

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

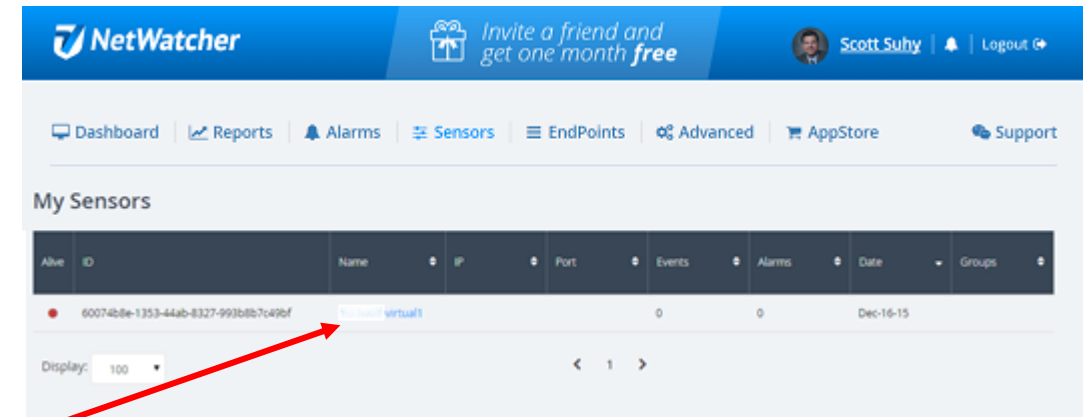
# Download NetWatcher Sensor VM

## How to login to the portal:

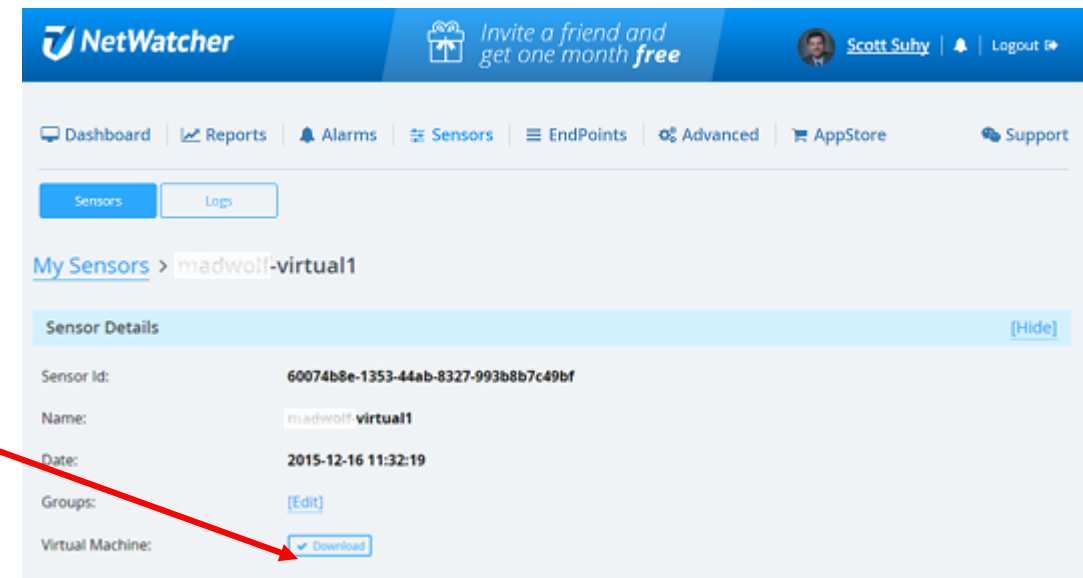
- You should have received an email to access the NetWatcher.com portal earlier. If you can't find it, log in to <https://portal.netwatcher.com/login> with your email address and reset your password.

## 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.

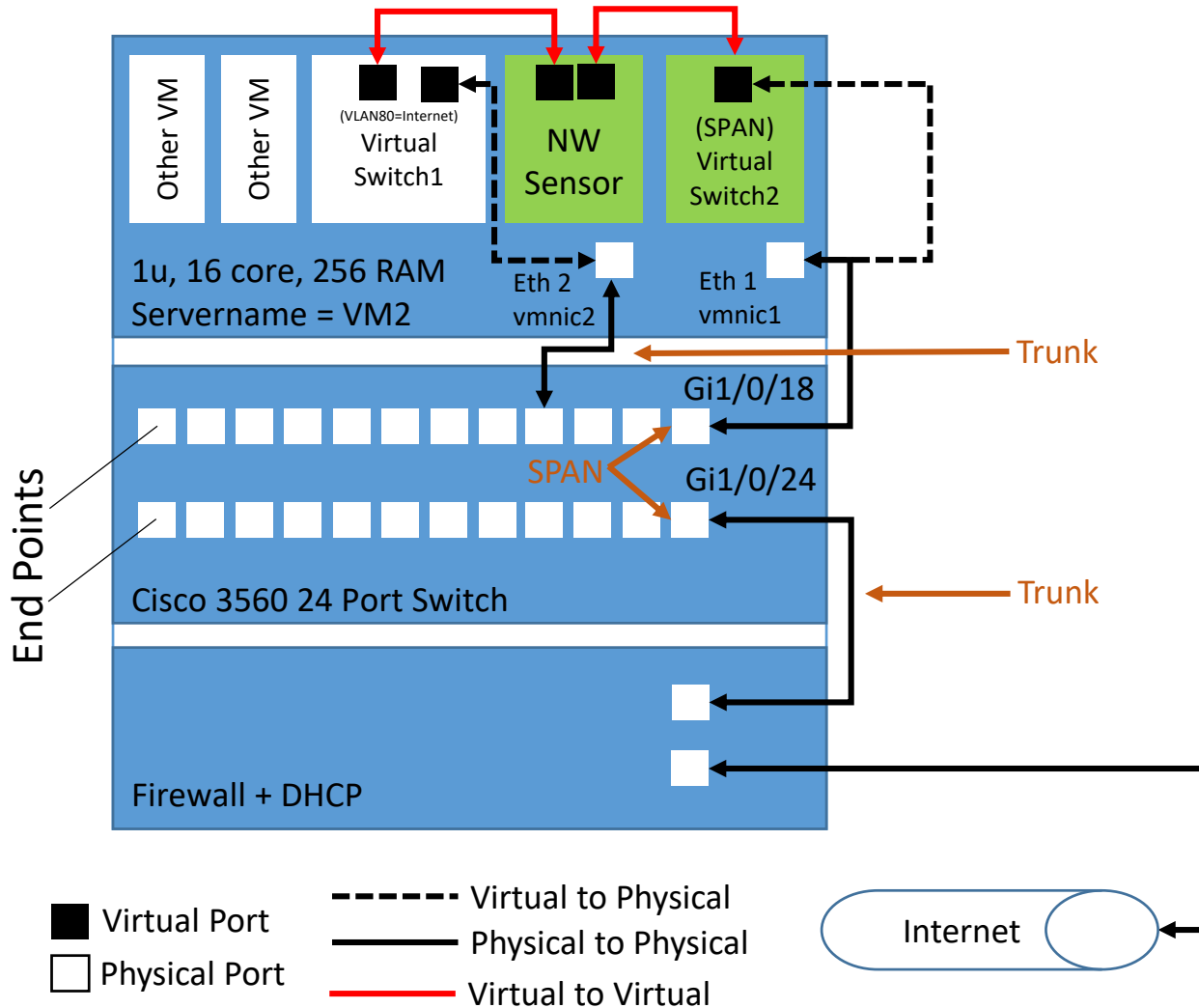


The screenshot shows the NetWatcher portal interface. At the top, there is a navigation bar with the NetWatcher logo, a promotional banner for a free month, and user information for Scott Suhy. Below the navigation bar, there are tabs for Dashboard, Reports, Alarms, Sensors, EndPoints, Advanced, AppStore, and Support. The main content area is titled 'My Sensors' and contains a table with columns for Name, IP, Port, Events, Alarms, Date, and Groups. A single sensor is listed with the name 'madwolf-virtual1' and a date of 'Dec-16-15'. A red arrow points from the 'madwolf-virtual1' link in the table to the 'Download' button in the second screenshot.



