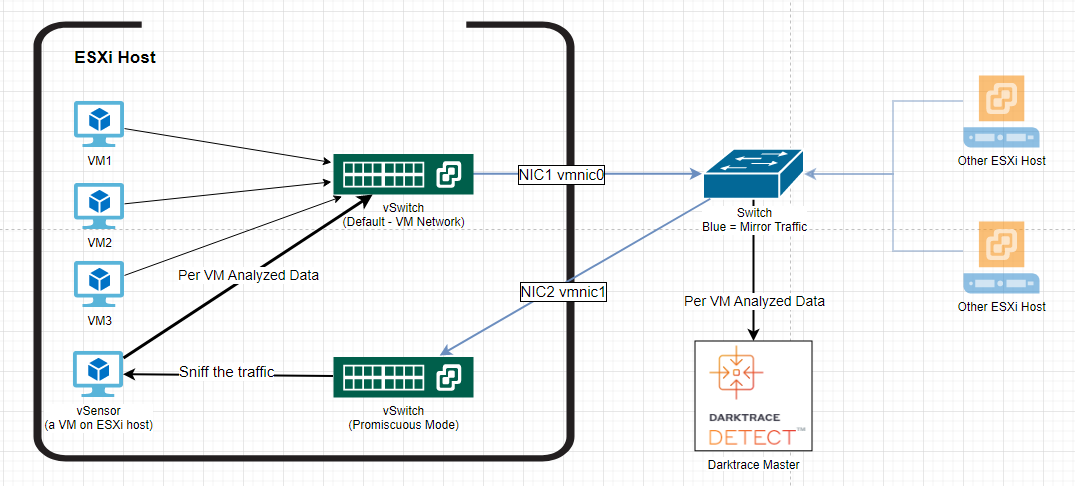
Topology & Roadmap

Thursday, June 1, 2023

4:07 PM

**Topology**



Topology Description:

VM send data to the Physical switch, mirroring back the data to ESXi Host and finally reach vSensor.

vSensor is able to parse the data, making it possible to differentiate different source VMs. Then, such data will be sent to the Darktrace Master's Admin port, and we can view data on its Threat Visualizer.

Static IP is used throughout this tutorial, as we do not have a DHCP server in this environment.

**Roadmap**

1. Prerequisites Checking
   1. Follow the **Cisco Switch Port Mirroring** guide to config port mirroring.
   2. Make sure you have the credentials for accessing Darktrace Console and ThreatVisualizer
2. ESXi host [Page 2]
   1. Plug cables according to topology
   2. Check the connected physical port and create vSwitch accordingly
   3. Install & Config vSensor
3. DarkTrace Master [Page 10]
   1. Plug cables according to topology
   2. Confirm probing
   3. Validate results

**Reference**

<https://portal.darktrace.com/product-guides/main/vsensor-introduction>

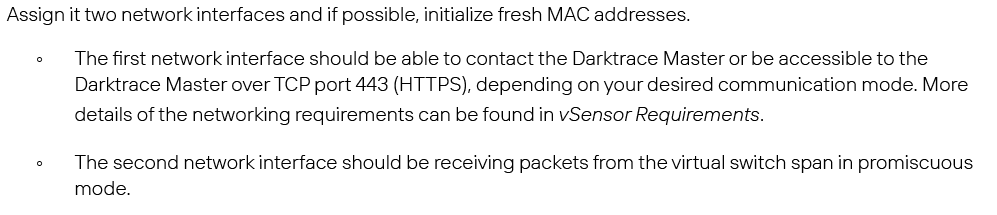
Similar tutorial, but not for Darktrace vSensor. <https://support.vectra.ai/s/article/KB-VS-1075>

Install vSensor & Config vSwitch

Thursday, June 1, 2023

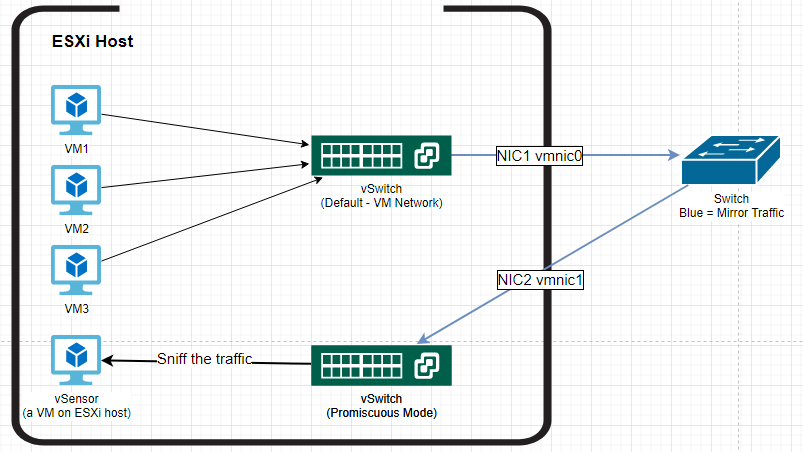
4:08 PM

According to the darktrace guide, we need to have two VM Networks (aka.,Port Groups), corresponding to two vSwitchs for the DarkTrace vSensor.

