# Setting Up A Virtual Sensor In a VMware/vSphere/vCenter Environment

NETWATCHER™

support@netwatcher.com

# Download NetWatcher Sensor VM

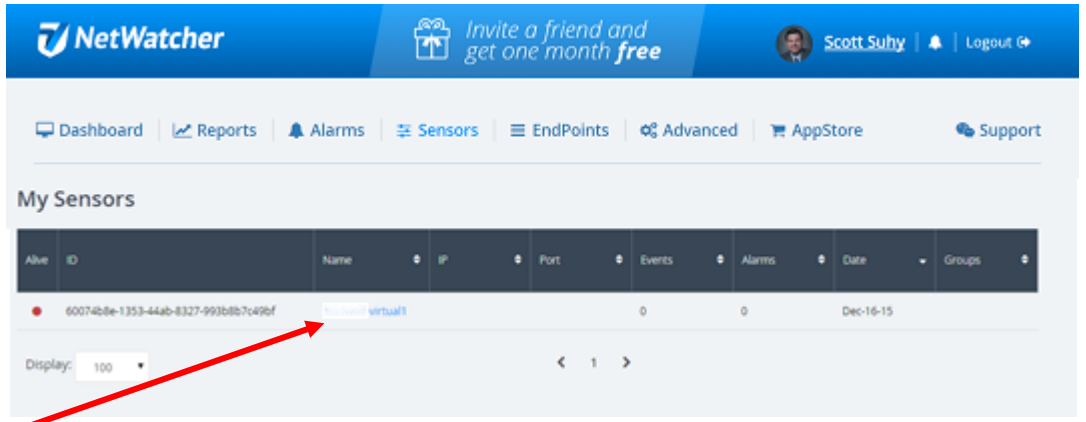
**How to login to the portal:**

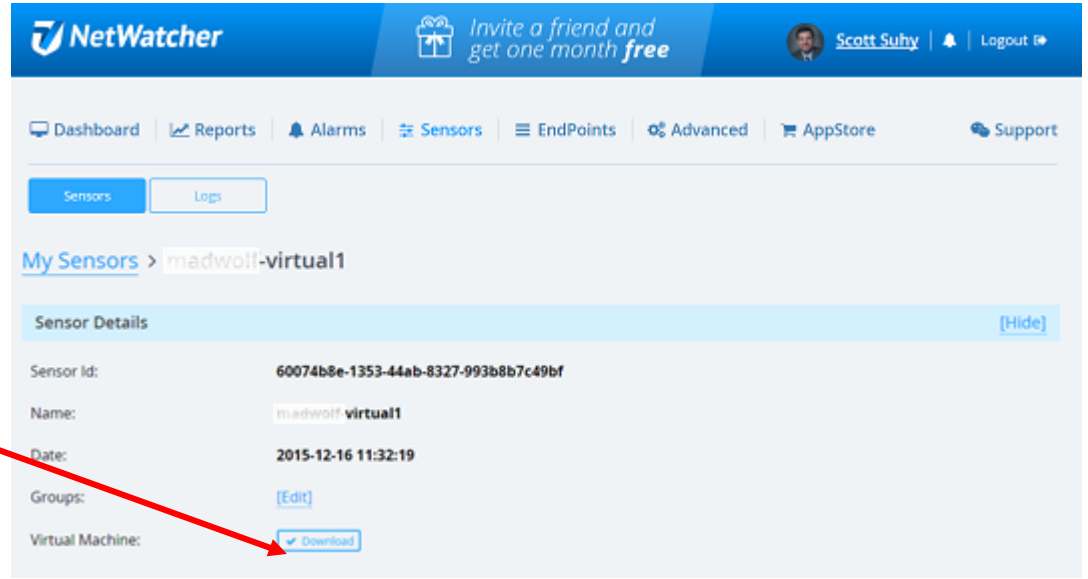
- You should have received an email to access the NetWatcher.com portal earlier. If you can't find it, log in to https://portal.netwatcher.com/login with your email address and reset your password.

**How to download the Virtual Machine/Sensor:**

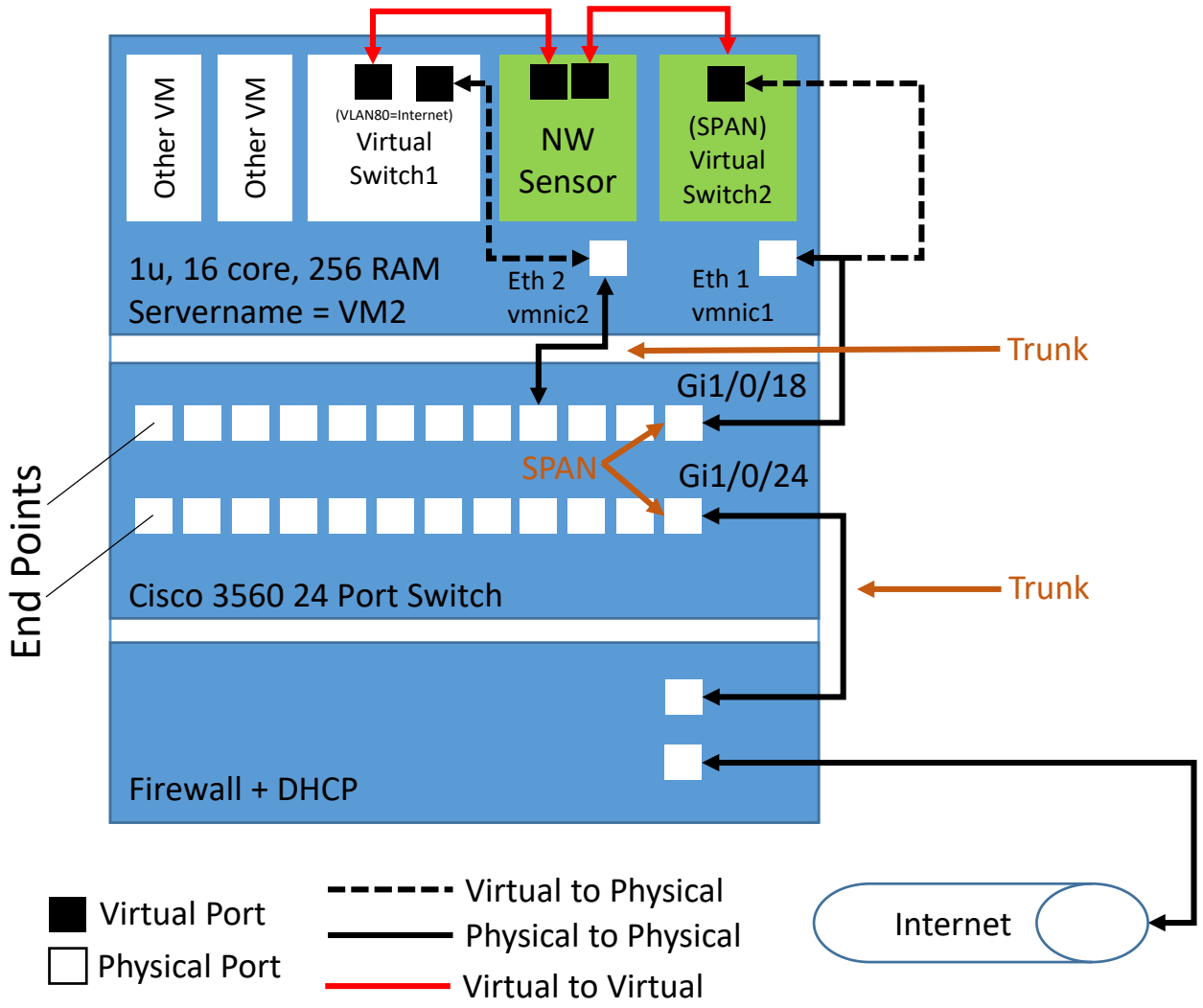
- Once you log in to your account, navigate to https://portal.netwatcher.com/sensor/sensors, click on your sensor, and press download. It will take a while to download as it's a large file. We use http://www.7-zip.org for compression and there is no password. There are two parts, extract the first one and it will continue into the second one.