The screenshot shows the 'Sensor Details' page for the sensor 'madwolf-virtual1'. The page has a navigation bar and tabs for Sensors and Logs. The main content area is titled 'My Sensors > madwolf-virtual1' and contains a 'Sensor Details' section with a '[Hide]' button. The details include: Sensor Id: 60074b8e-1353-44ab-8327-993b8b7c49bf, Name: madwolf-virtual1, Date: 2015-12-16 11:32:19, Groups: [Edit], and Virtual Machine: [Download]. A red arrow points from the 'Download' button in this screenshot to the 'Download' button in the first screenshot.

# 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

## 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
```

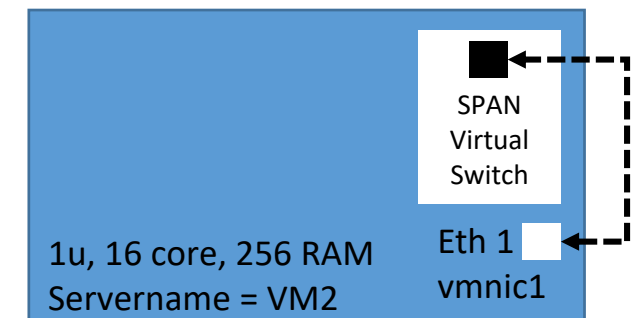
