DDS-M Bible – IP

SGT Humphrey and Friends

2024

Table of Contents

1 Introduction

This is intended to be a living document, a collection of useful information relating to the DDS-M kit. This includes, but is not limited to, instructions to complete common tasks, advice on troubleshooting common problems, and general wisdom regarding the kits, accrued through experience, that may be helpful to junior and senior soldiers alike. As knowledge is accumulated, adding that knowledge to this document is encouraged, that it may serve as an enduring and evolving reference.

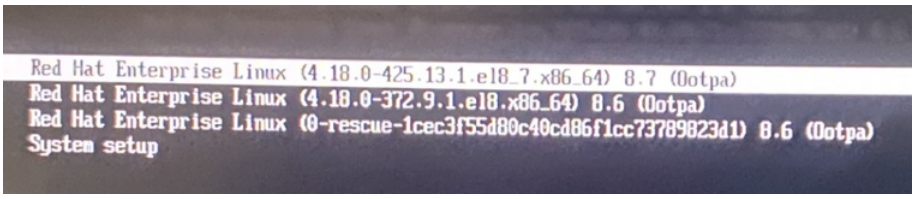
2 Updating the DDS-M Kit

2.1 Re-image Master Laptop

NOTE: The Master Laptop can be updated without being connected to the kit.

1. Plug the FML drive into the master laptop.
   1.1 If the drive has not already been checked, run a file system check against it (useful if there is a new FML drive received)
   1.2 **Command:** `fsck -y /dev/sd[a-z]#`
2. Power off the master laptop.
3. Power on the master laptop and enter BIOS by pressing F12
4. Search for "Thunderbolt Integrated Devices Enable" in the BIOS and enable it.
5. Return to boot menu and select the FML Drive to boot from **USB UEFI**.
6. Enter the kit number when prompted by the FML drive setup.
7. During the installation process accept the risks: **I ACCEPT THE RISKS AND UNDERSTAND THINGS MAY NOT WORK**
8. **URGERNT:** Once update is complete, press **ENTER** to finish the process. Failure to do so will result in the FML drive not being properly mounted and you will have restart the process.

   NOTE: When you re-image the Master Laptop, the **passwords.yml** file will also change.
9. Verifying that that the FML was properly installed.
   9.1 Restart Master Laptop.
   9.2 If install was successful, you will see an additional Red Hat OS present during boot.



9.3 Verify that the FML version matches the system via command line.

9.3.1 **Command:** `$ rpm {qa | grep ddt` (version # should match FML version)

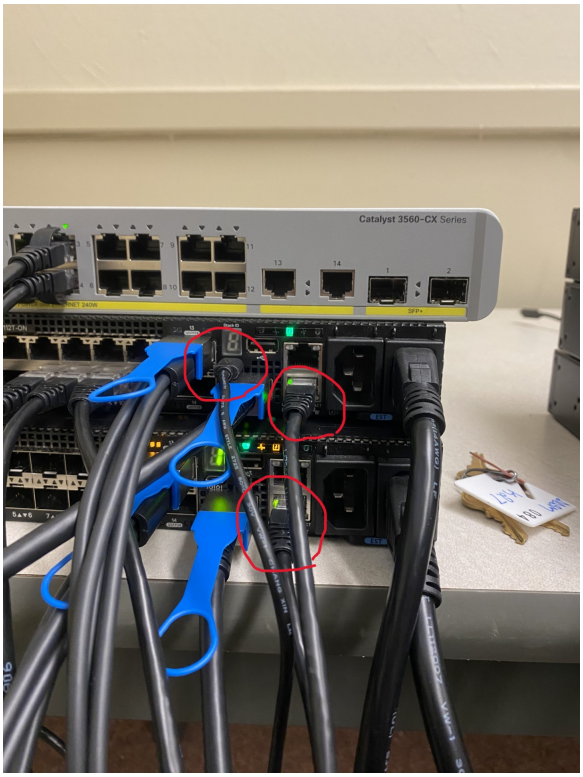
2.2 Perform ONIE Installation on T and F Switches (SW)

1. Reconnect up the Master Laptop to the rest of the 3-node setup ensuring proper cabling.

2. Properly connect to each SW following the steps below:

   2.1 **Direct Ethernet Connection** from Master Laptop to the **MGMT port** of the SW

   2.2 Direct **USB connection** from Master Laptop to **micro-USB** on the SW



3. minicom into SW

   3.1 **Command:** `sudo minicom dell0`

   NOTE: if minicom profiles are not created, see DDS-M Manual pg. 180-182

   NOTE: if minicom is still unable to be accessed, switch to RJ45 USB cable and plug into management port of T or F-SW.

4. Identify which SW you have access to by the Host identifier in the terminal by pressing ***Enter*** and looking at hostname (**S4...T or F**).

5. Unplug the power cable from that switch.

6. Plug the power cable back into that switch.

7. Press the ↑ and ↓ to interrupt the SW boot sequence.

8. Select **ONIE**

9. Select **Install ONIE OS**

   NOTE: Installation will take ∼45 mins.

   NOTE: When SW is updated, fan volume should reduce in noise and connectivity lights on the SW will turn on.

10. Repeat steps 2-8 on the remaining SW.

2.3 Node Provision/Node Discovery

NOTE: should take ∼3 hours and 45 minutes to complete.

