ESXI S.O.P.

By:Cpl Sneed, Cpl Bletsch, LCpl Regan, LCpl Anderson, LCpl Hepton, LCpl Hundley

3rd PLT DCO-IDM

LU: 20240216

This document will serve as the guide to ESXI installation and usage for operations.

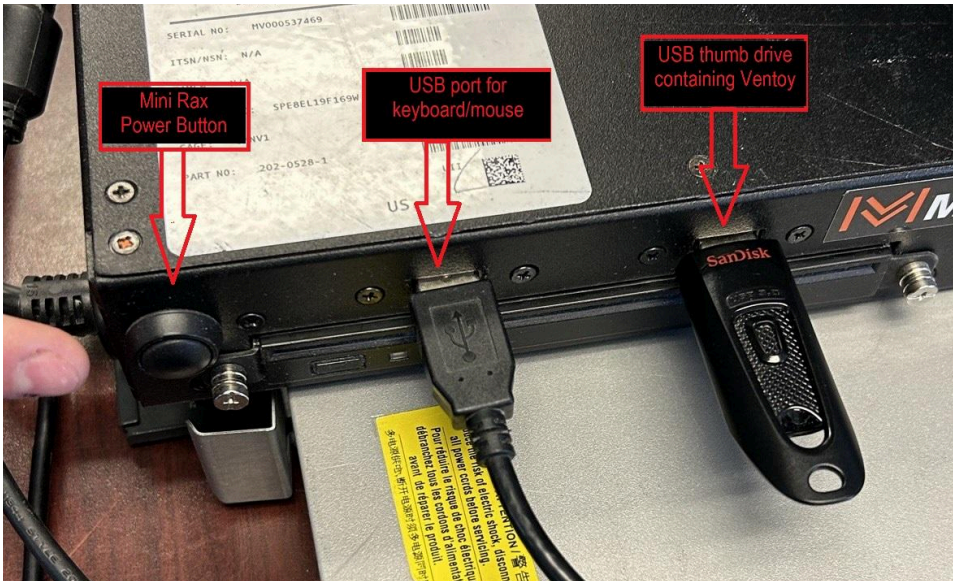
ESXI Overview.....1
ESXI Installation.....2
ESXI Networking Configuration Set-Up.....15
VSwitching..... 15
Port Groups.....16
Configuring IPMI.....18

ESXI Overview

ESXI is a type 1 hypervisor developed by VMWare for deploying and serving virtual computers. In our networks, we install it on a CyberPac, a type of mobile server. All of our tools like Splunk, Arkime and OpenVAS are VMs hosted on ESXI.

ESXI Installation

- **Before beginning** You will need:
  - -a Monitor plugged into the MiniRax via VGA
  - -a Ventoy multibootable USB with Gparted installed on it, plugged into the MiniRax
  - -a keyboard plugged into the MiniRax
  - -a mouse not plugged into the MiniRax (for now)
- Turn on the MiniRax

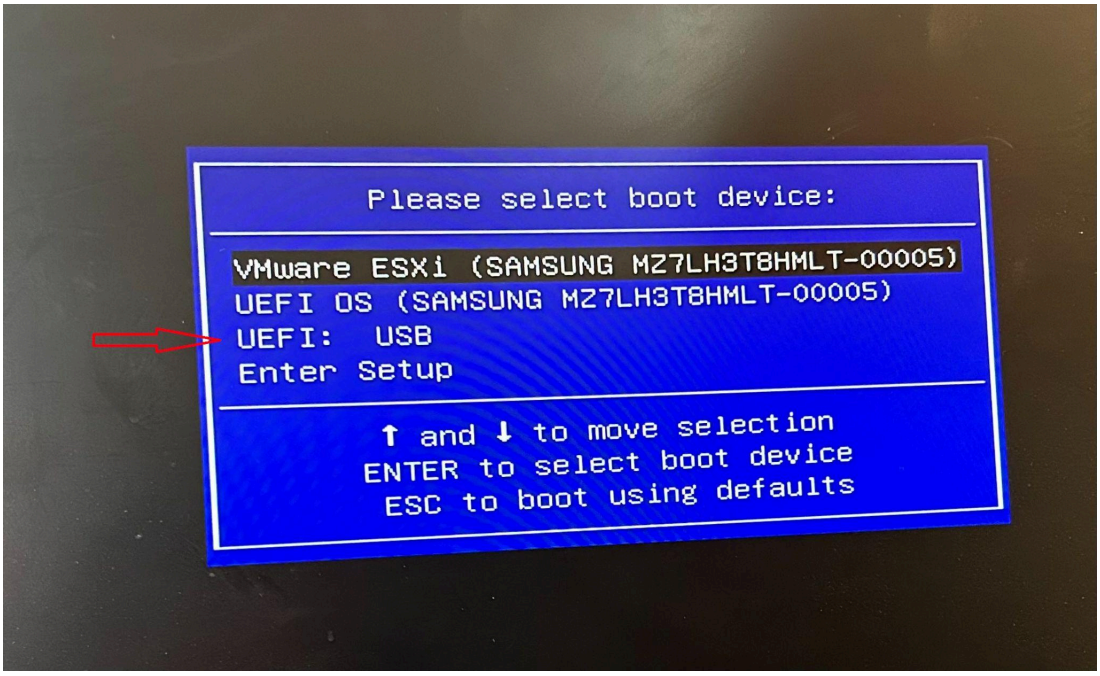


- Press F11 to invoke the boot menu
- Enter the BIOS password
- If the option to boot from USB is unavailable:
- Change the boot order in ‘UEFI Setup’ to boot from the USB first
- Save Changes and Reset
  - -MiniRax will reboot

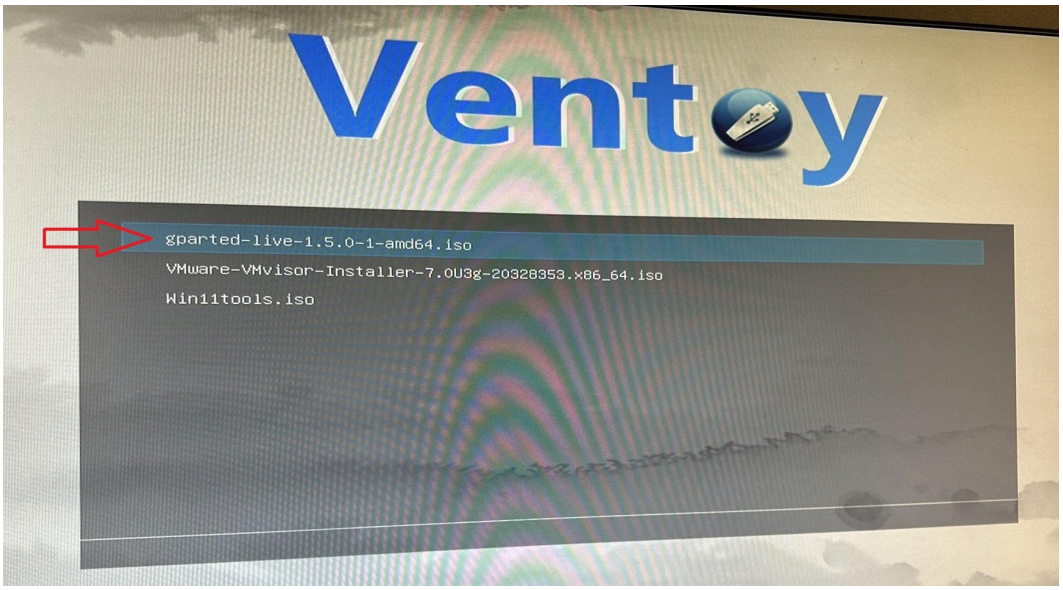
The next step is to wipe the drives using the Gparted tool on the USB:

- Press F11 as the CyberPac reboots and invoke the boot menu
- Press F2 to enter BIOS password
- Enter the BIOS Password

