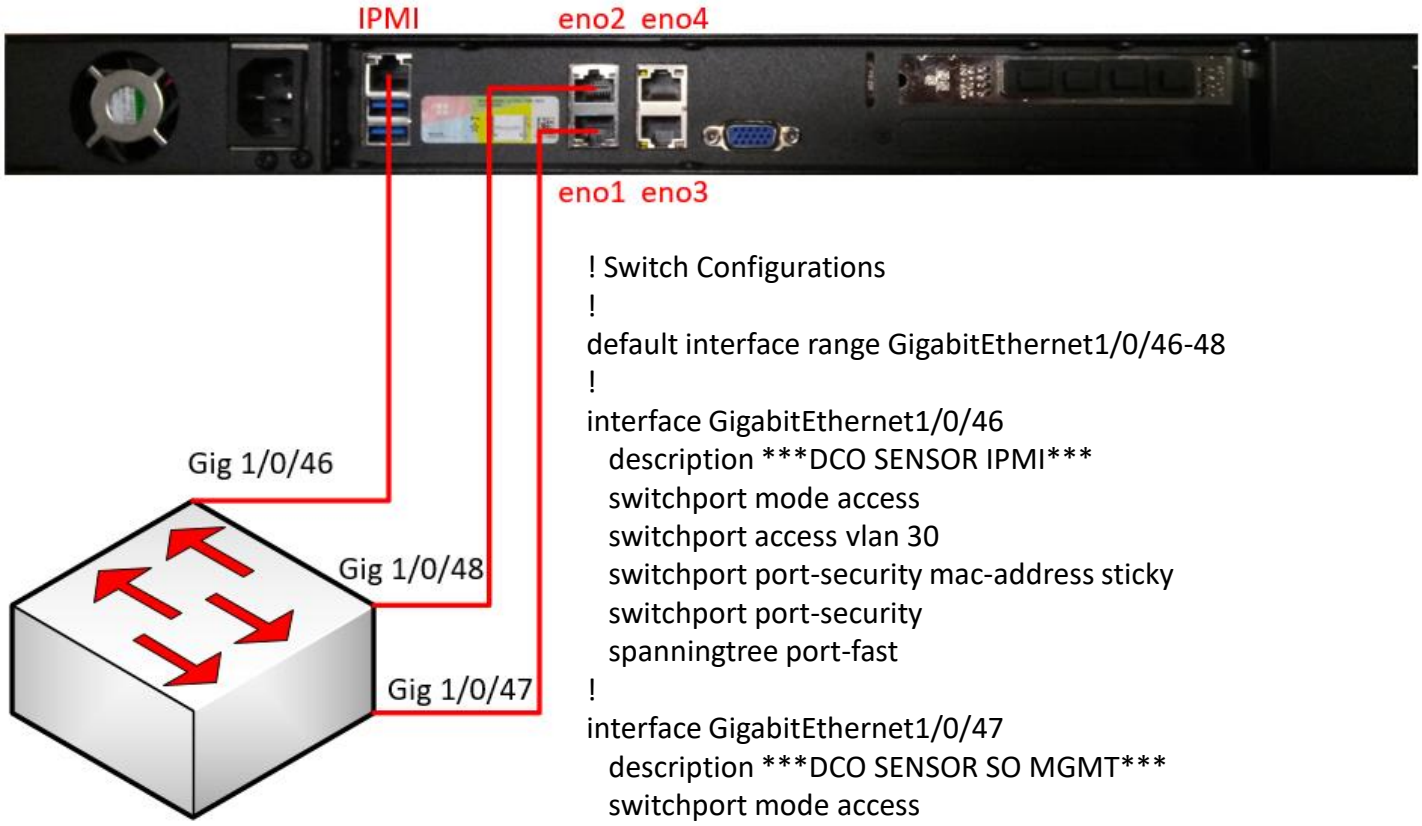
Using the MaxVision MiniRax as a SecurityOnion 2.3 Standalone Sensor

- Download the latest version of the SecurityOnion ISO from https://github.com/Security-Onion-Solutions/securityonion/blob/master/VERIFY_ISO.md to the computer where you will be deploying the operating system (OS) from
- Connect the Intelligent Platform Management Interface (IPMI) and the interface you will use as the OS management to the switch you will be plugging into. (See figure below)
- Connect the sniffing interface to the Switch Port Analyzer (SPAN) port on the switch. If you are using a tap, connect the sniffing interface to the tool port on the tap. If you use a tap the eno2 connection shown below would not apply.

Example: We will be connecting the sensor/server to a switch that has VLAN 10 (users), 20 (voice), and 30 (servers). In this example, we will be placing the management interfaces (IPMI and OS) on the server VLAN. We will assume that the server VLAN is on the 137.233.34.0/27 network. We will always require 2 IP addresses when dealing with any physical sensors; 1 for the IPMI and 1 for the OS.



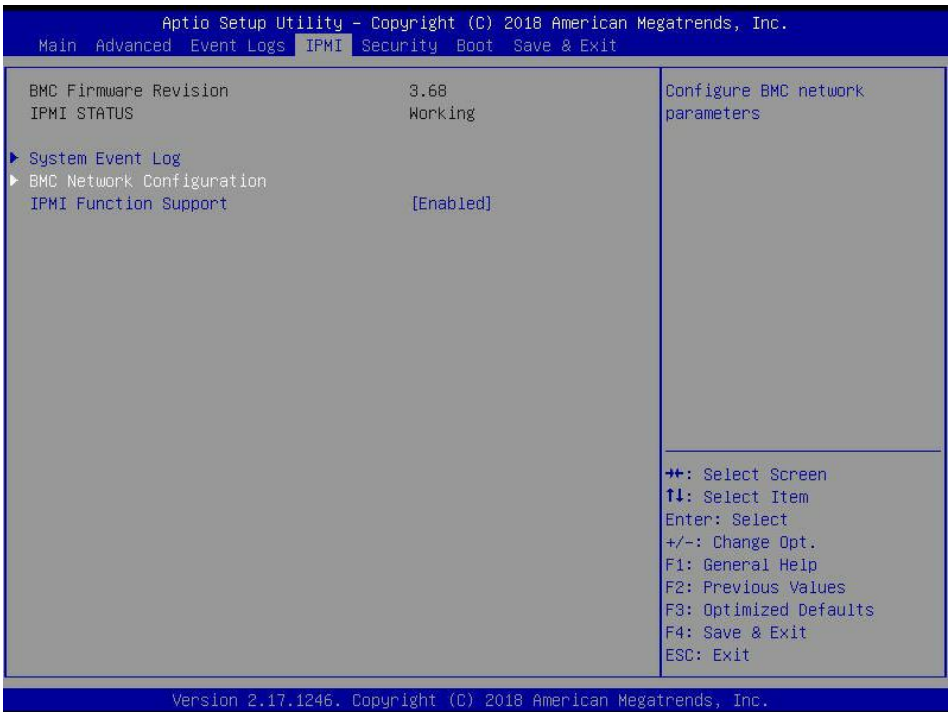

```
! Switch Configurations
!
default interface range GigabitEthernet1/0/46-48
!
interface GigabitEthernet1/0/46
  description ***DCO SENSOR IPMI***
  switchport mode access
  switchport access vlan 30
  switchport port-security mac-address sticky
  switchport port-security
  spanningtree port-fast
!
interface GigabitEthernet1/0/47
  description ***DCO SENSOR SO MGMT***
  switchport mode access
  switchport access vlan 30
  switchport port-security mac-address sticky
  switchport port-security
  spanningtree port-fast
!
monitor session 1 source vlan 10 , 20 ,30
monitor session 1 destination interface GigabitEthernet1/0/48
!
end
wr

!
```

If you have not assigned the IPMI interface an IP address and don't know the current IP, you will need to assign it through the BIOS using a monitor and keyboard

- During bootup, you will need to press the Delete key to get into the BIOS setup menu (you will need to enter the admin password to be able to access BIOS settings)

