Arkime S.O.P.

By: Cpl Harkleroad, LCpl Frost, LCpl Dorsey
Cpl Smucketelli
3rd PLT DCO-IDM
LU: 2023xxxx

This document will serve as the guide to Arkime installatio

n and usage for operations.

Arkime Overview

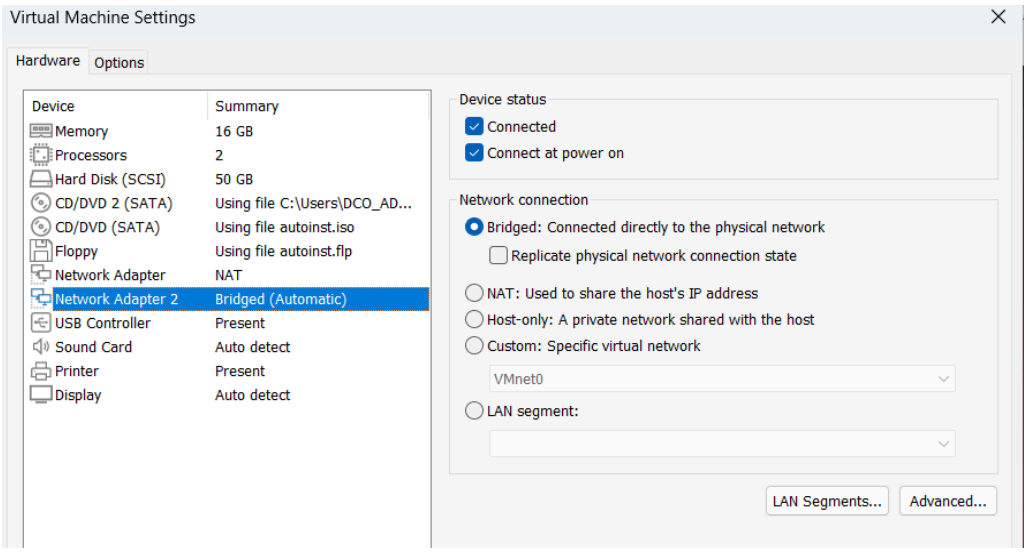
Arkime is a large-scale, open-source, indexed packet capture and search tool that indexes the PCAP data it collects. Arkime also comes with a web frontend for browsing and searching through the captured, and indexed, network traffic.

Arkime Installation

By: Cpl Harkleroad, Grant
3rd PLT DCO-IDM
LU: 20231016

- Download an Ubuntu 22.04 Desktop iso onto the workstation
- Acquire external workstation NIC
- **NOTE:** You cannot move on without these two things

- Open VMware Workstation Pro application to set up the VM.
- Select 'Create a New Virtual Machine'
- Select Typical
- Under Installer disc image, select the above iso -> Next
- Personalize Linux
  - Full Name: Admin
  - User Name: admin
  - Password: [shop_standard]
- Virtual Machine Name: Arkime
- Maximum Disc Size (GB): 50
- Split into multiple files
- Customize Hardware:
  - Memory: 16GB
  - Add -> Network Adapter -> bridged
  - Close
- Finish



- Allow time for Install

IMPORTANT There needs to be 2 VNICS on the virtual machine. The first one is for internet or internal network connection and the second will be bridged. Adding VNICS can be done in set up or after the VM is already made.

- Select Minimal Installation
- Erase disk and install Ubuntu
- Install Now
- Write changes to disk: continue
- Who are you?
  - Your name: DCO
  - Your computer's name: admin-virtual-machine
  - Pick a username: admin
  - Password: [shop_standard]
  - Require my password to login
  - Continue

- Allow time for installation
- If prompted for system info, select 'No, do not send system info'

Before and after installing new software always check for updates:

- Open terminal
  - Sudo apt update
  - Allow time for download
- This step requires internet connection

***** VERY IMPORTANT *****
Gparted needs to be downloaded using the following command:

- Sudo apt install gparted -y

Next will be the install of elasticstack:

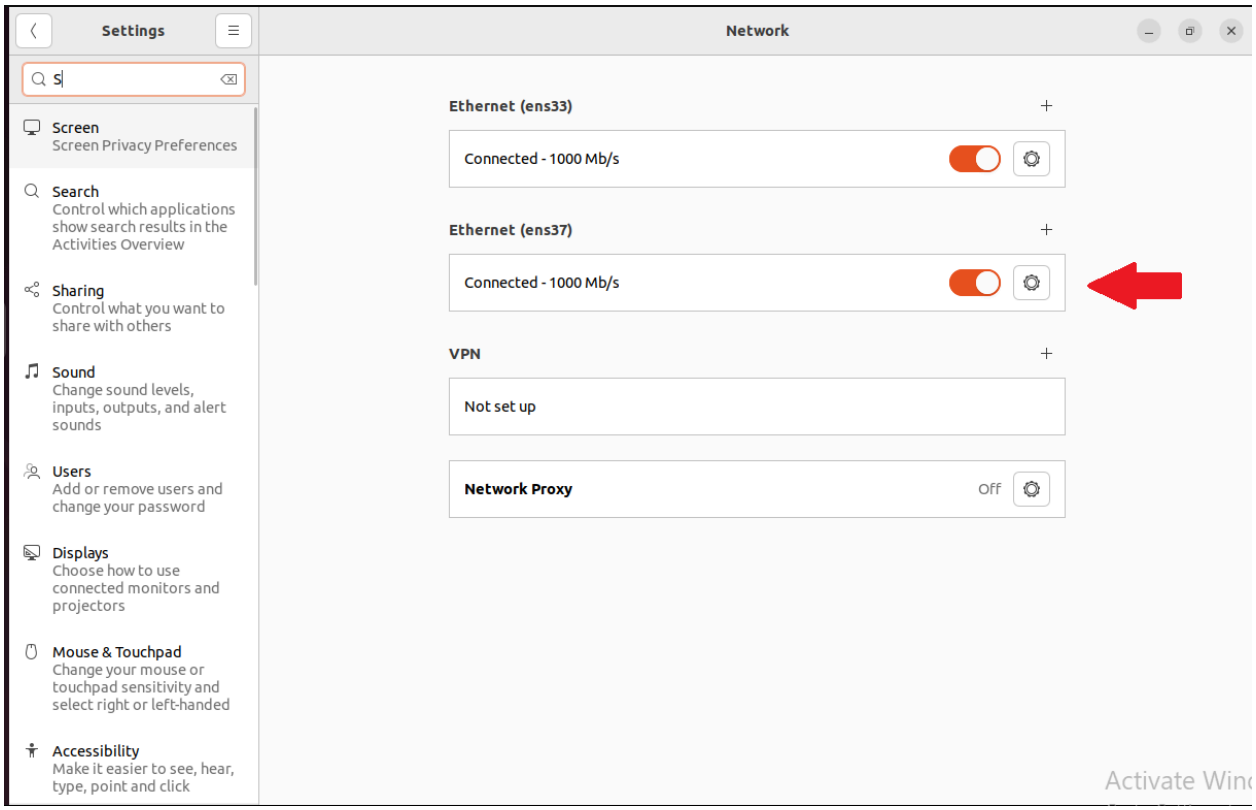
- sudo su (make yourself root)

