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



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 <u>https://portal.netwatcher.com/login</u> with your email address and reset your password.

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

- Once you log in to your account, navigate to <u>https://portal.netwatcher.com/sensor/sensors</u>, click on your sensor, and press download. It will take a while to download as it's a large file. We use <u>http://www.7-zip.org</u> 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**



#### Identify Source port for SPAN

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

#### **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

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



#### 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





## 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

| Add Network Wizard  |  |   |        | 🕢 Add Network Wizard  |  |                  |
|---|--|---|--------|---|--|------------------|
| Connection Type<br>Networking hardware can  | n be partitioned to accommodate each service that requires connectivity.   |   |        | Virtual Machines - N<br>Virtual machines                            | letwork Access<br>reach networks through uplink adapters attached to vSphere standard switches.  |                  |
| Connection Type<br>Network Access<br>Connection Settings<br>Summary   | Connection Types<br><b>Virtual Machine</b><br>Add a labeled network to handle virtual machine network traffic.<br><b>VMkernel</b><br>The VMkernel TCP/IP stack handles traffic for the following ESXI service<br>management.   | is: vSphere vMotion, ISCSI, NFS, and host |        | Connection Type<br>Network Access<br>Connection Settings<br>Summary | Select which VSphere standard switch will handle the network traffic for this connection. You may also create a new vSphere standard switch using the unclaimed network adapters listed below.            • Create a vSphere standard switch       Speed       Networks            • Emulax Corporation OneConnect 10Gb HIC (be3)         • I0000 Full         • I0.20.0.1-10.20.3.254 (VLAN 81         Intel Corporation 1350 Gigabit Network Connection         • I0000 Full         • I122.168.0.192-192.168.0.223 (VLAN 300         I000 Full         • I122.168.0.192-192.168.0.223 (VLAN 300         Preview:             Virtual Machine Port Group         Virtual Machine Port Gro |                  |
|   |  |   |        | Unselect<br>desired   | t in use physical ports (vmnic3 above) and dedicated/unused physical port (vmnic1 a  | select<br>bove). |
| 1   |  |   |        |   |  |                  |
| Help  |  | ≤ Back Next ≥                             | Cancel | <u>H</u> elp  | <u></u>  | Next ≥ Cancel    |
| Help  |  | ≤ Back Next ≥                             | Cancel | Help  | <u></u>  | Next ≥ Cancel    |
| Add Network Wizard<br>Virtual Machines - Connecti<br>Use network labels to ider   | ion Settings<br>ntfy migration compatible connections common to two or more hosts.   | ≤ Back Next ≥                             | Cancel | Help Add Network Wizard Ready to Complete Verfy that all ne         | ≤ Back   | Next 2 Cancel    |
| Heip Add Network Wizard Virtual Machines - Connectio Use network abels to ider Connection Type Network Access Connection Settings UNIN Preview VLAN Preview VI SP | ion Settings         entfy migration compatible connections common to two or more hosts.         : Group Properties         vork (Labei:         SPAN Target         N ID (Optional):         icone (0)         v:         vt:         vt: | <u>≤ Back</u> Next ≥                      | Cancel | Hep   |  | Next 2 Cancel    |
| Help Add Network Wizard Virtual Machines - Connecti Use network labels to ide Connection Tupe Connection Settings Connection Settings Summary Preview Summary     | ton Settings<br>entfy migration compatible connections common to two or more hosts.<br>Coroup Properties<br>work table:<br>I (Optional):<br>V:<br>Withal Machine Port Group<br>PAN Target:<br>PAN Target:<br>Change Network Label to<br>and VLAN ID to None (0)  | SPAN Target"                              | Cancel | Hep   | ≤ Back w and modified vSphere standard switches are configured appropriately.  Host networking will include the following new and modified standard switches:  Prevenue:  VIAW ID: All (4095)  Clicck Finish   | Next 2 Cancel    |