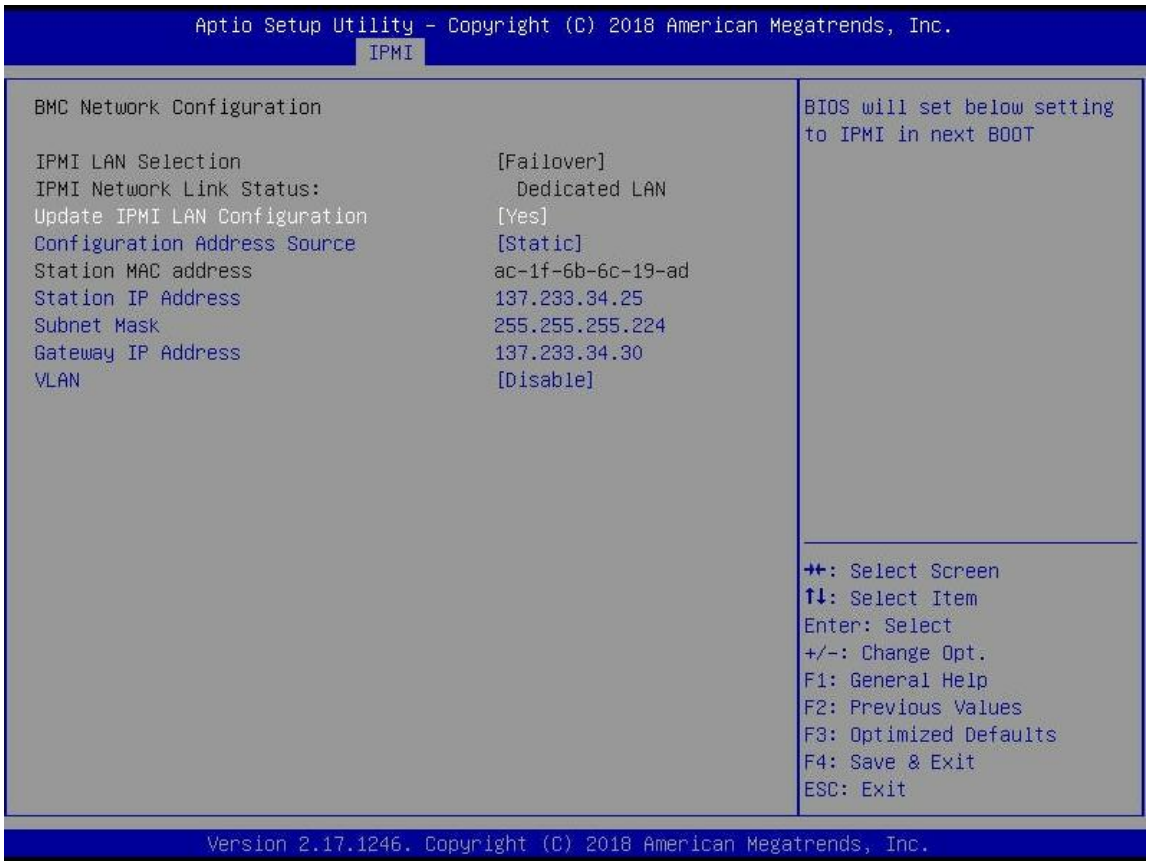
- Once you get into the BIOS, go to IPMI, select "BMC Network Configuation", and press the Enter key



- In the IPMI configuration screen, change the “Update IPMI LAN Configuration” value to Yes
- Change the IP address values according to the network the sensor/server will be placed in.

In this example, the sensor’s IPMI will have the 137.233.34.25 IP address and its gateway will be 137.233.34.30.

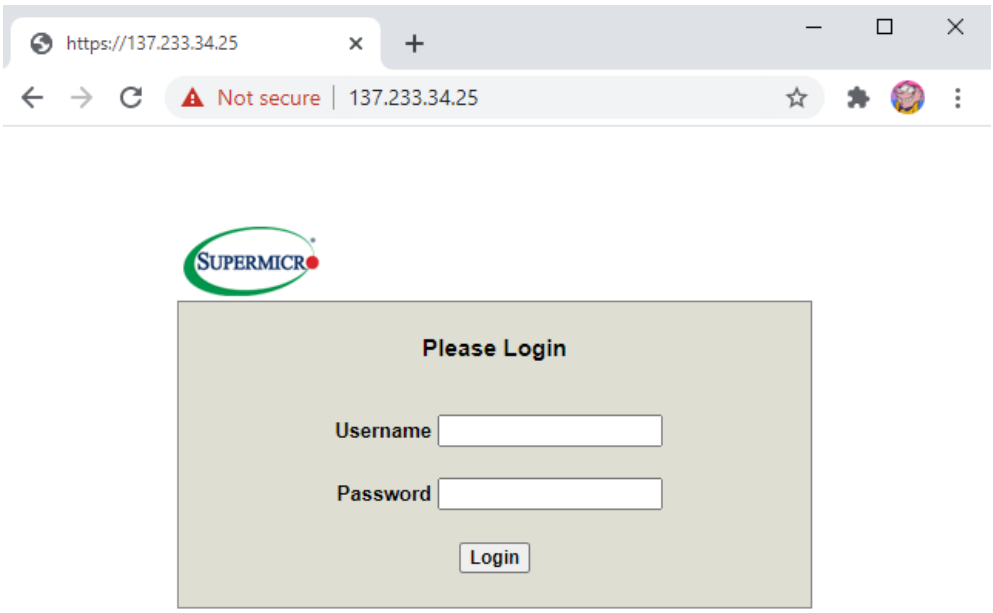
*Note: even though the sensor management interfaces will be placed on the server VLAN, we **DO NOT** need to specify a VLAN ID in the IPMI configuration screen. The only time you would specify a VLAN ID is if the switch port connected to the IPMI interface was configured as a trunk (802.1q).*



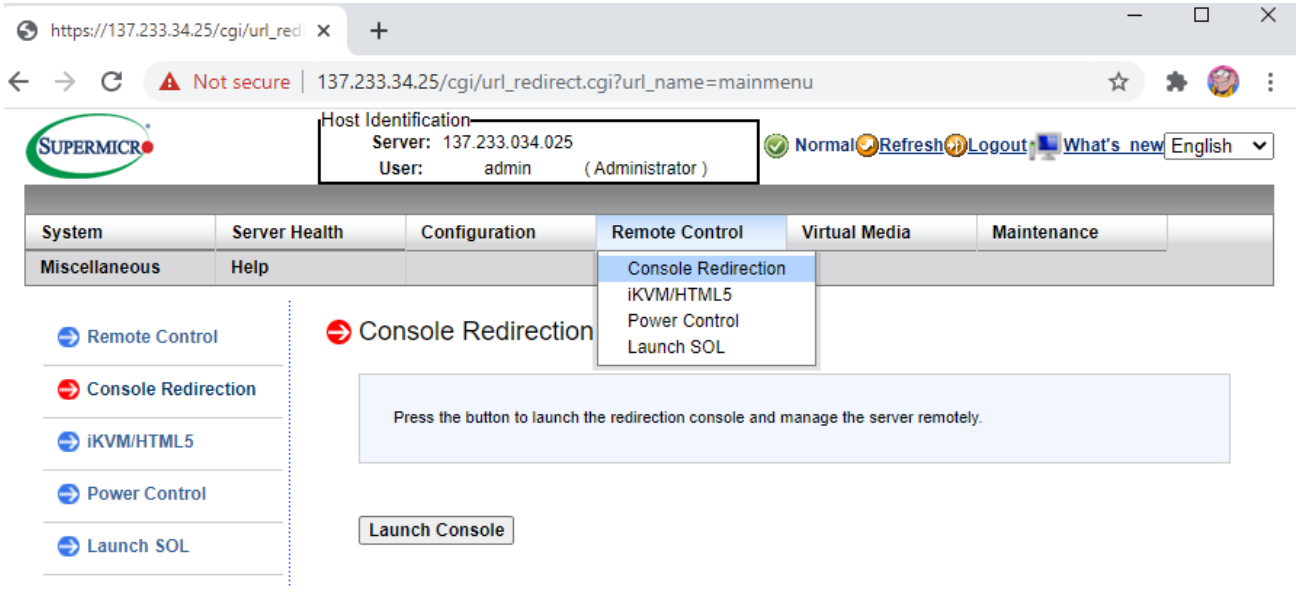
- Press the F4 key to save the configuration changes
- When you are prompted to save and exit, select Yes

- Once you have saved the IPMI configurations, navigate to the web user interface of the sensor/server's IPMI

Note: the username SHOULD be admin. If it is not, it will be ADMIN in all capital letters. If the standard password does not work for either admin or ADMIN, the password might be the SuperMicro defaults (username ADMIN and password ADMIN)



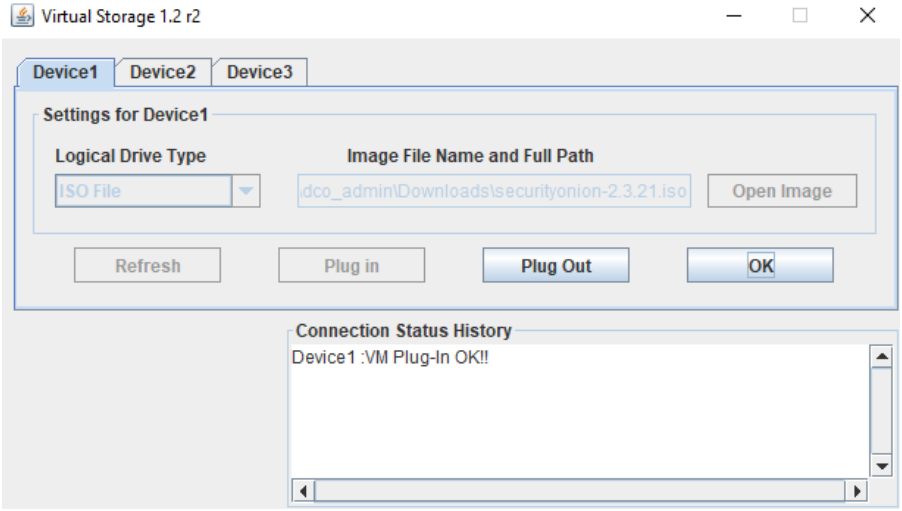
- Once you log in, access the server Java console by going to "Remote Control" and "Console Redirection"



