

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.

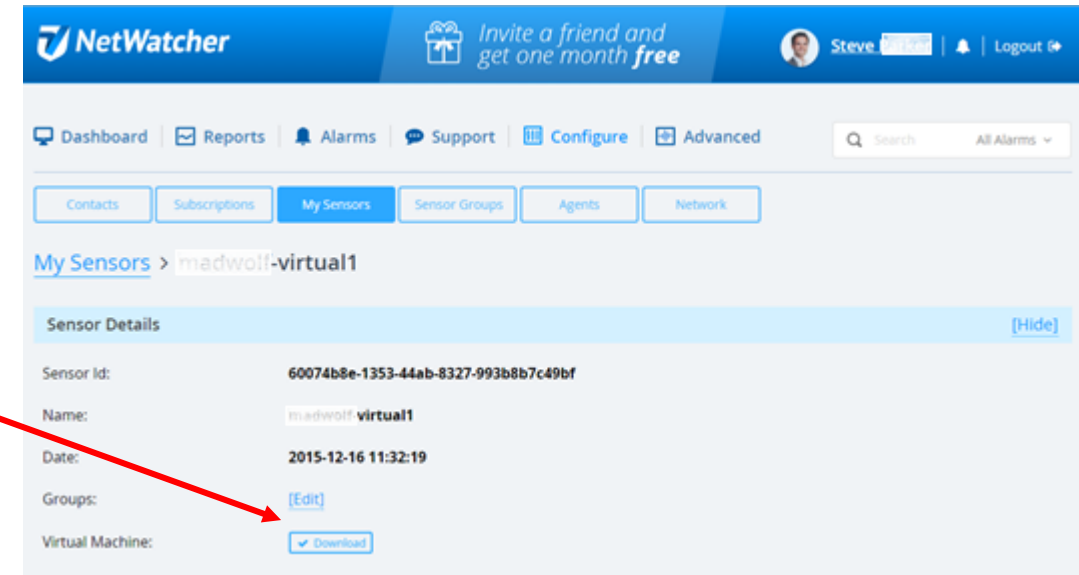
How to download the Virtual Machine/Sensor:

- Once you log in to your account, navigate to <https://portal.netwatcher.com/configure/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 a user profile for Steve. Below the navigation bar, there are tabs for Dashboard, Reports, Alarms, Support, Configure, and Advanced. A search bar is also present. The main content area shows a table of sensors under the 'My Sensors' tab. The table has columns for Alive, ID, Name, IP, Port, Events, Alarms, Date, and Groups. A red arrow points from the 'Name' column to the 'madwolf-virtual1' sensor entry.

Alive	ID	Name	IP	Port	Events	Alarms	Date	Groups
●	60074b8e-1353-44ab-8327-993b8b7c49bf	madwolf-virtual1			0	0	Dec-16-15	

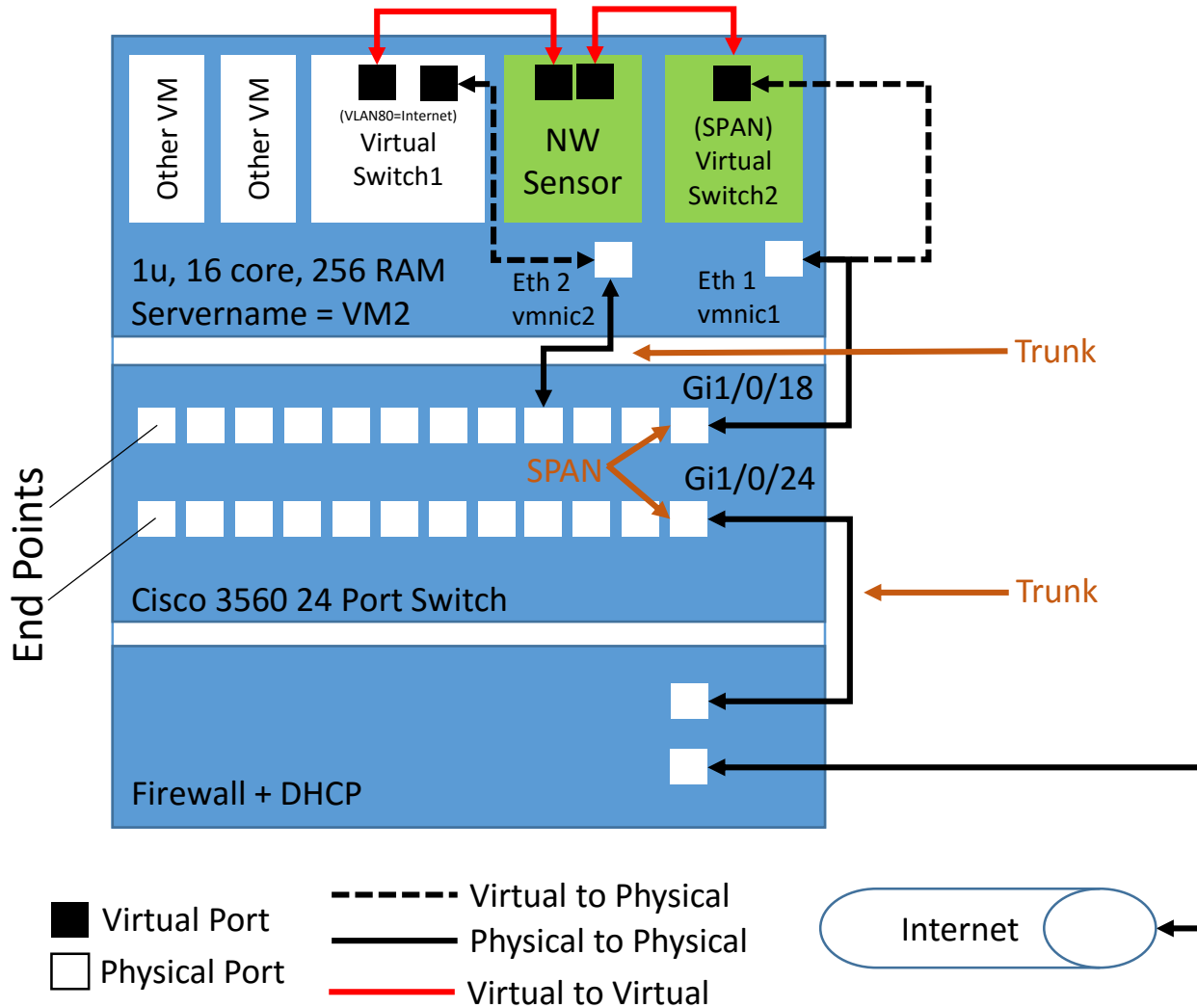


The screenshot shows the 'Sensor Details' page for the 'madwolf-virtual1' sensor. The page has a breadcrumb trail 'My Sensors > madwolf-virtual1'. The details are as follows:

Sensor Id:	60074b8e-1353-44ab-8327-993b8b7c49bf
Name:	madwolf-virtual1
Date:	2015-12-16 11:32:19
Groups:	[Edit]
Virtual Machine:	[Download]

A red arrow points from the 'Download' button to the 'Virtual Machine' field.

