Sensor Deployment

How-To Guide

Document Revision: 1.5
August 17, 2020

System Requirements

Prior to deploying a sensor, be sure to review the requirements below to ensure you meet the minimal hardware and/or software requirements of a sensor.

Hypervisor: VMware® vSphere 5.1 or above
RAM: 16GB
CPU: 4 cores, 2.4Ghz
Disk: 500 GB

Section-1 VMware vSphere/ESXi Sensor Deployment

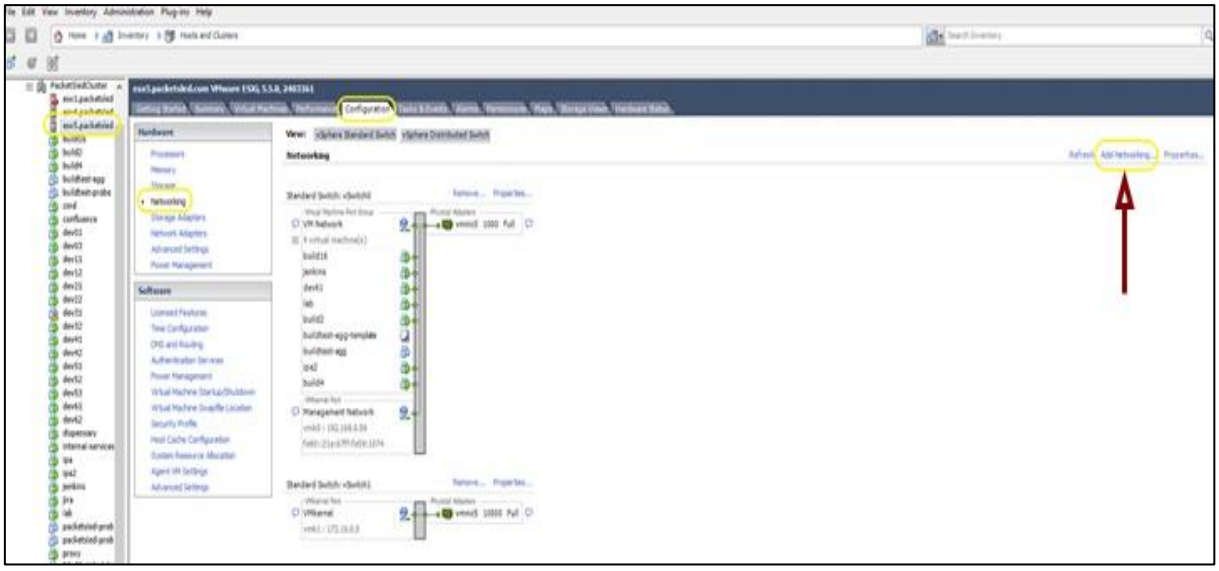
There are four (4) steps in the deployment of a MixMode sensor on virtual hardware:

1. Create and configure a virtual switch.
2. Download the MixMode OVA file and import it into a virtual machine.
3. Configure the virtual machine as a MixMode sensor.
4. Test the sensor.

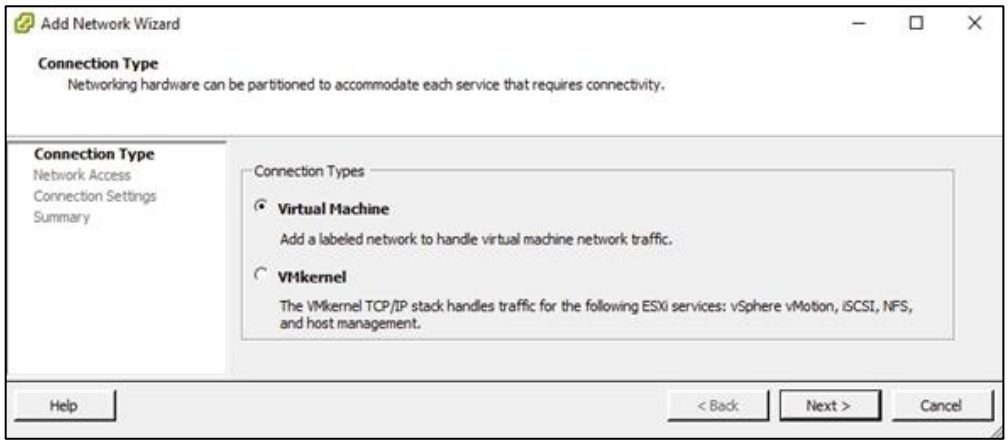
1. Create and configure a virtual switch.