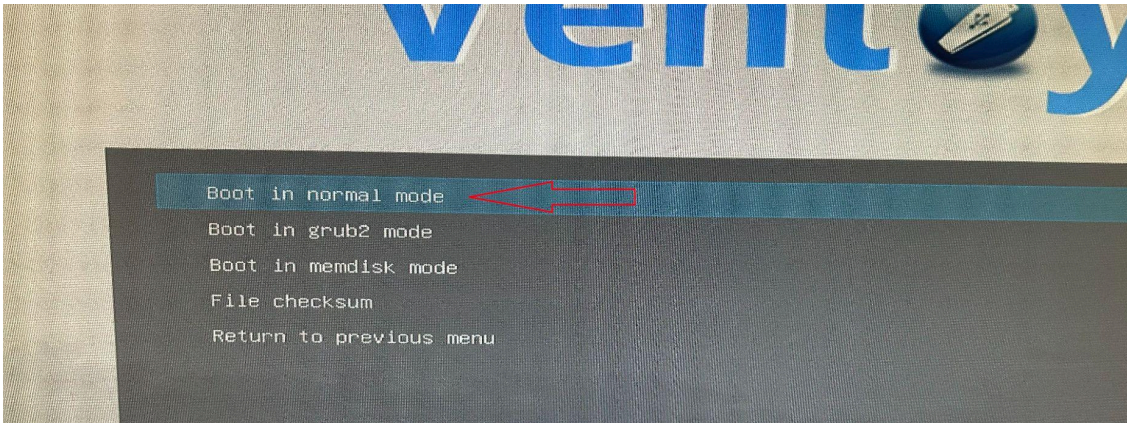
- Boot from the USB click USB option on screen using down arrow



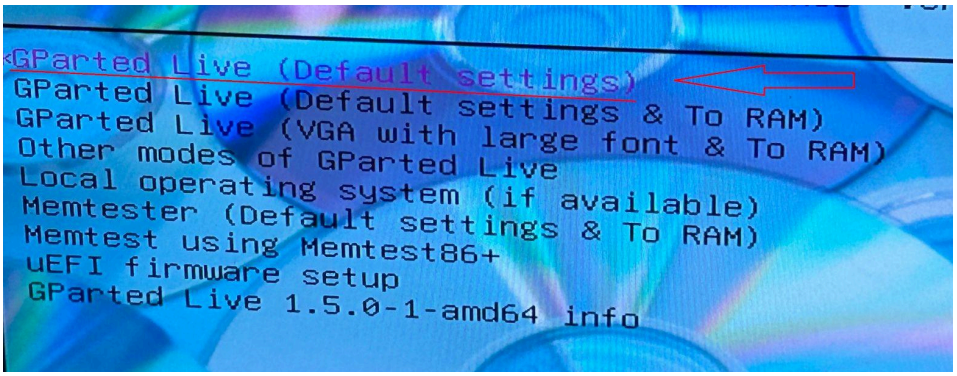
- In the Ventoy GUI use the down arrow to select "gparted-live*"
  -select this one with the ENTER key



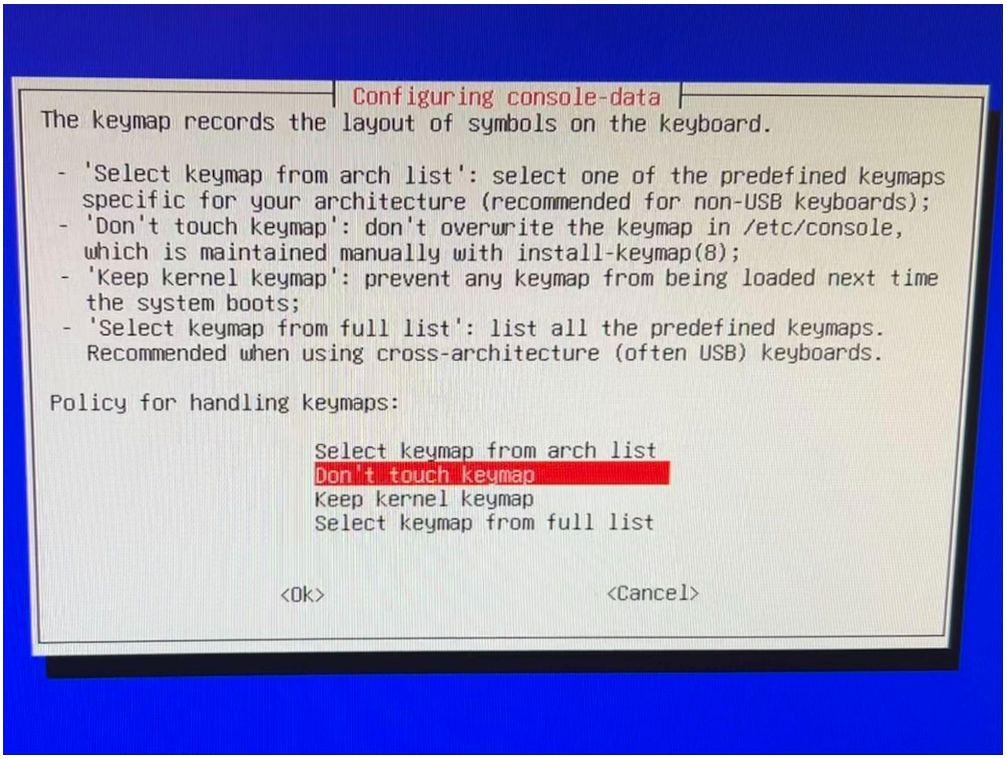
➢ Select Normal-Mode



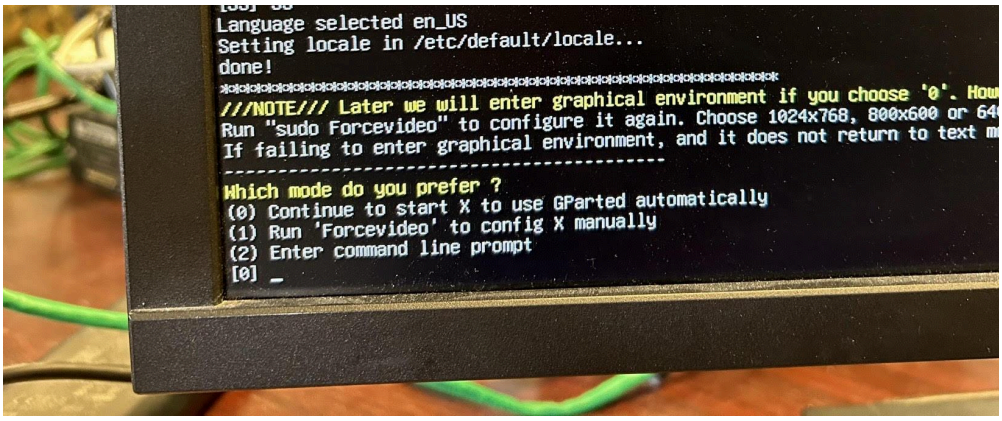
➢ Select Gparted Live (Default settings)



➢ Select Don't touch keymap (this leaves the layout of the keyboard default)