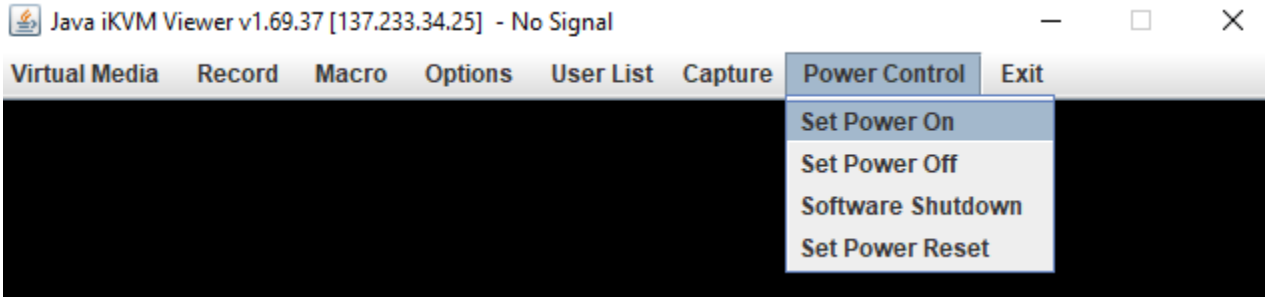
- Click the "Launch Console" button (this will download a Java file that will need to be launched). If you don't have Java installed, install it.

- From the IPMI console window, click “Virtual Media” and select “Virtual Storage”

- Once you log in, access the server Java console by going to “Remote Control” and “Console Redirection”
- Select “ISO File” from the Logical Drive Type drop-down menu.
- Click the “Open Image” button and select your ISO file
- Once you have your ISO selected, click the “Plug In” and “OK” buttons

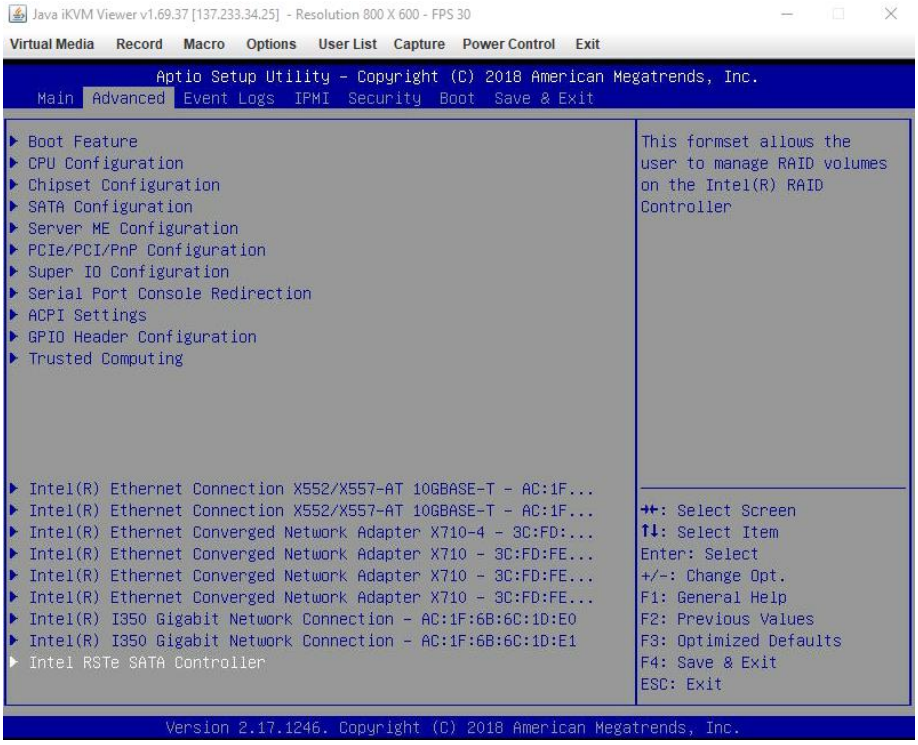


- If the sensor/server is already running, reset the power on it by going to “Power Control” and selecting “Set Power Reset.” If it’s off, turn it on.

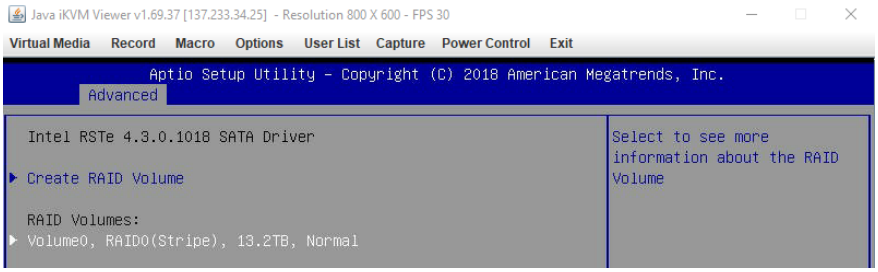


For SecurityOnion 2.3, we will have to delete the RAID configuration from the BIOS

- Interrupt the boot-up and go into the BIOS Settings
- From the BIOS screen, got to Advanced and select “Intel RSTe SATA Controller”

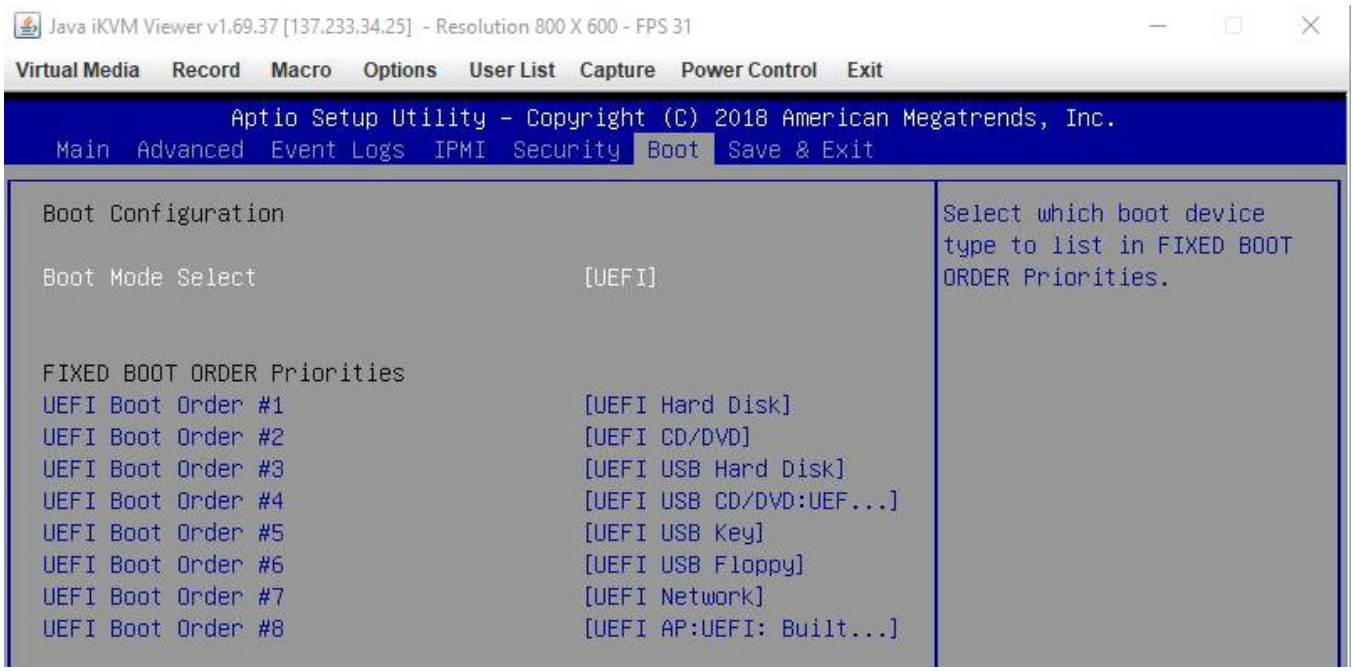


- From the RAID configuration screen, select any logical volume that might exist

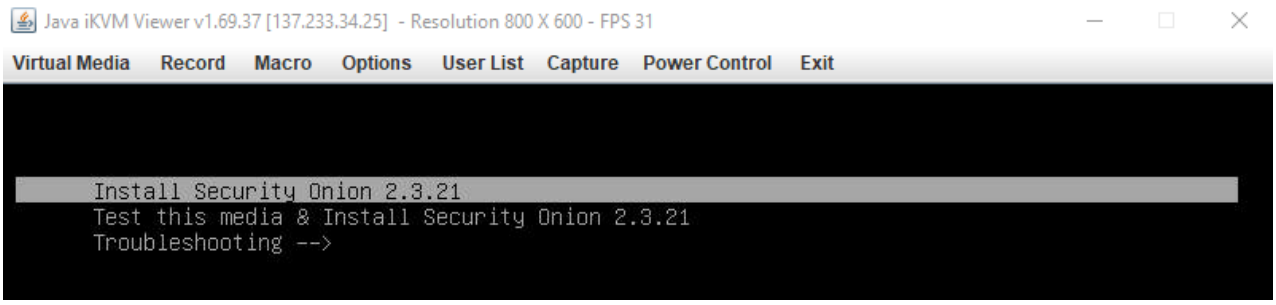


- From the RAID Volume Information screen, select Delete and confirm the deletion when prompted