1.1 Create a virtual switch in your *vSphere* environment.

The first step in a virtual sensor deployment is to create a new virtual switch in your *vSphere* environment. From the *vSphere* console open the "*Configuration Tab*" and then click on the "*Add Networking*" link in the upper right side of the interface as shown in *Figure 1-1.*



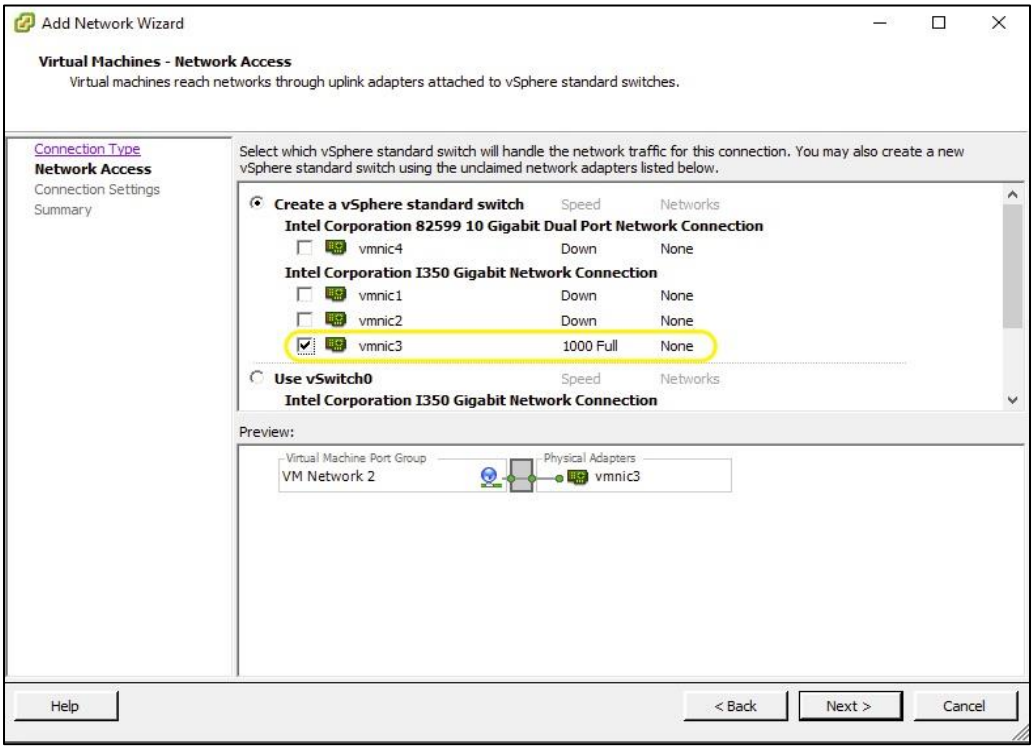
Next, click on the "Virtual Machine" radio button in the "*Connection Types*" dialog and then click "*Next*" as shown in *Figure 1-2*.



2.1 Add a virtual network interface card.

The networking wizard will next ask you to create a virtual switch so the VM can access the network. Click on the *"Create a vSphere standard switch"* and then select the virtual network interface card (vmnic) that you will use to feed network data to your sensor. This is shown in *Figure 1-3*. Remember, this must be a dedicated physical NIC in your *vSphere* environment that is connected to a SPAN, TAP, or port aggregator.

Once the correct vmnic has been selected, click "*Next*."



In the next dialog window, you are asked to configure your "*Port Group Properties.*" You need to enter a "*Network Label.*" It is important that you enter a unique identifier. In the sample screen shot shown in *Figure 1-4*, we have named our port group "*DMZ SPAN.*" For VLAN ID, select All (4095). Once you have entered a name and selected the VLAN, click "*Next*."