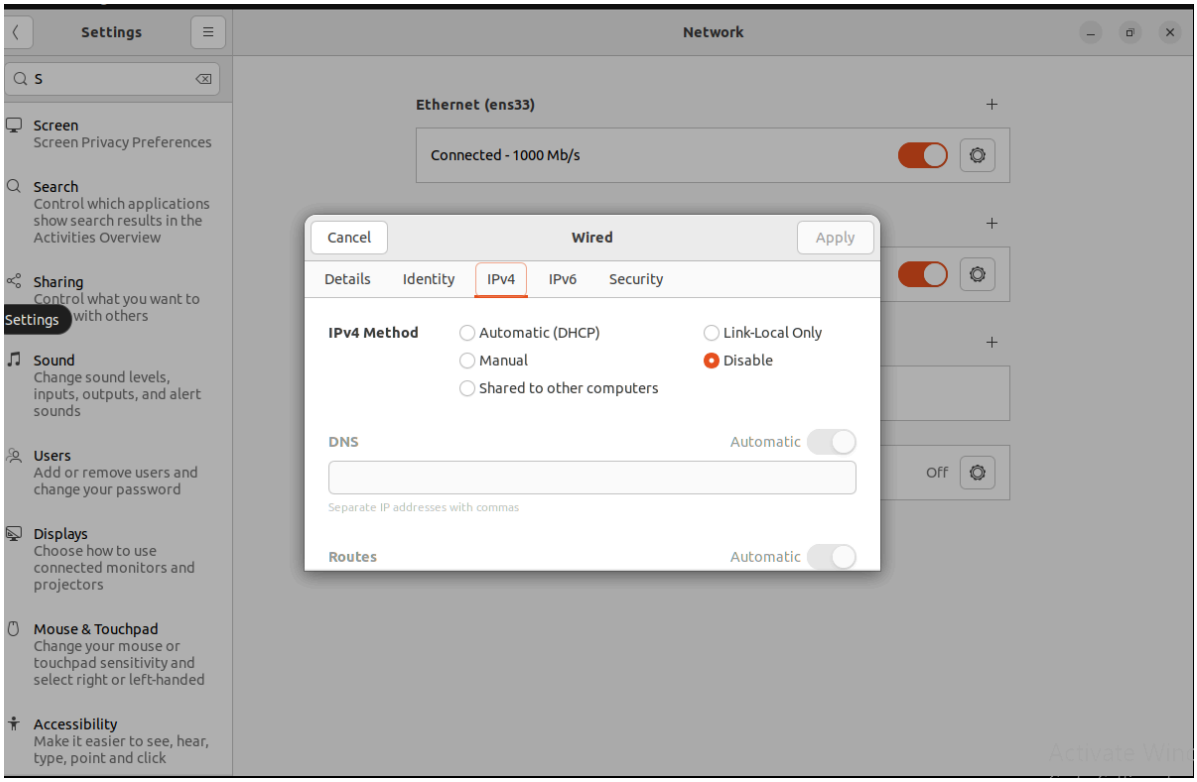
  - wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch --no-check-certificate \
    | sudo gpg --dearmor > /etc/apt/trusted.gpg.d/elastic.gpg
  - This step requires internet connection

- ➢ echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" \
  | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list

- ❖ Exit back to your original user:
  - ➢ sudo apt update
  - ➢ sudo apt install elasticsearch
  - ➢ This step requires internet connection

On your VM. Click on the top right on the network and select the SECOND interface(the one ingesting traffic). Select wired settings and then click on the edit. On the IPv4 and IPv6 tabs change the method to disable. Apply these settings and turn the interface off and back on. Check in the terminal using command: ip a to see if the interface no longer has an ip associated with it.





- Now to start elasticsearch.service and make it start up automatically on reboot by running the command:
  - sudo systemctl enable --now elasticsearch

- Check the service started by running a command to see the listening port:
  - ss -antpl | grep 9200

  - **OUTPUT:**
  - LISTEN 0 4096 [::ffff:127.0.0.1]:9200 *:*
  - LISTEN 0 4096 [::1]:9200 [::]:*

- Install Arkime 4.6 by using the command: **(Note** that it is always best to check the arkime website and make sure you are getting the most up to date version)
  - wget https://github.com/arkime/arkime/releases/download/v5.0.1/arkime_5.0.1-1.ubuntu2204_amd64.deb
  - This step requires internet connection

- This will download to the user's home directory. It needs to be run from the /tmp directory. Move the .deb to the /tmp directory using:
  - mv $HOME/arkime_5.0.1-1.ubuntu2204_amd64.deb /tmp

- Move to the /tmp directory and give the .deb full permissions:
  - cd /tmp
  - chmod 777 arkime_5.0.1-1.ubuntu2204_amd64.deb