1. If not setup already, complete a 3-node set up of the DDS-M.

2. Start an elevated tmux session.

   2.1 **Command:** `sudo tmux`

3. Navigate to **ansible_main**

   3.1 **Command:** `cd /opt/ddt/ansible/ansible_main`

4. Run play.py and designate the number of nodes in the setup.

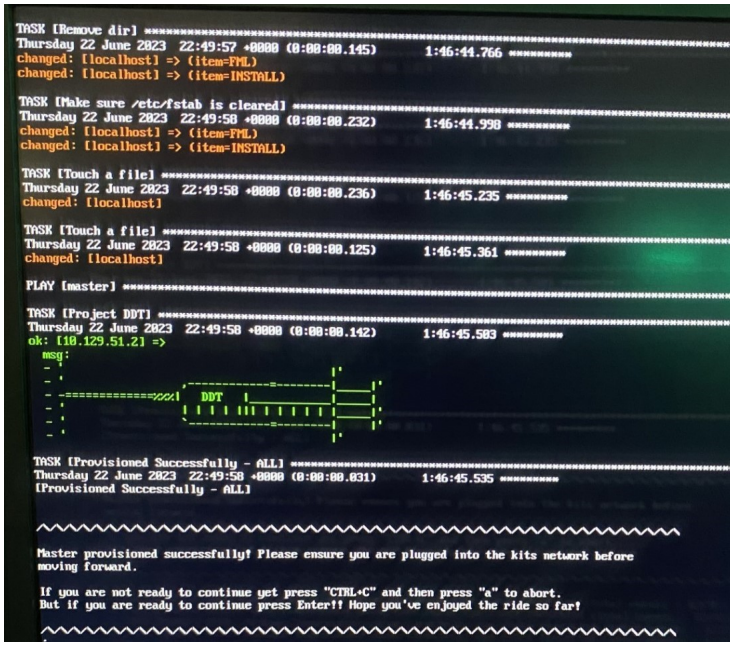
   4.1 **Command:** `./play.py -n #`

   4.2 **Alternate Command:** `./play.py -pe` (runs play.py and defaults to 3 nodes)

5. Use space to select playbooks 0 and 07-99.

6. Press **c** to continue and wait for host provisioning to finish.

   NOTE: when provisioning process is complete you will see the image below. If the process fails, please refer to Troubleshooting (include hyperlink to troubleshooting section)



7. Proceed through normal power up procedures.

2.4 Updating Node Firmware

1. **Reformat USB from NTFS to FAT32:**
2. **Prepare Laptop to use USB:**
3. **Access IPMI Super Micro Web Access on Nodes:**
4. **Firmware Maintenance:**
5. **Firmware Update:**
6. **Verify Firmware Update:**
   - 6.1 Access IPMI (`http:/10.<kit#>.53.200-1,2,3,4,5...`
   - 6.2 Navigate to Maintenance >Maintenance>Event Log
   - 6.3 Sort by time (gray time stamp) OR search “firmware and IPMI firmware was updated successfully”

6.4 Verify time frame matches the update time (e.g., if updated stated at 5 PM, the log should state the updated completed at 5:30 PM)

6.5 Look for event log name "IPMI firmware was updated successfully"

7. Change `usb-storage.old` and `blacklist.old` back to orginal file names:

7.1 **Command:** `$ mv usb-storage.old usb-storage.conf`

7.2 **Command:** `$ mv blacklist.old blacklist.conf`

3 Activating DOPE

1. Enable repo on master laptop (run as root).

1.1 **Command:** `$ subscription-manager list --all --available`
NOTE: will output a list of all the available subscriptions for the master laptop.

1.2 **Alternate Command:** `$ subscription-manager list --available pool | grep`

1.3 **Command:** `$ subscription-manager attach --pool <pool id of packages>`

2. Install DOPE and Security Onion rpms.

2.1 **Command:** `$ dnf install -y dope`

2.2 **Command:** `$ dnf install -y dope-securityonion-ansible`

2.3 **Command:** `$ dnf install -y dope-deploy_tools`

2.4 **Command:** `$ dnf install -y ddt-cde`

2.5 **Command:** `$ dnf install -y short-circuit`
NOTE: If you cannot locate the dnf modules you are trying to install, ensure you have attached all pools available in subscription-manager and that the name of the module is correct.

2.6 Use the following command to list and search for modules:
Command: `$ dnf list | grep <name of module>`

3. Run DOPE and Short-Circuit to ensure install.
    3.1 **Command:** `$ dope`
    3.2 **Command:** `$ sudo sccli`
4. Install rpm for DOPE and Short-Circuit
    4.1 **Command:** `$ dnf install -y ddt-cde short-circuit`
5. Run DOPE from `/opt/securityonion-automation/securityonion`
    5.1 **Command:** `$ cd /opt/securityonion-automation/securityonion`
    5.2 **Command:** `$ dope`
6. Proceed to Security Onion deployment.

4 Security Onion Deployment

4.1 Security Onion Manager and Search Nodes via DOPE

NOTE: the current setup is specifically for a 3-node setup.