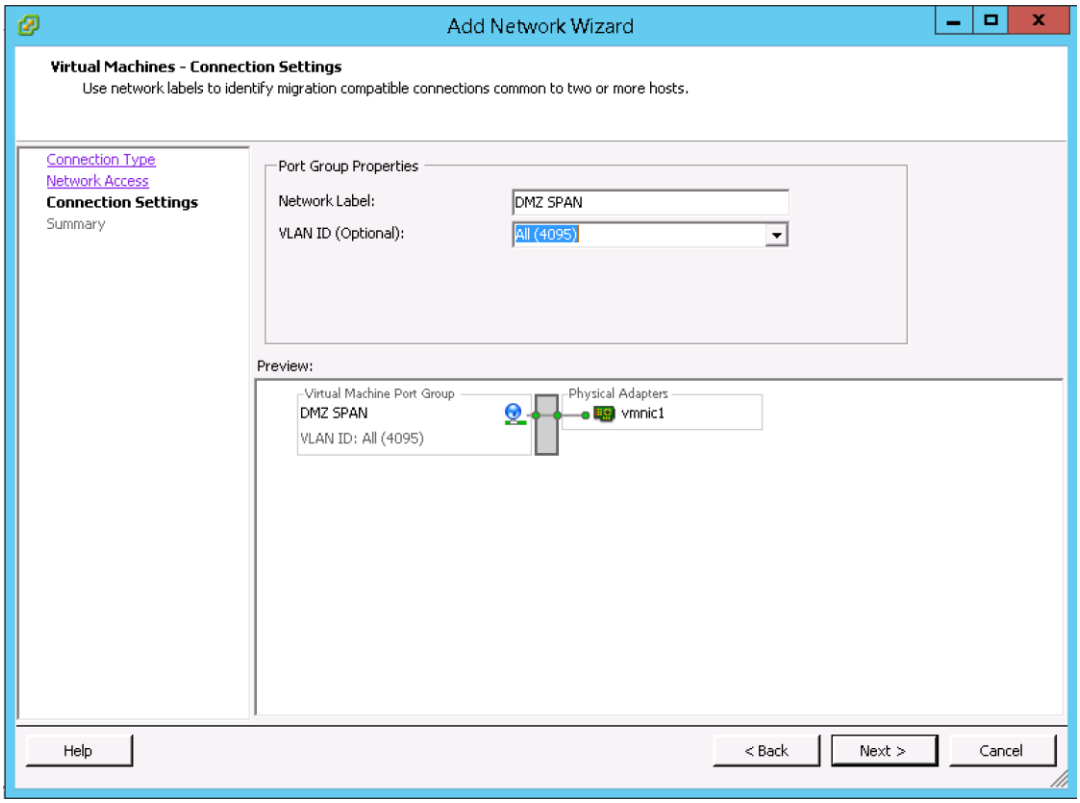


Figure 1-4: Port Group Properties

Review the summary screen to ensure the entries are correct, then click "*Finish*."

One final step in configuring the virtual switch is to ensure the vmnic is in promiscuous mode. In the "Standard Switch" dialog click on "Properties" as shown in *Figure 1-5.*

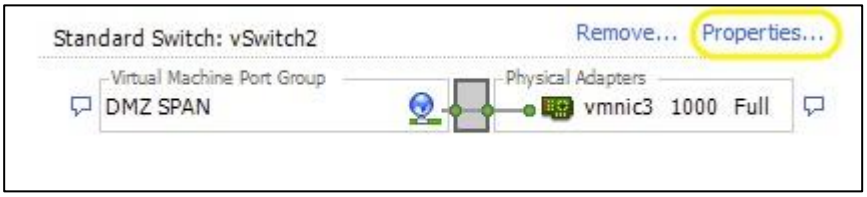
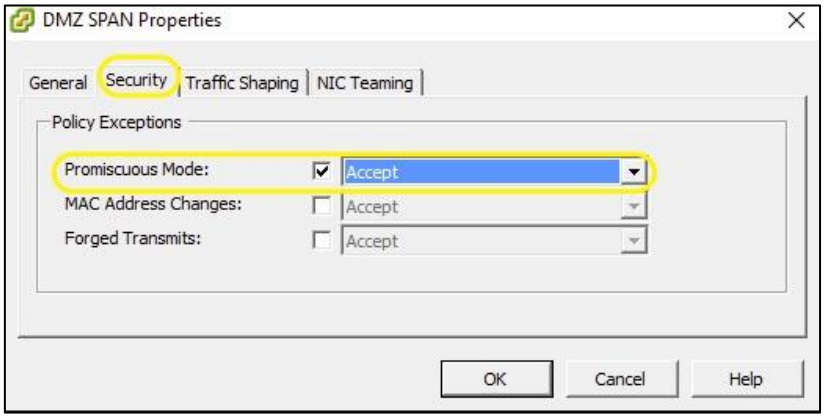


Figure 1-5: Standard Switch Properties

In the "*Properties"* dialog window click on the "Security" tab and make sure the "Promiscuous Mode" box is checked as shown in *Figure 1-6.*



2. *Download the MixMode OVA file and import it into a virtual machine.*

2.1 Download the MixMode OVA file.

Follow the BOX link provided by RAVENii to download the OVA.