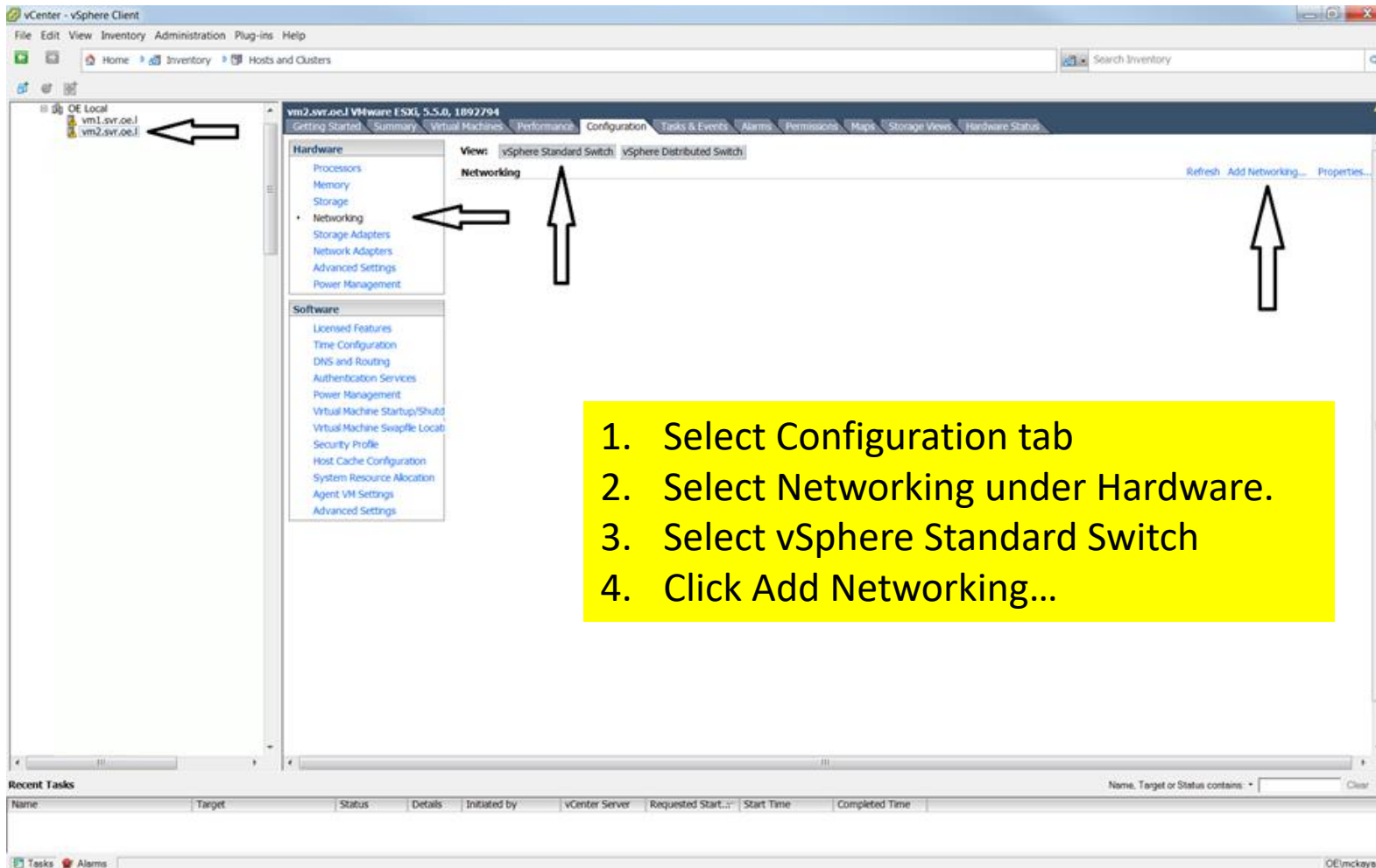
Ensure there is a physical cable connecting this destination port (Gi1/0/18 in this example) to the VMWare host physical port (vm2:vmnic1 in this example)

Note:

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

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

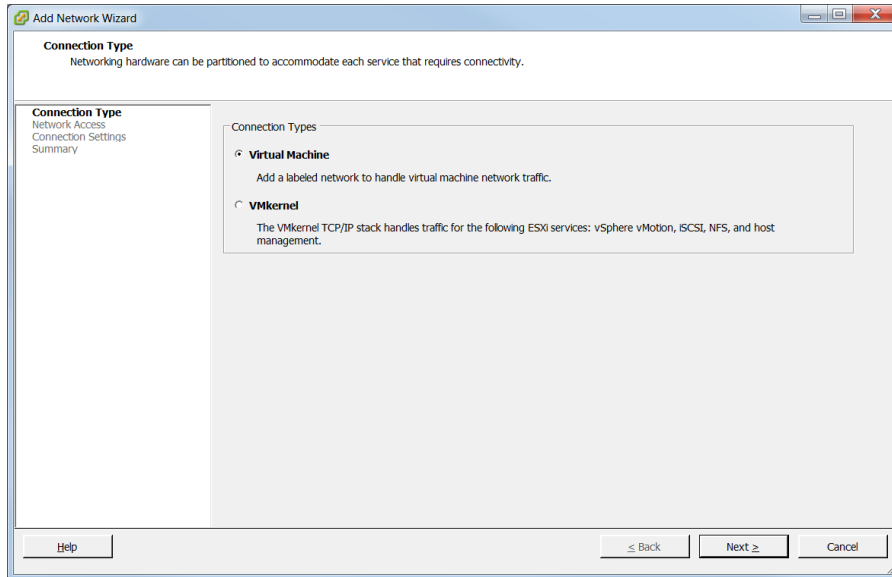
# Step 1: Create a Virtual Switch w/Virtual SPAN Port & Map it to a Physical Port



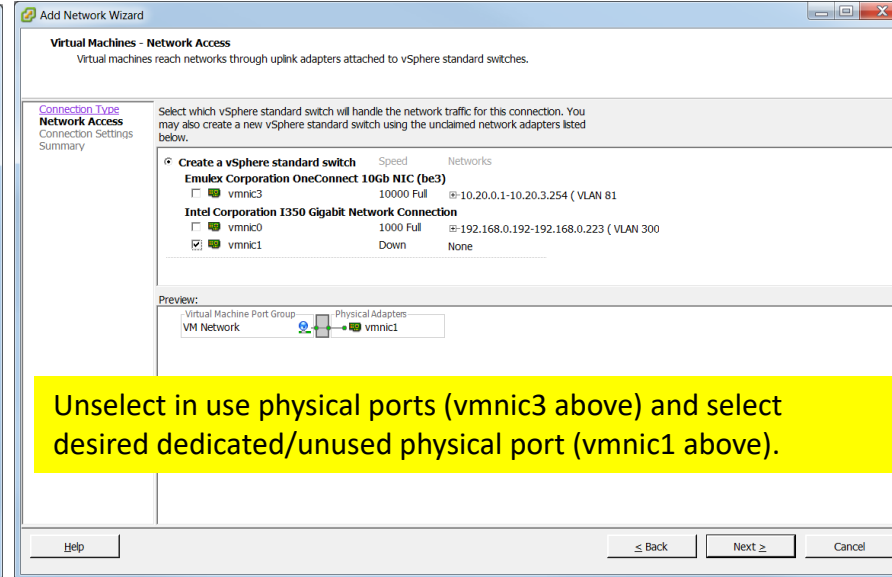
# Step 1-a: Create a Virtual Switch w/Virtual SPAN Port & Map it to a Physical Port

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

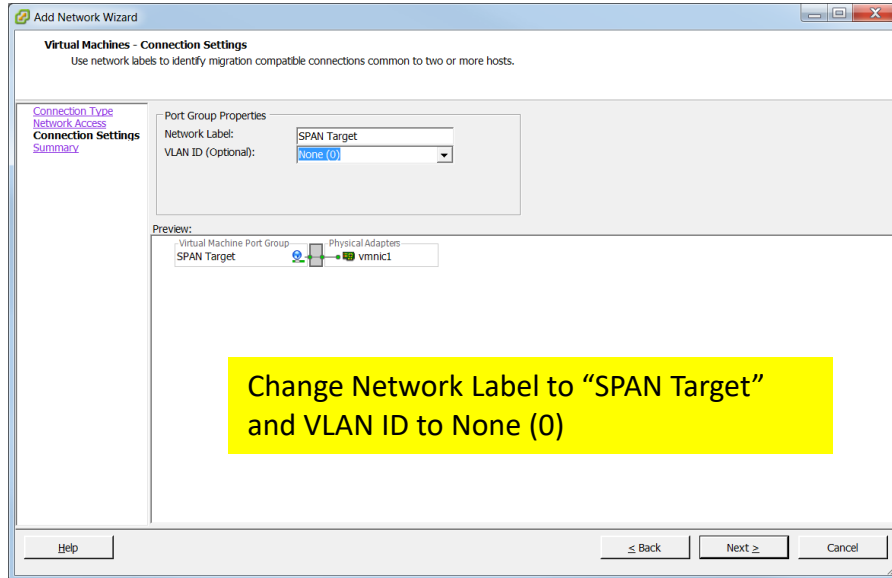
1



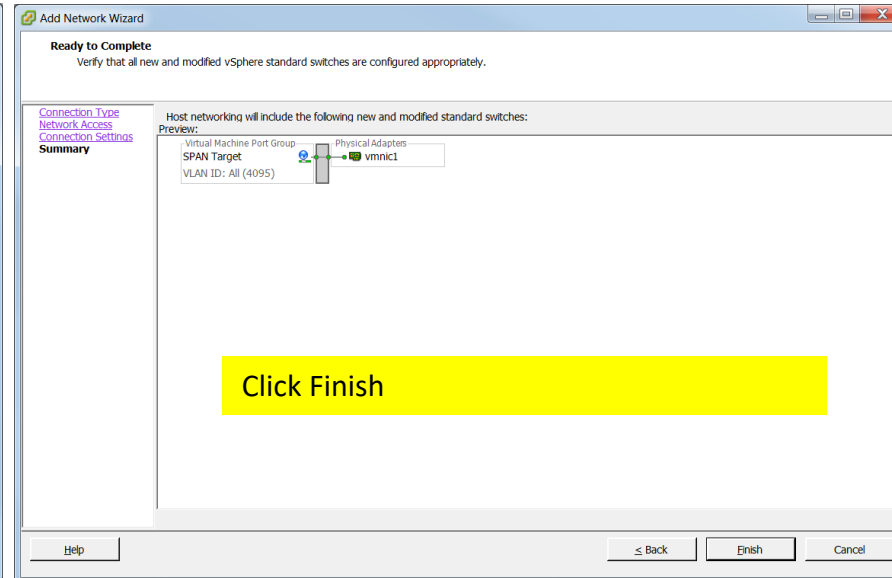