1. Change directories into `security_onion` if not already there:
    1.1 **Command:** `$ cd opt/securityonion_automation/security_onion`
2. Ensure DOPE is installed.
    2.1 **Command:** `$ dope`
3. Determine if licenses for plays are in use and still valid.
    3.1 **Command:** `$ sudo subscription-manager list --consumed`
4. Using ***space*** select the following plays to run **in order**:
    4.1 `$ SO deploy Endgame`

4.2 `$ SO install Endgame License`

4.3 `$ SO Template Build`

4.4 `$ SO Multi Node` (press ***Enter*** for all prompts)

5. Let the playbooks run.

6. Verify that Security Onion installation is complete:

   6.1 Navigate to – `https://10.<kit#>.102.100`

   6.2 Navigate to Engine to verify the following VMs:

   - `Endgame`
   - `Security Onion Manager`
   - `Security Onion Search Node 0`
   - `Security Onion Search Node 1`

4.2 Setting up a Security Onion Search Node via DOPE

1. Ensure both DOPE and COPE are installed.

   NOTE: If properly installed, DOPE will run successfully and COPE will be listed as an option (will be near the top of the list).

2. Navigate to `opt/securityonion_automation/security_onion`

   2.1 **Command:** `$ cd opt/securityonion_automation/security_onion`

   2.2 **Command:** `$ dope`

3. Using ***space***, select the following:

   - `COPE`
   - `Deployment Automation`
   - `Enable PXE of SO`

   This will automatically set up a PXE boot server with a security onion iso, on 10.**<kit#>**.51.12

4. Set up a designated bare-metal node with IPMI and breakout cables.

   NOTE: If you have a 3-node setup, use the remaining breakout cables to connect the additional node.

5. Externally label the designated forward node chosen.

6. Access the designated Security Onion search node via IPMI:

   - Navigate to `http://10.<kit#>.53.200-205` (`ADMIN::ADMIN`)

7. Use the UID control to verify that you are connected to the correct node.

   - Navigate to: `Miscellaneous/UID/Turn On`

8. Restart the node and enter the PXE boot menu by pressing **F12** on laptop or remote console keyboard during boot process at the white splash screen.

9. Select the ***Wipe MBR*** option.

10. Restart the node and return to the PXE boot menu (**F12**) and select option containing **Security Onion**.

4.3 Configuration of Designated Security Onion Forward Node

NOTE: Most of the options should be configured correctly by default. **Be sure to install on nvme0n1**. As the installation runs move on to the next step.

1. When prompted with same device for NSM storage select **yes**

2. As Security Onion is installed on the node, **designate an empty port on the T-SW to give access to VLAN 102**

3. Close out of all minicom sessions, connect to T-SW via console cable, and run the following commands to configure:

   3.1 **Command:** `$ sudo minicom dell0`

3.2 **Command:** `$ show vlan`

3.3 **Command:** `$ config`

3.4 **Command:** `$ interface ethernet 1/1/<physical port # not in use>`

3.5 **Command:** `$ switchport access vlan 102`

3.6 **Command:** `$ exit`

3.7 **Command:** `$ show running-configuration`

3.8 **Command:** `$ show VLAN`

4. Setting up the **Ingest Interface**

   4.1 Secure an Ethernet cable.

   4.2 Place one end into the configured VLAN 102 port on T-SW.

   4.3 Place the other end into the designated forward node and connect to **eno5** (10 gpbs).
   NOTE: eno1,2,3, and 4 may also be set as Ingest Interfaces, but have a lowest throughput (1 gbps).

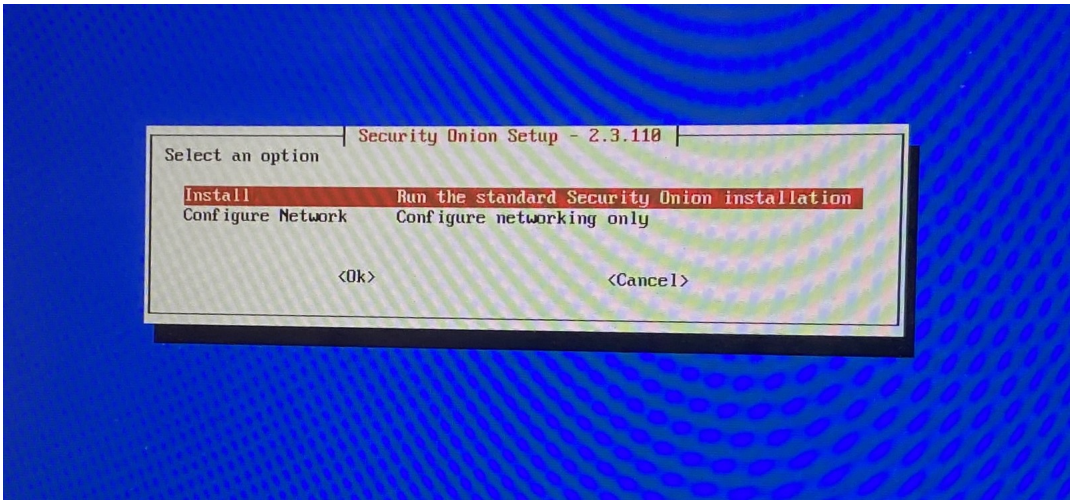
   4.4 Remove the breakout cables.

5. Restart sensor from IPMI and enter boot menu (**F11**).

6. Select(**TS2TMTE...**) as boot option.

7. Once it boots, log in with default credentials set during install **(defender::1,2)**

8. Once logged in, Security Onion will automatically start the set-up process and you will see the following if successful:



NOTE: Security Onion installation is NOT forgiving, be careful during the setup process.