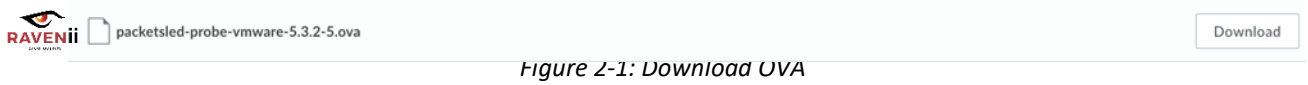
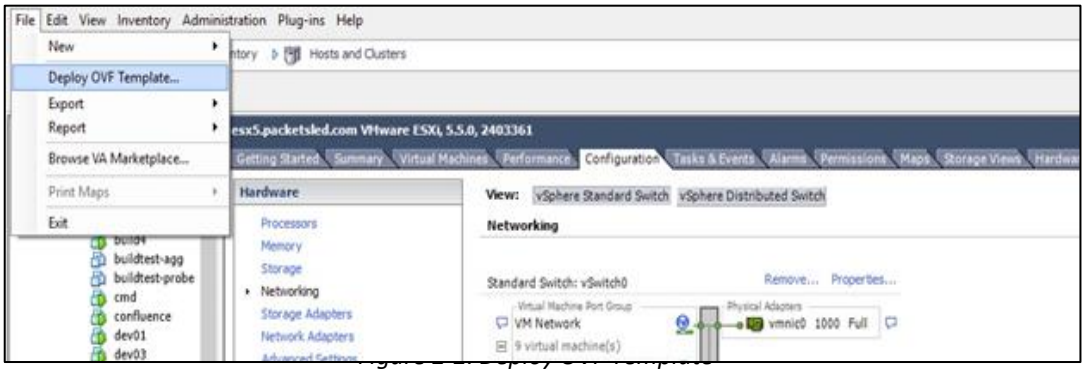