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

| jie jut Veg Ipentory Administration                                      | Ngo mi (bit)<br>Il nota and Cutim and   | e Seach Investory                           | Ports Network Adapters  |  |  |            |
|--|---|---|---|--|--|------------|
|  | transformed Vitrement CSE, SUA, BROZHA     result (Sound & Vitrement CSE, SUA, BROZHA     result)     result (Sound & Vitrement CSE, Sound & Vitrement CSE, Result, - R |   | Generation         Summary  | vSphere Standard Switch Pro<br>Number of Ports:<br>Advanced Properties<br>MTU:<br>Default Policies<br>Security<br>Promiscuous Mode:<br>MAC Address Changes:<br>Forged Transmits:<br>Traffic Shaping<br>Average Bandwidth:<br>Peak Bandwidth:<br>Burst Size:<br>Failover and Load | Perties<br>120<br>1500<br>Reject<br>Accept<br>Accept<br><br> |            |
| r in Alassening<br>Boost talk<br>Nove Tapp                               |   | Them. Toget of bina softeen + ( ( ) are _ X | Select Edit   | Balancing<br>Load Balancing:<br>Network Falure Detection:<br>Notfly Switches:<br>Faiback:<br>Active Adapters:<br>Standby Adapters:<br>Unused Adapters:   | Port ID<br>Link status only<br>Yes<br>vmnic1<br>None<br>None | Close Help |
| Tasis 🕈 Aana   | erties  | Conter                                      | vSwitch0 Properties   |  |  |            |
| General Securit<br>Policy Except<br>Promiscuo<br>MAC Addre<br>Forged Tra | y   Traffic Shabing   NIC Teaming  <br>ions<br>us Mode: Reject  |   | General Security   Traffic Shabind   NIC Tea<br>Policy Exceptions<br>Promiscuous Mode:<br>MAC Address Changes:<br>Forged Transmits: | mina  <br>Accept<br>Accept<br>Accept   | 2  |            |
|  |   |   |   |  |  |            |
| S  | elect Security Tab  |   | Enable Promiscuou   | s Mode   |  |            |