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)

■ 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
```

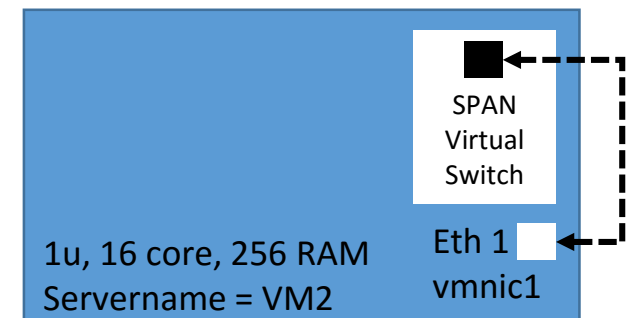
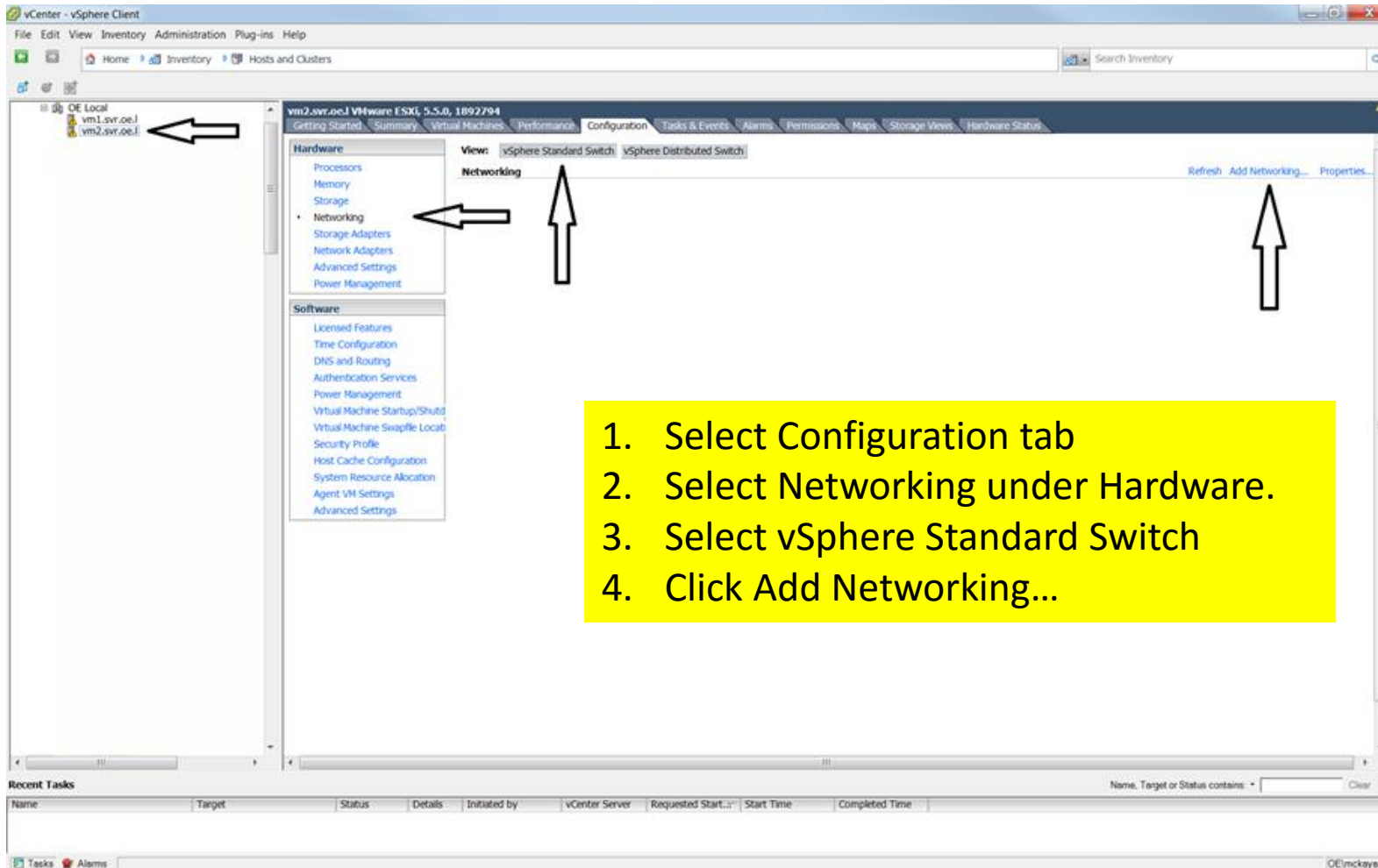
Ensure there is a physical cable connecting this destination port (Gi1/0/18 in this example) to the VMWare host physical port (vm2:vmnic1 in this example)

Note:

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

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

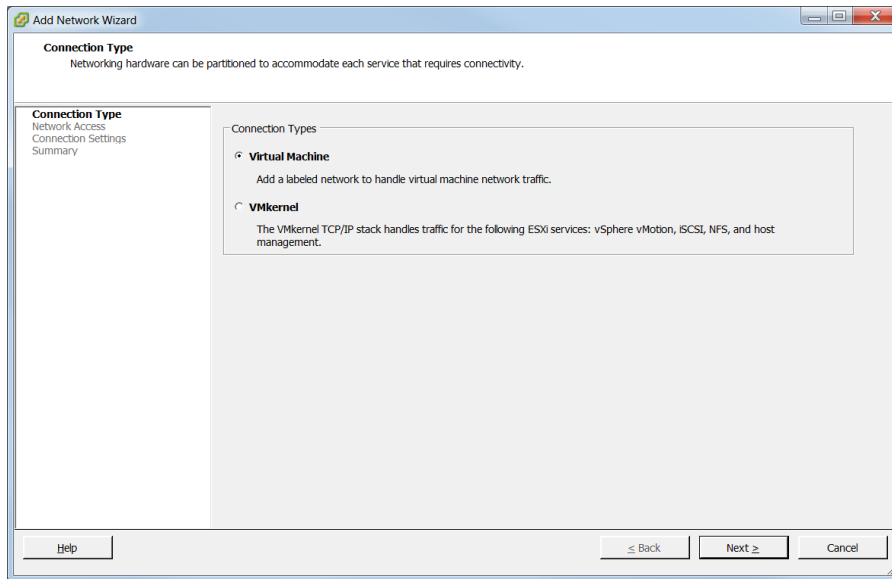
