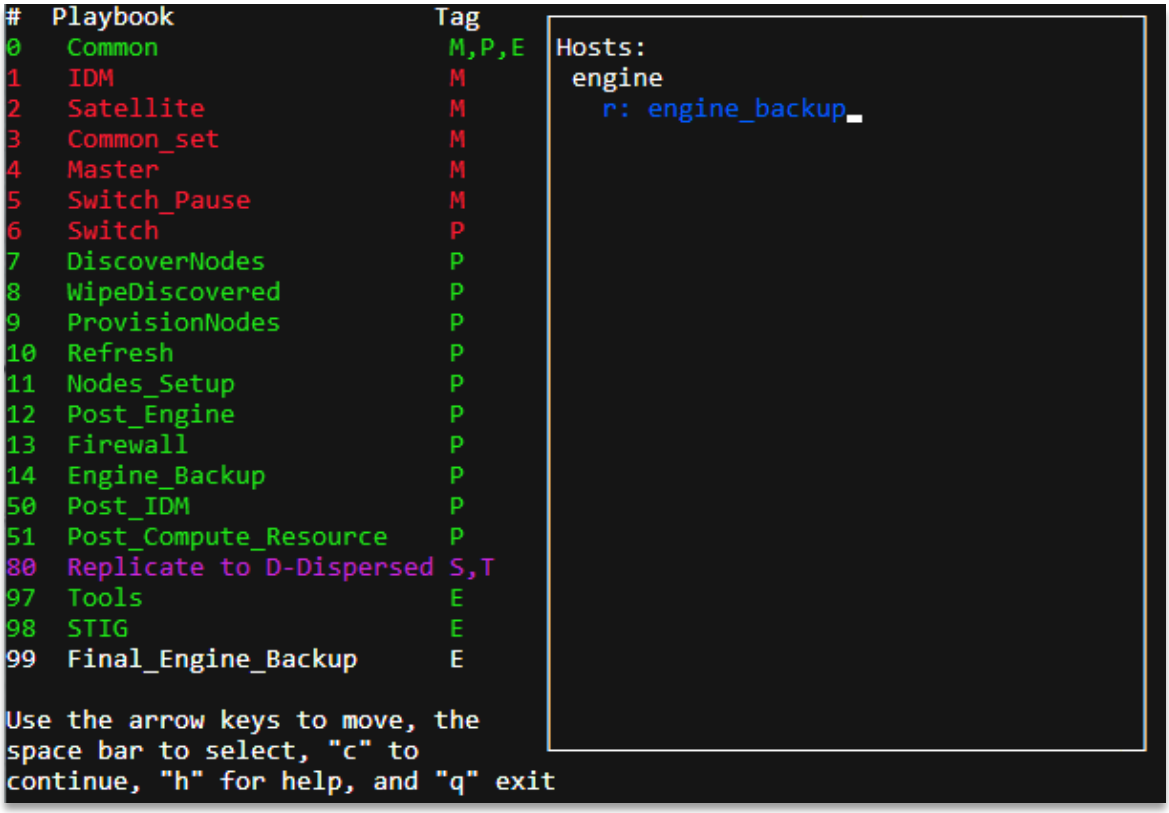
3. Enter the number of nodes currently in the RHEV cluster using the following command (where # is the number of nodes; 3 or 6):

✎ **Note**: Ensure that **ONLY** the required number of nodes are connected by ethernet cable (**IPMI**) or connected to a power source at this time.

```
[root@master ansible_main]# ./play.py -n #     (Replace # with cluster size)
```

4. Select the necessary operator playbooks by pressing [**SPACE**] to select playbooks **07 – DiscoverNodes** to **99 - Final_Engine_Backup**. Press [**c**] to continue.

✎ **Note**: Passwords must be changed every 60 days.



4.6.4 Play.py Provisioning Nodes

Reporting Issues with Node Deployments

Task completed by: **Operator (Optional During Kit Re-Deployment)**

The **Host-Based Error Retrieval Platform (HERP)** reporting tool will assist support personnel in resolving issues if a deployment fails for any reason. Collect any logs from the following directory.

1. Pre-Requisite:
    - Failure Condition impacting node deployment.
2. Navigate to **/root/HERP/**

```
[defender@master ~]$ sudo tmux
[root@master ~]# cd /root/HERP
[root@master ~]# ls
HERP_K150_collect_2022-04-11-17-51-32.tgz
```

✎ **Note**: To run HERP manually, navigate to **/opt/ddt/ansible_main** and execute the following syntax:

```
[defender@master ~]$ cd /opt/ddt/ansible_main
[defender@master ~]$ sudo ./play.py --herp
```

✎ **Note**: The HERP tool must complete the automated collection process. If this process is interrupted, it is possible that some log collection will not be available for review:

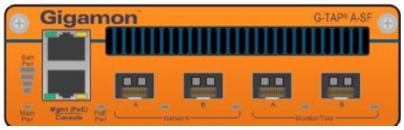
5 Appendix

5.1 Illustrated Reference

5.1.1 Visual Components Breakdown

This section serves to provide illustrative reference for the physical components included in DDS-M.

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
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

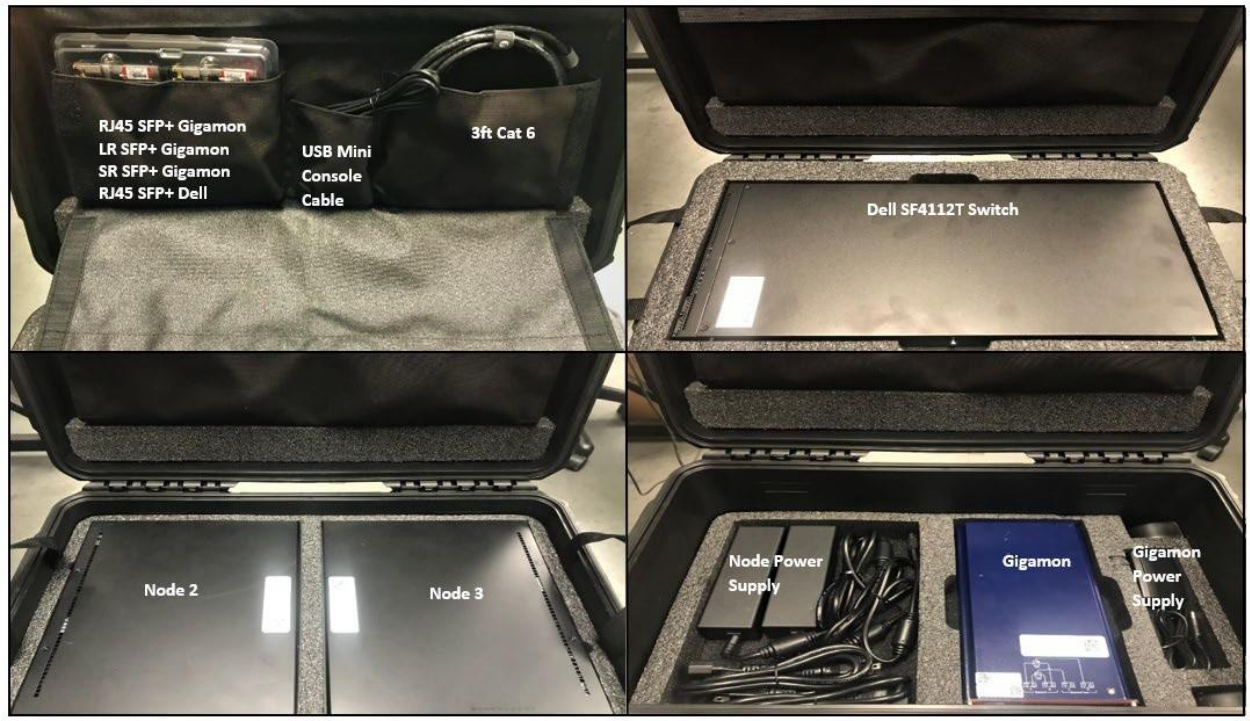
RJ45 SFP+ Module (DELL)		4
LR-Fiber SFP+ Module (DELL)		4
SR-Fiber SFP+ Module (DELL)		4
3.0 ft CAT 6e (Black)		9
6.0 ft CAT 6e (Black)		3
2.0m Ruggedized SM Fiber Cable		3
1.0m Ruggedized MM Fiber Cable		3

Dell 100G QSFP28 Cable		1
Sonnet 10Gbps SFP+ Thunderbolt Adapter		1
Backpack		1
SKB Fly Away Case		3

5.1.2 DDS-M Layout

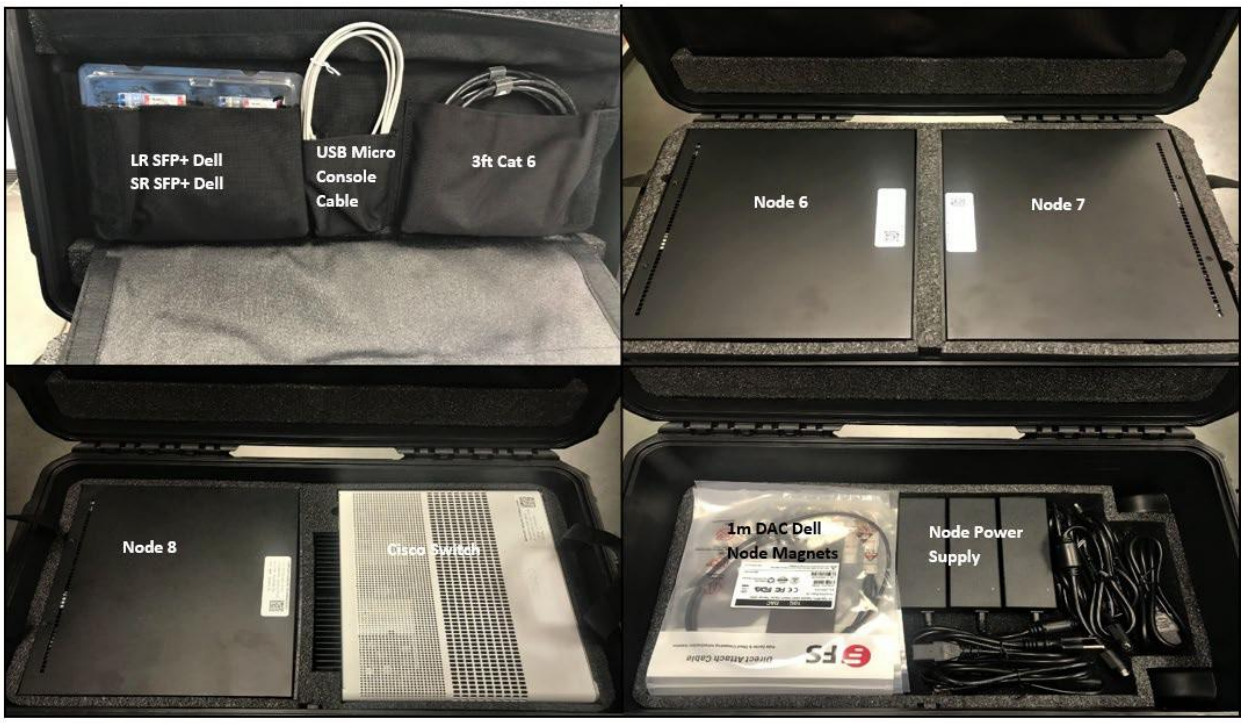
Each kit will include layout sheets similar to the images provided below. Refer to Section 4.2.1 (List of DDS-M Physical Components) when completing re-packing.

Case 1



Case 2

Case 3



Backpack

5.2 Equipment Check-Out Procedures (CPB)

✎ **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.

5.3 Use Cases

Scenario 1

Function:	DDS Modular
Technique:	Large Cloud Environment – infrastructure for virtualization
Description:	Deploy six (6) small form factor nodes in which each node is being used as both the hypervisor (host) and controller (storage) in a virtualization environment. Deploy two (2) small form factor nodes as network sensors to feed data back to the virtualization platform.
Primary / Secondary Actors:	DCO Forces
Objectives:	Deploy all required DCO tools for a small-medium sized network and have two network sensors feeding into the environment.
Preconditions:	An installation campus area network at a high-risk base, post, camp, or station with approximately 5,000 hosts and associated Layer 2,3,4 devices. Installation supports both business and military (phase I and II) operations.
Trigger:	In preparation for following actions, a DCO Force is tasked to perform (hasty response, proactive DCO, recon/counter-recon, or deliberate defense) on a designated network utilizing DCO-IDM methods.
Post-Conditions:	The DCO Force obtains detailed information about the specified AO and all terrain from which the enemy could influence the use of K-TC and tasked critical assets. Countermeasures are implemented that lead to the survivability of cyberspace capabilities.
Main Success Scenario:	Success is achieved upon the generation of a comprehensive virtualization infrastructure baseline environment on the defended network. Success Criteria 1 – DCO Force has full use of virtualization environment to deploy DCO capabilities in support of DCO-IDM mission. Success Criteria 2 – DCO Force has distributed network sensors deployed, which can be queried and controlled from the virtualization infrastructure. Success Criteria 3 – Virtualization environment is deployed in an almost 100% automated process. Success Criteria 4 – DCO Force can remotely access virtualization environment through VPN and/or MPLS network.
Notes:	

Scenario 2

Function:	DDS Modular
Technique:	Distributed sensor platform
Description:	Deploy eight (8) small form factor nodes as network sensors to perform distributed sensing of network data
Primary / Secondary Actors:	DCO Forces
Objectives:	Deploy all nodes as network sensors for a small-medium sized.
Preconditions:	An installation campus area network at a high-risk base, post, camp, or station with approximately 5,000 hosts and associated Layer 2,3,4 devices. Installation supports both business and military (phase I and II) operations.
Trigger:	In preparation for following actions, a DCO Force is tasked to perform (hasty response, proactive DCO, recon/counter-recon, or deliberate defense) on a designated network utilizing DCO-IDM methods.
Post-Conditions:	The DCO Force obtains detailed information about the specified AO and all terrain from which the enemy could influence the use of K-TC and tasked critical assets. Countermeasures are implemented that lead to the survivability of cyberspace capabilities.
Main Success Scenario:	Success is achieved upon the generation of a comprehensive distributed sensor platform on the defended network. Success Criteria 1 – DCO Force has distributed network sensors deployed, which can be queried and controlled. Success Criteria 2 – DCO Force can remotely access sensors through VPN and/or MPLS network.
Notes:	

Scenario 3

Function:	DDS Modular
Technique:	Hyper-converged cloud environment with distrusted sensor platform
Description:	Deploy 3 small form factor nodes in which each node is being used as both the hypervisor (host) and controller (storage) in a hyper converged virtualization environment. Deploy two (5) small form factor nodes as network sensors to feed data back to the virtualization platform.
Primary / Secondary Actors:	DCO Forces
Objectives:	Deploy all required DCO tools for a small-medium sized network on a virtualization platform with high availability and load balancing capabilities. Have two network sensors feeding into the environment.
Preconditions:	An installation campus area network at a high-risk base, post, camp, or station with approximately 5,000 hosts and associated Layer 2,3,4 devices. Installation supports both business and military (phase I and II) operations.
Trigger:	In preparation for following actions, a DCO Force is tasked to perform (hasty response, proactive DCO, recon/counter-recon, or deliberate defense) on a designated network utilizing DCO-IDM methods.
Post-Conditions:	The DCO Force obtains detailed information about the specified AO and all terrain from which the enemy could influence the use of K-TC and tasked critical assets. Countermeasures are implemented that lead to the survivability of cyberspace capabilities.
Main Success Scenario:	Success is achieved upon the generation of a comprehensive virtualization infrastructure baseline environment on the defended network. Success Criteria 1 – DCO Force has full use of hyper converged virtualization environment to deploy DCO capabilities in support of DCO-IDM mission. Success Criteria 2 – DCO Force has distributed network sensors deployed, which can be queried and controlled from the virtualization infrastructure. Success Criteria 3 – Virtualization environment is deployed in an almost 100% automated process. Success Criteria 4 – DCO Force can remotely access virtualization environment through VPN and/or MPLS network.
Notes:	

Scenario 4

Function:	DDS Modular
Technique:	Stacking multiple DDS
Description:	Deploy two DDS Modular systems as a single large virtualization environment with distributed network sensors.
Primary / Secondary Actors:	DCO Forces
Objectives:	Deploy all required DCO tools for a medium-large sized network on a virtualization platform with high availability and load balancing capabilities. Have four network sensors feeding into the environment.
Preconditions:	An installation campus area network at a high-risk base, post, camp, or station with approximately 5,000 hosts and associated Layer 2,3,4 devices. Installation supports both business and military (phase I and II) operations.
Trigger:	In preparation for following actions, a DCO Force is tasked to perform (hasty response, proactive DCO, recon/counter-recon, or deliberate defense) on a designated network utilizing DCO-IDM methods.
Post-Conditions:	The ARMY DCO Force obtains detailed information about the specified AO and all terrain from which the enemy could influence the use of K-TC and tasked critical assets. Countermeasures are implemented that lead to the survivability of cyberspace capabilities.
Main Success Scenario:	Success is achieved upon the generation of a comprehensive virtualization infrastructure baseline environment on the defended network. Success Criteria 1 – DCO Force has full use of virtualization environment to deploy DCO capabilities in support of DCO-IDM mission. Success Criteria 2 – DCO Force has distributed network sensors deployed, which can be queried and controlled from the virtualization infrastructure. Success Criteria 3 – Virtualization environment is deployed in an almost 100% automated process. Success Criteria 4 – DCO Force can remotely access virtualization environment through VPN and/or MPLS network.
Notes:	

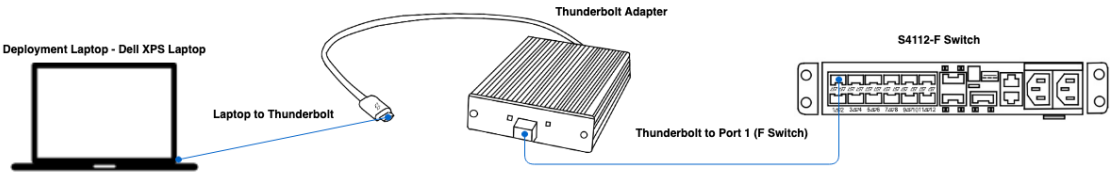
5.4 Additional Procedures

5.4.1 Reconfigure the Deployment Laptop for 10gig Operations TOC

Scenario: **Operational Re-Configuration**

✎ Note: The following procedure will reconfigure the deployment laptop's primary network interface to use interface **p11p1** and the SONNET thunderbolt adapter.

Cables Needed for F-Switch Connections
(1) SFP DAC 3m Cable – indicated by the blue line
(1) SONNET 10gig Thunderbolt Adapter



5.4.1 Sonnet Thunderbolt Adapter

1. Using an **SFP DAC** cable, connect the **Thunderbolt** adapter to **Port 1** on the **S4112-F** switch. Connect the **Thunderbolt** cable from the SONNET adapter to the **Deployment Laptop**.
2. Connect the SONNET Thunderbolt adapter to the interface on the left lower panel of the laptop. Ensure the SFP+ interface is connected to an appropriate network interface.
3. Open a terminal window and perform the following steps.

```
[defender@master ~]$ sudo ifdown em1
[defender@master ~]$ cd /etc/sysconfig/network-scripts
[defender@master ~]$ sudo mv ifcfg-em1 .ifcfg-em1
[defender@master ~]$ sudo cp .ifcfg-em1 ifcfg-p11p1
[defender@master ~]$ sudo sed -i 's/em1/p11p1/g' ifcfg-p11p1
[defender@master ~]$ sudo ifup p11p1
```

4. Verify that connectivity lights are green and blinking on the SONNET 10G thunderbolt adapter.

5. Test gateway connectivity by executing the following command in a terminal window:

✎ **Note**: The following **br-ex** configuration is present if **play.py** playbooks 1-5 have successfully completed and the Satellite, IDM, and IDM2 virtual machines are correctly configured. Playbook tasks 1-7 are completed by Armory Personnel prior to issuing the DDS kit. The Operator should never execute playbook tasks 1-5 during operational deployment of the DDS kit.

6. Verify bridged interface configuration in a terminal window:

```
[defender@master ~]$ sudo brctl show
 bridge name  bridge id             STP enabled     interfaces
 br-ex        8000.52540072a6ec     no               p11p1
                                                     vnet0
                                                     vnet1
                                                     vnet2
```

7. The interface **p11p1** should be present in the bridge configuration for **br-ex**. If not present type:

```
[defender@master ~]$ sudo brctl addif br-ex p11p1
```

5.4.2 Verify Deployment Laptop License Enrollment

Scenario: play.py (Kit Troubleshooting or Re-Deployment Procedures)

✎ **Note**: The following steps are applicable if the Deployment Laptop is fully provisioned and is connected to the DDS-M kit internal environment.

1. Verify current host enrollment:

```
[defender@master ~]$ sudo subscription-manager list --consumed
```

Verify in output that Subscription Name is "**Red Hat Cloud Suite Premium (2 Sockets, 32 Cores)**" and that *Status Details* shows "**Subscription is current**". If the system is not entitled correctly, execute the following commands:

2. Open Firefox and navigate to: **`http://satellite.[kit number]cpt.cpb.mil/pub/`**
3. Save the following file to the Downloads directory:

`http://satellite.[kit number]cpt.cpt.mil/pub/katello-ca-consumer-latest.noarch.rpm`

4. On command line type:

```
[defender@master ~]$ sudo yum install ~/Downloads/katello-ca-
consumer-latest.noarch.rpm

[defender@master ~]$ sudo subscription-manager register --
org="[kit number]cpt" --activationkey="RHVH_AK" --force

The system has been registered with ID: [UUID]
The registered system name is: master25.25cpt.cpb.mil
```

5.4.3 Enable Sharding in the Gluster File System

To efficiently store very large files (virtual machine disks) that span bricks (the basic unit of storage), the Shard Translator feature must be enabled. By default, *sharding* should be enabled. To enable it, perform the following steps:

✎ **Note**: Before continuing, ensure all virtual machines in the domain *vmstore* are powered off. The Palo Alto Virtual Firewall is an example of a virtual machine that must be powered off during this step. Hosted Engine does not need to be powered off as it runs from the hosted_storage domain.

1. From a terminal window on the **Deployment Laptop**, execute the following commands to determine if sharding is currently enabled:

```
[defender@master ~]$ sudo ssh node0
[root@node0 ~]# gluster volume info vmstore | grep shard
```

Output if sharding is enabled:

```
features.shard: on
```

2. To enable sharding, while connected to node0 execute the following command:

```
[root@node0 ~]# gluster volume set vmstore features.shard on
```

3. To verify that sharding is enabled, while connected to node0 execute the following command:

```
[root@node0 ~]# gluster volume info vmstore | grep shard
features.shard: on
```

Sharding is now enabled as described in Step 1.

5.4.4 Configure VM Interface Mirror or Passthrough

Advanced Features of oVirt Networks:

- Passthrough
- Port Mirroring

Passthrough enables a vNIC to connect directly to a Virtual Machine's internal network function. This feature reduces packet loss and memory overhead for large packet operations.

Port Mirroring will copy all visible Layer 3 traffic to a configured virtual machine. Use this feature to enable promiscuous mode for a sensor.

To enable *Port Mirroring* in a specific virtual machine.

1. Open Firefox and navigate to **`https://engine.[kit number]cpt.cpb.mil`**
2. Log in using the '**admin**' username to the '**internal**' domain.
3. Select **Compute -> Virtual Machines**.
4. Click the virtual machine name to enter the details view.
5. Click '**Shutdown**' and ensure the virtual machine has completed the power OFF tasks.
6. Select the tab labeled **Network Interfaces** and select an interface to edit.
7. Click '**Edit**'.
8. Change the '**Profile**' entry to '**Mirror_Port(SPAN)**' to enable port mirroring on that interface.
9. Click '**OK**' and then power ON the virtual machine. Verify that all expected span (mirror) traffic is visible.

5.4.5 Configure Trunking on the S4112 Series Switches

Scenario: Trunk connections supplying service to Nodes in the DDS-Modular system are pre-configured to support only limited kit internal networks.

Requirement: Assign trunked configurations that support `VLANs 52-54, 100-102` and Access interfaces as necessary.

Steps:

1. Connect to the switch by either an SSH or minicom (Console) session.

✎ **Note**: Screen is deprecated on RHEL 8. Minicom is the replacement for Screen. See **section 11.1.4** on Minicom on how to utilize the program.

2. Issue the following commands:

```
configure terminal
interface range ethernet 1/1/13:1-1/1/14:4
switchport trunk allowed vlan 52-54,100-102
end
write
```

3. Verify the configuration lists 1/1/13:1-4, 1/1/14:1-4 on `VLANS 52-54, 100-102`:

```
show vlan
```

4. Verify the interface configurations in an operating and connected status:

```
show ip interface brief
```

5. Verify the current global configuration by reviewing the updated ethernet 1/1/13 and 1/1/14 range of configurations:

```
show running-configuration
---- Alternate Syntax ----
show running-configuration interface ethernet 1/1/13:1
```

5.4.6 Configure Network Time Protocol from an Offline State

Scenario: DNS Time Synchronization using the CHRONY Daemon Service on Linux systems has an integrated maximum tolerance for time drift of ten (10) minutes.

Requirement: Issue the correct commands to re-establish time synchronization from a stale state.

Hosts:

- Satellite
- Deployment
- Laptop Nodes 0-5

Steps:

1. Connect to **EACH** system by remote SSH connection as the root user.

```
[defender@master ~]$ sudo ssh node0
```

2. Set Time to UTC.

```
[defender@master ~]$ timedatectl set-timezone UTC
```

3. Issue the following command:

```
[defender@master ~]$ sudo systemctl stop chronyd
```

4. Enter and edit the chrony file:

```
[root@node0 ~]# vim /etc/chrony.conf
```

5. Add the server information to chrony.conf and remove any references to non-kit servers.
    - Server 10.KITNUM.51.10 iburst
    - Server 10.KITNUM.51.11 iburst

6. Save the changes to chrony.conf

```
:wq
```

7. Sync the time.

```
[root@node0 ~]# systemctl start chronyd
[root@node0 ~]# chronyc -a 'burst 4/4'
[root@node0 ~]# chronyc -a makestep
```

8. To verify that the IDM time is correct, SSH into IDM.
9. Issue the following command:

```
[root@idm ~]# date
```

✎ **Note**: To ensure that the time is displayed in UTC, simply add "--utc" after date

5.4.7 Restore IDM (Corrupted ldf file)

Scenario: After rebooting the master laptop, all 3 VMs(Satellite, IDM, IDM2) on master laptop are running and Satellite's web service is available, but IDM web service is not accessible.

Steps:

1. Connect to IDM by SSH session.
2. Issue the following command to restart IDM services:

```
[root@idm ~]# systemctl restart ipa
```

3. Check the status of IDM services:

```
[root@idm ~]# ipactl status
```

4. The following output indicates the IDM web service should be accessible again.

```
Directory Service: RUNNING
krb5kdc Service: RUNNING
kadmin Service: RUNNING
named Service: RUNNING httpd
Service: RUNNING

ipa-custodia Service: RUNNING
ntpd Service: RUNNING

pki-tomcatd Service: RUNNING
ipa-otpd Service: RUNNING

ipa-dnskeysyncd Service: RUNNING

ipa: INFO: The ipactl command was successful
```

5. However, the following message suggests critical files required by IDM have been corrupted due to improper shutdown of the VM.

```
Directory Service: STOPPED

Directory Service must be running in order to obtain status of other
services
```

✎ **Note**: IDM can be restored by following the procedures below, but the system date will be reverted and unknown/unexpected authentication errors may occur.

6. Change the current directory to /etc/dirsrv/slapd-<kit_num>CPT-CPB-MIL/ **(Replace <kit_num> with DDS kit number)**

```
[root@idm ~]# cd /etc/dirsrv/slapd-#CPT-CPB-MIL
```

7. Delete the corrupted backup file and copy the old configuration file.

```
[root@idm's slapd-#CPT-CPB-MIL]# rm -f dse.ldif.bak
[root@idm's slapd-#CPT-CPB-MIL]# cp dse.ldif.startOK dse.ldif.bak
```

8. Restart IPA service as described in **Step 2** and check its status using the 'ipactl status' command from **Step 3**. If output shows all services *RUNNING* as in **Step 4** IDM has been restored using the backup configuration.

5.4.8 Replacement of License Manifests in Red Hat Satellite

Scenario: When license allocations for Red Hat Products have expired, the following procedures will import a refreshed manifest and re-subscribe all relevant hosts.

Requirement: Updated manifest.zip.

1. Enable USB temporarily on the Deployment Laptop:
   - Use vi, vim, gedit, or nano to edit the following files:

```
[defender@master ~]$ sudo nano /etc/modprobe.d/blacklist.conf
[defender@master ~]$ sudo nano /etc/modprobe.d/usb-storage.conf
```

   - Place a '#' symbol in front of all '**usb-storage**' modules and save the change.
   - Load the **usb-storage** module:

```
[defender@master ~]$ sudo modprobe usb-storage
```

2. Connect a USB device containing the updated **manifest.zip**. Permit the device using '**usbguard**' (In this example, the USB Mass Storage device is #17)

```
[defender@master ~]$ usbguard list-devices
17: allow id 058f:6387 serial "########" name "Mass Storage"
[defender@master ~]$ sudo usbguard allow-device 17
```

3. Locate the manifest and copy to destination server:

```
[defender@master ~]$ sudo scp /run/media/defender/media/manifest.zip
satellite:/tmp/ .
```

4. Connect to the **satellite** server via SSH as the root user:

```
[defender@master ~]$ sudo ssh satellite
```

5. List the current manifest history:

```
[root@satellite ~]# hammer subscription manifest-history --organization-id 1
```

✎ **Note**: For all following tasks, replace **#cpt** with the kit number determined in Step 4 (example: 1cpt)

6. List the current manifest and verify the "Cloud Suite" subscriptions are no longer listed:

```
[root@satellite ~]# hammer subscription list --organization-label #cpt
```

7. Delete the current manifest:

```
[root@satellite ~]# hammer subscription delete-manifest --organization-id 1
```

8. Replace the manifest:

```
[root@satellite ~]# hammer subscription upload --file /tmp/manifest.zip --
organization-label #cpt --repository-url
"http://sat.forgedev.dco.mil/pub/exports/Library/"
```

9. Verify that the Manifest is successfully imported and Cloud Suite licenses are available:

```
[root@satellite ~]# hammer subscription list --organization-label #cpt
```

10. Re-subscribe the listed hosts in the following order by SSH root level connection:
- Master Deployment Laptop
- Satellite
- IDM
- IDM2

```
[root@satellite ~]# subscription-manager register --org="#cpt" --
activationkey="RHVH_AK" --force
```

11. If **RHV-H Nodes** are currently deployed, open the Firefox internet browser and complete the following steps:
    - Navigate to **`https://satellite.[kit number]cpt.cpb.mil`**
    - Select: **Content -> Content Hosts**. Enter 'node' in the filter box and Search.
    - Select the checkbox for all nodes in the matching results.
    - Select the right-hand dropdown to **Select Action -> Manage Subscriptions**.
    - Select the Cloud Suite license 'Physical' allocation checkbox.
    - Select **Done**.

12. Replace the source manifest on the Deployment Laptop:

```
[defender@master ~]$ sudo cp /run/media/defender/media/manifest.zip
/root/licenses/red_hat/manifest.zip
```

- Use vi, vim, gedit, or nano to edit the following files:

```
[defender@master ~]$ sudo nano /etc/modprobe.d/blacklist.conf
[defender@master ~]$ sudo nano /etc/modprobe.d/usb-storage.conf
```

- Remove the '#' symbol in front of all 'usb-storage' modules and save the change.

5.4.9 Reconfigure Routing Management on Dell S4112 Series Switches

Scenario: Routing operations must be currently redirected to the Palo Alto virtual Firewall after the initial deployment of the DDS-M systems. Follow these instructions to update the interface configurations on `VLAN Interface 51-53` and `Management Interface 1/1/1` on the S4112T and S4112F switches.

Cables Needed for Switch Connections	
(2) USB to Micro-USB Cables	
Index	IP Address
S4112F	10.[kit number].51.251/24
S4112T	10.[kit number].51.252/24

1. Perform the following procedure on the first switch.

✎ **Note**: Adjust the minicom profile from **dell0** to **dell1** if using the second USB cable connected to the **Deployment Laptop**.

- Open a new terminal window on the **Deployment Laptop** and type:

```
[defender@master ~]$ sudo minicom dell0
```

- Login using *switch_admin* credentials from **passwords.yml** and issue the following commands:

```
switch# configure terminal
switch(config)# interface range vlan 51-53
switch(conf-range-vl-51-53)# no ip address
switch(conf-range-vl-51-53)# exit

switch(config)# interface mgmt1/1/1
switch(conf-if-ma-1/1/1)# no ip address dhcp
switch(conf-if-ma-1/1/1)# ip address ##.##.##.###/##
switch(conf-if-ma-1/1/1)# end

switch# write
switch# exit
```

- Exit the screen session by pressing [**CTRL+A**] then [**:**] and typing **quit** in the input box and [**ENTER**].

2. Repeat Step 1 on the second switch.

3. Verify connectivity by issuing the following commands from a terminal session:

✎ **Note**: The ping/pong result will be delayed for a few seconds while the system refreshes its ARP cache entries.

```
[defender@master ~]$ ping -c 10 10.[kit number].51.1
64 bytes from 10.2.51.1: icmp_seq=1 ttl=64 time=0.299 ms

[defender@master ~]$ ping -c 10 10.[kit number].51.251
64 bytes from 10.2.51.251: icmp_seq=1 ttl=64 time=0.299 ms

[defender@master ~]$ ping -c 10 10.[kit number].51.252
64 bytes from 10.2.51.252: icmp_seq=1 ttl=64 time=0.299 ms
```

Additional Information
In some limited circumstances it may be necessary to reapply the gateway interface configuration. If advised, perform the procedures below:

4. Connect to the USB0 console connection as directed in Step 1 above.

```
switch# configure terminal
switch(config)# interface mgmt1/1/1
switch(conf-if-ma-1/1/1)# no ip address
switch(conf-if-ma-1/1/1)# exit

switch(config)# interface vlan 51
switch(conf-if-vl-51)# ip address 10.[kit number].51.1/24
switch(conf-if-vl-51)# exit

switch(config)# interface vlan 52
switch(conf-if-vl-52)# ip address 10.[kit number].52.1/24
switch(conf-if-vl-52)# exit

switch(config)# interface vlan 53
switch(conf-if-vl-53)# ip address 10.[kit number].53.1/24
switch(conf-if-vl-53)# end

switch# write
switch# exit
```

5.4.10 CPB Operational Playbook Extension (COPE)

Scenario: play.py (Kit Software Deployment)

COPE is an automation system that supports deployment of existing tools provided with the DDS-M system.

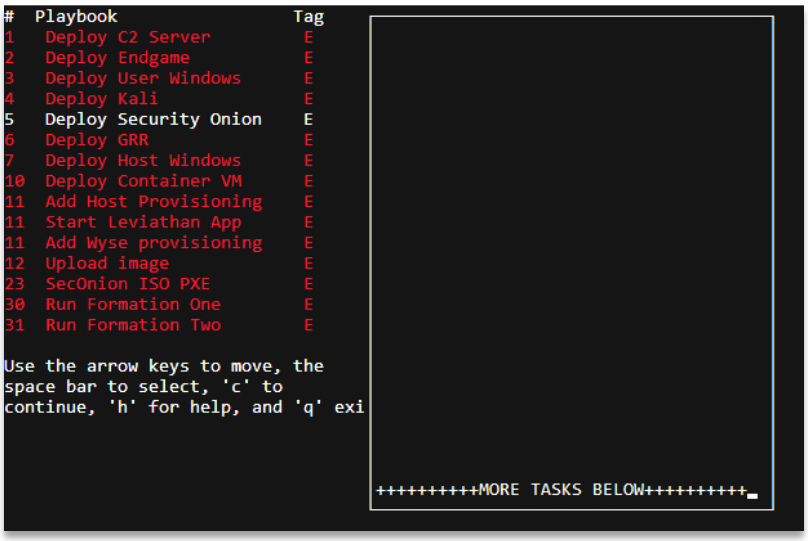
✎ **Note**: The following steps are applicable if the Deployment Laptop is fully provisioned and is connected to the DDS-M kit internal environment.

1. Verify that COPE is listed as an available extension:

```
[defender@master ~]$ sudo ./play.py -l

Installed extensions: cope
```

2. Run the COPE extension:

```
[defender@master ~]$ sudo ./play.py -c cope
```



5.4.10 COPE Playbook Selection Menu

3. Select a desired playbook and press '**c**' to continue. See below for additional tool supporting information.

Available Dashboards

Leviathan: **https://10.[kit number].51.123:8443**

Garden: **https://garden.<kitnum>cpt.cpb.mil:9090** or **https://10.[kit number].51.123:9090**

Deployed Host IP Addresses

Deployed Host	Host IP
#1 C2 Server	10.[kit number].54.10
#2 Endgame	10.[kit number].101.12
#3 User Windows	10.[kit number].101.13
#4 Kali	10.[kit number].101.11
#5 Security Onion	10.[kit number].102.10
#6 GRR	10.[kit number].101.10
#7 Host Windows	10.[kit number].54.10
#10 Container VM	10.[kit number].51.123

For further information on the Container VM platform, refer to the User Manual located in **/opt/extensions/cope/doc.**

For further assistance, contact the Networking, Engineering, Research, and Development team at **706-791-7117**.

5.4.11 Short Circuit (Operator Focused Site Reliability Script)

Short Circuit is designed to enable automatic collection of diagnostic information for the purposes of troubleshooting issues with DDS-M operational configurations.

✎ **Note**: The following steps are applicable if the Deployment Laptop is fully provisioned and is connected to the DDS-M kit internal environment.

1. Run **Short-Circuit** without any arguments to see list of available arguments:

```
[defender@master ~]$ sudo /opt/short-circuit/sccli
```

2. Build inventory by listing known hosts:

```
[defender@master ~]$ sudo /opt/short-circuit/sccli list
```

3. Run scan to perform diagnostics on host.

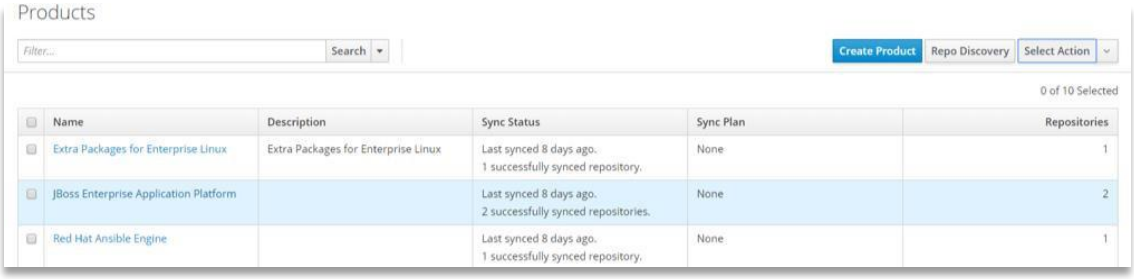
```
[defender@master ~]$ sudo /opt/short-circuit/sccli scan <Host_Name>
```

✎ **Note:** Reports are stored under /opt/short-circuit/data/artifacts.

For further assistance, contact the Networking, Engineering, Research, and Development team at **706-791-7117**.

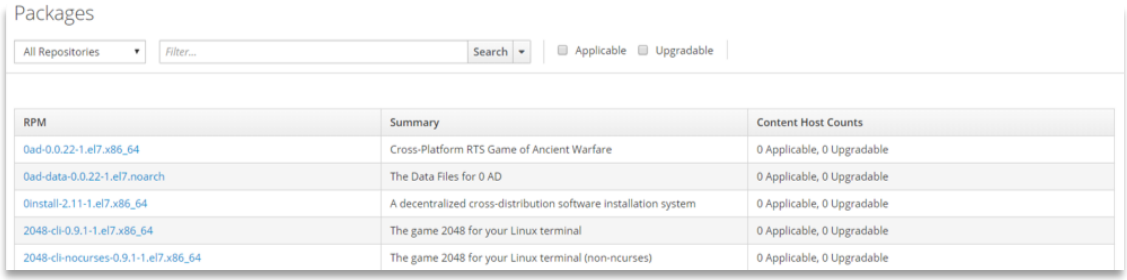
5.4.12 Managing repository packages via Satellite

To view the Red Hat products provided by the imported subscriptions, log in to Satellite and click on **Content > Products**.



5.4.12(a) Satellite Products

Finally, to view individual packages provided by the repositories, log in to Satellite and click on **Content > Packages**. Clicking on individual packages will give more details and indicate what repository they belong to.



5.4.12(b) Satellite Packages

Remove packages via DNF

```
# dnf remove <pkg name>
```

Install packages via DNF

```
# dnf install <pkg name>
```

Search packages via DNF

```
# dnf search <pkg name>
```

Enable modules via DNF

```
# dnf module --enable <module name>
```

For further assistance, contact the Networking, Engineering, Research, and Development team at **706-791-7117**.

5.4.13 FML Drive build and Deployment process

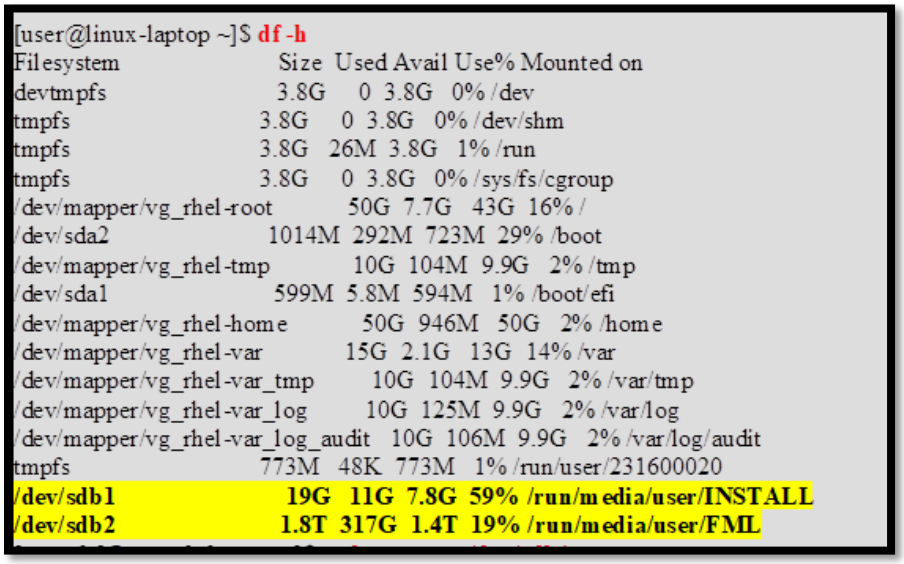
The Full Mission Loadset (FML) is a USB drive that includes everything needed to fully deploy a DDS-M kit. DDS-M FML drive testing is conducted within **3** days of a new DDT version moving to production. Testing includes the same procedures as a forge deployment.

To build an FML drive, you must use a computer connected to the Forge infrastructure and have a 1TB or larger USB drive.

1. Connect the drive to the laptop connected to the Forge infrastructure
2. Identify the drive mapping assigned by the computer to the drive
3. Open an elevated command prompt and type # **df -h**

```
[user@linux-laptop ~]$ df -h
```

Take note of the name assigned by Linux to the USB drive. It should be something similar to: **/dev/sd[a-z]**



5.4.13(a) df -h command

4. Unmount the drive to prepare it for formatting and imaging by going to an elevated prompt and typing **umount /dev/sd[a-z]**

```
[user@linux-laptop ~]$ sudo umount /dev/sdb*
```

Ensure that the previously identified drive has been unmounted correctly by validating again with the command # **df -h**

```
[user@linux-laptop ~]$ sudo umount /dev/sdb*
[sudo] password for user:
umount: /dev/sdb: not mounted.
[user@linux-laptop ~]$ df -h
Filesystem                  Size  Used Avail Use% Mounted on
devtmpfs                    3.8G     0  3.8G   0% /dev
tmpfs                       3.8G     0  3.8G   0% /dev/shm
tmpfs                       3.8G   26M  3.8G   1% /run
tmpfs                       3.8G     0  3.8G   0% /sys/fs/cgroup
/dev/mapper/vg_rhel-root     50G  7.7G   43G  16% /
/dev/sda2                  1014M  292M  723M  29% /boot
/dev/mapper/vg_rhel-tmp      10G  104M  9.9G   2% /tmp
/dev/sda1                  599M  5.8M  594M   1% /boot/efi
/dev/mapper/vg_rhel-home     50G  946M   50G   2% /home
/dev/mapper/vg_rhel-var      15G  2.1G   13G  14% /var
/dev/mapper/vg_rhel-var_tmp  10G  104M  9.9G   2% /var/tmp
/dev/mapper/vg_rhel-var_log  10G  125M  9.9G   2% /var/log
/dev/mapper/vg_rhel-var_log_audit  10G  108M  9.9G   2% /var/log/audit
tmpfs                       773M   48K  773M   1% /run/user/231600020
```

5.4.13(b) umount and df -h command

5. Run the podman container to start the format and imaging process.
   # **podman run --rm --privileged -ti harbor.forgedev.dco.mil/act/fml:1.8.2 /dev/sd<X>**

```
[user@linux-laptop ~]$ sudo -i
[root@linux-laptop ~]# podman run --rm --privileged  -ti harbor.forgedev.dco.mil/act/fml:1.8.2 /dev/sdb
```

✎ **Note:** Ensure the DDT build version matches the current production DDT version (1.8.2 in the example) and the correct dev/sd[a-z].

6. You will be prompted to confirm the drive. Type **YES** and press enter if correct.

```
WARNING: This will modify partition tables, if YOU select the wrong drive...
You selected: /dev/sdf
Are you sure this is the right drive? [YES]
```

5.4.13(c) Confirmation screen

✎ **Note:** This operation will modify partition tables. It is critical to select the correct drive partition.

7. Wait approximately 3 hours for the build process to complete, unmount the FML drive and exit.

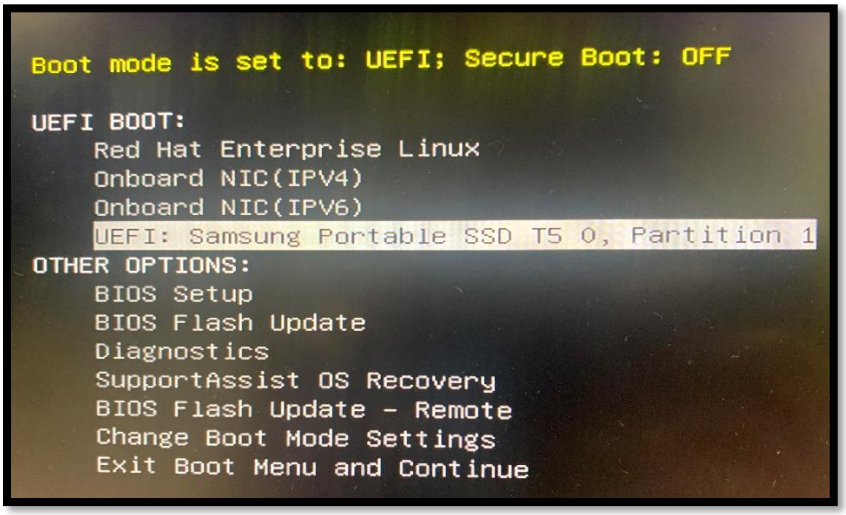
```
Are you sure this is the right drive? [YES] YES

umount: /dev/sdg: not mounted.
umount: /dev/sdg1: not mounted.
umount: /dev/sdg2: not mounted.
Warning: The resulting partition is not properly aligned for best performance: 1953s % 65535s != 0s
mkfs.fat 4.2 (2021-01-31)
mke2fs 1.46.3 (27-Jul-2021)
Creating filesystem with 483484462 4k blocks and 120872960 inodes
Filesystem UUID: 82472799-0a13-4f0b-81de-293a50c0ae5a
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000, 7962624, 11239424, 20480000, 23887872, 71663616, 78675968,
    102400000, 214990848

Allocating group tables: done
Writing inode tables: done
Creating journal (262144 blocks): done
Writing superblocks and filesystem accounting information: done

Building INSTALL Partition
No cache, trying to download
9.93GiB 0:01:11 [ 142MiB/s] [==========================================================================
Building FML Partition
No cache, trying to download
 359GiB 0:21:43 [ 282MiB/s] [==========================================================================
Flushing, and unmounting
Writing key e3b0c44298fc1c
Setting boots: 0
```

5.4.13(d) Screen showing completed process

8. Plug in the FML drive to master laptop and power-on the laptop

9. Press F12 at the Dell logo and ensure the "Preparing one-time boot menu" appears

10. Select your FML drive to boot from it

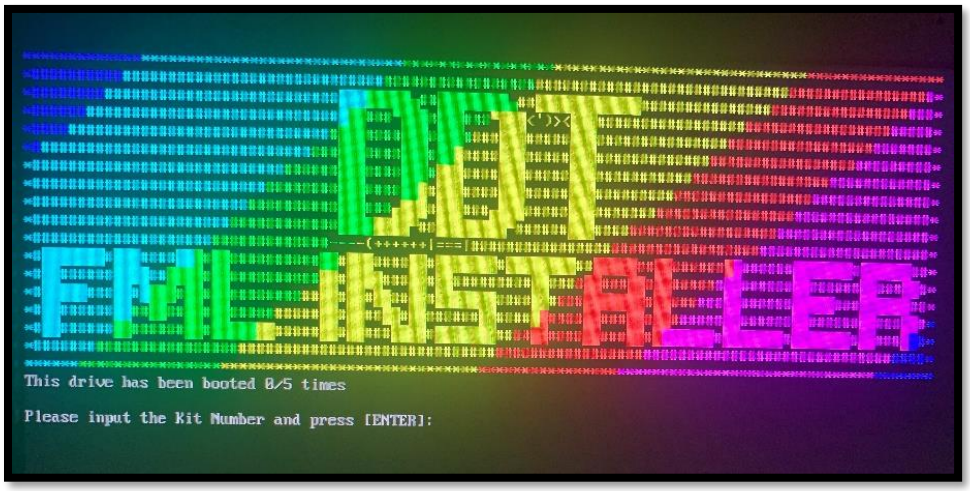


5.4.13(e) Selecting boot drive

11. Ensure the correct version is displayed: FML: Install DDT VX.X.X appears

5.4.13(f) Verifying correct deployment version

12. Enter the kit number when prompted



5.4.13(g) Enter correct kit number

Once the master laptop boots to the RHEL account login, you can log in and further track and continue the deployment process starting at **section 4.6.2** "Performing ONIE install".

For further assistance, contact the Networking, Engineering, Research, and Development team at **706-791-7117**.

DDS-M Kit
DDT Software Administration Manual

May 2023 Revision 19

Foreword

Introduction

The Deployable Defensive System (DDS) is a modular fly-away computing cluster that is purpose-built for conducting Defensive Cyber Operations (DCO) missions. This kit provides a platform with hardware and software for the US Army and their DoD mission partners. A standard DDS kit consists of 3 cases, 3 switches, 8 servers, a network tap, a crash cart adapter, and network cables provided for various connectivity scenarios.

✎ **Note**: The crash cart adapter turns the laptop into a portable console for accessing servers. It allows for transferring files from the laptop to the server, capturing screenshots of server configurations, error messages, and activity for faster troubleshooting.

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.

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)

6 Introduction to DDT

DDT (Deployable DCO Tool), formerly known as Project CURE, is a solution built by the Cyber Protection Brigade (CPB) Networking, Engineering, Research and Development (NERD) Cell in order to automate the deployment of the DDS kits. For administration purposes, DDT software can be defined in the following:

Operating System Administration
Master Laptop Infrastructure Services Administration
Virtualization Administration
Storage Administration
Firewall Administration

7 Operating System Administration

DDT is based on Red Hat Enterprise Linux (RHEL), a lightweight, enterprise-supported Linux Operating System (OS) developed by Red Hat. This OS gives users the flexibility of the Linux environment while also maintaining a level of support, security, and stability for production purposes.

7.1 Common Administration Commands

When using RHEL, there are many commands, concepts, and tools to familiarize yourself with as operators. These commands will be common across RHEL and RHVH Operating Systems. However, other distributions of Linux may vary. This section contains a list of commands related to common administration tasks that operators may need to perform.

7.1.1 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
`subscription-manager [command]`	Interact with Red Hat Network (RHN) for subscriptions, repositories, and licensing information
`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

7.2 User Management

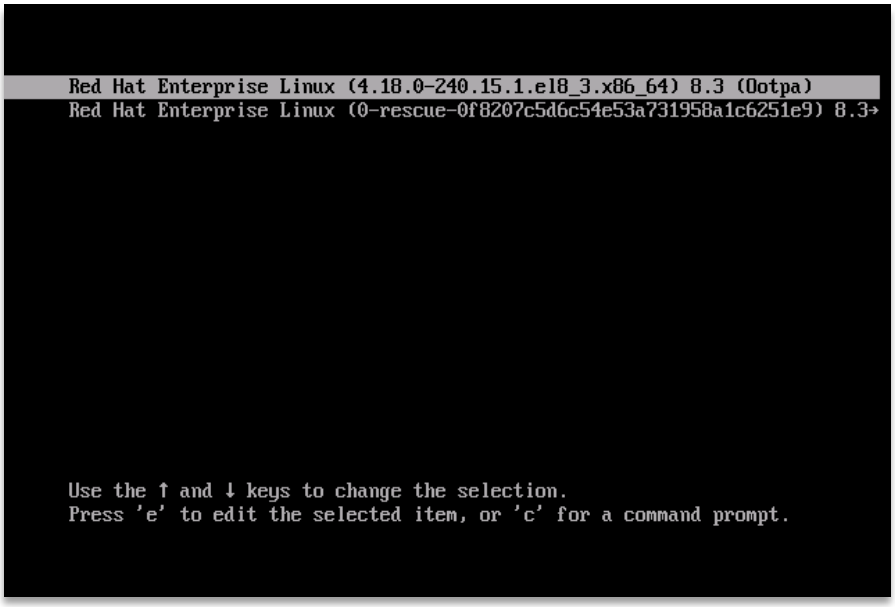
User and password management is critical for maintaining kit operations and access to all infrastructure, services, and tools. Passwords for all infrastructure and services deployed by DDT automation are stored in **/opt/ddt/ansible_main/passwords.yml.**

Most users should be managed within IdM to enable authentication across the cluster. Operators should not change local user passwords or application passwords unless necessary; they are randomly generated upon install. However, the loss of a root password requires a specific set of tasks to recover.

7.2.1 Reset Root Password

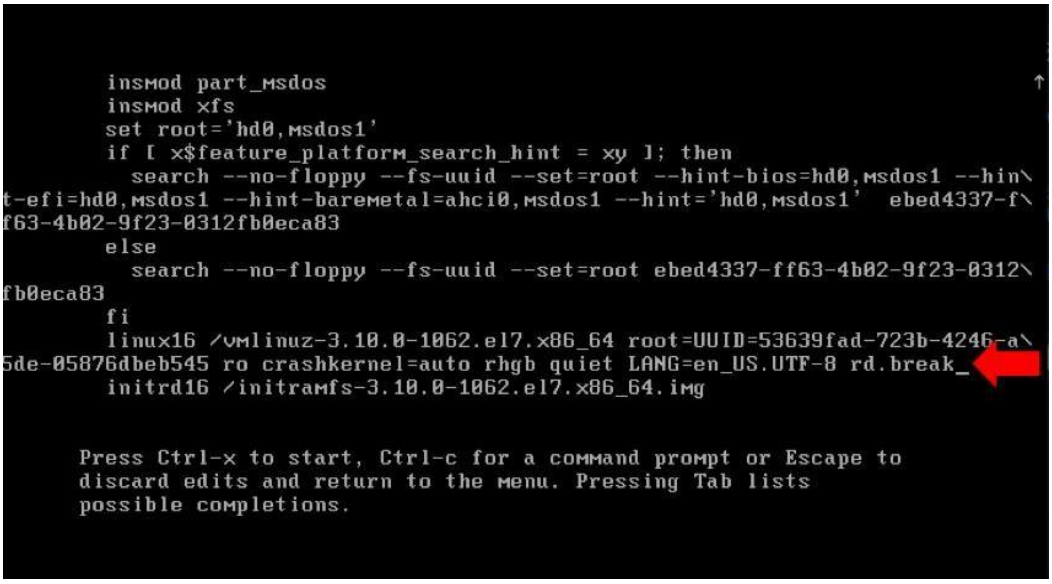
If the root password is known, simply login as root and use the **passwd** command to enter a new root password. However, if the root password is lost, create a new one by doing the following:

1. Reboot or power on the system and press '**e**' to edit the installed OS bootloader, (1st boot option), when the boot menu displays



7.2.1(a) Master Laptop Boot Menu

2. Towards the bottom of the page, locate the grub options (indicated by the 'linux16 /vmlinuz-\<kernel>' precursor) and add the rd.break option to the end of the line. This will allow edits to the initial ramdisk (initrd) environment.