2



3

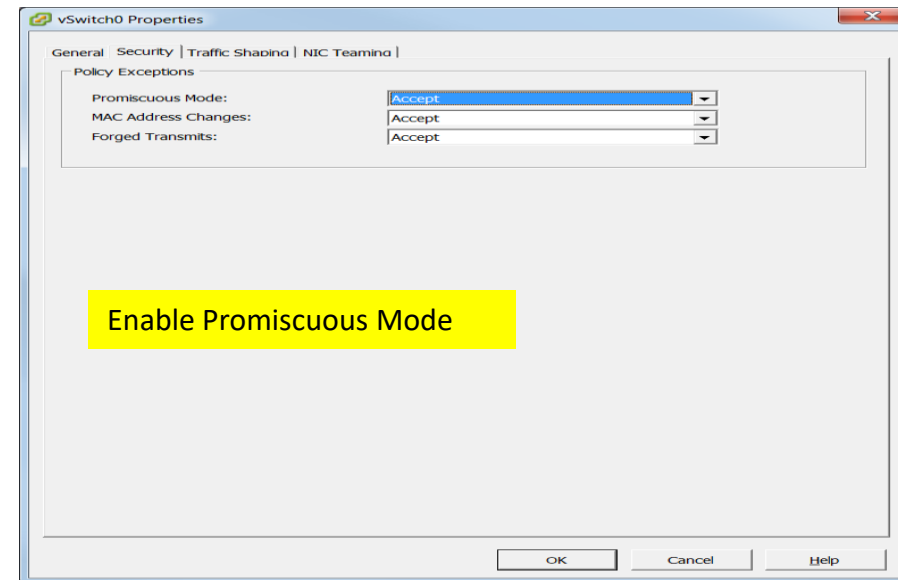
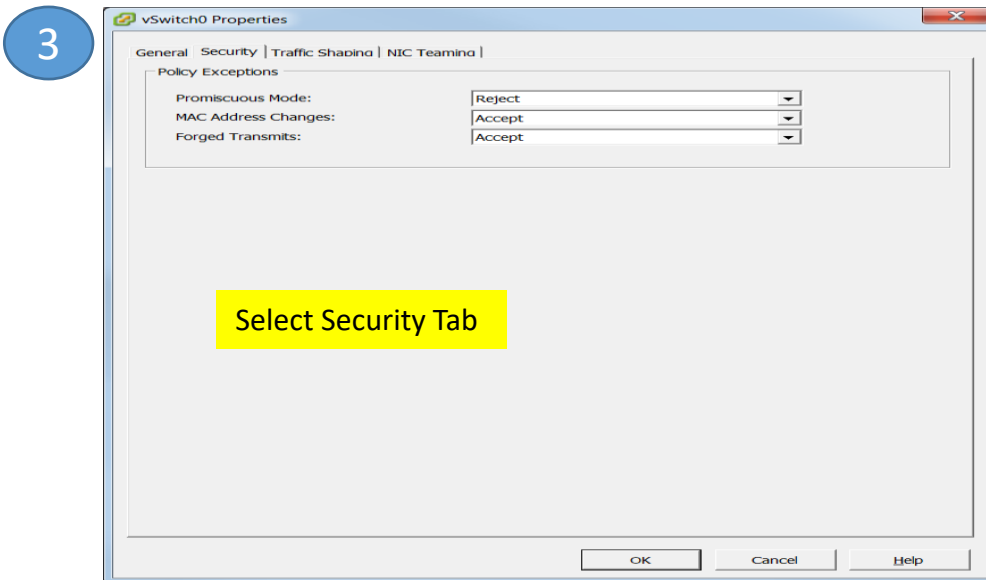
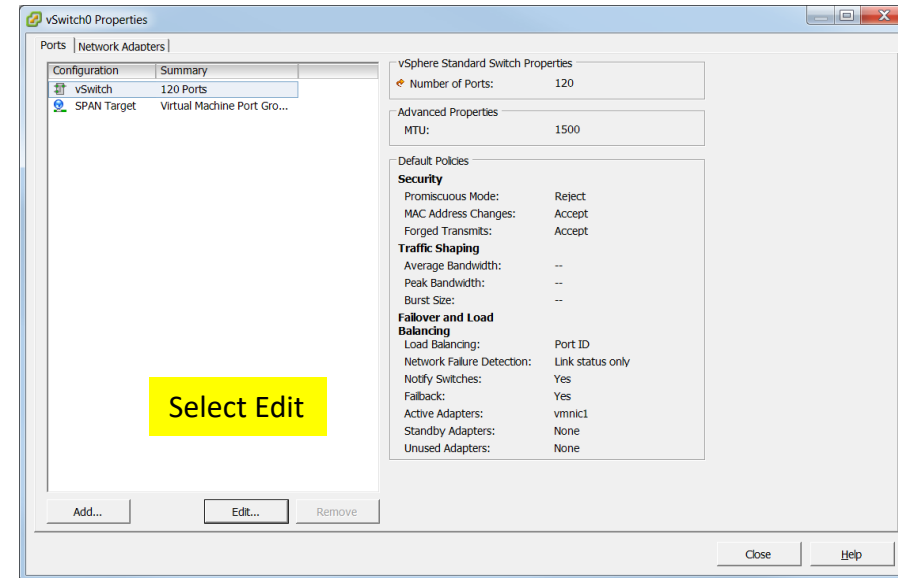
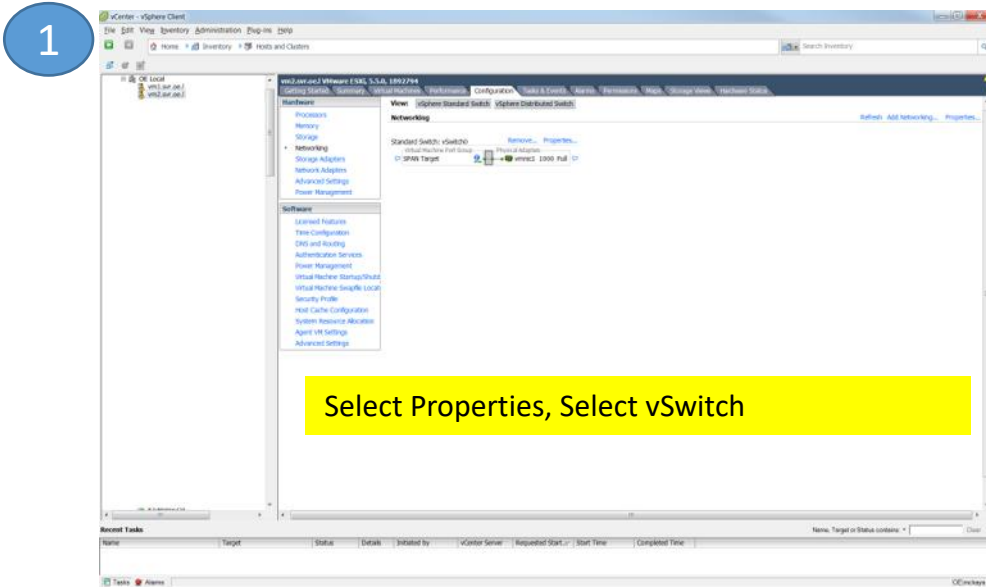


4



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

## --Enable Promiscuous Mode



# 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

Welcome to VMware vCenter Converter Standalone

Convert Machine

- Physical machines
- VMware virtual machines (.vms)
- VMware Consolidated Backup (.vcb)
- Microsoft Virtual PC or Virtual Server virtual machines (.vmc)
- Symantec LiveState Recovery Image (.sv2)
- Acronis True Image Backup (.tib)
- StorageCraft ShadowStor (.spr)
- Parallels Virtualization Products (.pvs)
- Hyper-V virtual machines