Step 1: Create a Virtual Switch w/Virtual SPAN Port & Map it to a Physical Port



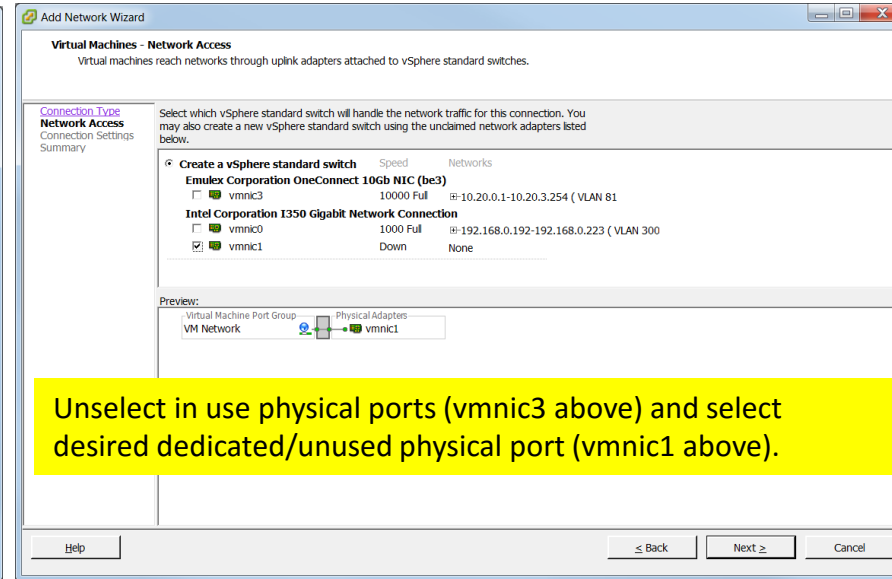
Step 1-a: Create a Virtual Switch w/Virtual SPAN Port & Map it to a Physical Port

--Create the SPAN Port to mirror all traffic

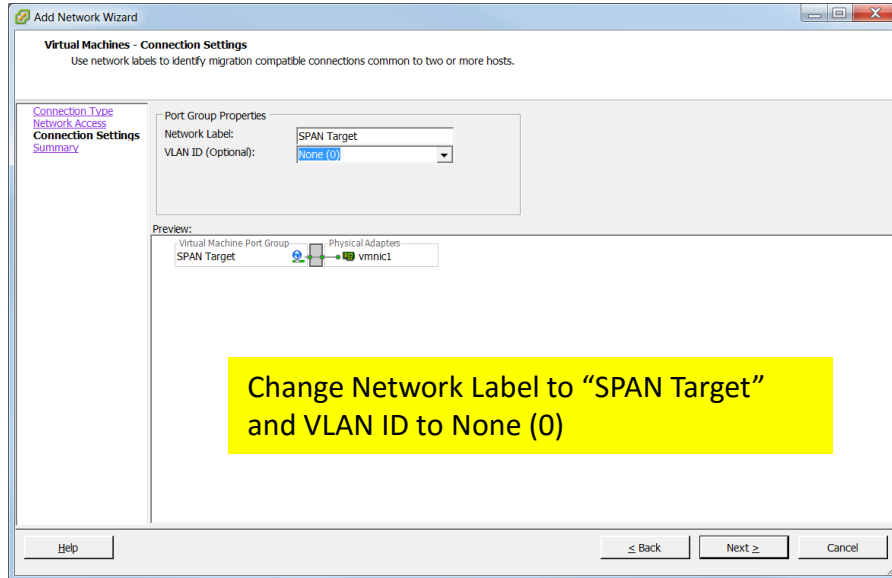
1



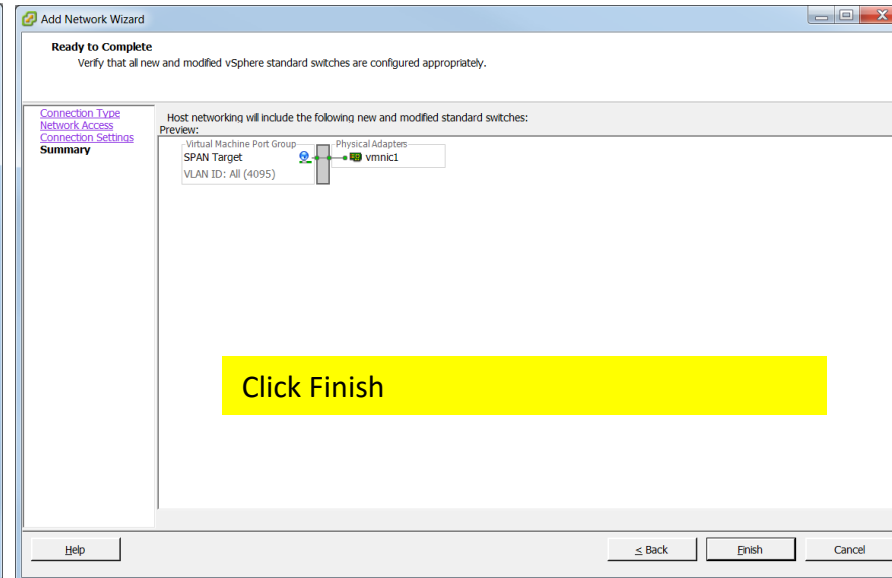
2



3

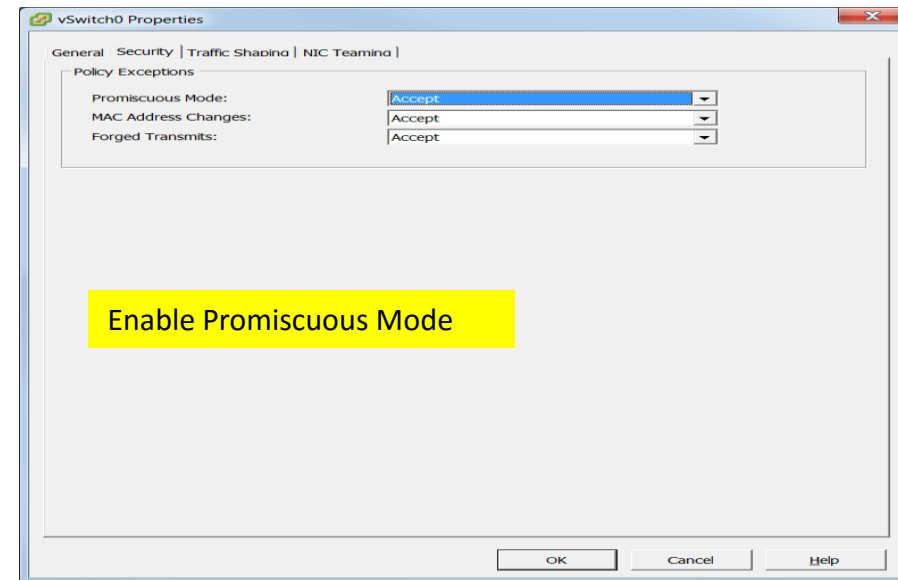
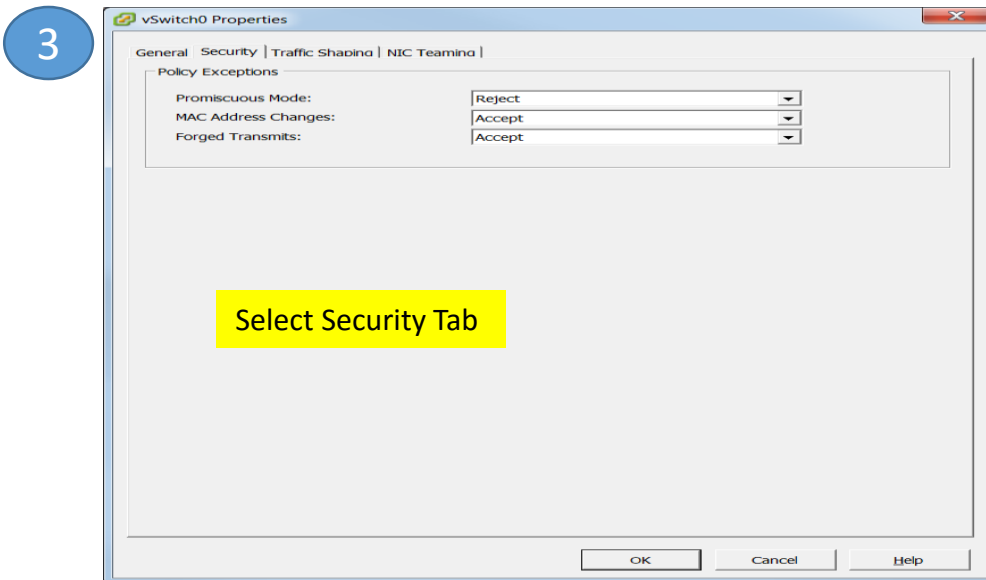
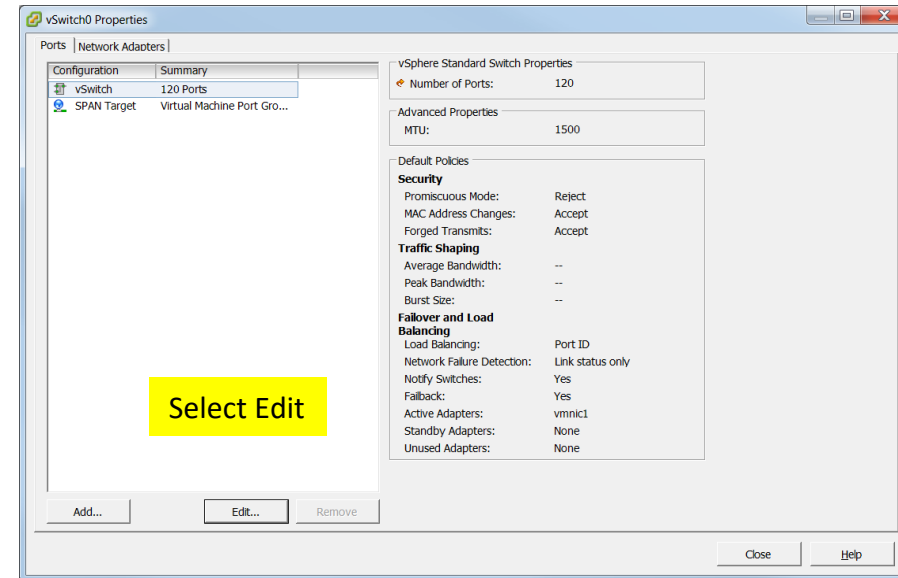
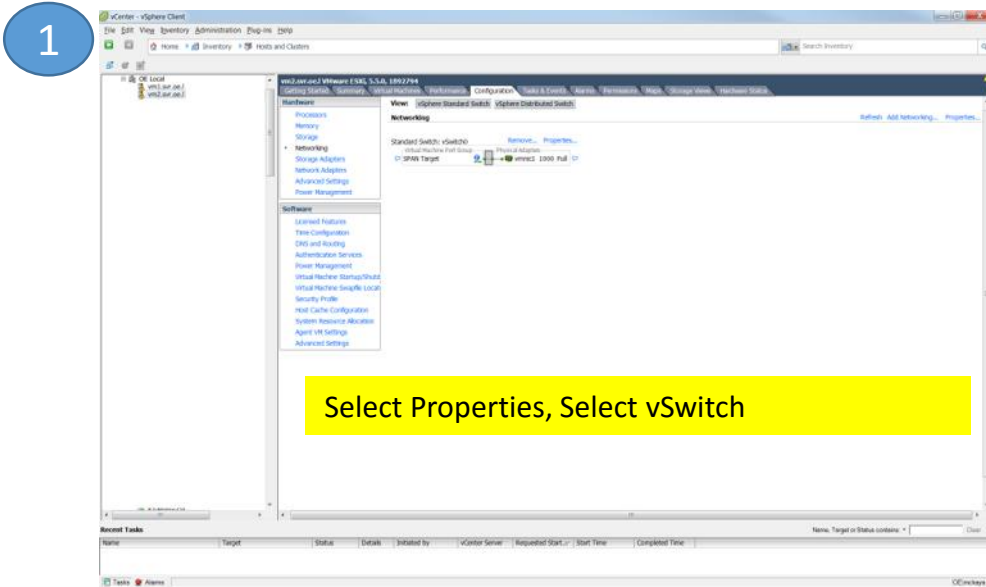


4



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 ShadowStar (.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

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]

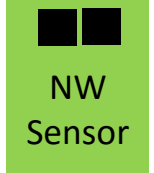
User name: m

Password: [masked]

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

Click on source details and it should look like this:

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

Destination Virtual Machine
Select the destination VM name and folder

Source System: I:\NetWatc...\NetWatcher - OVF.vmx (Other (32-bit)) Destination: Net...