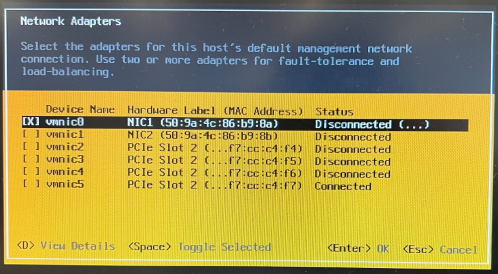


# Connect the ESXi Interface

Connect the ESXi host to the two mirrored Switch ports. In the diagram, ignore the vSwitchs at the moment, we will set them up later.

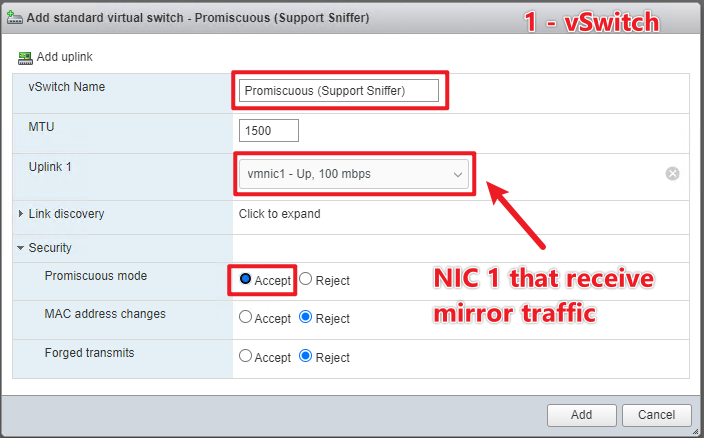


Check the ESXi configuration by plugging VGA to the Dell server and go to F2 ESXi Setup -> Configure Network ->Network Adapters. (Below is just an example of the UI, not the correct setup) You need to get vmnic0 and vmnic1 connected.

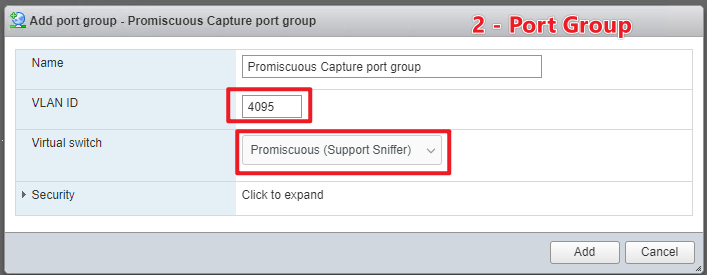


# Build Virtual Topology (vSwitch and Port Group/Interface)

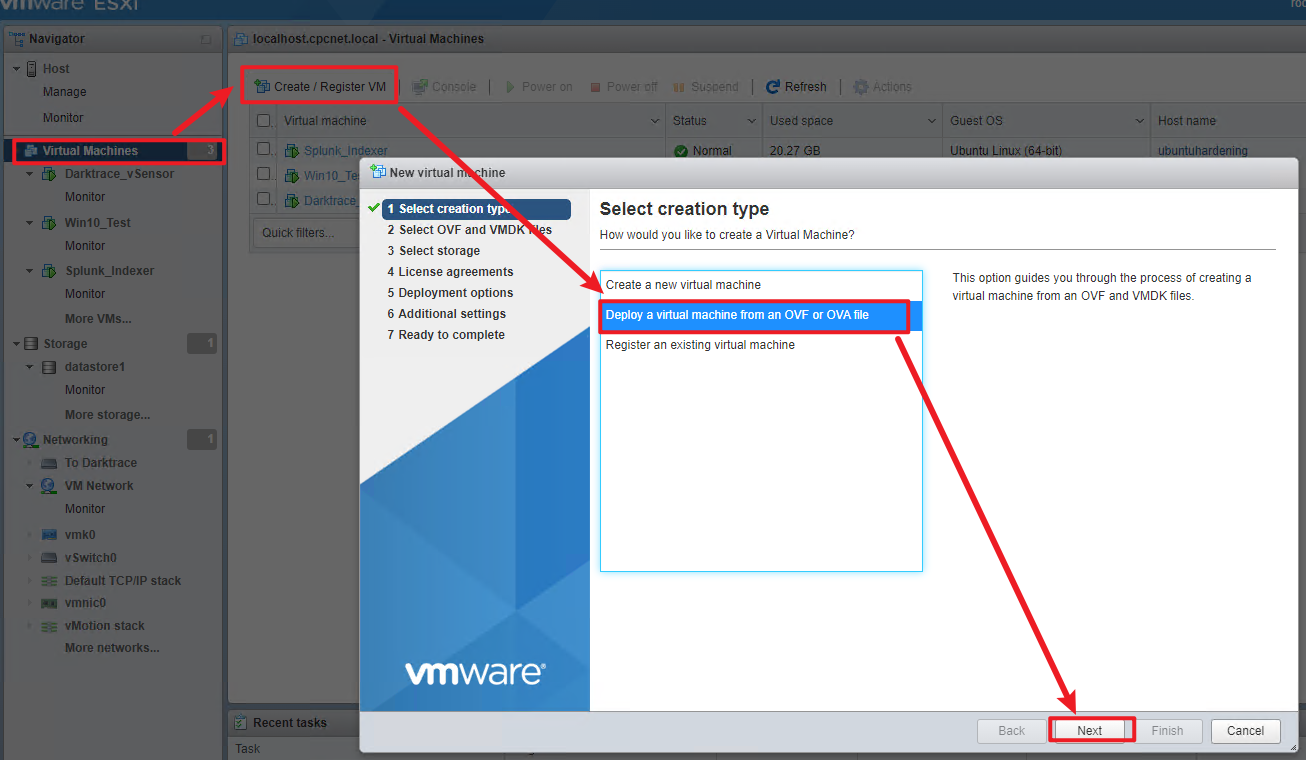
We will start with configuring a Sniffer vSwitch & its interface before we set up the VM, and we will later use the default vSwitch to send its log to the master.