2

Source System

Select the source system you want to convert

Source System

Source: none Destination: none

Select source type: VMware Workstation or other VMware virtual machine

Browse for source virtual machine or image

Virtual machine file: .\8e1d\NetWatcher - Virtual\NetWatcher - OVF.vmx

View source details...

Help Export diagnostic logs... < Back Next > Cancel

3

Machine Details for NetWatcher - OVF

Name: NetWatcher - OVF

Machine type: VMware desktop virtual machine

Firmware: BIOS

Operating system: Other (32 bit)

Total size: 500 GB

Number of vCPUs: 4 (4 sockets \* 1 cores)

RAM: 4096 MB

Network: ethernet0, ethernet1

Source disks/volumes layout:

Disk 1 <GPT> - 500 GB

- EFI-SYSTEM (Volume 1) - 62.97 MB used / 128 MB total <FAT>
- (Volume 2) - 2 MB used / 2 MB total <unknown>
- (Volume 3) - 1 GB used / 1 GB total <unknown>
- (Volume 4) - 1 GB used / 1 GB total <unknown>
- (Volume 5) - 128 MB used / 128 MB total <unknown>
- (Volume 6) - 64 MB used / 64 MB total <unknown>
- (Volume 7) - 497.68 GB used / 497.68 GB total <unknown>

Close

Click on source details and it should look like this:

4

Conversion

Destination System

Select a host for the new virtual machine

Source System

Destination System

Select destination type: VMware Infrastructure virtual machine

VMware Infrastructure server details

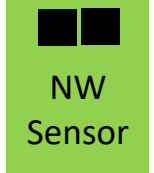
Server: [dropdown]

User name: m