- Unzip, then untar downloaded .xz file.



# Setup Example Using VMware and Cisco




## Assumptions about the environment

- These instructions assume a VMware vCenter environment and Cisco Switch however the same instructions apply to other platforms.
- Server has virtualized switch's that connect to the physical switch ports (example: 18)
- To support up to a network with ~200mb/s egress bandwidth you will need to create a VM with 4 cores, 4 GB RAM, >= 500 GB HDD

What you need to add to your virtual environment

# Cisco Setup

## 1 Identify Source port for SPAN

```
#show run int Gi1/0/24
Building configuration...

Current configuration : 92 bytes
interface GigabitEthernet1/0/24
 description Trunk to Internet Firewall
 switchport mode trunk
end
```

## 2 Identify destination port for SPAN

```
#show run int Gi1/0/18
Building configuration...

Current configuration : 86 bytes
interface GigabitEthernet1/0/18
 description Link to vm2 vmnic1
 switchport mode trunk
 switchport nonegotiate
end
```

## 3 Configure SPAN:

```
#monitor session 2 source interface Gi1/0/24
#monitor session 2 destination interface Gi1/0/18
```

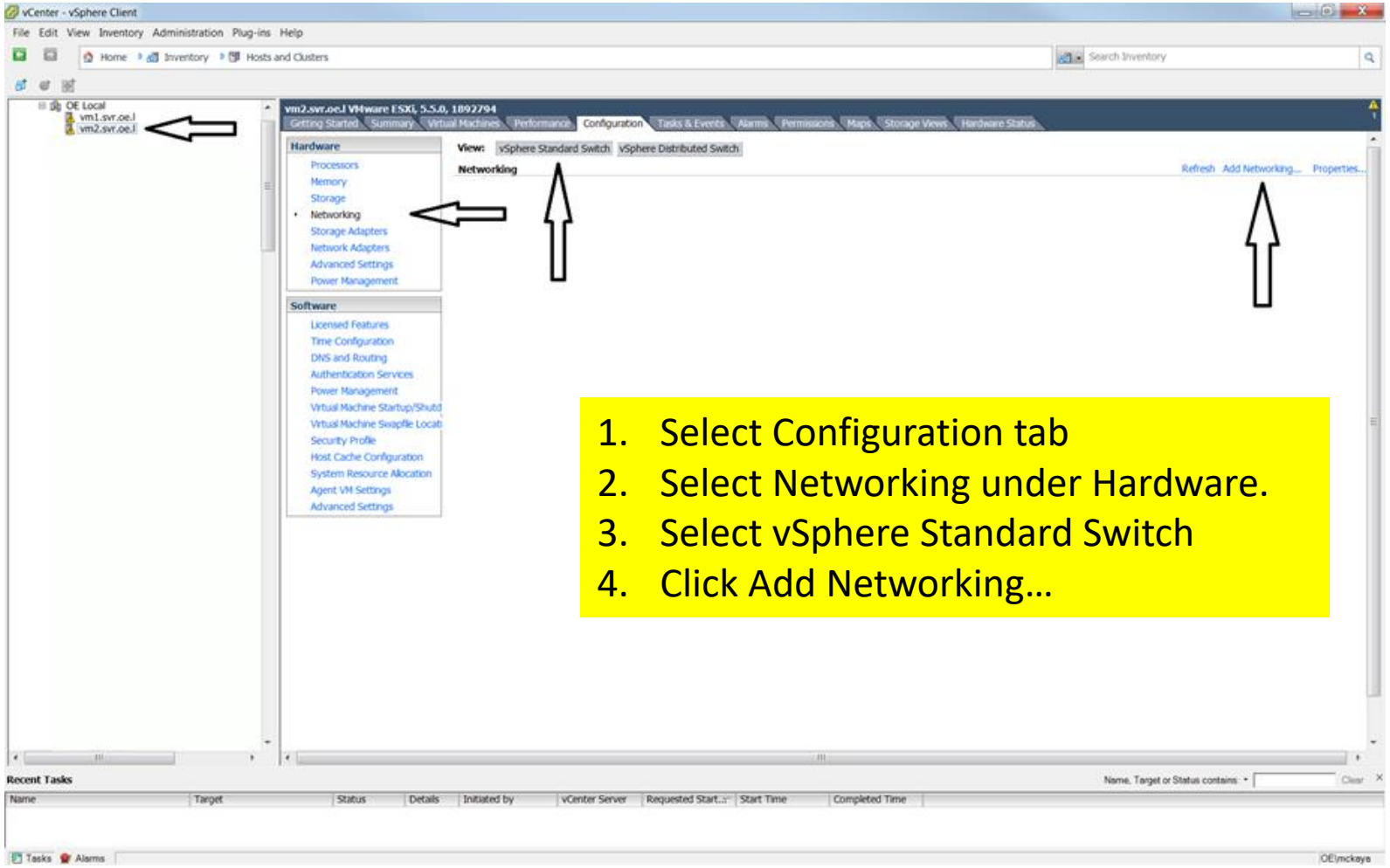
Ensure there is a physical cable connecting this destination port (Gi1/0/18 in this example) to the VMWare host physical port (vm2:vmnic1 in this example)

Note:

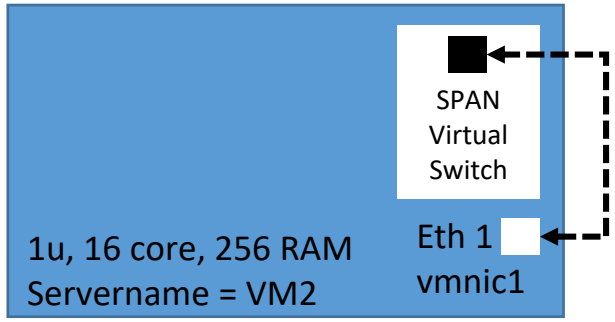
- Source = the actual traffic
- Destination = the copy of the traffic being sent to the sensor