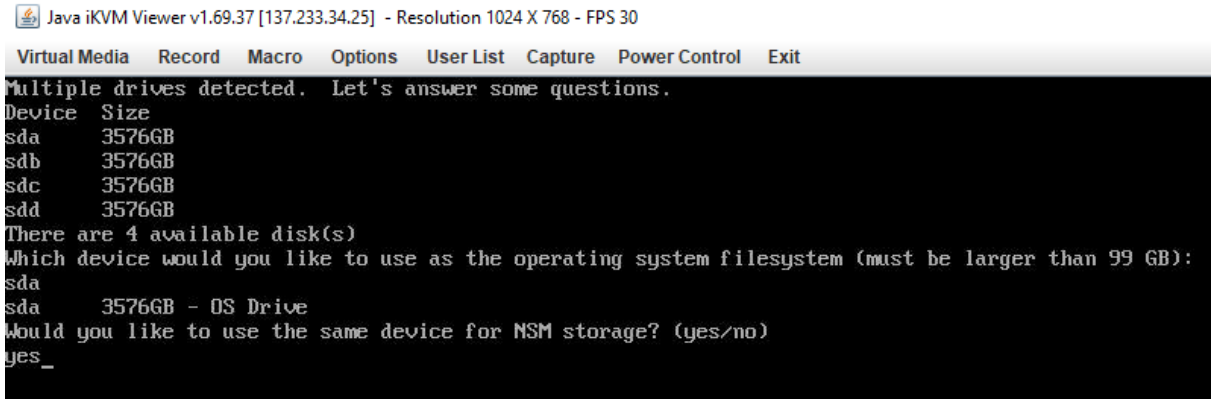
After you save the RAID configurations, the server should boot into the SecurityOnion installer wizard. If it does not, check the boot options on the sensor/server's BIOS to ensure the virtual CD-ROM is part of the boot sequence.



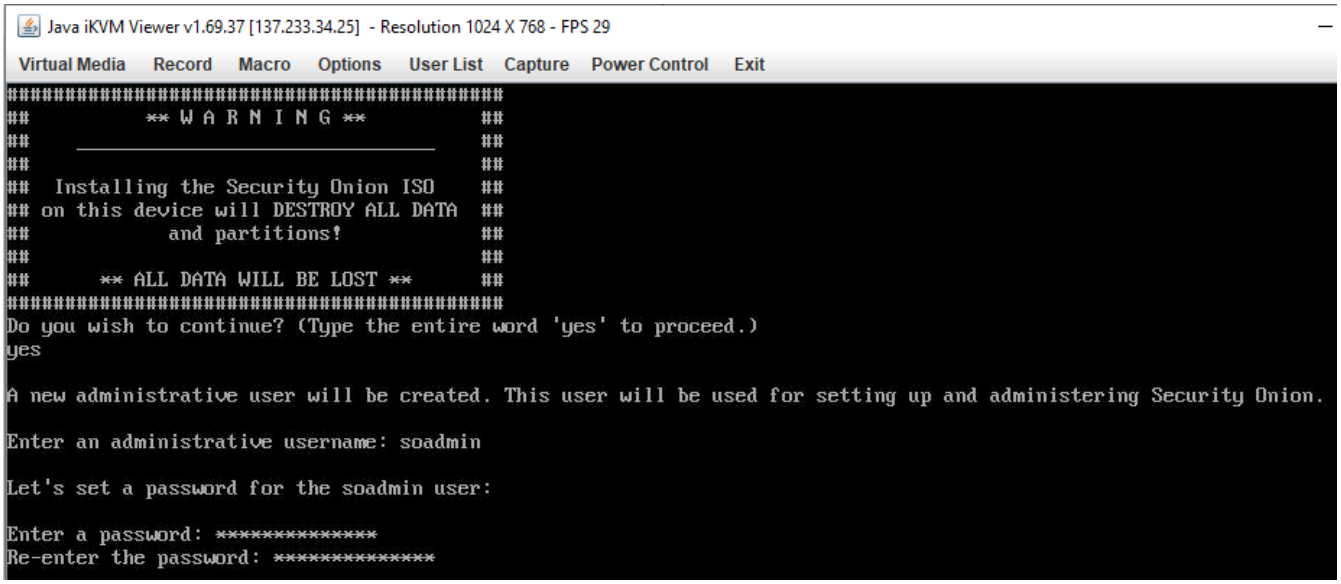
- When the Security Onion GRUB menu shows up, select "Install Security Onion 2.3.XX"



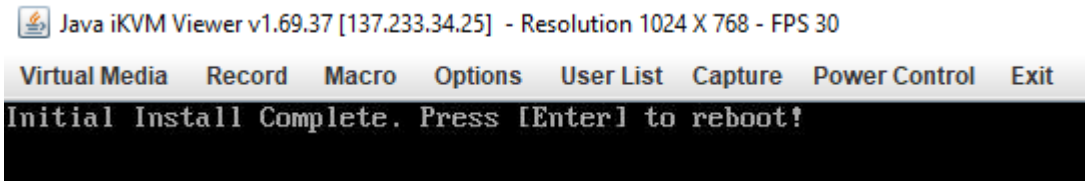
- Once the installer fully boots up, you should be prompted to select which of the 4 hard drives to install Security Onion on. Enter "sda" and press Enter.
- When you are prompted whether to install NSM on the same storage device, enter "yes"



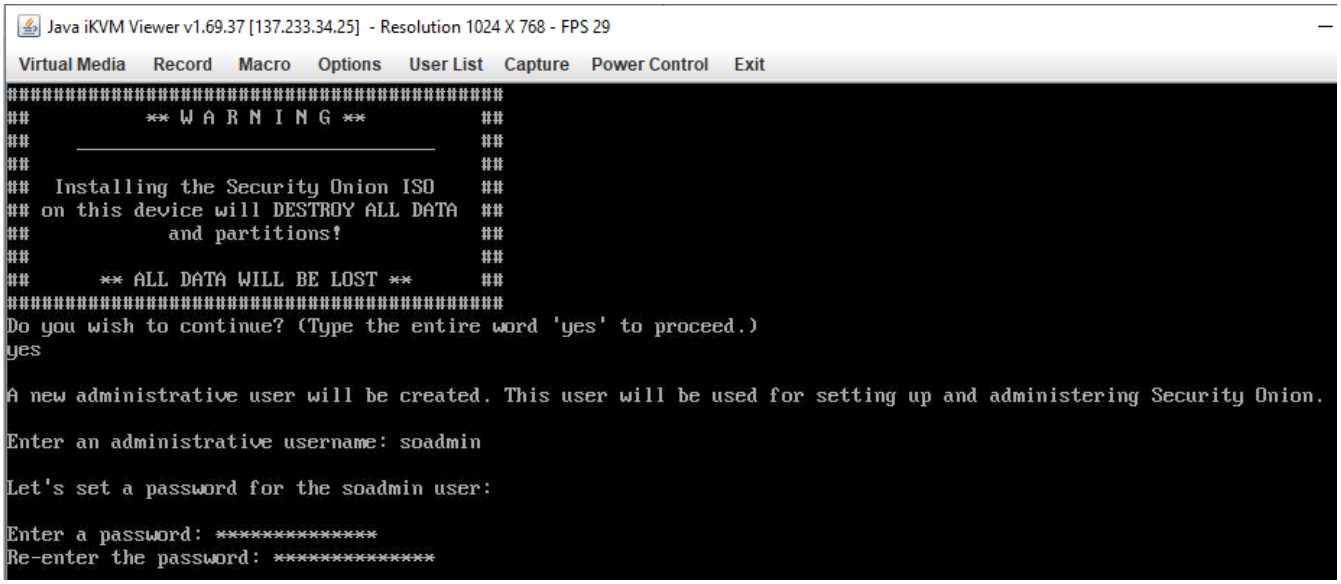
- You will be prompted to confirm the install. Enter “yes”
- When you are prompted for a username, use soadmin (change according to SOP)
- You will be prompted for a password for the user specified.