Destination System: Net...

Destination Virtual Machine: Name: NetWatcher - OVF

Inventory for: vcenter.svr.oe.l Search for name with: Clear

VM name	Power state
Windows 7 Ent -- Adam Running	

Click Next and Select Destination directory on vcenter server

2

Destination Location
Select the location for the new virtual machine

Source System: I:\NetWatc...\NetWatcher - OVF.vmx (Other (32-bit)) Destination: Net...

Destination System: Net...

Destination Location: Inventory for: vcenter.svr.oe.l Total source disks size: 500 GB

OE Local
vm1.svr.oe.l
vm2.svr.oe.l
vm3.svr.oe.l
vm4.svr.oe.l

Datastore
USE ME - zStax-NFS

Capacity: 14,381.59 GB
Free: 2,442.24 GB
Type: NFS

Virtual machine version
Version 10

Select Destination physical server and data store

3

Options
Set up the parameters for the conversion task

Source System: I:\NetWatcher...\NetWatcher - OVF.vmx (Other (32-bit)) Destination: Net...

Destination System: Net...

Destination Location: vcenter.svr.oe.l

Click on an option below to edit it.

Current settings:

- Data to copy: Copy type: Disk-based, VirtualDisk1: 500 GB
- Devices: vCPUs: 4 (4 sockets * 1 cores), Disk controller: Preserve source, Memory: 4GB
- Networks: NIC1: SPAN Target, NIC2: SPAN Target
- Advanced options: Power on destination: No, Install VMware Tools: N/A, Customize Guest OS: N/A, Reconfigure: N/A