https://learningnetwork.cisco.com/docs/DOC-26018

# Step 1: Create a Virtual Switch w/Virtual SPAN Port & Map it to a Physical Port



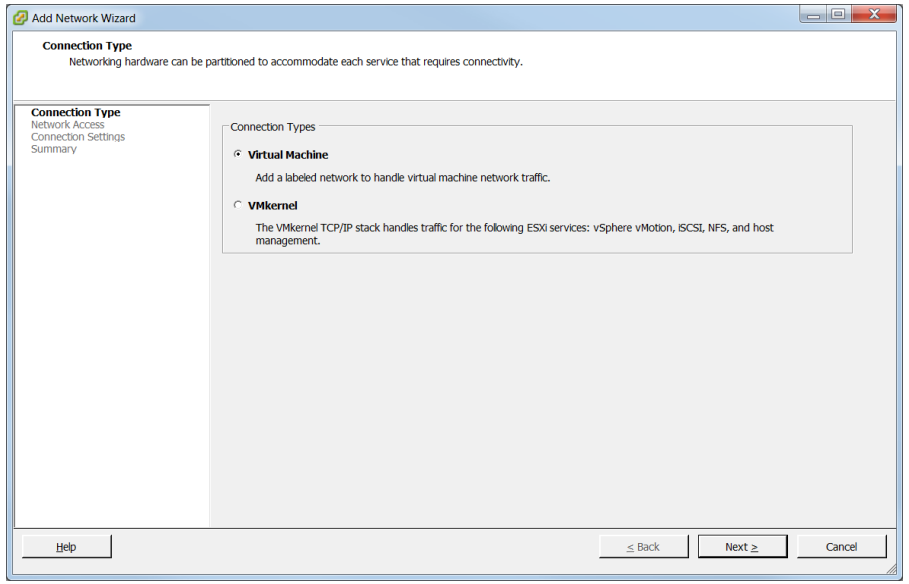

1. Select Configuration tab
2. Select Networking under Hardware.
3. Select vSphere Standard Switch
4. Click Add Networking…



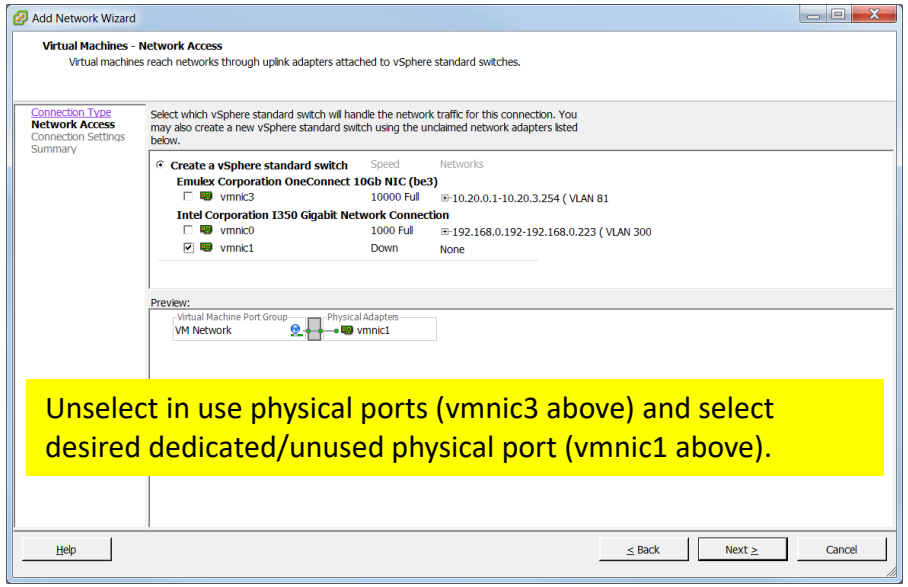
# Step 1-a: Create a Virtual Switch w/Virtual SPAN Port & Map it to a Physical Port