7.2.1(b) Master Laptop Grub

3. Press **Ctrl-x** to boot with the added options allowing access to a root shell within **initramfs**.
4. Once the shell starts, remount the **/sysroot** partition with read/write permissions. (It is currently mounted with read-only permissions):

```
switch_root:/# mount -o remount,rw /sysroot
```

5. After the partition is remounted, change the root directory of the process to **/sysconfig** with the chroot command:

```
switch_root:/# chroot /sysroot
```

6. Reset the root user password.

⚠ **Warning**: **DO NOT REBOOT! The next step is vital to maintaining a working system.**

7. By default, SELinux is running and will need to be updated after the password has been created. To fix the **/etc/shadow** file, enter the following command:

```
sh-4.2# touch /.autorelabel
```

8. Finally, exit the chroot and initram shells. Login with the new root password after the host boots into RHEL.

```
sh-4.2# exit
exit
switch_root: /# exit
logout
```

7.3 Network Management

Networking is a vital part of the RHEL OS and can be configured numerous ways. DDT uses a mixture of bridges, subnets and VLANs to separate network traffic into different areas. The most common administrative tasks are described below.

7.3.1 Viewing IP Address Information

1. o 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
```

7.3.2 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!

7.4 Partitions & File Systems: Mounted/Unmounted

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 such as Gluster.

1 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
```

7.4(a) Parted Disk Information

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
```

7.4(b) lsblk Output

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**.

7.5 Security Enhanced Linux

Security-Enhanced Linux (SELinux) is a Mandatory Access Control (MAC) security mechanism built into the kernel of modern Linux systems. The original concepts were first developed by the NSA (in conjunction with other vendors) and later adopted by Red Hat as a standard feature in CentOS and RHEL distributions.
It follows the 'least-privilege' model in which the default strict enforcing setting denies everything until exception policies are written. These policies define permissions for each element of the system that gives the minimum access required to function. Any action taken outside of the defined access level is denied by default and logged for review.

7.5.1 SELinux Enforcement Modes

SELinux has three basic modes with enforcing set as default:

Enforcing

The default mode that enables and enforces SELinux policies across the system that deny all and log access.

Permissive

SELinux is enabled but will not strictly enforce security policies. It only logs system actions and issues warnings about potential policy violations.

Disabled

SELinux is turned off - there is no logging, warning, or enforcing of policies.

To view the current status of SELinux, use the **sestatus** command.

```
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      31
```

7.5.1(a) SELinux Enforcement State

To change the SELinux mode, use the **setenforce** command to put it in **enforcing (1)** or **permissive (0)**.

```
[user@host ~]$ getenforce
Enforcing
[user@host ~]$ sudo setenforce 1
Result is “Enforcing”
[user@host ~]$ sudo setenforce 0
Result is “Permissive”
```

✎ **Note**: SELinux cannot be disabled on a live system. Follow the next steps to disable SELinux permanently.

The **setenforce** command is only temporary and will not survive a reboot. To permanently set the SELinux mode, edit the **/etc/selinux/config** file and change the ‘**SELINUX=**’ line.

```
[user@host ~]$ sudo vi /etc/selinux/config
```

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=enforcing

# SELINUXTYPE= can take one of three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

7.5.1(b) SELinux System Configuration

✎ **Note**: If disabling SELinux, reboot the host after saving this file.

7.5.2 SELinux Fundamentals

SELinux is built on the concept of labels in which every file, directory, object, and running process is given a label. The labels restrict and permit these system components based on the policies and processes defined. The proper format for labels is always **user:role:type:level** which can be viewed with the **ls** command:

```
[user@host ~]$ ls –dZ /opt/ddt/ansible_main
dr-xr-xr-x. root root system_u:object_r:usr_t:s0
```

✎ **Note**: The **-d** argument specifies just the directory and the **-Z** argument shows the SELinux security context.

Labels vary by location, file type, and associated services, and in this example the user is **system_u**,the role is **object_r**, the type is **usr_t**, and the level is **s0**. When creating a file or directory, it will inherit the context of the parent directory. For example, creating a new tool directory within **/var** will inherit the **/var** context **(var_t)**.

```
[user@host ~]$ sudo mkdir /var/tool
[user@host ~]$ ls -dZ /var/tool
drwxr-xr-x. user user unconfined_u:object_r:var_t:s0
```

7.5.3 Troubleshooting SELinux

Although SELinux is good at preventing privilege escalation and controlling access to the system, sometimes it can get in the way of legitimate operations. SELinux logs every action it takes in what it calls an Access Vector Cache (AVC). AVC logs system operations it deems allowable or disallowable. When operations are denied SELinux will log these AVC denials in the following locations:

/var/log/audit/audit.log
/var/log/messages

✎ **Note**: Within Red Hat products SELinux AVC denials are also viewable by using the **ausearch –m avc** command, which queries audit logs and specifies the AVC module as a limiter.

One of the most common problems with SELinux is when labels are misconfigured or inherit incorrect contexts from parent directories. When installing an http server, the directory and file contexts should be of type **httpd_system_content_t**. If created outside of the default location (**/var/www/html**), the correct context will not be applied. To change contexts persistently, use the `**semanage** command:

```
[user@host ~]$ sudo mkdir /var/tool/html
[user@host ~]$ ls -dZ /var/tool/html
drwxr-xr-x. user user    unconfined_u:object_r:var_t:s0
[user@host ~]$ sudo semanage fcontext –a –t httpd_sys_content_t
“/var/tool/html”
```

✎ **Note**: **semanage** has different options for users (**-s**), roles (**-R**), and types (**-t**). The **–a** option specifies adding a record to the SELinux label database. To apply the context change to the directory, use the **restorecon** command to pull the correct context from the SELinux database:

```
[user@host ~]$ sudo restorecon –v /var/tool/html
restorecon reset /var/tool/html context unconfined_u:object_r:var_t:s0-
>unconfined_u:object_r:httpd_sys_content_t:s0
[user@host ~]$ ls -dZ /var/tool/html
drwxr-xr-x. user user unconfined_u:object_r:httpd_sys_content_t:s0
```

7.6 SSH Keys

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.

7.6.1 Create a New Pair

1 To begin, 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 (**~/.ssh/id_rsa**) 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 (**/.ssh/id_rsa**) and public key (**~/.ssh/id_rsa.pub**).

✎ **Note**: Although SSH keys are not utilized at installation of DDT, the master laptop should have keys copied to all nodes in the cluster after the install has finished.

7.6.2 Sharing Public Keys with Remote Hosts

2 After creating a key pair, copy them to the remote host using the following command:

```
[user@host ~]# ssh-copy-id <username>@<remote_host>
```

A prompt will follow requesting a password for this user. The key will be copied upon authentication. Test the key by attempting to SSH to the remote host with the associated username.

```
[user@host ~]# ssh <username>@<remote_host>
```

7.6.3 Managing the Passphrase of a private key

3 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, (which defaults to **~/.ssh/id_rsa**), the old passphrase, and the new passphrase (leave empty for no passphrase).

7.7 Subscription Manager Repositories

Licensing within RHEL is handled by **subscription-manager**. The registration process has the following order of operations:

1. First, each system requires registration with Red Hat and a valid account that contains licenses for different products.
2. After registering, each system needs to be attached to a specific pool, granting access to the individual Red Hat products.
3. Finally, after registering and subscribing, the system is ready to configure software repositories.

7.7.1 Register System

To begin, the system must be subscribed to either Red Hat directly or a local Satellite server. The username and password of the associated Red Hat account or the local Satellite credentials will be needed.

```
[user@host ~]$ sudo subscription-manager register --username <username> --
password <password>`
```

7.7.2 Available Pools

After registering use the command, below, to view all pools available under the Red Hat account. Each pool will list what products it provides access to.

```
[user@host ~]$ sudo subscription-manager list --available
```

7.7.3 Subscribe a System

Once the appropriate pool ID is obtained, use the following command to subscribe to that pool and gain access to the software it provides.

```
[user@host ~]$ sudo subscription-manager attach --pool=<pool_id>
```

7.7.4 Enable Repositories

At this stage, the system should be fully subscribed and registered with Red Hat or a local Satellite server. However, to download the products provided by the pool, the system needs to enable the corresponding repositories.

1 To determine what repos are available to the system, enter the below command:

```
[user@host ~]$ sudo subscription-manager repos --list
```

2 After locating the desired repositories, enable them by entering the following command:

```
[user@host ~]$ sudo subscription-manager repos --enable=<repository>
```

✎ Note: Use wildcard * entries if all repositories are needed under a specific naming scheme. For example, **rhel-7-server-***

3 Conversely, if a repository needs to be disabled, use the **--disable** option:

```
[user@host ~]$ sudo subscription-manager repos --disable=<repository>
```

7.7.5 Subscription Troubleshooting

In order to download packages, receive updates, and access support services, all RHEL and RHVH systems must be subscribed. However, hosts can end up in an invalid subscription state, have the wrong product subscriptions attached, or lose their subscription for various reasons.

Registration Status

To see the subscription status of a system, use the **subscription-manager status** command. This example shows the output of a fully subscribed, up-to-date system.

```
[user@host ~]$ sudo subscription-manager status
System Status Details
Overall Status: Current
```

✎ **Note**: If a system is stuck in an invalid subscription state, use the **subscription-manager unregister** command to remove the current subscription. After, the system can be subscribed again.

Subscription Consumption

If the system has a valid subscription, use the **subscription-manager list --consumed** command to see the type of license(s) attached to that system and what products they provide. If the system is attached to the wrong type of license, certain products may be unavailable and other systems may be missing licenses if a limited number are available.

```
[user@host ~]$ sudo subscription-manager list --consumed
Consumed Subscriptions

Subscription Name: Provides:
...
System Type:
```

✎ **Note**: If the system is consuming more subscriptions than needed, remove the unnecessary licenses with **subscription-manager remove --pool=<pool_id>**. If all licenses need to be removed, use the **-- all** argument instead.

Repositories and Packages

After registering and attaching licenses, the repositories are the last piece to troubleshoot if something goes wrong. The **subscription-manager repos --list** command will show what repositories are available and if they are enabled with the value of **1**. Disabled repositories will have the value of **0**.

```
[user@host ~]$ sudo subscription-manager repos --list

Available Repositories in /etc/yum.repos.d/redhat.repo

Repo ID:    rhel-7-server-rpms
Repo Name: Red Hat Enterprise Linux 7 Server (RPMs)
Repo URL:
https://satellite.52cpt.cpb.mil/pulp/repos/52cpt/Library/RHEV_CV/cont
ent/dist/rhel/server/7/$releasever/$basearch/os
Enabled:    1
Repo ID:    rhel-7-server-rhevh-rpms
Repo Name: Red Hat Enterprise Virtualization Hypervisor 7 (RPMs)
Repo URL:
https://satellite.52cpt.cpb.mil/pulp/repos/52cpt/Library/RHEV_CV/content
/dist/rhel/server/7/$releasever/$basearch/rhevh/os
Enabled:  0
```

To see what repository provides a certain package, search for that package with **yum whatprovides**.

```
[sudo@host ~]$ sudo yum whatprovides bash-completion
Loaded plugins: enabled_repos_upload, langpacks, package_upload, product- id,
               : search-disabled-repos, subscription-manager
1:bash-completion-2.1-6.el7.noarch : Programmable completion for Bash Repo
             : rhel-7-server-rpms
```

7.8 Introduction to Ansible

Ansible is an open-source configuration management and automation tool produced by Red Hat, using a YAML-based syntax to script deployments with states. Everything written in Ansible can be accomplished through regular Bash/Python scripts, but Ansible allows tasks to run repeatedly (with confidence) due to its checking of end-states. With Ansible, there's no required installation of agents on hosts to run the tasks.
Ansible uses SSH to connect to the hosts specified in the inventory. Thinking back to the training on SSH keys, Ansible is a big part of the reason for configuring them across the cluster. By passing the SSH keys to Ansible it can easily configure the nodes through password-less authentication.

7.8.1 Sample Ansible Playbooks

Ansible is based around the concept of modularity, with all tasks contained in what Ansible calls a Playbook. A Playbook is just a fancy name for a group of tasks to run on a host or a number of hosts to achieve a desired state. Playbooks are the highest level component within Ansible because they run directly alongside an inventory file. Before looking at an inventory file, let's look at what a playbook needs in a file named **simple_playbook.yml**:

```
# This is a comment - playbook.yml
- name: Example playbook
  hosts: example_hosts
  tasks:
    - name: Example task - ping host
    - ping:
```

In the example above, one task pings the **example_hosts** defined in the hosts line – more on this later. The **ping** keyword is an Ansible module, which are open-source Python scripts designed to accomplish a specific task. There are thousands of modules that accept many different options, arguments, and keywords, making common tasks readily available. Ansible's website provides documentation for each module and scenarios for the module's parameters and uses.

In the previous section, **example_hosts** was defined in the hosts line. This host is where the inventory file comes into play. Every playbook is connected to an inventory file whether it is specified or not. Ansible will look for configurations in the default location of **/etc/ansible/hosts** if no inventory file is specified.

Within an inventory file, define hosts, host groups, variables, and other configuration to support playbooks. Hosts files use the **INI** format with every section of the **INI** file starting with a group name in brackets. A list of hosts, variables, IP addresses, or other related configuration will be displayed within each section. Take a look at the example hosts file below:

```
# This is a comment - hosts_file [example_hosts]
host1
host2
host3
```

This host file, above, defines a host group with the name **example_hosts** and lists three hosts for Ansible to use. The hosts file within the example playbook in the previous section would loop through all three of these hosts and attempt to ping each one. Hosts can be defined with fully qualified domain names, CNAMES, or IP addresses. Make sure they're reachable within the network. Ansible supports different host groups in a hosts file and sections for variables with certain keywords in the group name like the example below. This example is saved to a file named **inven**:

```
# This is a comment - hosts_file
[example_hosts]
host1
host2
[example_hosts2]
host3
[all:vars]
example_variable=”myvar”
```

After creating a hosts file and playbook, run the playbook using the command, below, to use the example hosts file instead of the default configuration.

```
[user@host]$ sudo ansible-playbook -i inven -v simple_playbook.yml
```

```
[root@master52 ansible_test]# ansible-playbook -i inven -v simple_playbook.yml
Using /etc/ansible/ansible.cfg as config file

PLAY [Example playbook] ********************************************************

TASK [Gathering Facts] *********************************************************
ok: [host3]
ok: [host2]
ok: [host1]

TASK [Example task - ping host] ************************************************
ok: [host2] => {"changed": false, "ping": "pong"}
ok: [host3] => {"changed": false, "ping": "pong"}
ok: [host1] => {"changed": false, "ping": "pong"}

PLAY RECAP *********************************************************************
host1                      : ok=2    changed=0    unreachable=0    failed=0    s
kipped=0    rescued=0    ignored=0
host2                      : ok=2    changed=0    unreachable=0    failed=0    s
kipped=0    rescued=0    ignored=0
host3                      : ok=2    changed=0    unreachable=0    failed=0    s
kipped=0    rescued=0    ignored=0
```

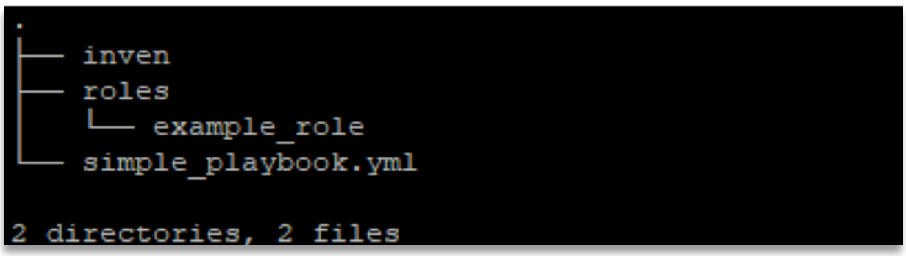
7.8.1 Ansible Simple Playbook Activity

Let's breakdown the syntax of the command. Begin with **ansible-playbook** and then use the **-i** option to tell Ansible to use the **inventory** file named **inven**. This inventory file is located in the same directory as the playbook, so the full path of the file is not needed. The **-v** option indicates **1** level of verbosity to see output results of the ping and corresponding pong. After the options, end with the name of the playbook to tell Ansible what to run.

7.8.2 Ansible Roles and Tasks

This scenario defined all tasks in the playbook, but in production most tasks are delegated to roles so they can be reused across different playbooks. At a high level, roles are directories that contain tasks that are available for any playbook created. Roles condense actions to a set of related tasks that can be referenced in any playbook. To begin, create a '**roles**' directory in the same directory as the playbook file. Ansible will look here first and then recursively check directories in its path. After creating the roles directory, begin by creating an **example_role** directory within it. The names of these directories are then referenced in the playbook.

Folder structure:



7.8.2(a) Ansible Folder Structure

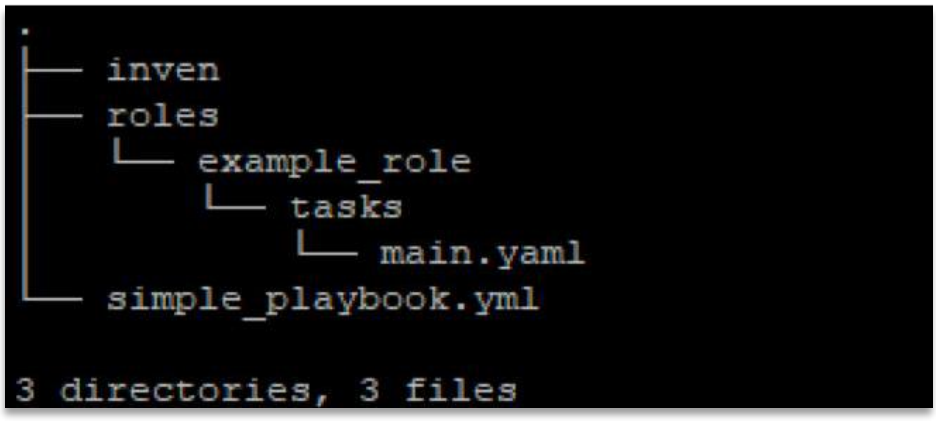
After creating roles and **example_role** directories, create the tasks directory to achieve the minimum requirements for an Ansible role.

Within the **example_role** directory, create another directory named **tasks**. This keyword tells Ansible where to look for the role's tasks. Begin by recreating the original playbook task as a role task instead:

```
# This is a comment - main.yml
---
- name: Example role task (Ping)
  ping:
```

Task files within roles are '.**yml**' formatted files. Ansible depends on a primary task named **main.yml**. Ansible supports multiple task files within a role, but **main.yml** is the reference file to run them. Tasks include a name and a module and support many different types of actions. To reuse the created role, revisit the original **playbook.yml** and replace the task section with the relative path and name of the roles directory:

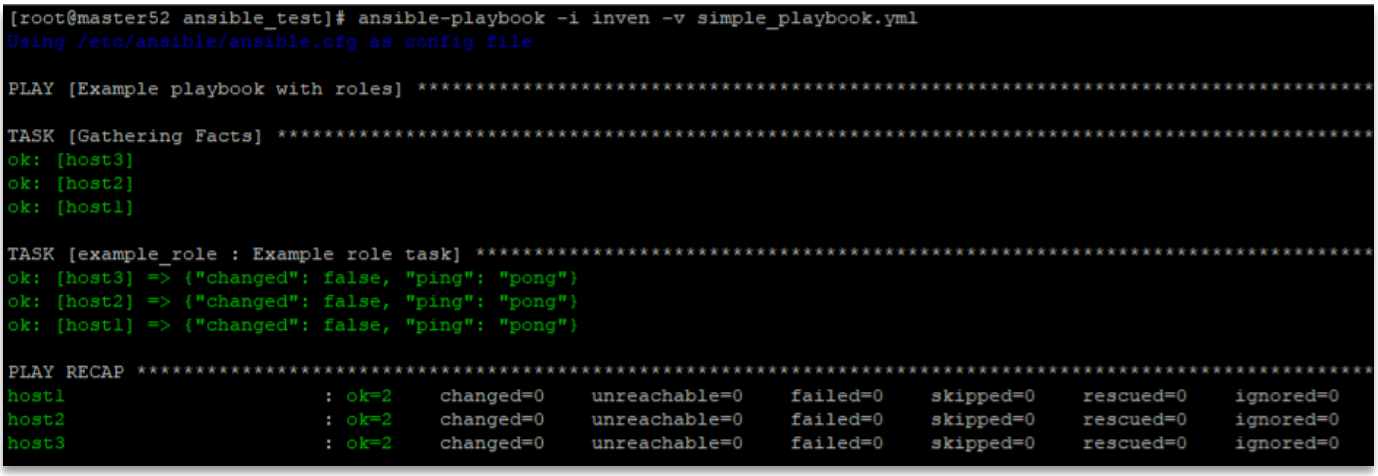
At this point, our folder structure should look like the following:



7.8.2(b) Ansible Folder Structure

Run the playbook with roles using the following command:

```
[user@host~]$ sudo ansible-playbook -i inven -v simple_playbook.yml
```



7.8.2(c) Ansible Playbook Activity

7.8.3 Ansible Vars Files

Although optional, Ansible allows users to specify variables in vars files that can be referenced throughout playbooks. Within DDT, any variables operators that need to change will be located in **group_vars/all.yml**. Keep in mind, vars files are also **.yml** files, so let's take a look at an example **vars.yml** file:

```
# This is a comment - vars.yml
---
example_variable: "my_var"
example_list:
  - "var1"
  - "var2"
example_object_variable:
  - name: "object1"
  - object_variable: "obj1_var"
  - name: "object2"
  - object_variable: "obj2_var"
```

Vars files can be referenced throughout Ansible playbooks for individual plays or included within a roles directory to be available for that specific role. Add this vars file to the example playbook as below:

```
# This is a comment - playbook.yml
---
- name: Example playbook with roles
- hosts: example_hosts
  vars_files:
    - vars.yml
  roles:
    - example_role
```

Optionally, create a **vars** directory within the example role and rename the vars file to **main.yml**. Just like the roles **main.yml** file, this keyword tells Ansible to automatically add these variables to any task run within that specific role.

8 Project DDT Master Laptop Services

Passwords for all DDT components are available within **/opt/ddt/ansible_main/passwords.yml** on the laptop. The three of the most important passwords are:

```
[defender@master ~]$ sudo cat /opt/ddt/ansible_main/passwords.yml
engine_admin_pass: <RHVH Hosted Engine Admin Password>
ipa_admin_pass: <Red Hat IdM Admin Password>
sat_admin_pass: <Satellite Admin Password>
```

Web interfaces should be accessed with the admin accounts and their associated passwords of each respective application. Root passwords can be used to SSH into hosts and complete tasks from the command line.

8.1 Red Hat Identity Management

Introduction

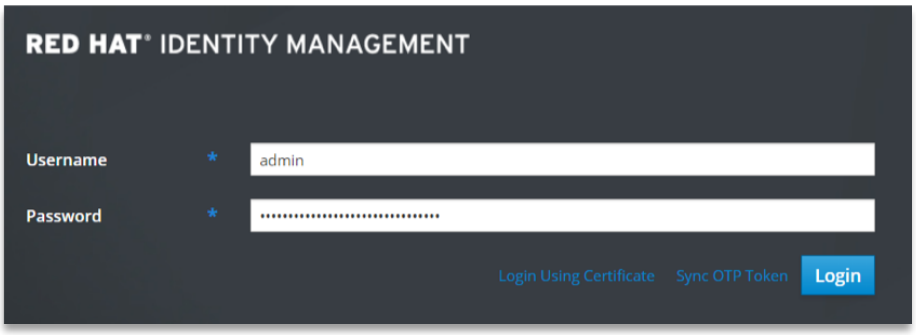
Red Hat IdM is Red Hat's Identity Management solution consisting of LDAP, Kerberos, DNS and PKI. IdM can be thought of as the Active Directory of Linux as it allows for secure authentication and authorization throughout the domain.

8.1.1 Role within DDT

Red Hat IdM is deployed as a VM on the master laptop within DDT and is used to provide DNS and central authentication for the kit. Administrators can set group and domain level policies on multiple hosts using IdM.

8.1.2 Web Interface

The Red Hat IDM web interface is available at **`https://idm.{kit#}cpt.cpb.mil`** after installation of the master laptop.



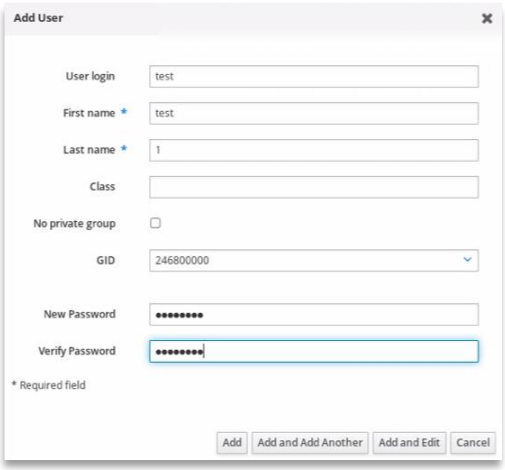
8.1.2 IdM Login Prompt

8.1.3 Common IdM Administration Tasks

Some common administration tasks that may need to be performed within IdM are managing users, hosts, groups, and editing DNS entries.

Add Users

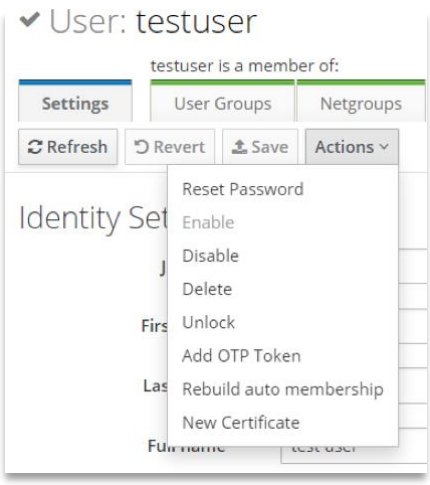
1. Login to the IdM web interface.
2. Click the **Identity** tab and then click on **Users**.
3. Click the **Add** button to add a user.
4. Fill in the fields as desired and press **Add** when finished.



8.1.3(a) IdM Add Users

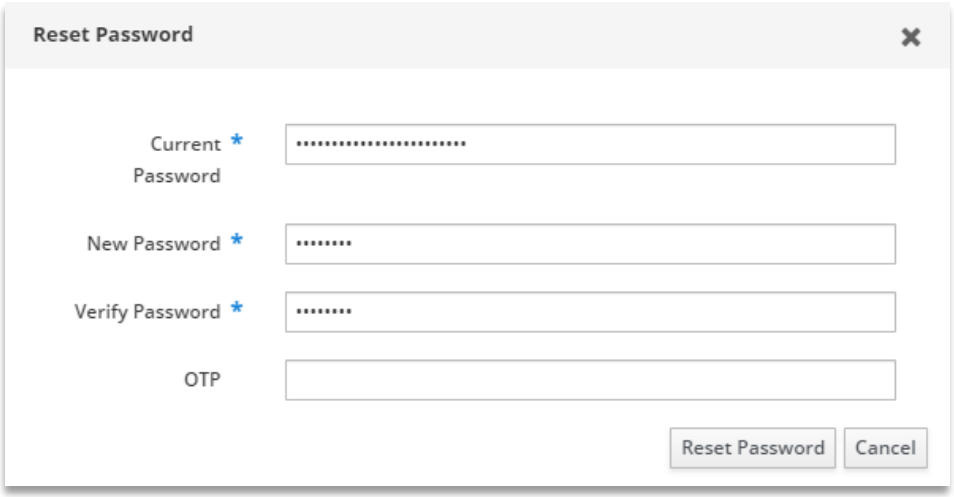
Reset User Password

1 Login to the IdM web interface.
2 Click the **Identity** tab and then click on **Users**.
3 Select a user to open the user management interface.
4 Click the **Actions** dropdown and then **Reset Password**.



8.1.3(b) IdM User Actions

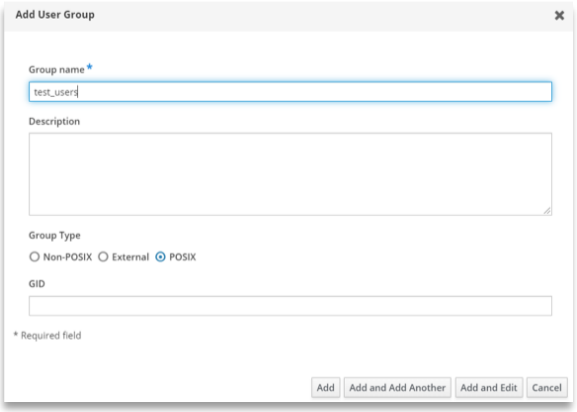
5 In the popup box, enter a new password and click **Reset Password** to finalize changes.



8.1.3(c) IdM User Password Reset

Add Groups

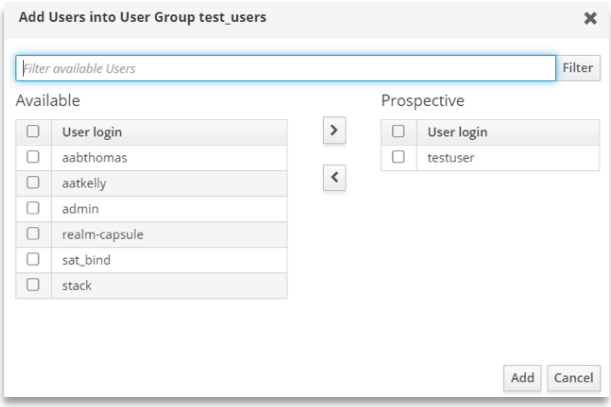
1. Login to the IdM web interface
2. Click the **Identity** tab and then click on **Groups**.
3. Click the **Add** button to add a group.
4. Fill in the fields as desired and press **Add** when finished.



8.1.3(d) IdM Group Creation

Add a User to a Group

1. Login to the IdM web interface.
2. Click the **Identity** tab and then click on **Groups**.
3. Click the group that the user should be added to.
4. Within the **Users** tab, click the **Add** button.
5. Select the user to be added and then click the arrow pointing towards the **Prospective Users** column to move the user.

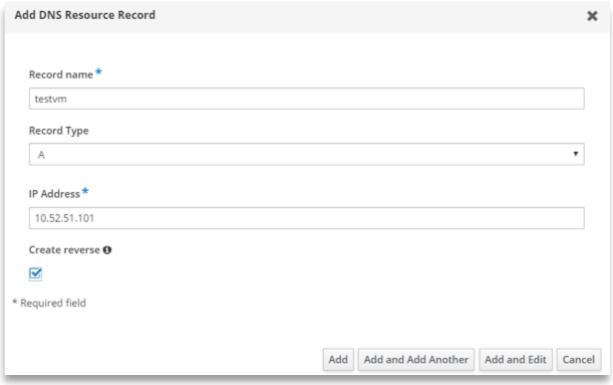


8.1.3(e) IdM Group User Assignments

Once all applicable users have been added to the Prospective pool, click **Add** to add them to the group.

Add a DNS Entry

1 Login to the IdM web interface.
2 Click on the **Network Services** tab and then select **DNS Zones** from the DNS dropdown menu.
3 Click the **[kit_num]cpt.cpb.mil**.zone
4 Click the **Add** button and then fill out the fields as desired.



8.1.3(f) IdM DNS Entries

8.2 Red Hat Satellite

Introduction

Red Hat Satellite is a system management tool that allows operators to deploy, maintain, and manage hosts within their environment. Satellite handles all of the licensing required for RHEL systems and functions as a local repository for all content needed for deployments.

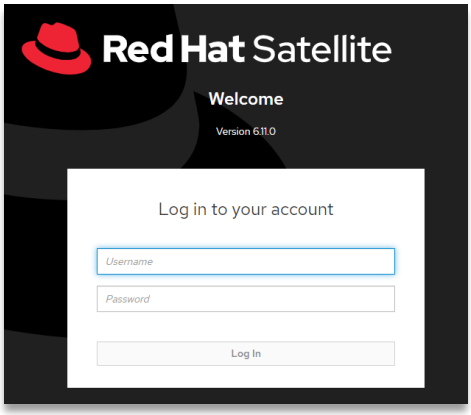
8.2.1 Satellite's Role with DDT

Satellite is deployed as a VM on the master laptop within DDT. It helps to manage and maintain the 8 physical nodes included with the kit and any VMs hosted on any of the nodes. In order to deploy in air- gapped environments, Satellite also hosts all of the content (RPMs, licensing, images, etc.) needed to install nodes, VMs, and other tools. Satellite uses IPMI discovery to find hosts on the network and then acts as a PXE server to provision nodes and Virtual Machines. Finally, Satellite acts as the DHCP server for each subnet to provide dynamic IP addresses for any added capabilities.

8.2.2 Web Interface

The Red Hat Satellite web interface is available at **`https://satellite.{kit#}cpt.cpb.mil`** after installation of the master laptop.

8.2.3 Satellite Features



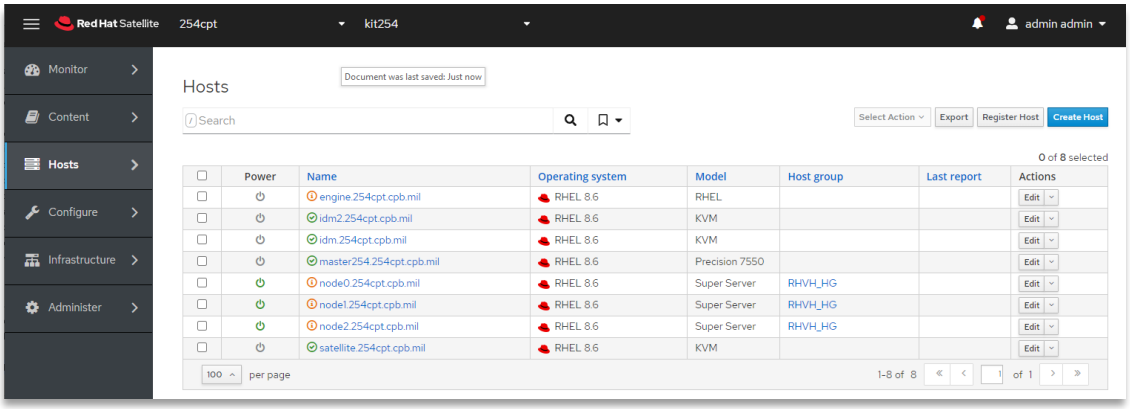
8.2.2 Satellite Login Prompt

Satellite has several dashboards and features available for operators to gain insight into their environment. The default monitor dashboard is shown upon login to give a high-level summary of the environment.

Host Monitoring

The Satellite hosts dashboard allows operators to manage hosts registered to that Satellite instance. From this dashboard, operators can view currently managed hosts, retrieve host specific information, add, or delete hosts, or make any host specific changes. Operators can view hosts discovered through IPMI discovery, view the available content, find installation media or templates available for provisioning, and much more.

After deployment, the Hosts dashboard should have the following hosts displayed:

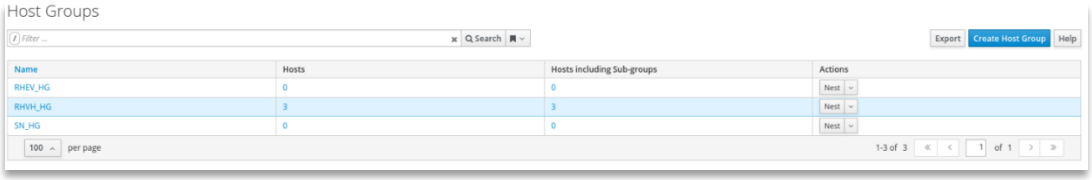


8.2.3(a) Satellite Host Overview

Host Groups

Host groups within Satellite allow operators to separate hosts into different logical groups to share common configuration and attributes. Instead of manually configuring each host with the same settings, host groups allow hosts within them to inherit defined configuration. Within DDT, RHVH nodes are automatically assigned to a host group called “**RHVH_HG**” that defines the networking, puppet settings, operating system settings, and Satellite metadata for provisioning.

To view host groups, log in to Satellite and click on **Configure > Host Groups**.

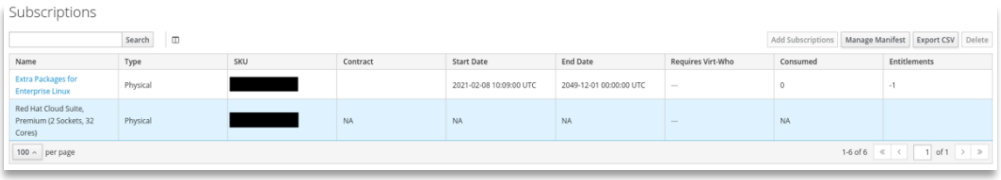


8.2.3(b) Satellite Host Groups

Subscriptions and Licensing

Satellite is responsible for all subscriptions, licensing, and Red Hat authentication to enable the kit to be deployed in isolated environments. On installation, the subscription allocations created earlier in this document are imported into Satellite and made available to all hosts connected to it. After registration with Satellite, hosts consume subscription allocations one-by-one until Satellite is at capacity.

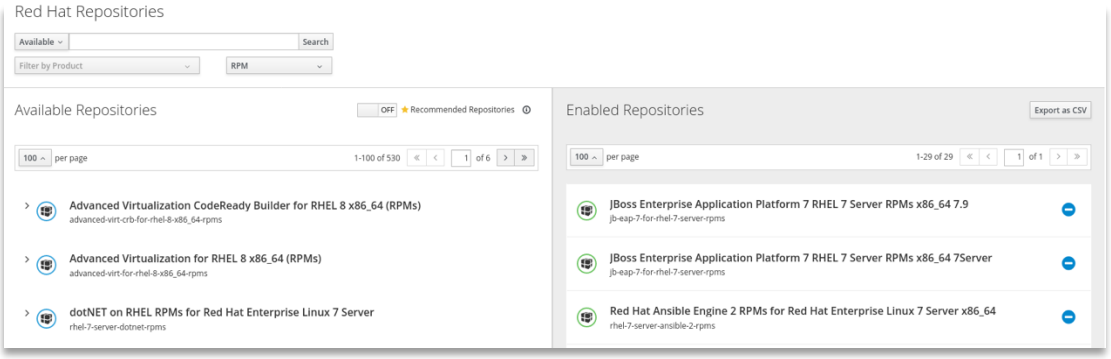
To view the current subscriptions available within Satellite, log in to the web interface and click on **Content > Subscriptions**.



8.2.3(c) Satellite Subscription Entitlement Overview

Repositories, Software, and Packages

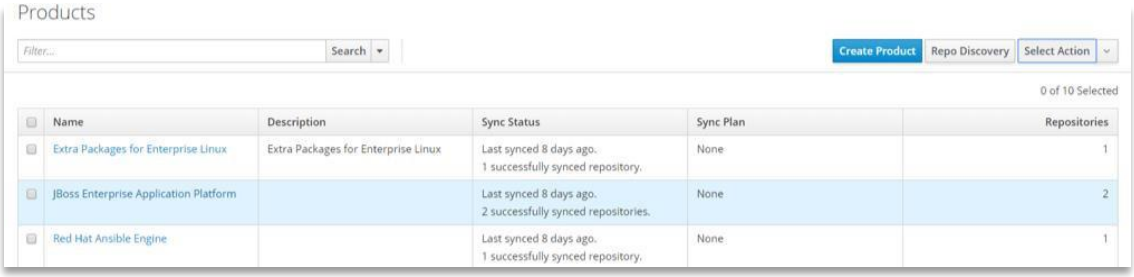
The subscriptions imported into Satellite provide it with access to several repositories that provide software, packages, and security updates. Hosts can subscribe to these repositories through **subscription-manager** and then install desired packages with **yum**. To view available repositories, log in to Satellite and click on **Content > Red Hat Repositories**. Within this page, operators can enable and disable repositories.



8.2.3(d) Satellite Content

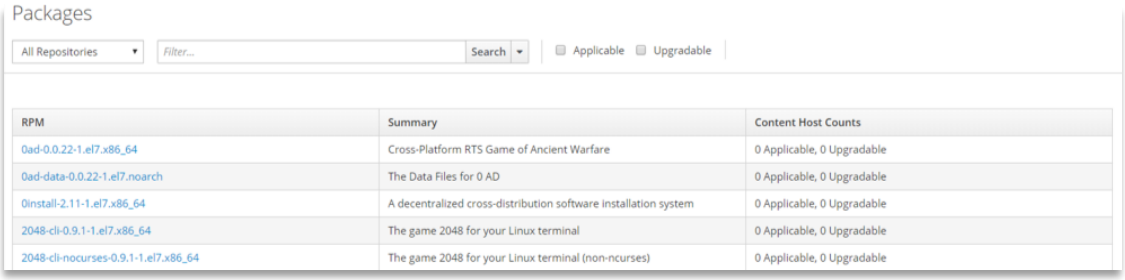
✎ **Note**: RHVH depends on many of the currently enabled repositories, do not disable repositories DDT enables by default.

To view the Red Hat products provided by the imported subscriptions, log in to Satellite and click on **Content > Products**.



8.2.3(e) Satellite Products

Finally, to view individual packages provided by the repositories, log in to Satellite and click on **Content > Packages**. Clicking on individual packages will give more details and indicate what repository they belong to.



8.2.3(f) Satellite Packages

8.2.4 Common Satellite Administration Tasks

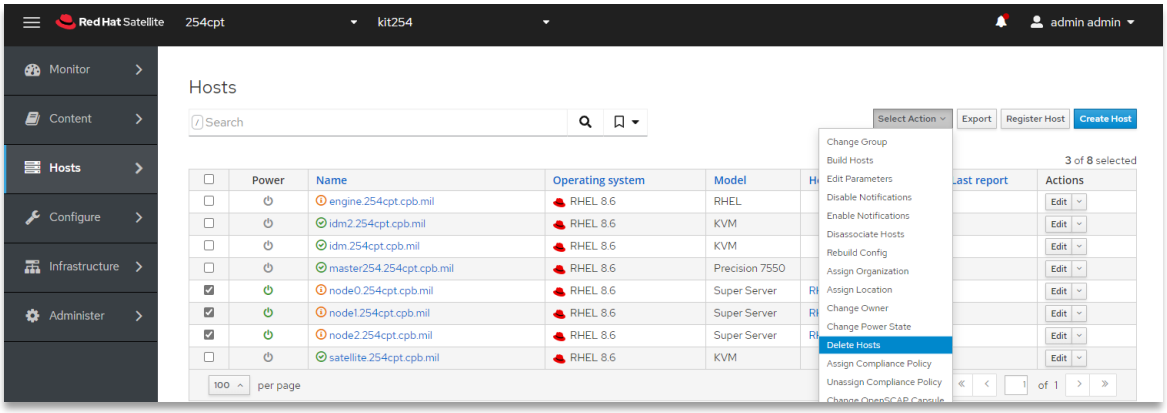
Delete Hosts

To delete a host deployed manually by Satellite or automatically by DDT, first unregister the host, if subscribed, and remove it from Satellite.

1 If deleting a RHEL host, login to the host and unregister the system from Satellite to free up a license.