Rebooting the node resets the configuration, to reboot Security Onion installation perform the following from command line:

8.1 **Command:** `$ sudo bash so-setup iso`

9. Use the following to navigate through Security Onion:
   - ***enter*** = select and proceed to the next option
   - ***spacebar*** = select option (*)
   - ***arrow keys*** = move up and down list of options
   - ***tab*** = shortcut to **<Ok>** and <**Cancel**> options
10. Configure the sensor with the following options:
    10.1 Yes
    10.2 Install
    10.3 Distributed
    10.4 Existing
    10.5 Sensor
        10.5.1 Name – `seconionsensor-node#`

10.5.2 Description – `dedicated T-SW <port#> statically assigned to VLAN 102`

10.6 Setting up **MGMT/Monitor Interface**

10.6.1 Select **eno5** (port on sensor that is connected via Ethernet to port assigned to VLAN 102 on T-SW).
NOTE: there will be a **"link up"** indicating that an Ethernet connection between the node and T-SW has been established.

10.7 **Static IP** = `10.<kit#>.102.103,4,5.../24`
NOTE: For each forward node deployed after, **add 1 to .103**

10.8 **Enter Gateway** = `10.<kit#>.102.1`

10.9 **DNS Server (IDM IP)** = `10.<kit#>.51.10`

10.10 **Search Domain** = `defender@<kit#>cpt.cpb.mil`
NOTE: Username for Security Onion website (http://10.**<kit#>**.101.100)

10.11 **OK**

10.12 **Manager Name** = `securityonion-manager`

10.13 **Security Onion Manager IP** = `10.<kit#>.102.100`

10.14 **OK**

10.15 **OK**

10.16 **Yes**

10.17 Select `Proxy + Manager OR Direct + Manager`

11. Verify Access to Security Onion Manager + Sensor:

- Enter Security Onion Manager
  - **Command:** `$ ssh defender@10.<kit#>.102.100`
- Access Search/Sensor Node from Security Onion Manager
  - **Command:** `$ ssh defender@10.<kit#>.102.101,2,3...`

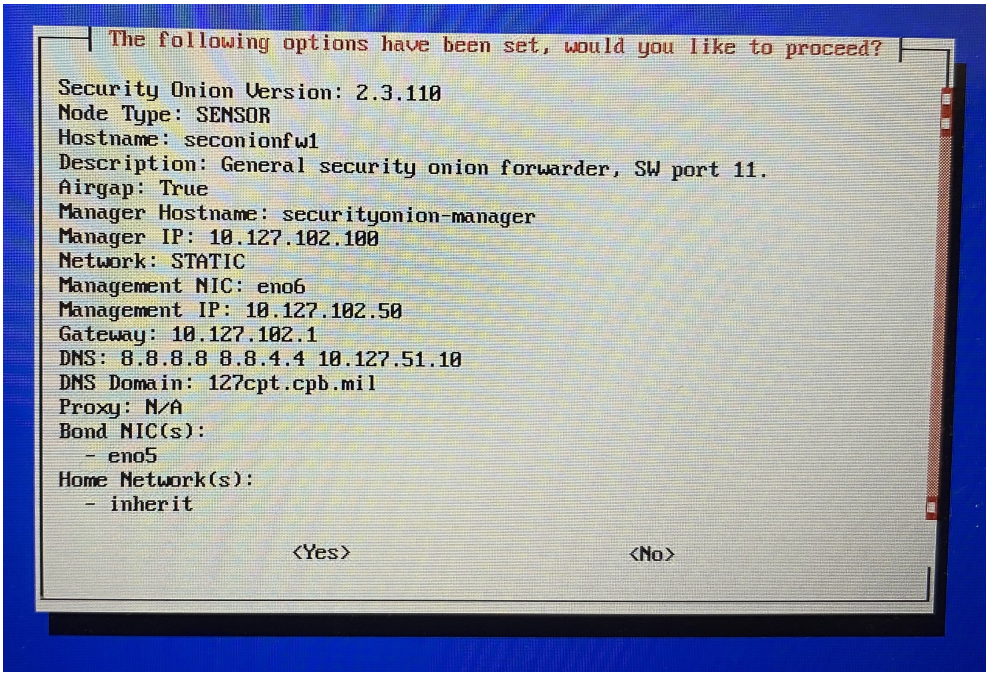
12. IPMI Access to Designated Security Onion Forward Node:

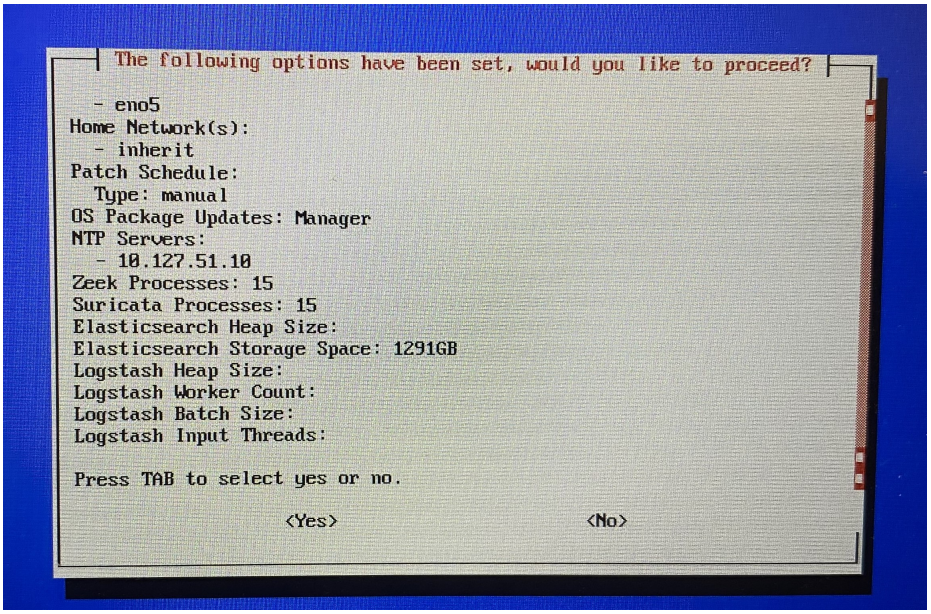
- Navigate to `http://10.<kit#>.53.203,4,5...`