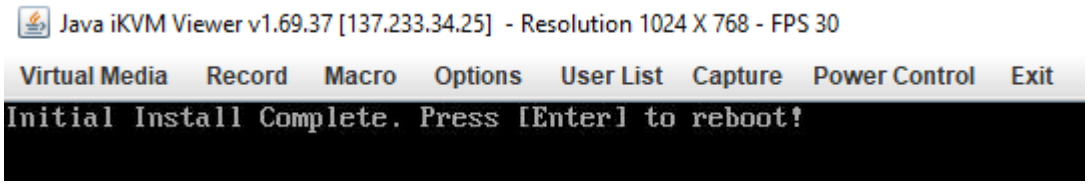
- After the OS installation is complete, you will be prompted to reboot.



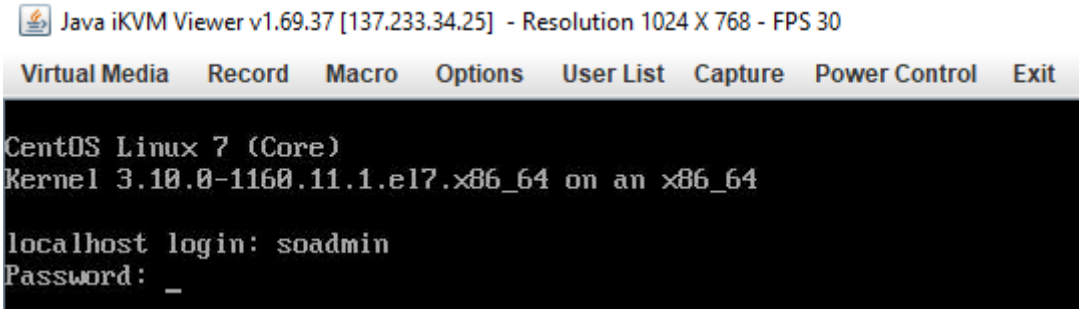
- You will be prompted to confirm the install. Enter “yes”
- When you are prompted for a username, use soadmin (change according to SOP)
- You will be prompted for a password for the user specified.



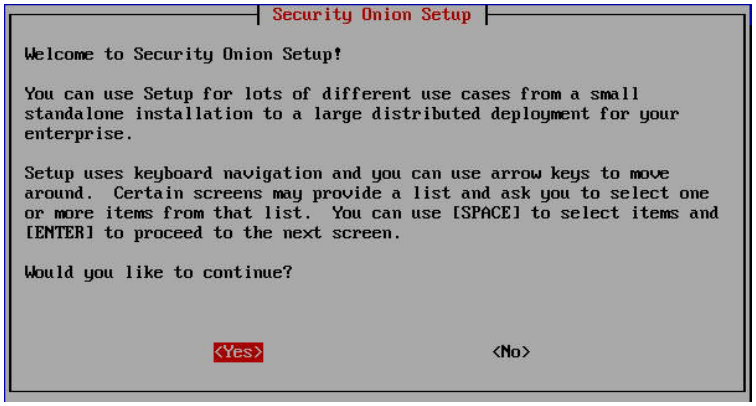
- After the OS installation is complete, you will be prompted to reboot.



- Once the sensor/server reboots, login with the username created during the install process

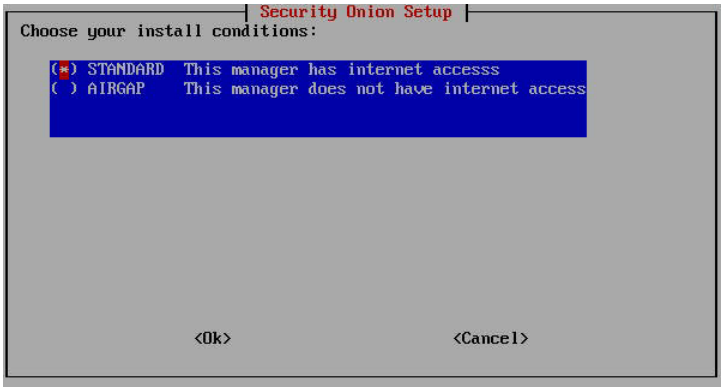


- Once the Security Onion setup wizard starts, select yes to continue

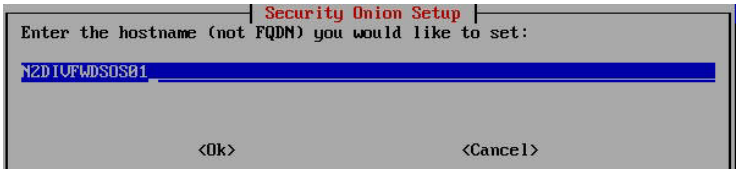


- Since this guide is specific to a Standalone setup, we will select STANDALONE as the install type

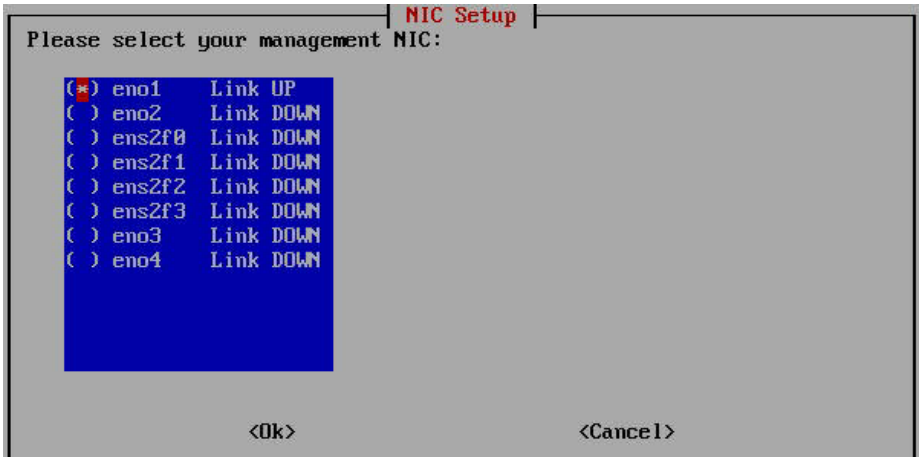
- If the guide is being followed to setup a NIPR sensor, select STANDARD for the install condition. Otherwise, select AIRGAP for other networks (i.e SIPR, MS, etc.)



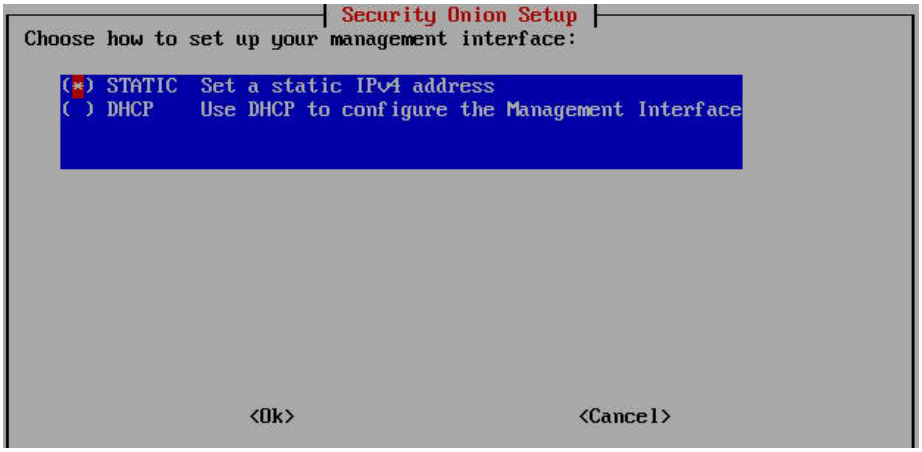
- For the hostname, follow the local site's naming standards



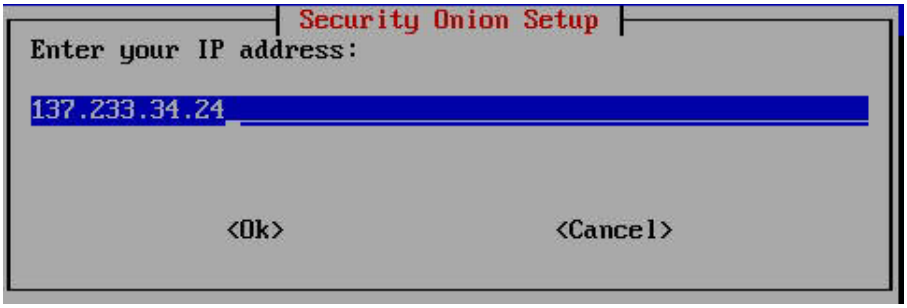
- If you followed the guidance in page 2 of this document, choose eno1 as the management interface. Otherwise, choose the interface you designated as management.



- For the addressing type, choose STATIC

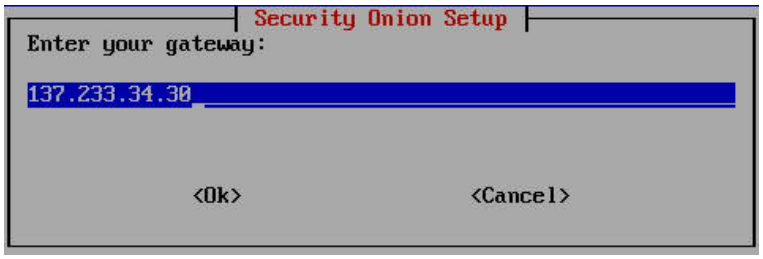


- When assigning the IP address for the sensor, assign it the IP address given to you by the local administrators. This guide assumes the IP given is on the same VLAN as the rest of the servers.