```
[user@host~]$ sudo subscription-manager unregister
```

2 Login to the Satellite web interface and go to **Hosts > All Hosts**
3 Check only the host(s) marked for deletion, then click the **Select Action** dropdown box above the table.
4 Select **Delete Hosts** in the dropdown menu and then click **OK** to the popup screen asking for confirmation

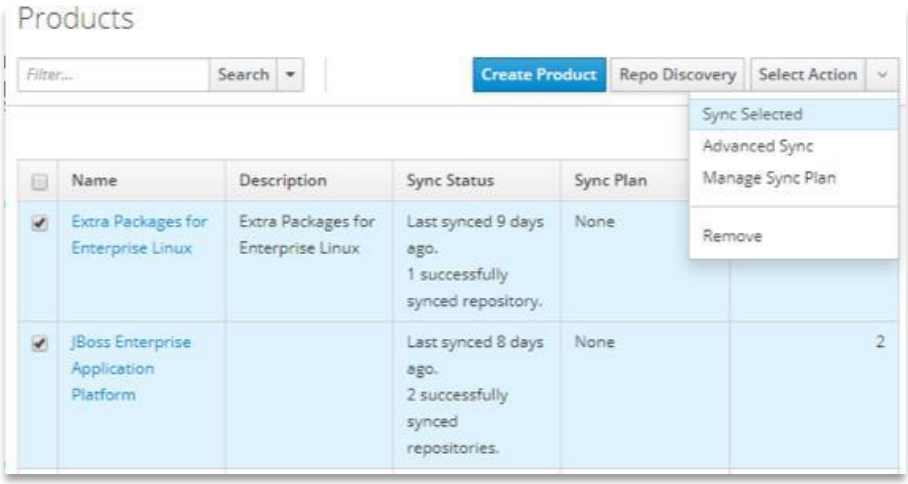


8.2.4(a) Satellite Host Deletion

Sync Repositories

If connected to the PM-DCO PLACT Forge Infrastructure, the local kit Satellite can sync upstream repositories to receive updates or pull new content if additional repositories were enabled.

1 Login to Satellite and go to **Content > Products**
2 Select the products to sync and click the **Select Action** dropdown.
3 Click **Sync Selected** and wait for updates to finish downloading. To view the status of the sync, go to **Content > Sync Status** for a visual representation of progress.



8.2.4(b) Satellite Repository Synchronization

✎ **Note**: If an optimized (default) sync is not working or gives errors, click **Advanced Sync** instead of **Sync Selected** and make sure to check **Validate Content Sync** before starting.

9 DDT Virtualization Administration

9.1 Red Hat Virtualization Hosts (RHVH)

A RHVH cluster is a group of Linux Hypervisors utilizing Kernel-based Virtual Machine (KVM) technology. It enables management of an entire virtual infrastructure including hosts, virtual machines, networks, storage, and users from a centralized graphical interface.

9.1.1 Introduction to Hyperconverged Concept

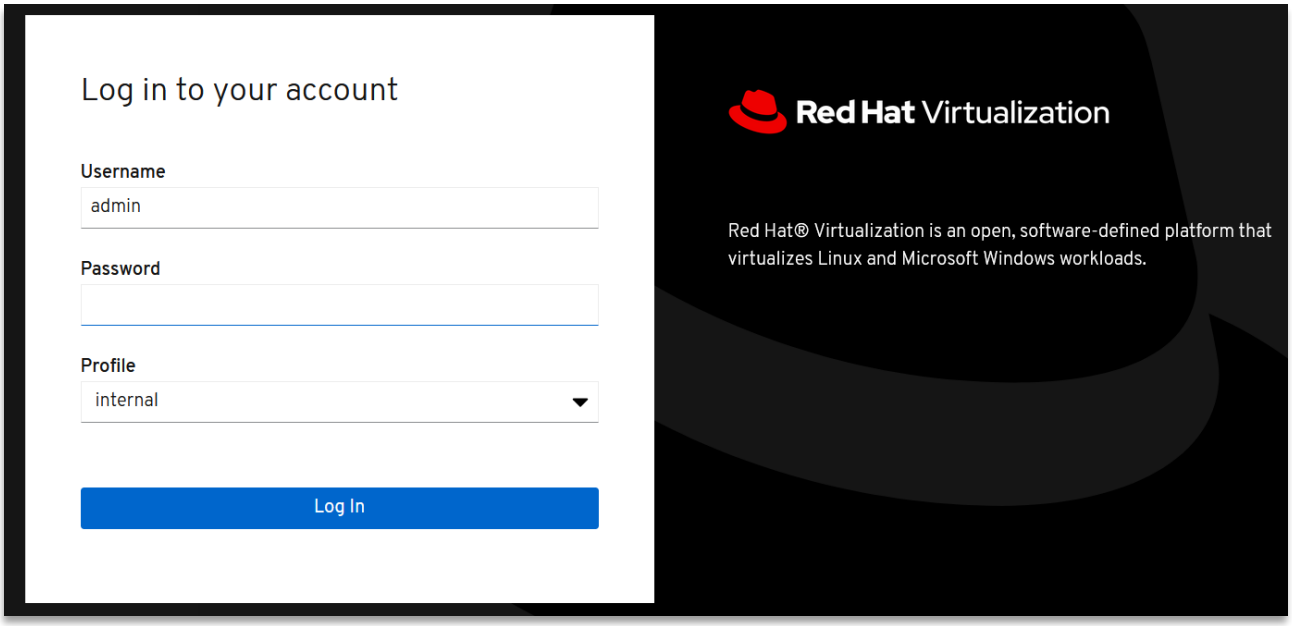
DDT uses a hyperconverged RHVH cluster. Servers within the cluster act as both compute and storage nodes by running both **oVirt** and **Gluster** and combining their services. RHVH provides low overhead cost virtualization and allows CPTs to deploy tools quickly and efficiently as virtual machines.

9.1.2 Introduction to Hosted Engine

Hosted Engine is a Red Hat product deployed to a RHVH environment to manage cluster nodes and their resources. The Hosted Engine is deployed as a virtual machine on top of these nodes and is highly available in case of a node failure.

9.1.3 RHVH Hosted Engine Web Interface

The Hosted Engine is also responsible for providing operators a web interface to manage the cluster. This web interface is available at **`https://engine.{kit#}cpt.cpb.mil`** within the **Administration Portal** after installation of nodes and the Hosted Engine.



9.1.3 Red Hat Virtualization Login Prompt

9.1.4 Common Cluster Administration Tasks

Monitoring RHVH Cluster

Upon login to the Hosted Engine Administration Portal, operators are greeted with the Hosted Engine RHVH dashboard. This dashboard provides operators an aggregate resource overview of their RHVH cluster.
Highlighted displays include:

- CPU
- Memory Raw
- Storage
- Storage Domains and Volumes
- Number of Hosts
- Number of Virtual Machines
- Events and Errors

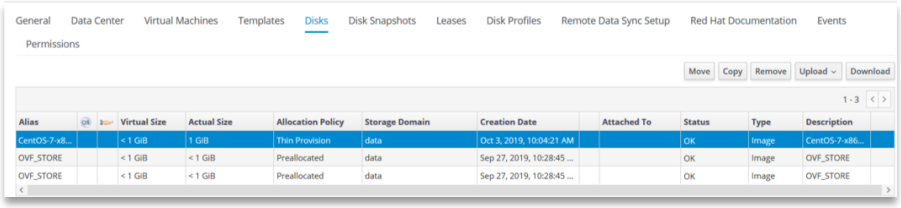
Disk Management

RHVH stores data in logical volumes provisioned for a specific purpose. Each domain is mapped to different physical disks in the DDS nodes and is provisioned with different percentages of that disk's capacity. Below are the use cases for each domain:

- **data:** all templates and installation media should be stored here including ISOs, base QCOW2s, OVA and OVF templates, etc.
- **hosted_storage:** reserved for the Hosted Engine, do not upload or provision anything here.
- **isostore:** reserved for ISOs uploaded through DDT scripts. Soon to be deprecated.
- **vmstore:** all VM disks should be stored here as it is provisioned with the most storage space and replicated across the cluster for high availability.

To manage the content of each domain, adhere to the following steps:

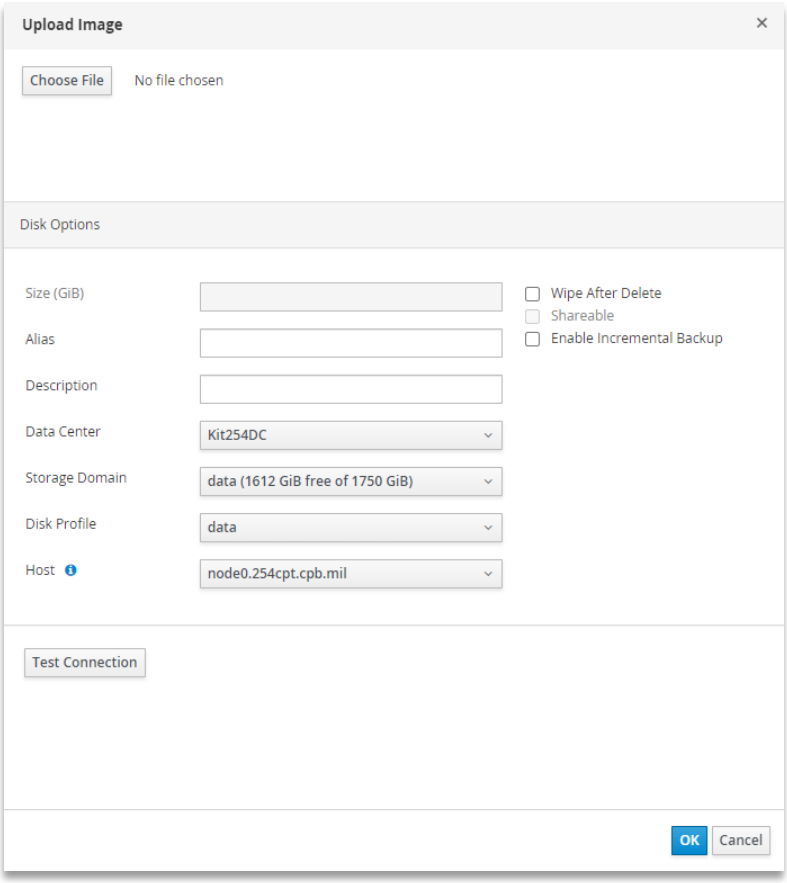
11 Login to the RHVH Hosted Engine web interface.
12 Navigate to **Storage > Domains**.
13 Click a domain to see its configuration.
14 Switch to the **Disks** tab to see all data belonging to that domain.
15 Select a disk to move, copy, remove, or download it from that domain.



9.1.4(a) Storage Domain Disks

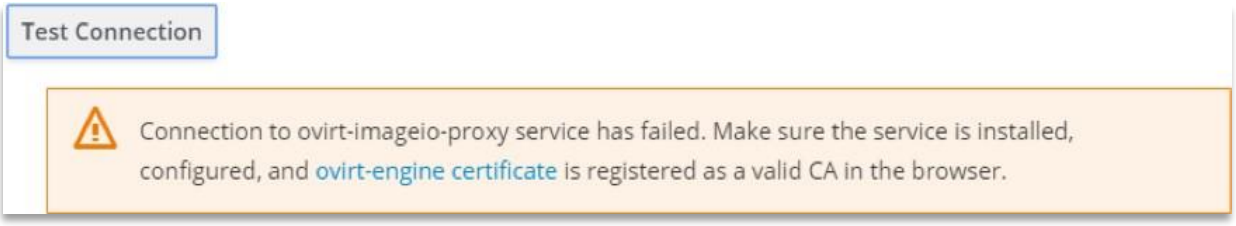
Uploading an ISO/QCOW2

1 Log in to the RHVH Hosted Engine web interface and navigate to **Storage > Disks**
2 Select **Upload** then **Start**



9.1.4(b) Manually Upload an Image

3 Click **Test Connection** at the bottom, and then click the link to download the **ovirt-engine certificate** if an error is shown.

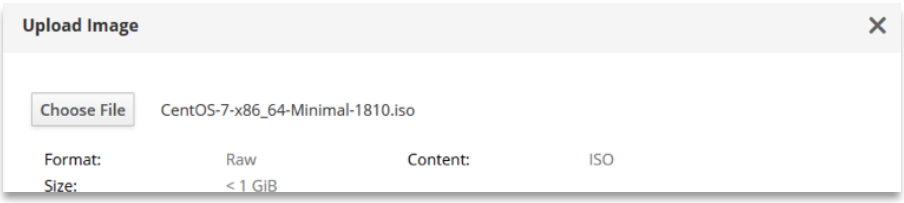


9.1.4(c) Downloading the ovirt-engine Certificate

4 In Firefox, a popup box will appear asking to trust the new Certificate Authority (CA). Select **Trust this CA to identify websites** and click **Ok**.

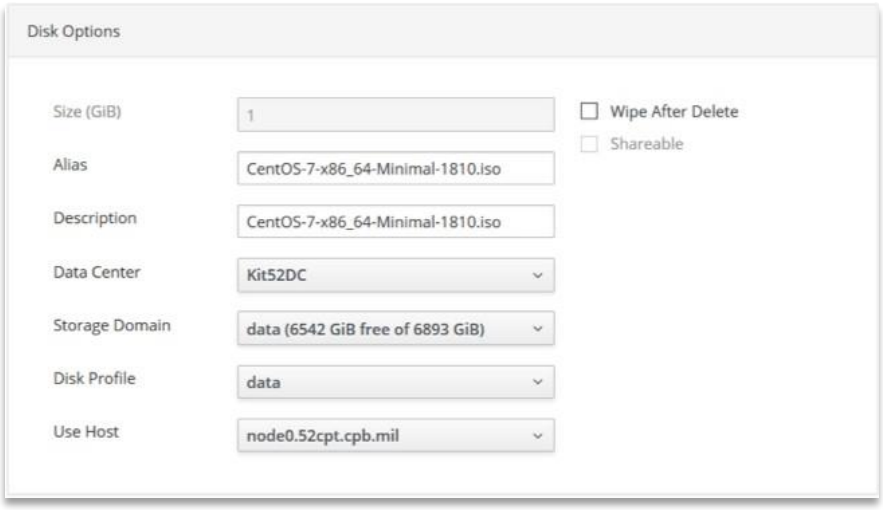
9.1.4(d) Installing the CA Certificate

5 Within the Upload Image tab, Select **Choose File** and search for a desired ISO, then click **Open**.



9.1.4(e) Selecting an ISO Image

6 Fill out the Disk Options for the file and upload it by clicking **OK** at the bottom right. Be sure to use **Data** for all ISO files or installation templates, and **vmstore** for any virtual disks.



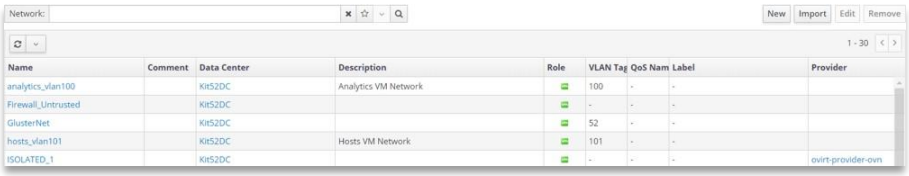
9.1.4(f) Image Disk Options

✎ **Note**: Although there is an **isostore** domain, the ISO domain type is being deprecated in favor of uploading VMs to data stores. The **isostore** domain should only be accessed by DDT scripts, all other ISOs should be uploaded as shown above.

Logical Network Interfaces

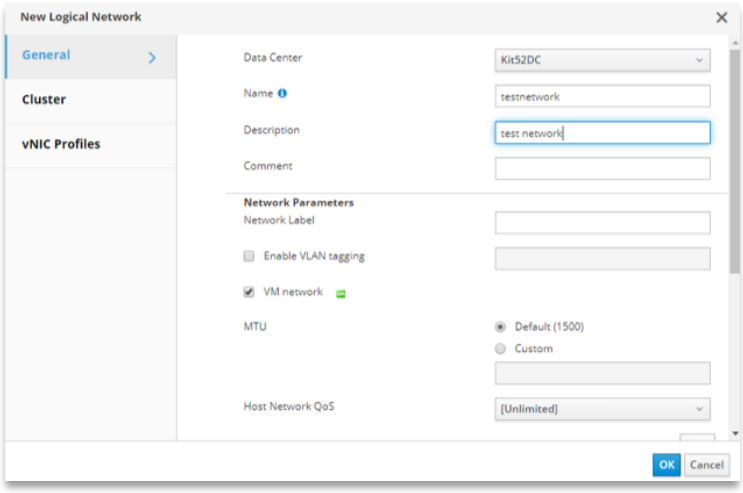
Logical networks can be created within RHVH to separate VMs by VLANs or isolate traffic to specific networks. Operators may need to create, change, or delete networks within RHVH to support tools and capabilities. To make any necessary changes or updates, follow the steps below.

1 Login to the RHVH Hosted Engine web interface
2 Click **Network**, **Networks again**, and finally click **New** towards the top right of the webpage.



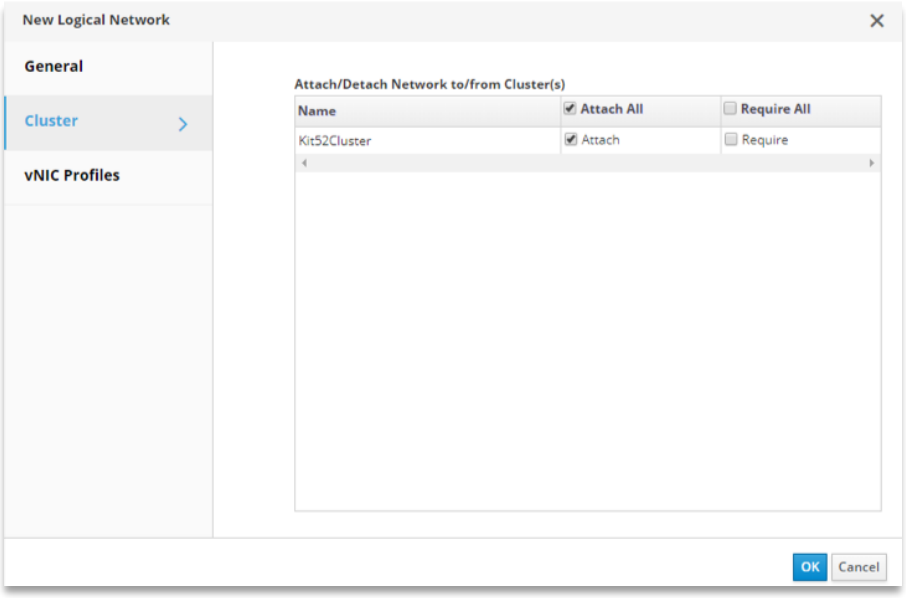
9.1.4(g) Logical Network Overview

3 Fill out the following required settings in the **General** tab (the rest are optional):
- **Data Center**: Make sure to select the datacenter associated with the kit.
- **Name**: Arbitrary name for the network.
- **Enable VLAN tagging**: Optionally, tag the network with a VLAN.
- **VM Network**: Make sure this setting is checked.



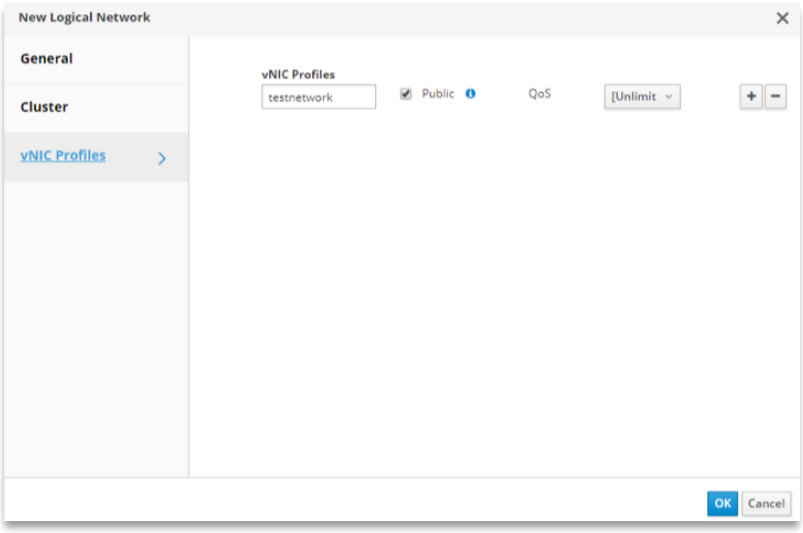
9.1.4(h) Logical Network Settings

4 Switch to the **Cluster** tab and make sure to disable the **Require All** setting.



9.1.4(i) Logical Network Cluster Assignment

5 Finally, switch to the **vNIC Profiles** tab and enter a name for the network's vNIC profile. The name of the network and vNIC profile should usually be the same.

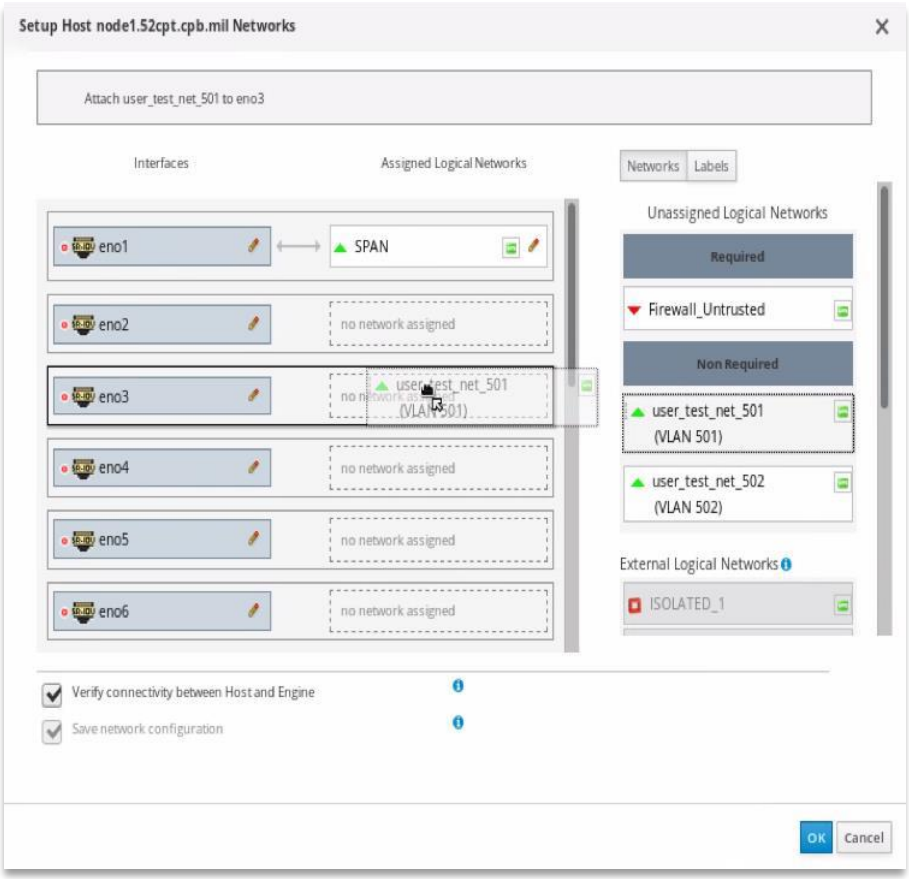


9.1.4(j) Logical Network vNIC Profiles

Attach Networks to Host Interfaces

After creation of a new host network, that network needs to be attached to hosts within the cluster. Generally, this network should be attached to all hosts on the same interface but depending on the configuration of VMs, it may vary.

1 Login to the RHVH Hosted Engine web interface.
2 Navigate to **Compute > Hosts**.
3 Select the host to attach to the logical network.
4 Switch to the **Network Interfaces** tab and click **Setup Host Networks**.
5 Drag the network to the desired interface to attach it. Press **OK** once finished.

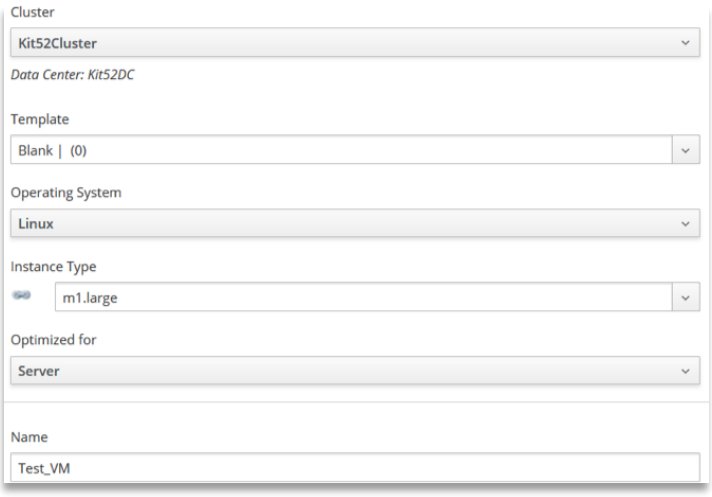


9.1.4(k) Attach Networks to Host Interfaces

9.1.5 Virtual Machine Administration

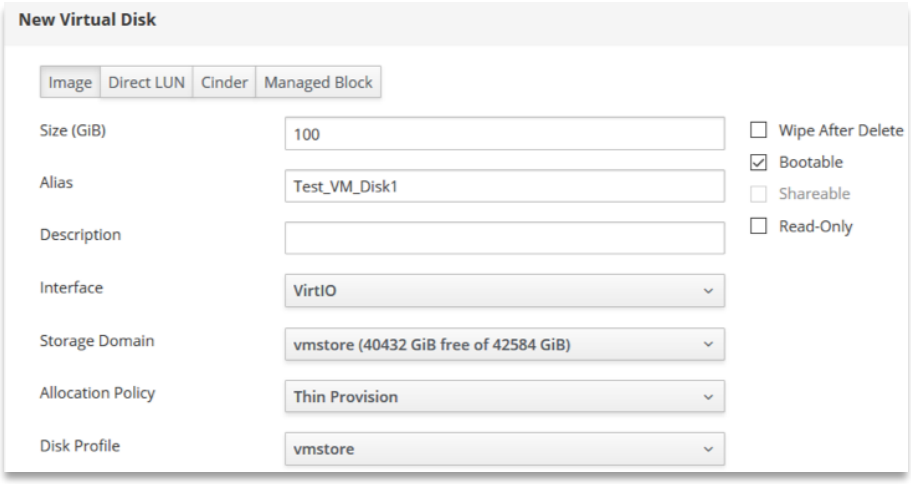
Creating a Virtual Machine

1. Login to the RHVH Hosted Engine web interface
2. Navigate to the **Compute** section on the left-hand side of the screen and then select **Virtual Machines**.
3. Click the **New** button at the top to create a new virtual machine
4. In the **General** tab, fill out the following settings:
   - **Cluster**: Kit**<kit>** Cluster
   - **Template**: Blank, otherwise operator created custom template
   - **Operating System**: Application specific OS
   - **Instance Type**:
     - **ddi.endgame**: Used for Endgame only
     - **ddi.splunk_index**: Used for Splunk Index only
     - **ddi.splunk_search**: Used for Splunk Search only
     - **ddi.windows10**: Used for Windows 10 VMs only
     - **m1.medium**: Provides 2 vCPUs with 4 GB of Memory (RAM)
     - **m1.large**: Provides 2 vCPUs with 8 GB of Memory (RAM)
     - **m1.xlarge**: Provides 4 vCPUs with 16 GB of Memory (RAM)
   - **custom**: Operator defined resources (Use System Tab to define)
   - **Optimized For**: Server or High Performance
   - **Name**: Unique VM name
   - **Description**: Optional
   - **Comment**: Optional
   - **VM ID**: Automatically assigned if not defined



9.1.5(a) Virtual Machine Settings

5 If a disk image already exists for the VM, select it by clicking the **Attach** button under Instance Images. Otherwise select **Create** and fill out the following:
- **Size (GiB)**: Maximum size of the disk
- **Alias**: Name of the disk
- **Description**: Optional
- **Interface**: VirtIO
- **Storage Domain**: vmstore – be sure to use this for all VMs
- **Allocation Policy**: Preallocated or Thin Provision
- **Disk Profile**: vmstore
- **Bootable**: At least one disk must be bootable



9.1.5(b) Virtual Machine Disk Selection

6 Choose which NIC to pass through to the virtual machine in the drop-down menu for **nic1** at the bottom. Add more NICs as needed.

7 (Optional for High Performance) In the **System** tab, define the virtual machine's NUMA architecture under **Advanced Parameters**. For these kits there is 1 Virtual Socket and 2 Cores per Socket. The number of threads per core can be up to 16. RAM and vCPU count can be adjusted here as well.

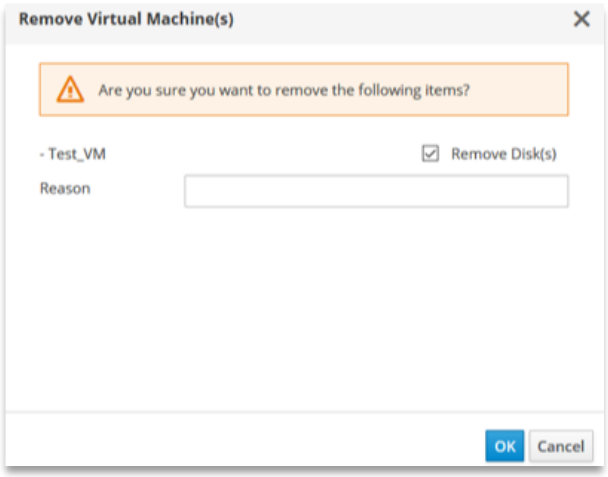
8 Navigate to **Boot Options** settings on the left-hand side.

9 Click the checkbox for **Attach CD** and select the ISO image to be installed in the drop-down menu on the right. Make sure to add the **CD-ROM** as the second boot option. Verify all settings, then click the **OK** button on the bottom-right to create the virtual machine and then confirm the Virtual Machine has been created.

10 To run the virtual machine, right-click on it and then click **Run**

Deleting a Virtual Machine

1. Login to the RHVH Hosted Engine web interface.
2. Navigate to **Compute > Virtual Machines**.
3. Select the VM to be deleted and make sure it is powered off. Click the **Remove** button and confirm the removal in the popup. If associated disks should be deleted as well, select the **Remove Disk(s)** option in the popup as well.

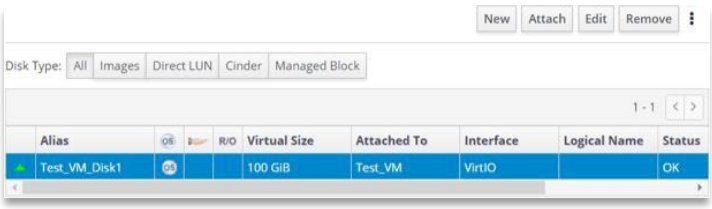


9.1.5(c) Virtual Machine Deletion

Manage Virtual Machine Storage

Virtual disks attached to VMs can be managed through the storage domains as detailed above or managed on a per-VM basis from within the VM settings.

1. Log in to the RHVH Hosted Engine web interface.
2. Navigate to **Compute > Virtual Machines**.
3. Click the name of the VM to be managed.
4. Switch to the **Disks** tab to view all disks associated with the VM.
5. From this tab, operators can create disks, attach disks to the VM, edit disk settings, or remove disks from the VM.



9.1.5(d) Virtual Machine Disk Information

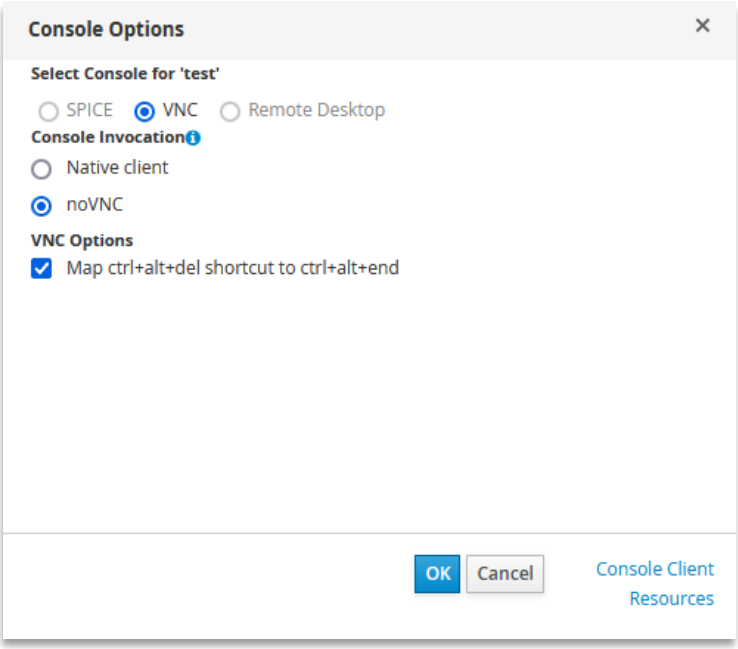
Manage Virtual Machine Network Interfaces

1 Log in to the RHVH Hosted Engine web interface.
2 Navigate to **Compute > Virtual Machines**.
3 Click the name of the VM to be managed.
4 Switch to the **Network Interfaces** tab to view all networks associated with the VM.
5 From this tab, operators can create NICs, edit existing NICs, or remove NICs from the VM.

9.1.5(e) Virtual Machine Network Interfaces

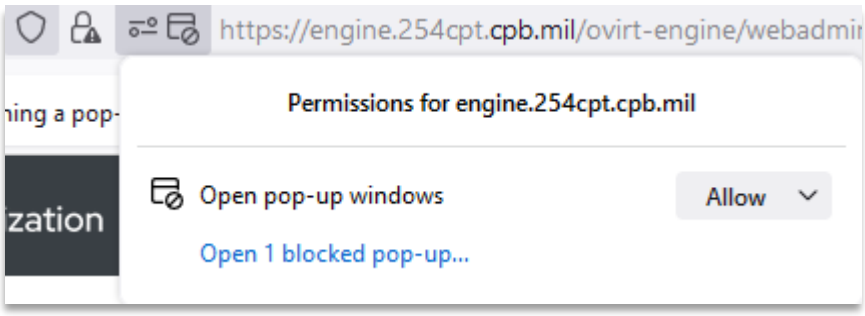
Console into Virtual Machines

1 Log in to the RHVH Hosted Engine web interface.
2 Navigate to **Compute > Virtual Machines**.
3 Select the desired virtual machine by left clicking on it from the list of available virtual machines.
4 Click the **Console** drop-down option to modify the remote connection mode from the available console options. Use the **noVNC** console invocation mode to open this session.



9.1.5(f) Virtual Machine Remote Viewing

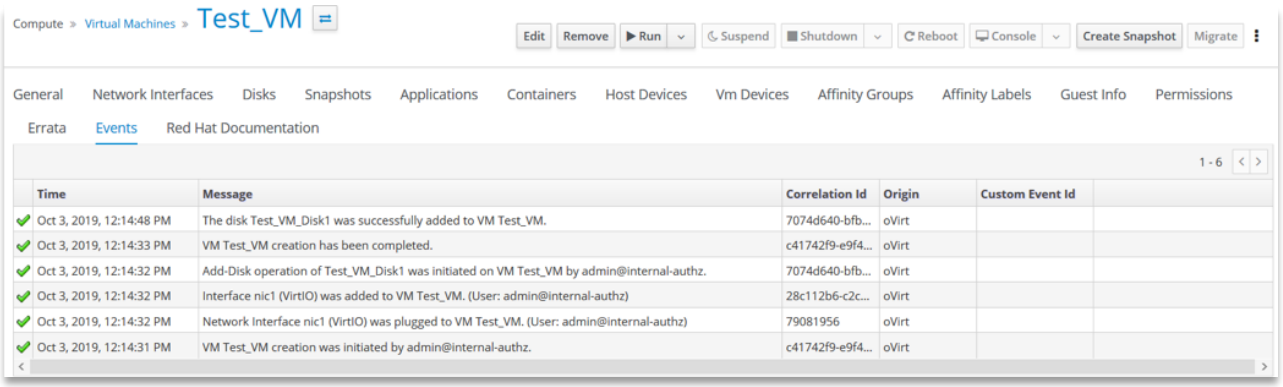
5 Click **Console**, then enable pop-ups by clicking the icon from the Firefox browser bar and selecting **Allow.** Re-selecting **Console** will then enable the remote connection.



9.1.5(g) Virtual Machine Remote Viewing

View Virtual Machine Event Logs

1 Log in to the RHVH Hosted Engine web interface.
2 Navigate to **Compute > Virtual Machines**.
3 Select the desired virtual machine by left clicking on it from the list of available virtual machines.
4 Switch to the **Events** tab to see a list of timestamped events.



9.1.5(h) Viewing Virtual Machine Events

9.2 GlusterFS Storage

GlusterFS is a distributed File system where data is spread throughout different servers while users can refer to it as one namespace. GlusterFS unifies data across the nodes in a scalable manner without excessive metadata usage. Red Hat Virtualization uses GlusterFS to divide available disk storage into volumes that can be purposed for different needs. The following domains are mapped to GlusterFS volumes and allocated per deployment requirements:

- **data:** all templates and installation media should be stored here including ISOs, base QCOW2s, OVA and OVF templates, etc.
- **hosted_storage:** reserved for the Hosted Engine, do not upload or provision anything here.
- **isostore:** reserved for ISOs uploaded through DDT scripts. Soon to be deprecated.
- **vmstore:** all VM disks should be stored here as it is provisioned with the most storage space and replicated across the cluster for high availability.

9.2.1 GlusterFS Volume Bricks

GlusterFS storage is based on the concept of exported brick directories from a trusted storage pool that make up a volume. These bricks can be distributed, replicated, dispersed, striped, or a mixture of types. For DDT, all bricks are distributed and the **vmstore** brick is also dispersed across all nodes and replicated once. On the RHVH nodes, bricks are in the following directory: **/srv/bricks**

9.2.2 Gluster Command Line Interface (CLI)

To interact with Gluster, operators must use the Gluster CLI to input commands. Gluster commands can be executed by entering the Gluster CLI or by denoting **gluster** before the appropriate command.

```
--- Example 1 : Launch interactive Gluster CLI ---
[root@node ~]# gluster
gluster> help

--- Example 2 : Invoke gluster through command options ---
[root@node ~]# gluster help
```

9.2.3 Common Administration Tasks

GlusterFS, as an application, is very hands-off for operators as RHVH is responsible for all interfacing with it directly. However for monitoring or troubleshooting purposes, the following tasks are outlined below.

Gluster Peers

In order to see connected Gluster nodes (peers), use the **peer status** command. Each node should have either two peers in a three-node setup, or five peers in a six-node setup.

```
[root@node ~]# gluster peer status
Number of Peers: 2

Hostname: 10.52.52.21
Uuid: 948614dc-271b-49e2-a71e-b6721fd11098
State: Peer in Cluster (Connected)

Hostname: 10.52.52.22
Uuid: 84aea0af-a79c-43fb-ab48-f9cecf40226d
State: Peer in Cluster (Connected)
```

List Gluster Volumes

To find a list of volumes in Gluster, use the **list** command.

```
[root@node ~]# gluster volume list
data
engine
isostore
vmstore
```

Gluster Volume Information

To view information about Gluster volumes, use the **info** command.

```
[root@node ~]# gluster volume info
<volume> Volume Name: <volume>
Type: Distribute
Volume ID: 18f4bbca-ad1b-46b6-8a73-dfbac8e282d9 Status: Started
Snapshot Count: 0 Number of Bricks: 3
Transport-type: tcp Bricks:
Brick1:
10.52.52.20:/srv/bricks/brick_data/data
Brick2:
10.52.52.21:/srv/bricks/brick_data/data
Brick3:
10.52.52.22:/srv/bricks/brick_data/data
Options Reconfigured:
nfs.disable: on transport.address-family:
inet storage.owner-gid: 36 cluster.quorum-type: auto storage.owner-uid: 36
network.ping-timeout: 10
```

✎ **Note**: To see information about all volumes, use the keyword “all.”
For Example: **gluster volume infoall**.

Gluster Volume Status

To see the current state of a Gluster volume, use the **status** command. This command will show the status of all bricks associated with the volume, the port it is running on, and the ID of the process.

```
[root@node ~]# gluster volume status <volume>
Status of volume: data
Gluster process                     TCP Port    RDMA Port    Online  Pid
------------------------------------------------------------------------------
Brick 10.52.52.20:/srv/bricks/           49157       0          Y       53618
brick_data/data
Brick 10.52.52.21:/srv/bricks/           49157       0          Y       48528
brick_data/data
Brick 10.52.52.22:/srv/bricks/           49157       0          Y       51937
brick_data/data


Task Status of Volume data
------------------------------------------------------------------------------
There are no active volume tasks
```

Start/Stop Gluster Volumes

If a Gluster volume has failed or needs to be restarted, use the **start/stop** command to bring the volume bricks online/offline. This will attempt to start bricks on all nodes.