## --Create the SPAN Port to mirror all traffic

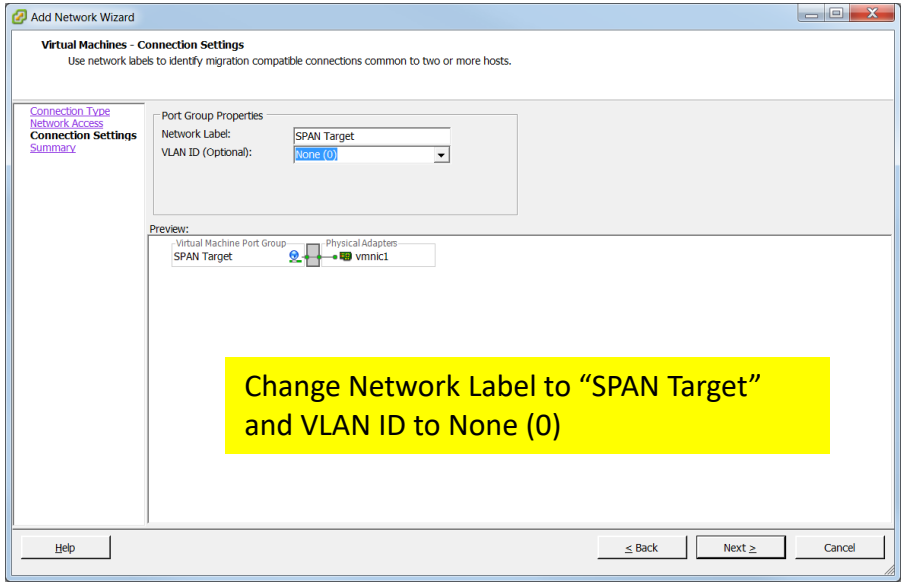
1



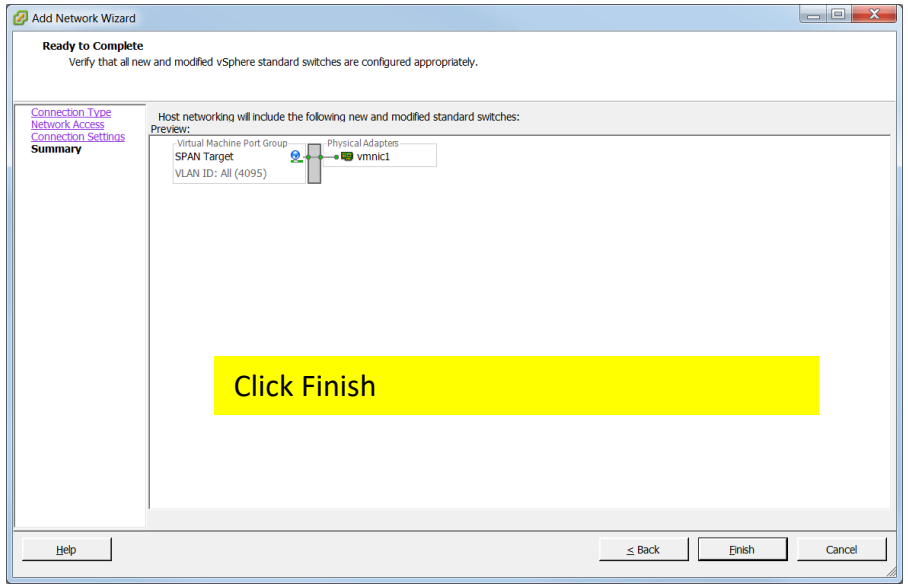

2




3



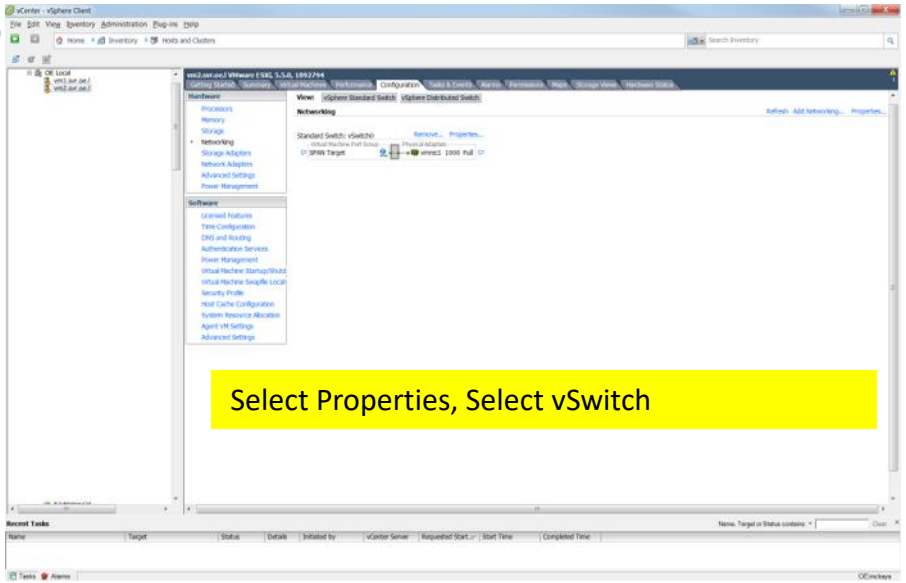

4



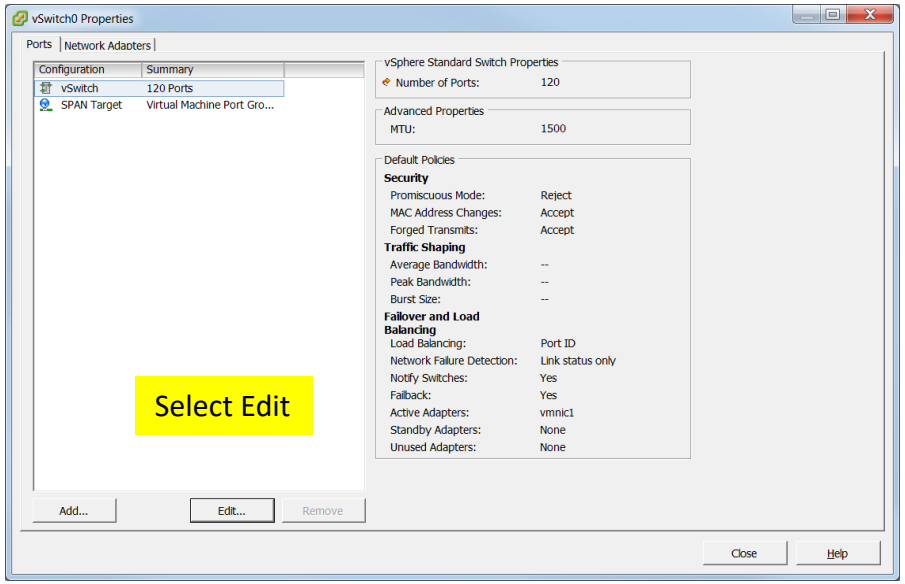
# Step 1-b: Create a Virtual Switch w/Virtual SPAN Port & Map it to a Physical Port

## --Enable Promiscuous Mode

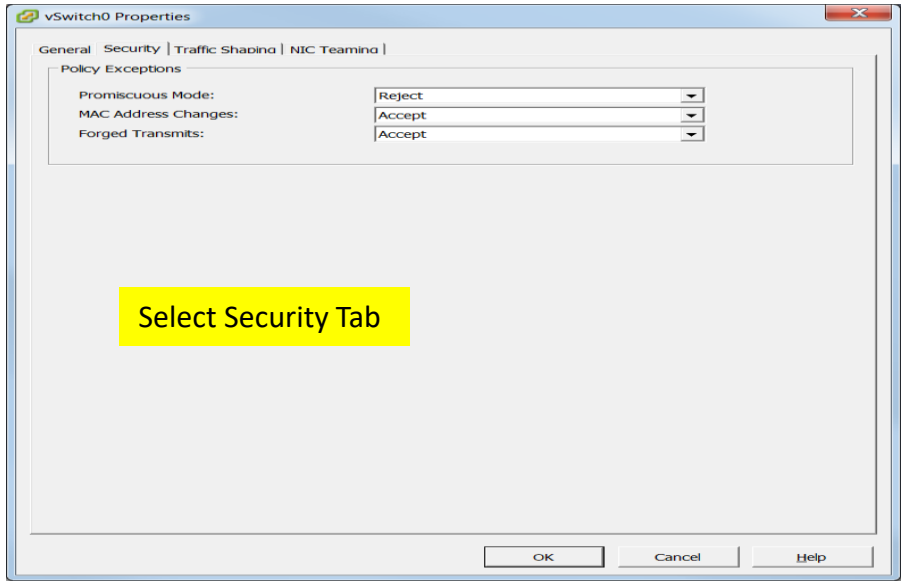
1



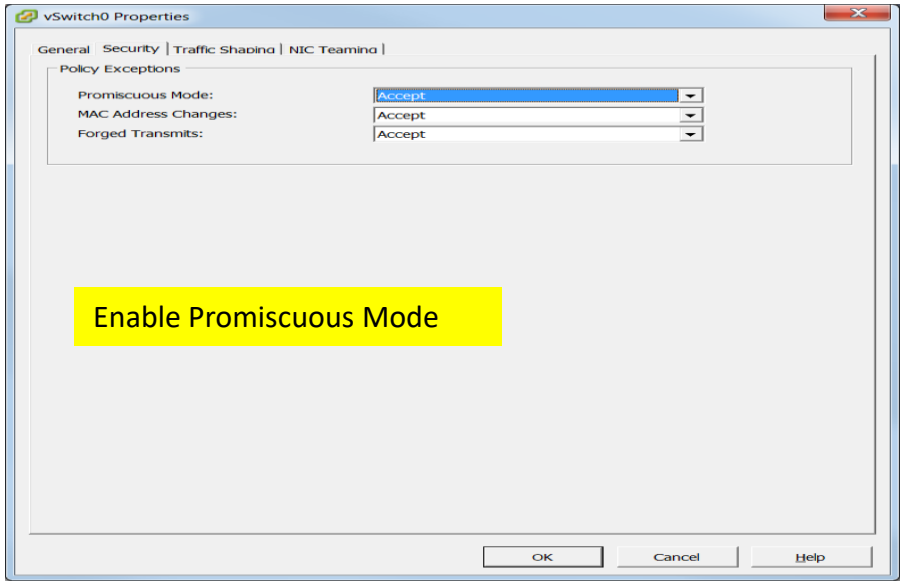

2




3



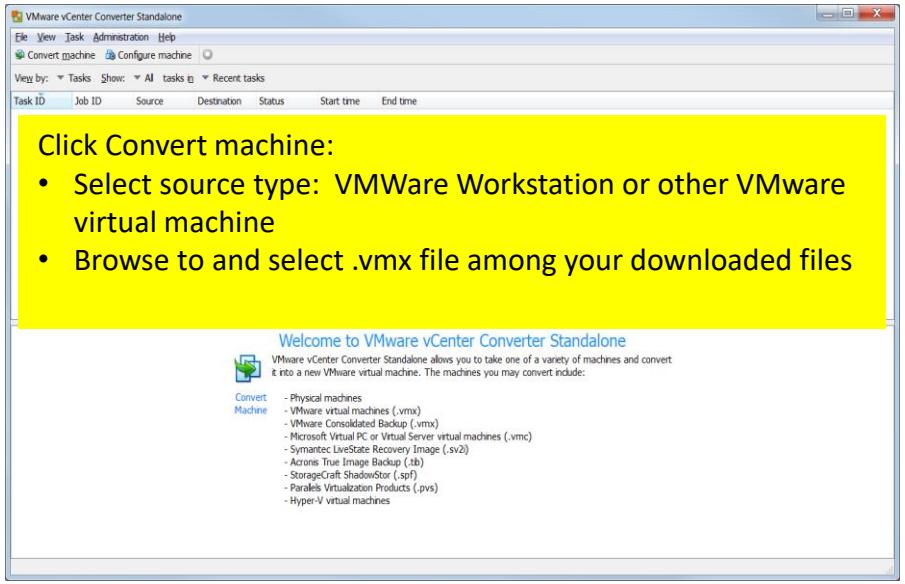

4



# Step 2: Import NetWatcher Sensor VM

Run VMWare Converter
(https://www.vmware.com/products/converter)