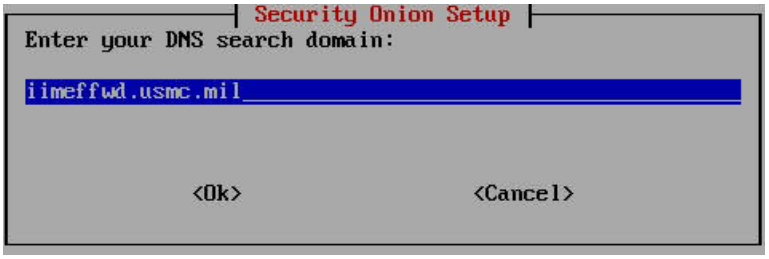
- Ensure the subnet mask is correct according to the network the sensor will be in

- Enter the default gateway accordingly

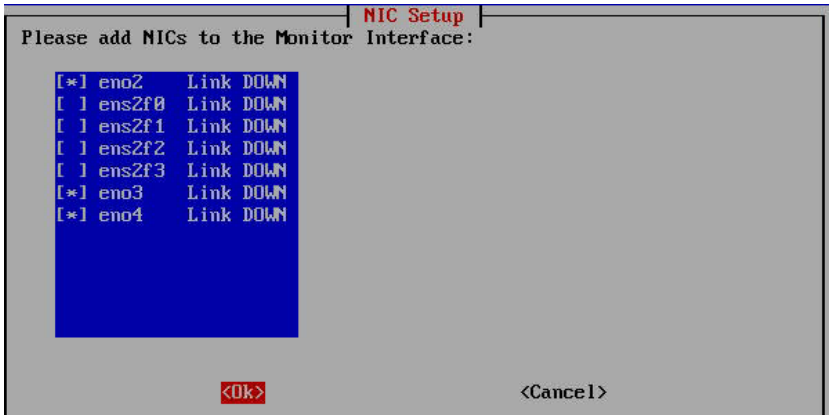


- Enter the IP address of the local site's DNS server

- Enter the DNS search domain for the local site



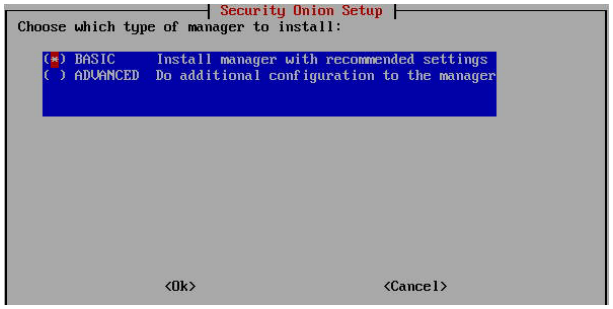
- In the Monitor Interface screen, select all the interfaces that will be used to receive traffic to be sniffed.

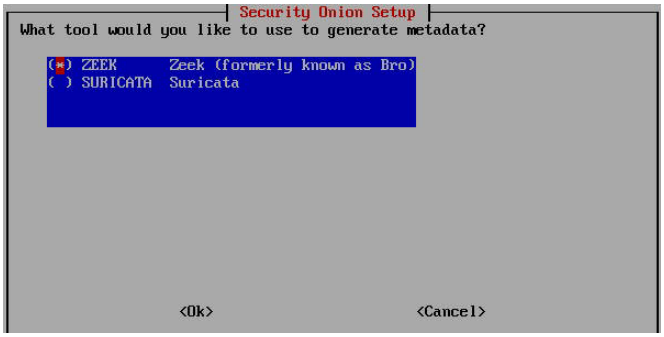


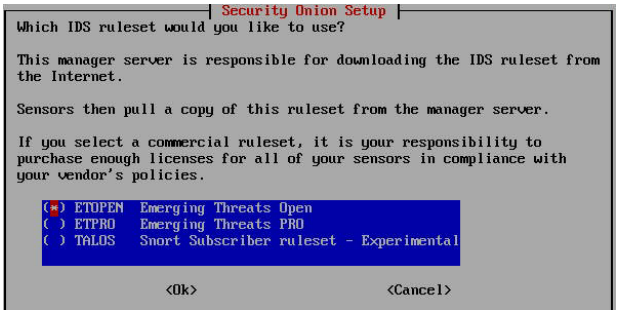
- Select Automatic as the OS patch schedule

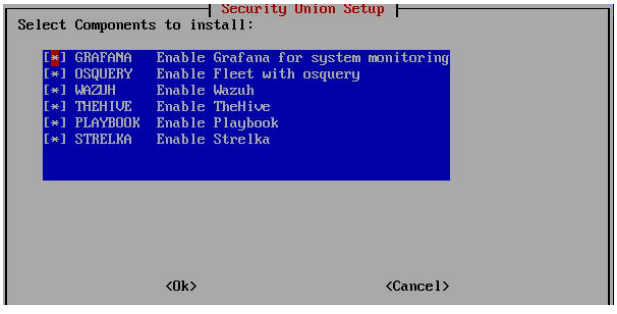
- Change the HOME_NET value to the local network

- Use the defaults for the next set of screens

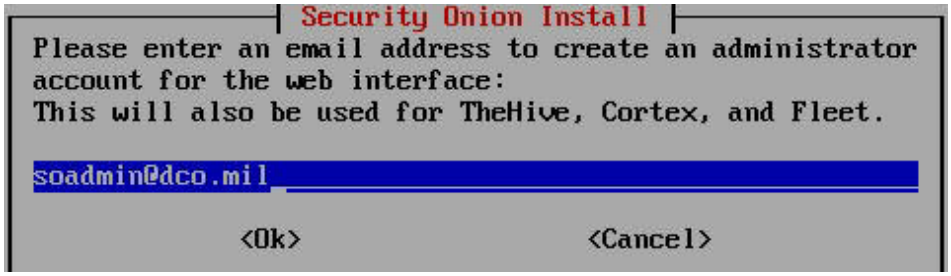




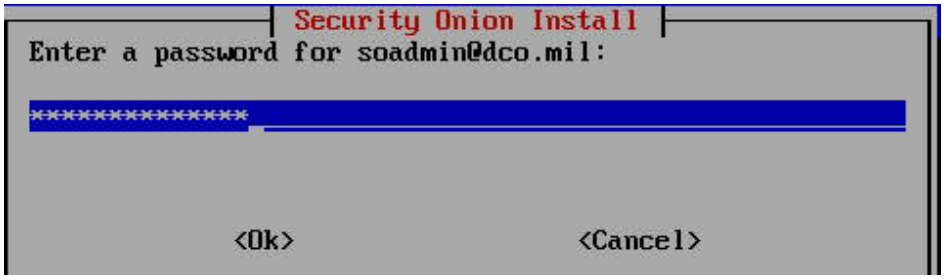




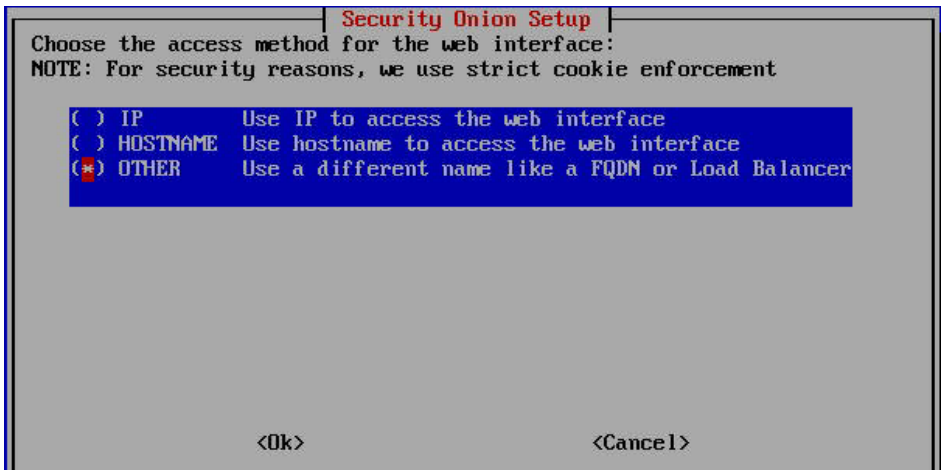
- When asked for an application use, enter soadmin@dco.mil (change according to SOP)