```
[root@host ~]# gluster volume start <volume>
```

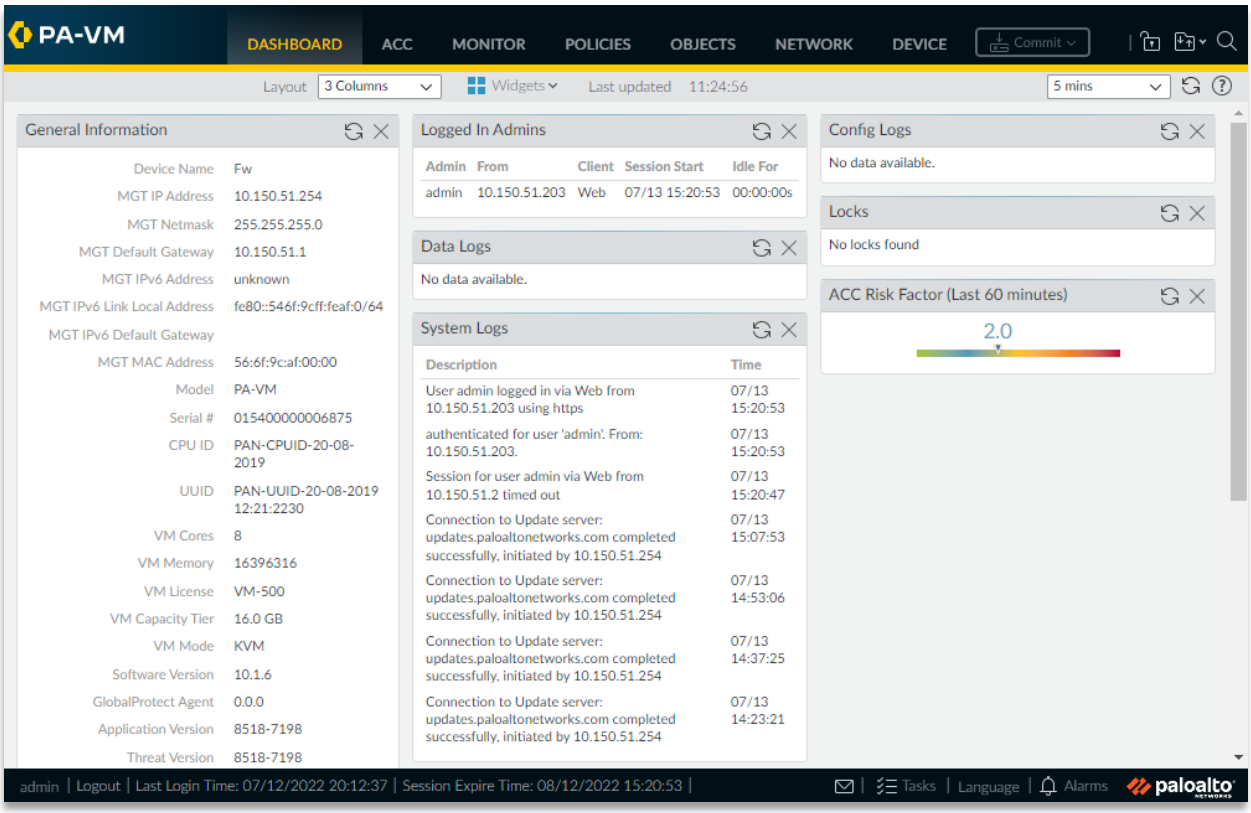
10 Palo Alto Virtual Firewall

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.

10.1 Palo Alto Web Interface

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#}.51.254`** with the following default credentials:

Username: admin
Password: [password from passwords.yml]

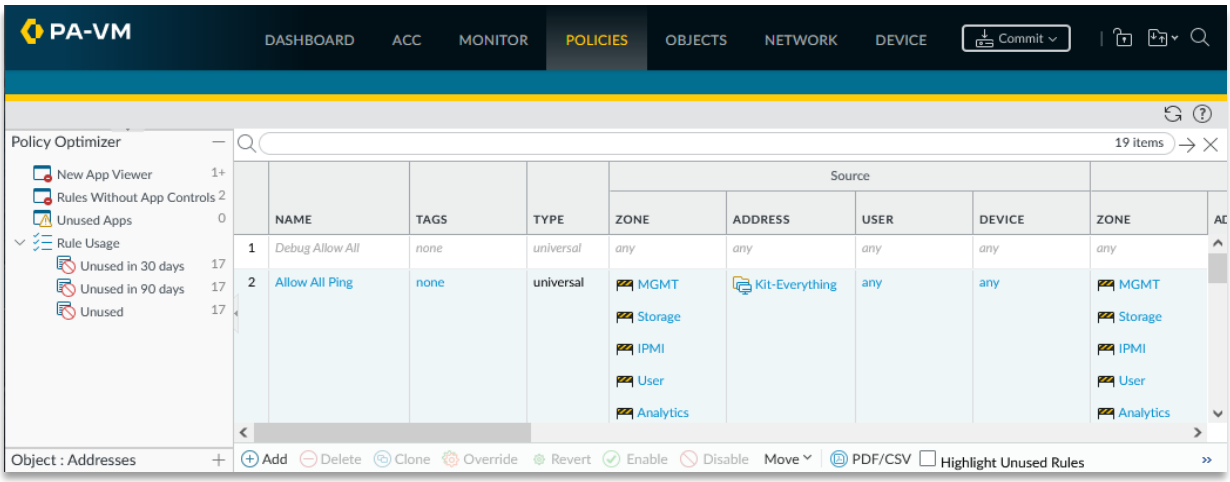


10.1 Palo Alto Web Interface

10.2 Common Administration Tasks

10.2.1 Creating Security Policy Rules

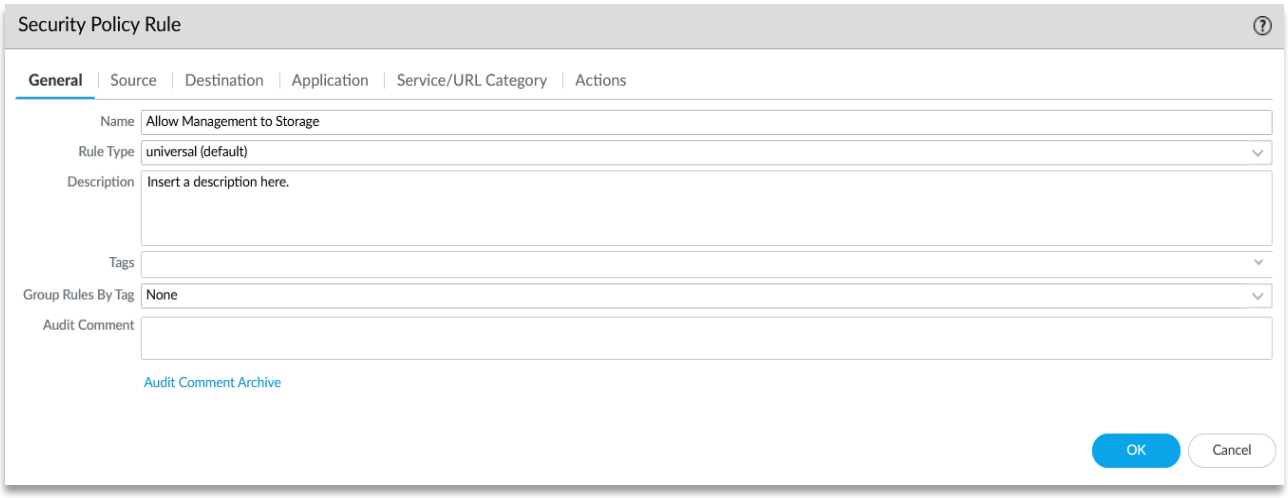
1 Select the **Policies** tab at the top of the webpage.
2 From within, click **Add** to create a new policy.
3 Fill in the following required settings within the General tab (the rest are optional):



10.2.1(a) Security Policy Overview

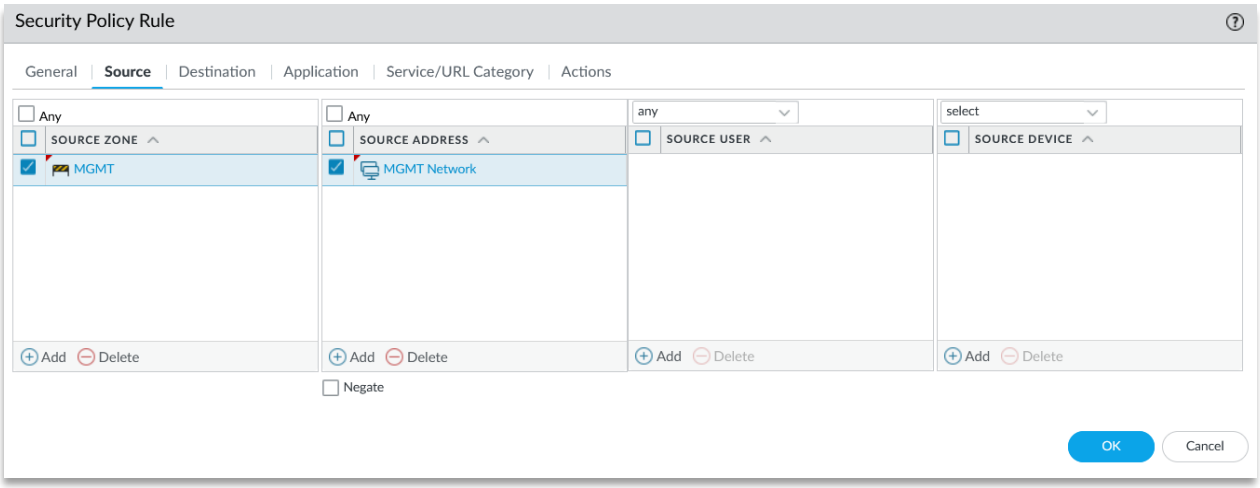
Name: Select an appropriate description.

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.



10.2.1(b) Security Policy Rule Settings

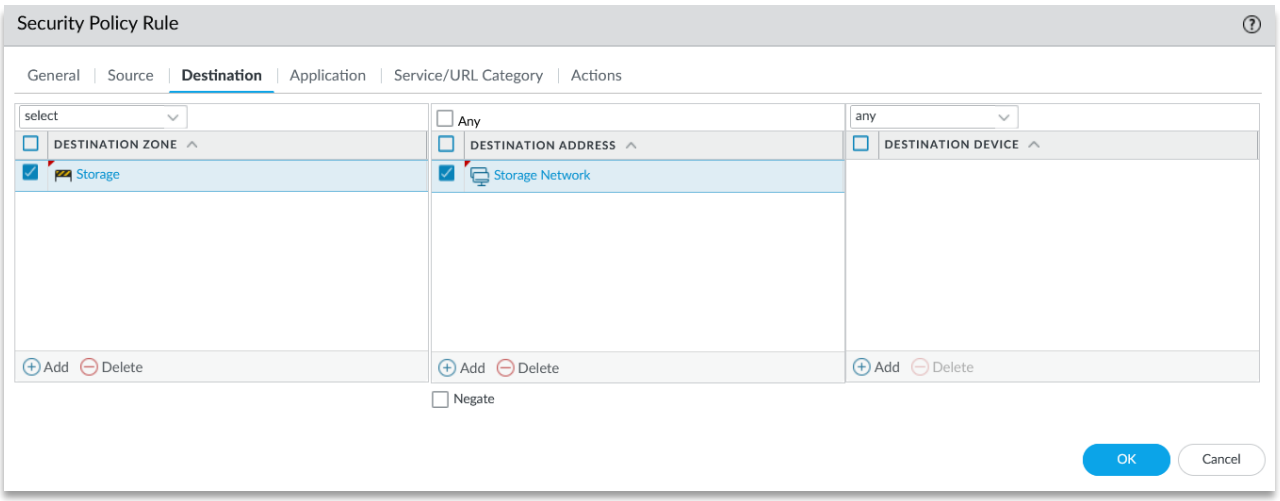
4 Switch to the **Source** tab. Add the desired source zone and source address range.



10.2.1(c) Security Policy Source Options

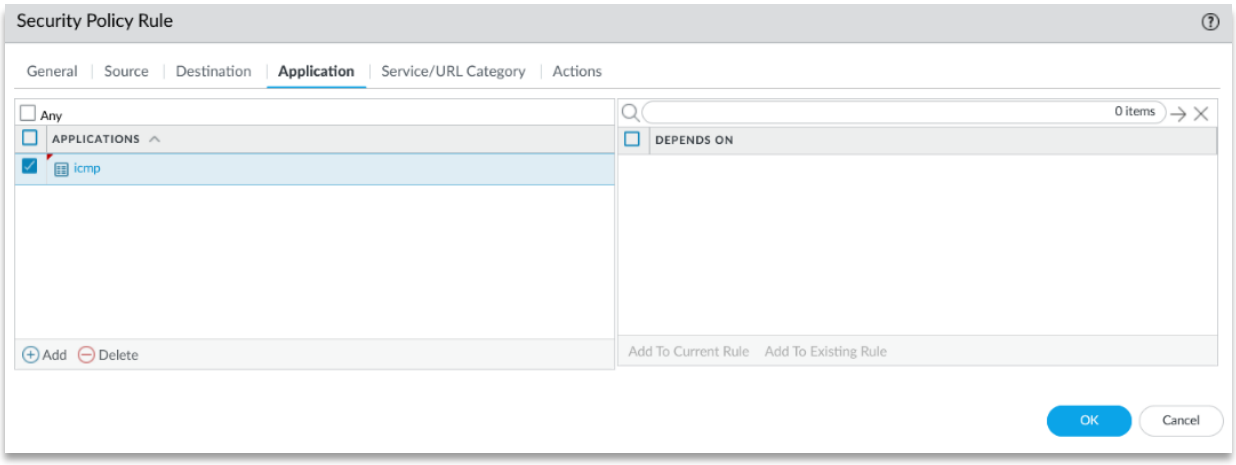
✎ **Note**: The **User** tab is not typically used but can add a user and HIP Profile to this policy if desired.

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



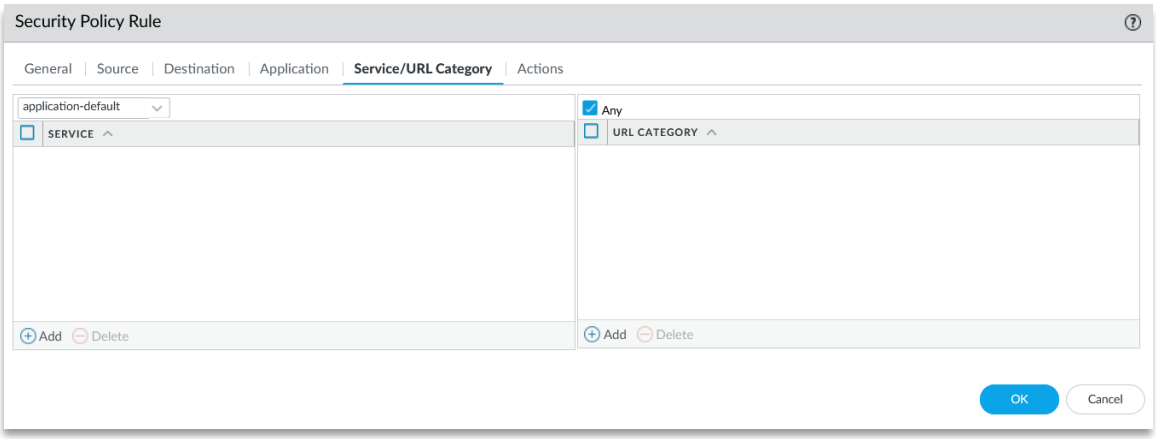
10.2.1(d) Security Policy Destination Options

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



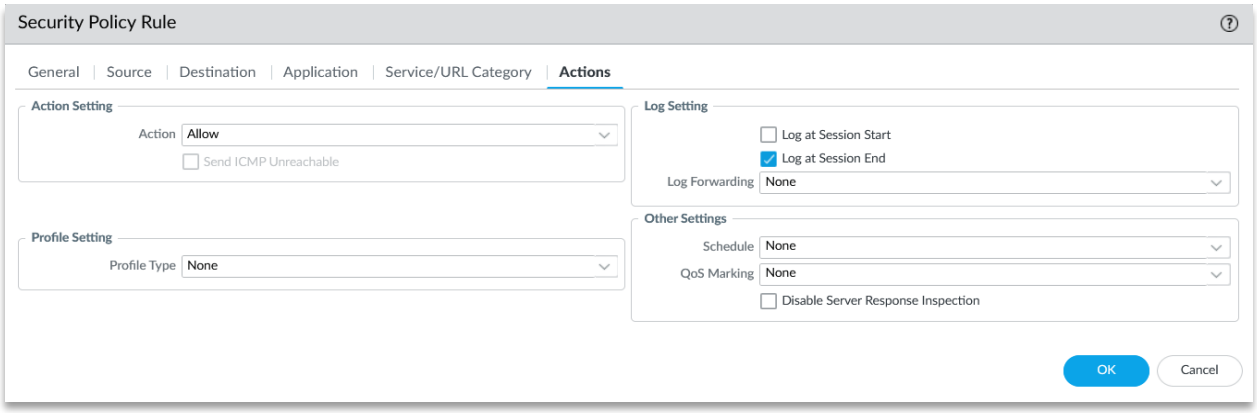
10.2.1(e) Security Policy Application Settings

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



10.2.1(f) Security Policy Service/URL Settings

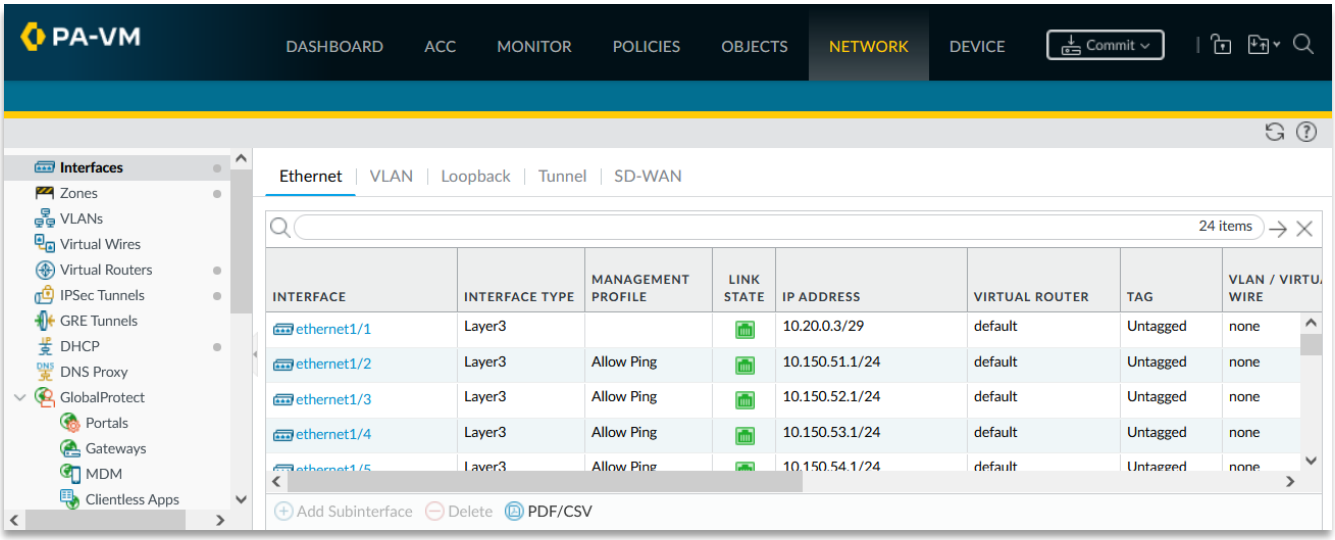
8 Switch to the **Actions** tab and fill in the settings as desired and click **OK** when finished.



10.2.1(g) Security Policy Rule Actions

10.2.2 Interface Management

1 Log in to the Palo Alto web interface.
2 Navigate to the **Network** tab at the top of the webpage.

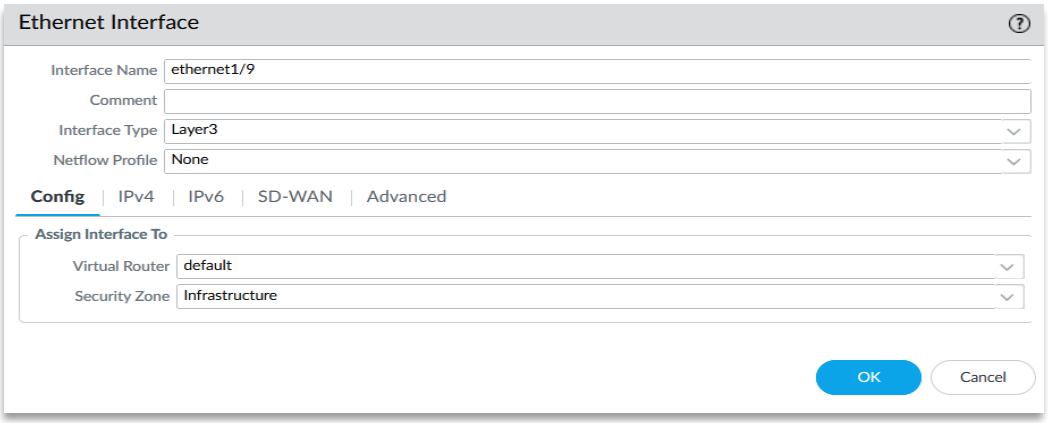


10.2.2(a) Ethernet Interface Overview

3 Within the **Ethernet** tab, click the desired interface.
4 Fill out the **Interface Type:** Choose between Layer2, Layer3, Virtual Wire, TAP and HA.

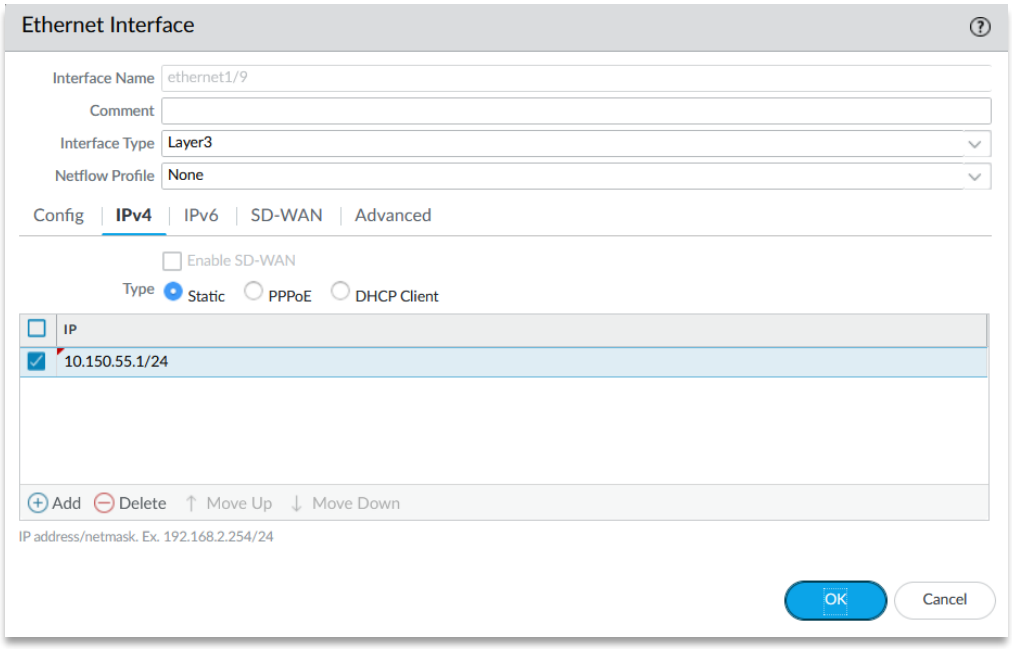
✎ **Note**: Configuration options below are dependent on the selected interface type. The next steps will go over the configuration for a layer 3 interface.

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



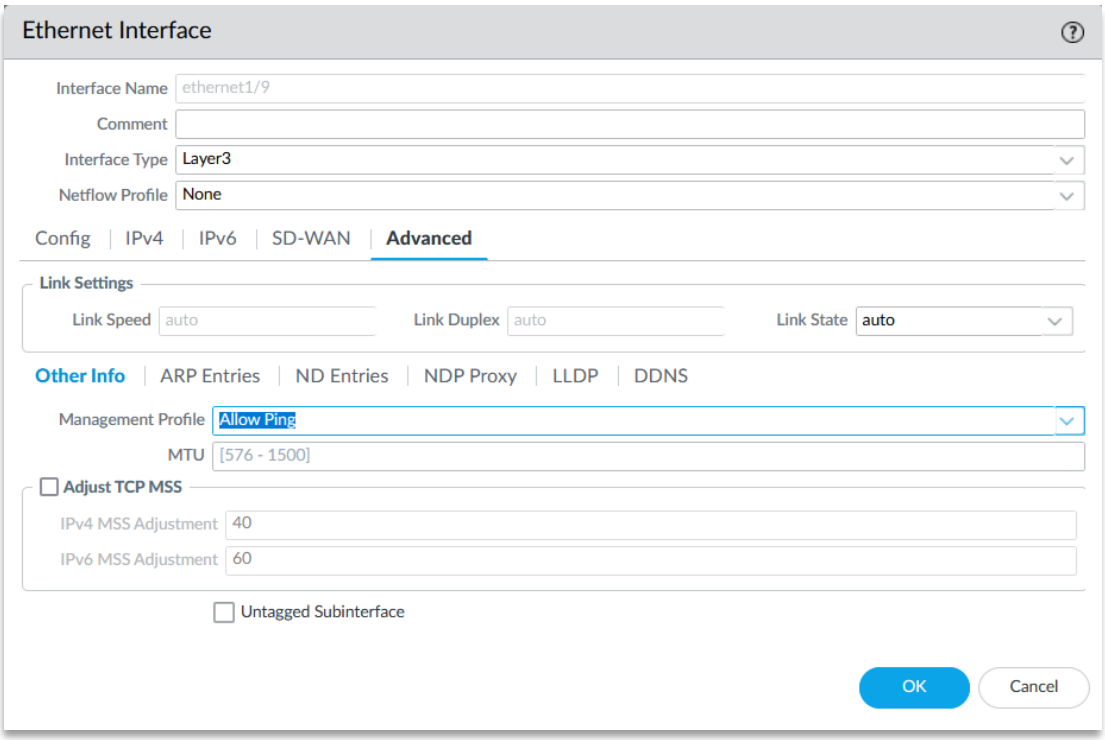
10.2.2(b) Ethernet Interface Settings

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



10.2.2(c) Ethernet IPv4 Settings

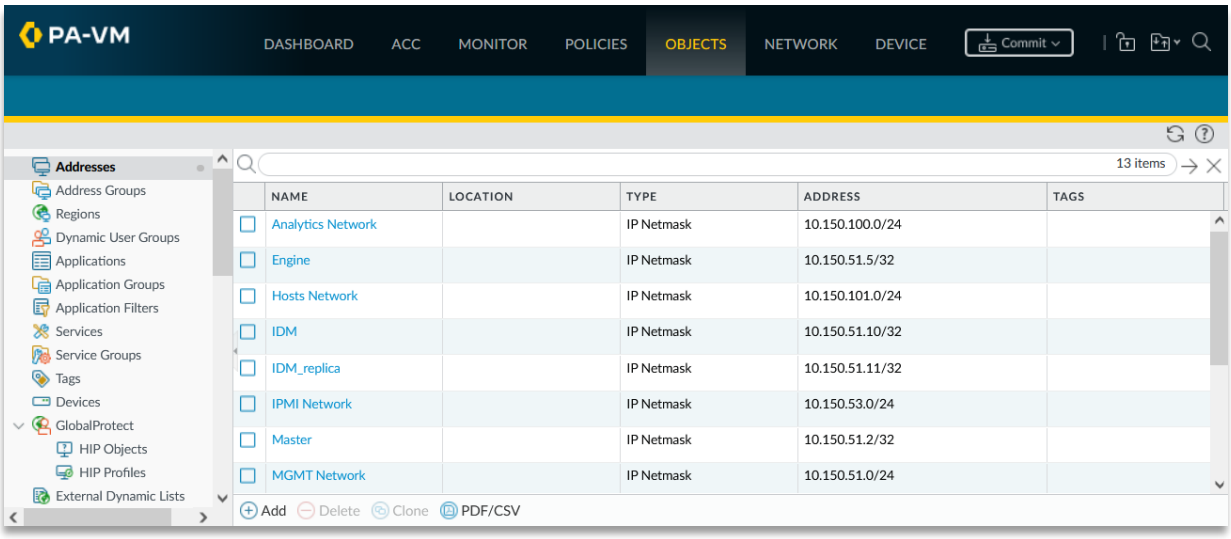
7 Click **Advanced** and populate additional fields as needed. Important fields to consider are MTU, Management profiles and LLDP. The “Allow Ping” profile is selected below.



10.2.2(d) Ethernet Advanced Settings

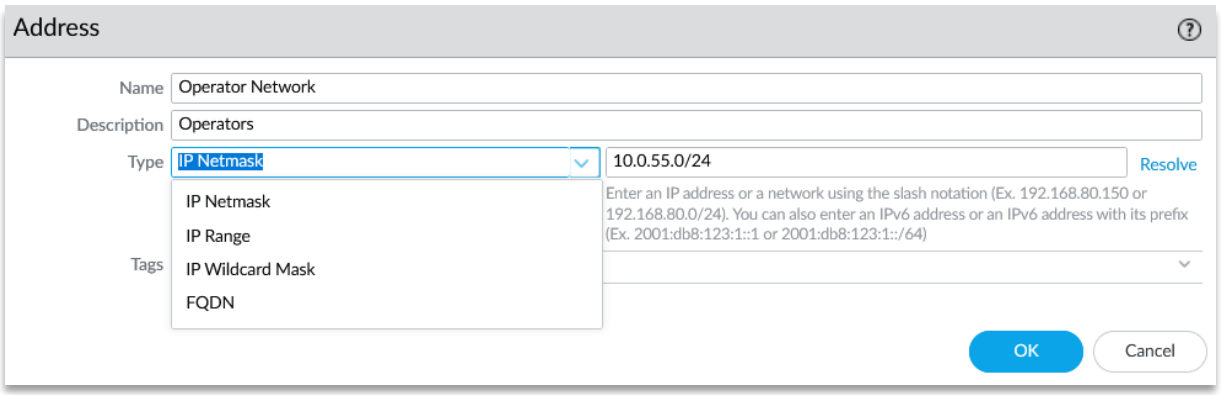
10.2.3 Objects

1 Click **Objects** on the top of the webpage.
2 Click **Add** at the bottom of the webpage.



10.2.3(a) Objects

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.



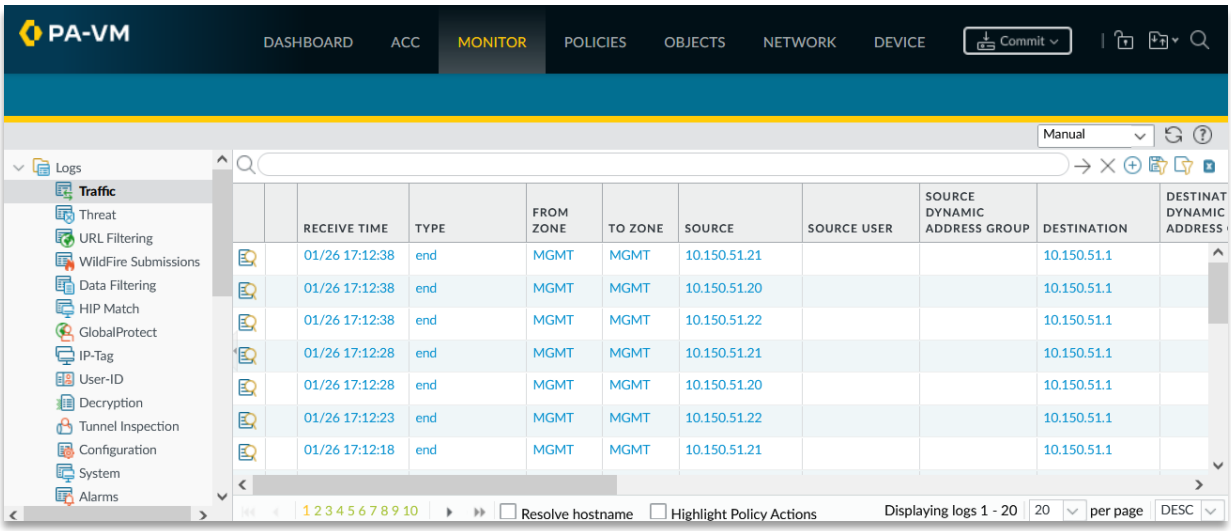
10.2.3(b) Address Object Settings

10.2.4 Monitor Traffic

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

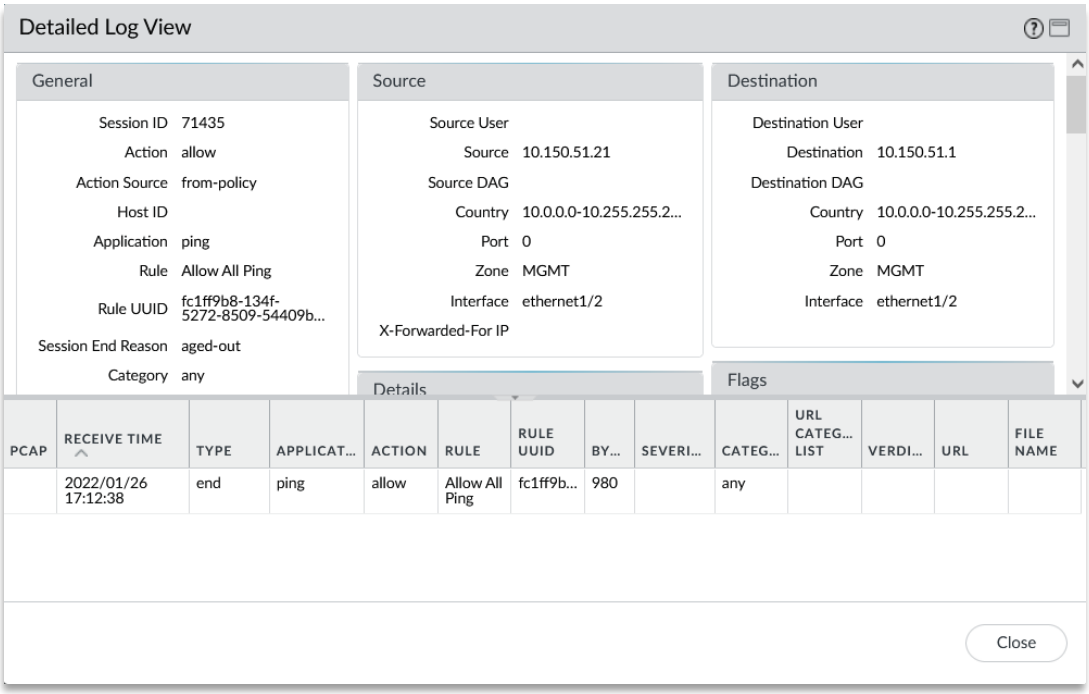
1 Navigate to the **Monitor** tab at the top.
2 Click **Traffic** in the **Logs** category tree to the left.

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



10.2.4(a) Monitoring Network Traffic

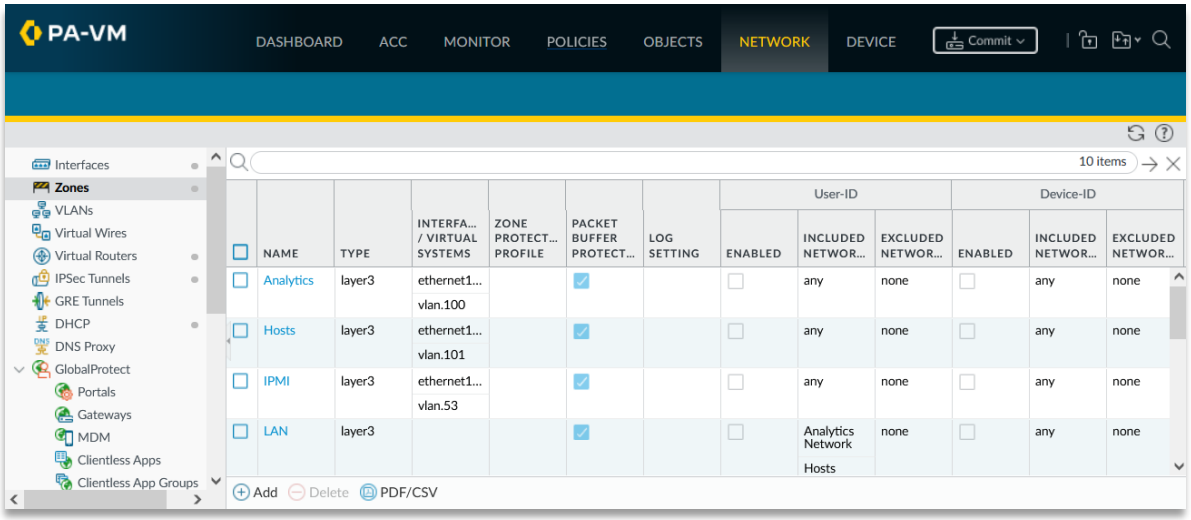
3 Click on the magnifying glass to view more details.



10.2.4(b) Inspecting Network Traffic

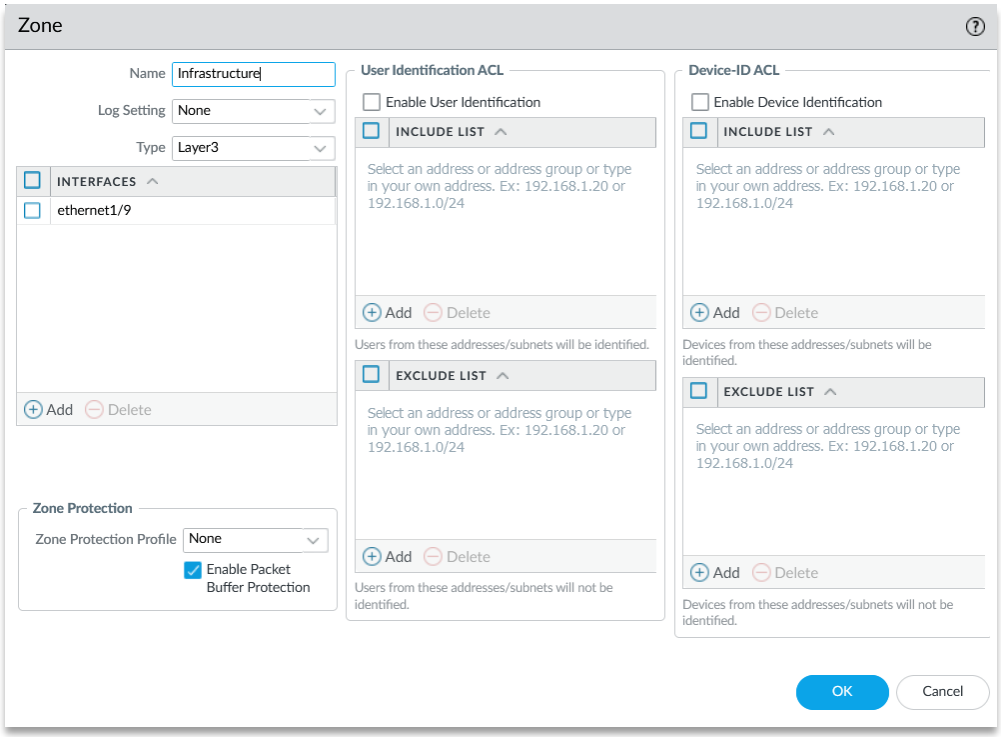
10.2.5 Zones

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



10.2.5(a) Network Zones Overview

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.

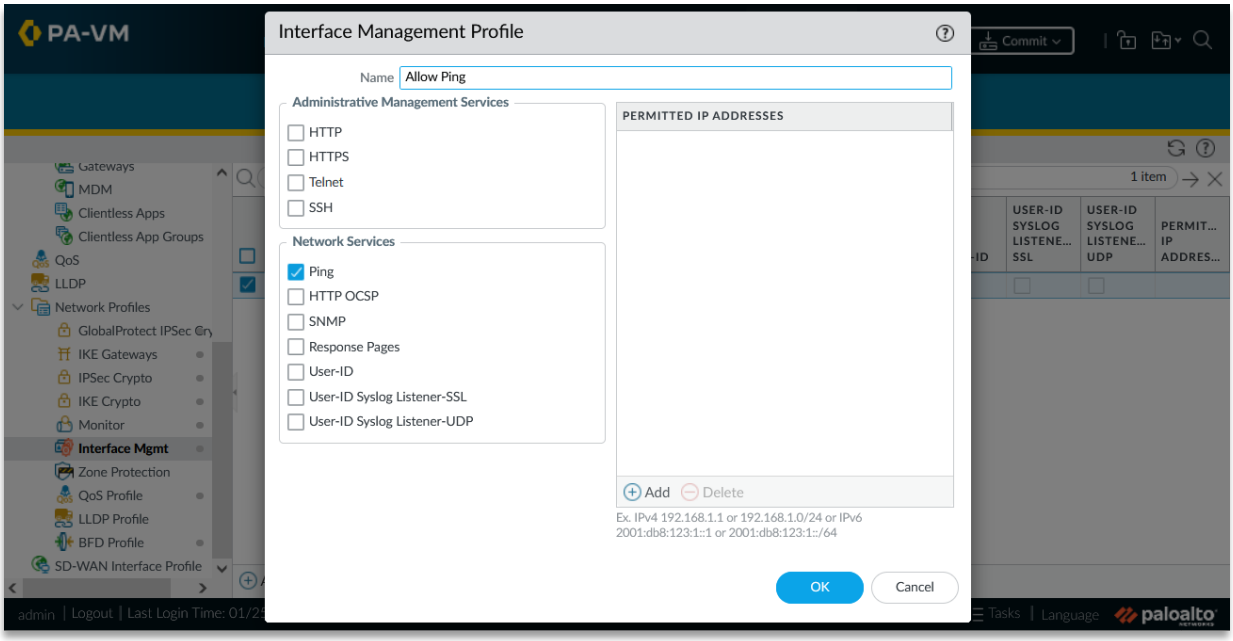


10.2.5(b) Zone Settings

10.2.6 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.

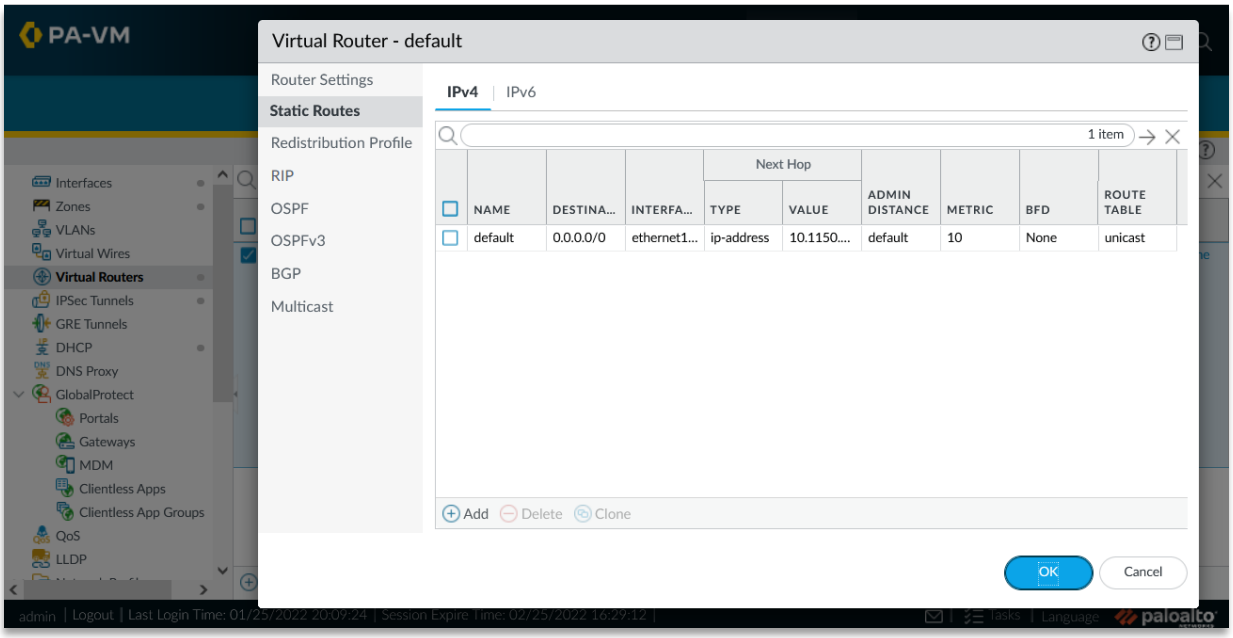


10.2.6 Interface Management Profile

5 Press **OK** once finished.

10.2.7 Routes

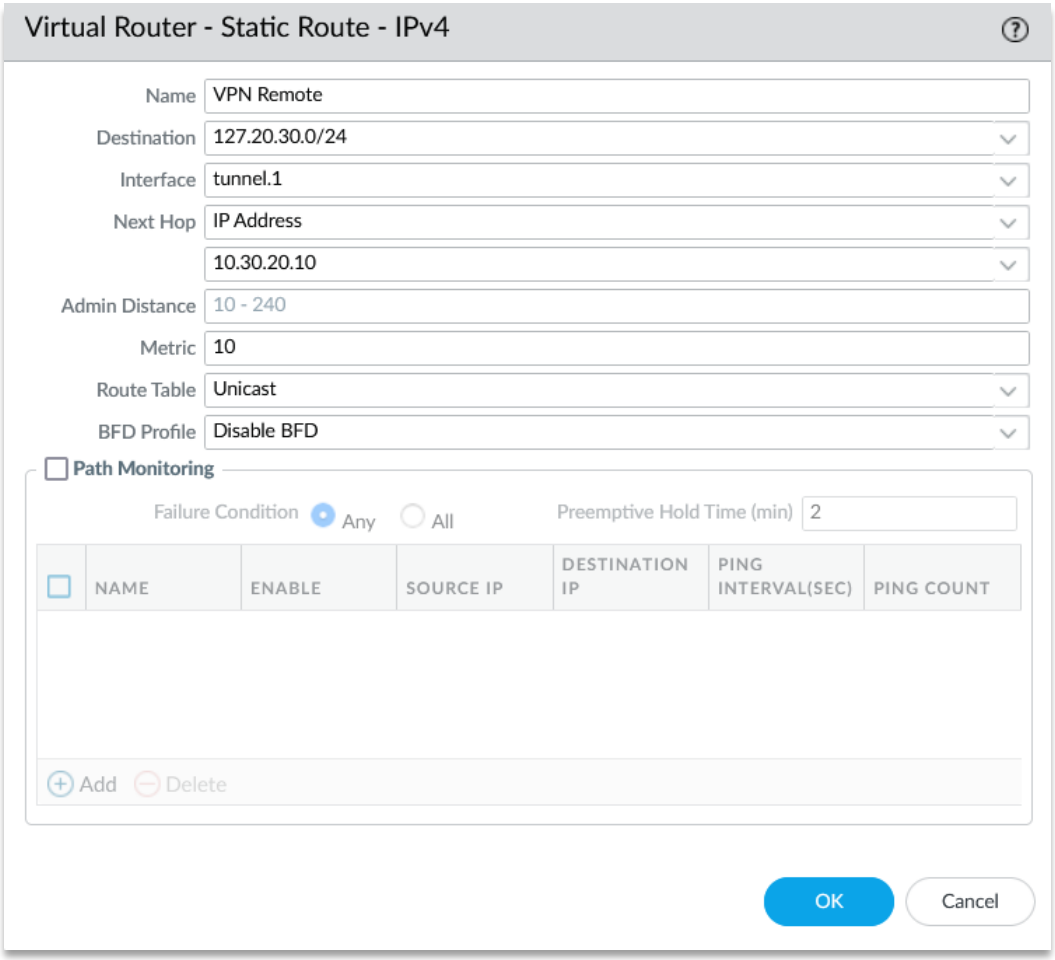
1 Click **Network** at the top of the web interface.
2 Select **Virtual Routers**.
3 Choose and edit the default or preferred virtual router.
4 Click **Static Routes** on the left.
5 Click **Add** towards the bottom of the page.



10.2.7(a) Virtual Router Static Routes Overview

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.



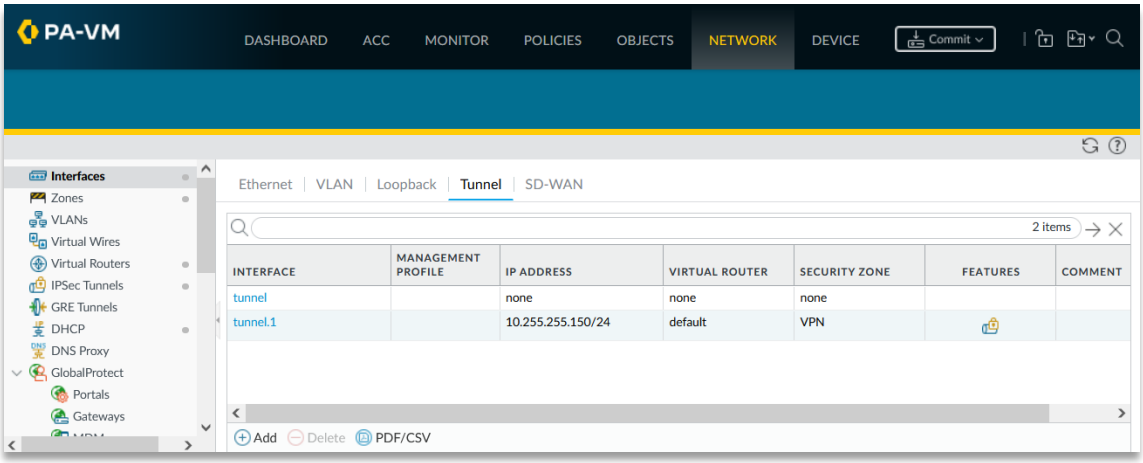
10.2.7(b) Virtual Router Static Route Options

10.2.8 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.

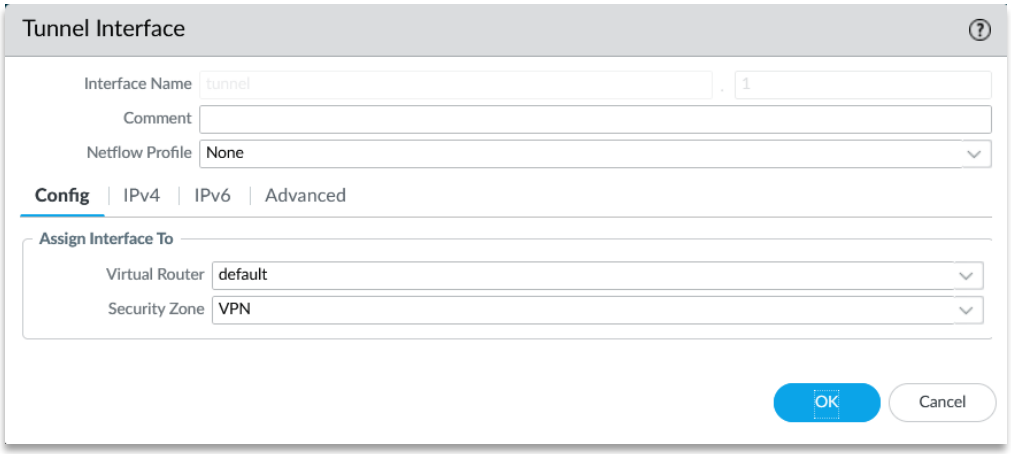
Create a Tunnel

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.**



10.2.8(a) Tunnel Interfaces

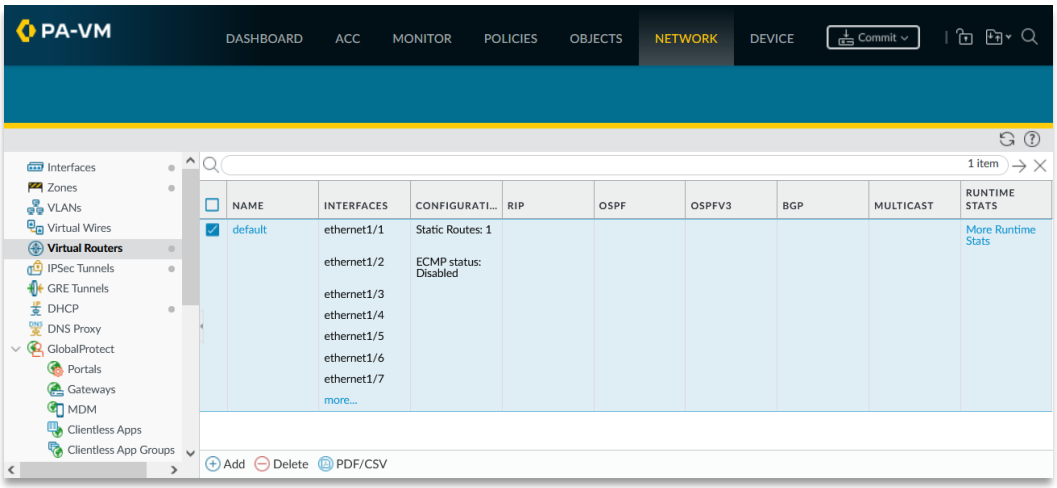
5 Populate the following settings:
- Provide an **Interface Number ID** (eg. tunnel.1)
- Set the **Virtual Router** to default
- Set the **Security Zone** according to traffic then press **OK**.



10.2.8(b) Tunnel Interface Configuration

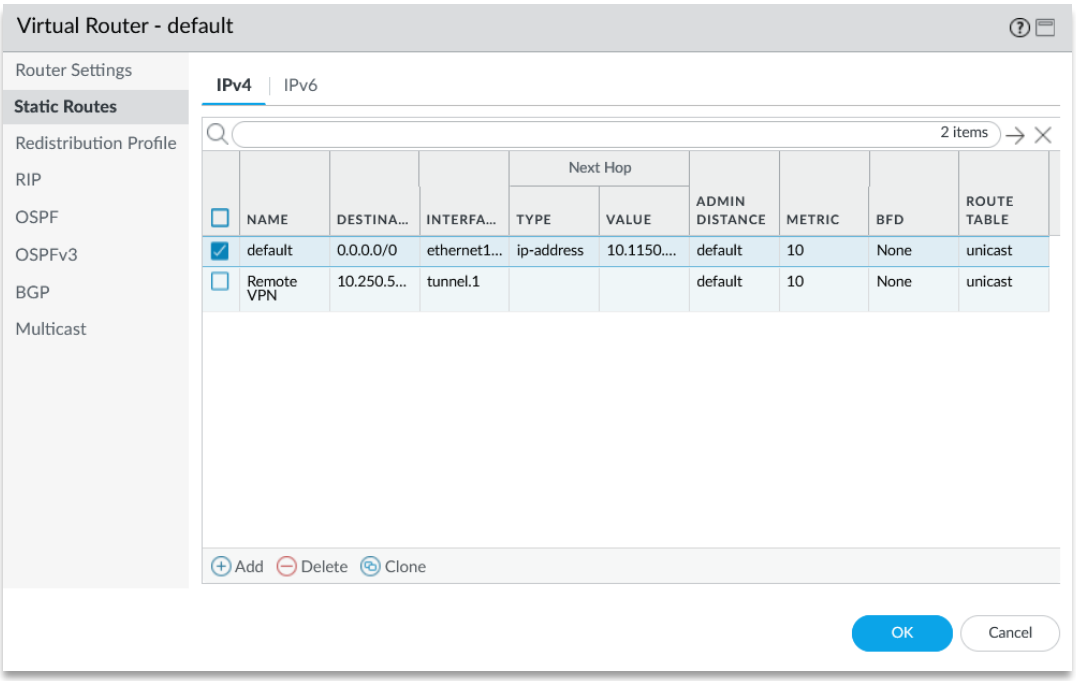
Add a Static Route

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



10.2.8(c) Virtual Router Summary

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

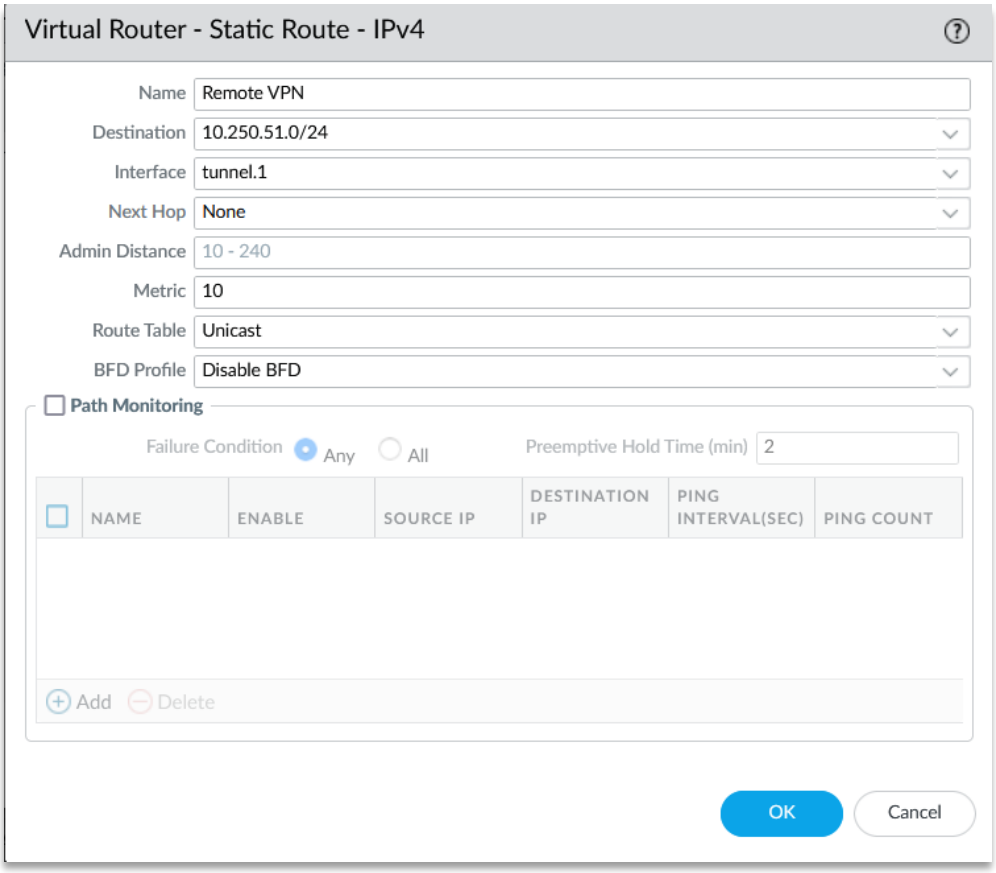


10.2.8(d) Virtual Router Static Routes Overview

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

6 Next, complete the following tasks:

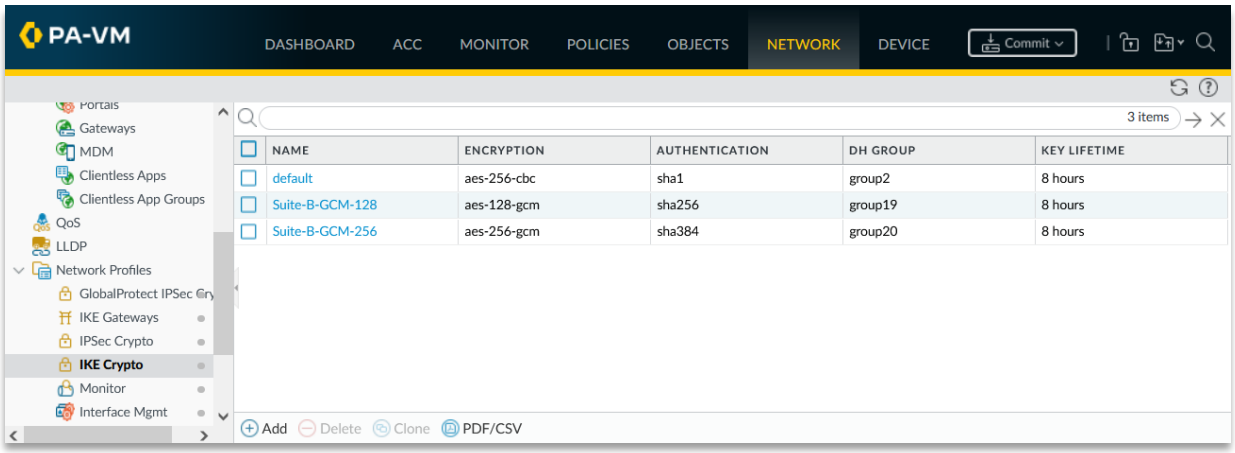
- Set a **Name**.
- Give a **Destination** IP as the IP address of the management interface on the other router.
- Give an **Interface** of tunnel.1.
- Give the **Next Hop** as none.
- Other fields can be left blank. Click **OK** to save.



10.2.8(e) Virtual Router Static Route Settings

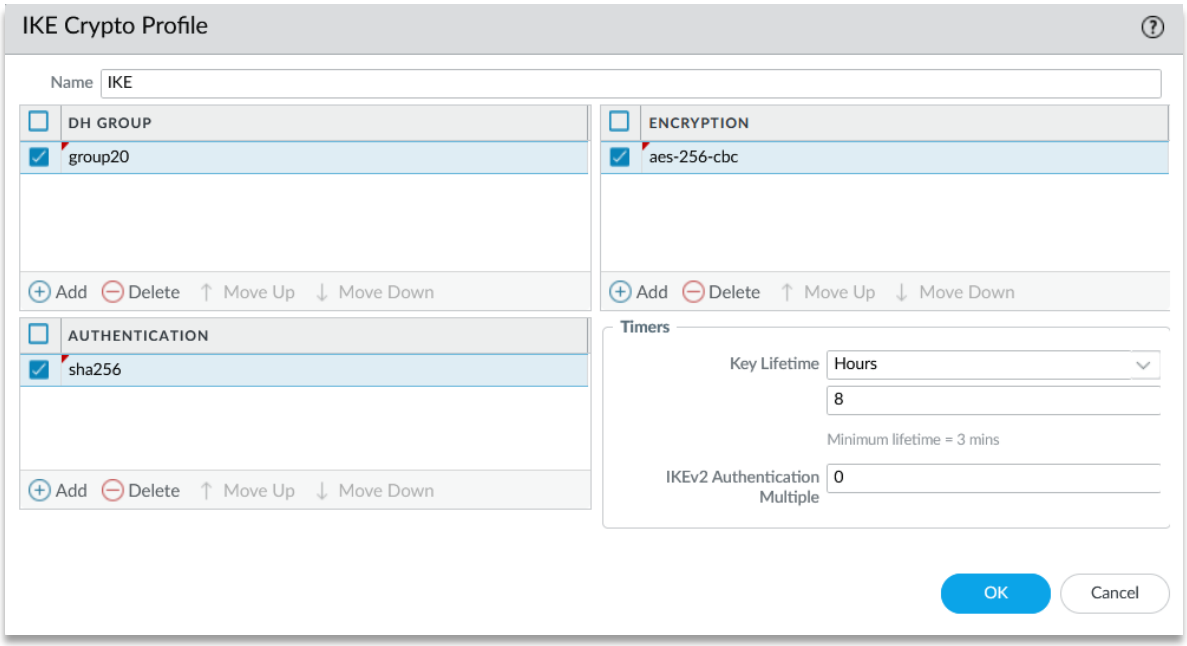
Create an IKE Crypto Profile

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.



10.2.8(f) IKE Crypto Overview

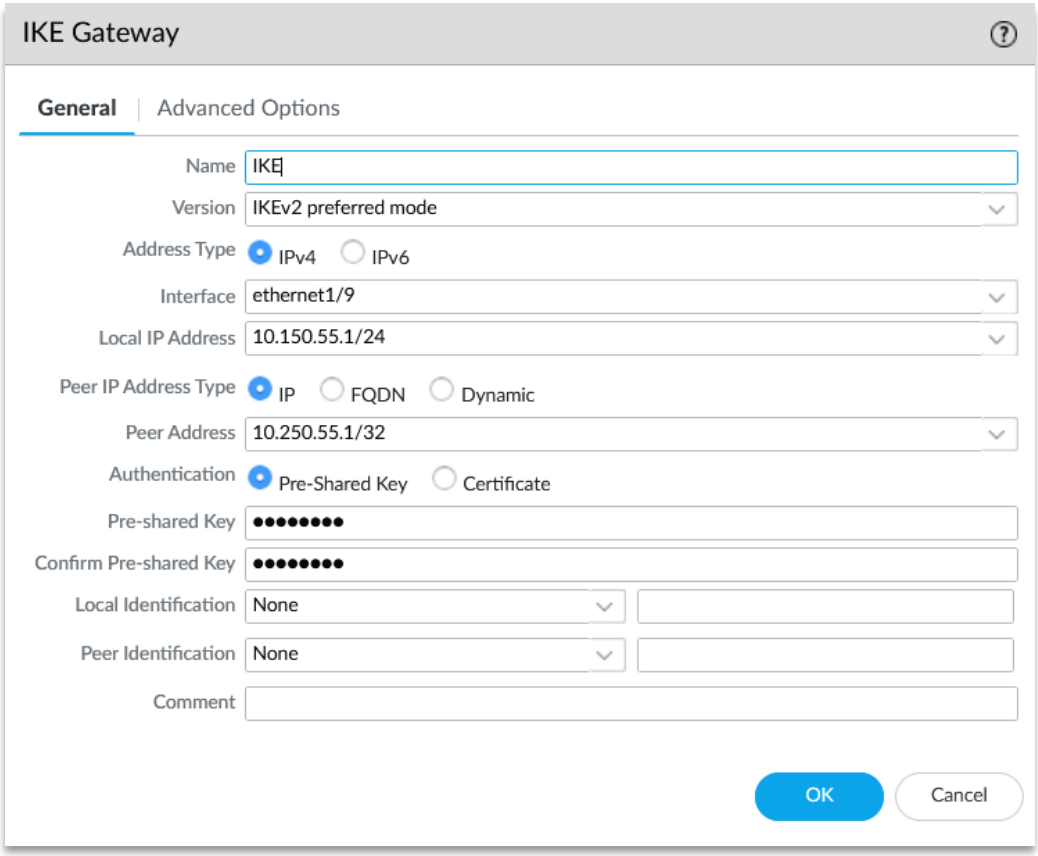
4 Complete the following tasks:
- Set a desired **Name**
- Set the **DH Group** to **group20**.
- Set the **Encryption** to **aes-256-cbc**.
- Set the **Authentication** to **sha256**.
- Finally set **Key Lifetime** to 8.
- Press **OK** to save and close.



10.2.8(g) IKE Crypto Profile

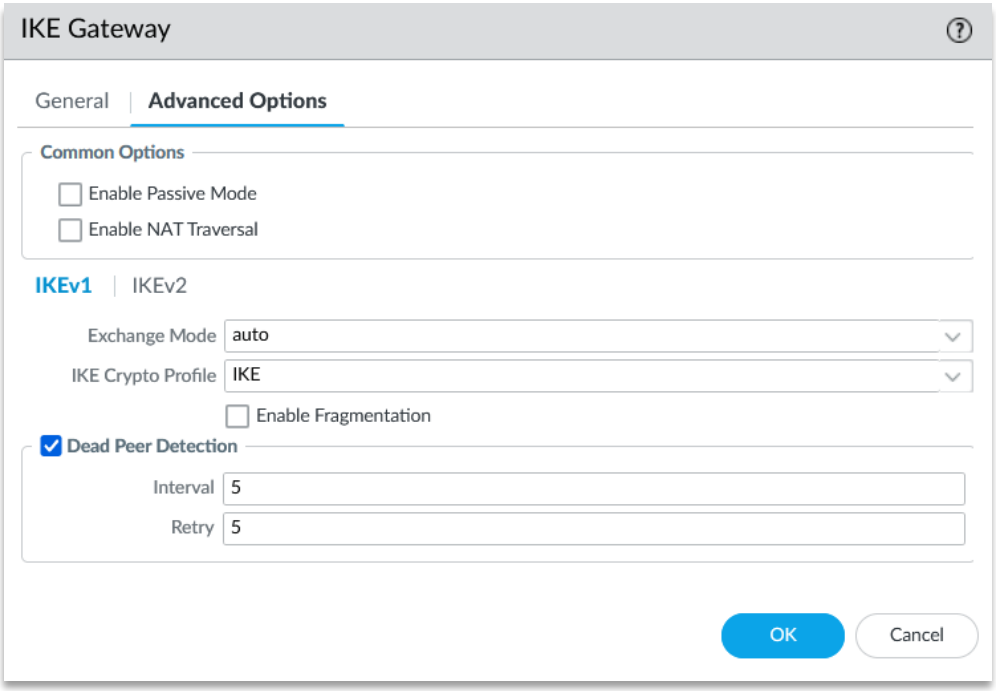
Create an IKE Gateway

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.



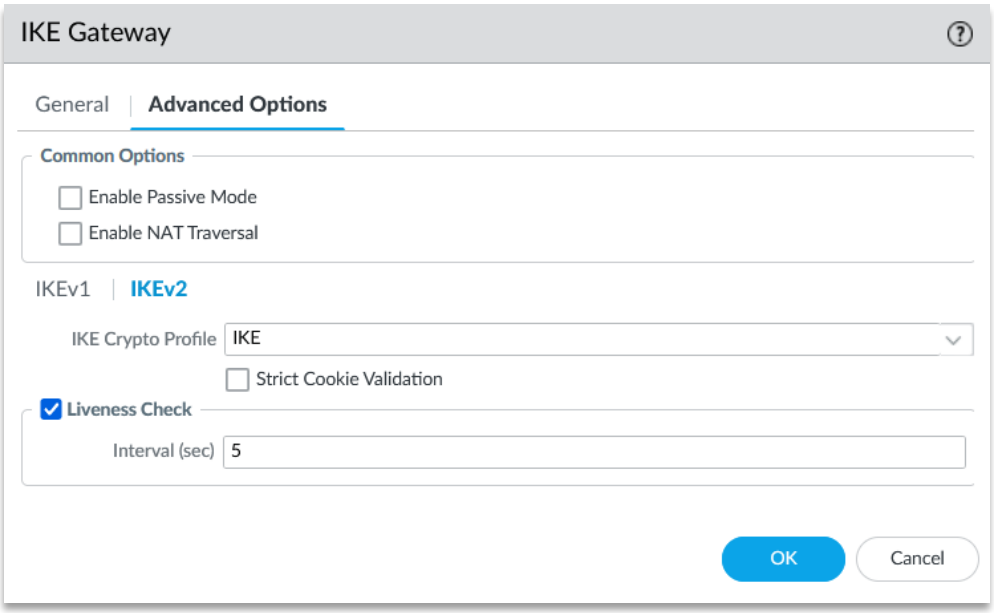
10.2.8(h) IKE Gateway Settings

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**.



10.2.8(i) IKEv1 Settings

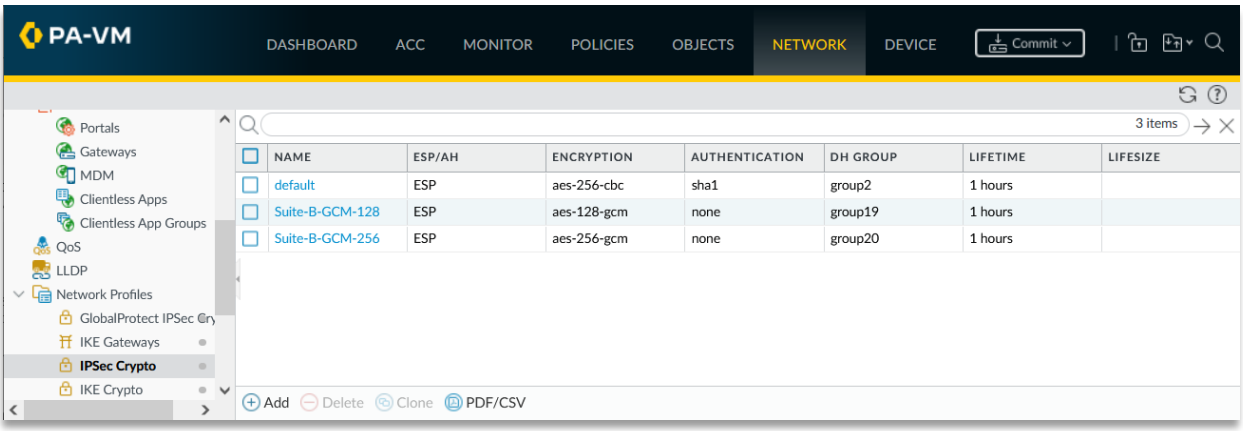
5 Within **Advanced Options**, switch to the **IKEv2** tab and select the **IKE Crypto Profile** previously created. Press **OK** to save and exit.



10.2.8(j) IKEv1 Settings

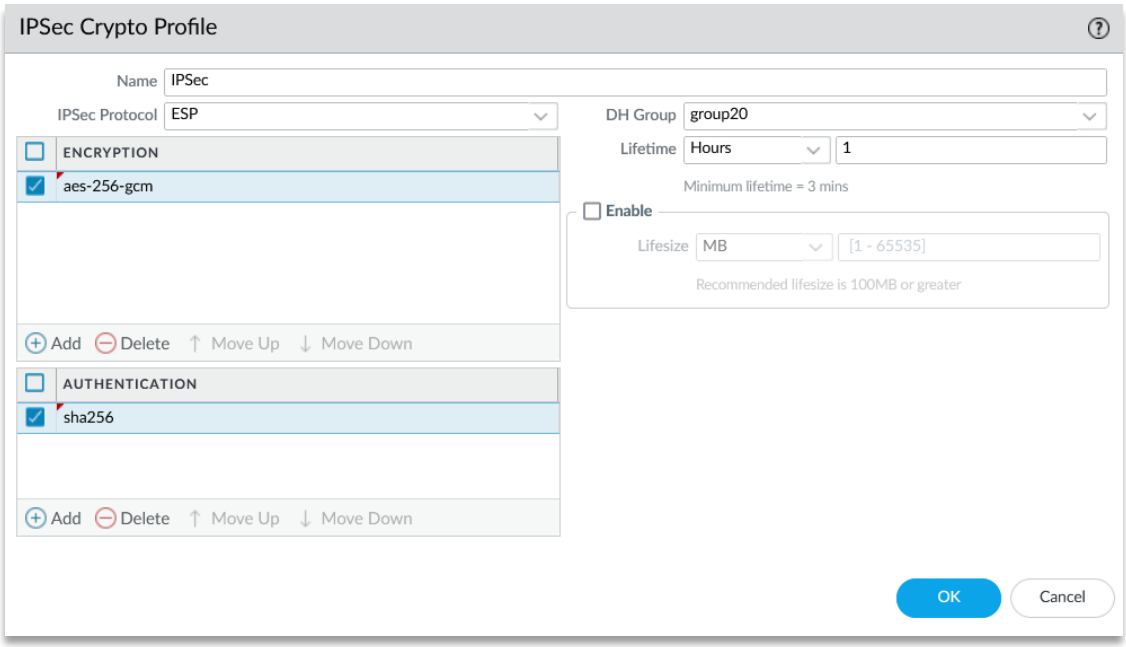
Create an IPSEC Crypto Profile

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



10.2.8(k) IPSEC Crypto Overview

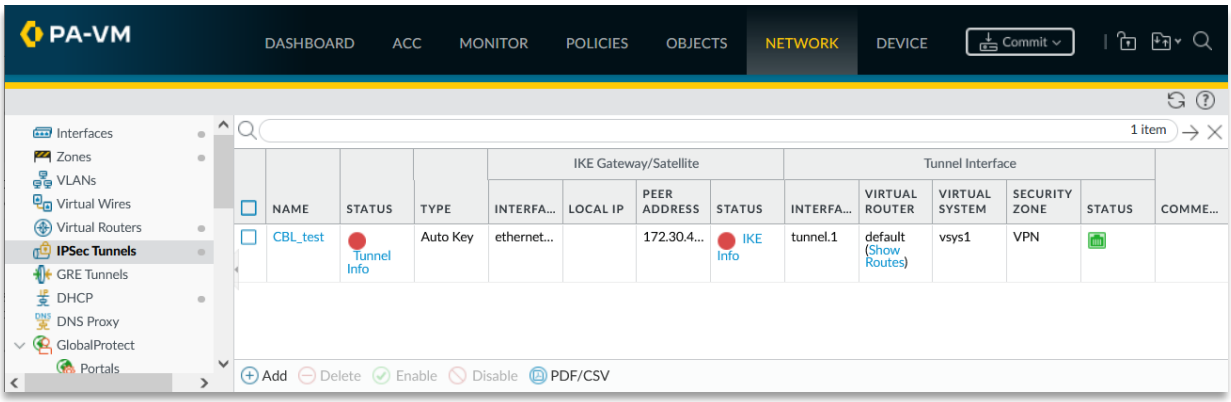
3 Press **Add** towards the bottom.
4 Complete the following tasks (the rest are optional):
- Set a desired **Name**
- Press **Add** and set the DH Group to **group20**.
- Set the **Encryption** to **aes-256gcm** and the **Authentication** to **sha256**.



10.2.8(l) IPSEC Crypto Profile

Create an IPSec Tunnel

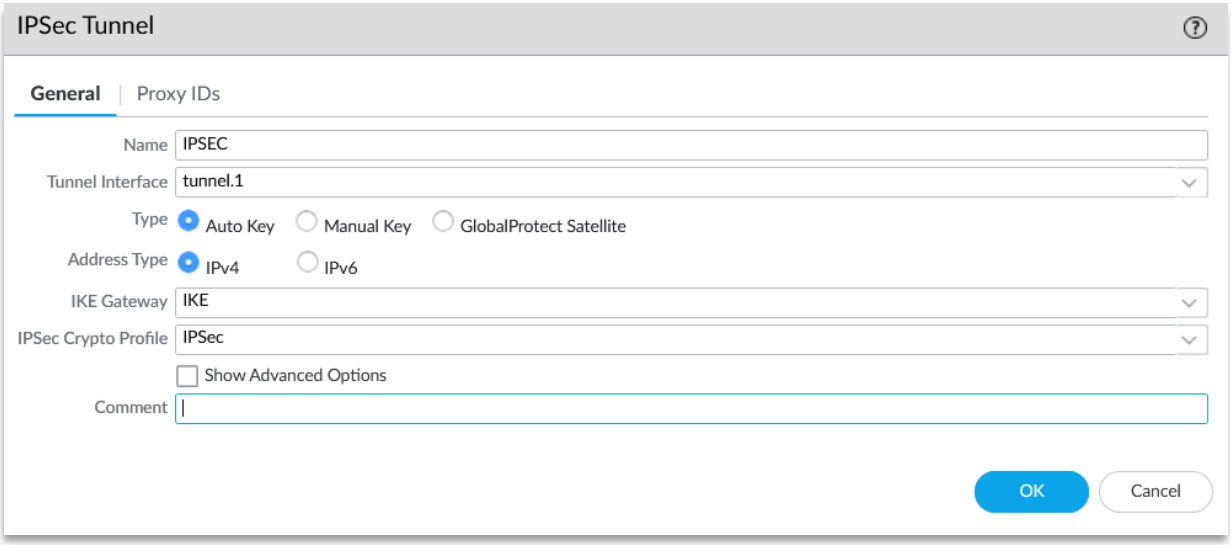
1 Navigate to the **Network** tab, then choose **IPSec tunnels** on the left.



10.2.8(m) IPSec Tunnel Overview

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.



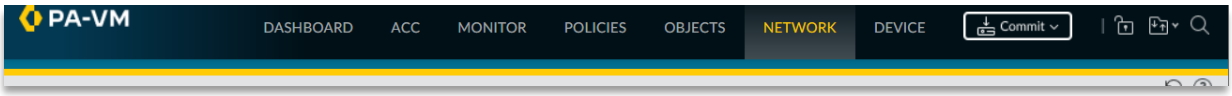
10.2.8(n) IPSec Tunnel Settings

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

10.3 Committing changes

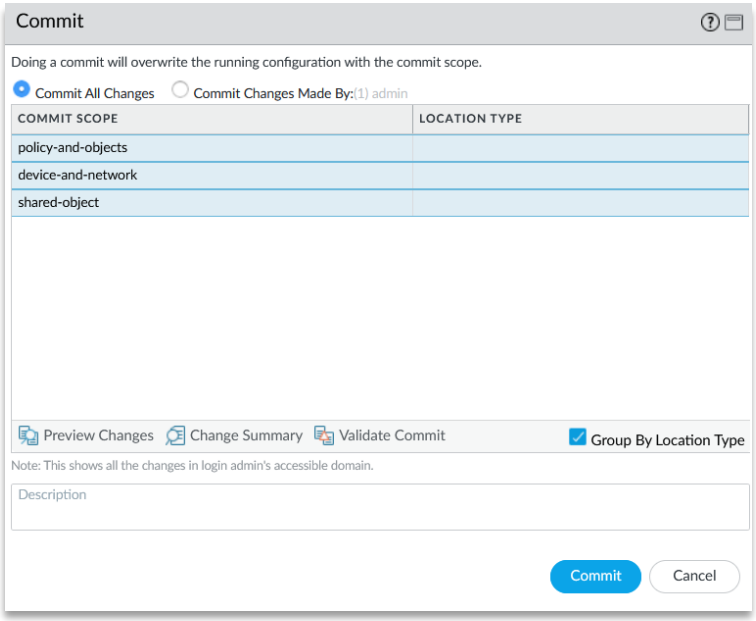
In Palo Alto it is important to frequently commit changes after modifying the configuration. Follow these steps to save all pending changes:

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



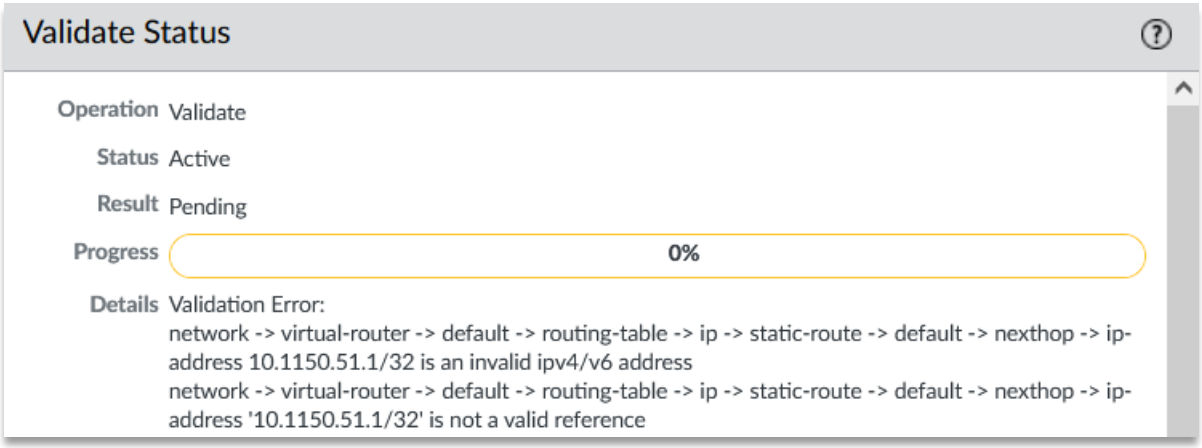
10.3(a) Commit Menu Location

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



10.3(b) Commit Menu Options

3 Optionally, use **Validate Commit** to review issues with any pending changes.



10.3(c) Commit Menu Options

11 Additional Notes on Kit's Configuration

11.1 Network (Firewall and Switch) Configuration

Managing proper network configuration of 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.

11.1.1 DDS-M Kit's Network (VLAN) Configuration

A deployed DDS-M kit, both 3 and 6 nodes cluster setup, will have total 7 networks.

Internal Networks	
`10.kit#.51.0/24`	Management Network
`10.kit#.52.0/24`	Storage Network
`10.kit#.53.0/24`	IPMI Network
`10.kit#.54.0/24`	User Network

Operational Networks	
`10.kit#.100.0/24`	Analytics Network
`10.kit#.101.0/24`	Hosts Network
`10.kit#.102.0/24`	NSM Network

Internal Networks are essential to deploy, manage, and operate a DDS-M kit. Operational Networks are there to provide networks to various VM tools and help users adapt to various mission environment.

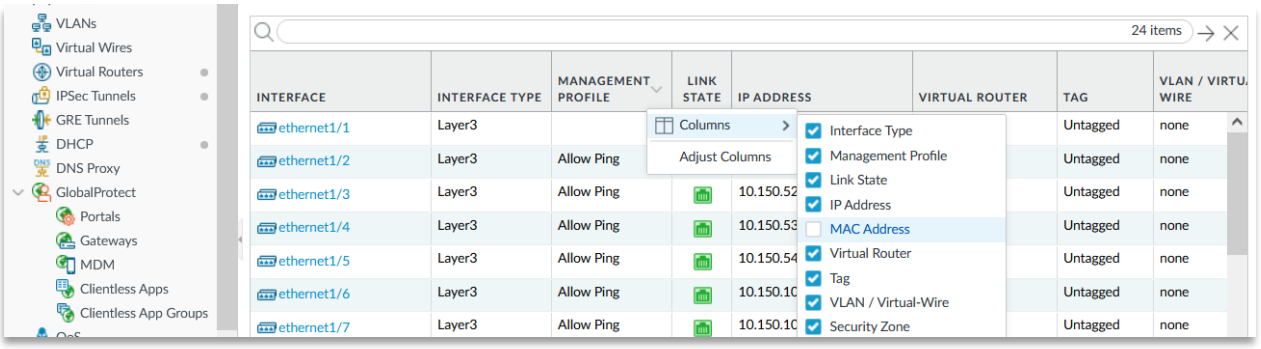
11.1.2 Palo Alto (virtual firewall) Configuration

As of DDT version 1.0.3, Palo Alto neither has any rules nor route traffic between VLANs when the kit is fully deployed. This is problematic because not only teams are required to use a firewall when conducting mission to secure mission environment, but also Palo Alto is required to make a VPN connection. In this section, recommended basic configurations of interfaces, zones, DHCP forwarding, objects, a virtual router, and basic policies will be covered.

11.1.3 Interfaces

Enabling MAC Addresses of Ethernet Interfaces

1 Login to Palo Alto web interface at **`https://10.[kit num].51.254`**.



11.1.3 Palo Alto Interfaces

2 Go to **Network -> Interfaces -> Ethernet.**
3 Click the down arrow next to **Interface** -> Move the cursor over **Columns** -> Click **MAC Address.**
4 Commit changes (**Section 10.3**).
5 Compare the MAC addresses of Palo Alto's ethernet interfaces to assigned virtual interfaces of the Palo Alto VM on Hosted Engine web interface to identify and correct any misconfiguration.

`Engine URL: https://engine.[kit num]cpt.cpb.mil`.

Policy

Understanding how security policies work on the Palo Alto firewall is important to allow and deny traffic accordingly and efficiently.

There are three things to be noted.

1 There are two kinds of security policies: **Explicit** and **Implicit**. Explicit policies are defined by the user and visible. Implicit policies deny cross-zone traffic and allow same-zone traffic.
2 The Palo Alto firewall is a **stateful** firewall, meaning all traffic passing through the firewall is matched against a session and each session is then matched against a security policy. Only the client (where traffic initiates) to server flow direction needs to be defined.
3 A traffic is filtered through explicit policies from **top to bottom**.

11.1.4 Minicom

With the implementation of RHEL 8 on the Master Laptop, **screen** is now a deprecated service. The replacement is **minicom**, which requires configuration before use. Below are the steps to configure **minirc** profiles to use serial connections to the Dell 4112 switches.

Minicom Included Profiles

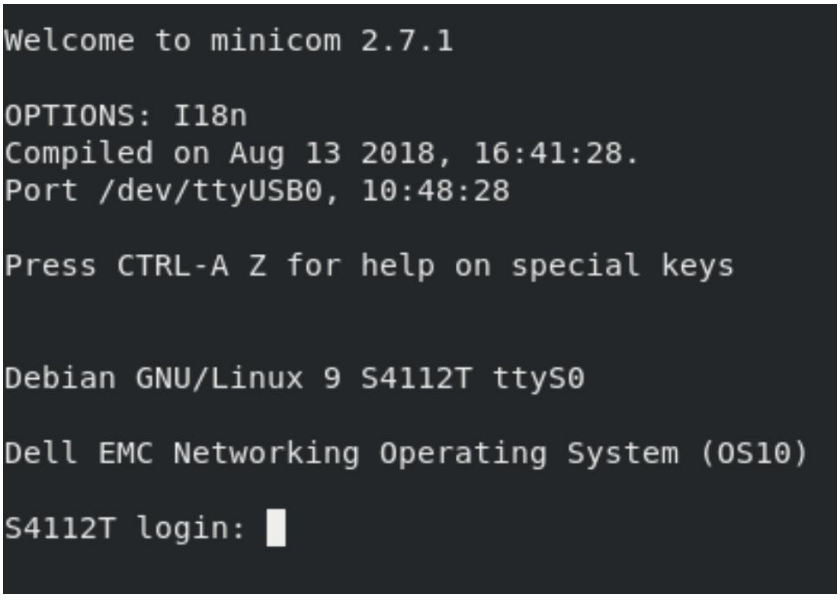
The following profiles are included for use with DDS-M equipment:

Profile Name	To Port	Baud Rate
cisco	ttyACM0	9600
dell0	ttyUSB0	115200
dell1	ttyUSB1	115200

Connecting using Minicom

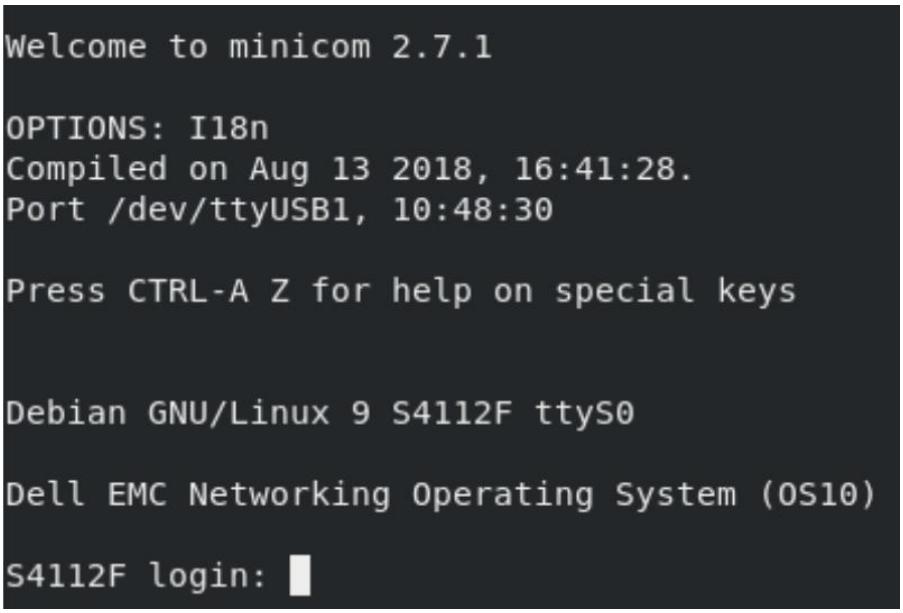
Use the minicom command followed by the profile name (**cisco, dell0**, **dell1** or a custom profile) to connect to the desired switch:

```
[defender@master ~]$ sudo minicom dell0
```



11.1.4(g) USB0 Connection Output

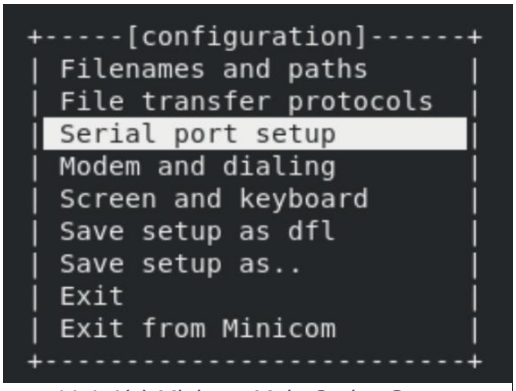
```
[defender@master ~]$ sudo minicom dell1
```



11.1.4(h) USB1 Connection Output

Minicom Setup

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

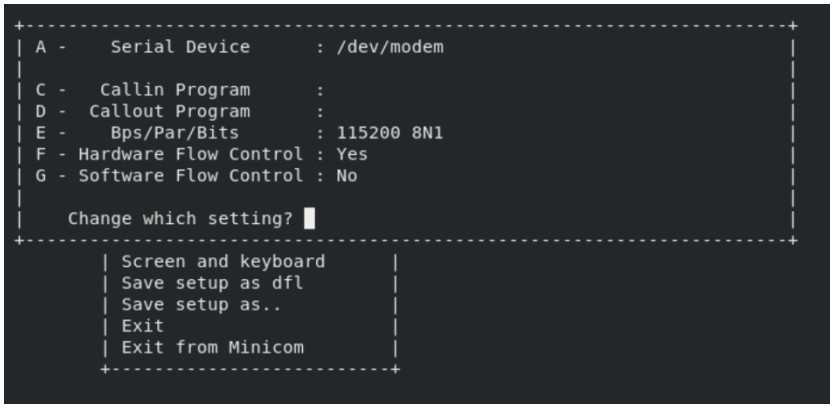


11.1.4(a) Minicom Main Option Screen

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

Scenario: Edit the Serial Device to map each USB serial interface, then set the correct baud rate and disable **Hardware Flow Control**. Create configurations and save them for both **ttyUSB0** and **ttyUSB1**.

Default configuration:



11.1.4(b) Minicom Serial Port Setup

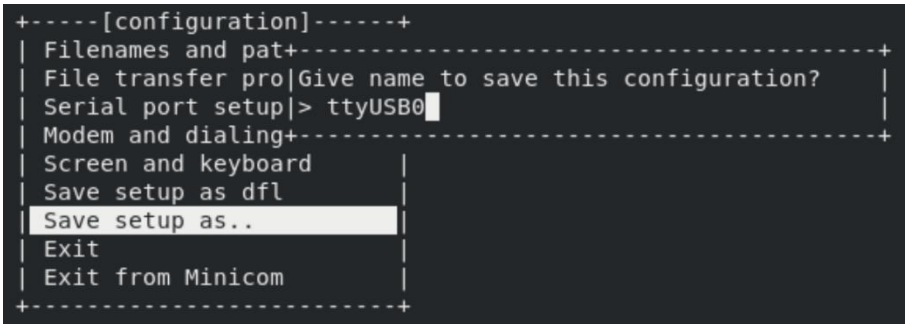
For ttyUSB0:

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

11.1.4(c) Minicom USB0 Configuration

Save the configuration to a profile.

5 Navigate to '**Save setup as..**' and press [**ENTER**].
6 name this configuration **ttyUSB0**.
7 Press [**ENTER**] to save this configuration.



11.1.4(d) Minicom Save Options

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

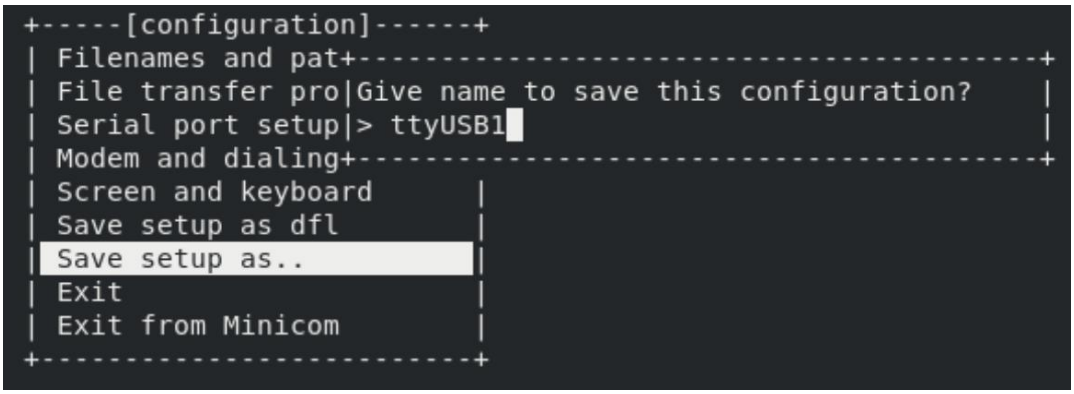
For ttyUSB1

1 Edit the Serial Device by entering [**A**] to modify the line and change the entry to **/dev/ttyUSB1**.
2 After editing the line, press [**ENTER**] to save this change.
3 Press [**F**] to set **Hardware Flow Control** to **No**
4 then press [**ENTER**] to exit the setup configuration.

11.1.4(e) Minicom USB1 Configuration

Save the configuration to a profile.

5 Navigate to '**Save setup as..**' and press [**ENTER**].
6 Name this configuration **ttyUSB1**.
7 Press [**ENTER**] to save this configuration.



11.1.4(f) Minicom Save Options

8 Navigate to '**Exit from Minicom**' and press [**ENTER**] to exit the minicom configuration.

11.1.5 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 total 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 dell0
[defender@master ~]$ sudo minicom dell1
```

✎ **Note**: "#" If the dell0 or dell1 profile does not exist, perform *Minicom Setup* in Section 11.1.4.

Using the management IP of each Dell 4112 switch:

```
[defender@master ~]$ ssh admin@10.kit#.51.251
[defender@master ~]$ ssh admin@10.kit#.51.252
```

✎ **Note**: This method can be used after assigning management IPs to switches (See User Manual Section 5.4.9).

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 cisco
```

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

The switch password is stored in "**/opt/ddt/ansible_main/passwords.yml**" file following "**switch_admin:** ". With this access level (admin), a user can view and change configuration accordingly. The baseline configuration for both switches are shown below.

4112F Switch Configuration

```
S4112F# show ip interface brief
Interface Name            IP-Address          OK       Method       Status     Protocol
================================================================================
Ethernet 1/1/1            unassigned          NO       unset        admin down  down
Ethernet 1/1/2            unassigned          NO       unset        admin down  down
Ethernet 1/1/3            unassigned          NO       unset        admin down  down
Ethernet 1/1/4            unassigned          NO       unset        admin down  down
Ethernet 1/1/5            unassigned          NO       unset        admin down  down
Ethernet 1/1/6            unassigned          NO       unset        admin down  down
Ethernet 1/1/7            unassigned          NO       unset        admin down  down
Ethernet 1/1/8            unassigned          NO       unset        admin down  down
Ethernet 1/1/9            unassigned          NO       unset        admin down  down
Ethernet 1/1/10           unassigned          NO       unset        admin down  down
Ethernet 1/1/11           unassigned          NO       unset        admin down  down
Ethernet 1/1/12           unassigned          NO       unset        admin down  down
Ethernet 1/1/13:1         unassigned          YES      unset        up          up
Ethernet 1/1/13:2         unassigned          YES      unset        up          up
Ethernet 1/1/13:3         unassigned          NO       unset        up          down
Ethernet 1/1/13:4         unassigned          YES      unset        up          up
Ethernet 1/1/14:1         unassigned          NO       unset        up          down
Ethernet 1/1/14:2         unassigned          NO       unset        up          down
Ethernet 1/1/14:3         unassigned          NO       unset        up          down
Ethernet 1/1/14:4         unassigned          NO       unset        up          down
Ethernet 1/1/15           unassigned          YES      unset        up          up
       Management 1/1/1          unassigned          YES      unset        up          up
       Vlan 1                    unassigned          NO       unset        admin down  down
       Vlan 2                    unassigned          NO       unset        up          down
       Vlan 51                   10.78.51.251/24     YES      manual       up          up
       Vlan 52                   10.78.52.1/24       YES      manual       up          up
       Vlan 53                   10.78.53.1/24       YES      manual       up          up
       Vlan 54                   unassigned          YES      unset        up          up
       Vlan 100                  unassigned          YES      unset        up          up
       Vlan 101                  unassigned          YES      unset        up          up
       Vlan 102                  unassigned          YES      unset        up          up
       Vlan 999                  unassigned          NO       unset        up          down
```

```
S4112F# show vlan
Codes: * - Default VLAN, M - Management VLAN, R - Remote Port Mirroring VLANs,
       @ - Attached to Virtual Network, P - Primary, C - Community, I - Isolated,
       S - VLAN-Stack VLAN
Q: A - Access (Untagged), T - Tagged
    NUM    Status    Description                  Q Ports
    1      Inactive
*   2      Inactive  Native_VLAN
    51     Active                                 T Eth1/1/15
                                                  A Eth1/1/13:1-1/1/13:4,1/1/14:1-1/1/14:4
    52     Active                                 T Eth1/1/13:1-1/1/13:4,1/1/14:1-1/1/14:4,1/1/15
    53     Active                                 T Eth1/1/13:1-1/1/13:4,1/1/14:1-1/1/14:4,1/1/15
    54     Active                                 T Eth1/1/13:1-1/1/13:4,1/1/14:1-1/1/14:4,1/1/15
    100    Active                                 T Eth1/1/13:1-1/1/13:4,1/1/14:1-1/1/14:4,1/1/15
    101    Active                                 T Eth1/1/13:1-1/1/13:4,1/1/14:1-1/1/14:4,1/1/15
    102    Active                                 T Eth1/1/13:1-1/1/13:4,1/1/14:1-1/1/14:4,1/1/15
    999    Inactive  Unused_VLAN
```

Something to note from this configuration.

1 *IP addresses on VLAN interfaces.* `VLAN 51-53` have IP addresses of .1 of the corresponding networks. This enables the switch to do **layer 3 routing**. Once Palo Alto virtual firewall is fully configured, these IP addresses need to be dropped (See User Manual 5.4.9)

4112T switch configuration.

```
S4112T# show ip interface brief
Interface Name            IP-Address          OK       Method       Status     Protocol
=================================================================================================
Ethernet 1/1/1            unassigned          YES      unset        up         up
Ethernet 1/1/2            unassigned          YES      unset        up         up
Ethernet 1/1/3            unassigned          NO       unset        admin down down
Ethernet 1/1/4            unassigned          NO       unset        admin down down
Ethernet 1/1/5            unassigned          NO       unset        up         down
Ethernet 1/1/6            unassigned          YES      unset        up         up
Ethernet 1/1/7            unassigned          YES      unset        up         up
Ethernet 1/1/8            unassigned          YES      unset        up         up
Ethernet 1/1/9            unassigned          NO       unset        up         down
Ethernet 1/1/10           unassigned          NO       unset        up         down
Ethernet 1/1/11           unassigned          NO       unset        up         down
Ethernet 1/1/12           unassigned          NO       unset        up         down
Ethernet 1/1/13:1         unassigned          YES      unset        up         up
Ethernet 1/1/13:2         unassigned          YES      unset        up         up
Ethernet 1/1/13:3         unassigned          NO       unset        up         down
Ethernet 1/1/13:4         unassigned          YES      unset        up         up
Ethernet 1/1/14:1         unassigned          NO       unset        up         down
Ethernet 1/1/14:2         unassigned          NO       unset        up         down
Ethernet 1/1/14:3         unassigned          NO       unset        up         down
Ethernet 1/1/14:4         unassigned          NO       unset        up         down
Ethernet 1/1/15           unassigned          YES      unset        up         up
       Management 1/1/1          unassigned          YES      unset        up         up
       Vlan 1                    unassigned          NO       unset        admin down down
       Vlan 2                    unassigned          NO       unset        up         down
       Vlan 51                   10.78.51.252/24     YES      manual       up         up
       Vlan 52                   10.78.52.252/24     YES      manual       up         up
       Vlan 53                   10.78.53.252/24     YES      manual       up         up
       Vlan 54                   unassigned          YES      unset        up         up
       Vlan 100                  unassigned          YES      unset        up         up
       Vlan 101                  unassigned          YES      unset        up         up
       Vlan 102                  unassigned          YES      unset        up         up
       Vlan 999                  unassigned          NO       unset        up         down
```

```
S4112T# show vlan
Codes: * - Default VLAN, M - Management VLAN, R - Remote Port Mirroring VLANs,
       @ - Attached to Virtual Network, P - Primary, C - Community, I - Isolated,
       S - VLAN-Stack VLAN
Q: A - Access (Untagged), T - Tagged
    NUM    Status    Description                  Q Ports
    1      Inactive
*   2      Inactive  Native_VLAN
    51     Active                                 T Eth1/1/2,1/1/15
                                                  A Eth1/1/1,1/1/13:1-1/1/13:4,1/1/14:1-1/1/14:4
    52     Active                                 T Eth1/1/2,1/1/13:1-1/1/13:4,1/1/14:1-1/1/14:4,1/1/15
    53     Active                                 T Eth1/1/1-1/1/2,1/1/13:1-1/1/13:4,1/1/14:1-1/1/14:4,1/1/15
                                                  A Eth1/1/5-1/1/12
    54     Active                                 T Eth1/1/1-1/1/2,1/1/13:1-1/1/13:4,1/1/14:1-1/1/14:4,1/1/15
    100    Active                                 T Eth1/1/2,1/1/13:1-1/1/13:4,1/1/14:1-1/1/14:4,1/1/15
    101    Active                                 T Eth1/1/2,1/1/13:1-1/1/13:4,1/1/14:1-1/1/14:4,1/1/15
    102    Active                                 T Eth1/1/2,1/1/13:1-1/1/13:4,1/1/14:1-1/1/14:4,1/1/15
    999    Inactive  Unused_VLAN
```

The baseline configuration of S4112T switch is very similar to S4112F's, but the major difference is that the access ports for **`VLAN 53`** are assigned to ethernet **`Port 5-12`**.

✎ **Note**: The Palo Alto VM provides routing functions for the kit. Re-assign gateway **`10.<kit_num>.<vlan_id>.1`** network IP addresses to VLAN Interfaces (51-53) on the **Dell S4112F** switch if the Palo Alto VM or the Hosted Engine system is taken offline for any extended duration.

Follow tasks on **User Manual 5.4.5** and **5.4.9** to change the initial switch routing configuration once the Palo Alto VM is configured and the kit is operational.

DDS-M Kit

Troubleshooting Manual

May 2023 Revision 19

Foreword

General

The Deployable Defensive System (DDS) is a modular fly-away computing cluster that is purpose-built for conducting Defensive Cyber Operations (DCO) missions. This kit provides a platform with hardware and software for the US Army and their DoD mission partners. The flagship DDS kit consists of 3 cases, 3 switches, 8 servers, a network tap, and a crash cart adapter.

✎ **Note**: The crash cart adapter turns the laptop into a portable console for accessing servers. It allows for transferring files from the laptop to the server, capturing screenshots of server configurations, error messages, and activity for faster troubleshooting. 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.

Resources

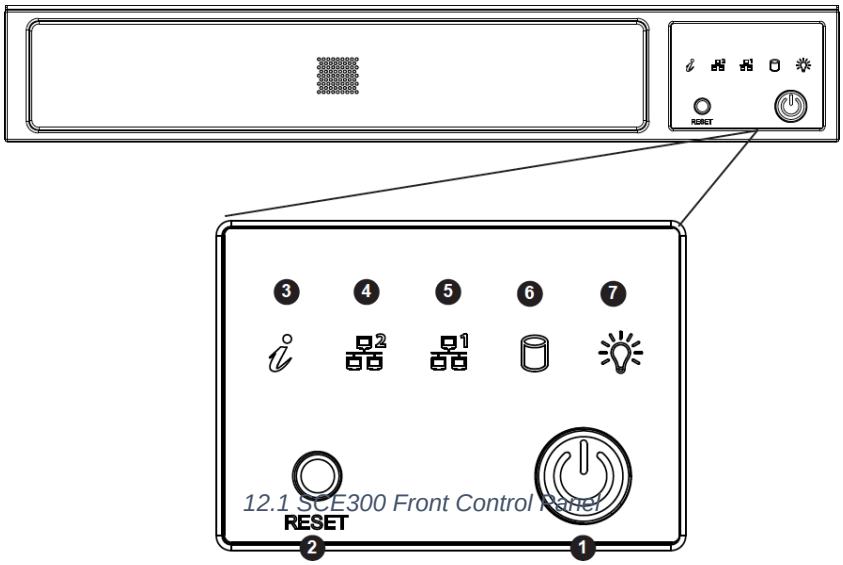
For support for installation or operation of this hardware, send an email request to the DCO helpdesk email at **dcohelpdesk@army.mil**.

12 SCE300 Chassis

Supermicro’s SCE300 is a compact embedded appliance chassis, optimized for a Flex-ATX or Mini-ITX motherboard. It supports three 2.5" fixed drives. The SCE300 chassis is ideal for variety of embedded applications.

12.1 Front Features

The front of the chassis includes the control panel.



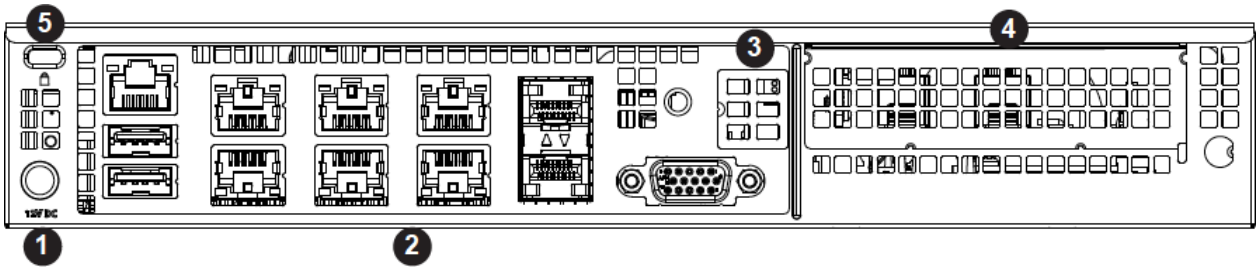
12.1 SCE300 Front Control Panel

Control Panel Features Table		
Item	**Features**	**Description**
1	Power button	The main power switch applies or removes primary power from the power supply to the server but maintains standby power. To perform most maintenance tasks, unplug the system to remove all power.
2	Reset button	Resets the system.
3	Information LED	Alerts operator to several states, as noted in the label below.
4 and 5	NIC LED	Indicates network activity on the LAN when flashing.
6	HDD LED	Indicates hard disk drive activity when flashing.
7	Power LED	Indicates power is being supplied to the system power supply units. This LED is illuminated when the system is operating normally.

Information LED Table	
Status	**Description**
Continuously on and red	An overheat condition has occurred. (This may be caused by cable congestion.)
Blinking red (1Hz)	Fan failure, check for an inoperative fan.
Blinking red (0.25Hz)	Power failure, check for a non-operational power supply.
Solid blue	Local UID has been activated. Use this function to locate the server in a rack mount environment.
Blinking blue	Remote UID is on. Use this function to identify the server from a remote location.

12.2 Rear Features

The chassis rear holds input/output ports.



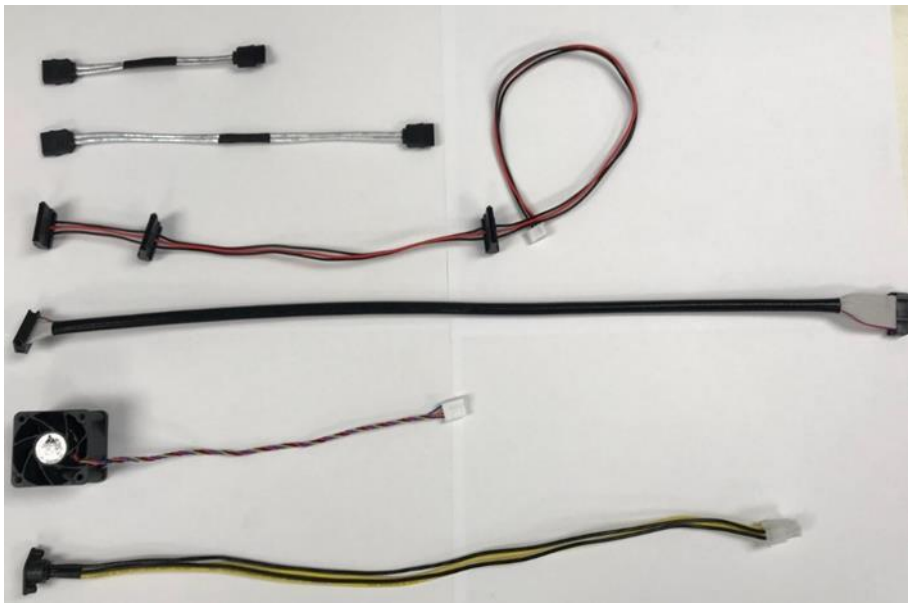
12.2 SCE300 / SN-3000 Rear View

Rear Chassis Features		
Item	**Features**	**Description**
1	Power Input	The main power switch applies or removes primary power from the power supply to the server but maintains standby power. To perform most maintenance tasks, unplug the system to remove all power.
2	I/O ports	IPMI LAN, USB, LAN, SFP LAN, VGA
3	RJ45 window	Opening for an optional serial connector using an RJ45 jack
4	PCI window	Standard low-profile
5	K-slot for lock	Accepts a standard Kensington cable locking device (not included).

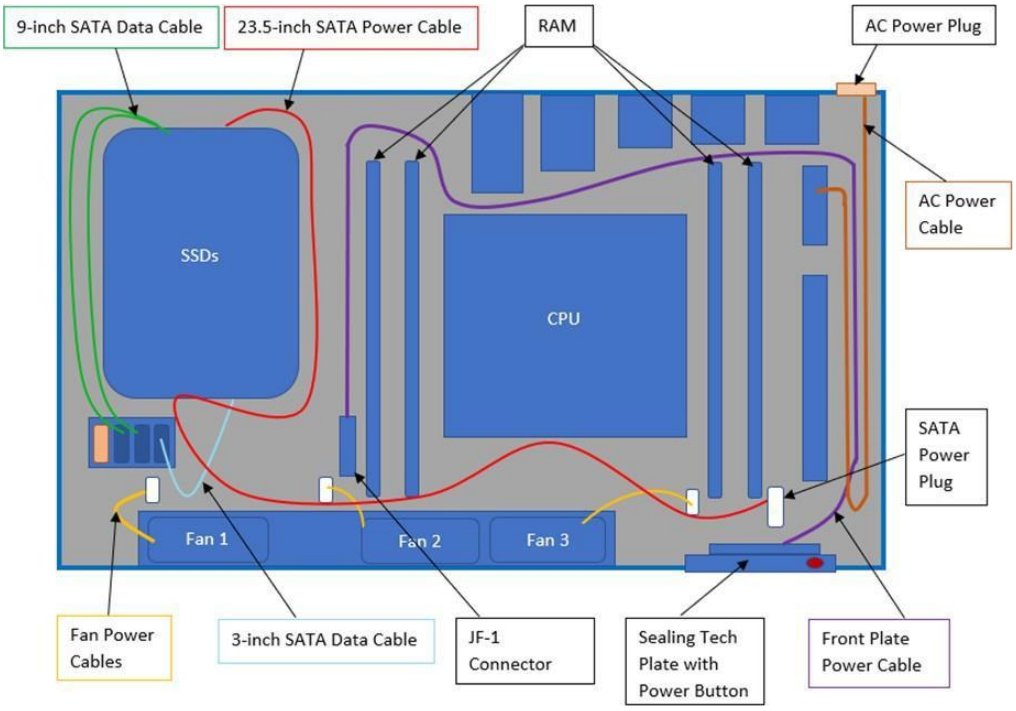
12.3 Maintenance and Component Installation of the SCE300 Chassis

This chapter provides instructions on installing and replacing main system components. To prevent compatibility issues, only use components that match the specifications and/or part numbers given.
Installation or replacement of most components require that power first be removed from the system. Please follow the procedures given in each section.

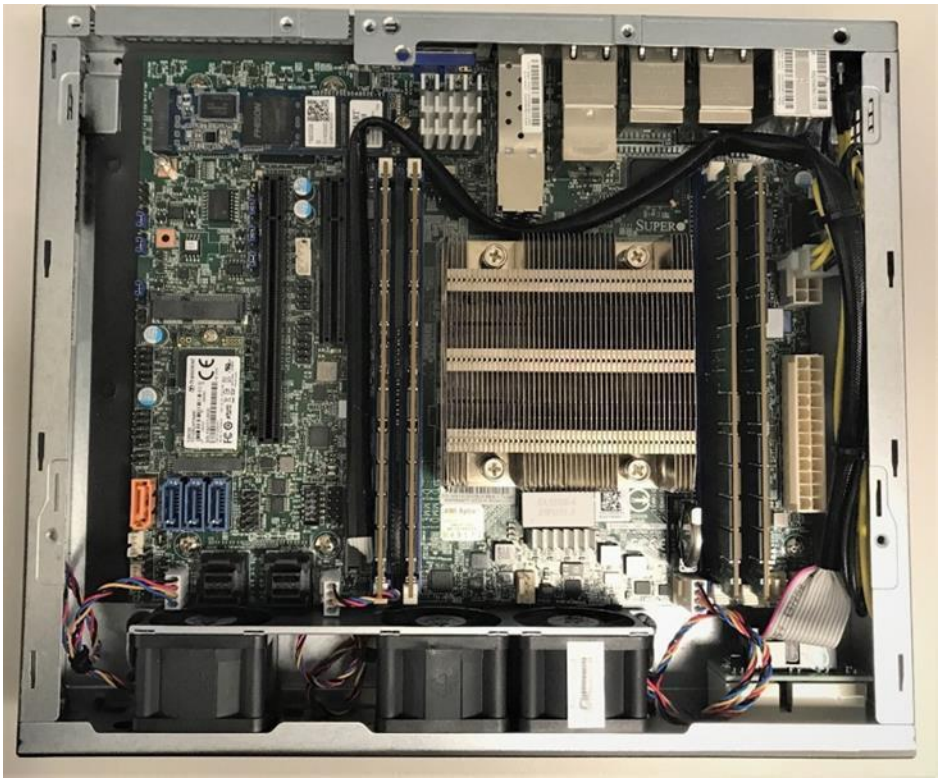
DDS-M Component Diagram		
Item	**Features**	**Description**
1	3-inch SATA Data Cable	Short cable to provide SSD with data connection
2	9-inch SATA Data Cable	Short cable to provide SSD with data connection
3	23.5-inch SATA Power Cable	Short cable to provide SSD with power connection
4	Front Plate Power Cable	Connects power button on front plate with motherboard
5	Node Fan	Cools DDS-M Nodes
6	AC Power Cable	Connects power supply with motherboard



12.3(a) DDS-M Internal Cables



12.3(b) DDS-M Internal Cable Suggested Paths



12.3(c) DDS-M Internal Physical View

12.3.1 Removing Power

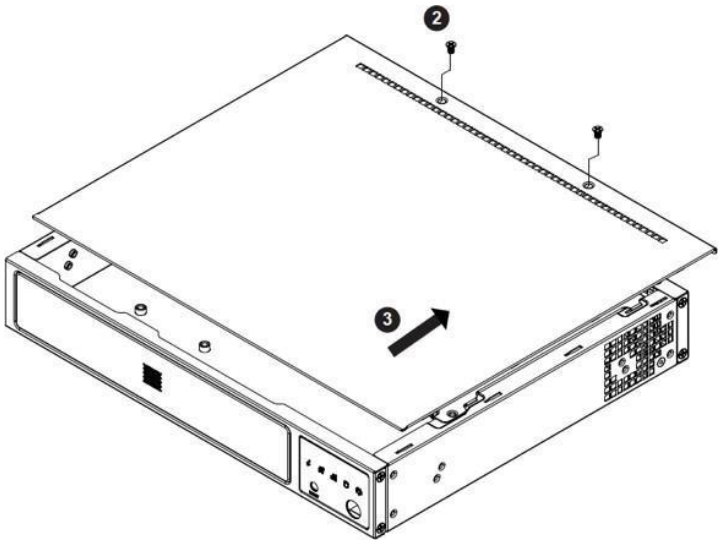
Use the following procedure to ensure that power has been removed from the system. This step is necessary when removing or installing non hot-swappable components.

12.3.2 Powering Down

1 Use the operating system to power down the system.
2 After the system has completely shut down, disconnect the AC power cord from the power source.
3 Disconnect the power cord from the chassis.

12.3.3 Accessing the System

The SCE300 features a removable top cover to access to the inside of the chassis.



12.3.3 SCE300 Top Cover

12.3.4 Removing the Top Cover

1 Power down the system as described in section 2.2.
2 Remove the two screws that hold the cover in place.
3 Slide the cover sideways as illustrated above to release the front and rear cover hooks from the chassis.
4 Lift the cover up and off the chassis.

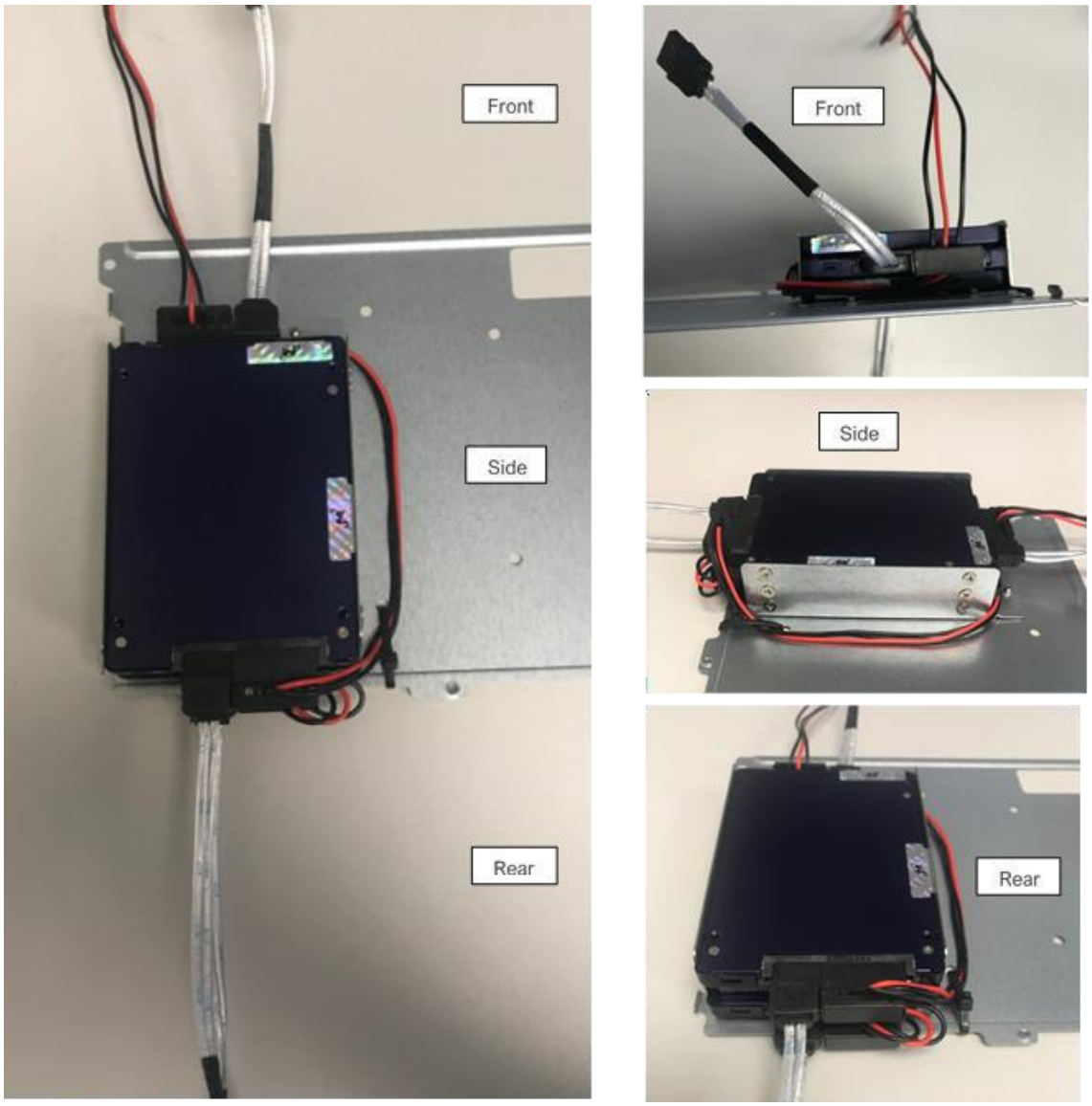
⚠ **Caution**: Except for short periods of time, do not operate the server without the cover in place. The chassis cover must be in place to allow proper airflow and prevent overheating.

12.3.5 Installing a Storage Drive

The SCE300 can accommodate up to three fixed 2.5" storage drives of 9.5 mm thickness. They are installed to a mounting tray inside the chassis. The layout of the SSD drives in a node is as follows. Two drives face the rear of the chassis (with the SFP connector, Ethernet, USB ports and AC Power Plug) and one SSD drive faces the front (with the vendor logo and power button).

✎ **Note**: With some drive configurations, a PCI-E expansion card cannot be installed.

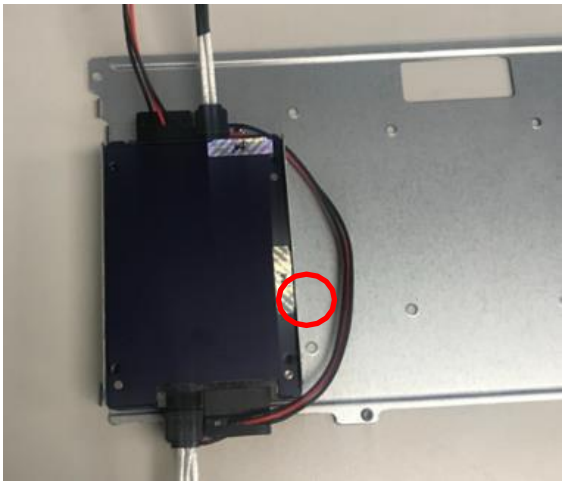
✎ **Note**: With the side view the cables are run on the side with a cable tie not under the SSD brackets.



12.3.5(a) SSD Installation

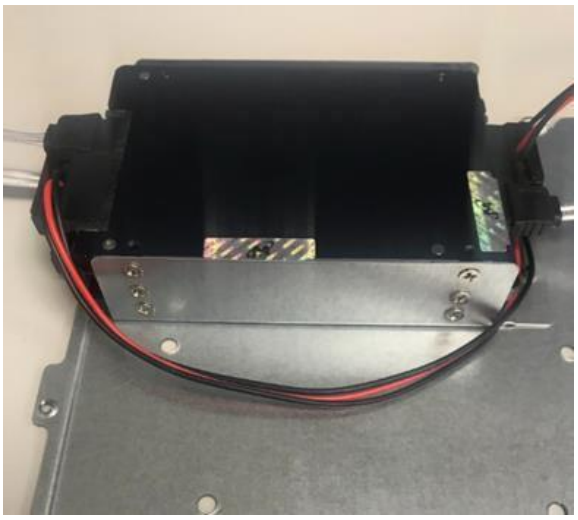
The motherboard should be installed before installing the drive. The position of the drive may be affected by the size of the motherboard.

1 Make sure there is no power to the system and remove the chassis cover.
2 Remove the screws securing the drive tray to the chassis and lift the tray out.
3 Orient the drives as shown above.
4 Locate the SSD Chassis Bracket.
5 Identify the hole in the SSD Chassis Bracket adjacent to the bracket circled in Red below. This hole will be used as the pass through for the zip tie that will secure the 23.5- inch SATA Power Cable.



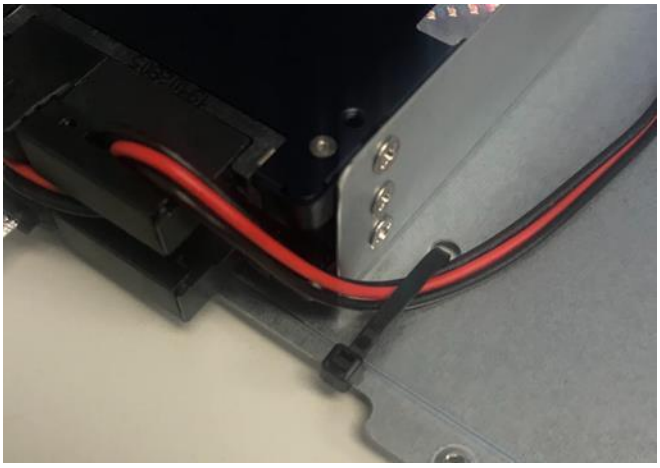
12.3.5(b) Securing the SSD Power Cable

6 Push the 23.5-inch SATA Power Cable flat against the SSD Chassis.



12.3.5(c) SSD Power Cable Routing

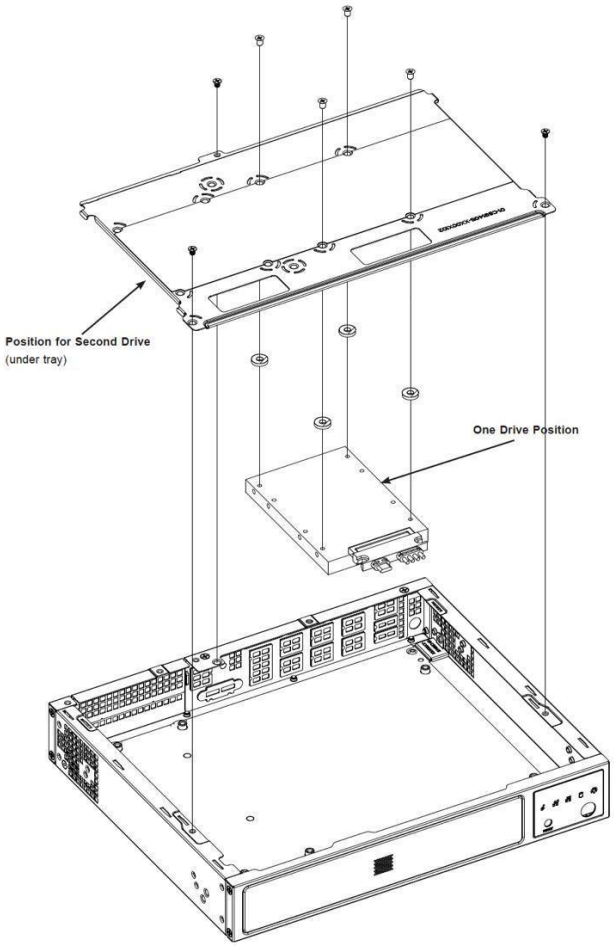
7 Locate a Zip tie, pass it through the hole and around the chassis. Carefully shorten the zip tie.



12.3.5(d) SSD Power Cable Zip Tie

8 Cut off the excess.
9 Return the drive tray assembly into the chassis, aligning the tabs of the tray with the slots in the chassis. Secure the tray to the chassis with the screws previously set aside.
10 Attach the cable SATA connector and to the motherboard connector. This cable carries both the SATA signal and the SATA power.

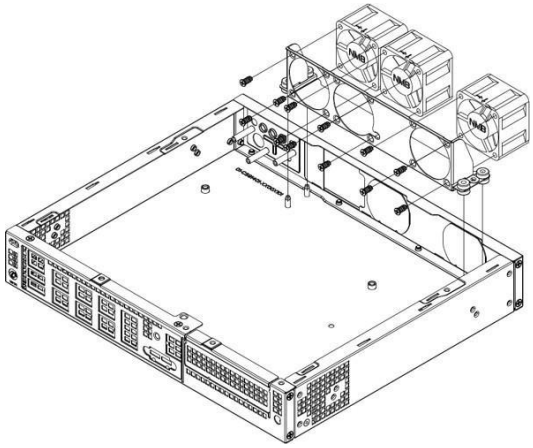
11 Reinstall the chassis cover and power up the system.



12.3.5(e) Inserting the Chassis Cover

12.3.6 Installing a System Fan

1 Power down the system as described in section 2.1 and remove the AC power cord and the chassis cover.
2 Align the fan with the holes in the wall of the chassis and secure it with screws.
3 Connect the fan cable to motherboard.
4 Reinstall the chassis top cover, reconnect the AC power cord and power up the system.

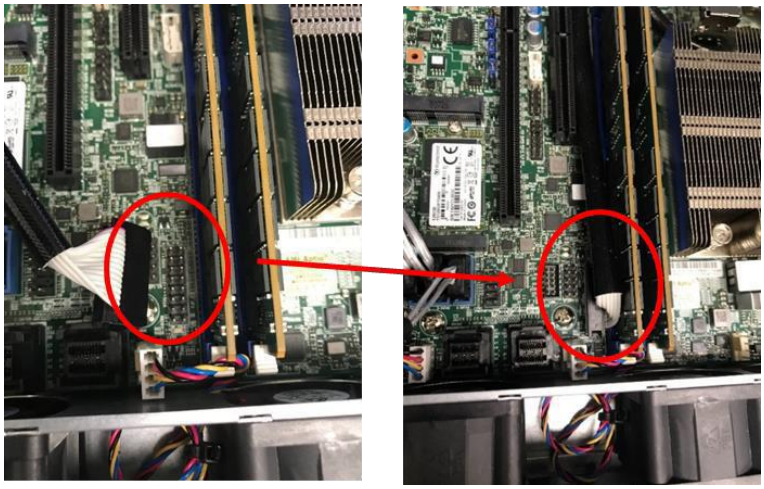


12.3.6 System Fan Installation

12.3.7 Cabling the Front Plate Power Plug

The Front Plate Power cable must be oriented as shown in these instructions or the Power Button on the front of the node will not function.

1 Locate the Front Plate Power Plug Cable as depicted in the DDS-M Component Diagram (Feb 2020).
2 Identify the JF-1 Connector Located between the SSDs and the CPU adjacent to Fan 2 depicted in the Node Cable Diagram.
3 Insert the 16-pin connector of the ribbon cable into the JF-1 connector on the motherboard next to the RAM DIMMs, ensure that no pins are bent in the process.



12.3.7 Front Plate Power Cable Installation

12.3.8 Closing the Node

✎**Note**: When closing the node ensure that the red and black SATA Power Cables are not under the SSD brackets.

1 Orient the drives as Appendix II depicts before starting.
2 Line up the SSD Chassis Bracket with the node as shown.

12.3.8(a) SSD Chassis Bracket

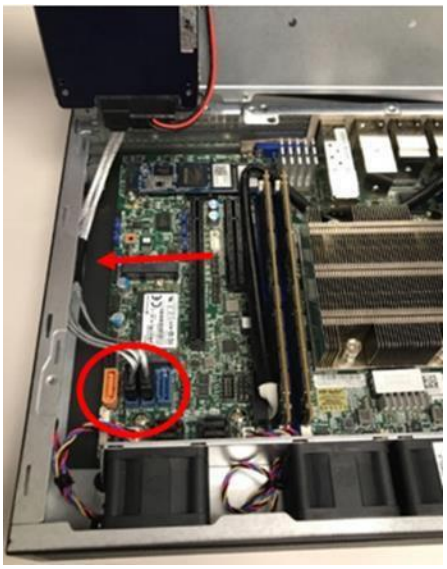
3 Locate Two 9-inch SATA Data Cables and plug those into the two left SATA sockets.

12.3.8(b) SATA Sockets

4 Plug in the two 9-inch SATA Data Cables in the two left SATA data sockets.

12.3.8(c) SATA Data Cable Installation

5 Push the two 9-inch SATA Data Cables to the left side of the node ensuring that the cables are free of the motherboard.



12.3.8(d) SATA Cable Orientation

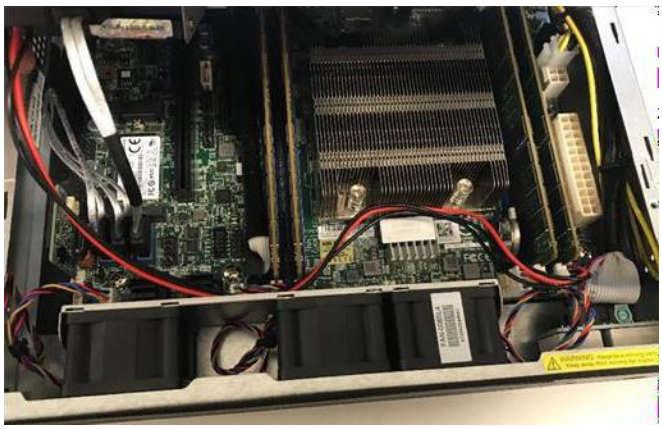
6 Locate the right SATA Data Socket.

12.3.8(e) SATA Sockets

7 Take the 3-inch SATA Data Cable and plug it into the right most Data Socket.

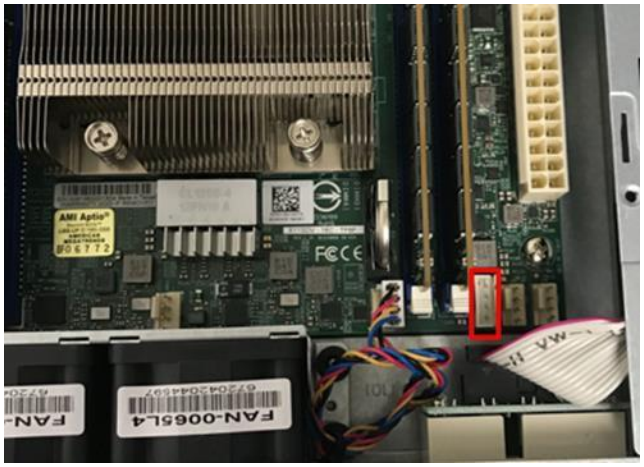
12.3.8(f) SATA Cable Installation

8 Locate the 23.5-inch SATA Power Cable and route it as shown.



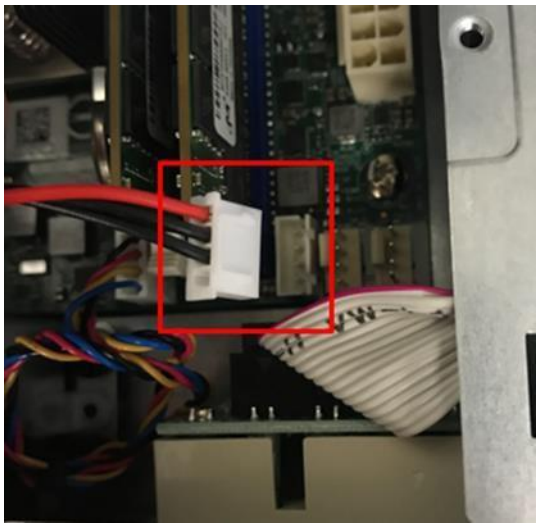
12.3.8(g) SATA Power Cable Orientation

9 Locate the SATA Power Plug.



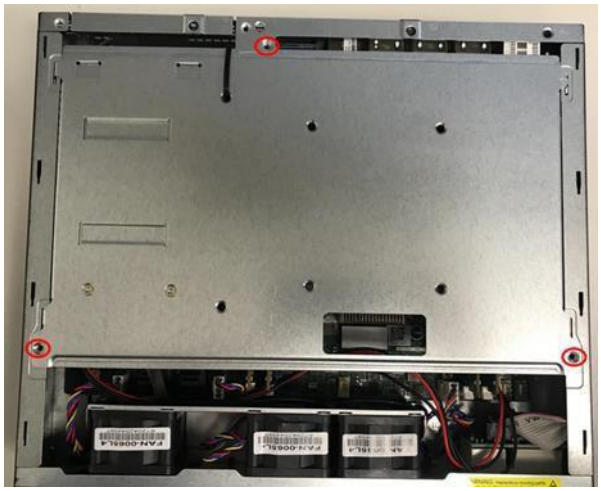
12.3.8(h) SATA Power Plug Location

10 Plug the 4-pin end of the 23.5-inch SATA Power Cable into the SATA Power Plug.



12.3.8(i) SATA Power Plug Orientation

11 Gently compress the SSD Chassis Bracket closed. Ensuring that no cables are caught.
12 Locate the SSD Chassis Bracket screws and secure into the 3 screw holes marked in Red.



12.3.8(j) SSD Chassis Bracket Installation

13 Locate the Black Node Cover and place it on the chassis gently squeezing the node and sliding the lid close.
14 Screw in the last two screws black screws in the outside of the chassis.

12.3.8(k) Chassis Top Panel Installation

12.3.9 Rear Screw Replacement

Some of the earlier DDS-M nodes originally shipped with round screws to secure the power supply to the chassis. These are to be replace with flat screws.

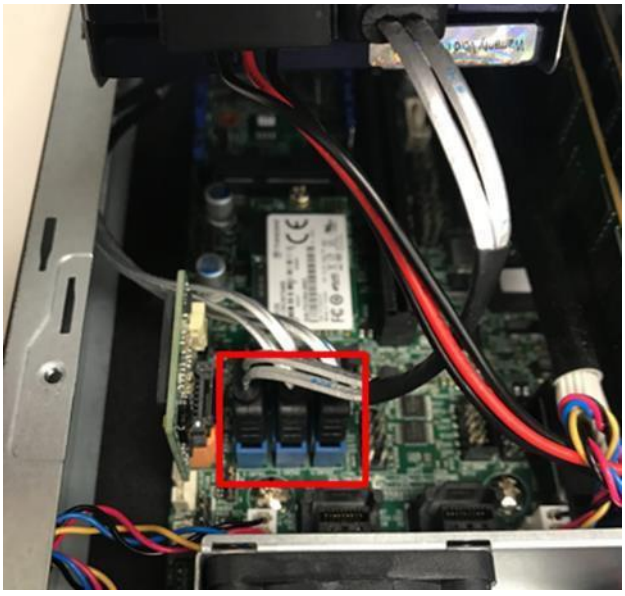
1 Locate two Flat Head screws.
2 Unscrew one of the Round Head power screws and replace it with one Flat Head one.
3 Unscrew the second Round Head power screw and replace with a Flat Head one.

12.3.9 Rear Screw Identification

12.3.10 SATADOM Removal

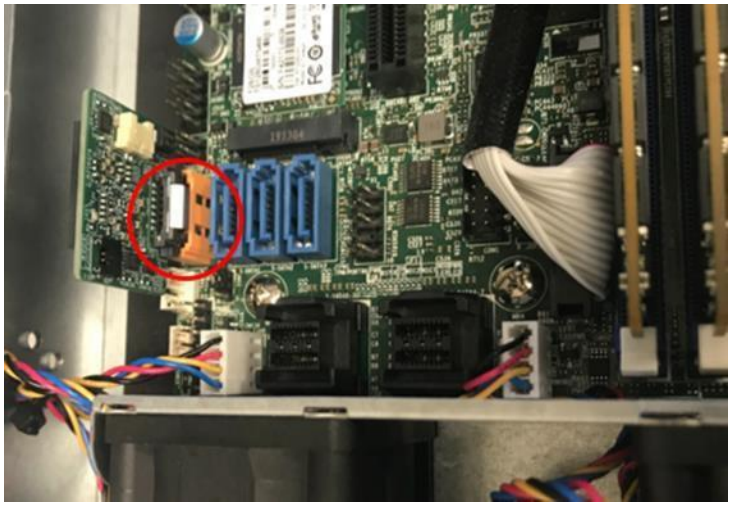
Some of the earlier DDS-M nodes originally shipped with a small 128GB SATA DOM SSD. This caused compatibility issues and needs to be removed in all DDS-M Nodes.

1 Open the node and disconnect all three SATA SSD Data Cables.



12.3.10(a) SATA SSD Data Cable Removal

2 Locate the SATA DOM and push on the metal clip to release it.

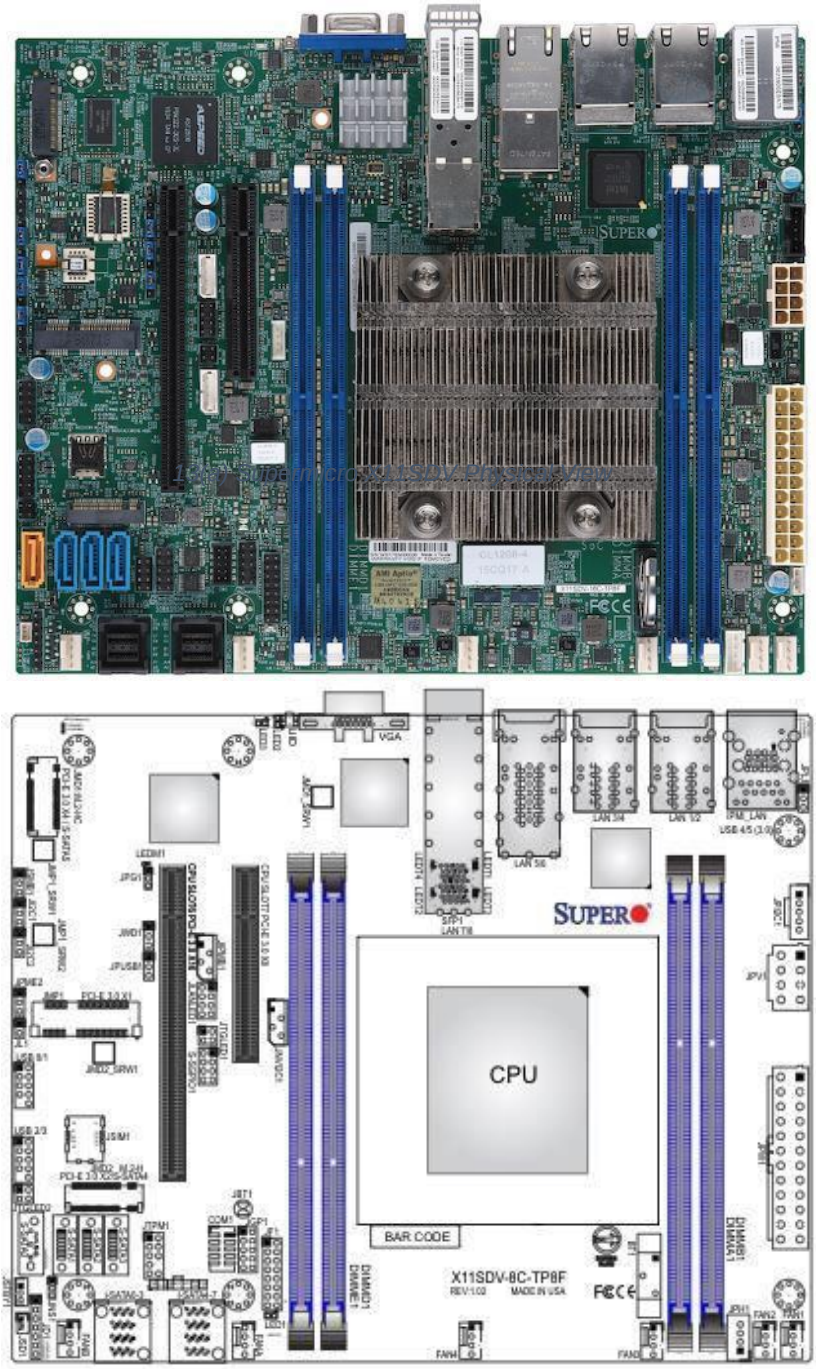


12.3.10(b) SATADOM Removal

3 Upon removal of the SATA DOM, follow section 2.8 to close the node properly.

13 Supermicro X11SDV-16C-TP8F Motherboard

The Supermicro X11SDV-16C-TP8F motherboard supports an Intel® Xeon® D-2100 SoC processor. This a high performance, low powered Flex ATX motherboard that is ideal for embedded networking and storage systems. The latest features for this motherboard include support for eight LAN ports with dual 10GbE SFP+ and dual 10Gbase-T ports, M.2 M-Key/B-Key connections, and an NVMe connection.



13(b) Supermicro X11SDV Component View

13.1 Special Features

This section describes the health monitoring features of the X11SDV-16C/-12C/-8C/-4C-TP8F motherboard. The motherboard has an onboard System Hardware Monitor chip that supports system health monitoring.

13.2 Recovery from AC Power Loss

The Basic I/O System (BIOS) provides a setting that determines how the system will respond when AC power is lost and then restored to the system. Choose for the system to remain powered off (operators must press the power switch to turn it back on), or for it to automatically return to the power-on state. See the Advanced BIOS Setup section for this setting. The default setting is Last State.

13.3 System Health Monitoring

The motherboard has an onboard Baseboard Management Controller (BMC) chip that supports system health monitoring.

13.3.1 Onboard Voltage Monitors

The onboard voltage monitor will continuously scan crucial voltage levels. Once a voltage becomes unstable, it will give a warning or send an error message to the screen. Users can adjust the voltage thresholds to define the sensitivity of the voltage monitor. Real time readings of these voltage levels are all displayed in the BIOS.

13.3.2 Fan Status Monitor with Firmware Control

The system health monitor chip can check the RPM status of a cooling fan. The CPU and chassis fans are controlled by BIOS Thermal Management through the back panel. Refer to the below table for available fan modes to choose the most appropriate one for nominal operation.

Fan Speed Modes	
Fan Mode	**Description**
Full Speed	Use this mode to set fan speed at full speed for maximum system cooling
Standard	Use this mode to set fan speed for normal system cooling
Heavy I/O	Use this mode to set fan speed for higher PCI-E add-on card area cooling
Optimal	Use this mode to set fan speed for normal PCI-E add-on card area cooling
PUE2	Use this mode to set fan speed for best power efficiency and maximum noise reduction

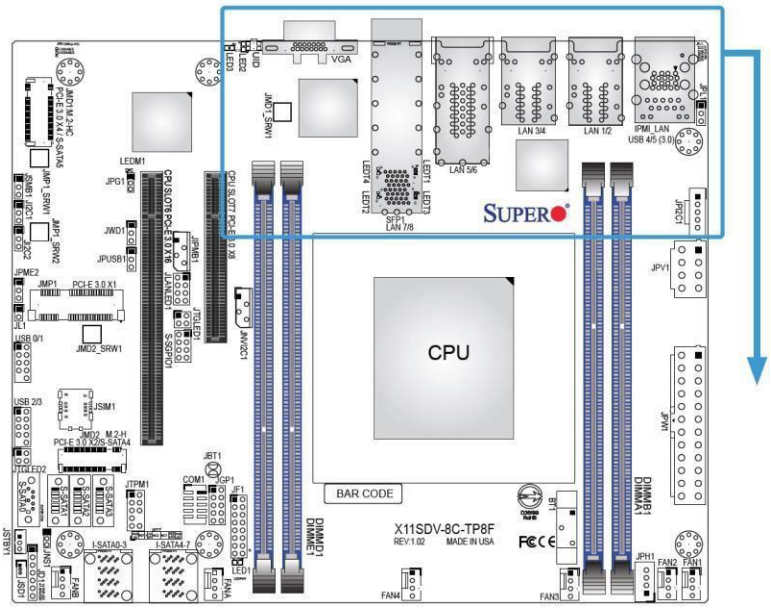
13.3.3 Environmental Temperature Control

System Health sensors monitor temperatures and voltage settings of onboard processors and the system in real time via the IPMI interface. Whenever the temperature of the CPU or the system exceeds a user-defined threshold, system/CPU cooling fans will be turned on to prevent the CPU or the system from overheating

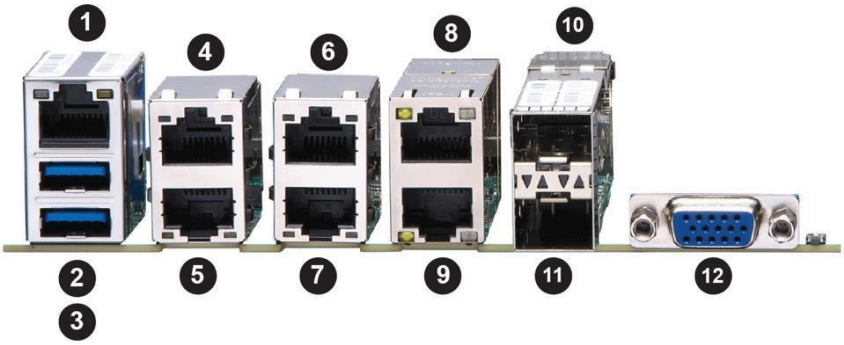
✎ **Note**: To avoid possible system overheating, please provide adequate airflow to each device.

13.4 Rear I/O Ports

See below for the locations and descriptions of the various I/O ports on the rear of the motherboard.



13.4(a) Motherboard I/O Port Top View



#	Description	#	Description	#	Description
1	IPMI LAN	5	LAN1	9	LAN5
2	USB5	6	LAN4	10	SFP LAN8
3	USB4	7	LAN3	11	SFP LAN7
4	LAN2	8	LAN6	12	VGA

13.5 Universal Serial Bus (USB) Ports

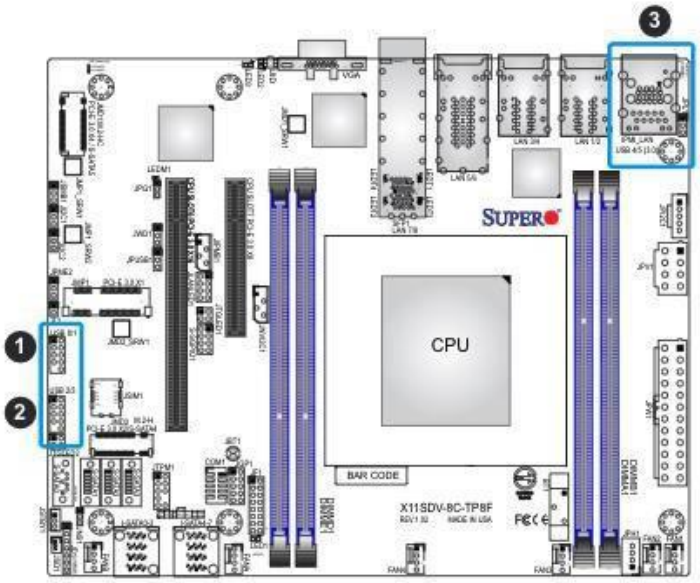
There are two USB 3.0 ports (USB4/5) on the I/O back panel. The motherboard also has two front access USB 2.0 headers (USB0/1, USB2/3). The onboard headers can be used to provide front side USB access with a cable (not included).

Back Panel USB 4/5 (3.0) Pin Definitions

Pin#	Definition	Pin#	Definition
A1	VBUS	B1	Power
A2	D-	B2	USB_N
A3	D+	B3	USB_P
A4	GND	B4	GND
A5	Stda_SSRX-	B5	USB3_RN
A6	Stda_SSRX+	B6	USB3_RP
A7	GND	B7	GND
A8	Stda_SSTX-	B8	USB3_TN
A9	Stda_SSTX+	B9	USB3_TP

Front Panel USB 0/1, 2/3 (2.0) Pin Definitions

Pin#	Definition	Pin#	Definition
1	+5V	2	+5V
3	USB_N	4	USB_N
5	USB_P	6	USB_P
7	Ground	8	Ground
9	Key	10	NC



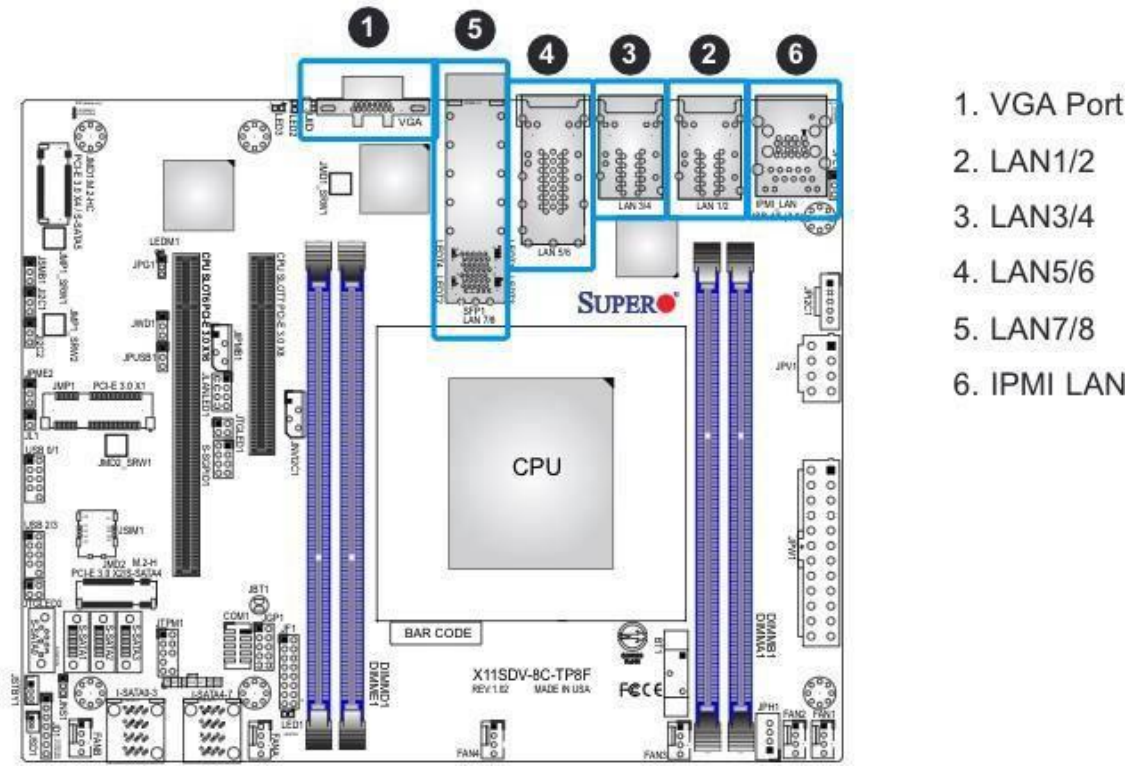
1. USB0/1
2. USB2/3
3. USB4/5

13.5 Motherboard USB Ports

13.6 LAN Ports

There are eight LAN ports located on the I/O back panel of the motherboard. LAN1 - LAN4 are RJ45 1GbE Ethernet ports, LAN5 - LAN6 are 10GbE ports, and LAN7 - LAN8 are 10G SFP+ ports. The motherboard also offers one IPMI LAN port.

LAN Port Pin Definitions			
Pin#	**Definition**	**Pin#**	**Definition**
1	TX_D1+	5	BI_D3-
2	TX_D1-	6	RX_D2-
3	RX_D2+	7	BI_D4+
4	BI_D3+	8	BI_D4-



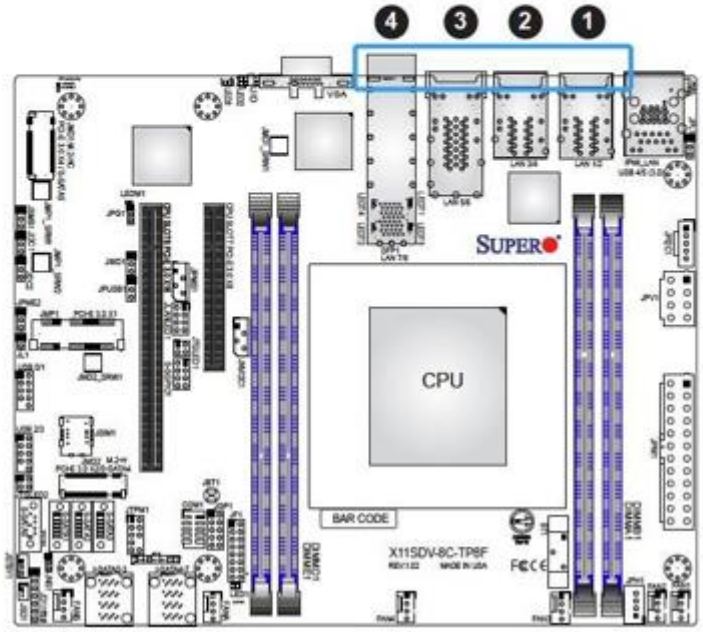
13.6 Motherboard LAN Ports

13.7 LAN LEDs

Eight LAN ports (LAN1 - LAN8) are located on the I/O back panel. Each Ethernet LAN port has two LEDs. The green LED indicates activity, while the other Link LED may be green, amber, or off to indicate the speed of the connection. Refer to the tables below for more information.

LAN Link LEDs (Left) LED State	
LED Color	**Definition**
Off	No Connection/10 Mbps/100 Mbps
Amber	1 Gbps
Green	10 Gbps

LAN Activity LEDs (Right) LED State		
Color	**Status**	**Definition**
Green	Flashing	Active



1. LAN1/2 LEDs
2. LAN3/4 LEDs
3. LAN5/6 LEDs
4. LAN7/8 LEDs

13.7 Motherboard LAN LEDs

13.7.1 Power LED Indicator

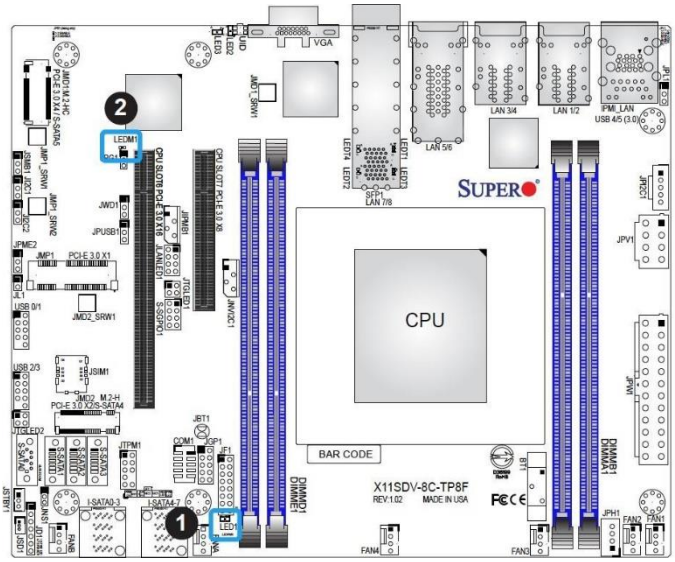
LED1 is an Onboard Power LED. When this LED is lit, it means power is present on the motherboard. In suspend mode, this LED will blink on and off. Be sure to turn off the system and unplug the power cord(s) before removing or installing components.

Onboard Power LED Indicator	
LED Color	**Definition**
Off	**System Off (power cable not connected)**
Green	**System On**

13.7.2 BMC Heartbeat LED

LEDM1 is the BMC heartbeat LED. When the LED is blinking green, BMC is working. Refer to the table below for the LED status.

Onboard Power LED Indicator	
LED Color	**Definition**
Blinking Green	BMC Normal



1. Onboard PWR LED
2. BMC Heartbeat LED

13.7.2 Onboard Power LEDs

13.7.3 Overheat/PWR Fail/Fan Fail LED

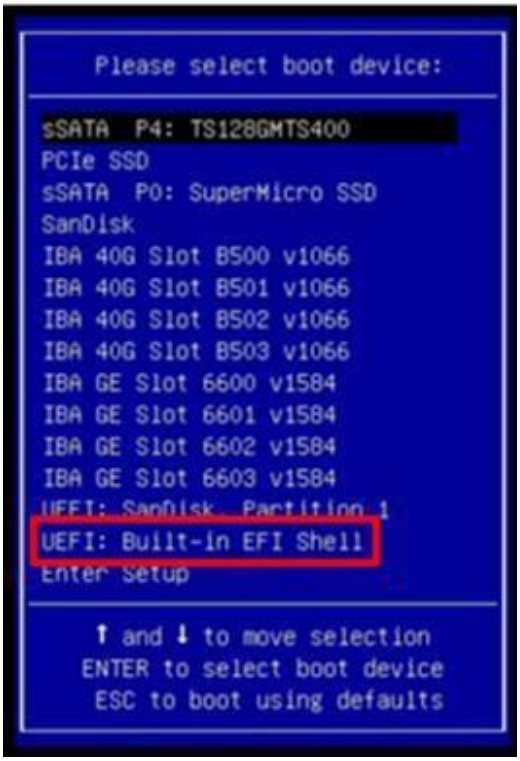
LED3 is the Overheat/Power Fail/Fan Fail LED.

13.8 DDS-M X722 NIC Firmware Flash Update

The latest NIC update will allow for the latest version of Data Plane Development Kit (DPDK) that some third-party software may require to operate. Please note that this firmware update is not required for overall system functionality and failure to update will not result in a compromised system.

✎ **Note**: This procedure should only be done by Armory personnel.

1. Go to the Sealing Tech Downloads site.
2. Download the X11SDV2C_NUP folder which contains the required Firmware flash Update files.
3. Copy files from X11SDV2C_NUP folder to a USB drive.
4. Insert USB drive into server node.
5. Start the node. When the POST splash screen displays press F11 to load the boot menu. Select the option for Built-in EFI Shell



13.8(a) Boot Screen UEFI Selection

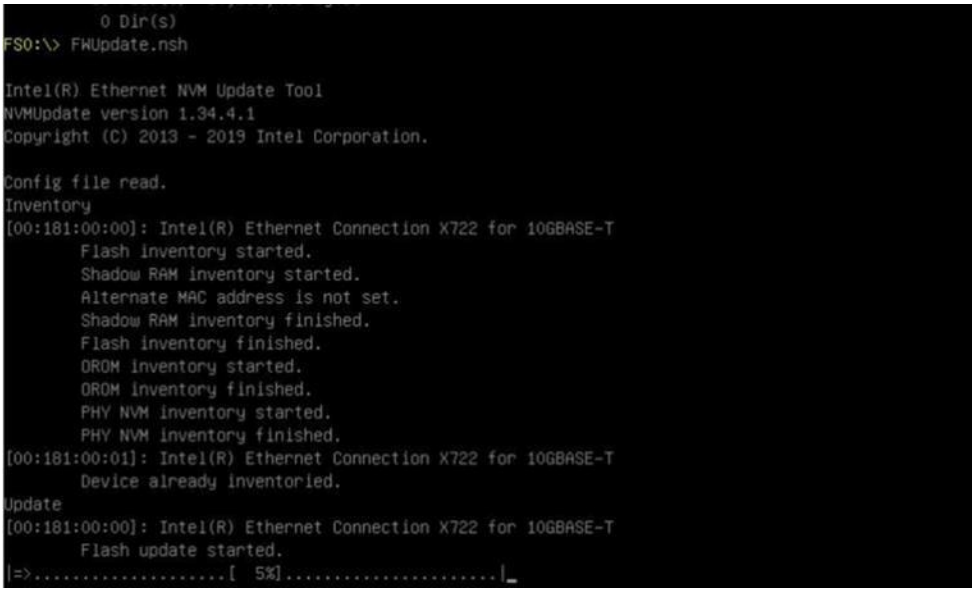
6 Once the system loads to the EFI shell, switch over to the USB drive with the command and verify the contents of the USB with the following commands:

```
Shell>fs0:
FS0:\>ls
```

13.8(b) NIC Firmware Flash Commands

7 Start the NIC firmware flash with the following command

```
FS0:\>FWUpdate.nsh
```



13.8(c) NIC Firmware Flash Commands

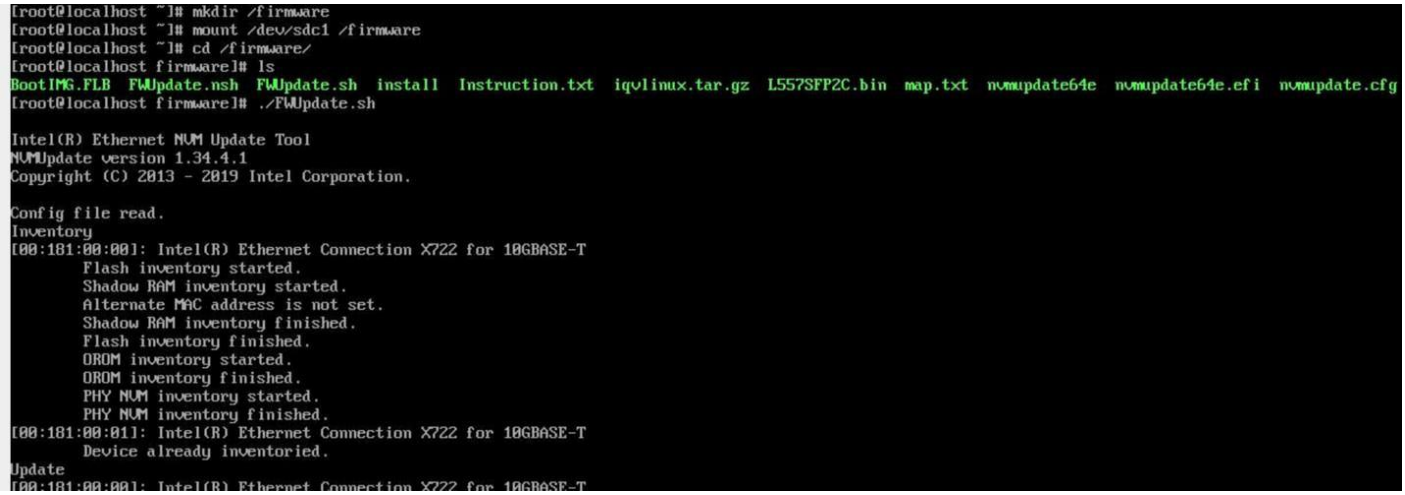
8 Once the firmware update is complete, restart the server with the command reset

9 Boot into a Unix environment and make a directory to mount the USB drive.
10 Find the USB drive device reference by using **fdisk -l** or **lsblk** commands, then mount the USB drive partition to that directory using mount:

```
[root@localhost~]# mount /dev/sdXX /firmware
```

11 Run the script to update the firmware:

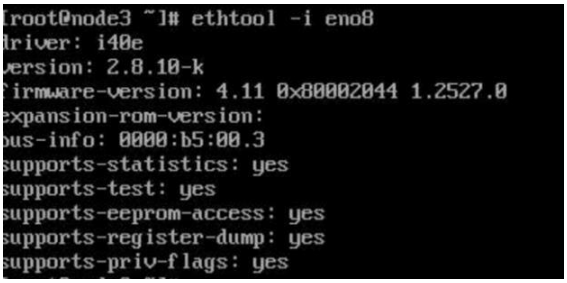
```
[root@localhost~]# ./FWUpdate.sh
```



13.8(d) NIC Firmware Flash Commands

12 This firmware update can be verified with **ethtool -i eno6** which should report a firmware minimum version of 4.11:

13.8(e) ethtool output (Before)



13.8(f) ethtool output (After)

14 Replacing a Motherboard

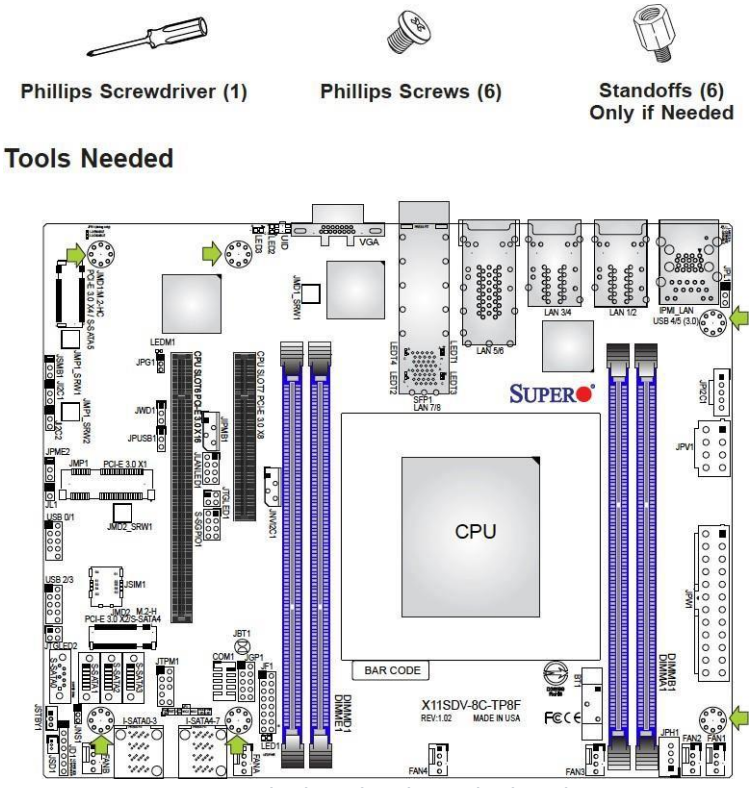
Electrostatic Discharge (ESD) can damage electronic components. The following measures are generally sufficient to protect sensitive equipment from ESD.

Precautions

- Use a grounded wrist strap designed to prevent static discharge.
- Touch a grounded metal object before removing the board from the antistatic bag.
- Handle the board by its edges only; do not touch its components, peripheral chips, memory modules or gold contacts.
- When handling chips or modules, avoid touching their pins.
- Put the motherboard and peripherals back into their antistatic bags when not in use.
- For grounding purposes, make sure the computer chassis provides excellent conductivity between the power supply, the case, the mounting fasteners and the motherboard.
- Use only the correct type of onboard CMOS battery. Do not install the onboard battery upside down to avoid possible explosion.

14.1 Motherboard Installation

All motherboards have standard mounting holes to fit different types of chassis. Make sure that the locations of all the mounting holes for both the motherboard and the chassis match. Although a chassis may have both plastic and metal mounting fasteners, metal ones are highly recommended because they ground the motherboard to the chassis. Make sure that the metal standoffs click in or are screwed in tightly.



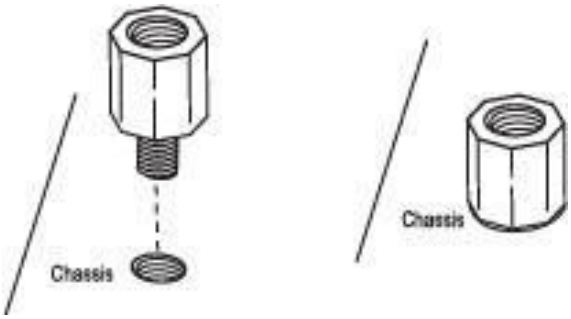
14.1 Motherboard and Required Tools

14.1.1 Location of Mounting Holes

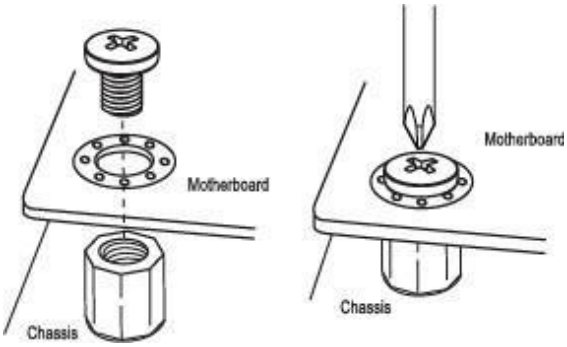
1 To avoid damaging the motherboard and its components, please do not use a force greater than 8 lb./inch on each mounting screw during motherboard installation.
2 Some components are very close to the mounting holes. Please take precautionary measures to avoid damaging these components when installing the motherboard to the chassis.

14.1.2 Installing the Motherboard

1 Locate the mounting holes on the motherboard. See the previous page for the location.
2 Locate the matching mounting holes on the chassis. Align the mounting holes on the motherboard against the mounting holes on the chassis.



14.1.2(a) Standoff Installation



14.1.2(b) Retaining Screw Installation

3 Install standoffs in the chassis as needed.
4 Install the motherboard into the chassis carefully to avoid damaging other motherboard components.
5 Using the Phillips screwdriver, insert a Phillips head #6 screw into a mounting hole on the motherboard and its matching mounting hole on the chassis.
6 Repeat Step 5 to insert #6 screws into all mounting holes.
7 Make sure that the motherboard is securely placed in the chassis.

✎ **Note**: Images displayed are for illustration only. Some chassis or components may look different from those represented in this manual.

15 Memory Support and Installation

The X11SDV-16C-TP8F motherboard supports up to 256GB of ECC RDIMM or 512GB of ECC LRDIMM DDR4 memory with speeds of up to 2400MHz in four memory slots. Populating these DIMM slots with memory modules of the same type and size will result in interleaved memory, which will improve memory performance.

⚠ **Important:** Exercise extreme care when installing or removing DIMM modules to prevent any possible damage.

15.1 DIMM Module Population Configuration

For optimal memory performance, follow the table below when populating memory.

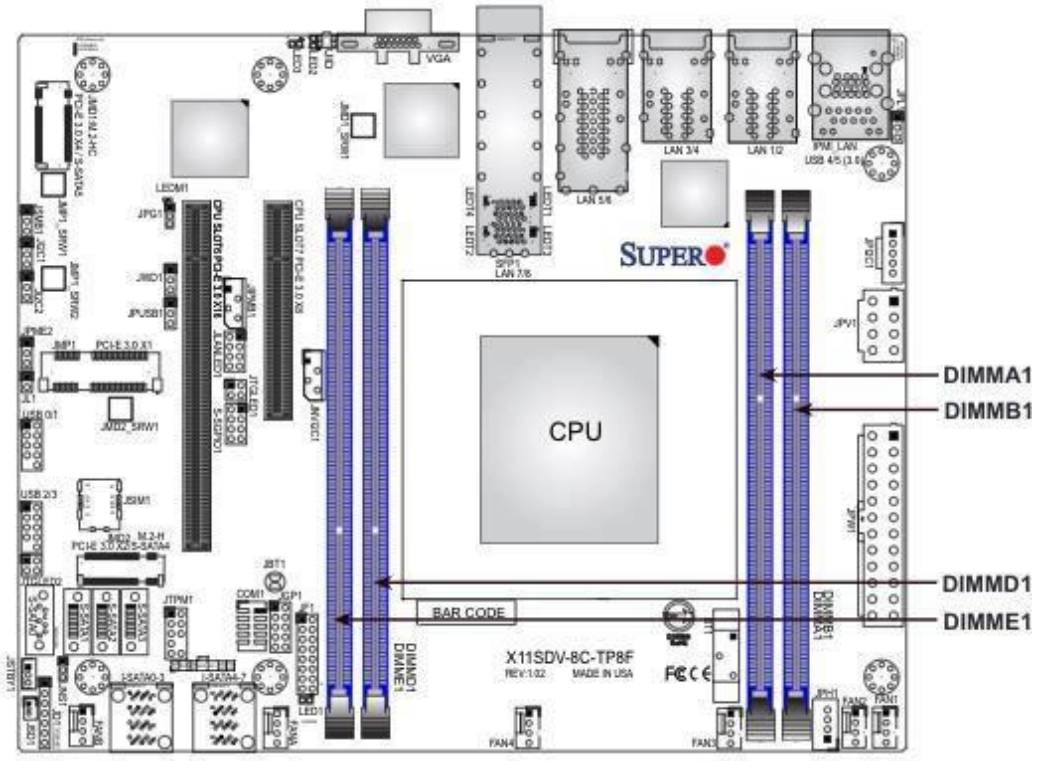
Memory Population (Balanced)				
DIMMA1	DIMMB1	DIMMD1	DIMME1	Total System Memory
4GB	4GB			8GB
4GB	4GB	4GB	4GB	16GB
8GB	8GB			16GB
8GB	8GB	8GB	8GB	32GB
16GB	16GB			32GB
16GB	16GB	16GB	16GB	64GB
32GB	32GB			64GB
32GB	32GB	32GB	32GB	128GB
64GB	64GB			128GB
64GB	64GB	64GB	64GB	256GB
128GB	128GB			256GB
128GB	128GB	128GB	128GB	512GB

15.1 DIMM Population Configurations

15.2 DIMM Module Population Sequence

When installing memory modules, the DIMM slots should be populated in the following order: DIMMB1, DIMMA1, DIMME1, DIMMD1.

- Always use DDR4 DIMM modules of the same type, size, and speed.
- Mixed DIMM speeds can be installed. However, all DIMMs will run at the speed of the slowest DIMM.
- The motherboard will support odd-numbered modules (one or three modules installed). However, for best memory performance, install DIMM modules in pairs to activate memory interleaving.

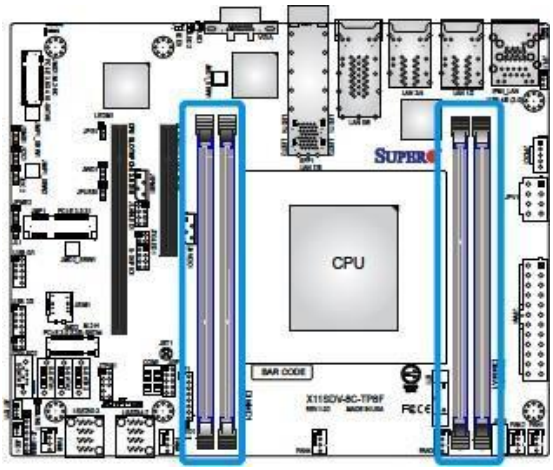


15.2 DIMM Module Population Sequence

15.3 DIMM (Memory)

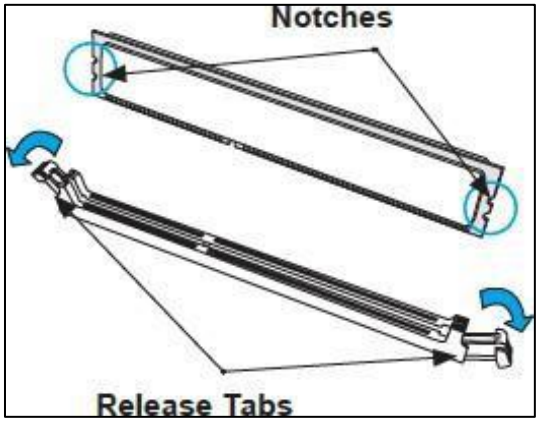
Installation

1 Insert the desired number of DIMMs into the memory slots, starting with DIMMB1, DIMMA1, DIMME1, DIMMD1. For best performance, please use the memory modules of the same type and speed in the same bank.



15.3(a) DIMM Slot Locations

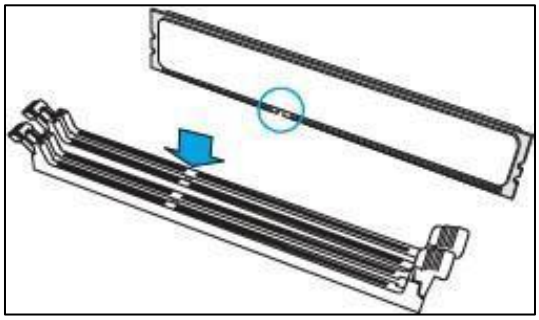
2 Push the release tabs outwards on both ends of the DIMM slot to unlock it.



15.3(b) DIMM Installation

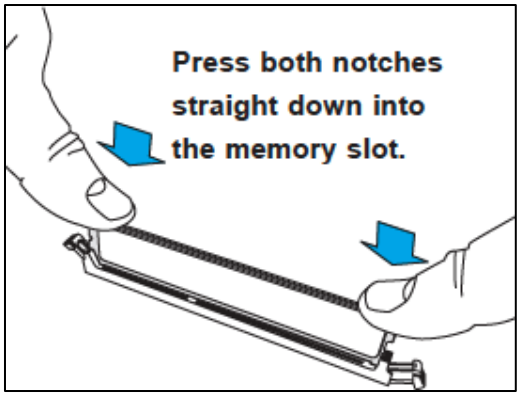
3 Align the key of the DIMM module with the receptive point on the memory slot.

4 Align the notches on both ends of the module against the receptive points on the ends of the slot.



15.3(c) DIMM Installation

5 Press both ends of the module straight down into the slot until the module snaps into place.
6 Press the release tabs to the lock positions to secure the DIMM module into the slot.



15.3(d) DIMM Installation

DIMM Removal

Press both release tabs on the ends of the DIMM module to unlock it. Once the DIMM module is loosened, remove it from the memory slot

15.4 Drive Wipe Procedures

Use the following procedures to securely delete data from the SSDs in the DDS-M Nodes and the Dell Master Laptops.

Wiping SATA SSDs

1 Use the following command to verify that the identified drive is not frozen:

```
hdparm -I /dev/sda
```

2 Set a temporary password using the following command:

```
hdparm -user-master u -security-set-pass <Password> /dev/sda
```

3 Check that the security password is enabled:

```
hdparm -l /dev/sda
```

4 Use the following command to completely wipe the drive:

```
hdparm --user-master u --security-erase-enhanced <password> /dev/sda
```

Wiping NVMe SSDs

1 Use the following command to verify that the identified drive is not frozen:

```
hdparm -l /dev/nvme0n1
```

2 Install the nvme-cli package

```
apt-get install nvme-cli
```

3 Check if the NVMe drive supports Secure Erase. Look for the line “Format NVM Supported”

```
nvme id-ctrl -H /dev/nvme0n1 | grep NVM
```

4 Use the following command to completely wipe the drive