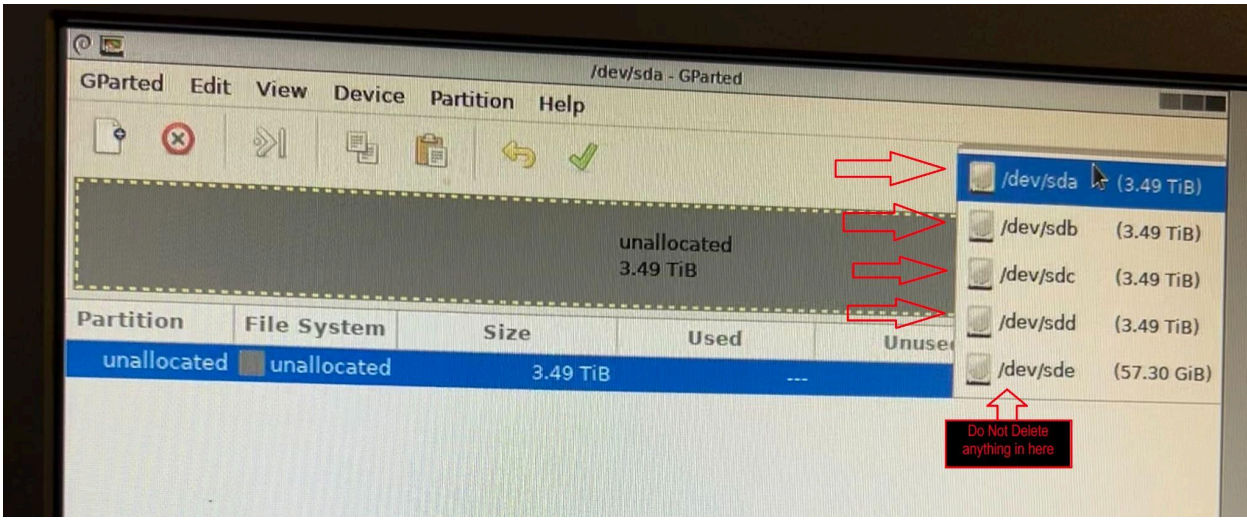


- Type 33 in the lower pane (this selects the english language for the keymap)
  -press enter



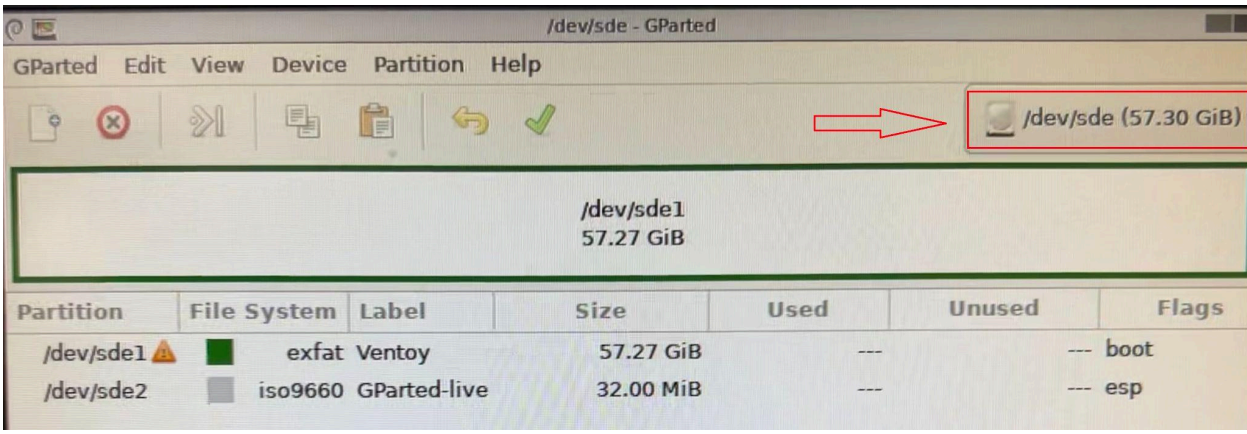
- Select mode, type 0 and press enter
- Unplug the keyboard and plug the mouse in where keyboard was plugged in

- Gparted will automatically open
- Select top right drop down menu



- -Note if the drive only has unallocated like the image above move on to the next drive

- -Note what drive you are booting from (reference the storage size of your flash media and the drives available)