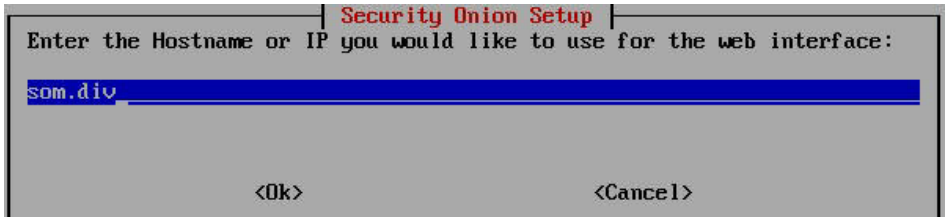


- Enter and verify the password for the application user



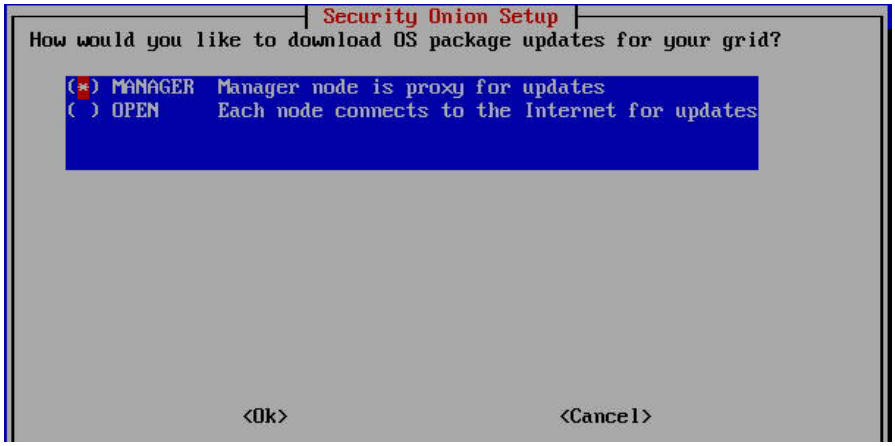
- For the web interface access method, select the method that best suites need. You can specify an alternate access method by selecting OTHER as follows:



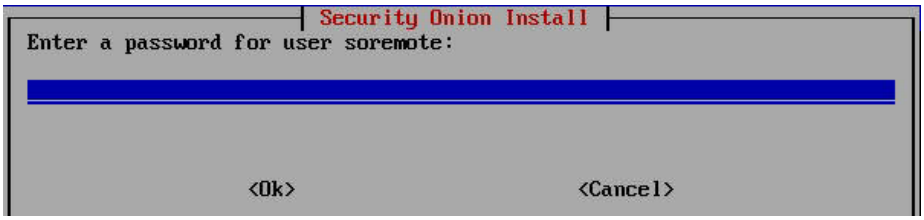


Note: the method shown above requires that the DNS infrastructure is setup to resolve som.div to the IP address of the sensor

- Select MANAGER for the update download method

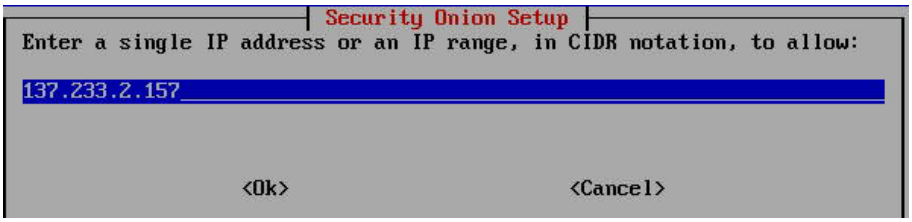


- You will be prompted to enter a password for the soremote user. Since this guide is intended for a standalone deployment, the soremote user will never be used.

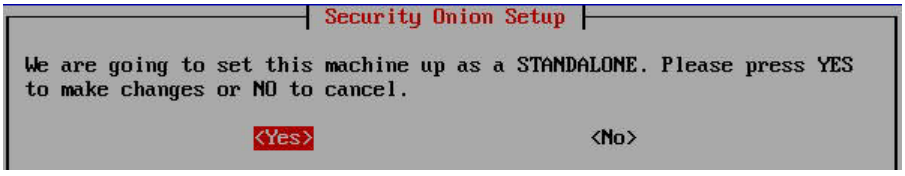


- Select the defaults through the next screen until you get to the prompt to run so-allow. Select Yes

- Enter the initial IP address that should have access to the sensor



- At the final screen, select Yes to start the setup process



- When the setup is finished, you will be prompted to reboot. Reboot the sensor. If the setup did not properly, read the log in /root/setup.log to troubleshoot the issue.

Once your sensor reboots, you will have to use lvm to combine the remaining 3 hard drives.

- Run “fdisk -l” to list your hard drives. You should see sda, sdb, sdc, and sdd. The sda disk is where the OS is currently installed on and should have multiple partitions. If you see any partitions on the other three disks, we will delete them in the upcoming steps.

```
Disk /dev/sda: 3840.8 GB, 3840755982336 bytes, 7501476528 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disk label type: gpt
Disk identifier: BA1DC455-D03E-4FA5-8EE7-3748A153795D


#         Start          End    Size  Type            Name
 1         2048      2099199      1G  EFI System      EFI System Partition
 2      2099200      3123199    500M  Microsoft basic
 3      3123200   7501475839    3.5T  Linux LVM
WARNING: fdisk GPT support is currently new, and therefore in an experimental phase. Use at your own discretion.
```

- Run “sudo fdisk /dev/sdb”. You will be presented with the fdisk prompt. You can press the M key to see what available options you have

```
[soadmin@N2DIVFWDSOS01 ~]$ sudo fdisk /dev/sdb
WARNING: fdisk GPT support is currently new, and therefore in an experimental phase. Use at your own discretion.
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.


Command (m for help):
```

- Press the P key to print the current partition table on sdb.

```
Command (m for help): p

Disk /dev/sdb: 3840.8 GB, 3840755982336 bytes, 7501476528 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disk label type: gpt
Disk identifier: AED963E9-BD4E-42AB-8757-7FB54ECAFF06


#         Start          End    Size  Type            Name
 1         2048   7501476494    3.5T  Linux LVM
```

- If any partitions were listed in the previous step, press the D key to delete it followed by the P key to ensure the partition table is empty.

```
Command (m for help): d
Selected partition 1
Partition 1 is deleted

Command (m for help): p

Disk /dev/sdb: 3840.8 GB, 3840755982336 bytes, 7501476528 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disk label type: gpt
Disk identifier: AED963E9-BD4E-42AB-8757-7FB54ECAFF06


#         Start          End    Size  Type            Name
```

- Press the W key to save the changes to the disk. You will get an error saying that the resource is in use.

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
```

- The previous step will give you an error. Perform the same actions on /dev/sdc and /dev/sdd. Once done, reboot the sensor to ensure the changes take effect.
- Once your sensor has been rebooted. Run “sudo fdisk /dev/sdb”
- Press the N key to create a new partition (partition 1). Use the default values (press enter through the prompts) that are auto-populated.

```
Command (m for help): n
Partition number (1-128, default 1):
First sector (34-7501476494, default 2048):
Last sector, +sectors or +size{K,M,G,T,P} (2048-7501476494, default 7501476494):
Created partition 1
```

- Press the T key to change the partition’s system ID followed by the L key to list all possible IDs. You will be presented with a large list. Identify the two-digit number associated with “Linux LVM.”

```
Command (m for help): t
Selected partition 1
Partition type (type L to list all types): L
  1 EFI System                     C12A7328-F81F-11D2-BA4B-00A0C93EC93B
  2 MBR partition scheme           024DEE41-33E7-11D3-9D69-0008C781F39F
  3 Intel Fast Flash               D3BFE2DE-3DAF-11DF-BA40-E3A556D89593
  4 BIOS boot                      21686148-6449-6E6F-744E-656564454649
```

- Enter the two-digit number (yours might not be 31).

```
Partition type (type L to list all types): 31
Changed type of partition 'Linux filesystem' to 'Linux LVM'
```

- Press the W key to save the partition changes.

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
```

- Perform the same steps to create the partition for sdc and sdd.