```
nvme format /dev/nvme0 --ses=1
```

16 Motherboard Troubleshooting Procedures

Use the following procedures to troubleshoot the system. Always disconnect the AC power cord before adding, changing, or installing any non-hot-swap hardware components.

16.1 Before Power On

1. Make sure that there are no short circuits between the motherboard and chassis.
2. Disconnect all ribbon/wire cables from the motherboard, including those for the keyboard and mouse.
3. Remove all add-on cards.
4. Install the CPU (making sure it is fully seated) and connect the front panel connectors to the motherboard.

16.2 No Power

1. Make sure that there are no short circuits between the motherboard and the chassis.
2. Make sure that the ATX power connectors are properly connected.
3. Check that the 115V/230V switch, if available, on the power supply is properly set.
4. Turn the power switch on and off to test the system, if applicable.
5. The battery on the motherboard may have expired. Check to verify that it still supplies ~3VDC. If it does not, replace it with a new one.

16.3 No Video

1. If the power is on but the system fails to display video, remove and re-seat all cables, and if necessary, remove or re-seat any modified hardware.
2. Use the speaker to determine if any beep codes are present. Refer to Appendix A for details on beep codes.
3. Remove all memory modules and turn on the system (if the alarm is on, check the specs of memory modules, reset the memory, or try a different module).

16.4 System Boot Failure

If the system does not display POST or does not respond after the power is turned on, check the following:

1. Check for any error beep from the motherboard speaker.
2. If there is no error beep, try to turn on the system without DIMM modules installed. If there is still no error beep, replace the motherboard.
3. If there are error beeps, clear the CMOS settings by unplugging the power cord and contacting both pads on the CMOS clear jumper (JBT1). Remove all components from the motherboard, especially the DIMM modules. Make sure that system power is on and that memory error beeps are activated.

4 Turn on the system with only one DIMM module installed. If the system boots, check for bad DIMM modules or slots by following the Memory Errors Troubleshooting procedure in this chapter.

16.5 Memory Errors

When a no-memory beep code is issued by the system, check the following:

1 Make sure that the memory modules are compatible with the system and that the DIMMs are properly and fully installed. Click on the Tested Memory List link on the motherboard product page to see a list of supported memory.
2 Check if different speeds of DIMMs have been installed. For optimal performance use the same RAM type and speed for all DIMMs in the system.
3 Use the correct type of ECC DDR4 UDIMM modules recommended by the manufacturer.
4 Check for bad DIMM modules or slots by swapping a single module among all memory slots and check the results.
5 Make sure that there are no short circuits between the motherboard and the chassis. Make sure that all memory modules are fully seated in their slots.
6 Make sure that there are no short circuits between the motherboard and the chassis. Please follow the instructions given in the DIMM population tables listed in **Section 15.3** to install memory modules.

16.6 Losing the System's Setup Configuration

1 Always use a high-quality power supply. A poor-quality power supply may cause the system to lose the CMOS setup information or may cause power inconsistencies.
2 The battery on the motherboard may be old. Check to verify that it still supplies ~3VDC. If it does not, replace it with a new one. If the above steps do not fix the setup configuration problem, contact the vendor for repairs.

16.7 When the System Becomes Unstable

If the system becomes unstable during or after OS installation, check the following:

1. CPU/BIOS support: Make sure that the CPU is supported and that the latest BIOS is correctly installed.
2. Memory support: Make sure that the memory modules are supported by testing the modules using memtest86 or a similar utility.

✎ **Note**: Click on the Tested Memory List link on the motherboard product page to see a list of supported memory.

3. HDD support: Make sure that all hard disk drives (HDDs) work properly. Replace the bad HDDs with good ones.
4. System cooling: Check the system cooling to make sure that all heatsink fans and CPU/system fans, etc., work properly. Check the hardware monitoring settings in the IPMI to make sure that the CPU and system temperatures are within the normal range. Also check the front panel Overheat LED and make sure that it is not on.
5. Adequate power supply: Make sure that the power supply provides adequate power to the system. Make sure that all power connectors are connected. Please refer to our website for more information on the minimum power requirements.
6. Proper software support: Make sure that the correct drivers are used.

If the system becomes unstable before or during OS installation, check the following:

1. Source of installation: Make sure that the devices used for installation are working properly, including boot devices such as CD/DVD.
2. Cable connection: Check to make sure that all cables are connected and working properly.
3. Using the minimum configuration for troubleshooting: Remove all unnecessary components (starting with add-on cards first) and use the minimum configuration (but with the CPU and a memory module installed) to identify the trouble areas.
4. Identifying bad components by isolating them: If necessary, remove a component in question from the chassis, and test it in isolation to make sure that it works properly. Replace a bad component with a good one.
5. Check and change one component at a time instead of changing several items at the same time. This will help isolate and identify the problem.
6. If necessary, swap this component with a new one to see if the system will work properly. If so, then the old component is bad. Test the component in question in another system. If the new system works, the component is good, and the old system has problems.

17 UEFI BIOS

This chapter describes the AMIBIOS™ Setup utility for the X11SDV-16C-TP8F motherboard. The BIOS is stored on a chip and can be easily upgraded using a flash program.

✎ **Note**: Due to periodic changes to the BIOS, some settings may have been added or deleted and might not yet be recorded in this manual. Please refer to the Manual Download area of the SealingTech website for any changes to the BIOS that may not be reflected in this manual.

17.1 Starting the Setup Utility

To enter the BIOS Setup Utility, hit the [**DELETE**] key while the system is booting-up. (In most cases, the [**DELETE**] key is used to invoke the BIOS setup screen. There are a few cases when other keys are used, such as [**F1**], [**F2**], etc.) Each main BIOS menu option is described in this manual.

The Main BIOS screen has two main frames. The left frame displays all the options that can be configured. “Grayed-out” options cannot be configured. The right frame displays the key legend. Above the key legend is an area reserved for a text message. When an option is selected in the left frame, it is highlighted in white. Often a text message will accompany it.

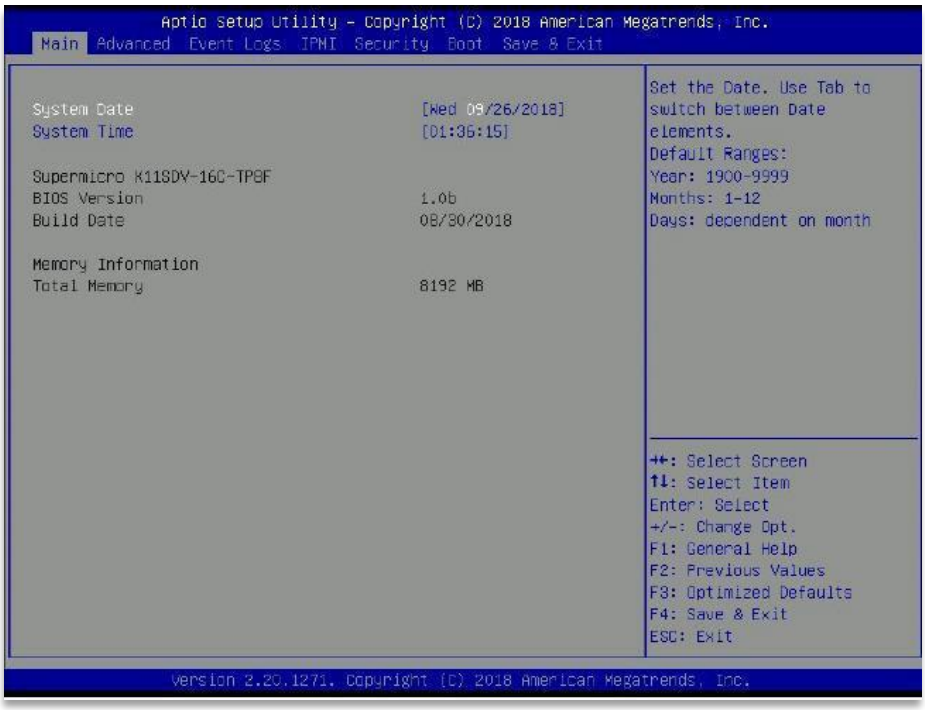
✎ **Note**: The BIOS has default text messages built in. SealingTech retains the option to include, omit, or change any of these text messages. Settings printed in Bold are the default values.

The “►” icon indicates a submenu. Highlighting such an item and pressing the <Enter> key will open the list of settings within that submenu.

The BIOS setup utility uses a key-based navigation system called hot keys. Most of these hot keys ([**F1**], [**ENTER**], [**ESC**], *Arrow* keys, etc.) can be used at any time during the setup navigation process.

17.2 Main Setup

The AMI BIOS setup utility enters the Main setup screen. Return to the Main setup screen by selecting the Main tab on the top of the screen. The Main BIOS setup screen is shown below, and the following features are available:



17.2 BIOS Main Screen

17.3 System Date/System Time

Use this option to change the system date and time. Highlight System Date or System Time using the arrow keys. Enter new values using the keyboard. Press the <Tab> key or the arrow keys to move between fields. The date must be entered in MM/DD/YYYY format. The time is entered in HH:MM:SS format.

✎ **Note**: The time is in the 24-hour format. For example, 5:30 P.M. appears as 17:30:00. The date's default value is the BIOS build date after RTC reset.

17.4 BIOS Version

This feature displays the version of the BIOS ROM used in the system.

17.5 Build Date

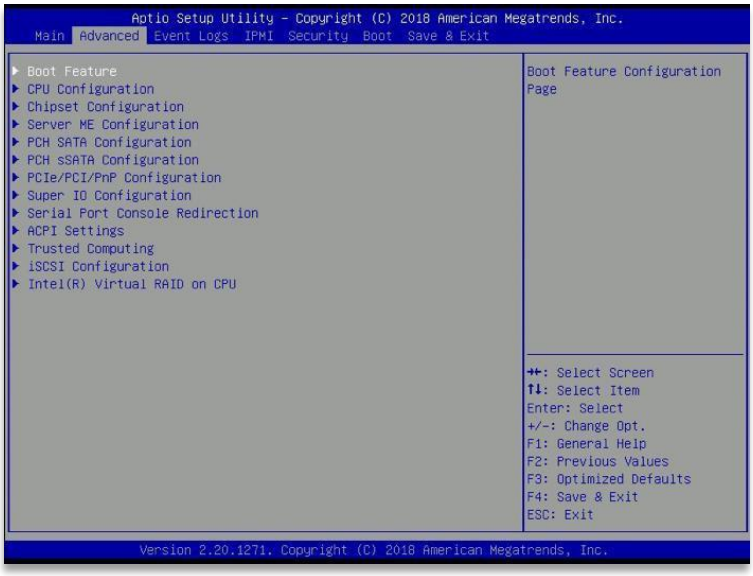
This feature displays the date when the version of the BIOS ROM used in the system was built.

17.6 Memory Information

17.6.1 Total Memory
This feature displays the total size of memory available in the system.

17.6.2 Memory Speed
This feature displays the default speed of the memory modules installed in the system.

17.7 Advanced
Use this menu to configure advanced settings.



17.7 BIOS Advanced Screen

⚠ **Warning**: Take caution when changing the Advanced settings. An incorrect value, a very high DRAM frequency or an incorrect BIOS timing setting may cause the system to malfunction. When this occurs, restore to default manufacturer settings.

17.8 Boot Feature

17.8.1 Quiet Boot

Use this feature to select the screen display between POST messages or the OEM logo at bootup. Select Disabled to display the POST messages. Select Enabled to display the OEM logo instead of the normal POST messages. The options are Disabled and Enabled.

17.8.2 Option ROM Messages

Use this feature to set the display mode for the Option ROM. Select Keep Current to display the current AddOn ROM setting. Select **Force BIOS** to use the Option ROM display set by the system BIOS. The options are Force BIOS and Keep Current.

17.8.3 Bootup NumLock State

Use this feature to set the Power-on state for the Numlock key. The options are Off and On.

17.8.4 Wait for “F1” if Error

This feature forces the system to wait until the F1 key is pressed if an error occurs. The options are Disabled and Enabled.

17.8.5 INT19 (Interrupt 19) Trap Response

Interrupt 19 is the software interrupt that handles the boot disk function. When this item is set to Immediate, the ROM BIOS of the host adaptors will “capture” Interrupt 19 at bootup immediately and allow the drives that are attached to these host adaptors to function as bootable disks. If this item is set to Postponed, the ROM BIOS of the host adaptors will not capture Interrupt 19 immediately and allow the drives attached to these adaptors to function as bootable devices at bootup. The options are Immediate and Postponed.

17.8.6 Re-try Boot

If this item is enabled, the BIOS will automatically reboot the system from a specified boot device after its initial boot failure. The options are Disabled, Legacy Boot, and EFI Boot.

17.8.7 Port 61h bit-4 Emulation

Select Enabled to enable the emulation of Port 61h bit-4 toggling in SMM (System Management Mode). The options are Disabled and Enabled.

17.9 Power Configuration

17.9.1 Watch Dog Function

If enabled, the Watch Dog timer will allow the system to reboot when it is inactive for more than five minutes. The options are Disabled and Enabled.

17.9.2 Power Button Function

This feature controls how the system shuts down when the power button is pressed. Select 4 Seconds Override for the user to power off the system after pressing and holding the power button for four seconds or longer. Select Instant Off to instantly power off the system as soon as the user presses the power button. The options are 4 Seconds Override and Instant Off.

17.9.3 Restore on AC Power Loss

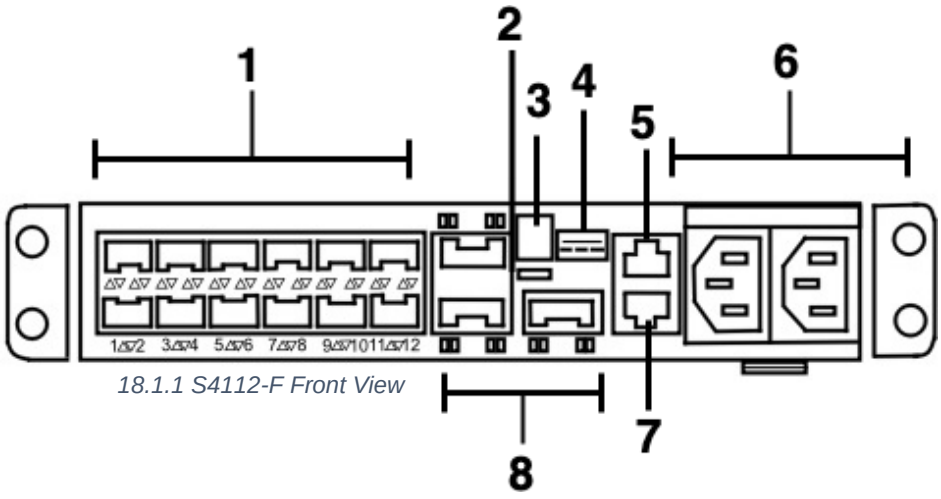
Use this feature to set the power state after a power outage. Select Power Off for the system power to remain off after a power loss. Select Power On for the system power to be turned on after a power loss. Select Last State to allow the system to resume its last power state before a power loss. The options are Stay Off, Power On, and Last State.

18 S4112-ON Series (S4112F-ON and S4112T-ON Switches)

The S4112F-ON and the S4112T-ON switches are robust fixed form-factor switches for 10G servers.

18.1 Features

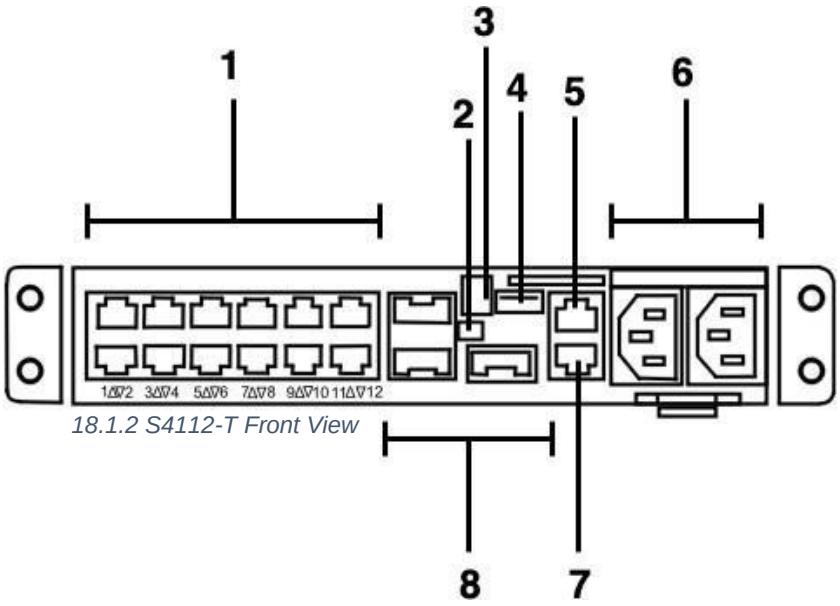
18.1.1 S4112-F Switch I/O Front View



18.1.1 S4112-F Front View

S4112-F Switch Ports and Descriptions	
Port Series	**Descriptions**
1	**Twelve SFP+ ports**
2	**Micro USB-B console port**
3	**Stack ID**
4	**Ethernet management port**
5	**RS-232 console port**
6	**AC PSUs**
7	**RJ-45 management port**
8	**Three QSFP28 ports**

18.1.2 S4112-T Switch I/O Front View

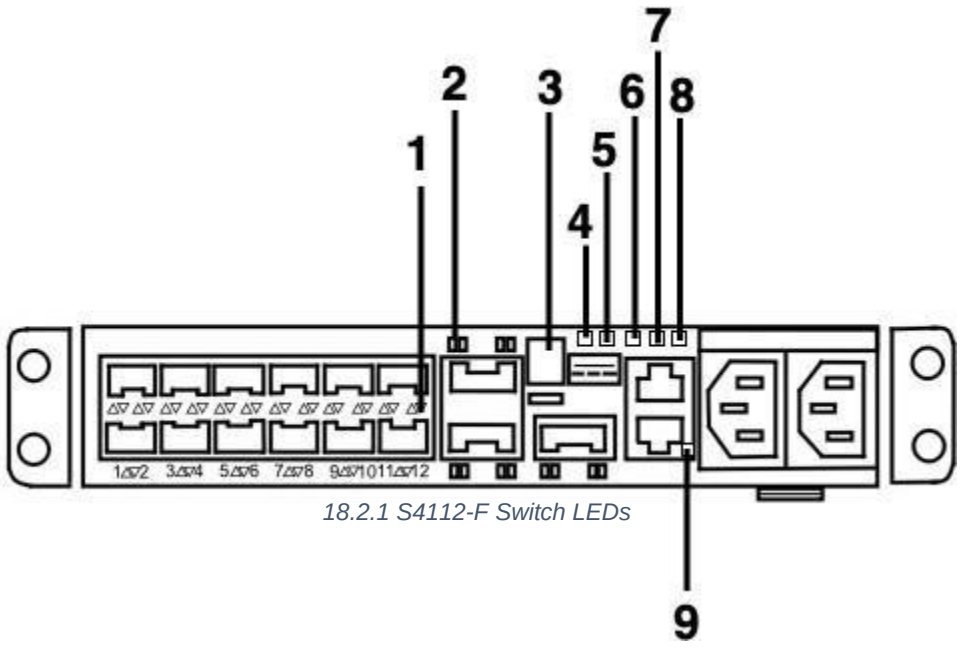


18.1.2 S4112-T Front View

S4112-T Switch Ports and Descriptions	
Port Series	**Descriptions**
1	**Twelve RJ-45 ports**
2	**Micro USB-B console port**
3	**Stack ID**
4	**Ethernet management port**
5	**RS-232 console port**
6	**AC PSUs**
7	**RJ-45 management port**
8	**Three QSFP28 ports**

18.2 LED Behavior

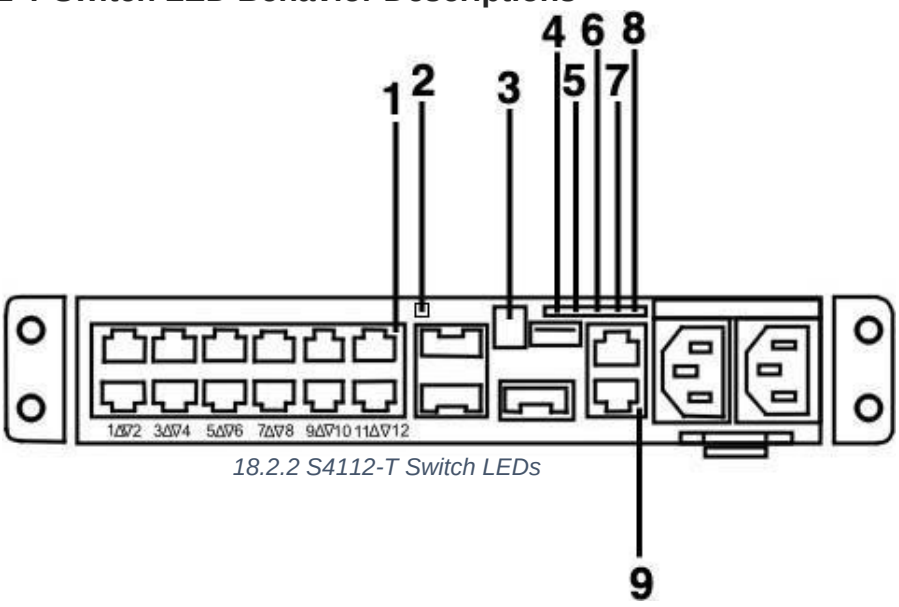
18.2.1 S4112-F Switch LED Behavior Descriptions



18.2.1 S4112-F Switch LEDs

S4112-F LED Ports and Descriptions	
Port Series	**Descriptions**
1	**SFP+ port LED**
2	**QSFP28 port LED**
3	**Stack ID**
4	**Master LED**
5	**System LED**
6	**Power LED**
7	**Fan LED**
8	**Locator LED/System Beacon**
9	**RJ-45/RS-232 LED**

18.2.2 S4112-T Switch LED Behavior Descriptions



18.2.2 S4112-T Switch LEDs

S4112-T LED Ports and Descriptions	
Port Series	**Descriptions**
1	**RJ-45 port LED**
2	**QSFP28 port LED**
3	**Stack ID**
4	**Master LED**
5	**System LED**
6	**Power LED**
7	**Fan LED**
8	**Locator LED/System beacon**
9	**RJ-45/RS-232 LED**

18.2.3 LED Behavior Definitions

LED	Definition
System Status/Health LED	Solid green — Normal Operation
	Flashing green — Booting
	Solid yellow — Critical system error
	Flashing yellow — Noncritical system error, fan failure, or power supply failure
Power LED	Off — No power
	Solid green — Normal
	Solid yellow — POST is in process
	Flashing yellow — Power Supply failure or loss of power redundancy
Fan LED	Off — No power
	Solid green — Fan powered and running at the expected RPM
	Flashing yellow — Fan failed or loss of cooling redundancy
PSU LED	Off — No power
	Solid green — Normal
	Flashing yellow — PSU failure
	Flashing green — FW update
Locator LED/System Beacon	Off — Locator function is disabled
	Flashing blue — Locator function is enabled
Master LED	Off — system is the stack slave
	Solid green — System is the stack master or a standalone unit
7-segment LED	Off — No power
	Solid green — displays a hex digit representing the stack unit ID

System Management Ethernet Port LEDs

LED	Description
Link LED	Off — No link
	Solid green — Link operating at a maximum speed, auto-negotiated/forced or 1G
	Solid yellow — Link operating at a lower speed, auto-negotiated/forced or 10/100M
Activity LED	Off — No link
	Flashing green — Port activity

SFP+ port LEDs

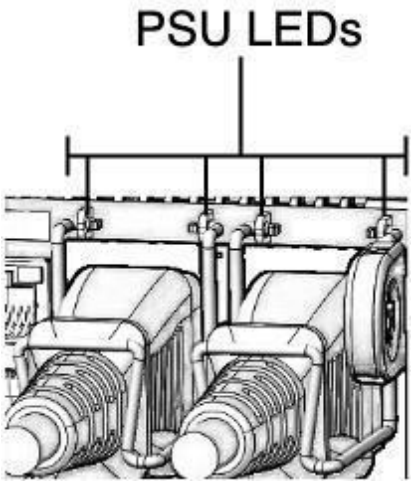
LED	Description
Link LED	Off — No link
	Solid green — Link operating at maximum speed — 10G on an SFP+ port
	Solid yellow — Link operating at a lower speed — 1G on,an SFP+ port
Activity LED	Off — No link
	Flashing green — Port activity
	Solid blue, 1 second on/off — Port beacon

QSFP28 port LEDs

LED	Description
Link/Activity LED	Off — No link
	Solid green — Port link, operating at maximum speed— 100G on a QSFP28 port or 40G on a, QSFP+ port
	Flashing green — Port activity operating at maximum speed — 100G on, a QSFP28 port
	Solid yellow — Port link operating at a lower speed
	Flashing yellow, 1 second on/off — Port beacon — Port activity at 100G on a QSFP28 port
Link/Activity LED—4x25G mode or 4x10G mode	Off — No link
	Solid green — Port link, at 4x25G on a QSFP28 port or 4x10G on a QSFP+ port
	Flashing green — Port activity at 4x25G on a QSFP28 port
	Solid yellow — Port link, at 4x10G on a QSFP28 port
	Flashing yellow, 1 second on/off — Port beacon — Port activity at 4x10G on a QSFP28 port
Link/Activity LED—2x50G	Off—No link
	Solid yellow — Port link, at 2x50G on a QSFP28 port
	Flashing yellow — Port activity at 2x50G on a QSFP28 port
	Flashing yellow, 1 second on/off — Port beacon

Power Supply Unit (PSU) LEDs

After connecting the AC power cable to the switch, attach the metal wire clip over each AC power cable.

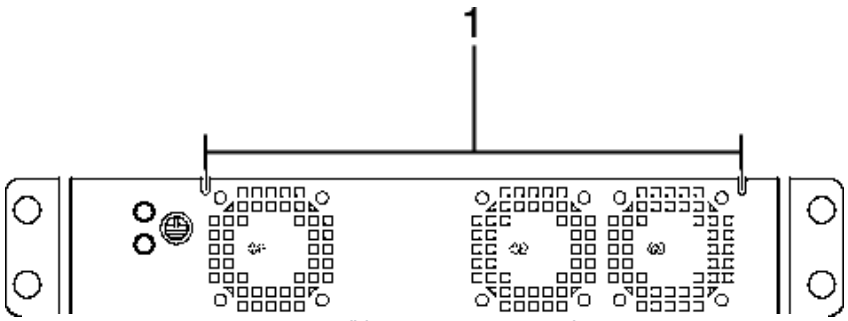


18.2.3(a) S4112 Front Panel PSU LEDs

LED	Description
Solid green	**Input is OK**
Flashing yellow	**There is a fault with the PSU**
Flashing green	**System update**
Off	**PSU is off**

Fan Component LEDs

The fans on the S4112-ON switches support two airflow options: normal and reverse. Integrated Fan number 1 is on the left PSU-side, number 2 is in the center PSU-side, and the last on the right PSU-side.

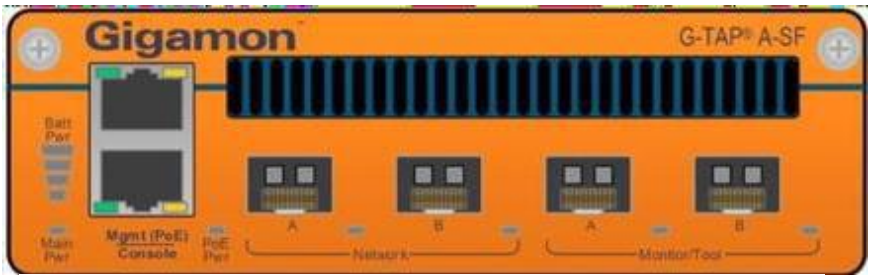


18.2.3(b) S4112 Rear Panel

Fan Modules LED and Descriptions	
LED	**Description**
Solid green	**Fan function is normal**
Flashing yellow	**There is a fan fault**
Off	**Fan is off**

19 GIGAMON A-TAP

The G-TAP A Series implements Gigamon's unique Always-On architecture, eliminating network link downtime through the use of up to four power sources, including primary AC, DC, or Power over Ethernet (PoE) sources, and a secondary on-board battery backup. Primary power sources charge the backup battery until it is at100 percent capacity and starts charging at 95 percent capacity, so it is ready to assume the power load in the event of a power failure on the primary sources.



19 Gigamon G-TAP Front Panel

The transceivers in the Monitor/Tool ports must run at the same speed as those in the network ports, but do not need to be the same medium. For example, install 1G SX SFP transceivers in both Network A and B while using 1G copper SFPs in Monitor/Tool A and B. The external devices connected to Network A and B determine the traffic speed.

✎ **Note**: The Copper SFP RJ45 10Gbe does not work with the G-TAP A-SF.

19.1 Installing the G-TAP A Series Battery

Use the following instructions to replace the battery:

G-TAP A-TX shown; G-TAP A-SF does not include the DIP switches.

19.1(a) Gigamon G-TAP Rear View

1 Place the tap upright on a flat surface
2 Loosen the thumbscrews on the battery cover (shown at right) and remove it.
3 Disconnect the fan connector.
4 Orient the battery so that the battery connector is on the bottom.
5 Slide the battery into the battery slot.
6 Reconnect the fan connector.
7 Reinstall the battery cover, being careful not to touch the fan.
8 If a primary power source is not already connected, connect one now.

19.1(b) Gigamon G-TAP Battery Insertion

⚠ **Caution**: **ALWAYS USE BATTERIES PROVIDED BY GIGAMON. RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE.**

When a battery is installed to a G-TAP A Series module for the first time, manual battery cycling ensures that battery management is set to the normal condition. The battery exercise cycle is defined as follows:

1 With battery installed in unit, charge the battery for 12 hours or until battery is full.
2 Discharge the battery by unplugging the external power resource for 3 hours or until the battery is empty.
3 Plug in the external power resource. The G-TAP A Series module is ready for use.

✎ **Note**: When a battery is connected to the DW01+ for the first time, it may not enter the normal condition (discharge may not be enabled). In this case, short the CS and VSS pins or connect to a charger to restore to the normal operating condition.

19.2 Power Loss

The G-TAP A Series implements Gigamon's unique Always-On architecture, eliminating network link downtime through the use of up to four power sources, including primary AC, DC, or Power over Ethernet (PoE) sources, and a secondary on-board battery backup. Primary power sources charge the backup battery until it is at 100 percent capacity and starts charging at 95 percent capacity, so it is ready to assume the power load in the event of a power failure on the primary sources.
When all primary power sources are lost, the on-board battery takes over, maintaining operations for up to one hour. SNMP traps are generated at 25 percent increments as the available battery charge falls to - 75%, 50%, and 25%.

The last **Battery Level %** trap is then generated when the available battery charge falls to 15 percent. The G-TAP A-SF keeps traffic flowing as long as it can with the power available. However, once all power is exhausted, no traffic passes through the tap, either through the Network or Tool ports.

19.3 Transceiver Notes and Rules

The G-TAP A-SF supports SFP(SX/LX/ZX) and SFP+(SR/LR/ER/LRM) transceivers, as well as 1M and 5M Direct Attach Cables (SFP+ Copper) for connectivity to 1G/10G fiber Ethernet links.

Keep in mind the following notes and rules for transceivers used with the G-TAP A-SF:

• Tap speed is determined by the external devices connected to the Network ports. The external devices must be running at the same speed for data to be passed to the Monitor/Tool ports.
• The Tool port transceivers must support the same speed as the Network port transceivers. However, the Tool port transceivers do not need to be the same medium, either as one another or as those in the Network ports.

For example, if the network ports both use 1G multi-mode fiber transceivers, the G-TAP supports a 1G single-mode fiber transceiver in Tool Port A and a 1G copper SFP transceiver in Tool Port B. This is summarized in the following table:

Tool Port A	Tool Port B
1G SFP MM	1G SFP Copper

• When using 1G SFP Optical Transceivers in the Monitor/Tool ports, the connected tools must have auto negotiation disabled for the link to establish successfully.

Copper SFP transceivers can only be used at 1G speeds (1000BASE-T). There are no configurable auto negotiation, speed, or duplex settings for these transceivers that would allow 10/100 Mbps use.

20 Technical Support Procedure

Prior to performing any technical modification first check with the DCO helpdesk for troubleshooting services. DCO will diagnose problems with the specific system configuration. If the steps from the Motherboard Troubleshooting Procedures does not resolve the issue, please submit a help desk ticket to the following:

dcohelpdesk@army.mil

21 Appendix A

21.1 BIOS Error POST (Beep) Codes

During the POST (Power-On Self-Test) routines, which are performed upon each system boot, errors may occur.

- Non-fatal errors are those which, in most cases, allow the system to continue to boot. These error messages normally appear on the screen.
- Fatal errors will not allow the system to continue with bootup. If a fatal error occurs, consult with the system manufacturer for possible repairs.

Fatal errors are usually communicated through a series of audible beeps. The table below lists some common errors and their corresponding beep codes encountered by users.

System POST: Bios Beep Codes		
Beep Code	**Error Message**	**Description**
1 beep	Refresh	Circuits have been reset (Ready to power up)
5 short 1 long	Memory error	No memory detected in system
5 long 2 short	Display memory Read/Write error	Video adapter missing or with faulty memory
1 long continuous	System OH	System overheat condition

21.2 BIOS Optimized Configuration

If nodes fail to operate correctly during the **Node Deployment or Redeployment** section, ensure the following configuration is applied to each node:

1 Access the node's IP Management Interface at **`https://10.[kit num].53.[200-205]`**. **Credentials**: ADMIN / ADMIN
2 Select **Configuration** -> **Network** -> **LAN Interface** and change the setting to **Dedicate** from the default of 'Failover'.
3 Select the **Remote Control** tab and choose **IKVM/HTML5**.on the left sidebar.
4 Launch an HTML5 console by clicking IKVM/HTML5 in the main window. Once Firefox loads, review the options at the top IKVM navigation bar within the browser window.
5 Choose **Power Control** then tree option **Set Power OFF** then **Set Power ON**.

✎ **Note**: During reboot, the display window will flash multiple times.

6 Interrupt the normal boot sequence by pressing [**DELETE**] to invoke the BIOS setup screen. Alternatively, use [**F12**] to select BIOS setup from the boot option menu.
7 Choose the options on the following page within the BIOS setup utility:

Save and Exit -> **Restore Optimized Defaults**

Main -> System Date and System Time -> Verify that date and time match the Deployment Laptop.
IPMI -> BMC Network Configuration -> Configuration Address Source -> **DHCP**
IPMI -> BMC Network Configuration -> Update IPMI LAN Configuration -> **Yes**
Boot -> Hard Disk Drive BBS Priorities -> **Set boot option #1 to SATA P4** (TS128)

Boot -> Hard Disk Drive BBS Priorities -> **Set boot option #2 to SATA P1**

(MICRON_5200/5300)

Boot -> Hard Disk Drive BBS Priorities -> **Set boot option #3 to SATA P2**

(MICRON_5200/5300)

Boot -> Hard Disk Drive BBS Priorities -> **Set boot option #4 to SATA P3**

(MICRON_5200/5300)

Boot -> Hard Disk Drive BBS Priorities -> **Set boot option #5 to PCIe SSD** (NVME)

Advanced -> Advanced Power Management Configuration -> Power Technology ->

Custom

Advanced -> Advanced Power Management Configuration -> Power Performance Tuning -> **BIOS Controls EPB**
Advanced -> Advanced Power Management Configuration -> ENERGY_PERF_BIAS_CFG mode -> **Maximum Performance**
Advanced -> Advanced Power Management Configuration -> CPU P State Control -> Config TDP -> **Level 2**
Advanced -> PCIe/PCI/PnP Configuration -> SR-IOV Support -> **Enabled**

Advanced -> PCIe/PCI/PnP Configuration -> NVME Firmware Source -> **AMI Native**

Support

Advanced -> PCIe/PCI/PnP Configuration -> JMD1:M.2-HC PCI-E 3.0 X4 OPROM ->

Legacy

Advanced -> PCIe/PCI/PnP Configuration -> JMD2:M.2-H PCI-E 3.0 X2 OPROM ->

Legacy

Advanced -> PCIe/PCI/PnP Configuration -> PCI-E 3.0 X1 OPROM -> **Legacy**

Advanced -> PCIe/PCI/PnP Configuration -> Onboard LAN Option ROM Type ->

Legacy

Advanced -> PCIe/PCI/PnP Configuration -> Onboard LAN1 Option ROM -> **PXE**

Advanced -> PCIe/PCI/PnP Configuration -> Onboard LAN2 Option ROM -> **PXE**

Advanced -> PCIe/PCI/PnP Configuration -> Onboard LAN3 Option ROM -> **PXE**

Advanced -> PCIe/PCI/PnP Configuration -> Onboard LAN4 Option ROM -> **PXE**

Advanced -> PCIe/PCI/PnP Configuration -> Onboard LAN5 Option ROM -> **Legacy**

Advanced -> PCIe/PCI/PnP Configuration -> Onboard LAN6 Option ROM -> **Legacy**

Advanced -> PCIe/PCI/PnP Configuration -> Onboard LAN7 Option ROM -> **Legacy**

Advanced -> PCIe/PCI/PnP Configuration -> Onboard LAN8 Option ROM -> **Legacy**

Advanced -> PCIe/PCI/PnP Configuration -> Onboard Video Option ROM -> **Legacy**

Press **F4** or navigate to Save and Exit -> **Save Changes and Reset**

DOPE Manual

May 2023 Revision 19

Foreword

General

The DDT Operational Play Book Extension (DOPE) is a modular RPM package that consists of various tools needed by a CPT on mission. The tools provided in DOPE must be deployed in a manner consistent with the instructions in this manual in order for the continued accreditation of the tool. DOPE tools are self-packaged individual templates that are deployed on OS versions of either **RHEL, CentOS, Ubuntu, or Windows** and are the only fully STIG'd, tested, accredited, and approved versions for use in a DDS-M kit. This manual is for **DOPE v1.0**

✎ **Note**: DOPE deploys all tools with default passwords. It is the end-user's responsibility to change default passwords after deployment.

Tool Name	Base OS	Version	Capability	IP Address
Endgame	CentOS 7	3.27	Endpoint Security	10.{{kit_num}}.101.100
Security Onion	CentOS 7	2.3.110	IDS/IPS/PCAP	10.{{kit_num}}.102.100
C2	Rhel 8.7	Nextcloud **20.0.8** Mattermost **5.3.1** Redmine **4.1.1**	Project Management	10.{{kit_num}}.51.100
Ghidra	Rhel 8.7	10.1.5	Reverse Engineering	10.{{kit_num}}.51.101
Kali	Debian	2020.2	Penetration Testing	10.{{kit_num}}.51.102
Rhel 8	Rhel 8.7	Rhel 8.7	Host OS	10.{{kit_num}}.51.103
VSCode	Rhel 8.7	1.5.8	Code & Text Editor	10.{{kit_num}}.51.104
RedSeal	CentOS 7	9.4.2	Network mapping & Auditing	10.{{kit_num}}.51.105
MySQL WB	Rhel 8.7	8.0.27	Database visualizer	10.{{kit_num}}.51.106
Windows	Windows 10	21H2	Host OS	10.{{kit_num}}.51.111

22 DOPE Setup

22.1 DOPE Installation

DOPE is available from the RedHat subscription manager on a deployed kit. In order to make the content available, execute the following commands as root from the master laptop:

1. dnf install dope* --nogpgcheck

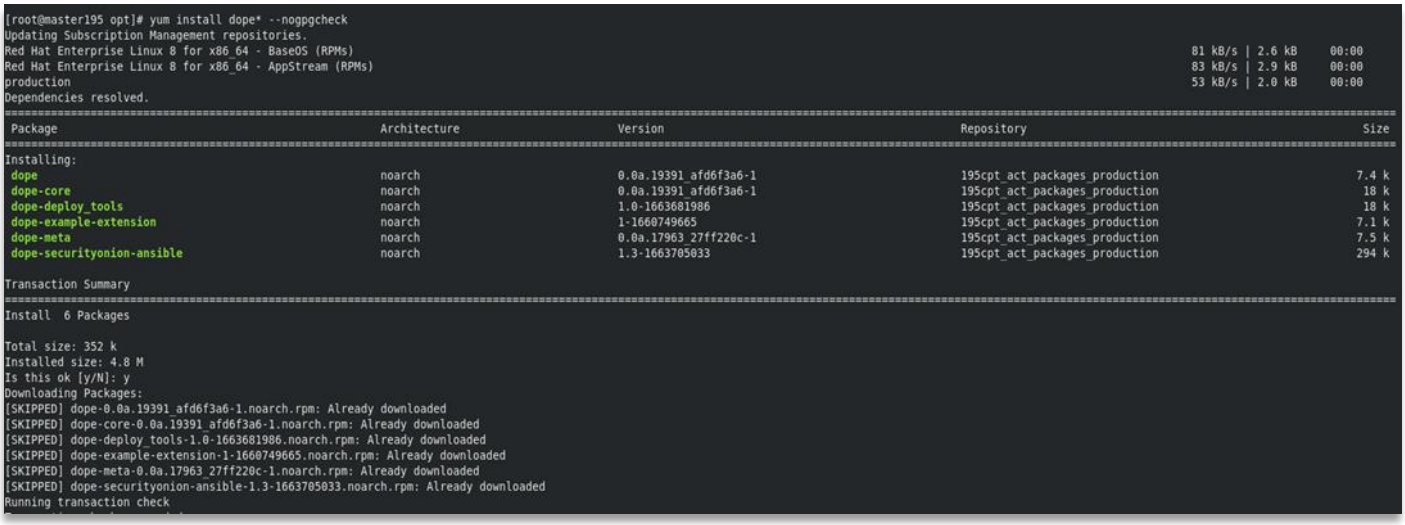


Figure 22.1: Installing DOPE

22.2 DOPE Execution

Once installed, depending on the tool being deployed, dope must be executed from:

1. **/opt/deploy_tools/deploy_tools/**

   or

   /opt/securityonion_automation/securityonion/

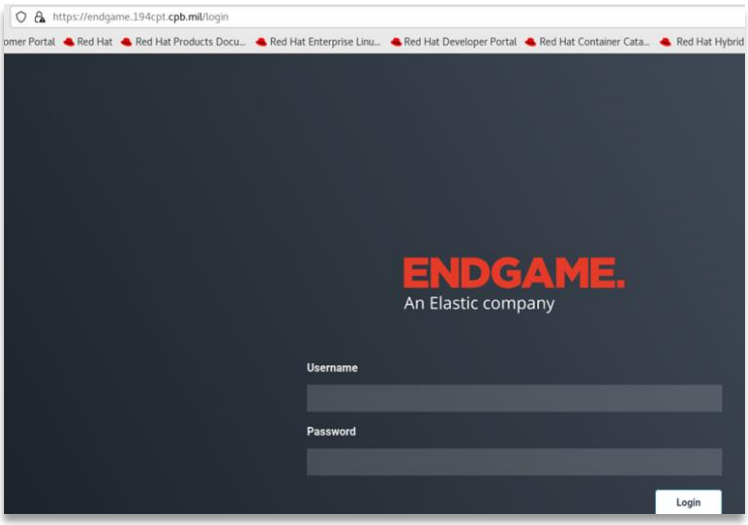
2. From the appropriate directory, type “dope”