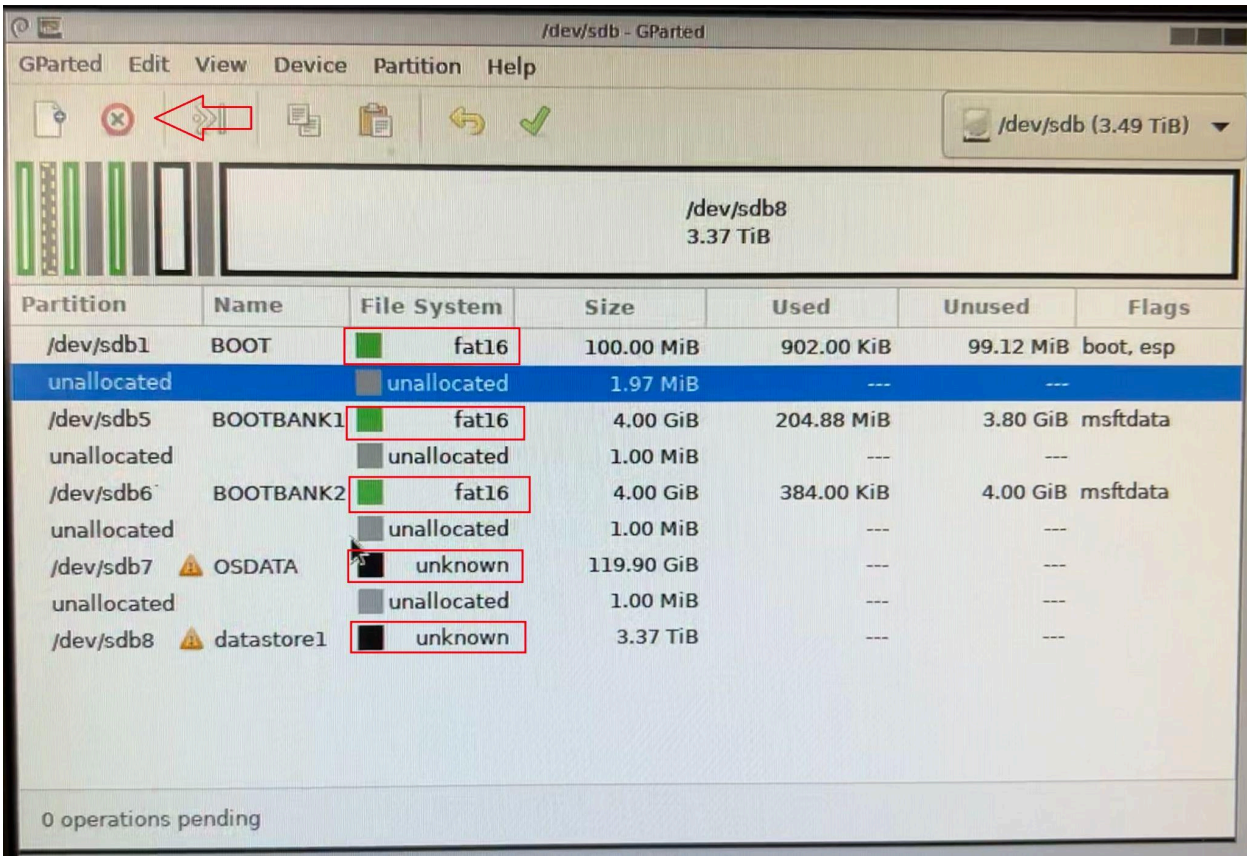


-Note DO NOT DELETE IT

-Note the media you are booting from will likely be the last partition

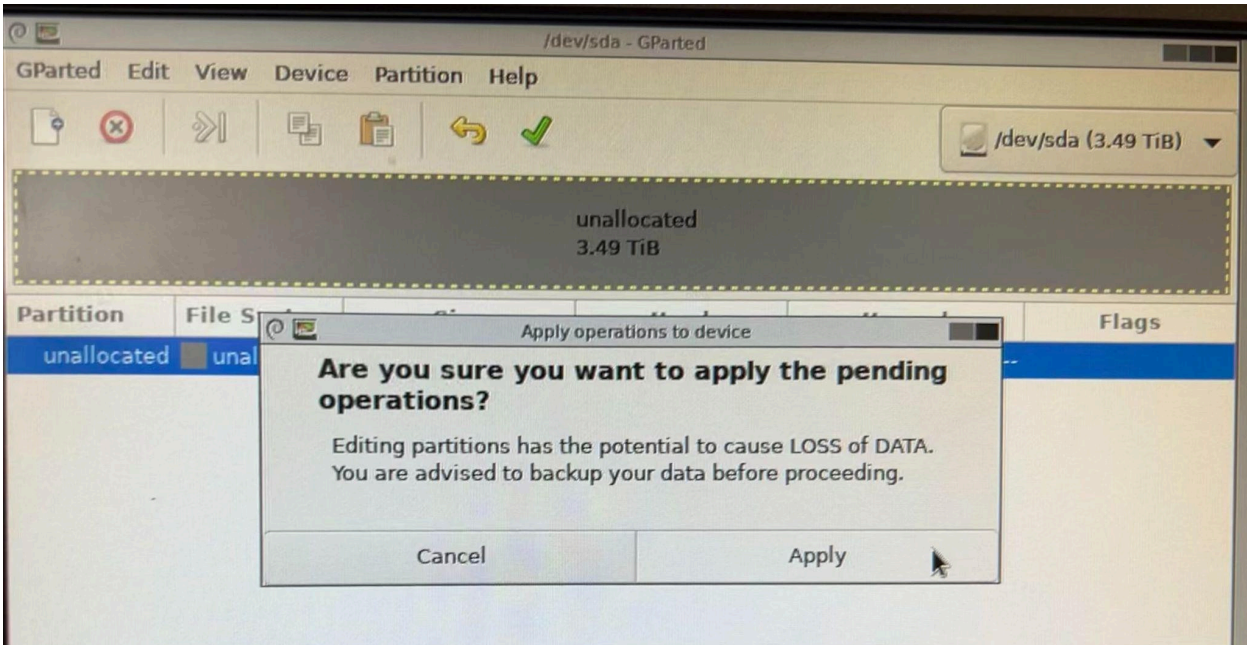
- For each of the partitions click the name of the partition and click on the X with the red circle around it

-Do it for each of the drives/partitions

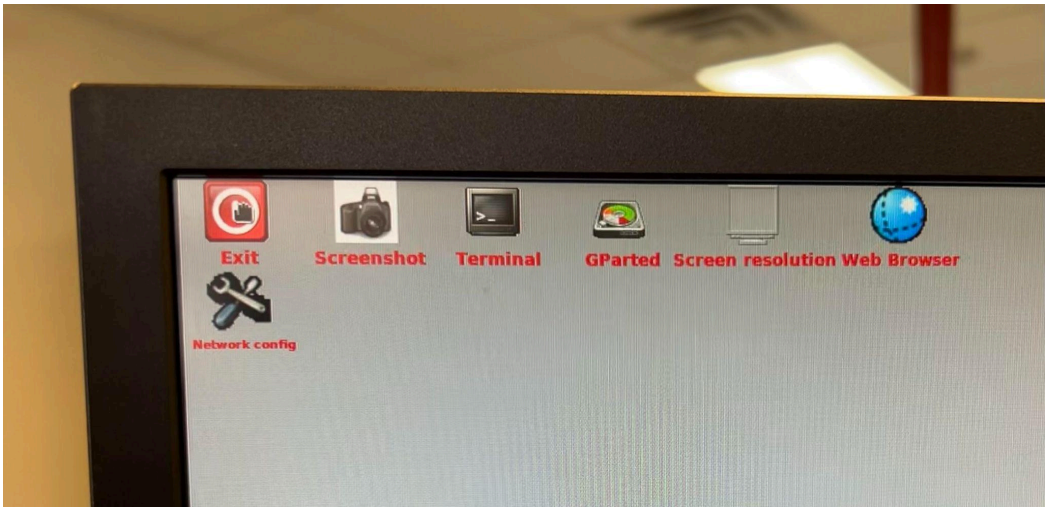


- When done there should only be unallocated space in the middle pane
- Click the green check mark

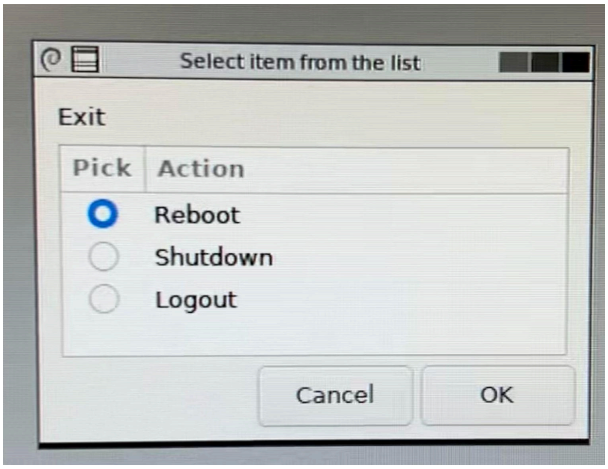
- Click apply



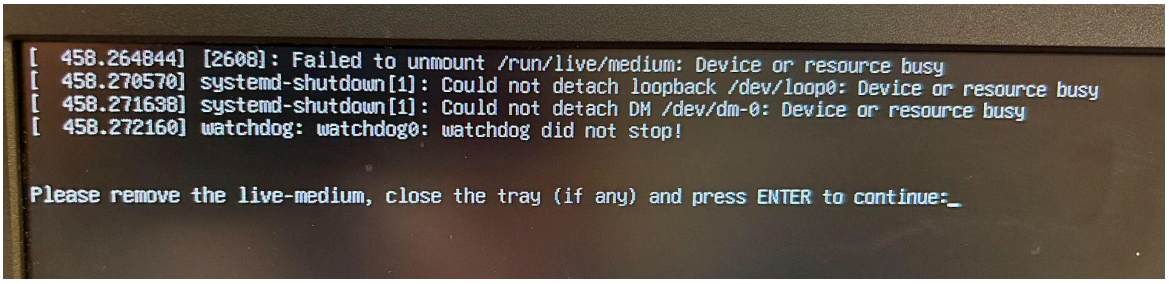
- Click close on the popup
- Click the dark gray box in the top right to close the Gparted application
- Click the Exit button in the top left to exit Gparted
- Double click ONCE (This will take time) *if nothing happens after about 30 seconds, try again.



- When the pop up appears select reboot and select ok

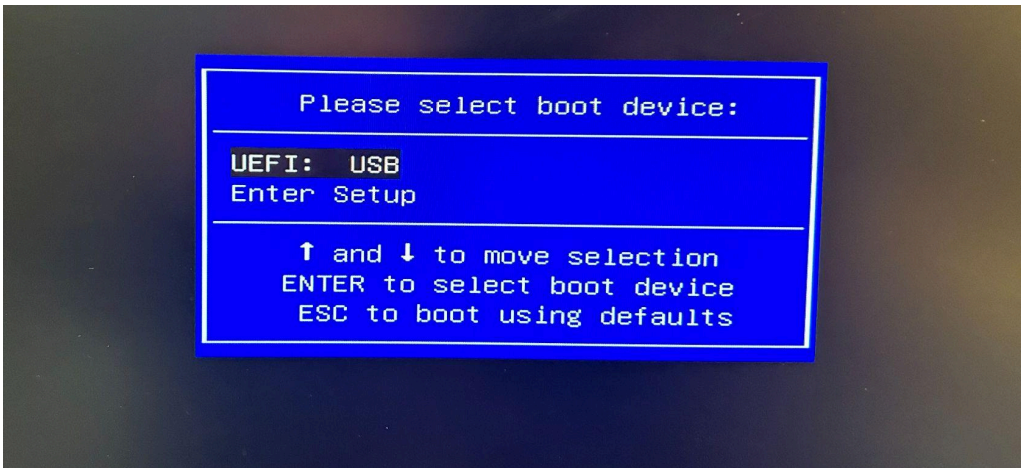


- While rebooting swap the keyboard and mouse
- REMOVE media (USB drive) and then press enter