- Run the command to install Arkime:
  - sudo apt install ./arkime_5.0.1-1.ubuntu2204_amd64.deb
  - This step requires internet connection

Configuration

- Next Arkime needs to be configured:
  - sudo apt update -y
  - sudo /opt/arkime/bin/Configure

  <enter the interface you are going to be capturing on, most likely ens34>
  - No

  <hit enter>
  - Standard password
  - yes

- For first install run this command to be able to make a user:
  - sudo /opt/arkime/db/db.pl http://localhost:9200 init

- Make a new Arkime user:
  - sudo /opt/arkime/bin/arkime_add_user.sh admin "Admin User" <password with no special characters> --admin

- Start the Arkime services:
  - sudo systemctl enable --now arkimecapture
  - sudo systemctl enable --now arkimeviewer

Capture service sometimes doesn't work right away. Sometimes you need to stop and then start it for it to work. If the capture service fails to start multiple times. check the capture.log in /opt/arkime/logs/capture.log for a reason for the failure. There may be a script you will have to run.

Now we are going to edit the service files of the viewer and capture to make sure elasticsearch is running before the Arkime services start:

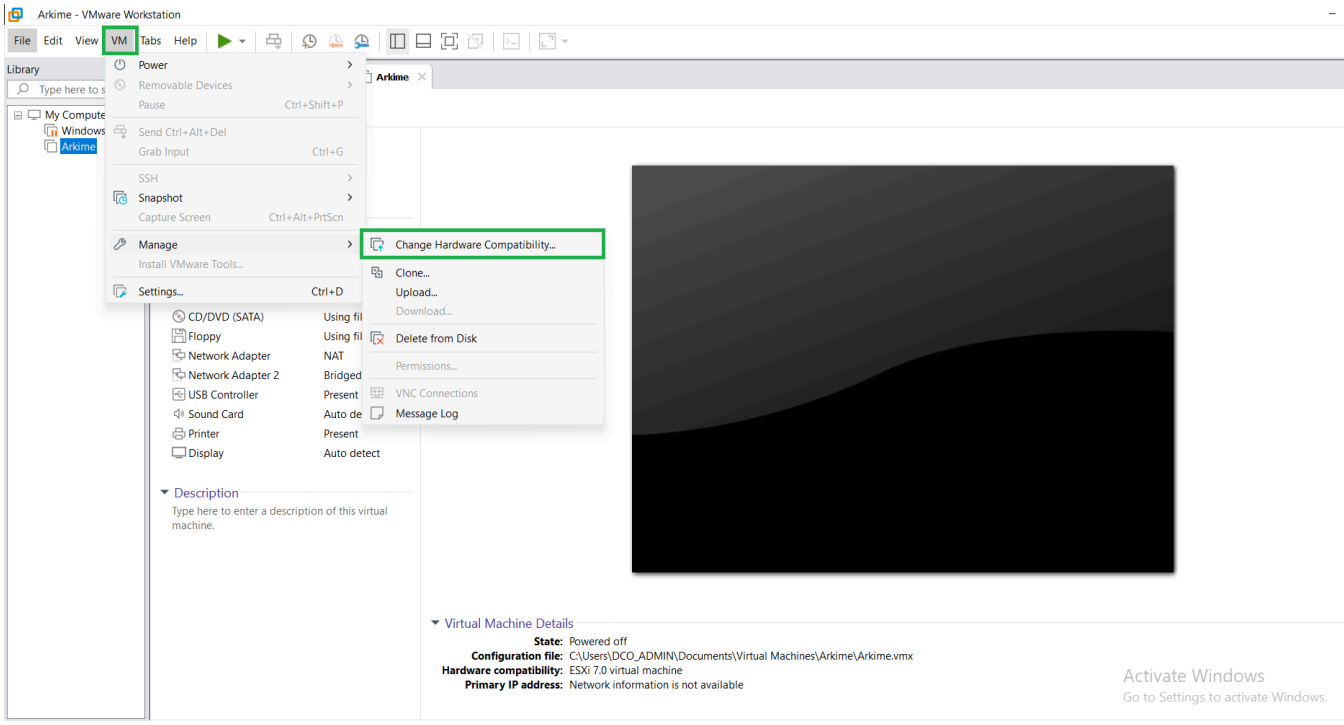
- sudo sed -i 's/network.target/network.target elasticsearch.service/' /etc/systemd/system/arkimecapture.service /etc/systemd/system/arkimeviewer.service