13. Select MGMT/Monitor Interface

13.1 Select **eno6** or port not selected from earlier

14. **Yes**
15. **Basic**
16. **Yes to all process defaults**
17. **Yes to all process defaults**
18. **NTP**
19. **NTP IDM IP** = `10.<kit#>.51.10`
20. **Confirm options** (see below for example configuration)





21. While the Security Onion sensor configures, login to the Palo Alto firewall and create a rule to **allow all bidirectional traffic between the sensor and the manager**.

22. After configuration is complete, change boot option to default from the previous Security Onion instance

    22.1 **Restart**

    22.2 **Enter boot sequence (Tab or F11)**

    22.3 **Select HDD DDS**

    22.4 **Set Boot Option #1**

    22.5 Select **TS2TMTE...**

23. Verification of Log Collection:

    23.1 Plug Ethernet into the **Monitor/MGMT Interface** of the designated Security Onion Sensor **eno6**

    23.2 From terminal access the designated Security Onion Sensor:

        23.2.1 **Command:** `$ ssh defender@10.<kit#>.102.103,4,5...`

        23.2.2 **Command:** `$ sudo tcpdump -i eno# -vv`

23.3 Plug the other end of the Ethernet into another laptop and run the following from terminal:

23.3.1 **Command:** `$ sudo nmap -n -v -Pn -T5 10.<kit#>.102.103,4,5...`

NOTE: if interface configuration is successful, you will receive packets the terminal window of the designated Security Onion Sensor.

5 General Troubleshooting

5.1 Troubleshooting Network Connections

1. Go to the firewall and enable the **Debug Allow All**.
2. If the issue is fixed, the issue is with the firewall and can probably be resolved with a new firewall rule.
3. If the issue persists then it is something else.

5.2 Cannot Login to a Node

1. Ask yourself the following:
   1.1 Do I need to login to do what I need to do?
   1.2 Did the node boot properly?

5.3 Sensor Not Receiving Traffic

1. Run **tcpdump** on the monitor interface to verify.
   1.1 **Command: $ tcpdump -i eno#**

5.4 Analyst Laptop Not Connecting

1. Is everything plugged in?
2. Is wired connection turned on?
3. Does the wired connection have an IP in the correct range?
4. Do the correct routes exist on the laptop?

5.5 Network Connection Issues

- Essential commands:
  - **ping**: test device reach-ability.
  - **traceroute/tracert**: used to display possible transit delays and paths of packets.
  - **nslookup**: resolves domain name to an IP, useful for checking if DNS is working and if the domain is properly assigned to the correct IP.

1. Ping the following in order:
   1.1 Your IP.
   1.2 Gateway.
   1.3 Device that you want to reach.

5.6 Accessing IPMI via Node IP Address

1. IP Range for Nodes = `10.<kit#>.53.200,1,2,3...`
2. Determine node IP address using nmap or ping sweep
   2.1 **Command:** `$ nmap 10.<kit#>`.53.0/24
   2.2 **Command:** `$ for i in ##..##; do ping -c 2 10.<kit#>.53.$i | grep 'bytes`

5.7 Security Onion Sensor Unable to Communicate with Manager

1. Minicom into the T-SW and ensure that the physical port configured for VLAN 102 has maintained its configuration.
   1.1 **Command: $ minicom dell0**
   1.2 **Command: show vlan**
2. If the physical port is not listed in 102 VLAN re-configure:
   2.1 **Command: $ config**

2.2 **Command: $ interface ethernet <port#>**

2.3 **Command: $ show**

2.4 **Command: $ switchport access vlan 102**

2.5 **Command: $ show**

2.6 **Command: $ exit**

2.7 **Command: $ exit**

2.8 **Command: $ show vlan**

5.8 Unable to Ping Windows Analyst Laptops

1. Check Windows built-in host firewall within Security Settings.
2. Add a new rule to allow traffic coming from DDS-M kit.

5.9 Unable to Reach VMs From Analyst Laptops

1. Add the proper 509 digital certificate to your browser to trust the kit's domain.
2. Create the certificate on the Master Laptop.

   2.1 **Command: $ trust list**

   2.2 **Command: $ trust extract −−filter=certificates −−format=x509-directory −−purpose=client-auth CERT**

   2.3 **Command: $ cd CERT**

   2.4 **Command: $ ls**

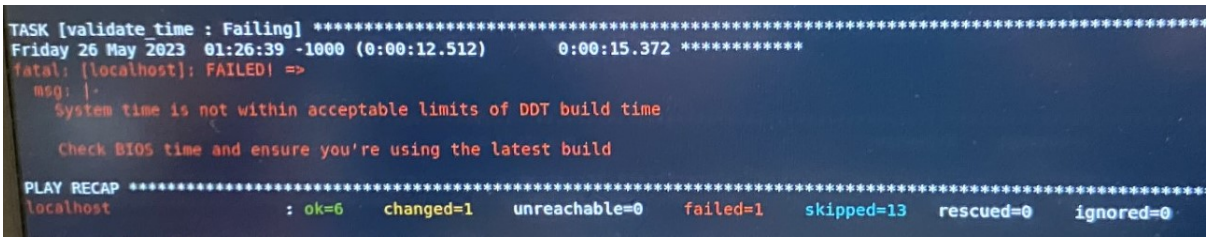
3. Secure copy created certificate to analyst laptop.