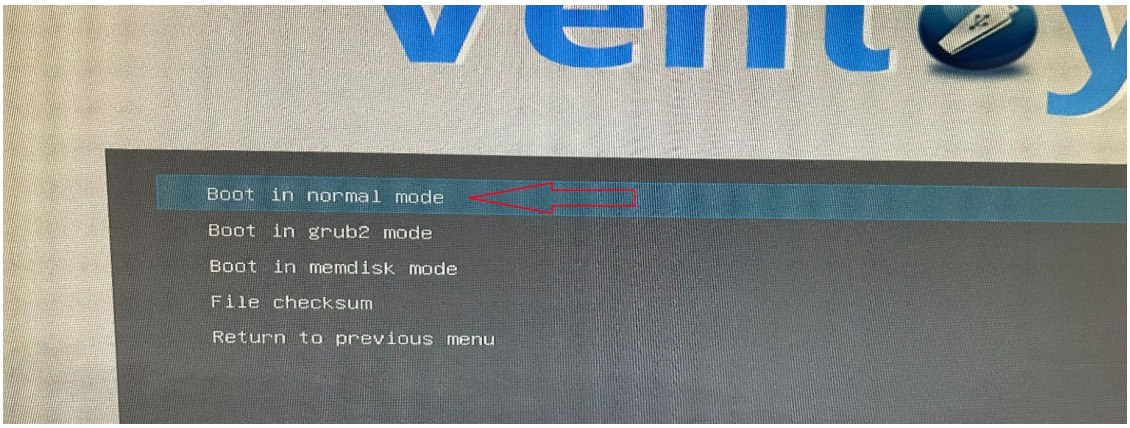
The next step is to install ESXI on the freshly wiped drives:

- Plug media (USB drive) back in
- Press F11 and invoke the boot menu
- Enter BIOS Password
- Boot from USB

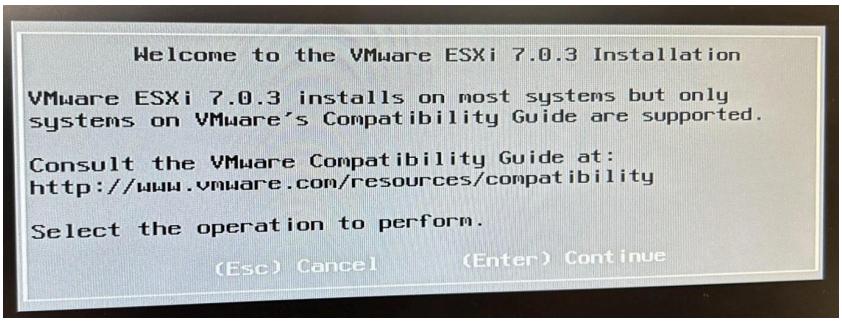


- In Ventoy GUI down arrow to the "VMware-VMvisor-Installer*"
  -select this one with the ENTER key

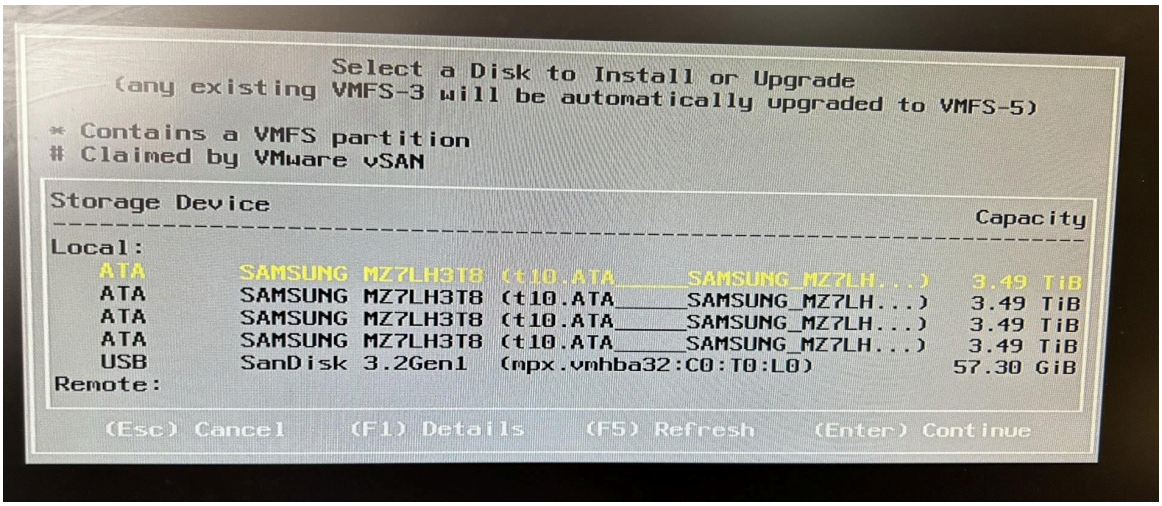
- Normal Mode



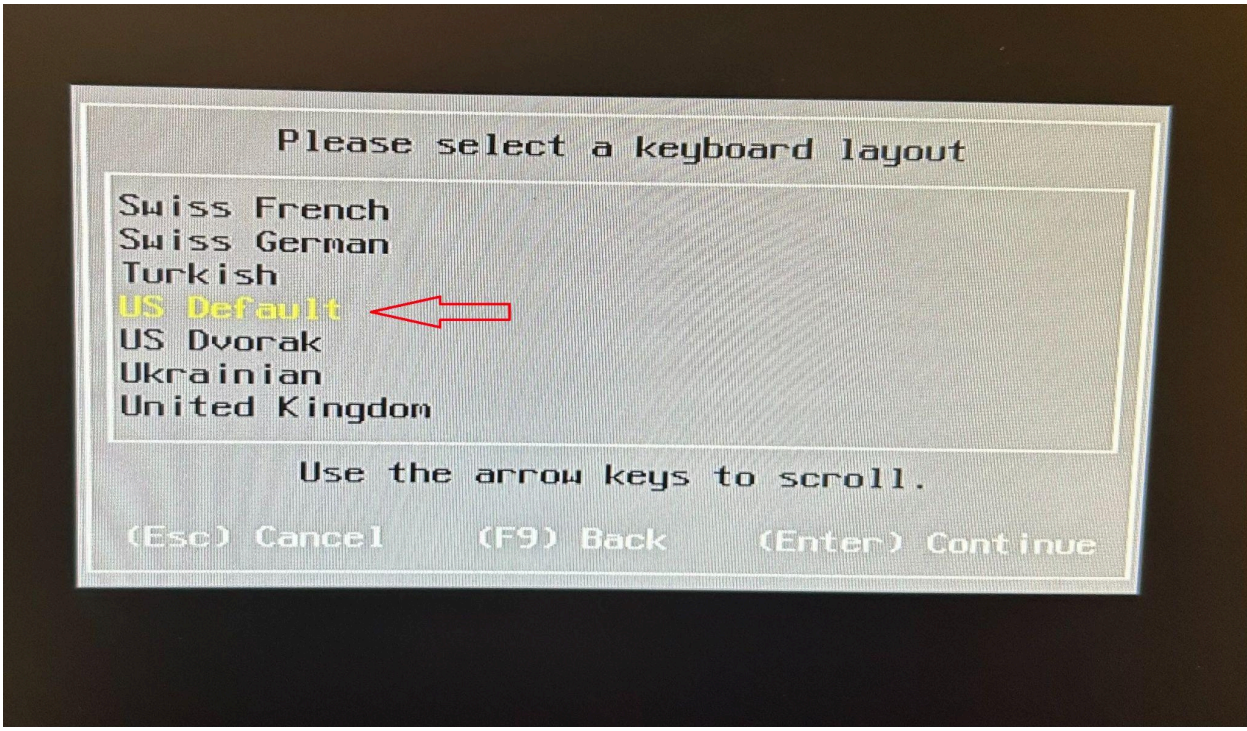
- ESXI Loader might take a couple minutes to load
- Press ENTER once prompted after loading continues