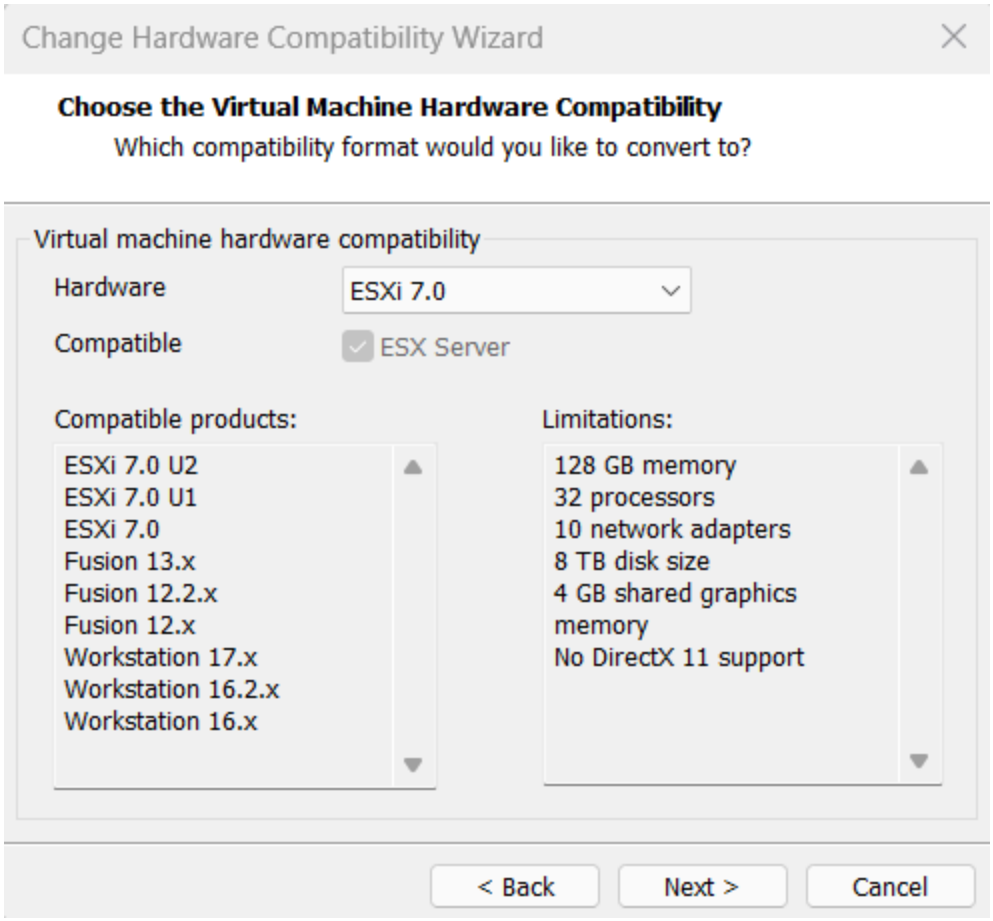
- sudo sed -i '/After=/a Requires=network.target elasticsearch.service' /etc/systemd/system/arkimecapture.service /etc/systemd/system/arkimeviewer.service

- Now reload the daemons:
  - sudo systemctl daemon-reload

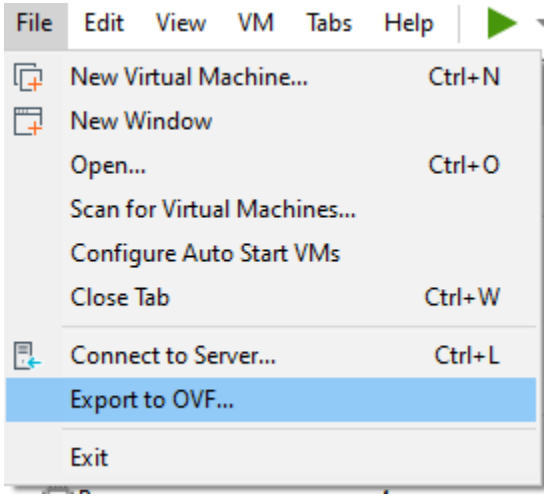
- may have to stop and start the services manually to make sure they start again properly.