   3.1 **Command: $ scp [file_name] defender@10.<kit#>.53.XX:/foo/bar/**

   3.2 Sign in to Engine and attempt to console into VM.

5.10 Out of Sync FML Build Time

NOTE: Below is a DDT Build Time Error



ESSENTIALLY: the time frame that the developers allotted for the installation of the prescribed update has passed and needs to be extended.

1. Identify the location of the failed task. (e.g., System time is not within acceptable limits...)
2. Navigate to role associated with the error and edit the .yml file:
   2.1 **Command:** `$ sudo nano -l opt/ddt/ansible_main/roles/ validate_time/tasks`
3. Extend the Epoch time range by adding 0s to the end of the value.
4. Comment the changes made to the file and save.
5. Re-run `play.py` from the tmux session to avoid erasing changes made to the `main.yml` file.

5.11 Log Drive Full Error on Laptop - Temporary Solution

1. Locate and remove the large log file generated:
   1.1 **Command: $ cd var/log/**
   1.2 **Command: $ sudo du -sch var/log/* | sort -h**
   1.3 **Command: $ sudo rm <specific log file>**

2. Restart laptop to empty drives.

3. Configure log rotate configuration file.

   3.1 **Command: $ cd etc/logrotate.conf/**

5.12 Device Error - Cannot Find /dev/usb/

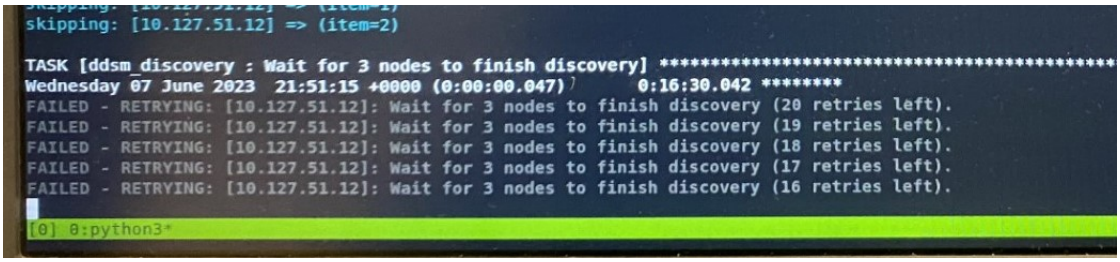
1. Enable a specific device via **usbguard** running as root.

   1.1 **Command: # usbguard list-devices**

2. Find device number you want connected "**#: block-id**" and allow the specific device:

   2.1 **Command: # usbguard allow-device <device #>**

5.13 DDSM Discovery Error



   2.1 Identify Foreman Discovery has failed via IPMI remote console
   NOTE: Foreman Discovery = Gray screen with **"SUCCESS"** seen inside all consoles except for the troubled node.

   2.2 Reset troubled node using Integrated Platform Management Interface (IPMI) by navigating to

      2.2.1 Navigate to **Remote Control/Remote Console/Power Control**

      2.2.2 Power off and then on

      2.2.3 Enter BIOS **(delete/F12)**

2.3 Reset the BIOS settings using pg. 246-247 going in order from top bottom

2.4 **SKIP** Advance/Advanced Power Management Configuration... to Advance/Advanced Power Management Configuration...