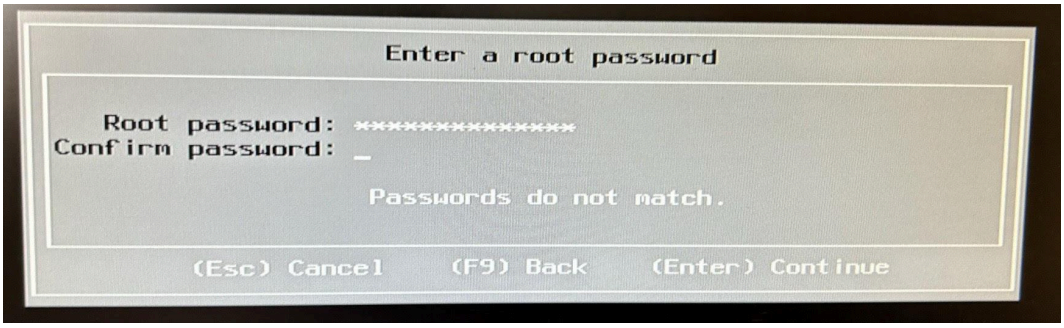
- Press F11 to accept and continue
- Select the the first option for storage location



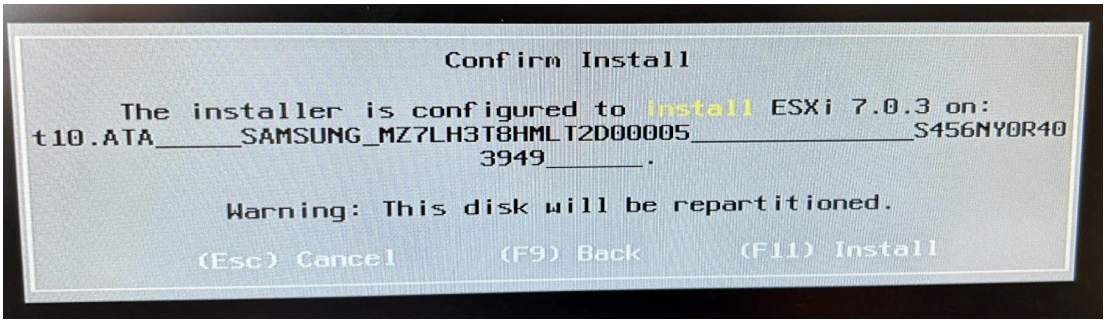
- Select US Default for keyboard layout



- Create Root Password and use down arrow to confirm password and then press ENTER

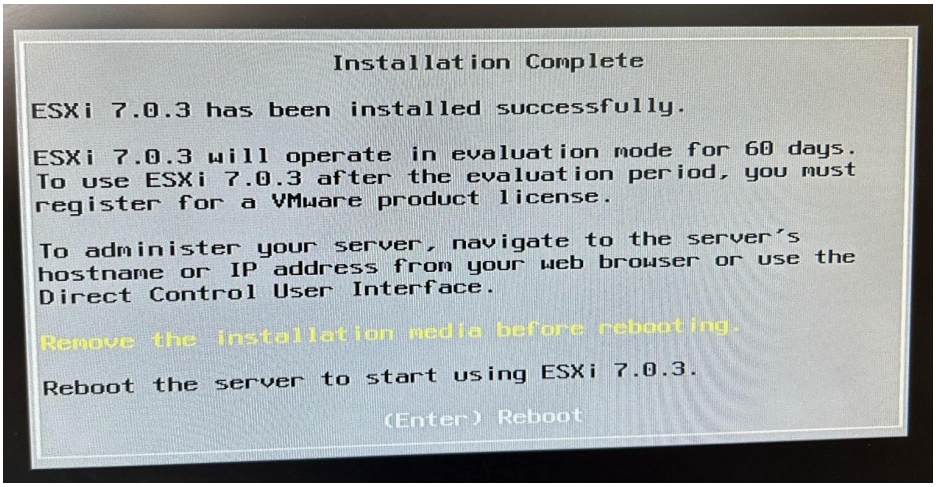


- Press F11 for install



- When Finished
- REMOVE THE FLASH MEDIA

- Press ENTER to Reboot

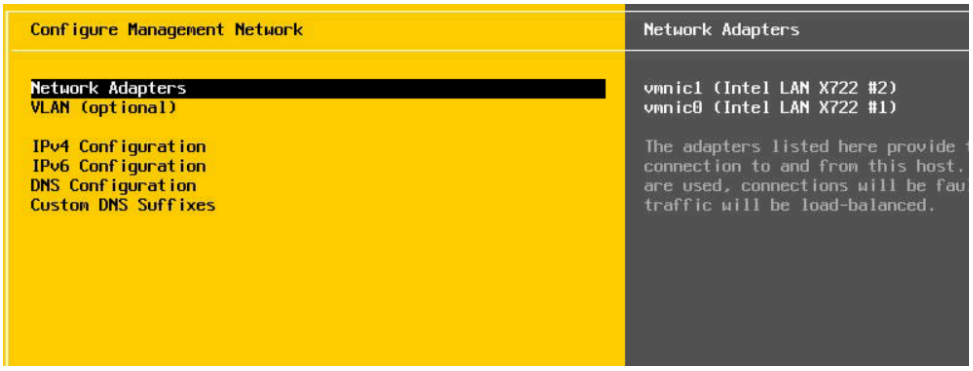


- Press F11 once rebooted
- Enter the BIOS Password
- Boot from VMWARE ESXI

ESXI CONFIGURATION

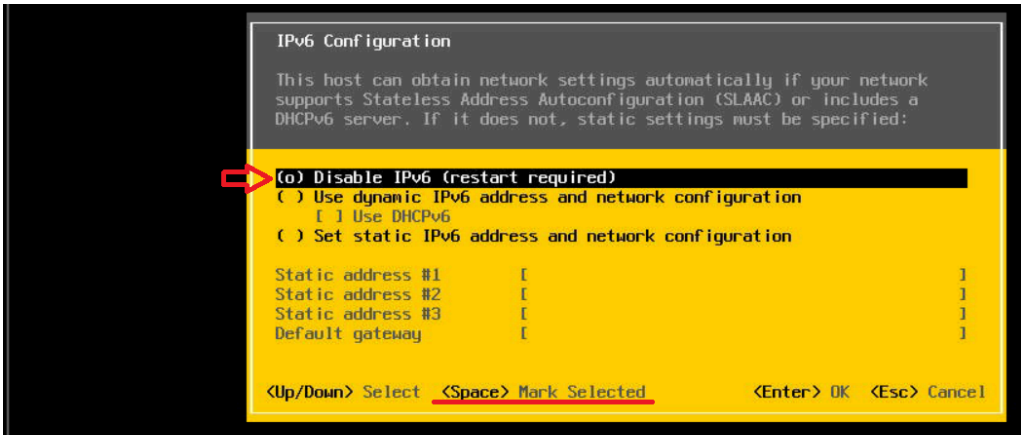
- Hit F2 to go to the configure management network
- Use down arrow to enter password
- Use down arrow to scroll down to configure management network

- Press ENTER
- IPv4 Configuration



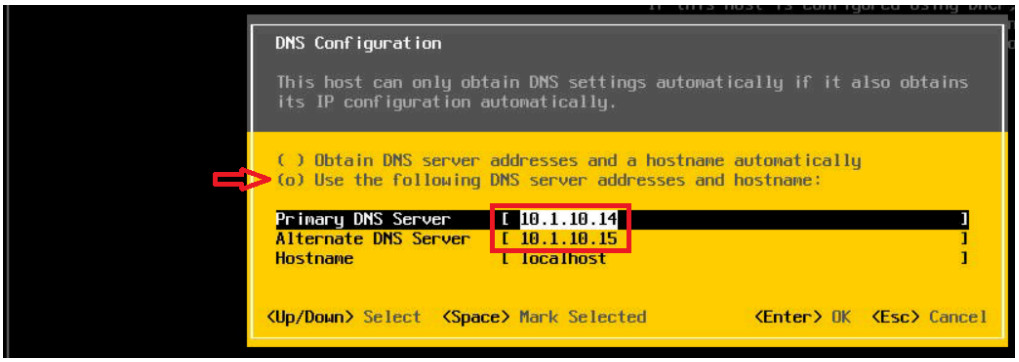
- Press ENTER
- Set Static IPv4 with SPACE
- Set up IPv4 address (10.1.5.11) , subnet mask (255.255.255.0), and default gateway (10.1.5.1)
- Press ENTER to confirm