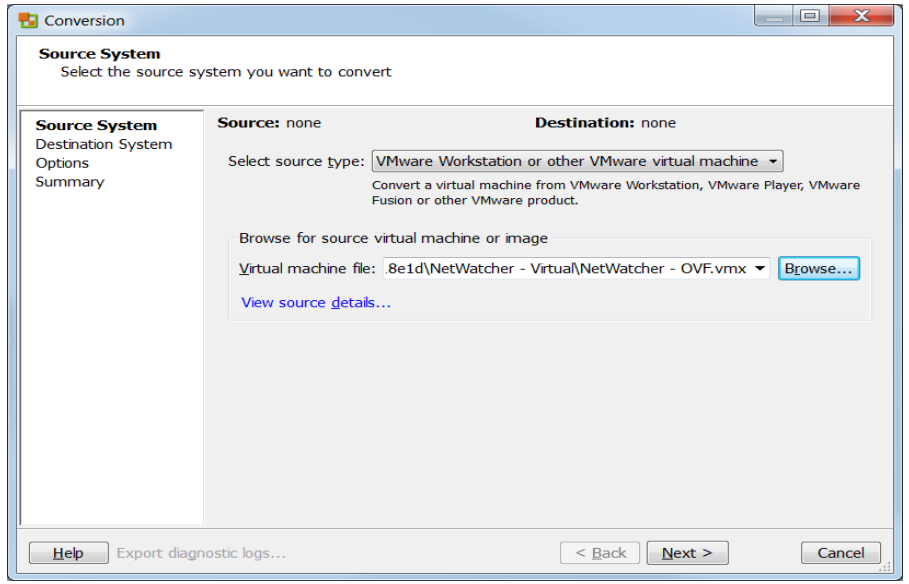
1



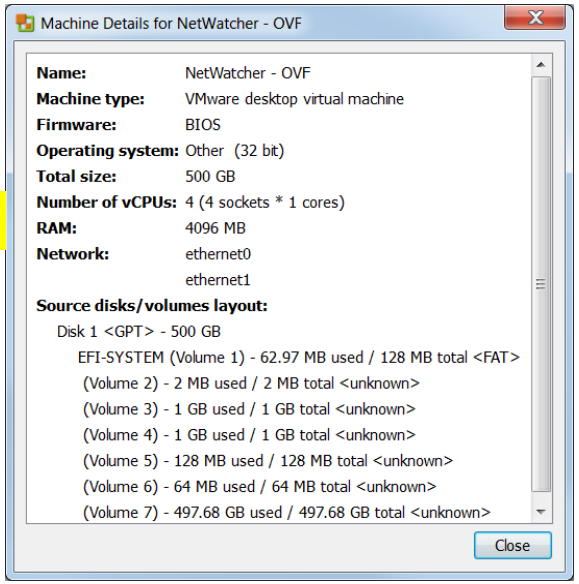

Click Convert machine:

- Select source type: VMWare Workstation or other VMware virtual machine
- Browse to and select .vmx file among your downloaded files

2

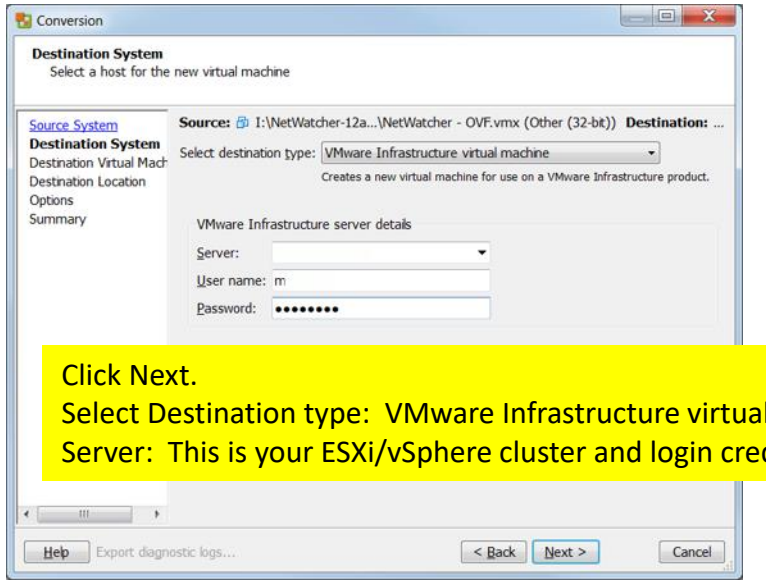



3




Click on source details and it should look like this:

4

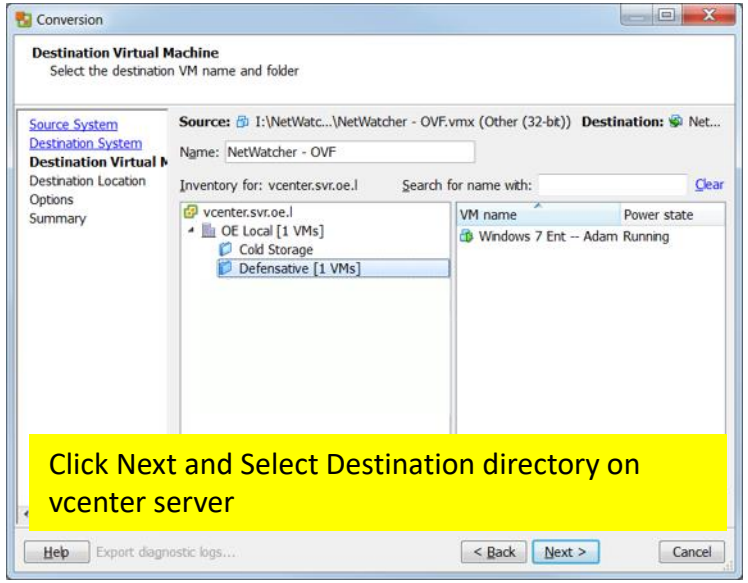



Click Next.
Select Destination type: VMware Infrastructure virtual machine
Server: This is your ESXi/vSphere cluster and login credentials.