- Run “sudo pvdisplay” to list the physical volumes

```
[soadmin@N2DIVFWDSOS01 ~]$ sudo pvdisplay
  --- Physical volume ---
  PV Name               /dev/sda3
  VG Name               system
  PV Size               3.49 TiB / not usable 0
  Allocatable           yes (but full)
  PE Size               4.00 MiB
  Total PE              915326
  Free PE               0
  Allocated PE          915326
  PV UUID               NDU1yT-vEnJ-fDRF-cdTf-0gd9-gNbY-pLu09X

  --- Physical volume ---
  PV Name               /dev/sdb1
  VG Name               nsm
  PV Size               3.49 TiB / not usable <1.32 MiB
  Allocatable           yes (but full)
  PE Size               4.00 MiB
  Total PE              915707
  Free PE               0
  Allocated PE          915707
  PV UUID               p55qCL-gmfl-heC5-ROC3-W3ik-ZY5B-16i47G
```

- If any partitions from /dev/sdb, /dev/sdc, or /dev/sdd show a value for VG Name, run “sudo vgremove <VG Name>” (Ex: sudo vgremove nsm)

```
[soadmin@N2DIVFWDSOS01 ~]$ sudo vgremove nsm
Do you really want to remove volume group "nsm" containing 1 logical volumes? [y/n]: y
Do you really want to remove active logical volume nsm/nsm? [y/n]: y
  Logical volume "nsm" successfully removed
  Volume group "nsm" successfully removed
```

- Run “sudo pvcreate /dev/sdb1 /dev/sdc1 /dev/sdd1” to prepare the volumes

```
[soadmin@N2DIVFWDSOS01 ~]$ sudo pvcreate /dev/sdb1 /dev/sdc1 /dev/sdd1
  Physical volume "/dev/sdb1" successfully created.
  Physical volume "/dev/sdc1" successfully created.
  Physical volume "/dev/sdd1" successfully created.
```

- Run “sudo vgcreate nsm /dev/sdb1 /dev/sdc1 /dev/sdd1” to create a volume group named nsm

```
[soadmin@N2DIVFWDSOS01 ~]$ sudo vgcreate nsm /dev/sdb1 /dev/sdc1 /dev/sdd1
  Volume group "nsm" successfully created
```

- Run “sudo vgdisplay” to list the volume groups (optional)
- Run “sudo lvcreate --name nsm --size 10.4T nsm” to create a logical volume named nsm in the nsm volume group. If you get prompted to wipe an existing signature, press y to purge it.

```
[soadmin@N2DIVFWDSOS01 ~]$ sudo lvcreate --name nsm --size 10.4T nsm
  Rounding up size to full physical extent 10.40 TiB
WARNING: ext4 signature detected on /dev/nsm/nsm at offset 1080. Wipe it? [y/n]: y
  Wiping ext4 signature on /dev/nsm/nsm.
  Logical volume "nsm" created.
```

- Run “sudo lvdisplay” to list the logical volumes. You should now see /dev/nsm/nsm

```
[soadmin@N2DIVFWDSOS01 ~]$ sudo lvdisplay
  --- Logical volume ---
  LV Path                /dev/nsm/nsm
  LV Name                nsm
  VG Name                nsm
  LV UUID                Lcwfvo-aIJE-s6Vs-xp4X-BH0z-2oce-o9cPrq
  LV Write Access        read/write
  LV Creation host, time N2DIVFWDSOS01, 2021-02-14 21:25:02 +0000
  LV Status              available
  # open                 0
  LV Size                10.40 TiB
  Current LE             2726298
  Segments               3
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     256
  Block device           253:2
```

- Run “sudo lvscan”

```
[soadmin@N2DIVFWDSOS01 ~]$ sudo lvscan
  ACTIVE            '/dev/nsm/nsm' [10.40 TiB] inherit
  ACTIVE            '/dev/system/nsm' [<3.21 TiB] inherit
  ACTIVE            '/dev/system/root' [<292.97 GiB] inherit
```

- Run “sudo mkfs.xfs -f /dev/nsm/nsm” to format the new logical volume as xfs

```
[soadmin@N2DIVFWDSOS01 ~]$ sudo mkfs.xfs -f /dev/nsm/nsm
Discarding blocks...Done.
meta-data=/dev/nsm/nsm           isize=512    agcount=11, agsize=268435455 blks
         =                       sectsz=4096  attr=2, projid32bit=1
         =                       crc=1        finobt=0, sparse=0
data     =                       bsize=4096   blocks=2791729152, imaxpct=5
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=1
log      =internal log           bsize=4096   blocks=521728, version=2
         =                       sectsz=4096  sunit=1 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

- Elevate your shell to root by running “sudo su”
- Run “docker stop $(docker ps -aq)”. This will stop all docker containers that are currently running.

```
[soadmin@N2DIVFWDSOS01 ~]$ sudo su
[root@N2DIVFWDSOS01 soadmin]# docker stop $(docker ps -aq)
13673ea2e043
5d0d543aa9e6
c7e84c8ed25a
3f8fa000a4d3
```

- Run “mount /dev/nsm/nsm /mnt” to mount the nsm volume in the /mnt directory
- Run “cp -av /nsm/* /mnt” to copy all files from the /nsm directory (currently located in a system LV) to the /mnt directory (currently located in the nsm LV)
- Edit the /etc/fstab file and change the “/dev/mapper/system-nsm” path to “/dev/nsm/nsm”

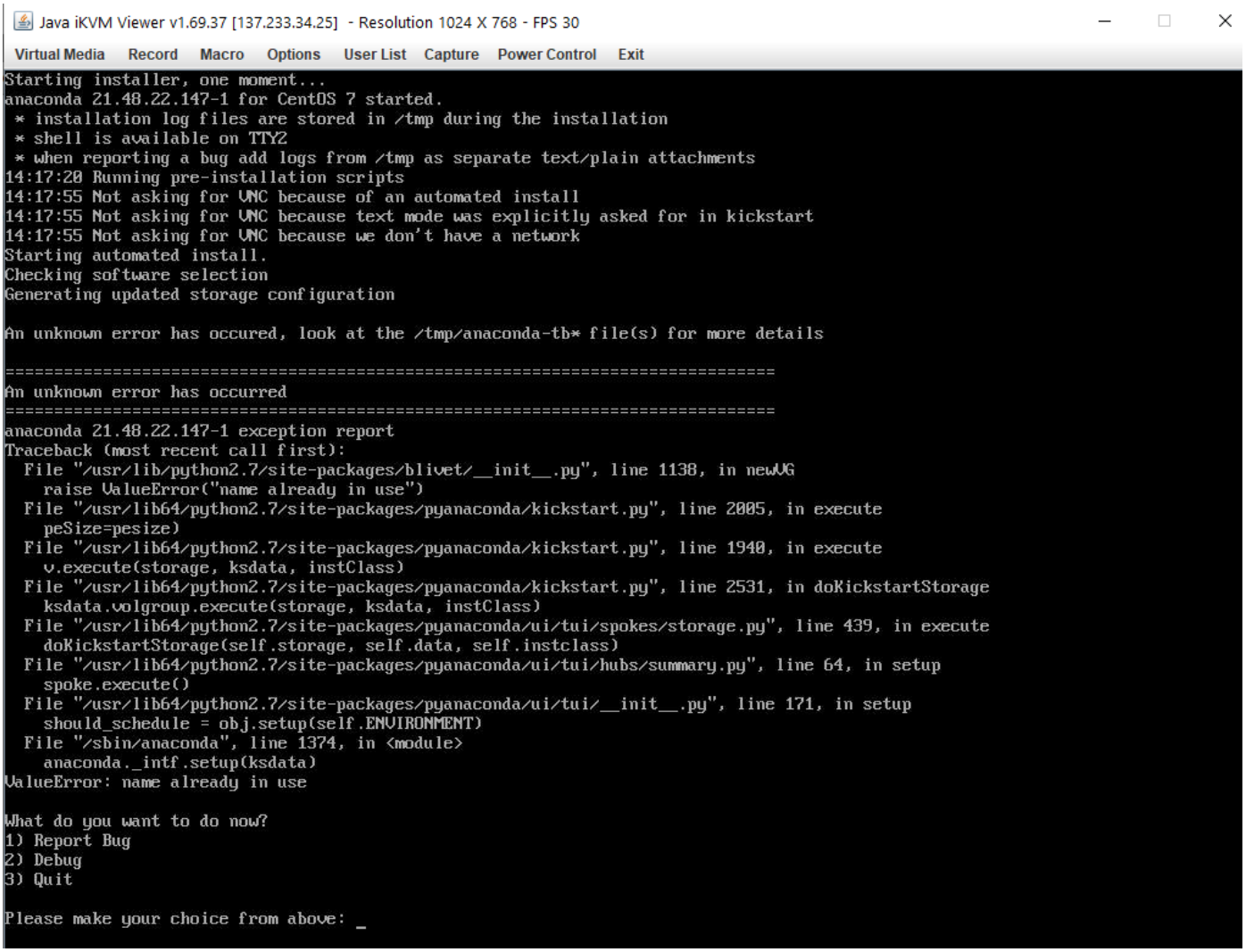
```
[root@N2DIVFWDSOS01 soadmin]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Sat Feb 13 14:34:31 2021
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/system-root /                       xfs     defaults        0 0
UUID=e3a0196c-acd4-4ecd-acaa-69d37b9c41c2 /boot                   xfs     defaults        0 0
UUID=3773-667D          /boot/efi               vfat    defaults,uid=0,gid=0,umask=0077,shortname=winnt 0 0
/dev/nsm/nsm  /nsm                    xfs     defaults        0 0
```

- Reboot the sensor
- Wait for the sensor to power back on and all SO services to start. If there are any errors, have fun googling, or running on only one 3.4T hard drive, or using a hypervisor to make a virtual sensor while dealing with the headache of making promiscuous vswitches, or quitting to start our new jobs at Walmart.

Troubleshooting

- If you run into errors during the OS installation process, it is most likely due to old files on the hard drives.



- If you run into issues when using fdisk for any one of the disks, other than the errors already documented in the steps, you will have to clean the disk with another utility (gparted, diskpart, etc