- Throttling: CPU: None, Network bandwidth: None

Confirm settings

4

Summary
Review the conversion parameters

Source System: I:\NetWatcher...\NetWatcher - OVF.vmx (Other (32-bit)) Destination: Net...

Destination System: Net...

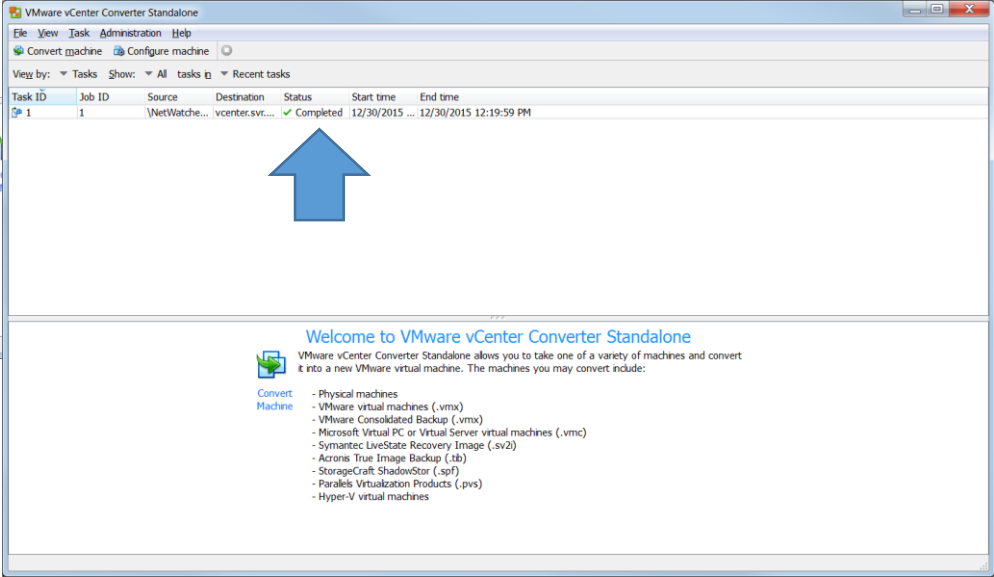
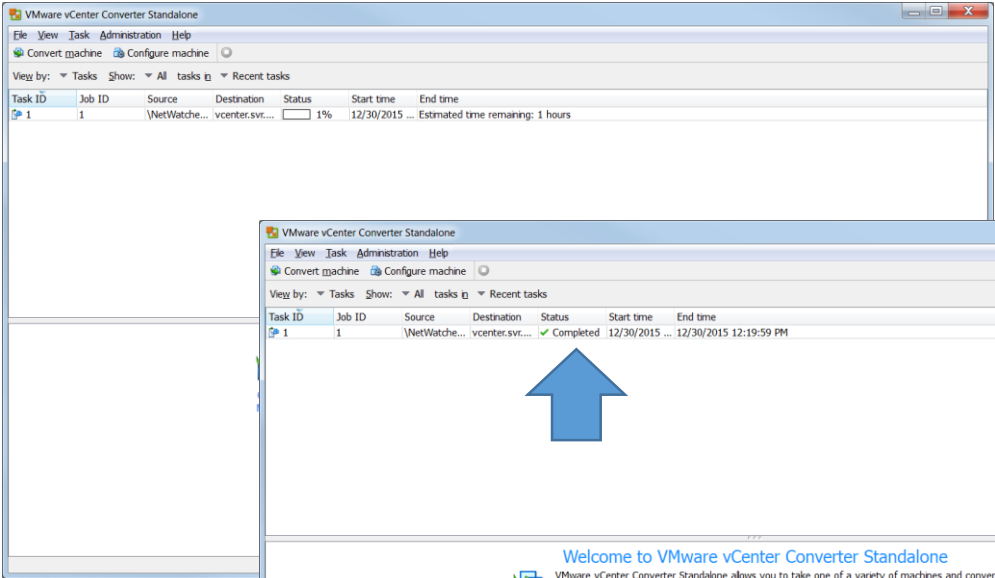
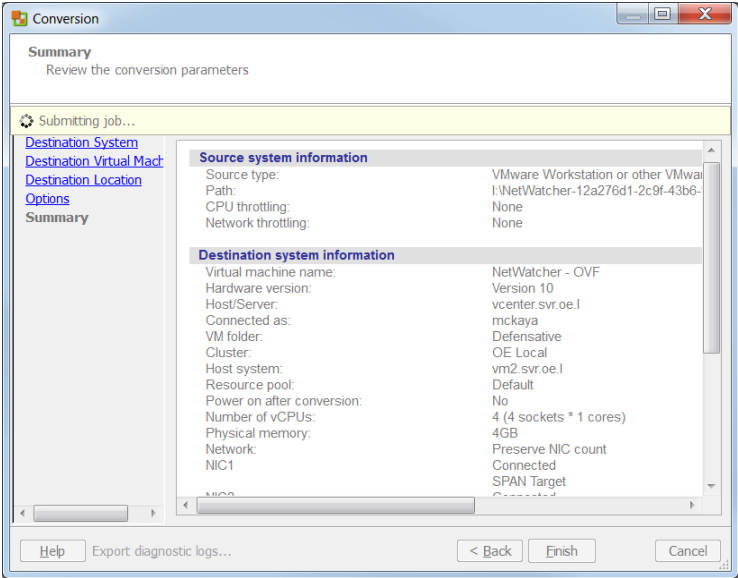
Destination Location: vcenter.svr.oe.l

Click Finish

Source system information
Source type: VMware Workstation or other VMwa
Path: I:\NetWatcher-12a276d1-2c9f-43b6-
CPU throttling: None
Network throttling: None

Destination system information
Virtual machine name: NetWatcher - OVF
Hardware version: Version 10
Host/Server: vcenter.svr.oe.l
Connected as: mckaya
VM folder: Defensative
Cluster: OE Local
Host system: vm2.svr.oe.l
Resource pool: Default
Power on after conversion: No
Number of vCPUs: 4 (4 sockets * 1 cores)
Physical memory: 4GB
Network: Preserve NIC count
NIC1: Connected
SPAN Target: Connected

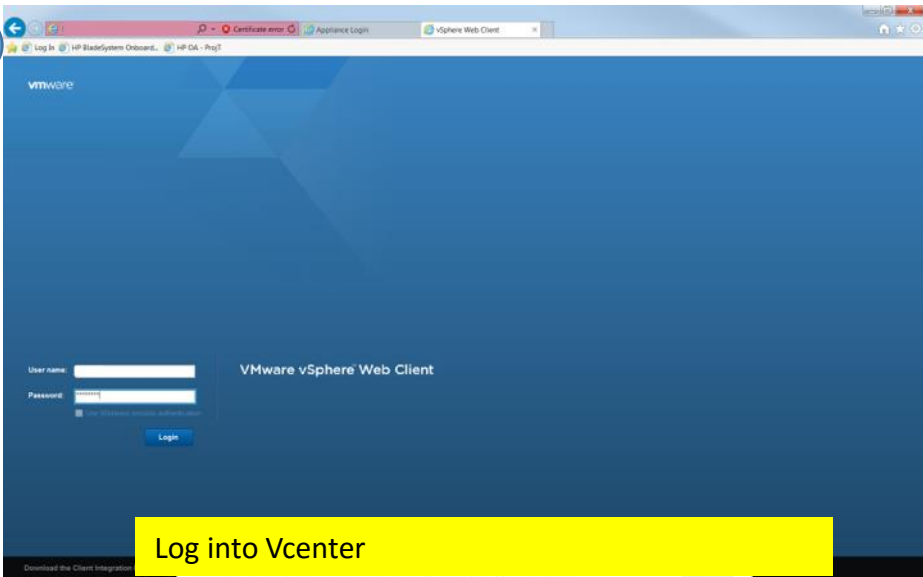
Step 2-b: Import NetWatcher Sensor VM



Let it build.

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

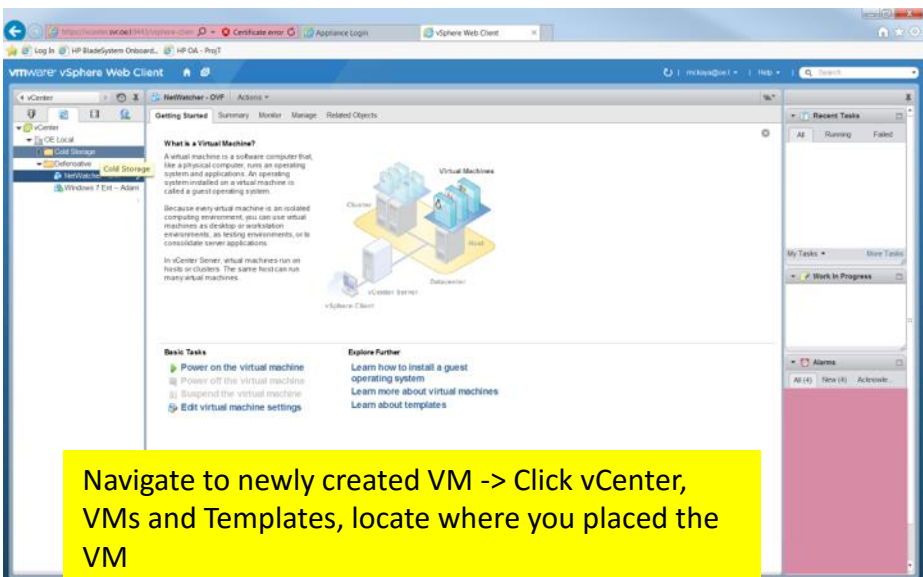
1



Log into Vcenter

The screenshot shows the VMware vSphere Web Client login page. The user name and password fields are visible, along with a 'Login' button. A yellow box highlights the 'Log into Vcenter' instruction.