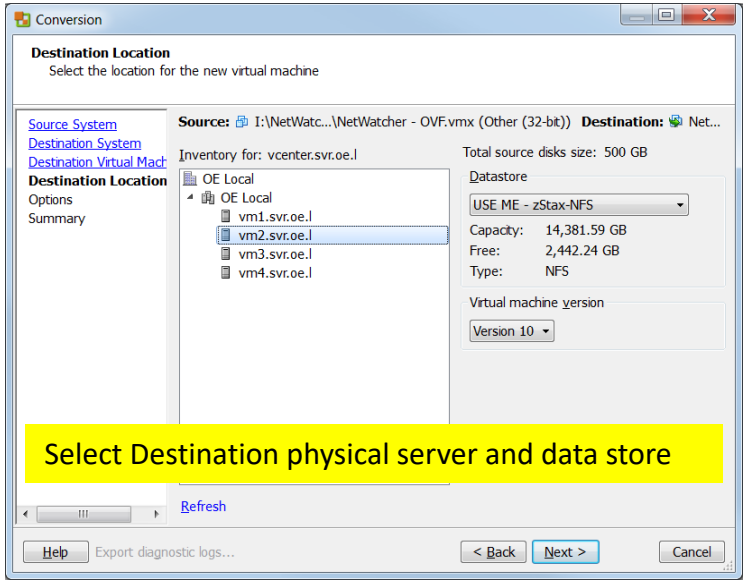
NW Sensor

# Step 2-a: Import NetWatcher Sensor VM

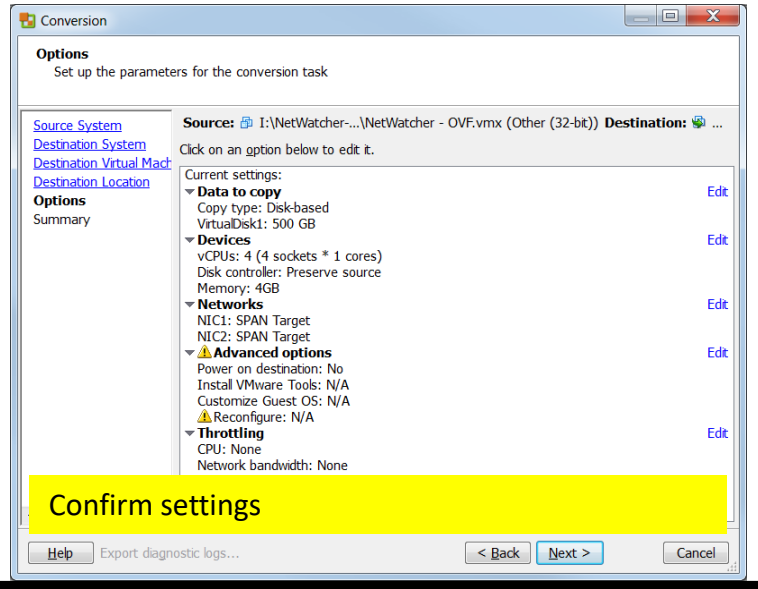
1



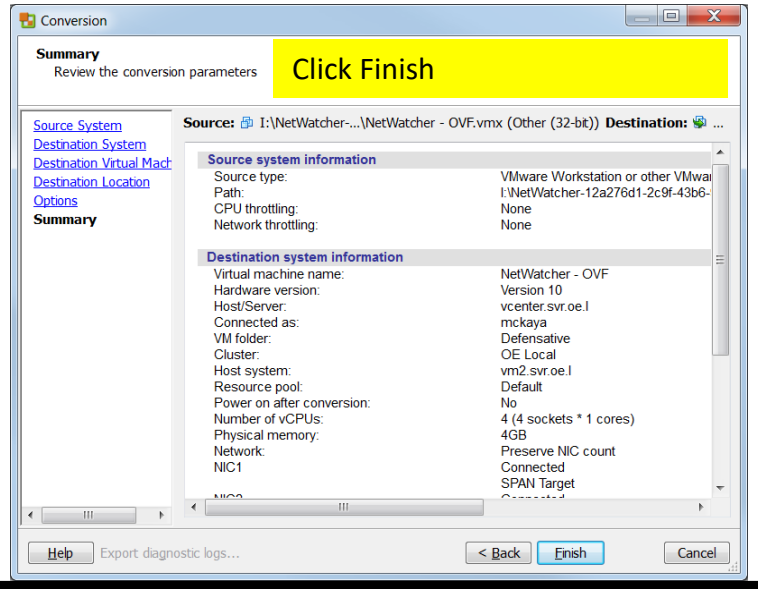

2



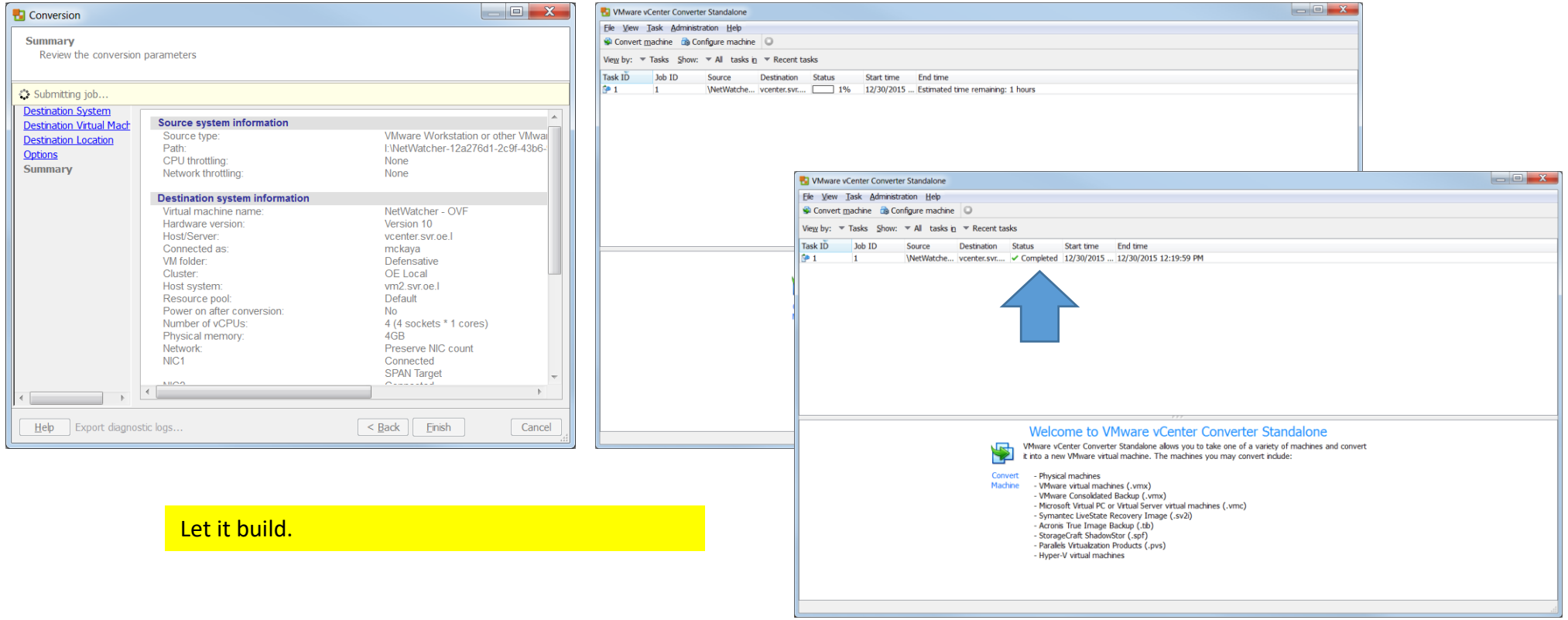

3




4



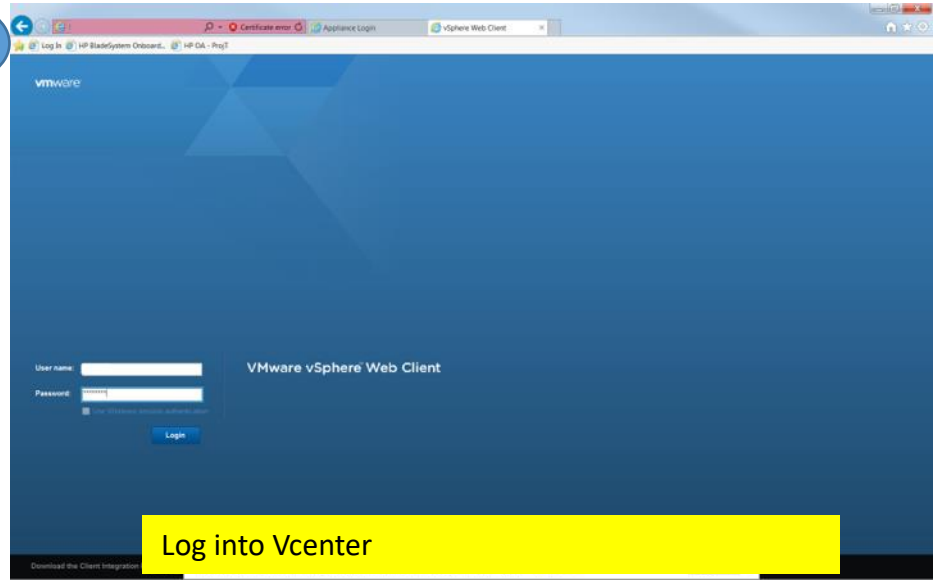
# Step 2-b: Import NetWatcher Sensor VM




Let it build.