Password: [masked]

Help Export diagnostic logs... < Back Next > Cancel

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





# Step 2-a: Import NetWatcher Sensor VM

1

Click Next and Select Destination directory on vcenter server

2

Select Destination physical server and data store

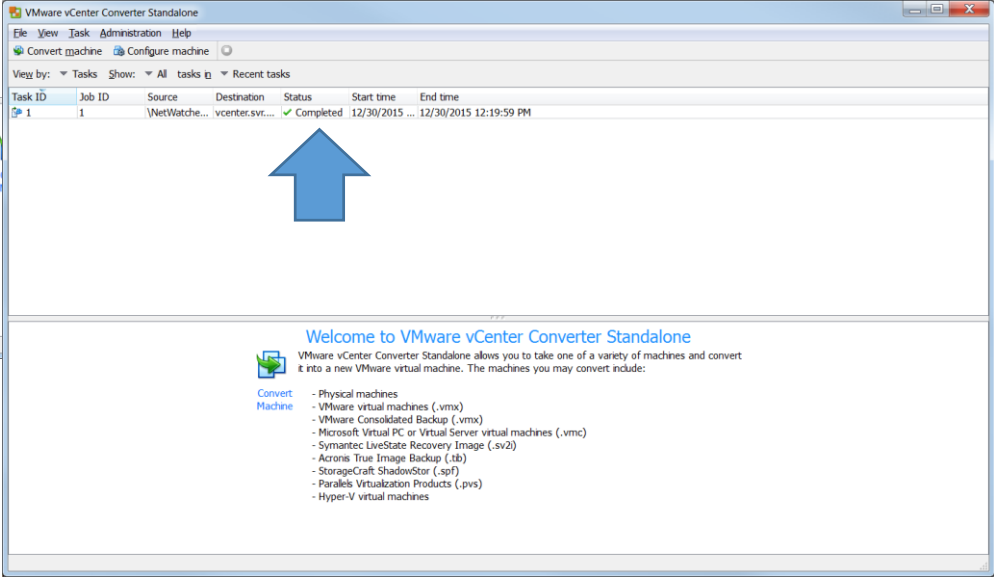
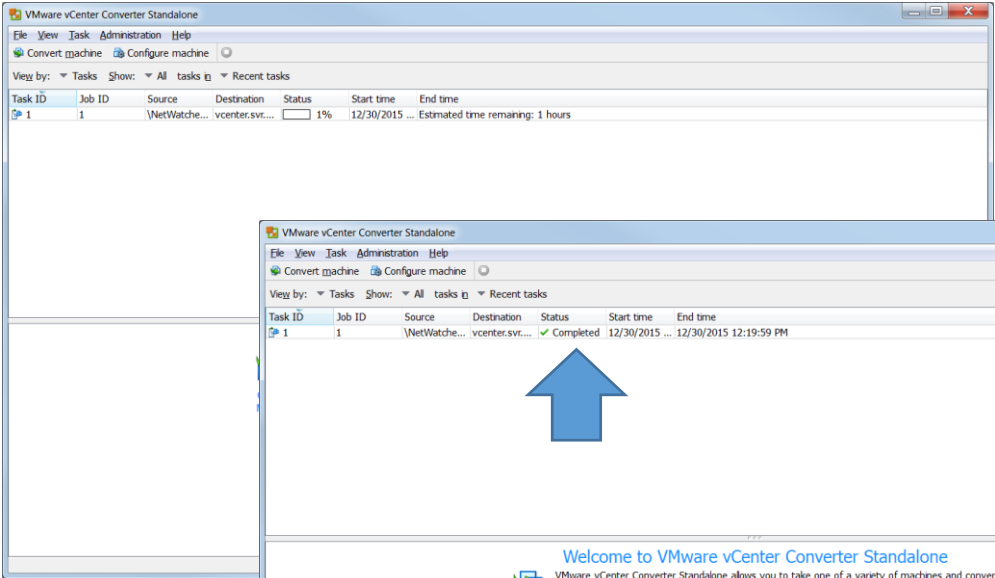
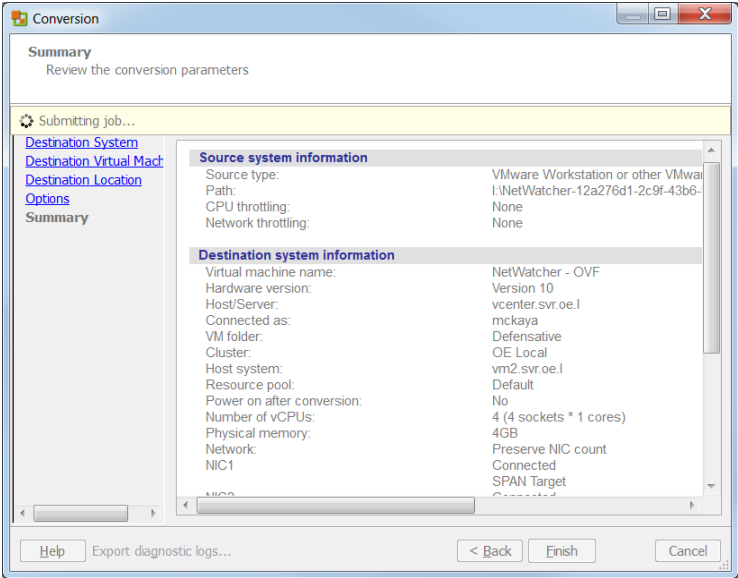
3

Confirm settings

4

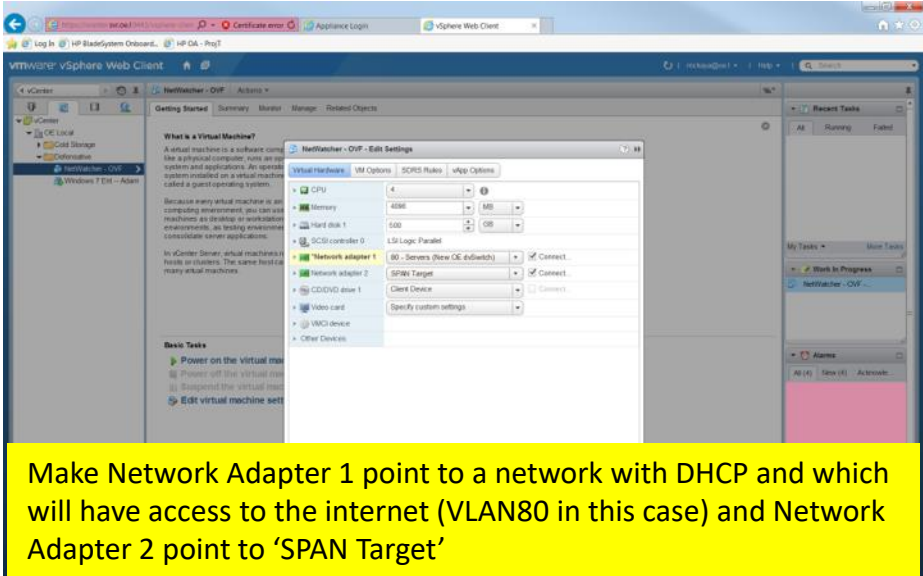
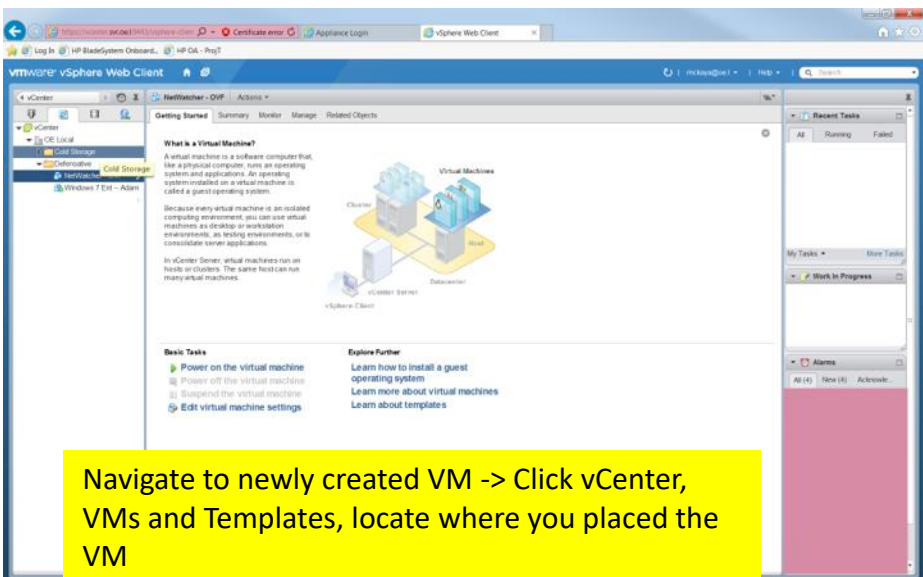
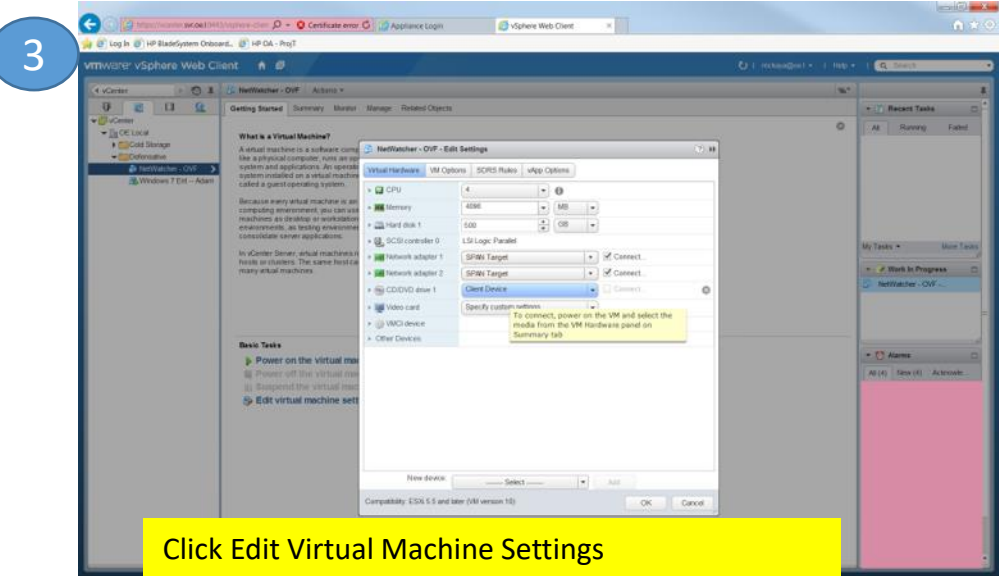
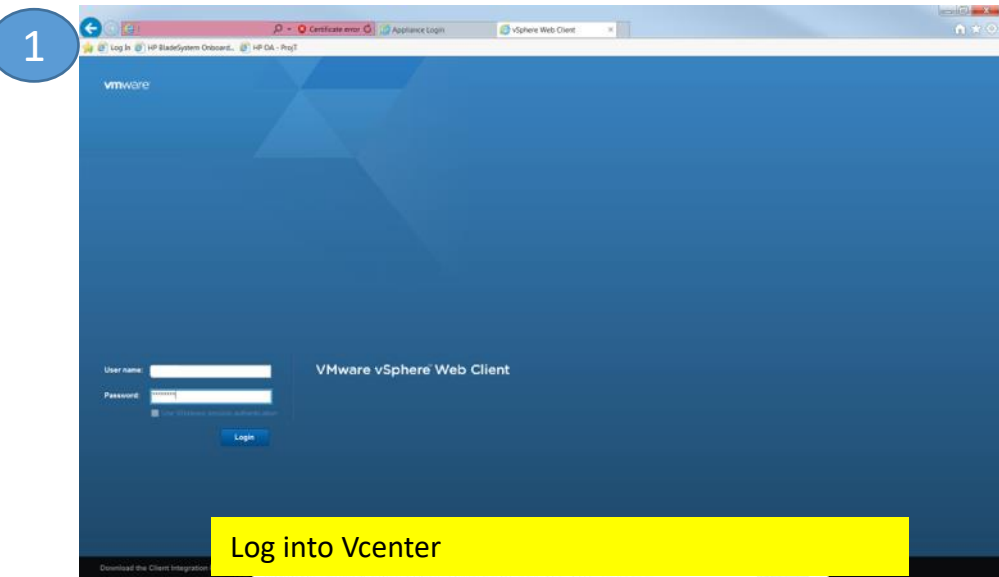
Click Finish

# Step 2-b: Import NetWatcher Sensor VM

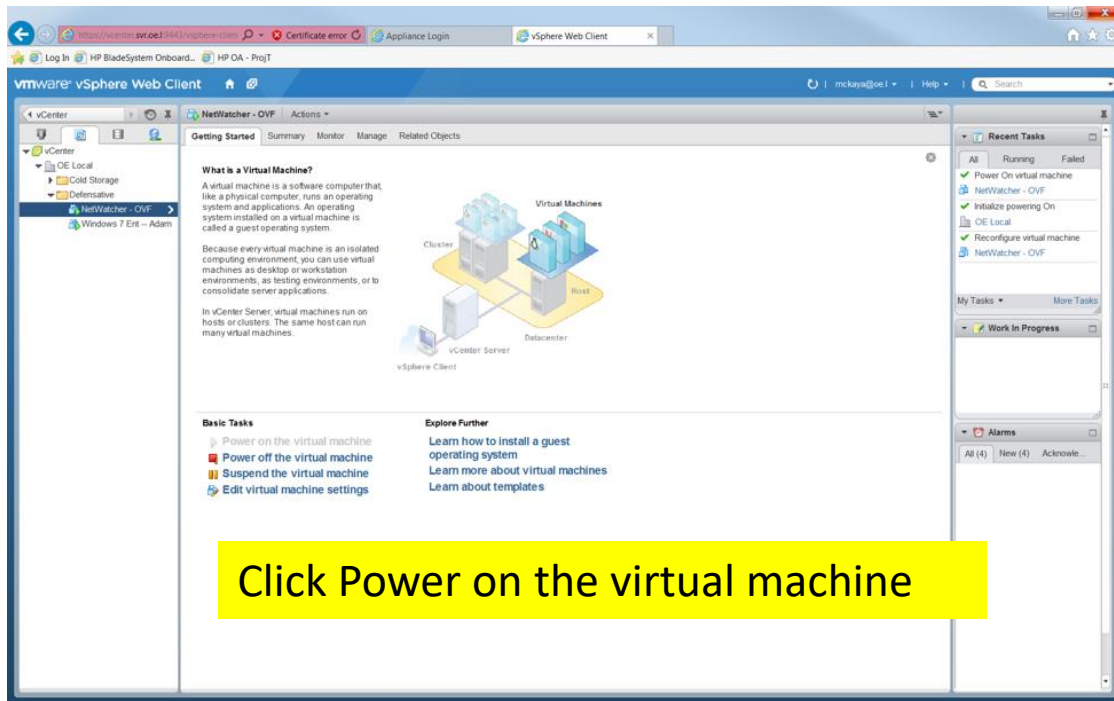


Let it build.