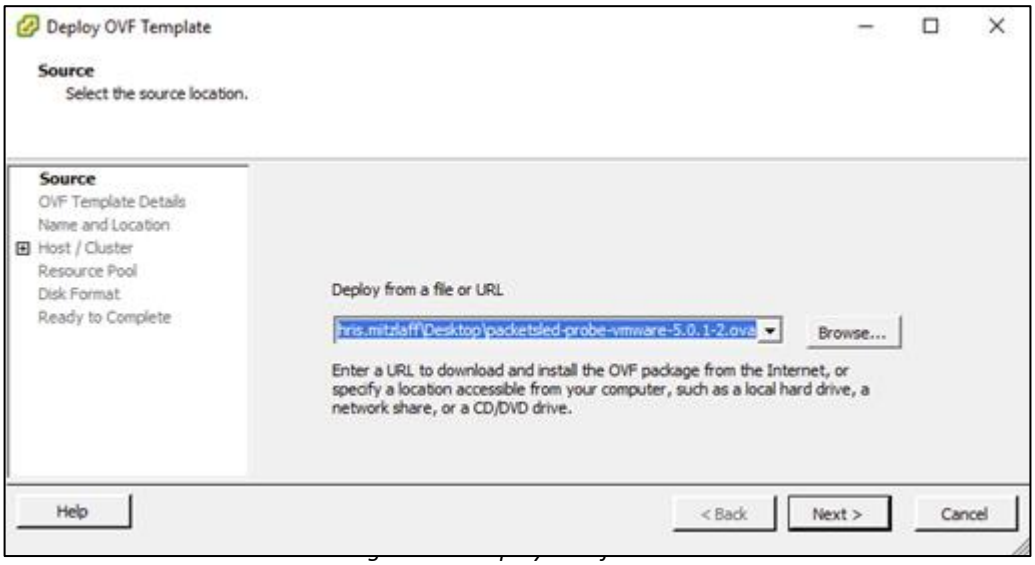
Figure 2-1: Download OVA

2.2 Import the MixMode OVA file into a VM.

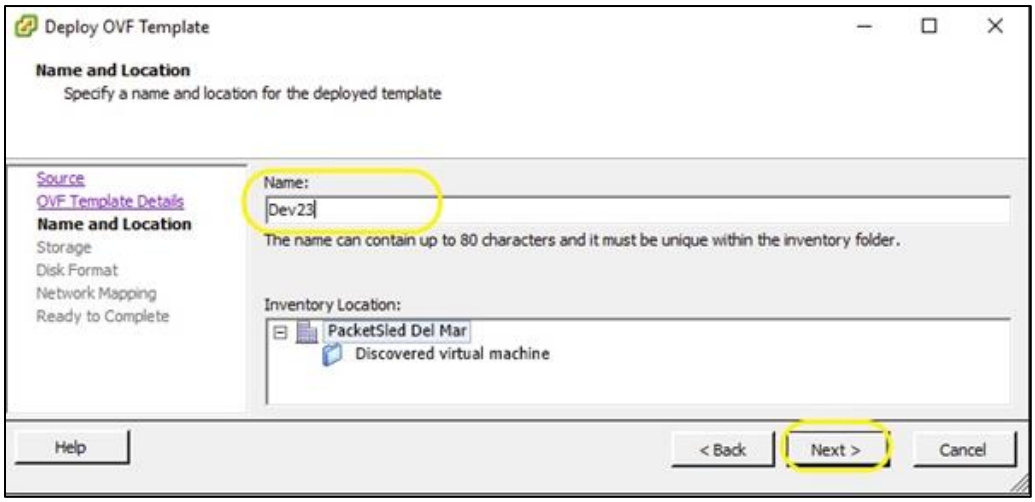
Next, import the OVA into your ESXi environment. On your ESXi server, click on "*File | Deploy OVF Template*" as shown in *Figure 2-4*.



In the next screen, click on the "*Browse*" button and traverse to where you saved the OVA file, select it, and then click "Next". This is shown if *Figure 2-5* below.

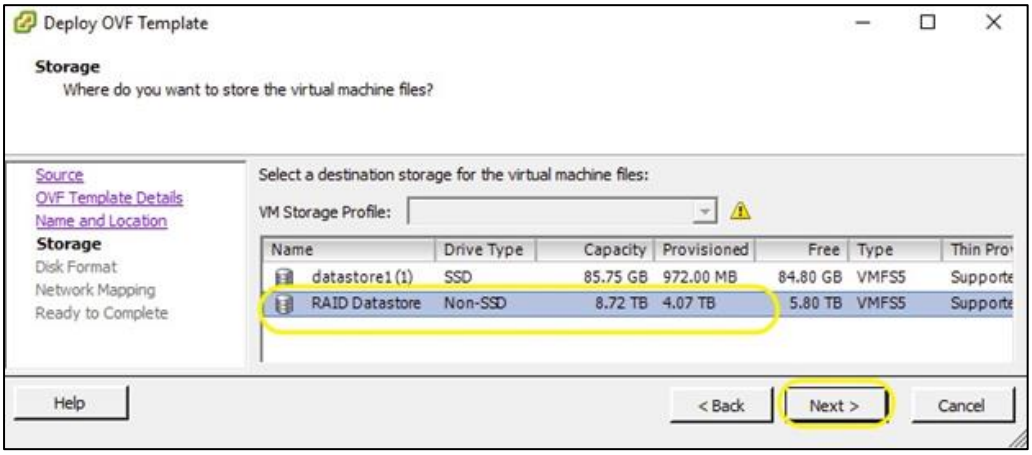


In the next window, give your VM sensor a name and then click "*Next*." *Figure 2-6*.