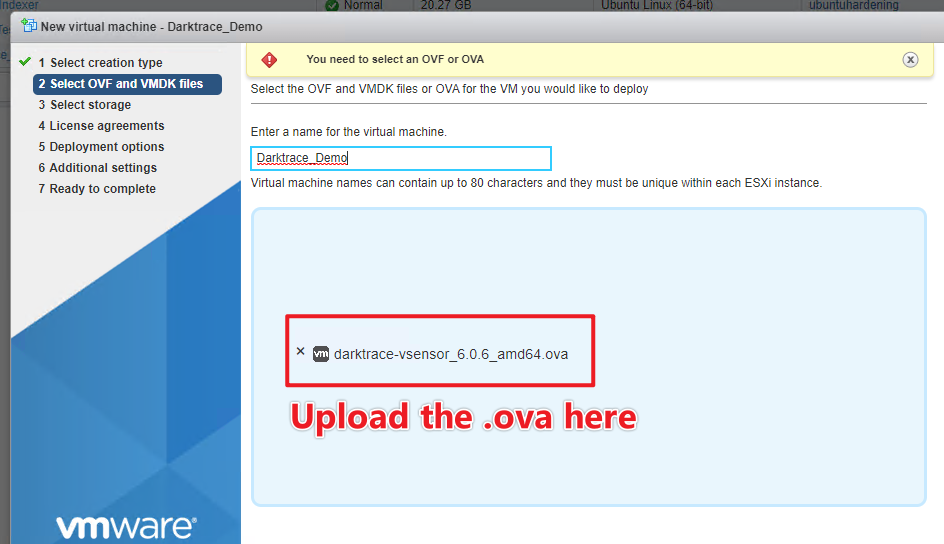


Set the VLAN ID to 4095. It is the best practice for a Sniffer vSwitch. Security settings for port group will inherit from vSwitch (Promiscuous)

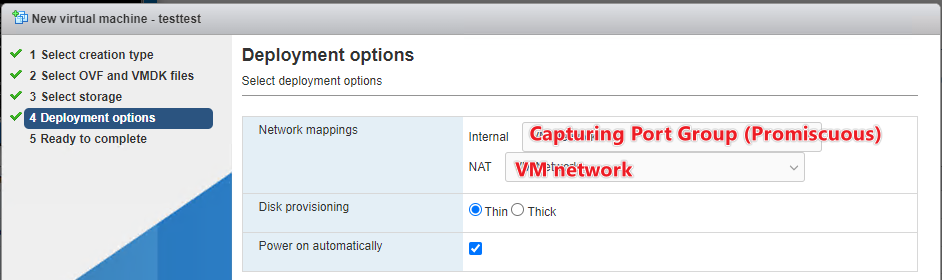


# Build and configure vSensor



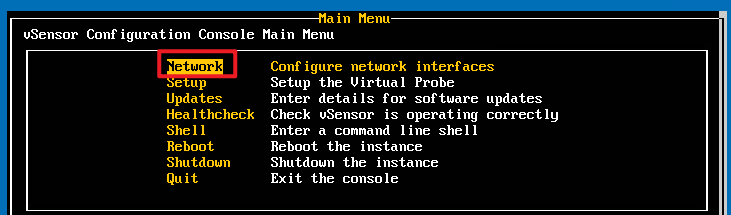


We would use the default VM Network port group for Management Interface (Notated NAT here). vSensor's management interface is also responsible sending the analyzed data to the master.

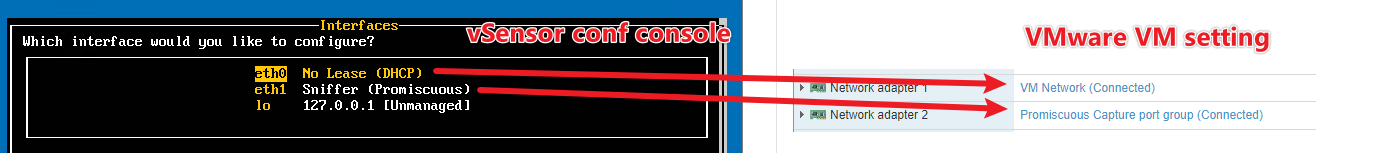


Boot the VM. Set up Keyboard layout (US) and the login password.

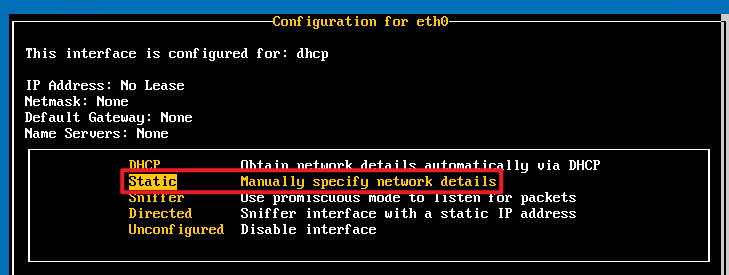
Enter the **Network** submenu.