#### Step 2: Import NetWatcher Sensor VM



NW





### Step 2-a: Import NetWatcher Sensor VM

| Desting with a bloches   Sex dystem   Sex dyst   | Conversion   |  |   |  | Tel Conversion   |  |  |                                  |
|---|--|--|---|--|--|--|--|----------------------------------|
| Sector States       Sector States<  | Destination Virtual N<br>Select the destination  | Machine<br>n VM name and folder  |   |  | Destination Location<br>Select the location for  | r the new virtual machine  |  |                                  |
| Click Next and Select Destination directory on vectors server       Select Destination physical server and data store            eb port degrest by::::::::::::::::::::::::::::::::::::   | Source System<br>Destination System<br>Destination Virtual M<br>Destination Location<br>Options<br>Summary                           | Source: D 1:\NetWatc\NetWatcher - C<br>Name: NetWatcher - OVF<br>Inventory for: vcenter.svr.oe.l Sear<br>Ovcenter.svr.oe.l<br>Inventory for: vcenter.svr.oe.l<br>Defensative [1 VMs]<br>Defensative [1 VMs]  | VF.vmx (Other (32-bit)) Destina<br>ch for name with:<br>VM name P<br>Windows 7 Ent Adam R | Clear<br>Clear<br>Power state<br>Running | Source System<br>Destination System<br>Destination Virtual Mach<br>Destination Location<br>Options<br>Summary  | Source: D I:\NetWatc\NetWatcher - (<br>Inventory for: vcenter.svr.oe.l<br>C E Local<br>M DE Local<br>Vm1.svr.oe.l<br>Vm1.svr.oe.l<br>Vm3.svr.oe.l<br>Vm4.svr.oe.l  | DVF.vmx (Other (32-bit)) Destination:<br>Total source disks size: 500 GB<br>Datastore<br>USE ME - zStax-NFS<br>Capacity: 14,381.59 GB<br>Free: 2,442.24 GB<br>Type: NFS<br>Virtual machine version<br>Version 10 •   | <ul> <li>Net</li> <li></li></ul> |
| Conversion       Conversion       Conversion         Options       Set up the parameters for the conversion task       Review the conversion parameters       Click Finish         Source System       Options       Click on an gpton below to edit t.       Source System         Destination Vitual Mach<br>Destination Vitual Mach<br>Destination Vitual Mach<br>Options       Source System       Source System       Source System         Options       Conversion       Conversion       Source System       Source System         Destination Vitual Mach<br>Destination Vitual Mach<br>Options       Source System       Source System       Source System         Options       Conversion       Conversion       Conversion       None         Vitual Dok: 1 Coreshow       Edit       Source System       Destination System       Destination System         Destination Vitual Mach<br>Destination Vitual Mach<br>Destination Vitual Mach       Source System       Destination System       Destination System         Vitual Dok: 1 Coreshow       Edit       Vitual Mach       Source System       Vitual Mach       Destination System         Vitual Mach       Source: Sin Na<br>Mice SPAN       Edit       None       Vitual Mach       Vitual Mach         Vitual Mach       Source: Sin Na<br>Mice SPAN       Edit       None       Vitual machine name:<br>None       Vitual machine name:   | Click Next   | t and Select Destinat<br>erver   | tion directory or   | n  | Select Des   | stination physical se  | rver and data store  | 2                                |
| Set up the parameters for the conversion task       Review the conversion parameters       CICK FINISh         Source System<br>Destination System<br>Destination Vitual Mach<br>Destination Locator<br>Options<br>Summary       Source System<br>Destination System<br>Destination System<br>Destination Locator<br>Options       Source System<br>Destination System<br>Destination Locator<br>Options       Source System<br>Destination System<br>Destination Locator<br>Options       Source System<br>Destination System<br>Destination Locator<br>Options       Source System<br>Destination System<br>Destination System<br>Destination Locator<br>Options       Source System<br>Destination System<br>Note:<br>Source System Information<br>Destination System<br>Note:<br>Source System Information<br>Destination System<br>Destination System<br>Note:<br>Source System Information<br>Source System Information<br>Vitual Mach Ine Amer:<br>Network Information<br>Destination System Information<br>Source System Information<br>Vitual Mach Ine Amer:<br>Network Information<br>Default<br>Destination System<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default<br>Default |  | osuc ogs   | < Back Next >   | Cancel                                   | Help Export diagno   | ostic logs   | <u>Next</u>  | Cancel                           |
| Confirm settings  | Conversion   | usic ugs   | < Back Next >   |  | Export diagno  | sstic logs   |  | Cancel                           |
|   | Conversion Options Set up the paramet Source System Destination System Destination Virtual Mach Destination Location Options Summary | ers for the conversion task Source:      I:\NetWatcher\NetWatcher Click on an gption below to edit it. Current settings:     Vata to copy Copy type: Dsk-based VrtuaDskl: 500 GB     Devices     vCPUs: 4 (4 sockets * 1 cores)     Disk controller: Preserve source     Memory: 4GB     Networks     NIC1: SPAN Target     NIC2: SPAN Target     NIC3: SPAN Target     NIC3: SPAN Target     NIC4: SPAN Target     NIC5: SPAN | r - OVF.vmx (Other (32-bit)) Des  | Edt<br>Edt<br>Edt<br>Edt<br>Edt          | Export diagno     Export diagno     Conversion     Summary     Review the conversion     Source System     Destination System     Destination Location     Options     Summary | In parameters Click Finisk Source: D I:\\NetWatcher\\NetWatcher Source: D I:\\NetWatcher\\NetWatcher Source type: Path: CPU throttling: Destination system information Virtual machine name: Hardware version: Host/Server: Cluster: Host system: Resource pool Power on after conversion: Number of vcPUs: Physical memory: Network: NIC1 | r - OVF.vmx (Other (32-bt)) Destinatio<br>v/Mware Workstation or other<br>i:VetWatcher-12a276d1-2c9f-<br>None<br>None<br>NetWatcher - OVF<br>Version 10<br>vcenter.svr.oe.1<br>mckaya<br>Defensative<br>OE Local<br>vm2.svr.oe.1<br>Default<br>No<br>4 (4 sockets * 1 cores)<br>4GB<br>Preserve NIC count<br>Connected | Cancel                           |



#### Step 2-b: Import NetWatcher Sensor VM





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





#### **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...

| VetWatcher  |          | nv ge         | ite a friend<br>t one monti | 0                          | Steve Parke | rker   🔺   Logout 6 |              |
|---|----------|---------------|-----------------------------|----------------------------|-------------|---------------------|--------------|
| 🖓 Dashboard 🛛 🖸 Reports 🔒 A                             | larms    | 🗭 Support     | Configur                    | e 🕑 Adva                   | inced       | Q terms             | All Alarms + |
| Contacts Subscriptions My S                             | ensors   | Sensor Groups | Agents                      | Networ                     |             |                     |              |
| Ay Sensors  |          |               |                             |                            |             |                     |              |
| Album 10  | Name     | • •           | • Port                      | <ul> <li>Events</li> </ul> | • Alarma    | • Date              | • Groups     |
| <ul> <li>6007458+1353-4445-8327-9936857c496f</li> </ul> | madworth | insult.       |                             | 0                          | 0           | Dec-16-15           | 6            |
|   |          |               |                             |                            |             |                     |              |



# **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)