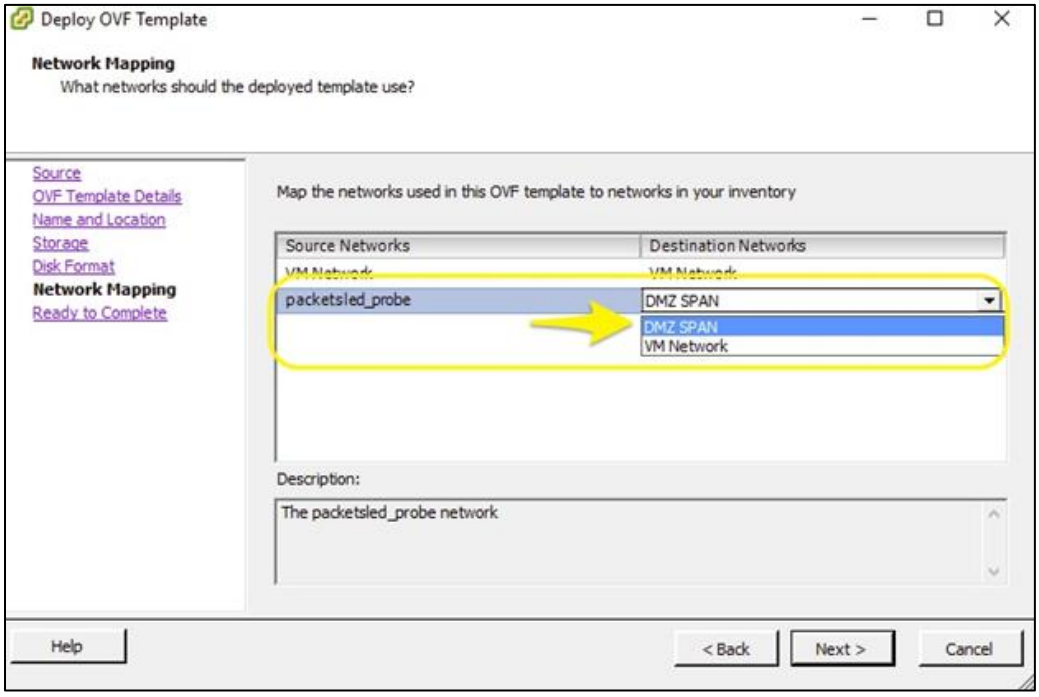
2.3 Select a datastore for your VM.

Now you need to select what datastore to use. As shown in *Figure 2-7,* we chose a very large data storage location. Once you have selected your datastore, click "*Next*."



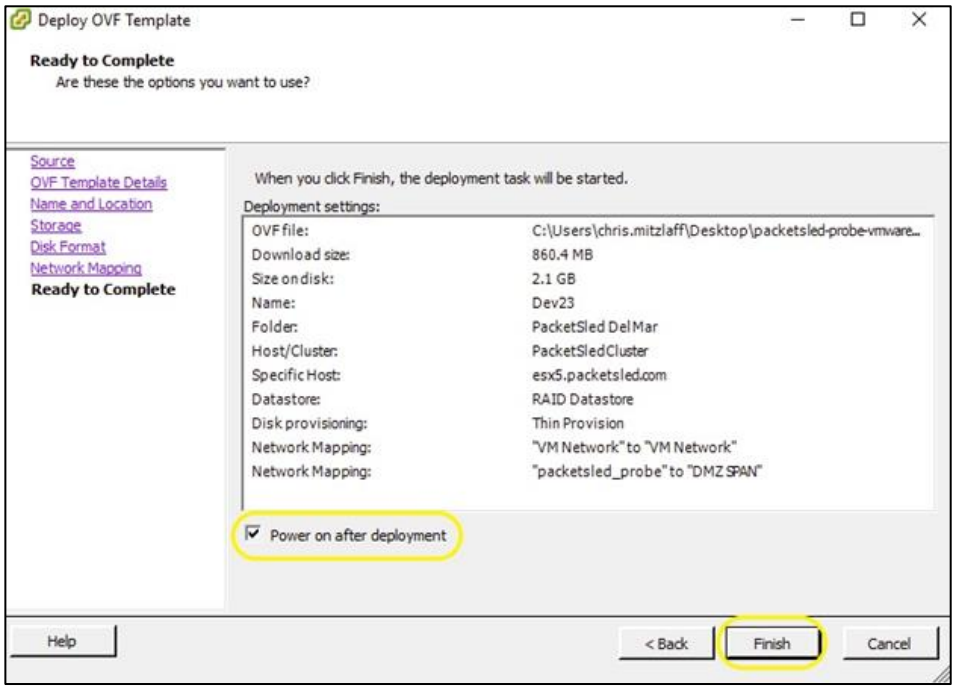
2.4 Select a destination network for your VM.

Next, select the network your sensor will use. As shown below in *Figure 2-8*, we selected the "DMZ SPAN" virtual switch network we created in *Section-2-1*. Select the destination network and click "*Next*."