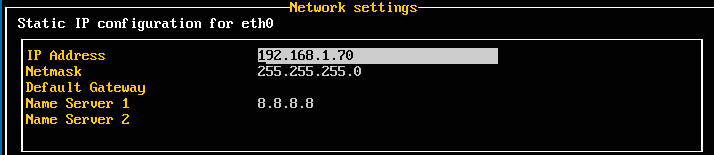


At Interfaces, make sure eth0 (Network Adapter 1) is connected to the VM Network port group, the default vSwitch. Make sure eth1 Sniffer (Network Adapter 2) is connected to the Promiscuous Capture port group, the vSwitch that is in Promiscous mode. If they do not correspond, change either on VMware or vSensor Interface config to make them match.

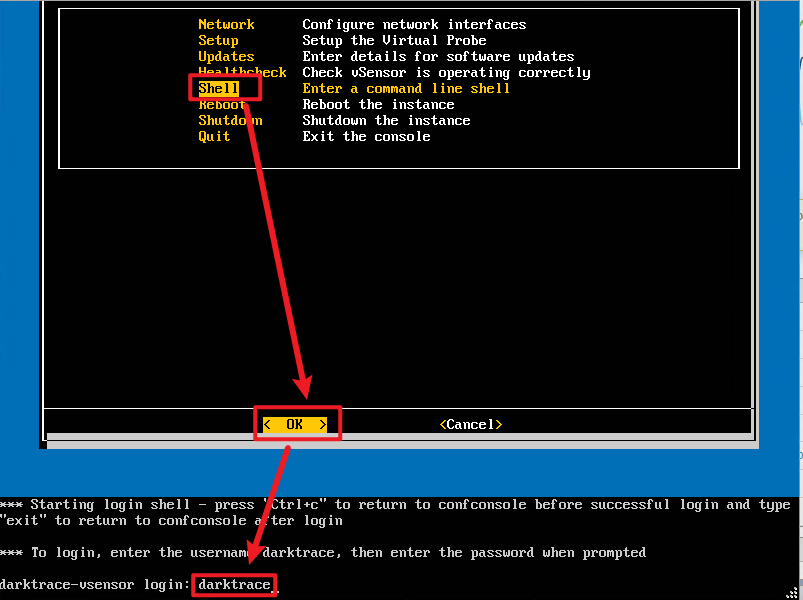


We will assign a static IP for the vSensor eth0 as shown below, so that the DarkTrace master knows its ID. When finished configuring, reboot the vSensor to apply the settings. After login, if still stuck in CLI, you may run "sudo confconsole" to enter the setup.