- Power off VM, click on “VM” tab up top when VM is fully powered off. In drop down, Manage -> Change Hardware Compatibility -> ESXi 7.0 -> Alter this machine

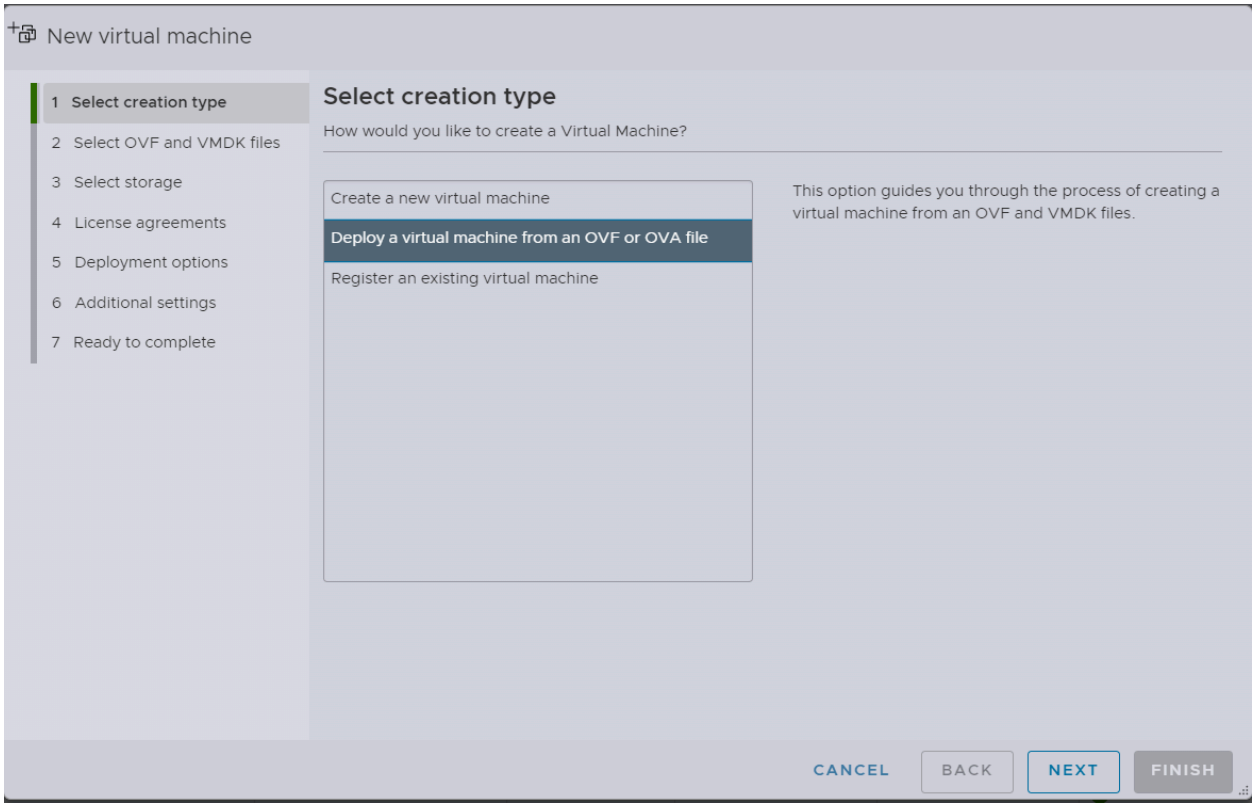


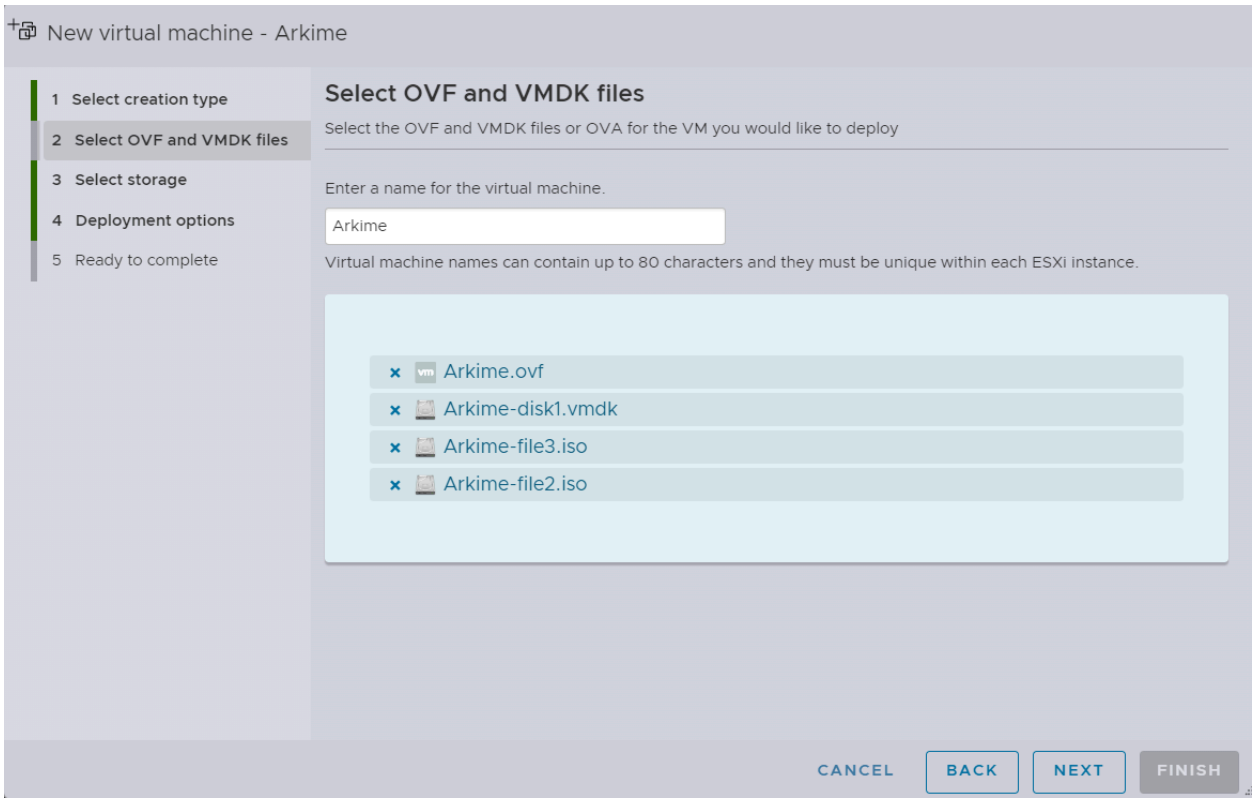


- File -> Export to OVF



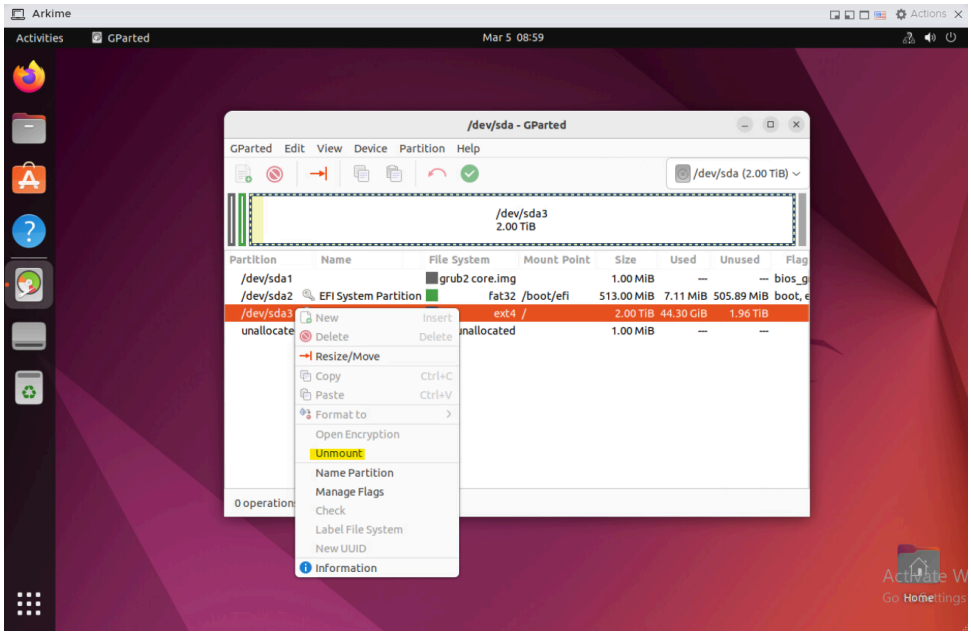