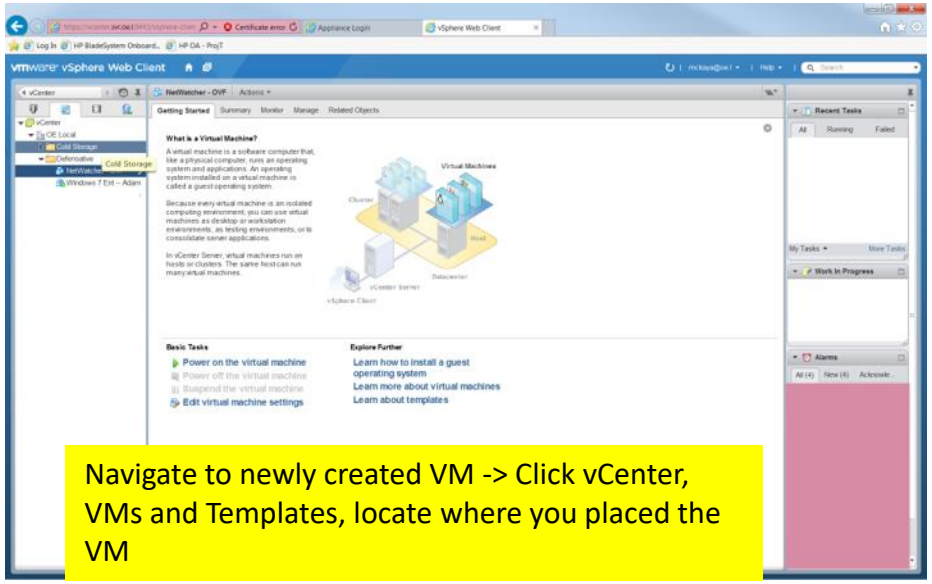
# Step 3: Map NetWatcher Sensors Network Adapter 1 and Network Adapter 2

1



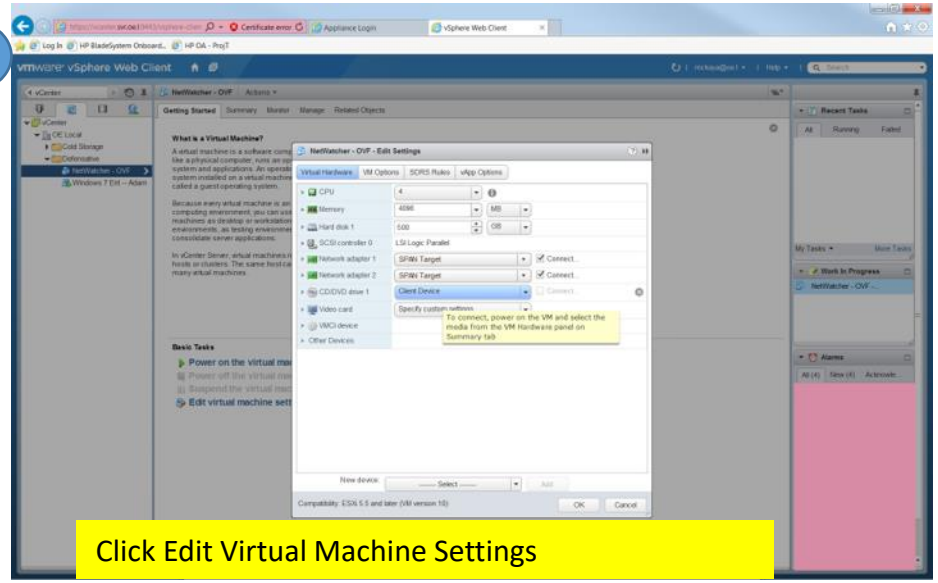

Log into Vcenter

2



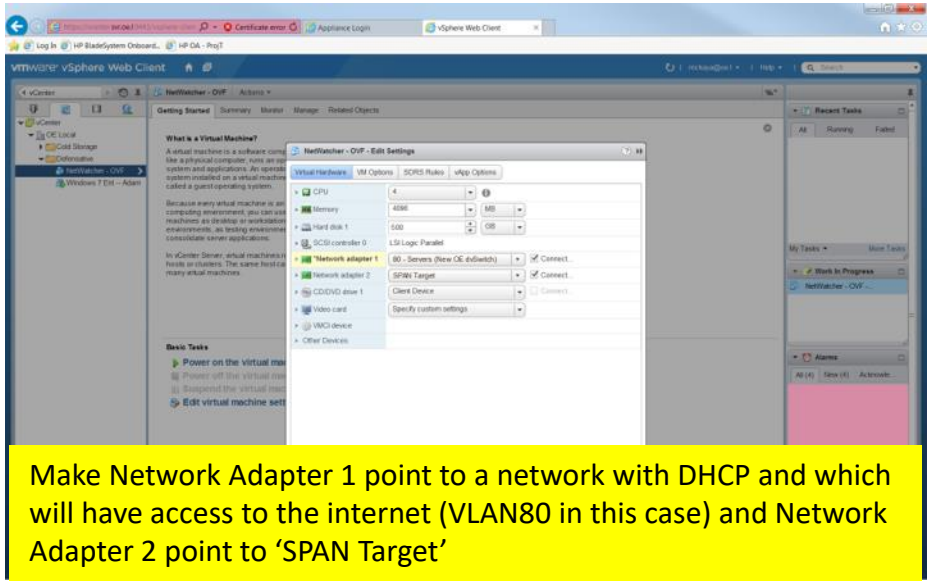

Navigate to newly created VM -> Click vCenter, VMs and Templates, locate where you placed the VM