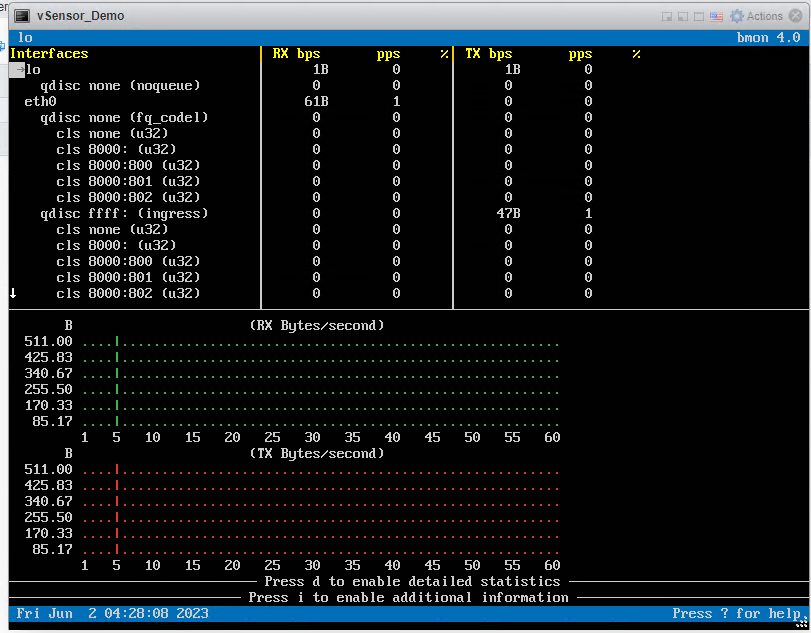




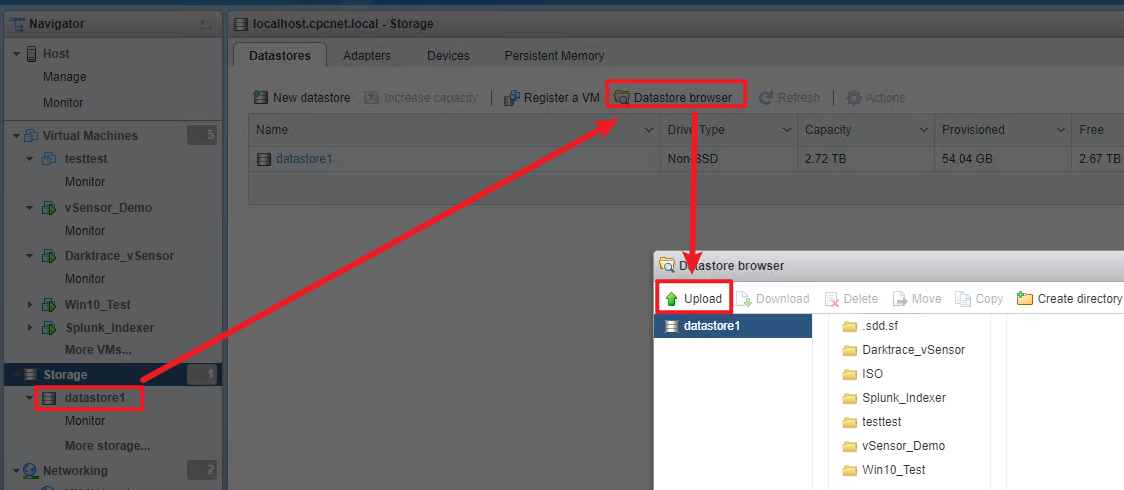
Then, enter the **Shell prompt**, we are going to check if the traffic really arrives. Login using the username **darktrace** and the password you have set up.



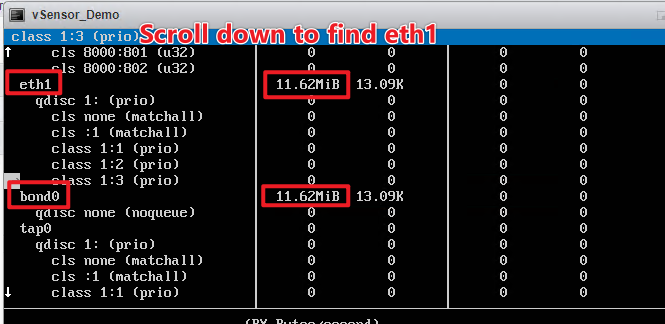
run bmon to see interface statistics



On the ESXi, upload a file to datastore, and we can observe the change in traffic statistics



Press down arrow to scroll down. It is expected that we see an increase in eth1 and bond0 traffic on vSensor bmon

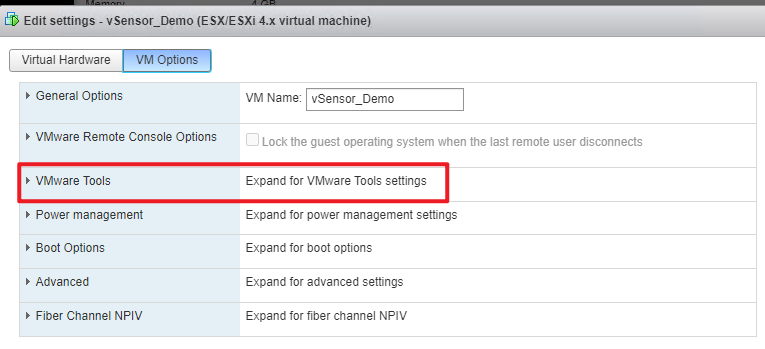


Type q followed by y to exit bmon.

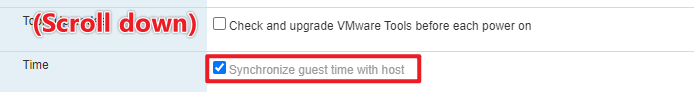
Then type exit to quit the Shell, back to conf console.

# Sync vSensor time with ESXi Host

Right click on the VM and select "Edit Settings". Expand the VMware tools section.



Scroll down and check the box.



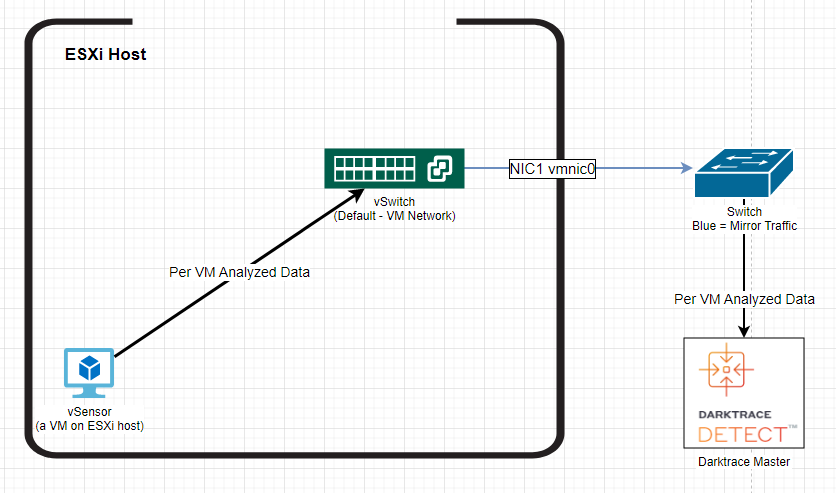
Send data to DarkTrace Master

Friday, June 2, 2023

2:10 PM

After the data is processed by the vSensor, we need to send them to the DarkTrace Master.