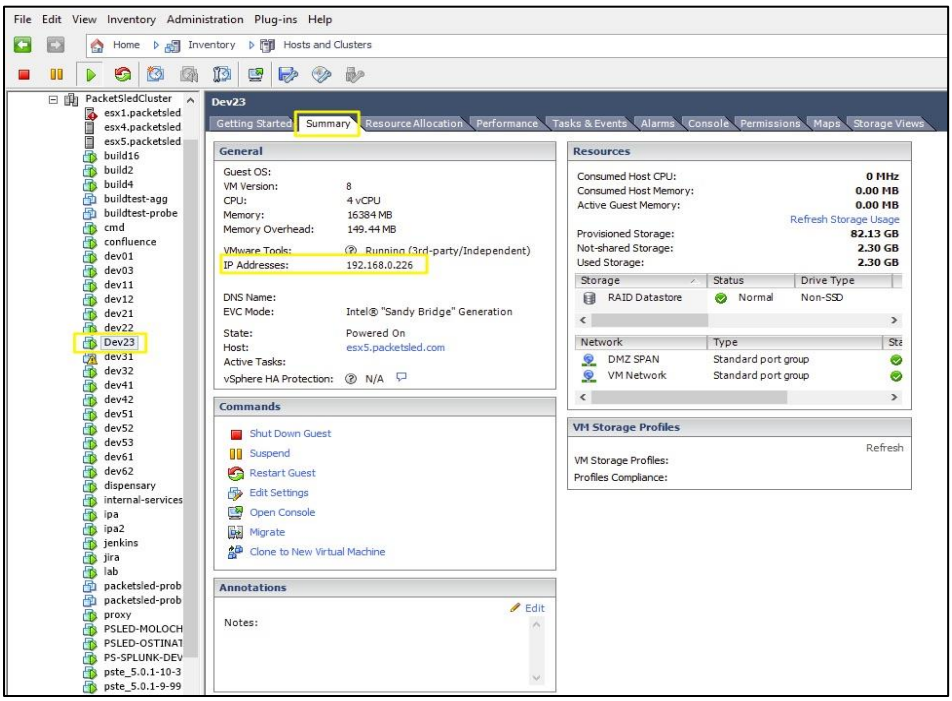
2.5 Deploy for your VM.

You will now be presented with a summary page (*Figure 2-9*). Review the information to make sure all your settings are correct. Click the “Power on after deployment” checkbox if you want to immediately power up your sensor VM.



2.6 Determine your VM’s IP address.

When your new VM is powered on, select it by name in the *Inventory* tree to determine the IP address of your sensor. In our case, it is 192.168.0.226 (*Figure 2-10*).



3. Configure the Network Settings

Open the Console for the VM and login with the root account. The username is root and the initial password is 'ch4ng3m3' (without quotes). You'll be required to change the password. Pick a strong password that you'll be willing to share with the RAVENii team.

Once logged in, edit the configuration file for eth0. Use the vi editor to make the changes:
[root@localhost ~]# vi /etc/sysconfig/network-scripts/ifcfg-eth0

Press the "i" key to enable to insert or edit mode. Using the arrow keys, move the cursor to the end of the line that starts with BOOTPROTO and erase dhcp and replace it with the word static. Be sure to leave the "s around the word static.

Add additional lines for IPADDR, NETMASK, GATEWAY, DNS1 and DNS2 (if applicable). Set the values to match your network. See figure 3-1 for an example of the final config file.

```
TYPE="Ethernet"
BOOTPROTO="static"
IPV6INIT="no"
NM_CONTROLLED="no"
NAME="eth0"
DEVICE="eth0"
ONBOOT="yes"
IPADDR=10.8.10.250
NETMASK=255.255.252.0
GATEWAY=10.8.11.254
DNS1=10.8.10.12
DNS2=10.8.10.13
```

Figure 3-1: eth0 Static IP

Once complete, save and exit the editor.
This is accomplished by pressing the following key sequence:
[esc][:][wq][Enter] (Escape key, colon key, w key q key, enter/return key)

Restart networking:
[root@localhost ~]# systemctl restart network

Validate new interface configuration:
[root@localhost ~]# ip a s eth0
The output should look similar to figure 3-2 below:

```
[root@localhost ~]# ip a s eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:80:5f:7c brd ff:ff:ff:ff:ff:ff
    inet 10.8.10.250/22 brd 10.8.11.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe80:5f7c/64 scope link
       valid_lft forever preferred_lft forever
```