- Scroll down to IPv6 configuration
- Press ENTER
- Disable IPv6 by pressing SPACE
- Press enter to confirm

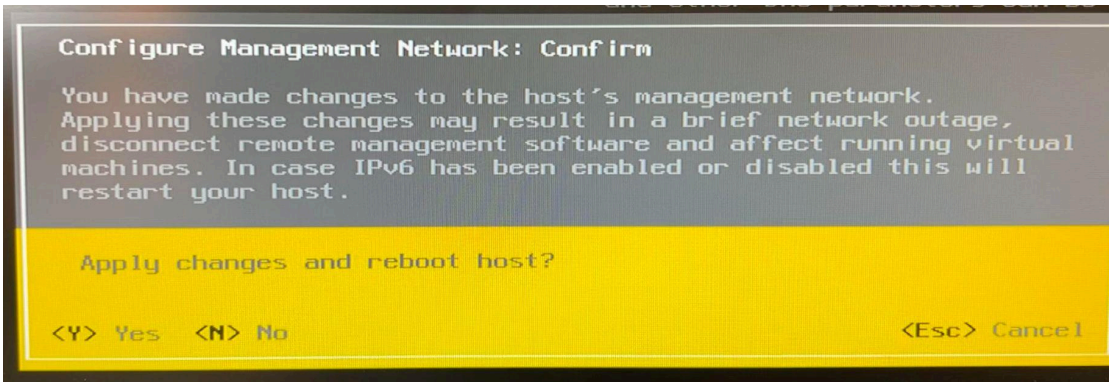


- Scroll down to DNS configuration and press ENTER to select
- Use down arrow to select “use the following DNS server address and hostname and press SPACE to select
- Set Primary DNS to 10.1.10.14 and Alternate 10.1.10.15

➢ Press ENTER to confirm



➢ Press ESC then press Y to save changes and reboot



➢

ESXI Networking Configuration Set-Up

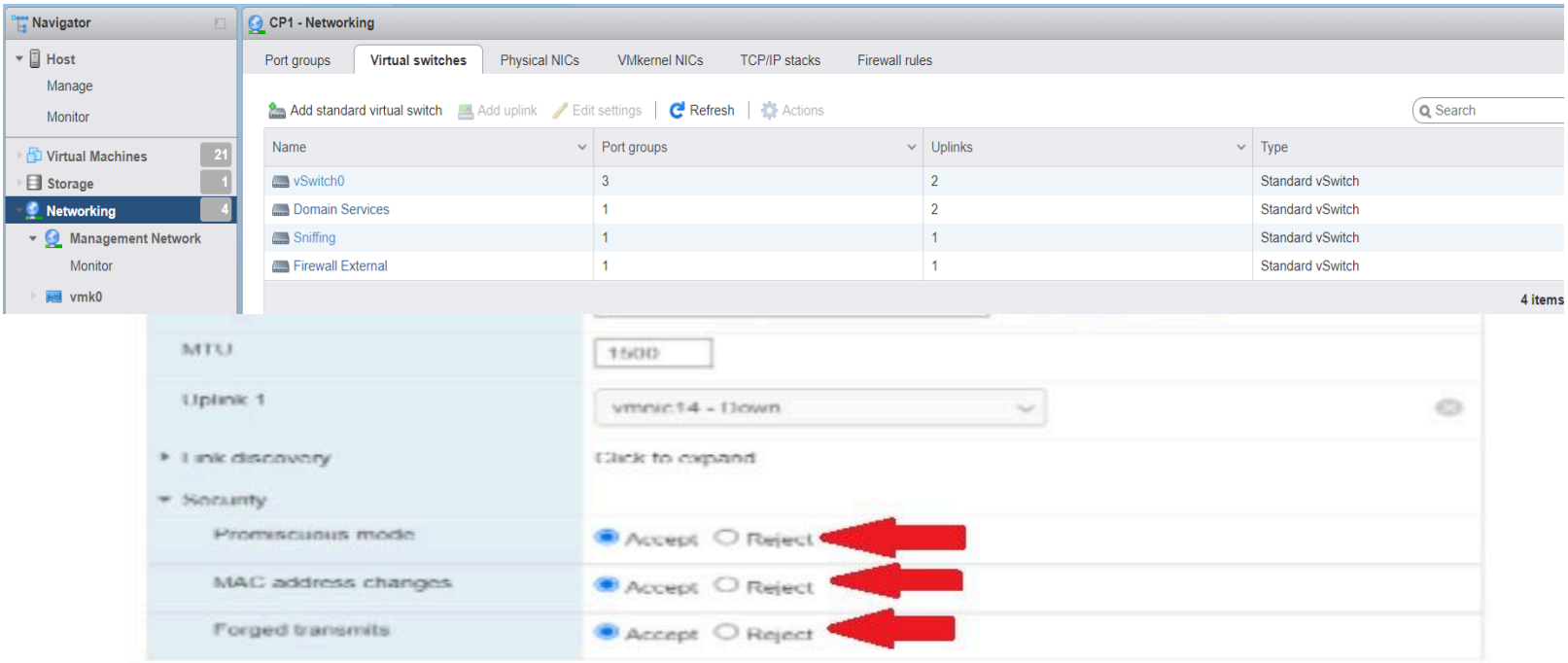
By: Cpl Uptmor, Connor

This section will serve as the guide to configuring the networking on ESXi.

VSwitching

- To create a virtual switch in ESXi you will click on the networking tab and then **Virtual Switches.**
- Once you are on this page you will click Add Standard Virtual Switch to create a vswitch.
- When you are creating the vswitch you will only need to name it and click accept for everything in the security tab, that is it.

- You will have to create three total vswitches for a deployment of the kit.
  - One for domain services (for all of your tools and domain controllers to talk to each other, and for your analyst laptops to talk to the tools).
  - One for the span port (sniffing).
  - One for the external interface of the firewall.



Port Groups

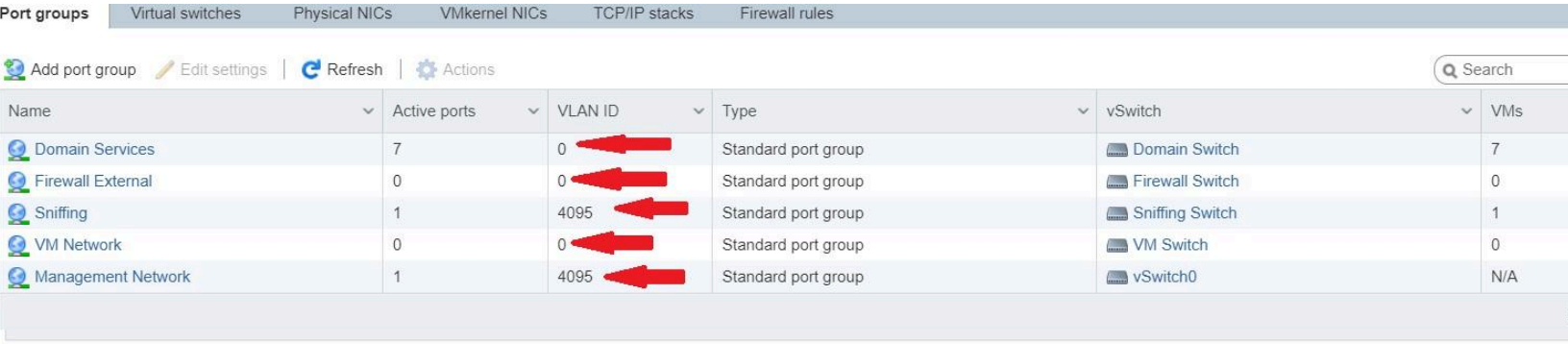
- You need to create port groups in order enable a VM to communicate to a vswitch. When you create a port group you will assign it to a vswitch.

- Port groups are what you assign to Virtual Machines so they can communicate. I would recommend naming your port groups and vswitches the same thing so there's no confusion.
  - Example:
    Portgroup: Domain services
    Vswitch: Domain Services

- The domain services port group and vswitch, the firewall external port group and vswitch can have a **vlan id of 0** which is the vlan of the user ports.