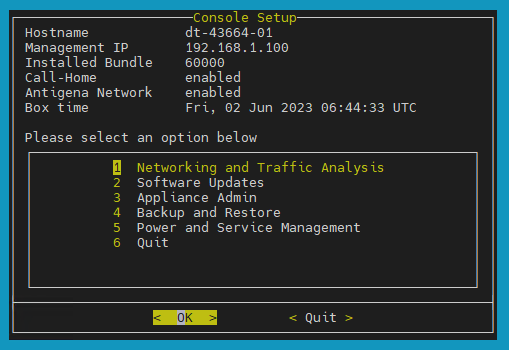
**Plug the cable**: Connect the DarkTrace Master's **Admin Interface** to the Switch port. The Switch port needs to have the same VLAN as the ESXi host's connection (blue). In this way, our vSensor data can reach the DarkTrace Master.



# Assign static IP for Analyst port

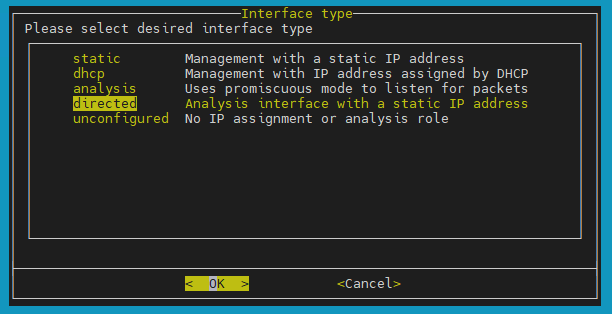
Although using the Dynamic IP might also work magically, we would like to keep it static to avoid potential error, since we have no DHCP server in this network.

SSH to the physical DarkTrace instance using the management IP, port 22. Use username "console" and the given password.

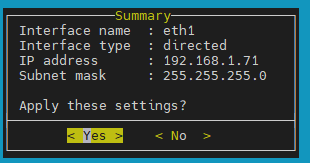


(1) Networking and Traffic Analysis -> (1) Configure network interfaces

Find the corresponding Analyst port, and select "Configure Interface"



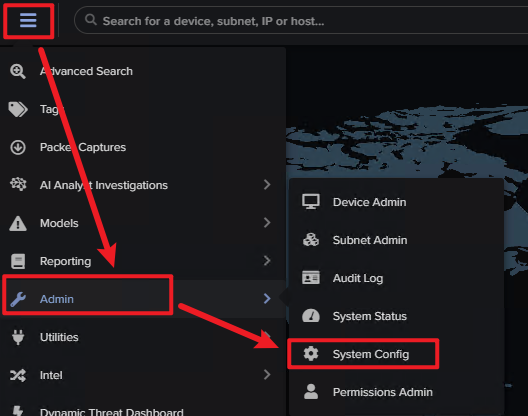
Apply the below settings:



# Set up the Master-vSensor communication

To access management IP via Browser, make sure you have already assigned a static IP to your PC under the **same subnet**. For example, if the Management IP is 192.168.1.100, your IP must be 192.168.1.x , with subnet mask 255.255.255.0. And it should not use an IP that is already in use.

Login the Threat visualizer by accessing the Master's Management IP on any browser. Use the "admin" account.

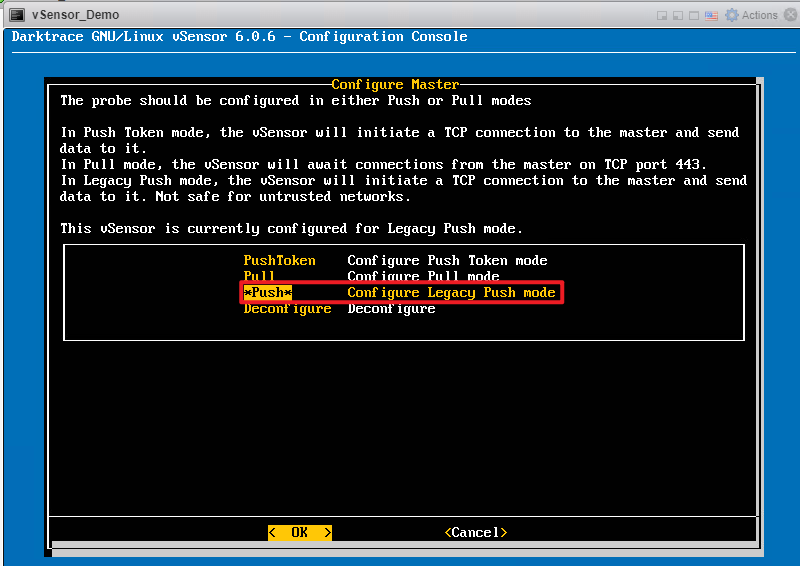


We will Configure the vSensor to send to the Master's **Management IP**. (Tested that we cannot use Analyst port IP)