2.5 **CONTINUE** with Advanced/PCIe/PCI/PnP Configuration

2.6 Navigate to Satellite and IDM and delete instance of nodes from Foreman discovery.

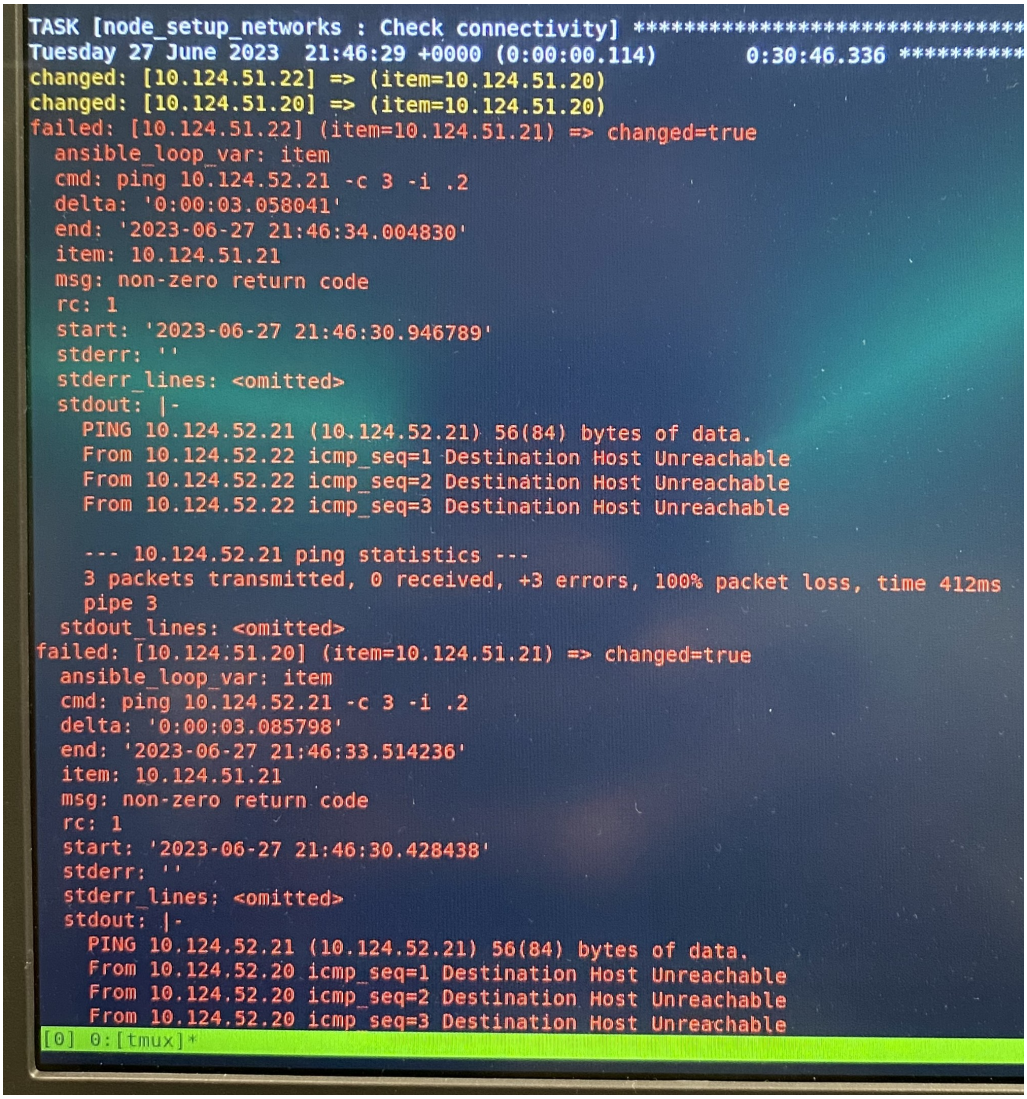
2.6.1 **Satellite/Discovered Hosts/*delete node instances***

2.6.2 **IDM/Hosts/*delete node instances***

2.7 Restart DDS-M following as many power down/up procedures as possible.

2.8 Repeat section **2.3 Provision Nodes (*insert hyperlink here*)**

5.14 ICMP Node Discovery Issue



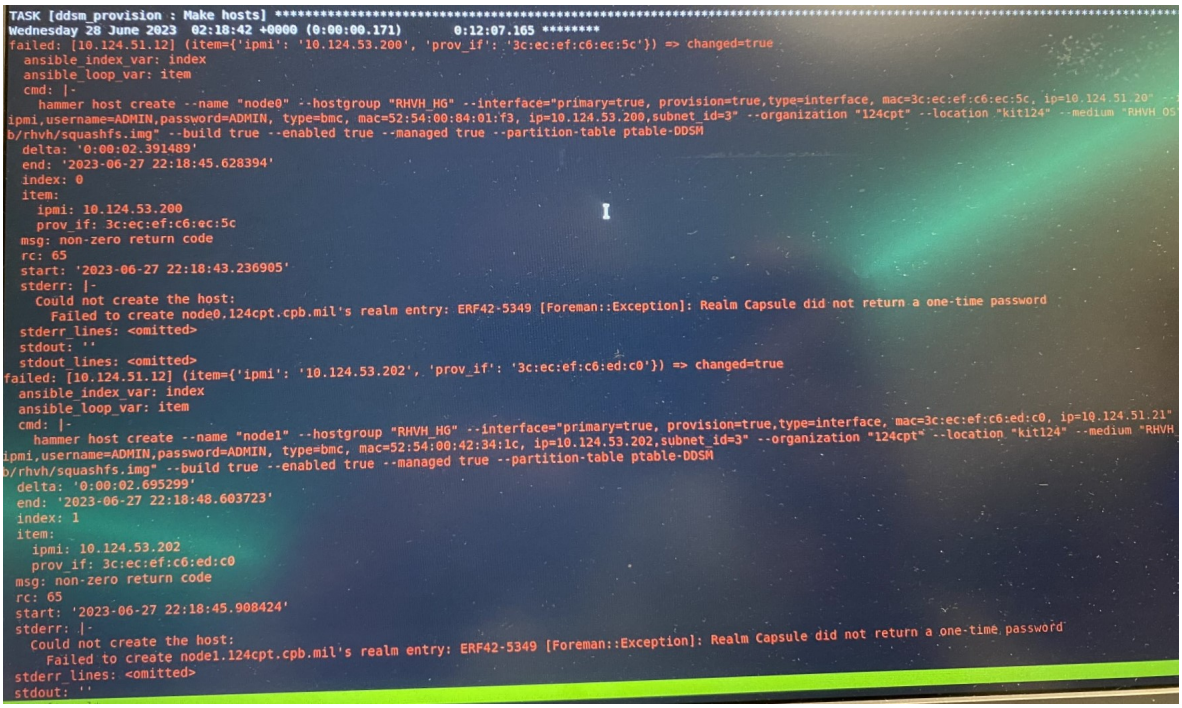
2.1 Confirm that breakout cables are properly connected.