- On ESXI, create a VM from the OVF file



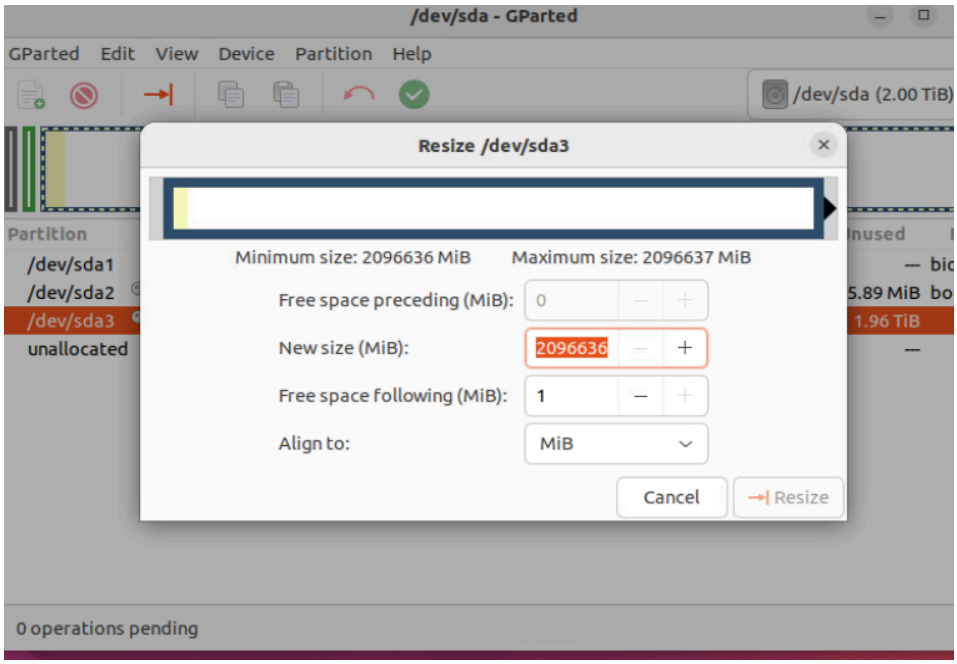


- Once VM is built on ESXi 7.0, edit the VM to have 2 TB disk storage.

- Log in and restart the Arkime VM.
- Top right, right click on Ethernet (ens34) Connected > Wired Settings
- Click on gear next to ens34, manually assign IP 10.1.10.80 255.255.255.0
- Open GParted and unmount /dev/sda3, ignore any errors that populate



- Right click /dev/sda3 and select Resize/Move, drag bar to allocate all available space to /dev/sda3



- Open mozilla, navigate to localhost:8005 and log in with admin/standard