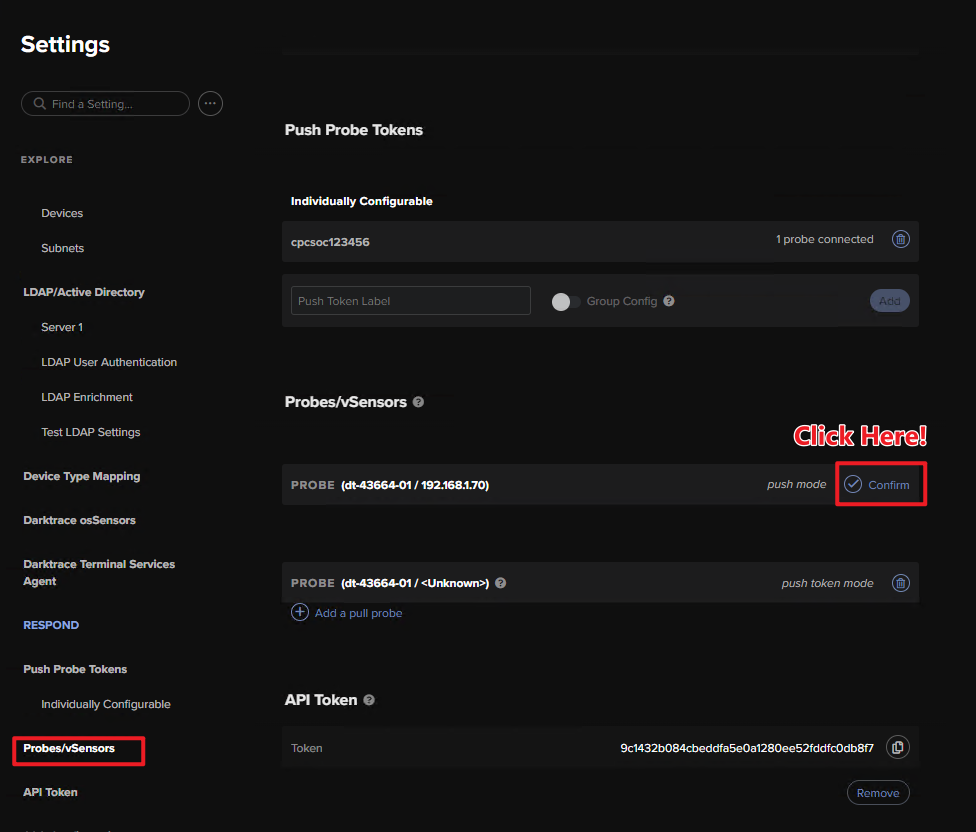
On vSensor conf console, Go to Main Menu > Setup > Master



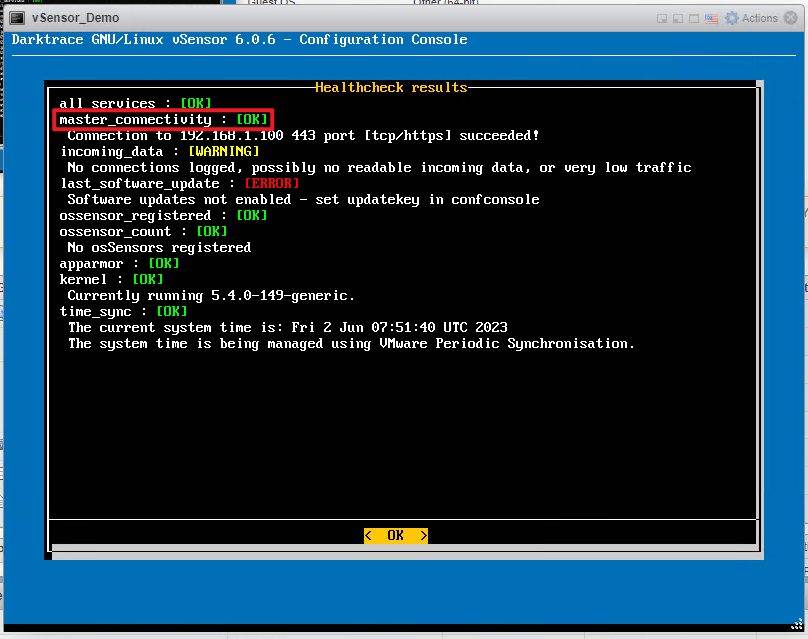
We will select the "push mode (legacy)". Enter the Management IP address for the Master and proceed.



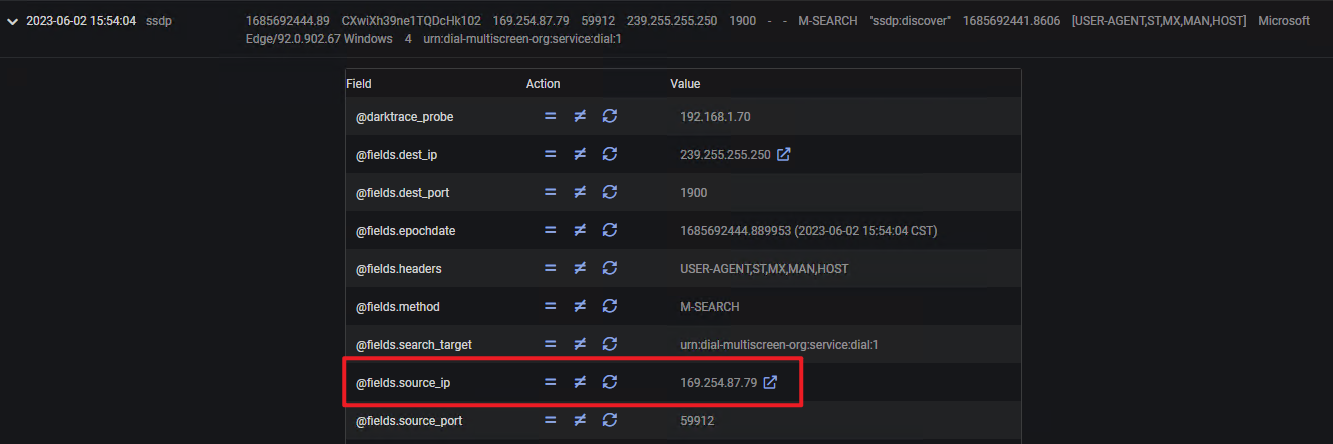
Shortly, on our Master's Threat Visualizer (Management IP via Browser), we can **Confirm probing** in Main Menu > Admin > System Config > Probes/vSensors