NOTE: Triangle lights indicating connectivity for breakout cables should **all be on**, if not mark and replace cable!

2.2 Replace broken breakout cable and reconnect to node.

5.15 Failure to Create Node

ERROR: Failed to create node...realm entry: ERF42-5349[Foreman::Exception]



2.1 Enter Identity Manager (IDM) and delete nodes.

2.1.1 **Hosts/Discovered Hosts/*delete anything present***

5.16 SSH Key Generation Error

NOTE: error occurs due to the Ansible playbook being unable to locate the credential "onedowntwodown" within the password.yml file for SSH Key Generation.

1. From within the tmux session, edit the password.yml file

   1.1 **Command:** `$ sudo nano -l /opt/ddt/ansible_main/password.yml`

2. Add the following credential:

2.1 **onedowntwodown : 1qaz2wsx!QAZ@WSX**

3. Save and exit your nano file.

5.17 COPE Not Present When Running DOPE

1. Compare **installed dnf list** against **available dnf list** to determine missing package:

   1.1 **Command:** `$ dnf list --installed grep | <kit#>cpt`

   1.2 **Command:** `$ dnf list grep | <kit#>cpt`

2. Run following from `/opt/ddt/securityonion_automation/securityonion`:

   2.1 **Command:** `$ dnf install -y ddt-cde --download only --destdir .`

   2.2 **Command:** `$ rpm -ivh --nodigest --nofiledigest ddt-cde*`

5.18 Locked Out of Dell Switch?

1. Login into hidden account names 'Linux Admin' (**see password.yml**)

2. From Linux Admin run the following:

   2.1 **Command:** `$ sudo /sbin/pam_tally2 --user=admin --reset`

5.19 Unable to Connect to Node via IPMI/ping

1. Assemble and utilize the crash cart adapter with gray Cisco Mini USB.

2. From command line enter to following to connect to node interface:

   2.1 **Command:** `sudo crash cart`

5.20 Security Onion Node Unable to Reach Manager

1. From designated Security Onion Sensor, run the following:

   1.1 **Command:** `$ ip a` – verify connectivity between the eno# and the port assigned to VLAN 102 on T-SW.

2. If eno# is “down”, change port on the Security Onion Sensor and verify connectivity

    2.1 **Command:** `ip a`

6 Other Useful Information

6.1 Options When Rebooting Nodes

1. **Delete** – Access to general setup.
2. **F11** – Access to bootstrap setup.
3. **F12** – Access to PXE boot setup.
4. **Tab** – Access to BIOS setup.

6.2 Launching a Console in Engine

1. Go to “Compute/VMs”
2. Select the name of the instance. you would like to console into.
3. Select noVIC.
4. Select Console again.

6.3 Generating a New Windows IP Address

1. Enter the following commands:

    1.1 **Command: $ ipconfig /?** – provides information on configuration options

    1.2 **Command: $ ipconfig /release** – drops the current endpoint IP.

    1.3 **Command: $ ipconfig /renew** – grabs new IP.

6.4 VLAN Designation

1. **.100** = Analytics (Engine)/Additional Tools (e.g., EndGame)
2. **.101** = Hosts/Additional VMs
3. **.53** = IPMI
4. **.51** = MGMT (IDM)
5. **.102** = NSM (Network Security Manager)/Security Onion VLAN
6. **.52** = Storage (Gluster)
7. **.54** = User
8. **.1** = VPN

6.5 Creating VMS for Analyst Laptops Within Engine

1. Navigate to **Engine/Compute/VMs/New**.
2. Template (select desired).
3. Fill out remaining information as needed.
4. Nic1 (select VLANS you would like your analyst laptop VMs to be a part of.)
5. Allow VMs to spin up.
6. Select your created VM and navigate to **Run/Run Once/Initial Run**.
7. Select Cloud Init.
8. Create credentials for VMs.

6.6 Allowing Removable Media (e.g., USBs) on Analyst Laptops

1. Navigate to the following:

   1.1 **Local Group Policy Editor/Administrative Templates/Windows Components/BitLocker Drive Encryption/Removeable Data Drives**

6.7 Security Onion Information

1. **MGMT Interface** – allows the Security Onion node to communicate with the Security Onion Cluster.

2. **Ingest/Monitor** – port on Security Onion node designated to connect to the customers sensor/TAP/SPAN and is statically assigned to VLAN 102.

3. After the DDS-M is restarted, the assigned VLAN for the MGMT interface may reset, be sure to check running configuration of T-SW during DDS-M start up.

7 Setting Up a SPAN Port on Cisco 3560

1. Once connected into the Cisco 3560 SW and enter the following:

   1.1 **Command: $ sudo minicom cisco**

   1.2 **Command: # enable**

   1.3 **Command: # show interfaces**
   NOTE: format = **GigabitEthernet1/0/1**

   1.4 **Command: # configure terminal**

   1.5 **Command: # monitor session 2 source interface GigabitEthernet1/0/1**
   NOTE: Add all necessary interfaces that you would like data to be ingested each in a different command (e.g., 1/0/2, 1/0/3, etc.)

   1.6 **Command: # monitor session 2 destination interface GigabitEthernet1/0/12**

1.7 **Command: # exit**

1.8 **Command: # show monitor session 2 detail**
NOTE: DO NOT monitor session 2 from source VLAN 1, this would remove VLAN 1 from source within current session.