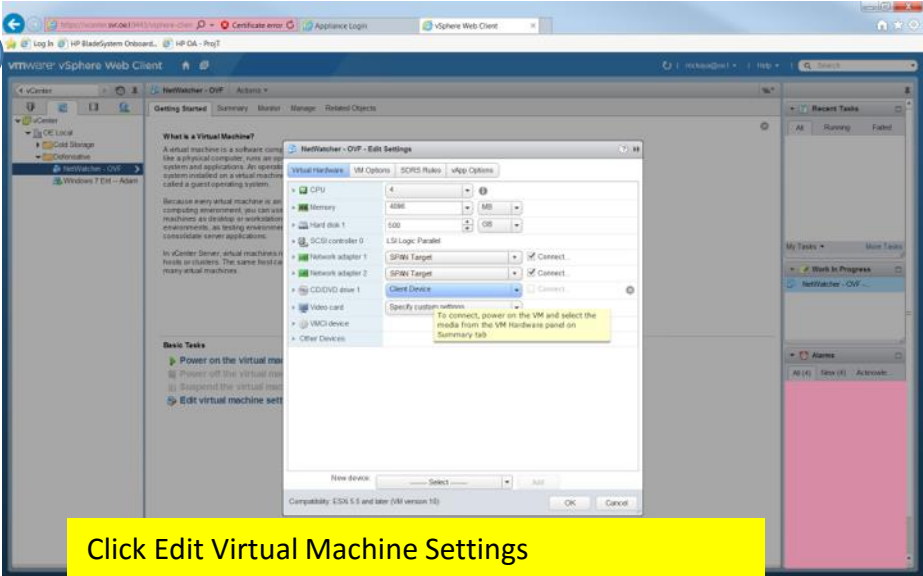
2



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

The screenshot shows the VMware vSphere Web Client interface. The 'vCenter' tree view on the left shows the path: vCenter > VMs and Templates > [Location]. A yellow box highlights the instruction to navigate to the newly created VM.

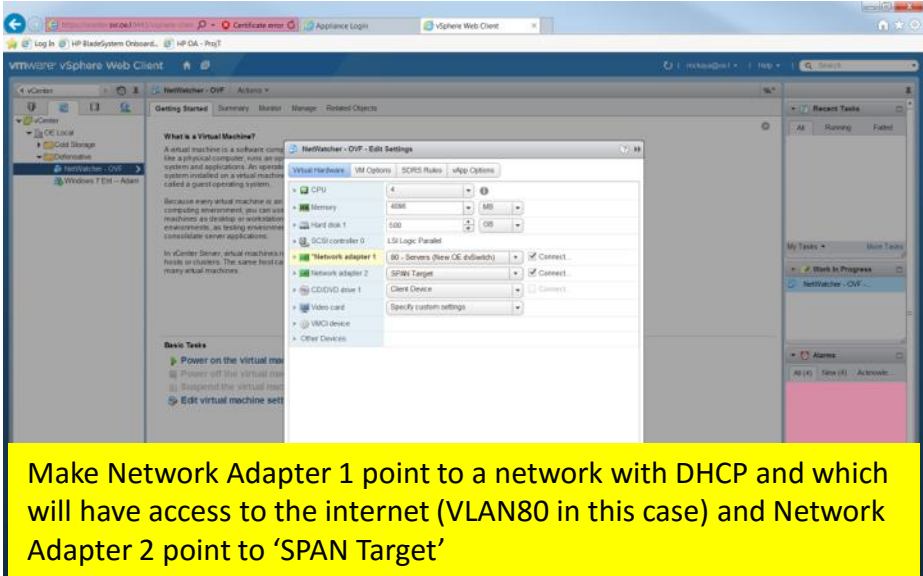
3



Click Edit Virtual Machine Settings

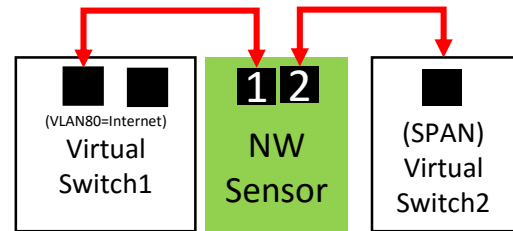
The screenshot shows the 'Edit Settings' dialog for a virtual machine. The 'Network Adapter 1' is selected, and the 'Client Device' is set to 'Client Device'. A yellow box highlights the instruction to click 'Edit Virtual Machine Settings'.