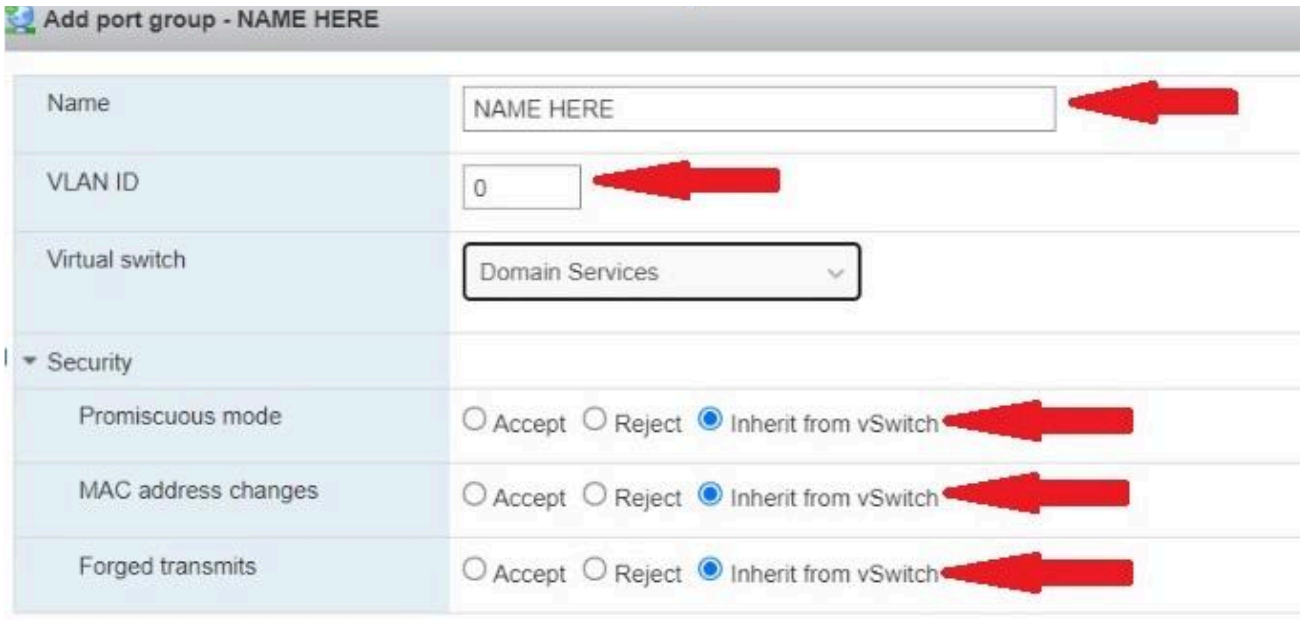
- The management (already configured) port group and vswitch and the sniffing port group and vswitch ***NEED to have a vlan id of 4095 because the sniffing interface needs to***

allow all vlans to capture all of the traffic. Also set the port group to promiscuous mode to allow all types of network traffic.



Name	Active ports	VLAN ID	Type	vSwitch	VMs
Domain Services	7	0	Standard port group	Domain Switch	7
Firewall External	0	0	Standard port group	Firewall Switch	0
Sniffing	1	4095	Standard port group	Sniffing Switch	1
VM Network	0	0	Standard port group	VM Switch	0
Management Network	1	4095	Standard port group	vSwitch0	N/A

- To make a port group you will click on the port groups tab in networking and click add port group.
- From here you will select which vswitch you would like to put it on and also what vlan ID. In the security tab leave everything as ***Inherit from vswitch.***



****NOTE**:** When working with a CyberPak, having unnecessary physical connections (vmnics) connecting to the Management vSwitch will confuse the Pak. In the event of unexplained connection loss, disconnect all cables and reconnect only the bare necessities.

Domain Services

Domain Services

Type:	Standard vSwitch
Port groups:	1
Uplinks:	1

⚠ This virtual switch has no uplink redundancy. You should add another uplink adapter. Actions

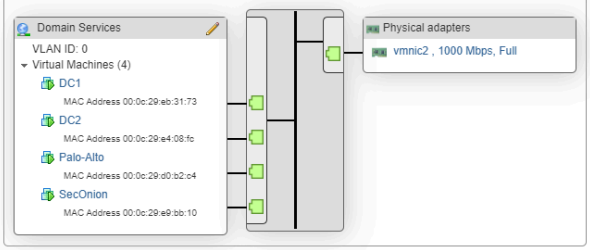
vSwitch Details

MTU	1500
Ports	9216 (9182 available)
Link discovery	Listen / Cisco discovery protocol (CDP)
Attached VMs	4 (4 active)
Beacon interval	1

NIC teaming policy

Notify switches	Yes
Policy	Route based on originating port ID
Reverse policy	Yes
Failback	Yes

vSwitch topology



Firewall External

Add uplink | Edit settings | Refresh | Actions

Firewall External

Type:	Standard vSwitch
Port groups:	1
Uplinks:	1

⚠ This virtual switch has no uplink redundancy. You should add another uplink adapter. Actions

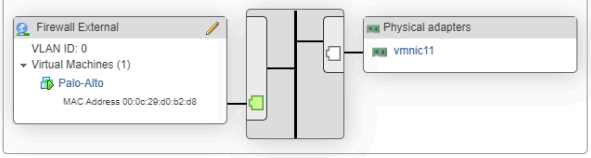
vSwitch Details

MTU	1500
Ports	9216 (9182 available)
Link discovery	Listen / Cisco discovery protocol (CDP)
Attached VMs	1 (1 active)
Beacon interval	1

NIC teaming policy

Notify switches	Yes

vSwitch topology



Sniffing

Add uplink | Edit settings | Refresh | Actions

Sniffing

Type:	Standard vSwitch
Port groups:	1
Uplinks:	1

⚠ This virtual switch has no uplink redundancy. You should add another uplink adapter. Actions

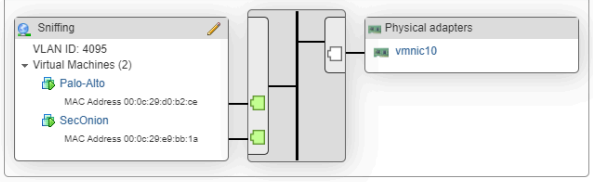
vSwitch Details

MTU	1500
Ports	9216 (9182 available)
Link discovery	Listen / Cisco discovery protocol (CDP)
Attached VMs	2 (2 active)
Beacon interval	1

NIC teaming policy

Notify switches	Yes

vSwitch topology



vSwitch0

Add uplink | Edit settings | Refresh | Actions

vSwitch0

Type:	Standard vSwitch
Port groups:	2
Uplinks:	2

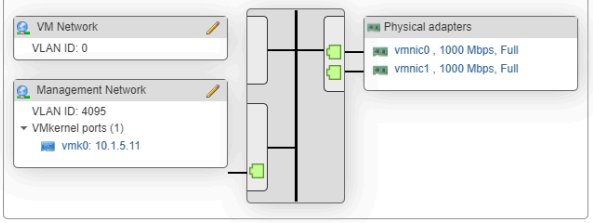
vSwitch Details

MTU	1500
Ports	9216 (9182 available)
Link discovery	Listen / Cisco discovery protocol (CDP)
Attached VMs	0 (0 active)
Beacon interval	1

NIC teaming policy

Notify switches	Yes
Policy	Route based on originating port ID
Reverse policy	Yes

vSwitch topology



Configuring IPMI

- Power On MiniRax
  - Press F11 to enter boot Menu
  - Select Enter Setup
  - Navigate to the IPMI tab
  - BMC Network Configuration
  - Update IPMI LAN Configuration set to ‘Yes’
  - Station IP Address set to ‘10.1.5.12’
  - Subnet Mask set to ‘255.255.0.0’
  - Gateway IP Address set to ‘10.1.5.1’
  - Press F4 to Save and quit