



Arkime S.O.P. <u>By: Cpl Harkleroad, LCpl Frost, LCpl Dorsey</u> <u>Cpl Smucketelli</u> <u>3rd PLT DCO-IDM</u> <u>LU: 2023xxxx</u>

This document will serve as the guide to Arkime installatio

n and usage for operations.

Arkime Overview	1
Arkime Installation	2
Configuration	7
Arkime Baselining	9
Arkime Use Cases	10

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

<u>By: Cpl Harkleroad, Grant</u> <u>3rd PLT DCO-IDM</u> <u>LU: 20231016</u>

- 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

		Device status
Device	Summary	
🛒 Memory	16 GB	Connected
Processors	2	Connect at power on
Hard Disk (SCSI)	50 GB	
🖲 CD/DVD 2 (SATA)	Using file C:\Users\DCO_AD	Network connection
OCD/DVD (SATA)	Using file autoinst.iso	O Bridged: Connected directly to the physical network
Floppy	Using file autoinst.flp	Replicate physical network connection state
Network Adapter	NAT	
中 Network Adapter 2	Bridged (Automatic)	NAT: Used to share the host's IP address
- USB Controller	Present	O Host-only: A private network shared with the host
(1) Sound Card	Auto detect	Custom: Specific virtual network
Printer	Present	VMnet0 ~
Display	Auto detect	O LAN segment:
		~





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.

\langle	Settings =	Network	- @ ×
С	s 🛛	Ethernet (ess3)	
Ţ	Screen Screen Privacy Preferences	Connected - 1000 Mb/s	
Q	Search Control which applications show search results in the Activities Overview	Ethernet (ens37) +	
Ś	Sharing Control what you want to	Connected - 1000 Mb/s	
n	Sound Change sound levels, inputs, outputs, and alert sounds	VPN + Not set up	
2	Users Add or remove users and change your password	Network Proxy Off	
A	Displays Choose how to use connected monitors and projectors		
O	Mouse & Touchpad Change your mouse or touchpad sensitivity and select right or left-handed		
Ť	Accessibility Make it easier to see, hear, type, point and click		Activate Wind

< Settings		Network	- @ ×
Q S		Ethernet (ans 33)	+
Screen Screen Privacy Prefer	rences	Connected - 1000 Mb/s	0
Q Search			
show search results in Activities Overview	n the	Cancel Wired Apply	+
Sharing	atto	Details Identity IPv4 IPv6 Security	٥
Settings with others		IPv4 Method O Automatic (DHCP) O Link-Local Only	+
Sound Change sound levels, inputs, outputs, and sounds	alert	Manual Shared to other computers	
© Users		DNS Automatic	
Add or remove users change your passwor	and	Separate IP addresses with commas	0
Displays Choose how to use connected monitors projectors	and	Routes Automatic	
Mouse & Touchpad Change your mouse of			

- 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

\succ	OUTPUT:				
≻	LISTEN 0	4096	[::ffff:127.0.0.1]:9200		*.*
\succ	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







Change Hardware Compatibility Wizard

Choose the Virtual Machine Hardware Compatibility

Which compatibility format would you like to convert to?

Virtual machine hardware	compatibility		
Hardware	ESXi 7.0	~	
Compatible	ESX Sen	ver	
Compatible products:		Limitations:	
ESXi 7.0 U2 ESXi 7.0 U1 ESXi 7.0 Fusion 13.x Fusion 12.2.x Fusion 12.x Workstation 17.x Workstation 16.2.x Workstation 16.x	•	128 GB memory 32 processors 10 network adapters 8 TB disk size 4 GB shared graphics memory No DirectX 11 support	
			Ψ
		< Back Next >	Cancel

✤ File -> Export to OVF





On ESXI, create a VM from the OVF file



+🗗 New virtual machine

	Select creation type				
 Select OVF and VMDK files Select storage License agreements Deployment options Additional settings Ready to complete 	Select creation type How would you like to create a Virtual Machine? Create a new virtual machine Deploy a virtual machine from an OVF or OVA file Register an existing virtual machine	This option guide virtual machine fr	es you through rom an OVF al) the process of nd VMDK files	of creating a
New virtual machine - Arl 1 Select creation type	kime Select OVF and VMDK files Select the OVF and VMDK files or OVA for the VM you	CANCEL	BACK	NEXT	FINISH
3 Select storage4 Deployment options	Enter a name for the virtual machine. Arkime				
5 Ready to complete	Virtual machine names can contain up to 80 characters	and they must be uniqu	ue within each	i ESXi instance	÷.
5 Ready to complete	Virtual machine names can contain up to 80 characters × Arkime.ovf × Arkime-disk1.vmdk × Arkime-file3.iso × Arkime-file2.iso	and they must be uniqu	Je within each	ESXI instance	.

✤ 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

	/dev/sda - G	Parted			0
GParted Edit Vie	ew Device Partition Help				
				/dev/s	sda (2.00 TiB)
	Resize /dev	/sda3		×	
Dartition					Inurod I
/dev/sda1	Minimum size: 2096636 MiB	Aaximum siz	ze: 2096637 M	1iB	bic
/dev/sda2 @	Free space preceding (MiB):	0			5.89 MiB bo
/dev/sda3 G	New size (Mip):	2005626			1.96 TiB
unallocated	New size (MIB):	2090030			-
	Free space following (MiB):	1	°- +		
	Align to:	MiB	~		
			Cancel	→ Resize	
					<i></i>
0 operations pendi	ng				

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