4

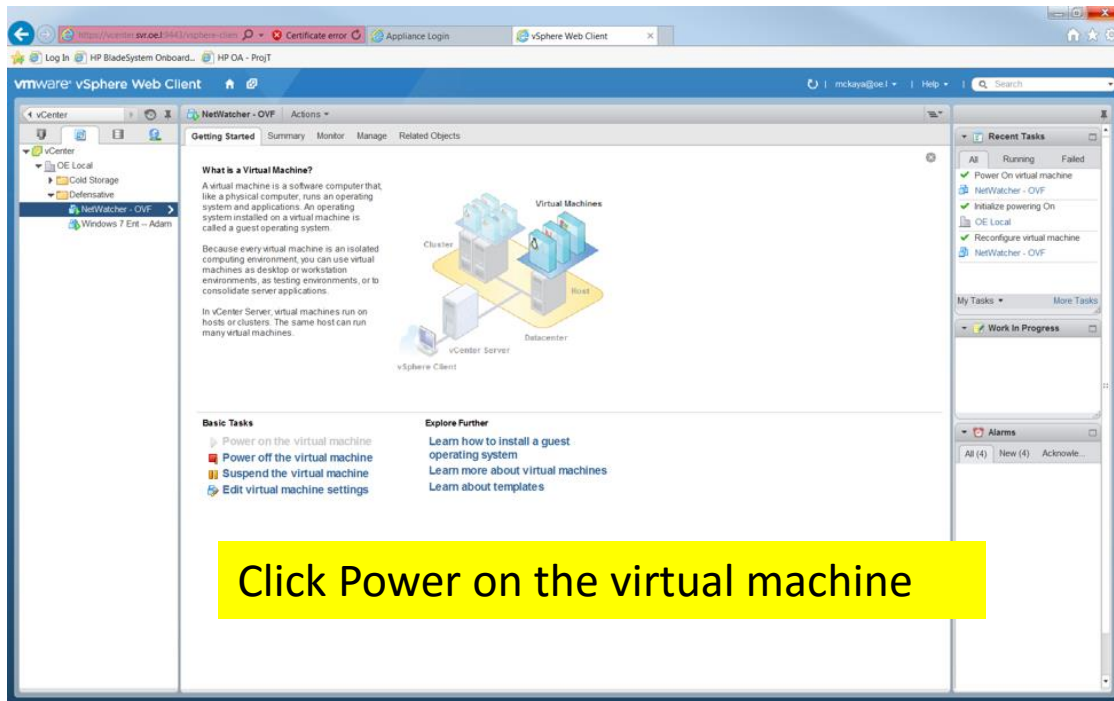


Make Network Adapter 1 point to a network with DHCP and which will have access to the internet (VLAN80 in this case) and Network Adapter 2 point to 'SPAN Target'

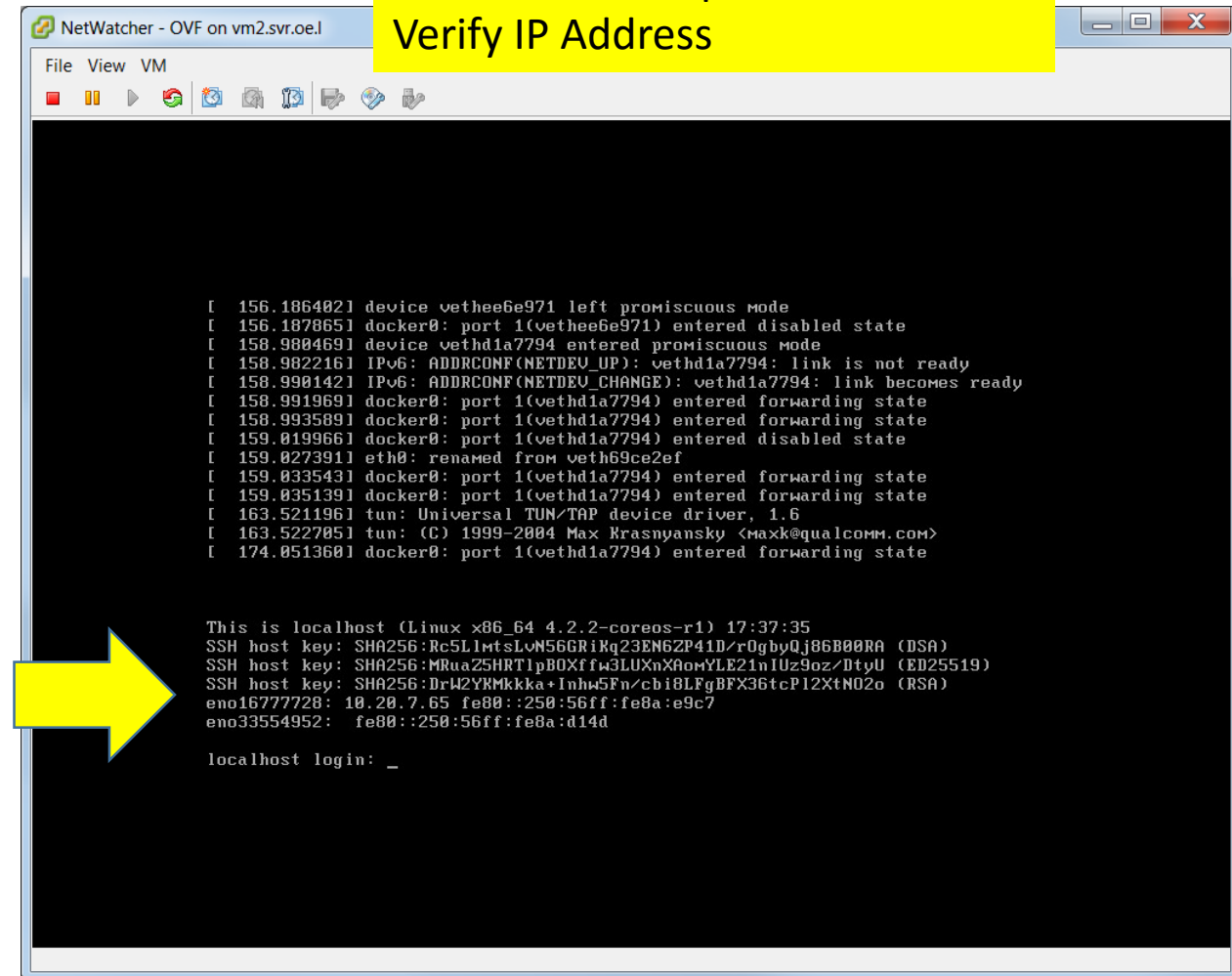
The screenshot shows the 'Edit Settings' dialog for a virtual machine. The 'Network Adapter 1' is set to 'VMXNET3 Adapter' and 'Network adapter 1' is selected. The 'Network adapter 2' is set to 'VMXNET3 Adapter' and 'SPAN Target' is selected. A yellow box highlights the instruction to configure the network adapters.



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. The top navigation bar includes the NetWatcher logo, a promotional banner for "Invite a friend and get one month free", and the user profile for Steve Parker with a Logout button. Below the navigation bar are tabs for Dashboard, Reports, Alarms, Support, Configure, and Advanced. A secondary set of tabs includes Contacts, Subscriptions, My Sensors (which is highlighted), Sensor Groups, Agents, and Network. The "My Sensors" section displays a table with the following data:

Alive	ID	Name	IP	Port	Events	Alarms	Date	Groups
●	6007428e-1253-444b-8327-993b857c49bf	madwolf-virtual1			0	0	Dec-16-15	

At the bottom of the table, there is a "Display: 100" dropdown menu and pagination controls showing "1" of 1 items.

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)