```
[root@master195 deploy_tools]# which dope
/bin/dope
[root@master195 deploy_tools]# pwd
/opt/deploy_tools/deploy_tools
[root@master195 deploy_tools]# ls
group_vars  playbooks  templates
[root@master195 deploy_tools]# cd /opt/securityonion_automation/securityonion/
[root@master195 securityonion]# pwd
/opt/securityonion_automation/securityonion
[root@master195 securityonion]# ls
25Jan22ElasticUpdates.ndjson  group_vars    license.lic   playbooks
ansible.cfg                   intca.crt     main.yml      roles
endgame_dashboards.ndjson     license.json  manifest.yml
[root@master195 securityonion]# dope
[root@master195 securityonion]#
```

Figure 22.2: dope execution directories

23 DOPE Tools

✎ **Note**: Unless otherwise stated for specific tools, default passwords can be found in /opt/deploy_tools/deploy_tools/tools_password.txt
as well as
/root/tools_passwords.txt.
It is the end-user's responsibility to change all default passwords after deployment.



23.1 Endgame

The **SO Deploy Endgame** playbook builds and deploys 1 Endgame VM from the endgame template located on the kit Engine Templates. Once deployed, the **SO Install Endgame License** playbook accesses the VM and copies the license to enable Endgame. Once the license has been installed, Endgame can be configured by accessing the WebUI at https://endgame.{{ kit_num }}cpt.cpb.mil/login .

To deploy Endgame, execute the following:

1. **cd /opt/securityonion_automation/securityonion/**
2. Type "dope"

Figure 23.1(a): Endgame WebUI interface login

3. Select SO Deploy Endgame

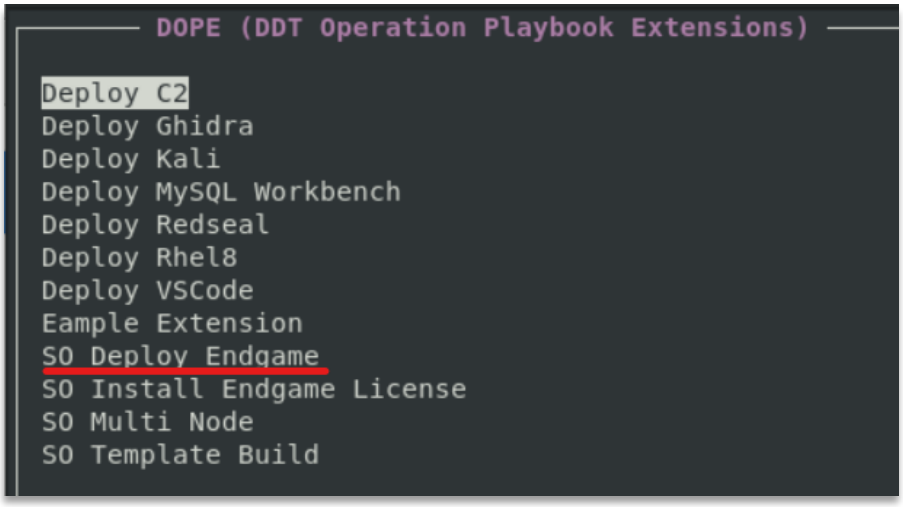


Figure 23.1(b): DOPE Endgame playbook

4. Once the playbook has successfully completed, validate Endgame VM exists on Engine

5. In **/opt/securityonion_automation/securityonion/**, type “dope”

6. Select SO Install Endgame License

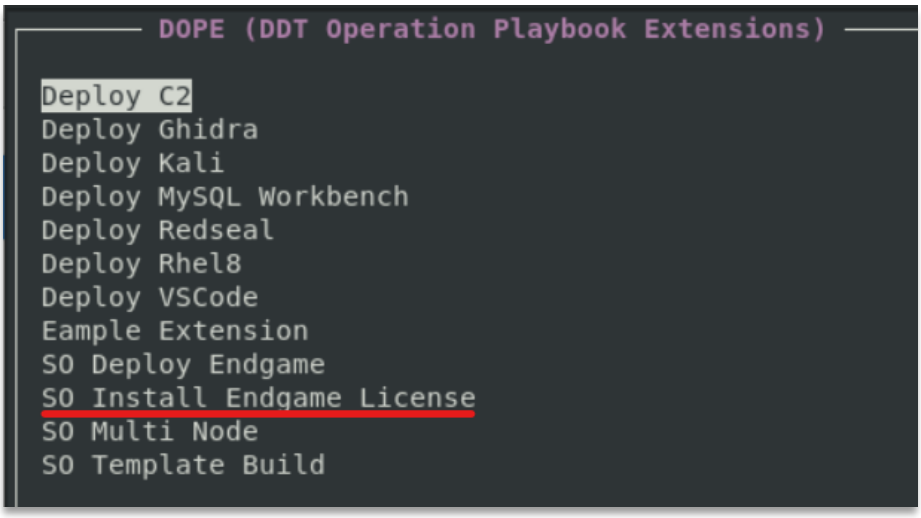


Figure 23.1(c): dope Endgame license playbook execution

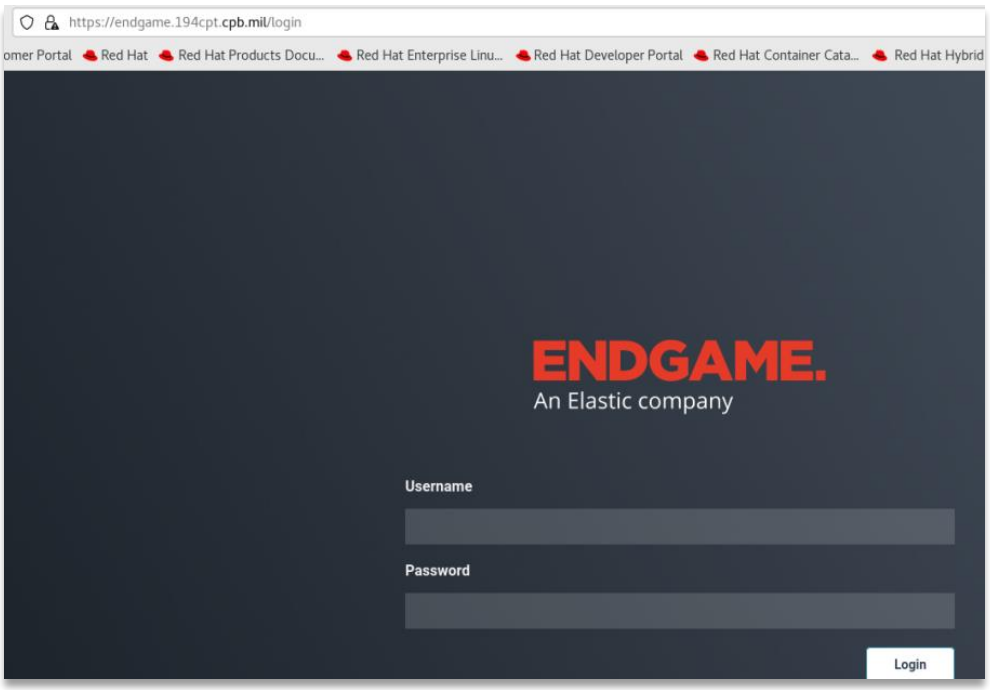


Figure 23.1(d): Endgame WebUI interface login
https://endgame.{{ kit_num }}cpt.cpb.mil/login

23.1.1 Configuring the Endgame Policy

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**."

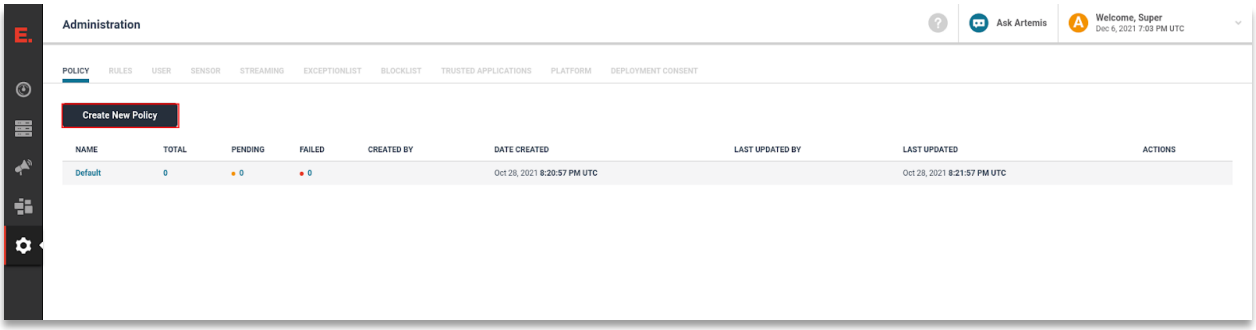


Figure 23.1.1(a): Endgame Policy Creation

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

   Name: SecurityOnion

   Base Policy: Default

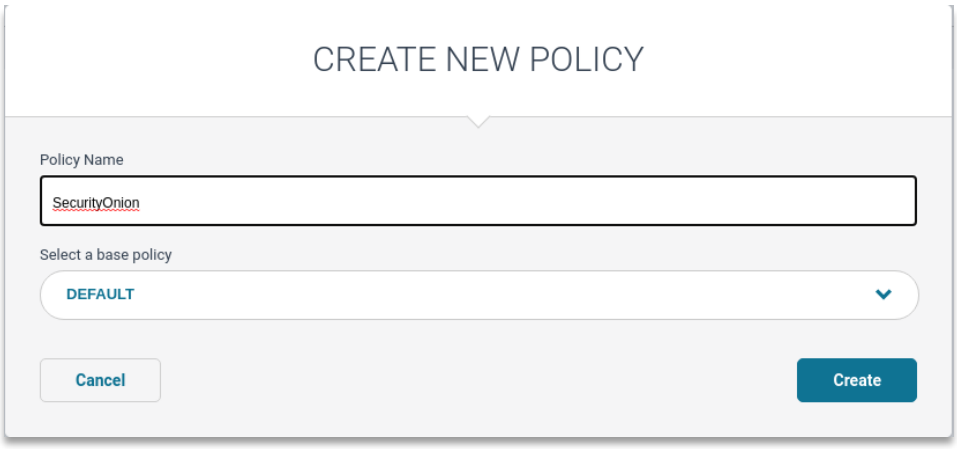


Figure 23.1.1(b): Endgame Policy Name

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**."

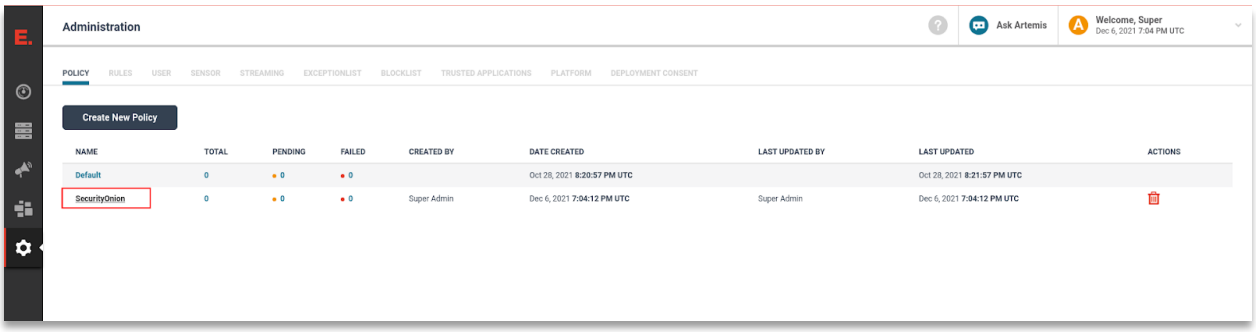


Figure 23.1.1(c): Endgame New Policy Selection

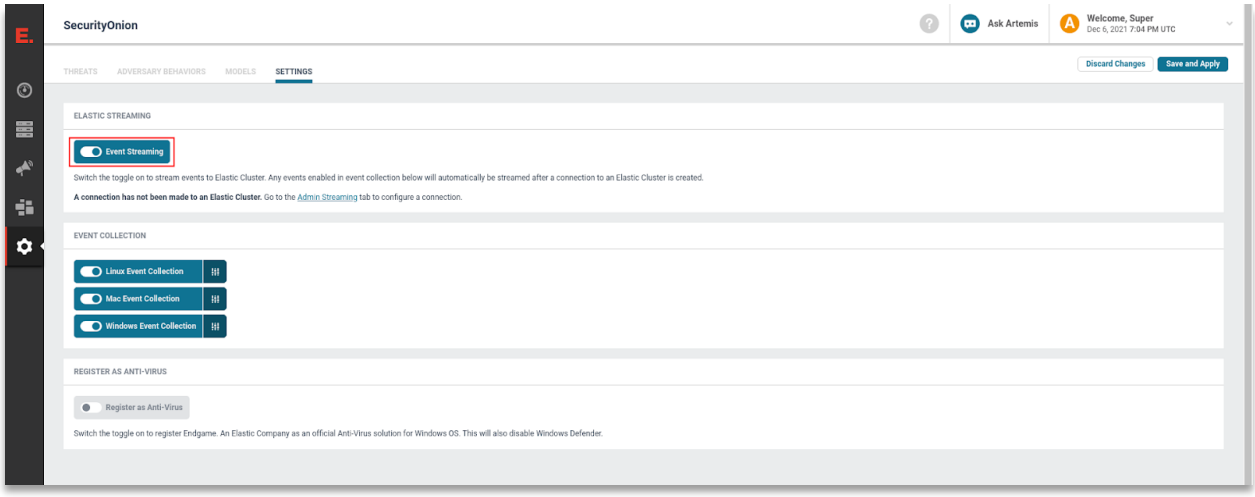


Figure 23.1.1(d): Endgame Policy Event Streaming

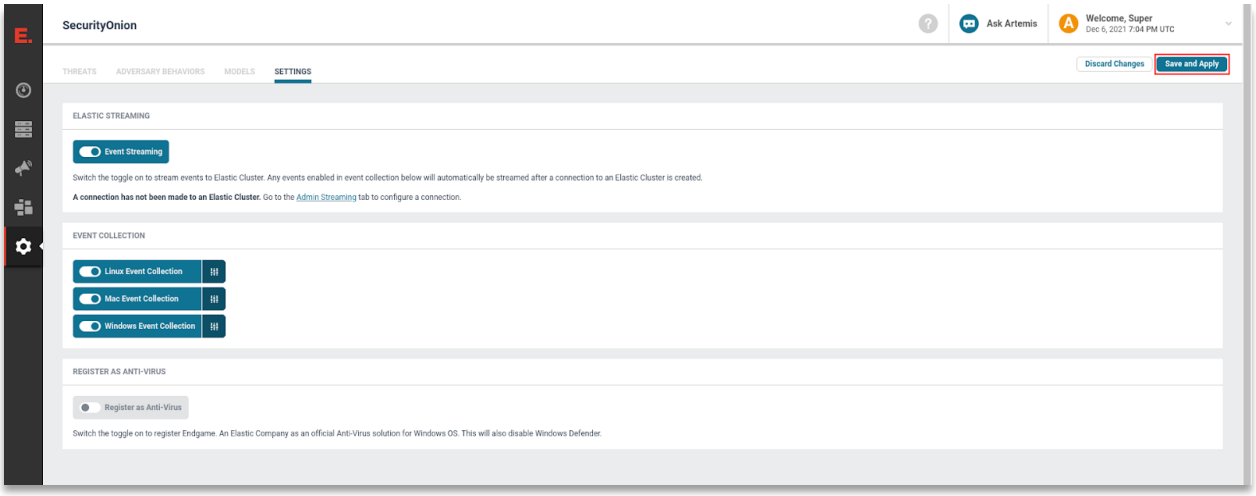


Figure 23.1.1(e): Endgame Policy Save and Apply

23.1.2 Configure Endgame Sensor Profile

1. Navigate to the **Administration** tab and click on **Sensor** then "**Create New Sensor Profile**"

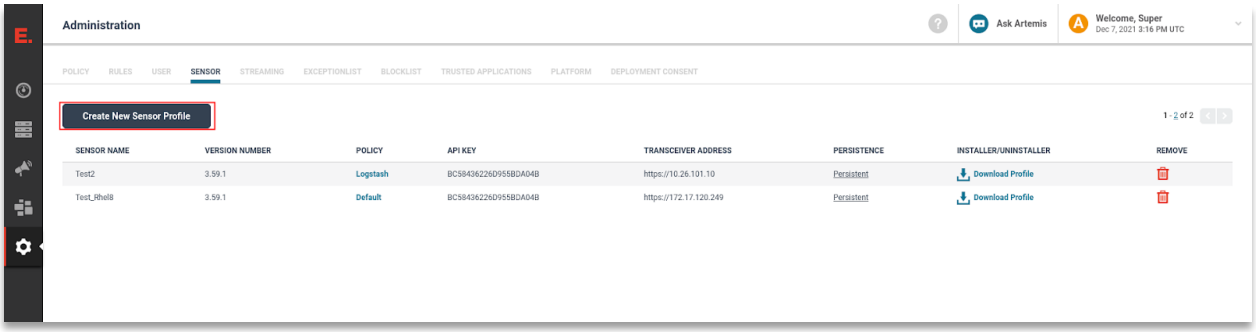


Figure 23.1.2(a): Endgame Profile Creation

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

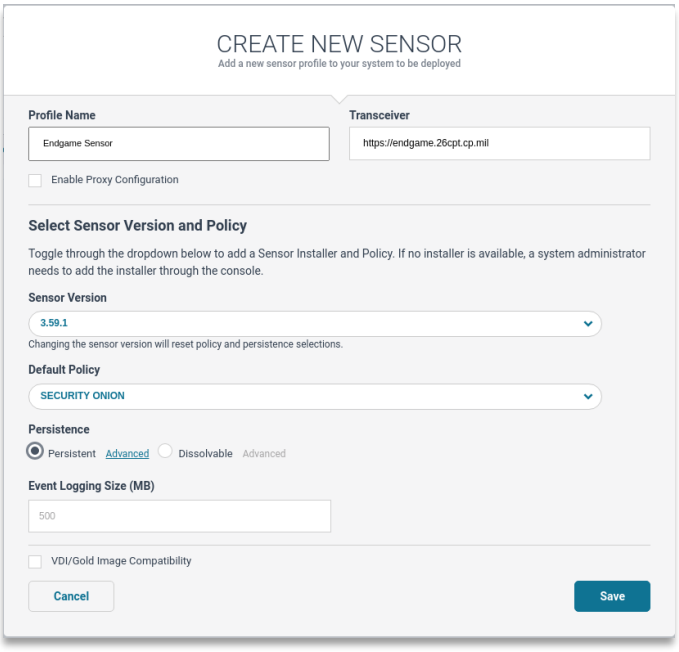


Figure 23.1.2(b): Endgame Sensor Profile Name and Settings

23.2 Security Onion

The DOPE Security Onion deployment is a fully STIG'd and DoD approved version of the free and open-source platform provided by Security Onion Solutions, LLC. The DOPE default deployment installs 1 security onion manager, with 2 search nodes. Sensors can be manually deployed on bare-metal nodes as needed through a provided ISO deployed on Engine.

In order to deploy Security Onion, you must build the Security Onion template from a STIG'd Centos template included as part of the kit installation on Engine. **If Endgame event streaming will be employed, Endgame must be deployed and licensed before SO Multi Node deployment is executed**. For multi-node deployment from the master laptop execute:

1. **cd /opt/securityonion_automation/securityonion/**
2. type **dope**
3. Select **SO Build Template**

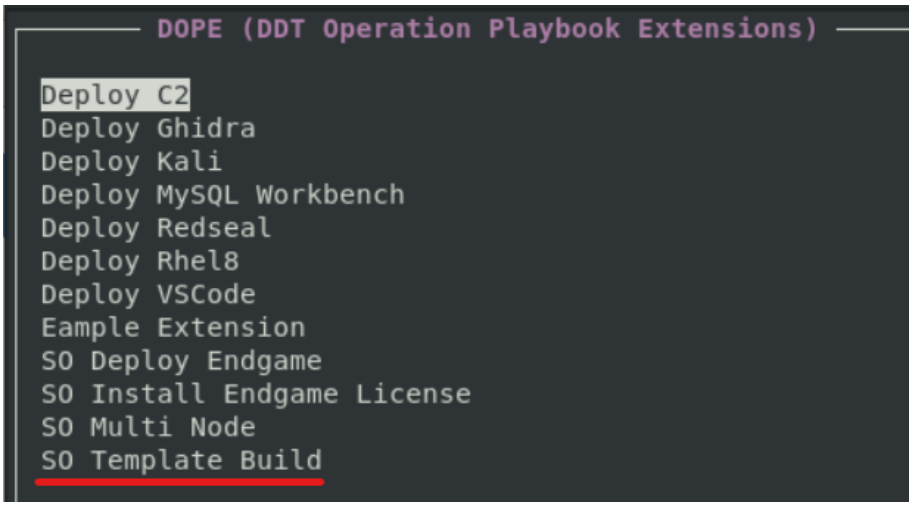


Figure 23.2(a): Build Security Onion template

4. Once the playbook has successfully completed, validate the Security Onion template is created on Engine

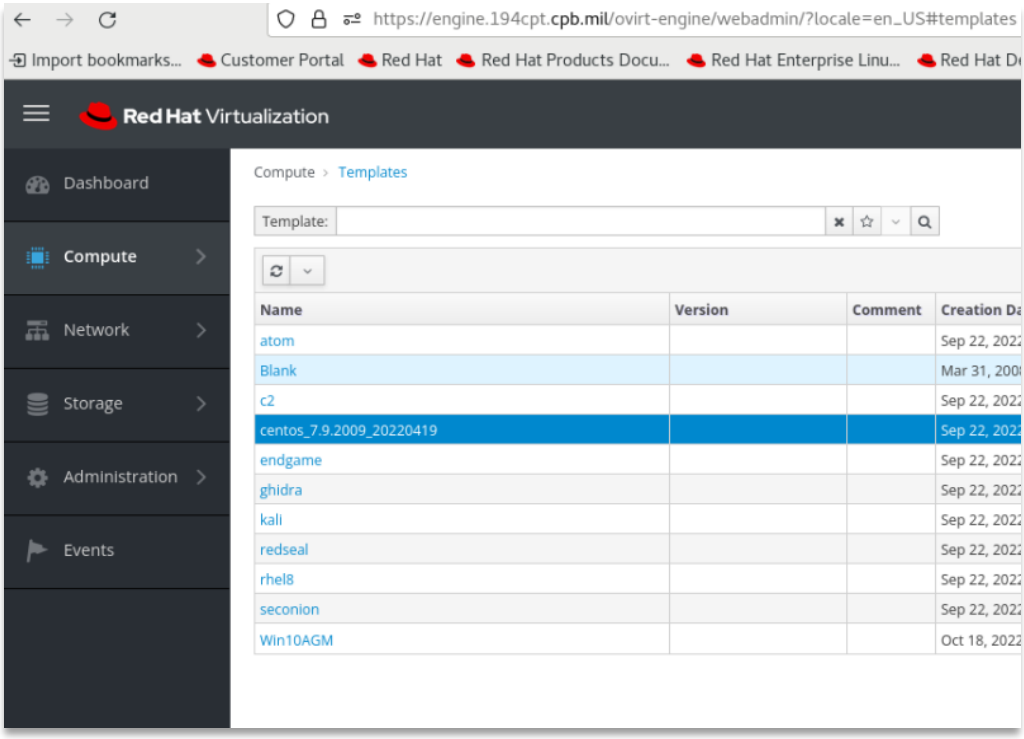


Figure 23.2(b): Centos Template on Engine used to build SO template

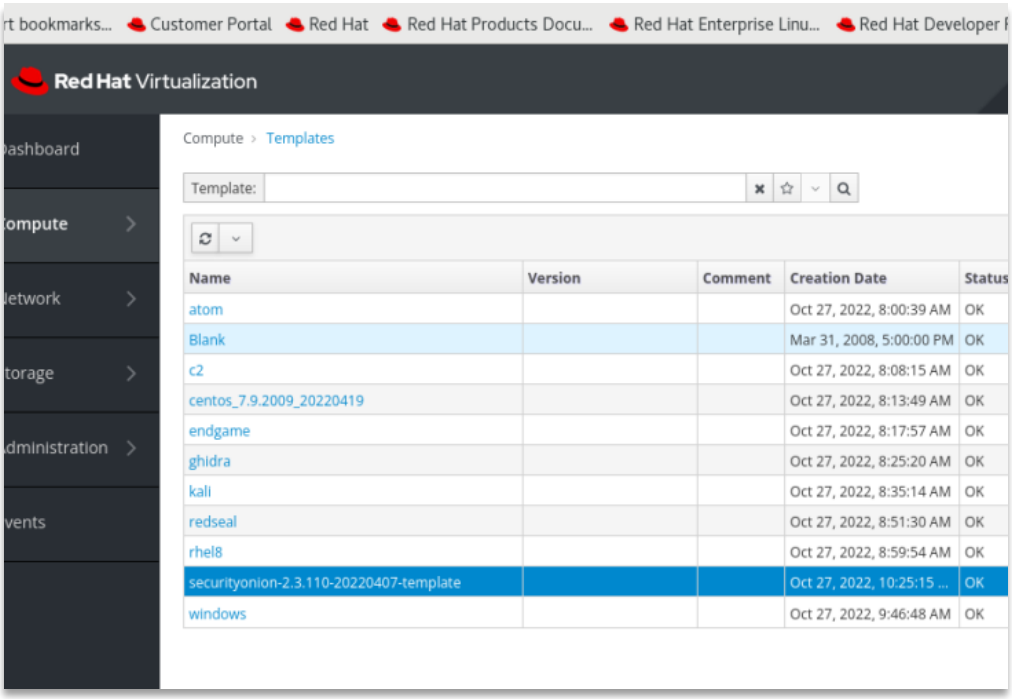


Figure 23.2(c): Security Onion Template available on Engine after Playbook completion

5. Type **dope**

6. Select **SO Multi Node** and follow the prompts to modify default settings as needed

    Number of Searchnodes

    OS username/password

    WEB username/password

    Monitored Networks

    Endgame alert streaming

    Endgame credentials

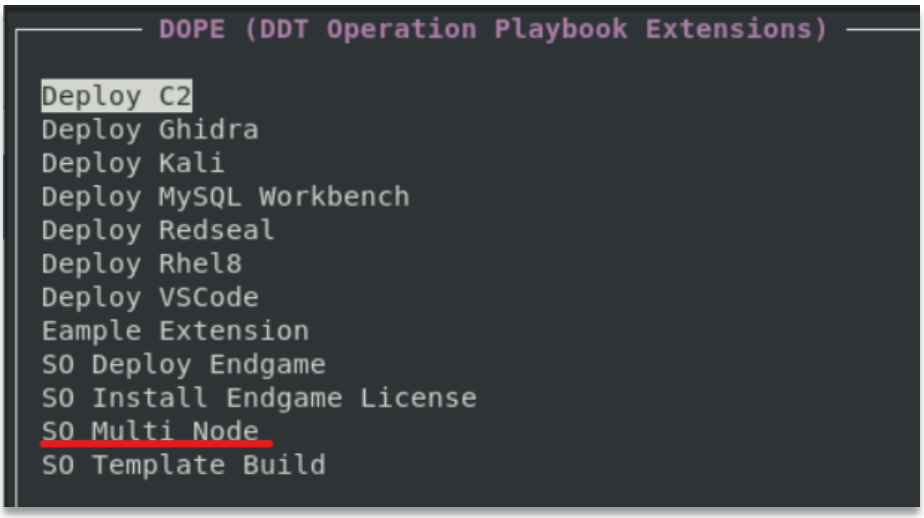


Figure 23.2(d): Security Onion Multi Node deployment

7. Once the playbook deployment completes, validate the manager and search nodes are deployed on Engine

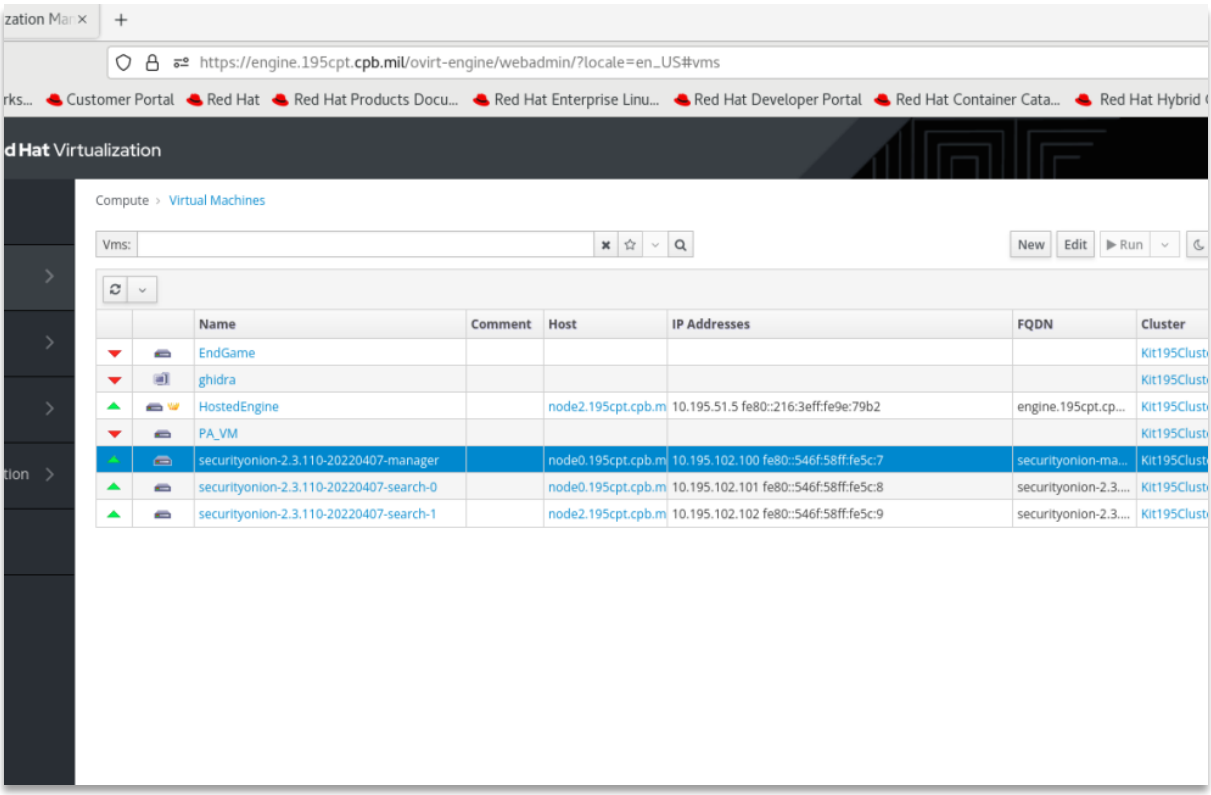


Figure 23.2(e): Security Onion Manager and Search Node deployment

8. Access the Security Onion Manager using Firefox and validate all **Grid** servers are green and with Status Ok

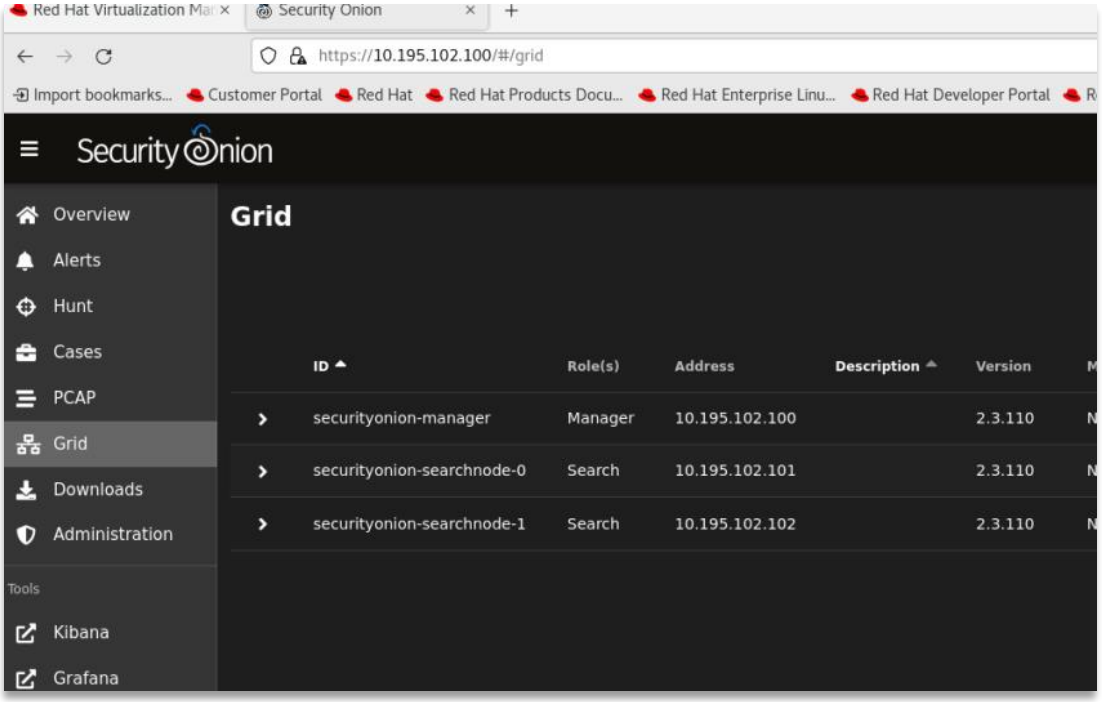


Figure 23.2(f): Security Onion WebUI Grid

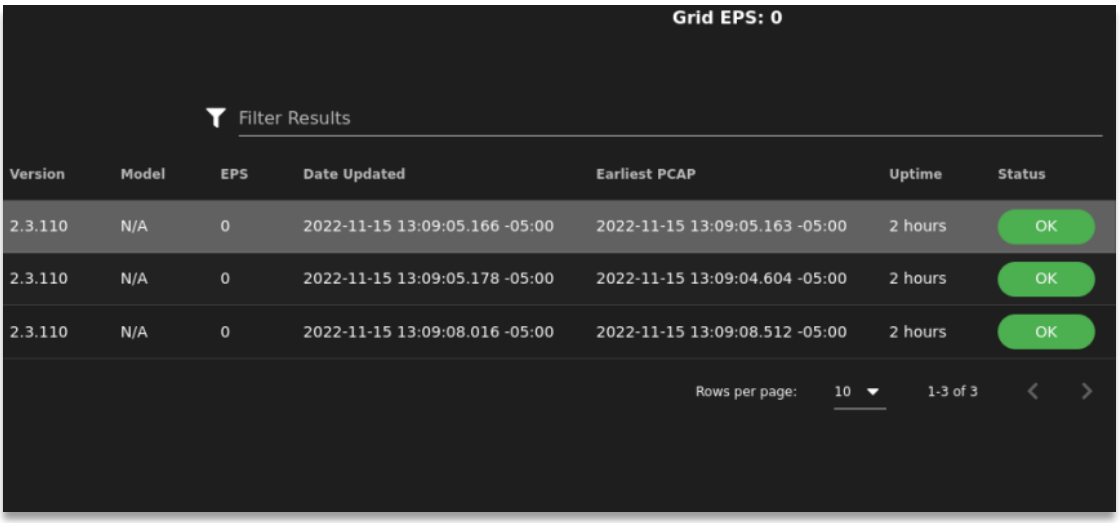


Figure 23.2(g): Security Onion WebUI Grid showing "OK" status

23.3 C2

The DOPE C2 tool includes Mattermost, Redmine, and Nextcloud. Once deployed the C2 individual tools can be accessed from their individual URL.

To deploy C2, execute the following:

1. Type **cd /opt/deploy_tools/deploy_tools/**

2. Type **dope**

3. Select **Deploy C2**

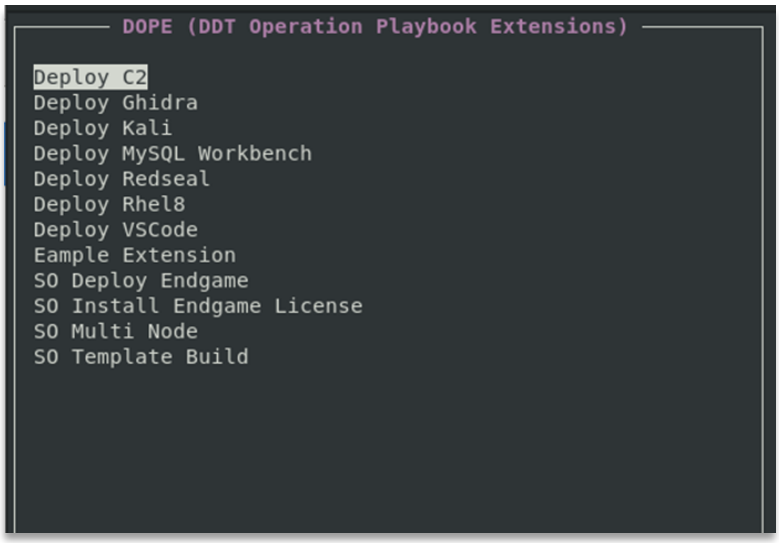


Figure 23.3: Deploy C2

4. Once the playbook has successfully completed, validate the C2 VM exists on Engine

5. To access each tool navigate using firefox to:

   https://mattermost.{{ kit_num }}cpt.cpb.mil/login

   https://nextcloud.{{ kit_num }}cpt.cpb.mil/login

   https://redmine.{{ kit_num }}cpt.cpb.mil/login

✎ **Note**: The login credentials for the applications are located on the C2 server: /home/defender/README.txt

23.4 RedSeal

The RedSeal appliance provides continuous monitoring and reporting capabilities. The RedSeal DOPE playbook deploys a RedSeal VM from the template on Engine.

To deploy the RedSeal appliance, execute the following:

1. Type **cd /opt/deploy_tools/deploy_tools/**

2. Type **dope**

3. Select **Deploy Redseal**

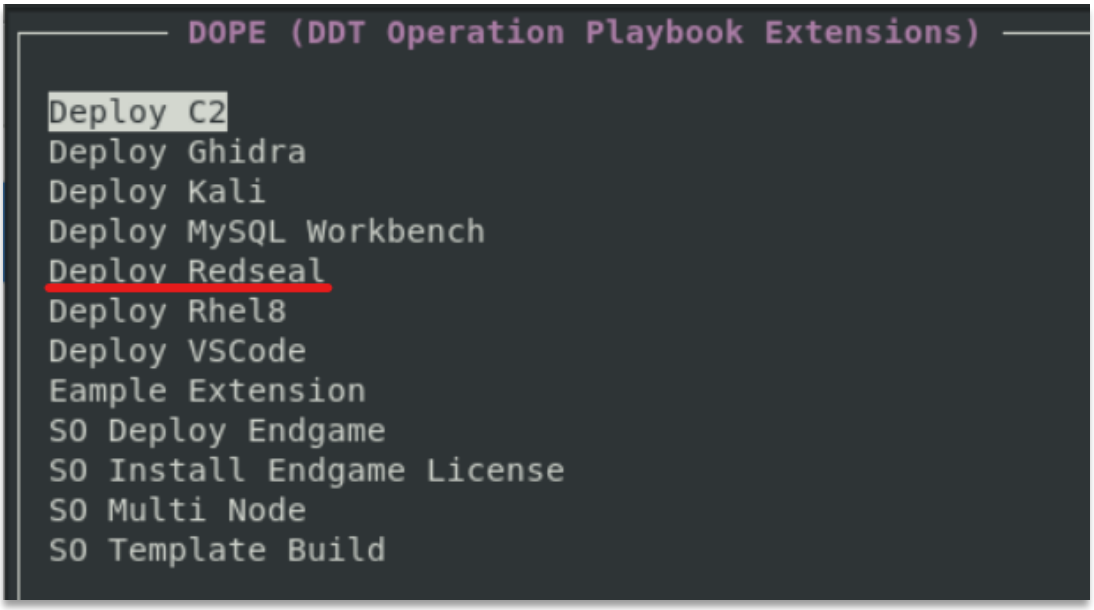


Figure 23.4(a): RedSeal Playbook Selection

4. Once the playbook has successfully completed, validate that RedSeal VM exists on Engine

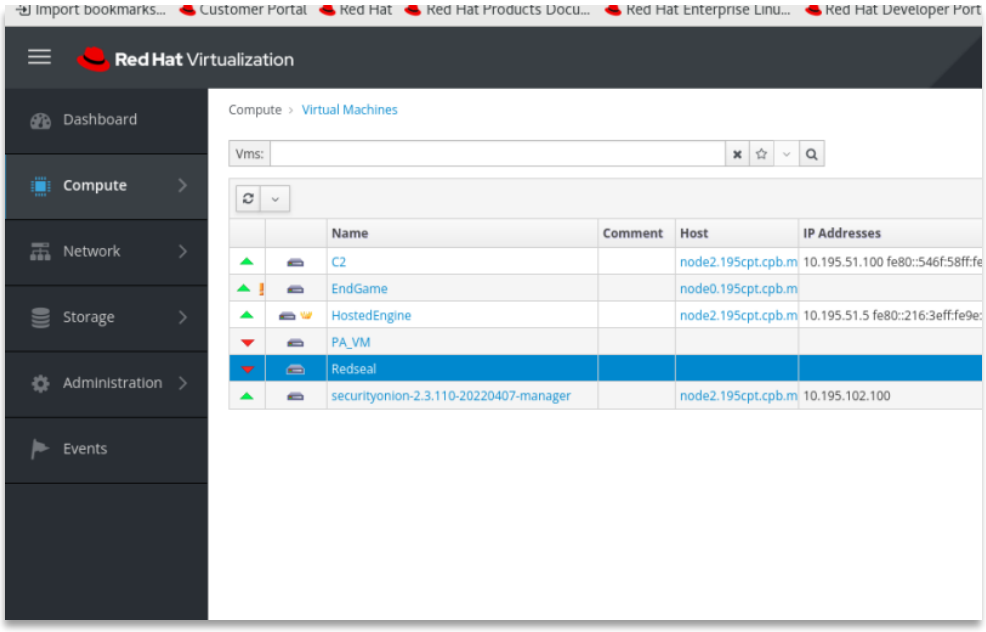


Figure 23.4(b): RedSeal Appliance build on Engine

5. Power off the VM, then click on the RedSeal VM and change the Virtual Disk Interface to **IDE**.

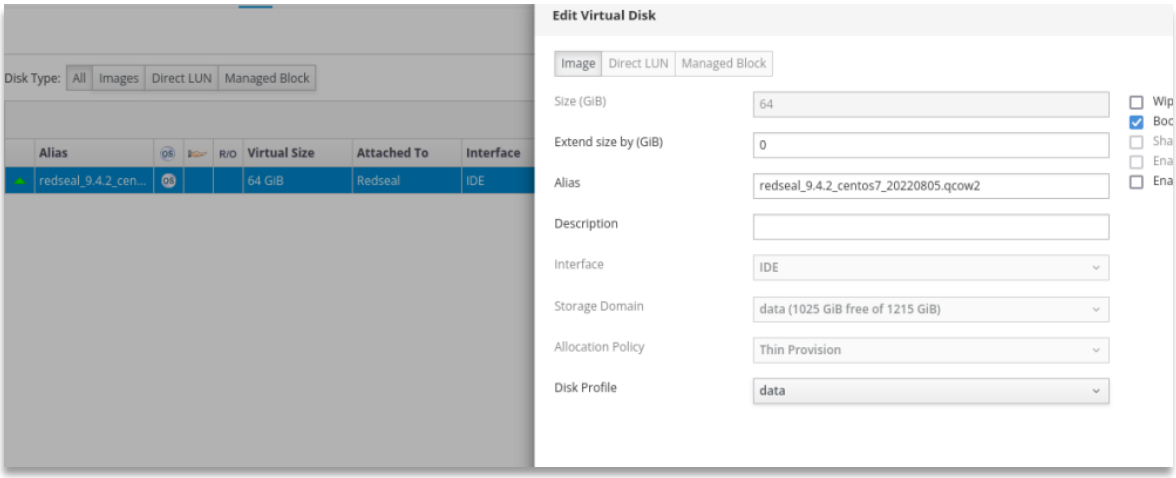


*Figure 23.4(c): RedSeal Virtual Disk Interface change to **IDE***

6. Power on the VM and access the console.

7. Type **set password cliadmin**

8. Type **set ip eth0 10. {{kit_num}}.51.105 255.255.255.0**

9. Type **set gateway eth0 10. {{kit_num}}.51.1**

10. Type **enable autostart ssh**

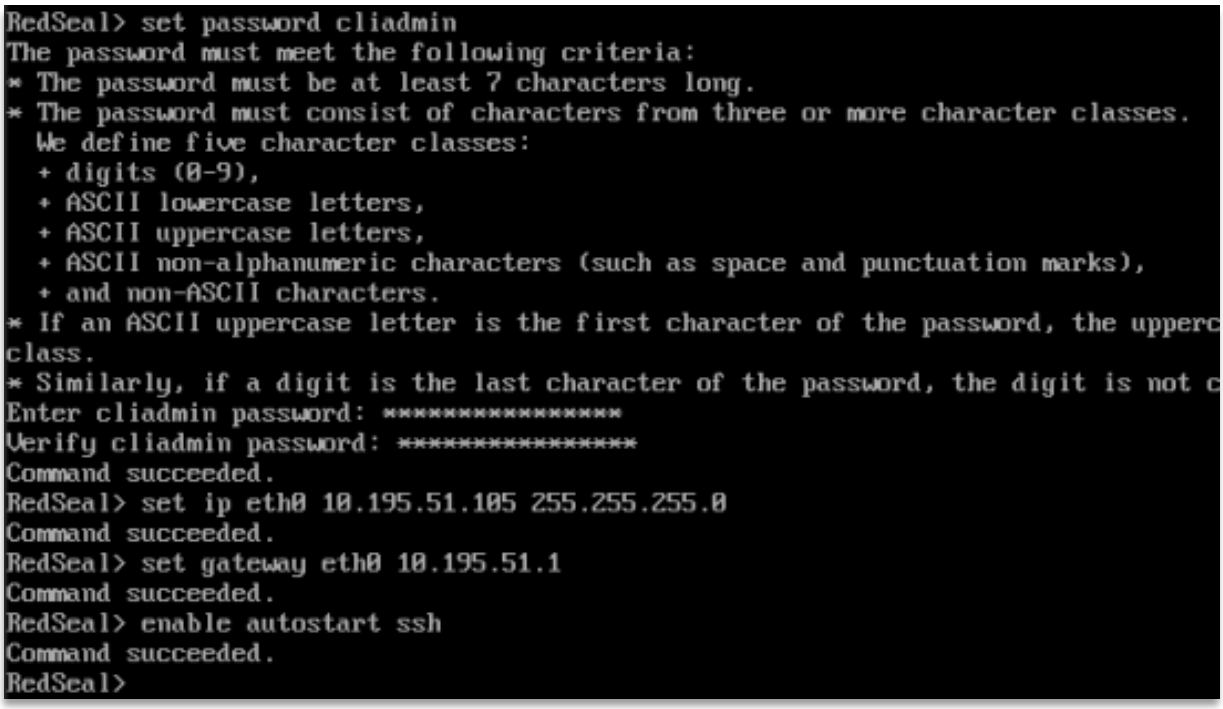


Figure 23.4(d): Setting Redseal cliadmin password and IP settings

11. SSH to the RedSeal VM IP

12. 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
Q0deDsPBXpAgc40XVdmv2iks0WvTQTiMwJ5pqGv4QYHBsKIqPzEcdwq/Zis4q5siKoR8qY7ldDht
```

Figure 23.4(e): Setting the Redseal license

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

14. Prese “Ctrl-D” once complete

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

```
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
```

Figure 23.4(f): Displaying the Redseal license

16. 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: ****************
```

Figure 23.4(g): Starting the Redseal server and setting data password

17. 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: ****************
```

Figure 23.4(h): Setting Redseal uiadmin password for Web UI

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

```
RedSeal> status all
admin                auto enabled    tcp 3835  running
server               auto enabled    tcp 3825  running
server-jms           auto enabled    tcp 3826  running
server-http          auto enabled    tcp 80    running
server-https         auto enabled    tcp 443   running
server-https-cert    auto disabled   tcp 10443 not running
db                   auto enabled    tcp 5432  running
ssh                  auto enabled    tcp 22    running
snmp                 auto disabled   udp 161   not running
RedSeal>
```

Figure 23.4(i): RedSeal server status

19. Use Firefox to access the RedSeal WebUI

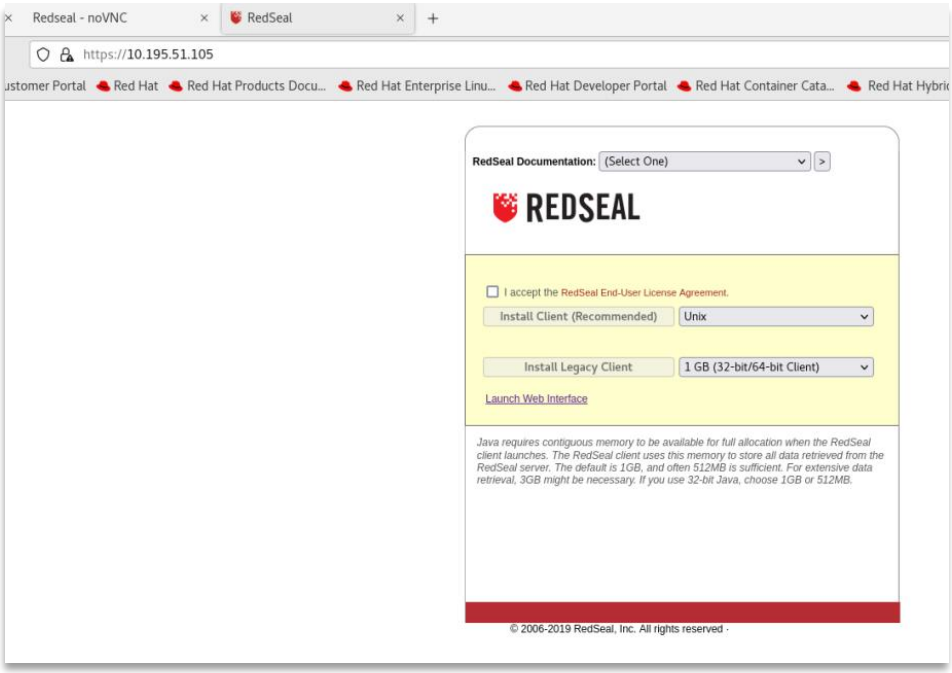


Figure 23.4(j): Accessing the Redseal Web UI and Launching Web Interface

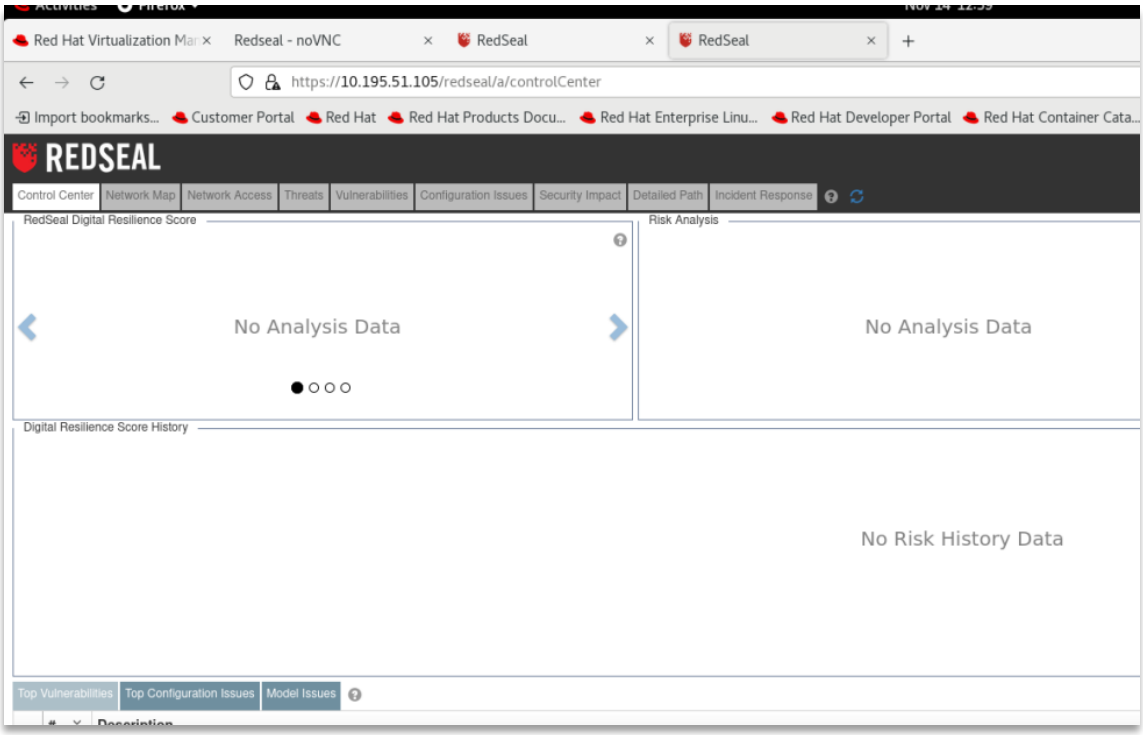


Figure 23.4(k): Redseal Web UI

23.5 Ghidra

The DOPE Ghidra tool is the same open-source software (OSS) project developed by the National Security Agency with the exception of being deployed and provided in a fully STIG'd RHEL 8.6 template. The Ghidra tool is installed in /usr/local/bin/Ghidra_9.2.4_PUBLIC. To deploy Ghidra, execute the following:

1. Type **cd /opt/deploy_tools/deploy_tools/**

2. Type **dope**

3. Select **Deploy Ghidra**

4. Once the playbook has successfully completed, validate the Ghidra VM exists on Engine

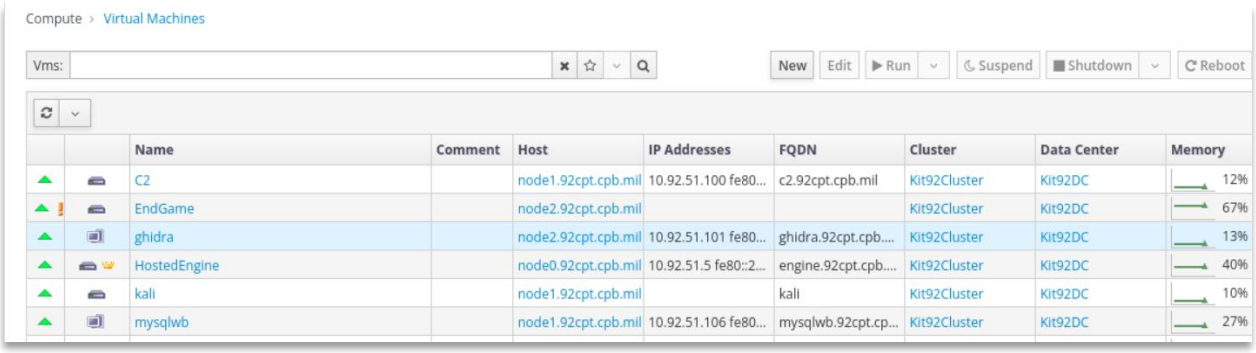


Figure 23.5(a): RedSeal Appliance build on Engine

5. Access the Ghidra VM from Engine

6. Open an elevated command prompt session

7. Type the command **ghidraRun** and Validate User Agreement

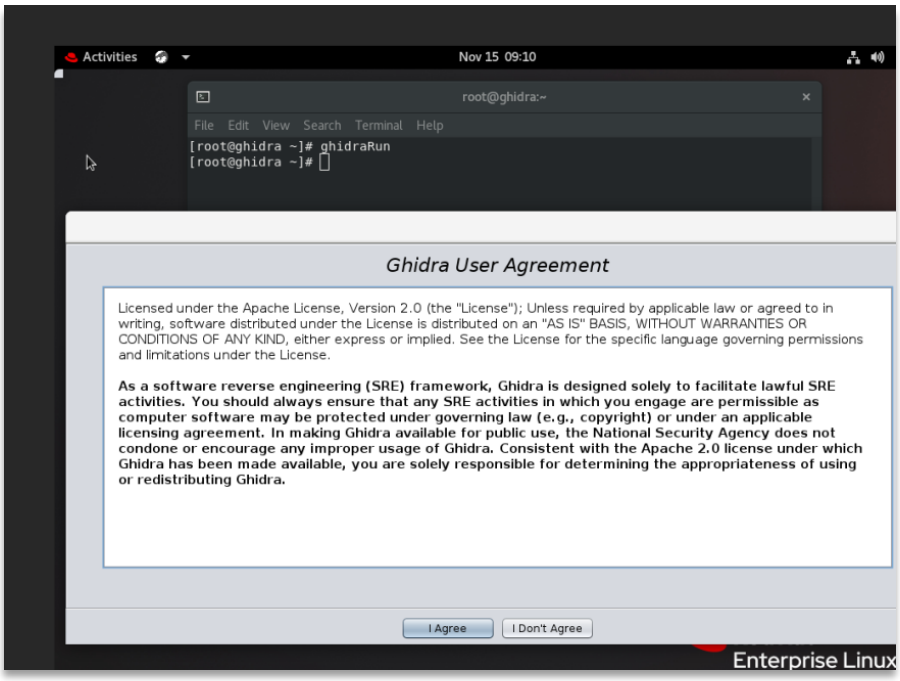


Figure 23.5(b): Ghidra User Agreement

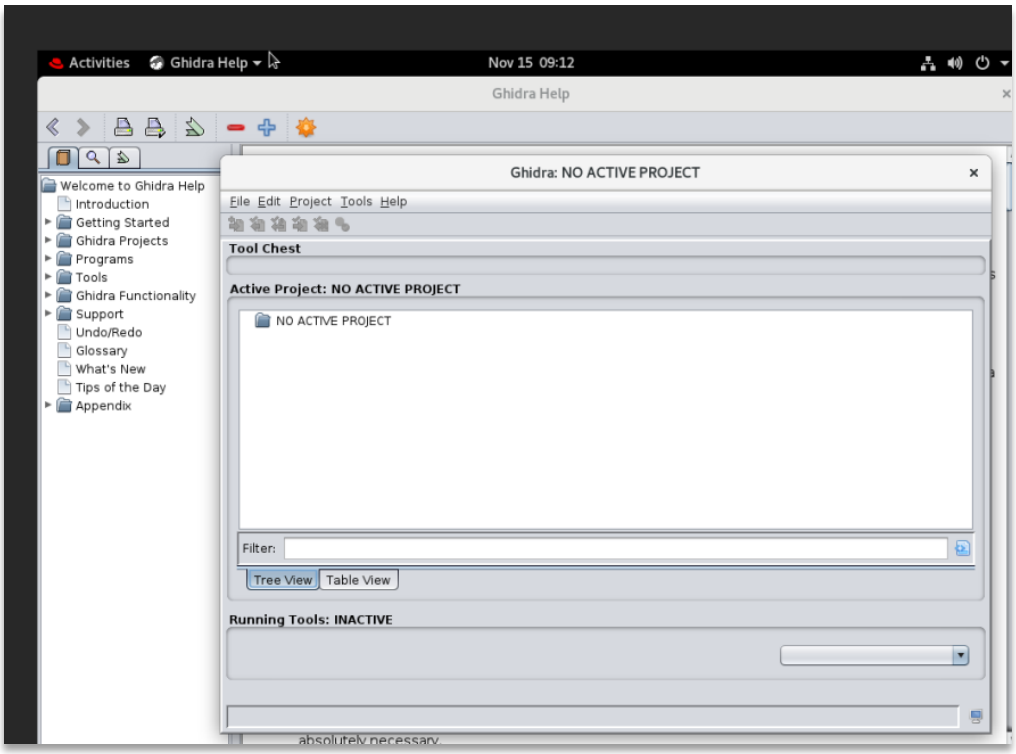


Figure 23.5(c): Ghidra Tool UI

23.6 Kali

The DOPE Kali tool is the same open-source software (OSS) project developed by Offensive Security. The deploy Kali DOPE playbook creates a VM from the Kali template, execute the following:

1. Type **cd /opt/deploy_tools/deploy_tools/**

2. Type **dope**

3. Select **Deploy Kali**

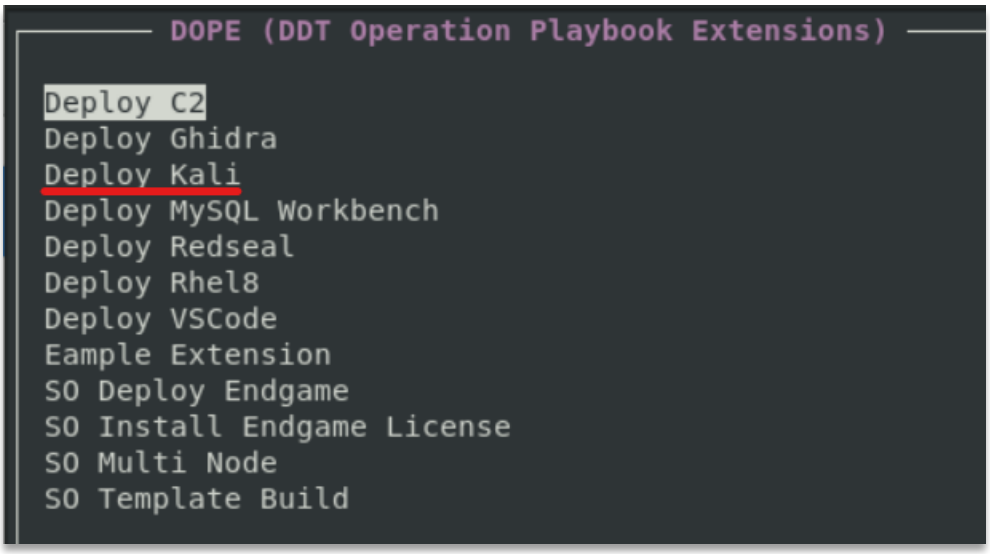


Figure 23.6(b): Kali Tool Deployment Playbook

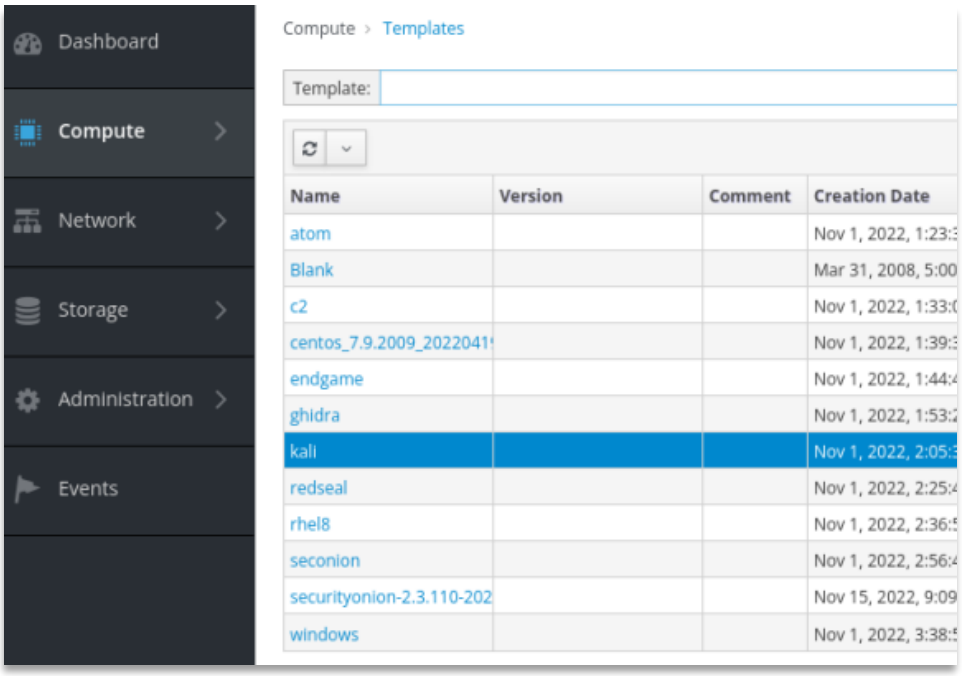


Figure 23.6(c): Kali Template

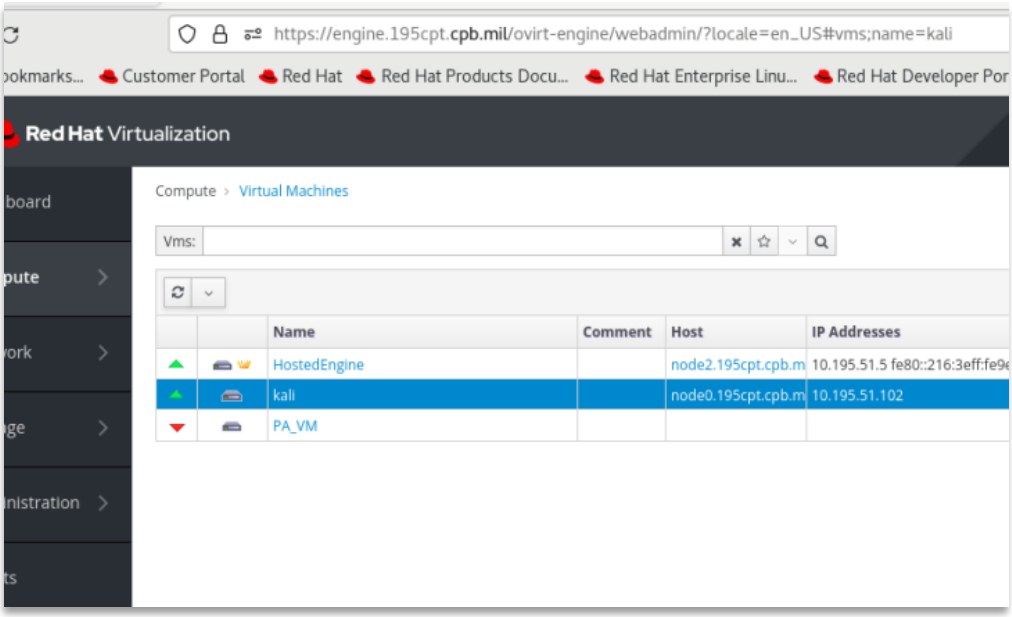


Figure 23.6(d): Kali Virtual Machine after Playbook deployment

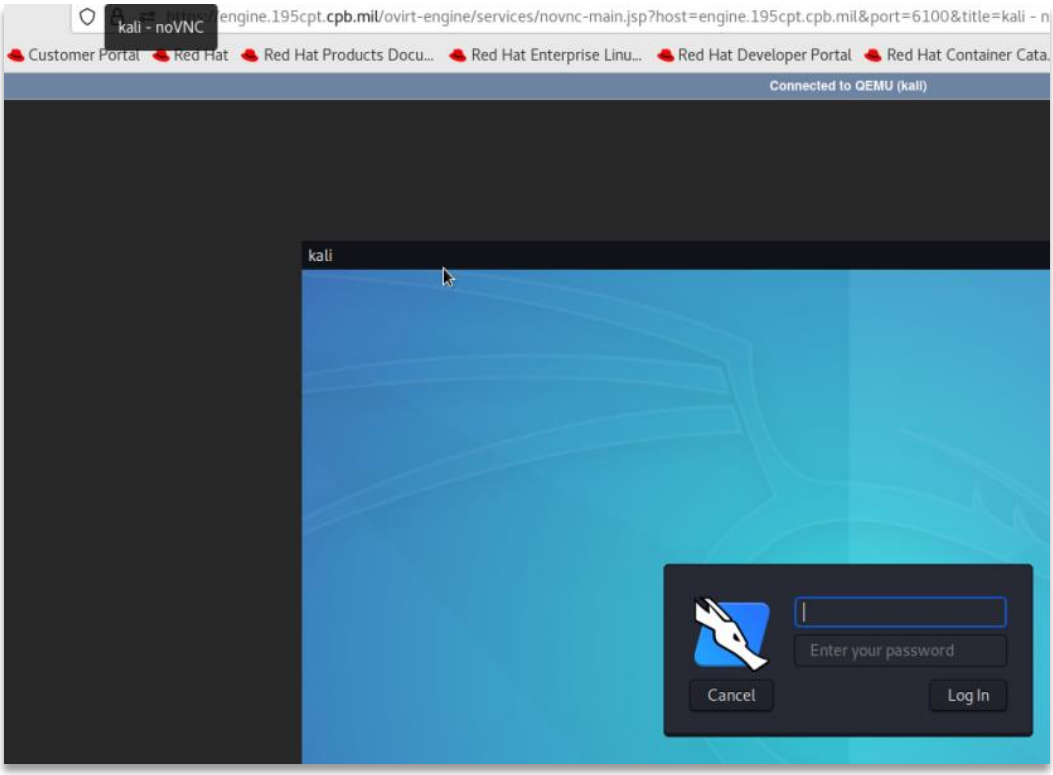


Figure 23.6(e): Kali console access

23.7 VSCODE

The deploy VSCode DOPE playbook creates a VM from the VSCode template, execute the following:

1. Type **cd /opt/deploy_tools/deploy_tools/**

2. Type **dope**

3. Select **Deploy VSCode**

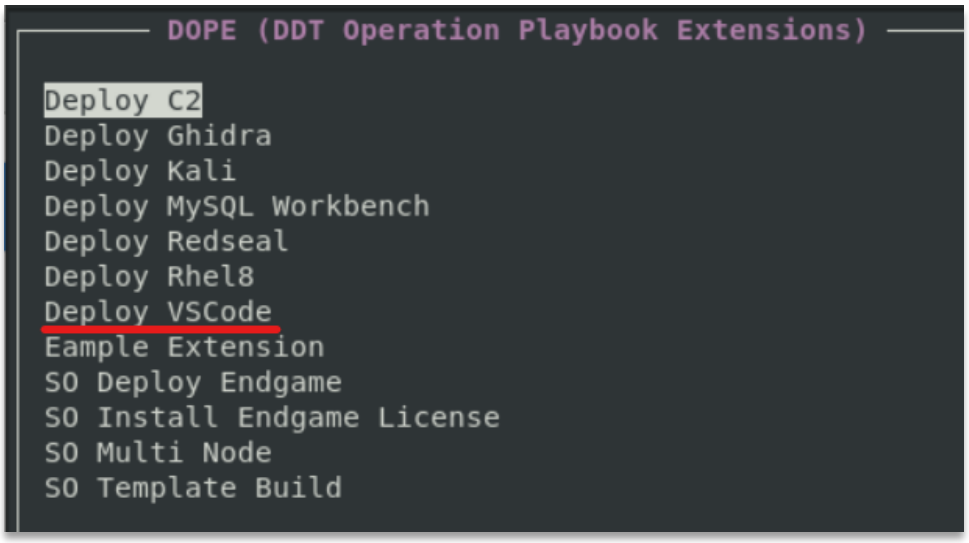


Figure 23.7: VSCode Deployment Playbook

23.8 Windows

The Windows VM will be a manual deployment from the template located on the kit Engine Templates.

To deploy VM, execute the following:

1. Select **new virtual machine**

2. Select the windows template.

3. Select **OK** to save

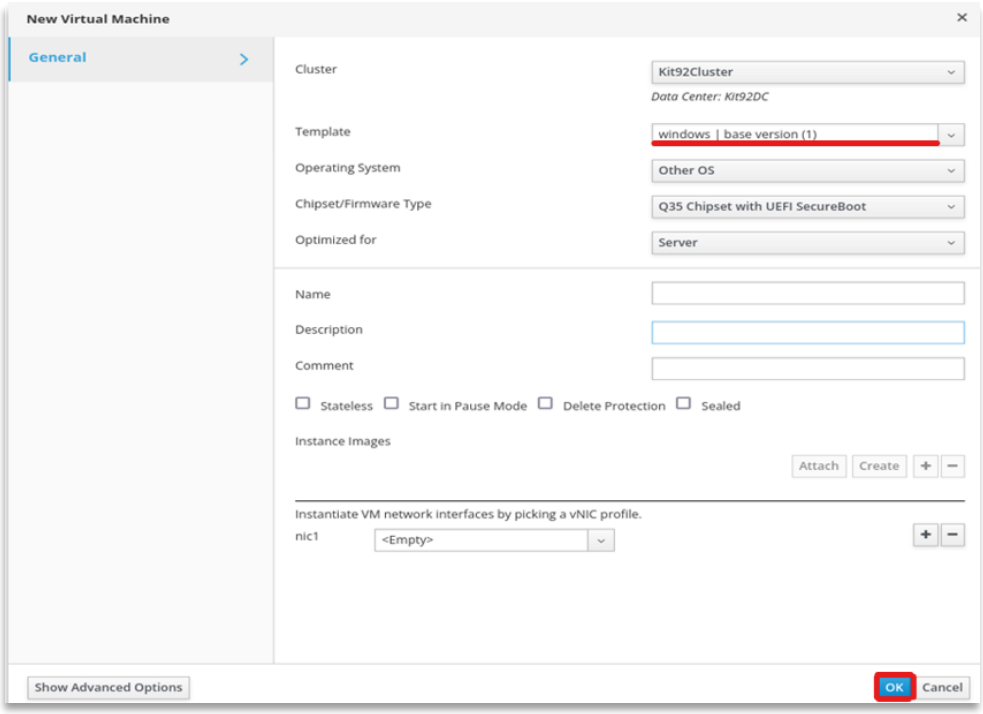


Figure 23.8(a): Windows VM Template setup

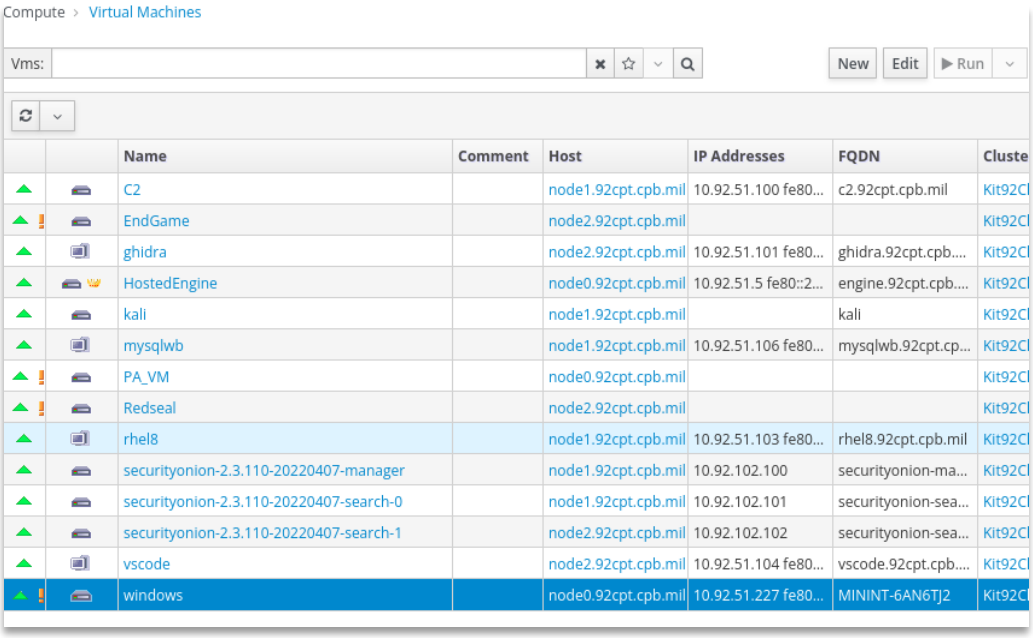


Figure 23.8(b): Windows VM running on the engine

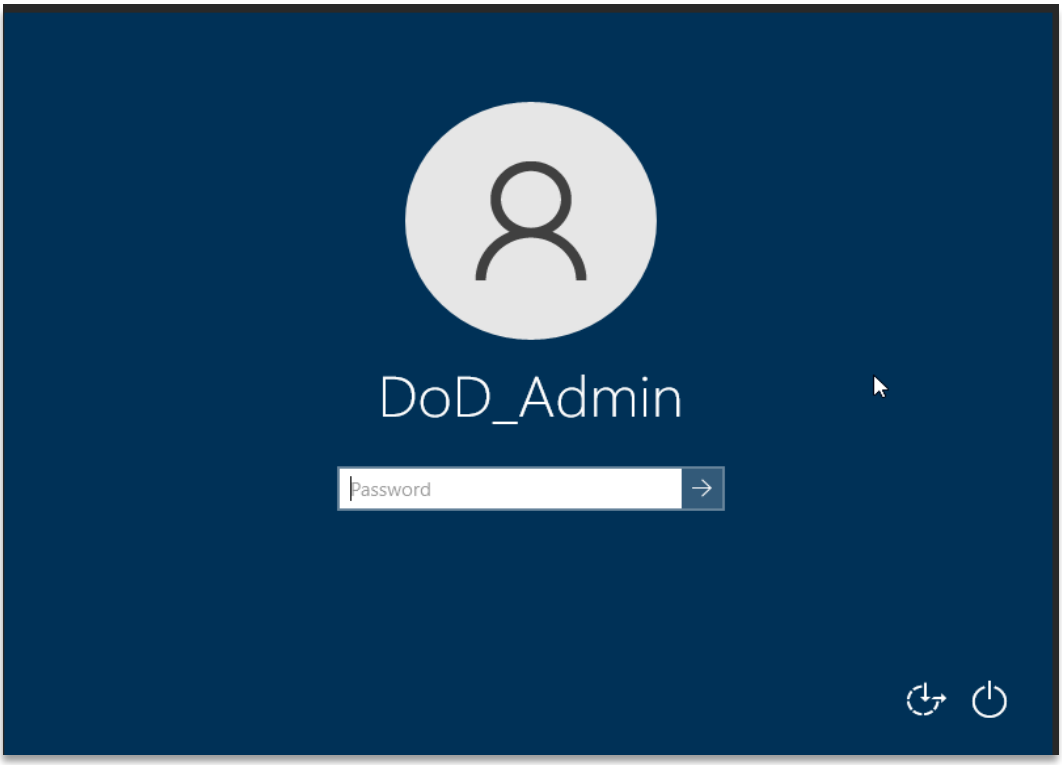


Figure 23.8(c): Windows login screen

24 Changing default DOPE passwords

As previously stated, DOPE deploys with a default password that needs to be changed by the end-user after deployment. Use the following methods to change passwords.

✎ **Note**: Instructions for changing RedSeal passwords is covered in section **23.4 RedSeal** of this manual.

For Endgame, Security Onion, Ghidra, Kali, and VSCode:

1. In the tool that you would like to change, type “passwd {user}”
2. Type in the new password you would like to use.

Example:

```
[defender@master ~]$ passwd defender
```

For the Windows VM:

1. Send a “Ctrl+Alt+Del” to the VM and select **Change a Password**
2. Enter the old password in the appropriate box.
3. Enter the new password in the “New password” and “Confirm password” boxes.