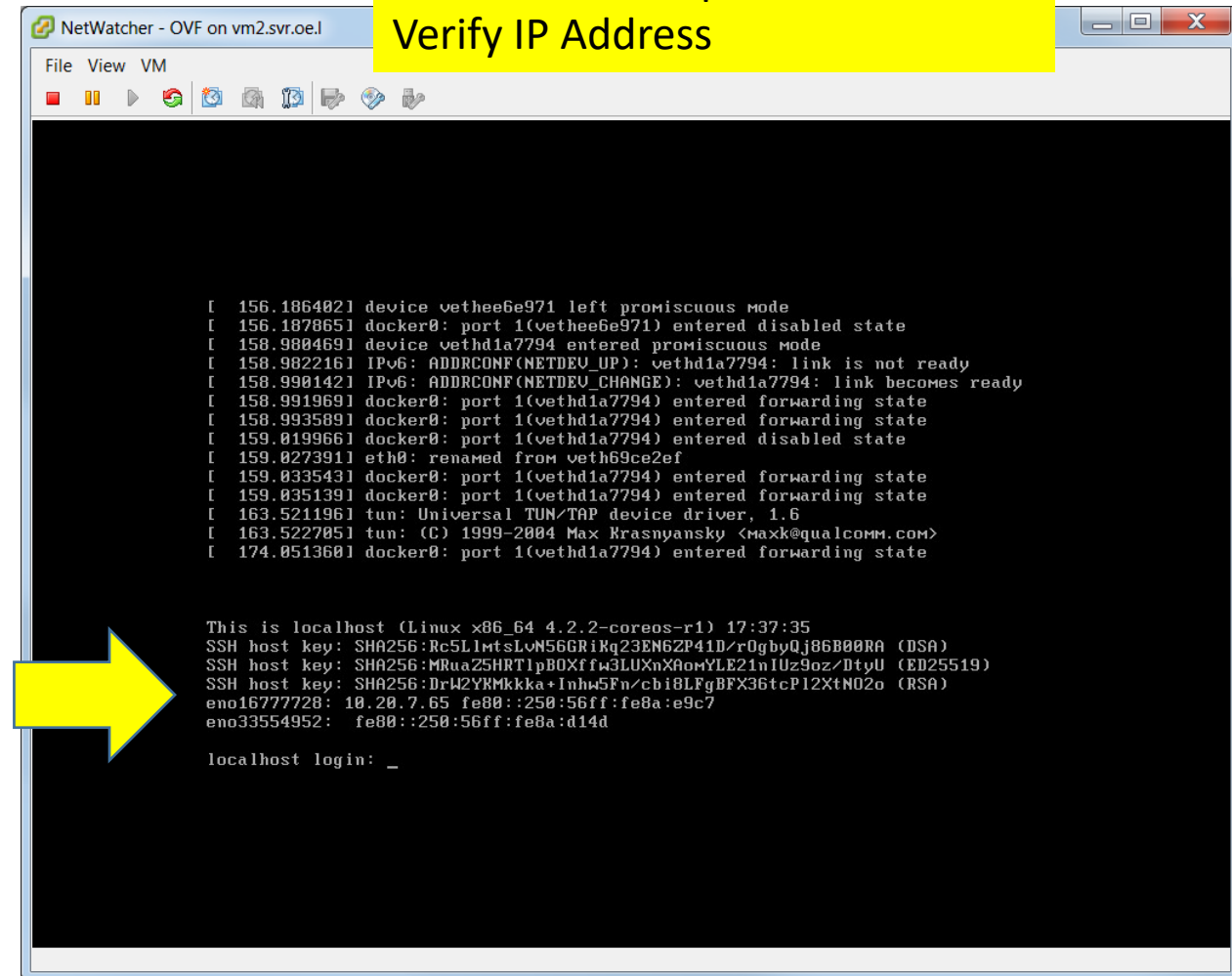
# Step 3: Map NetWatcher Sensors Network Adapter 1 and Network Adapter 2



# Step 4: Open NetWatcher Sensor Console



Click Actions->Open Console  
Verify IP Address



# 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...



The screenshot shows the NetWatcher customer portal interface. At the top, there is a blue header with the NetWatcher logo, a promotional banner for "Invite a friend and get one month free", and a user profile for "Steve Parker" with a "Logout" link. Below the header is a navigation bar with tabs for "Dashboard", "Reports", "Alarms", "Support", "Configure", and "Advanced". A search bar is located on the right side of the navigation bar. Below the navigation bar is a secondary set of tabs: "Contacts", "Subscriptions", "My Sensors" (which is highlighted in blue), "Sensor Groups", "Agents", and "Network". The main content area is titled "My Sensors" and contains a table with the following columns: "Alive", "ID", "Name", "IP", "Port", "Events", "Alarms", "Date", and "Groups". The table has one row with a green dot in the "Alive" column, indicating the sensor is live. The "ID" is "6007420e-1253-44ab-8327-993b8b7c49bf", the "Name" is "madwolf-virtual1", "Events" is "0", "Alarms" is "0", and "Date" is "Dec-16-15". Below the table, there is a "Display: 100" dropdown menu and pagination controls showing "1" of 1 page.

Alive	ID	Name	IP	Port	Events	Alarms	Date	Groups
●	6007420e-1253-44ab-8327-993b8b7c49bf	madwolf-virtual1			0	0	Dec-16-15	

# 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](https://portal.netwatcher.com) => Used for credential management
  - UDP 443 to [vpn.netwatcher.com](https://vpn.netwatcher.com) => connection to backend, SSL VPN
  - TCP 80 to [google.com](https://google.com) => Used to test internet/DNS connectivity
  - TCP 443 (HTTPS) to [index.docker.io](https://index.docker.io) (secure Docker container download)
  - TCP 443 (HTTPS) to [public.update.core-os.net](https://public.update.core-os.net) (CoreOS updates)