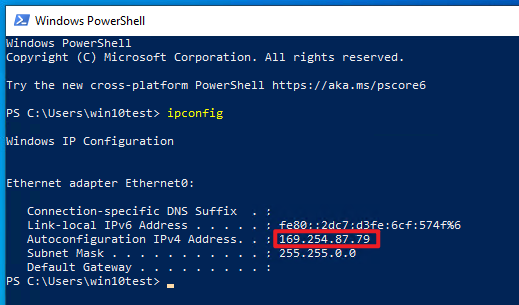
Running the "Healthcheck" on vSensor configuration Consol, we shall see the master\_connectivity is now [OK]



In the Threat Analyzer, we can use "Advanced Search" to double check the results.

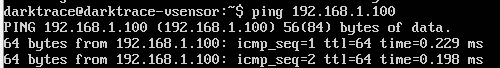


We can see traffic from one of our ESXi Windows VM, with IP 169.254.87.79



# Final Checking (Some TroubleShooting Ideas)

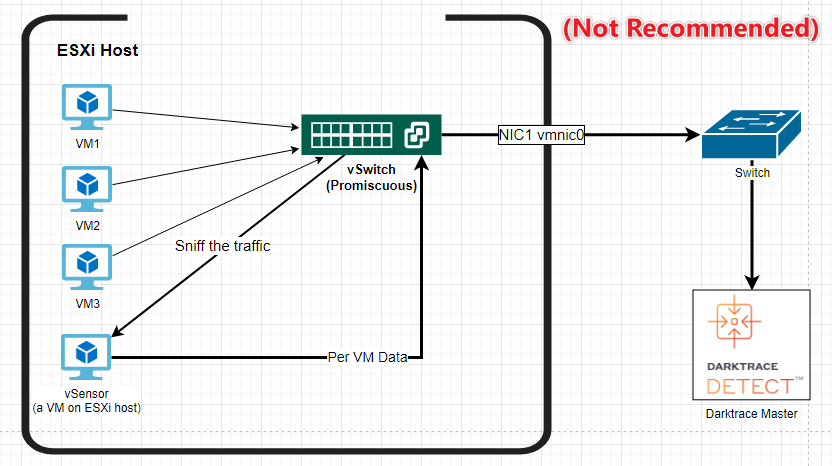
1. We have assgined a valid static IP for the DarkTrace Master Analyst port and the vSensor non-Sniff port (eth0).
2. The DarkTrace Master Analyst port interface and the ESXi VM Network interface (NIC1 vmnic0) are in the same VLAN, so that they can "talk" with each other.
3. The DarkTrace Master and the ESXi are connected via the physical Switch, and the Switch puts them in the same VLAN.
4. Use Roadmap (Verbose) to check what we have done. (At the end of this document)
5. Ping other devices at vSensor / DarkTrace master. If not reachable, first check physical connection, then check Switch VLAN, lastly check software-side configuration.
   1. Example: Enter the Shell prompt and ping.



# Extras

[Alternative way, for some insights]

Keep in mind that we can also change the default vSwitch - VM Network to Promiscuous and let the vSensor sniff it, but in our production we will potentially invovle more ESXi hosts for the vSensor to sniff. In terms of security, this is also not recommended as it allows the VMs to sniff each other as well, and we cannot guarantee 100% traffic. So that's why we must have a separate vSwitch in promiscuous mode.



# Roadmap (Verbose)

1. Prerequisites Checking
   1. Make sure mirroring at the physical switch is working. If you have not done so, follow the **Cisco Switch Port Mirroring** guide to do so.
   2. Make sure you can access the console (either locally or SSH) and the Management IP (ThreatVisualizer) of the DarkTrace.
2. Check Dell Server interface that accepts mirrored traffic and use it to config new vSwitch.
   1. Make a new vSwitch for the vSensor
      1. Promiscuous mode is required.
      2. It is a best practice to set the VLAN ID set to All (4095) to ensure that no packets are filtered by VMware before reaching the vSensor.
3. Install vSensor on ESXi host using the .ova.
4. Make sure vSensor can receive and parse the traffic.
   1. Check network interfaces of vSensor
   2. Config Static IP for vSensor Interfaces.
   3. Sync vSensor Clock with VMWare host
5. Configure vSensor to send data to its Master.
   1. Assign a static IP for the vSensor eth0.
   2. Default vSwitch will be used for sending data out.
6. Deployment Checks
   1. vSensor Health Check
   2. Check data arrival at Threat Visualizer advanced search
   3. Can also use packet tracer