Figure 3-2: eth0 IP Address/Mask

Validate Default Route:
[root@localhost ~]# ip r

The output should look similar to figure 3-3 below:

```
[root@localhost ~]# ip r
default via 10.8.11.254 dev eth0
10.8.8.0/22 dev eth0 proto kernel scope link src 10.8.10.250
169.254.0.0/16 dev eth0 scope link metric 1002
169.254.0.0/16 dev eth1 scope link metric 1003
```

Figure 3-2: Routing Table

Validate DNS settings:

[root@localhost ~]# cat /etc/resolv.conf

The output should look similar to figure 3-3 below:

```
[root@localhost ~]# cat /etc/resolv.conf
nameserver 10.8.10.12
nameserver 10.8.10.13
```

Figure 3-3: DNS Settings

Verify the internet connectivity:
[root@localhost ~]# ping -c 4 www.google.com

The output should look similar to figure 3-4 below:

```
PING www.google.com (172.217.4.100) 56(84) bytes of data.
64 bytes from ord36s04-in-f4.1e100.net (172.217.4.100): icmp_seq=1 ttl=52 time=22.9 ms
64 bytes from ord36s04-in-f4.1e100.net (172.217.4.100): icmp_seq=2 ttl=52 time=22.9 ms
64 bytes from ord36s04-in-f4.1e100.net (172.217.4.100): icmp_seq=3 ttl=52 time=22.8 ms
64 bytes from ord36s04-in-f4.1e100.net (172.217.4.100): icmp_seq=4 ttl=52 time=22.9 ms

--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 22.880/22.924/22.969/0.032 ms
```

Figure 3-4: Successful Ping

4. Configure storage locations for file and packet captures.

It is important that you allocate enough disk space on the sensor to store extracted files and full packet captures (pcaps). The more disk space allocated for these artifacts, the longer, time wise, they will be available. The system will use 75% of the allocated disk space to store this data.

3.1 The default disk layout for a MixMode virtual sensor is shown below:

```
Disk /dev/sda: 53.7 GB, 53687091200 bytes, 104857600 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000a8e00
   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048     1026047      512000   83  Linux
/dev/sda2         1026048     9414655     4194304   82  Linux swap / Solaris
/dev/sda3         9414656   104857599    47721472   8e  Linux LVM

Disk /dev/sdb: 107.4 GB, 107374182400 bytes, 209715200 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: gpt
Disk identifier: EE8FF0DE-0284-43A9-963F-9937B3215B69
#         Start          End    Size  Type            Name
 1         2048    209713151    100G  Microsoft basic primary

Disk /dev/sdc: 107.4 GB, 107374182400 bytes, 209715200 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: gpt
Disk identifier: EDA2FBCA-0303-4B3C-AD49-458BDC4381EE
#         Start          End    Size  Type            Name
 1         2048    209713151    100G  Microsoft basic primary
```

Figure 4-1: Default Disk Layout

Notice in Figure 3-1 there are two 100GB disk partitions, */dev/sdb* and */dev/sdc* (Highlighted in yellow). These partitions are mounted on the */data* mount point. One partition is mounted at */data/export*, and the other is mounted at */data/stenographer*. This is shown below in Figure 3-2.

```
/dev/mapper/rootvg01-lv01 on / type xfs (rw,relatime,attr2,inode64,noquota)
/dev/sda1 on /boot type xfs (rw,relatime,attr2,inode64,noquota)
/dev/sdb1 on /data/export type xfs (rw,relatime,attr2,inode64,noquota)
/dev/sdc1 on /data/stenographer type xfs (rw,relatime,attr2,inode64,noquota)
```

Figure 4-2: Mounted Partitions

NOTE: ***The default export and stenographer partitions are probably too small for your use. It is highly recommended that you reconfigure these partitions to be much larger. At a minimum, we recommend these partitions be at least 1TB in size, preferably 2-5TB depending on the bandwidth of the sensor.***

NOTE: ***Your sensor MUST have a /data mount point and the two partitions MUST be mounted on /data/export and /data/stenographer, or your sensor will not operate correctly.***

Summary

This document provides detailed instructions on how to deploy a MixMode sensor. It covers the deployment of a sensor in a virtualized environment, as well as on bare metal hardware.

If you have any problems deploying your sensor, please contact onboarding@ravenii.com.