3

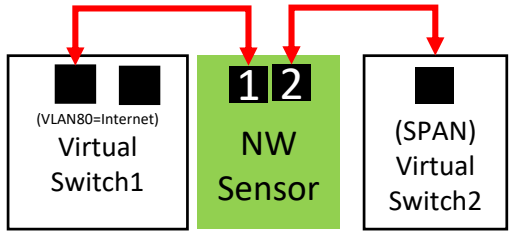



Click Edit Virtual Machine Settings

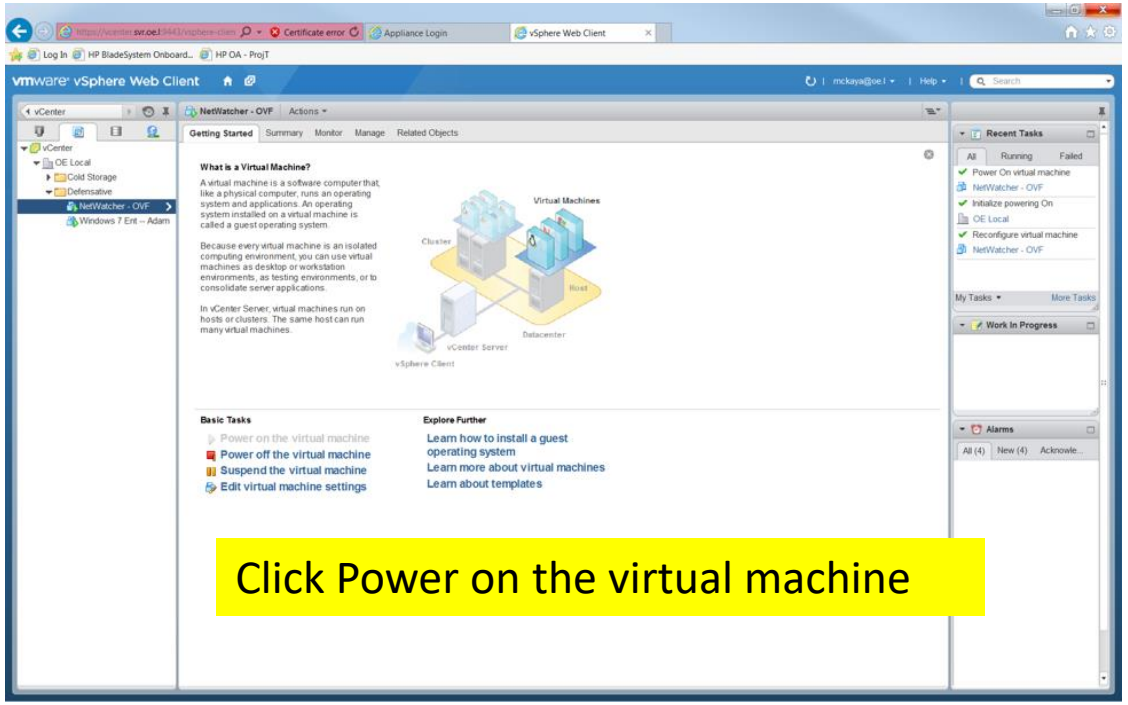
4

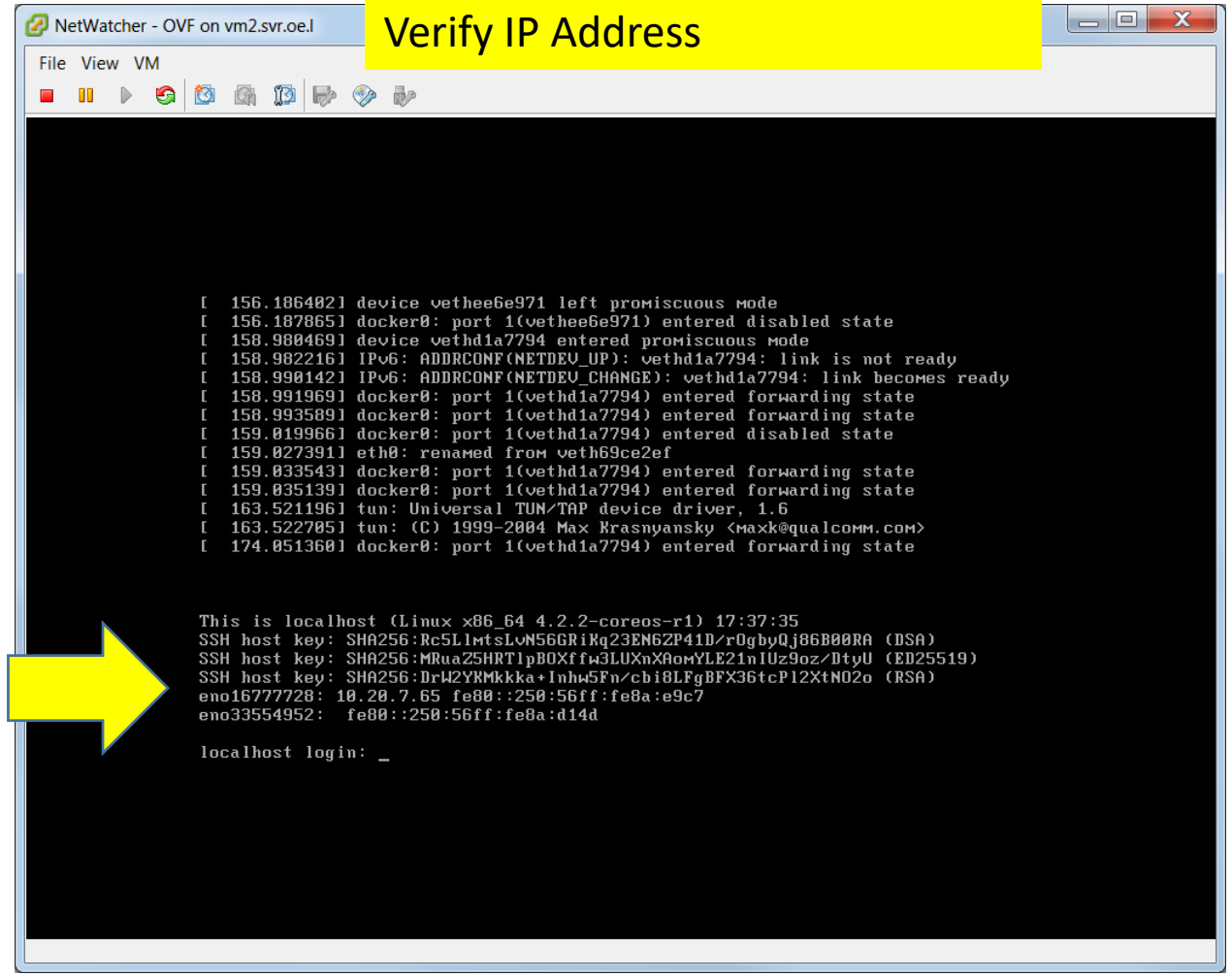



Make Network Adapter 1 point to a network with DHCP and which will have access to the internet (VLAN80 in this case) and Network Adapter 2 point to 'SPAN Target'



# Step 4: Open NetWatcher Sensor Console



# Log In to the Customer Portal to Verify Sensor is Live

Verify Color changed to Green

**This can take up to an hour As the sensor is downloading Additional containers…

# Notes & Troubleshooting

- If you deploy it in more than one location the sensors will kick each other off (it has a singular identity).
- The sensor does NOT need a static IP to work but it does require a DHCP address
- Here are the ports we use:
  - TCP 8443 to portal.netwatcher.com => Used for credential management
  - UDP 443 to vpn.netatcher.com => connection to backend, SSL VPN
  - TCP 80 to google.com => Used to test internet/DNS connectivity
  - TCP 443 (HTTPS) to index.docker.io (secure Docker container download)
  - TCP 443 (HTTPS) to public.update.core-os.net (CoreOS updates)