NetWatcher® Managed Detection & Response Service Installation Guide

What is NetWatcher?

NetWatcher is a Security-as-a-Service platform that enables customers to have a cost-effective 24 x 7 security service monitoring their networks for vulnerabilities and exploits. Many government and industry compliance requirements, and security best practices, outline the need for continuous monitoring, intrusion detection, active scanning, log monitoring, net-flow analysis, event management and endpoint integration. NetWatcher enables customers to immediately deploy these services and take advantage of a fully-staffed Security Operations Center (SOC). This means superior security that is easy to use, accurate and affordable.

Contents

Connecting Hardware Sensor to NetWatcher Cloud 3
Setting up Network Intrusion Detection (NIDS) 4
Setting up SYSLOG Ingestion 4
Setting up Server / Desktop / Laptop LOGS 6
Setting Up Reoccurring Vulnerability Scans 8
Setup Reoccurring Reports 10
Setup Notifications 11
Connecting Virtual Sensor to NetWatcher Cloud – VSphere 12
Installing the Virtual Sensor on Other Virtual Machine Platforms 19

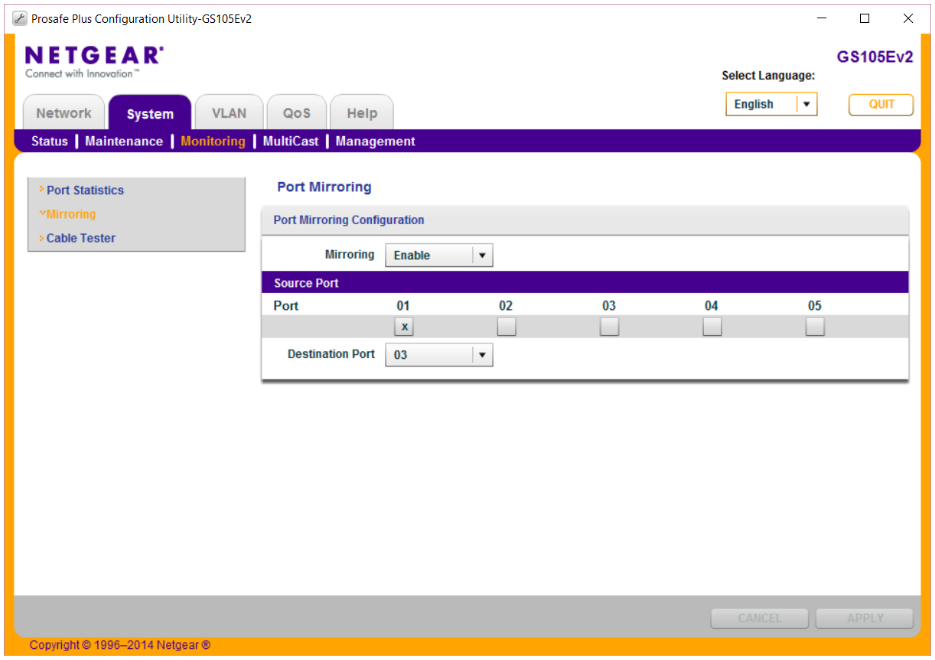
Connecting Hardware Sensor to NetWatcher Cloud

1. The NetWatcher team should have sent you an Activate email that will allow you to create your Customer Portal account. If you didn't get this send a note to info@netwatcher.com and someone will assist you.
2. Ensure you are not blocking any of the following ports OUTBOUND. These ports are what the sensor uses to communicate back to the NetWatcher cloud.
   - TCP 22 => portal.netwatcher.com
   - TCP 8443 => p.netwatcher.com
   - UDP 443 => vpn.netwatcher.com
   - TCP 443 => vpn-tcp.netwatcher.com
   - TCP 443 => index.docker.io
   - TCP 443 => registry-1.docker.io
   - TCP 443 => public.update.core-os.net
   - TCP 80 to google.com => Used to test internet/DNS connectivity
3. Connect one of the LAN ports on the sensors to the internet (doesn't matter which one) and let the sensor download its OS/Containers/Rulesets. This can take 20 min. The sensor light on the 'sensors' tab in the Customer Portal will go amber if the sensor sets itself up correctly.
4. If you need to setup a static IP address see this article.
5. Run Setup https://portal.netwatcher.com/setup

Setting up Network Intrusion Detection (NIDS)

6. Create a mirror of the port that the firewall is plugged into on the router/switch

   Here is an example of setting up a mirror on a NetGear managed switch:



Prosafe Plus Configuration Utility-GS105Ev2

NETGEAR® Connect with Innovation™ GS105Ev2

Select Language: English ▾ QUIT

Network | System | VLAN | QoS | Help

Status | Maintenance | Monitoring | MultiCast | Management

› Port Statistics
˅Mirroring
› Cable Tester

Port Mirroring

Port Mirroring Configuration

Mirroring: Enable ▾

Source Port

Port	01	02	03	04	05
	☒	□	□	□	□

Destination Port: 03 ▾

CANCEL APPLY

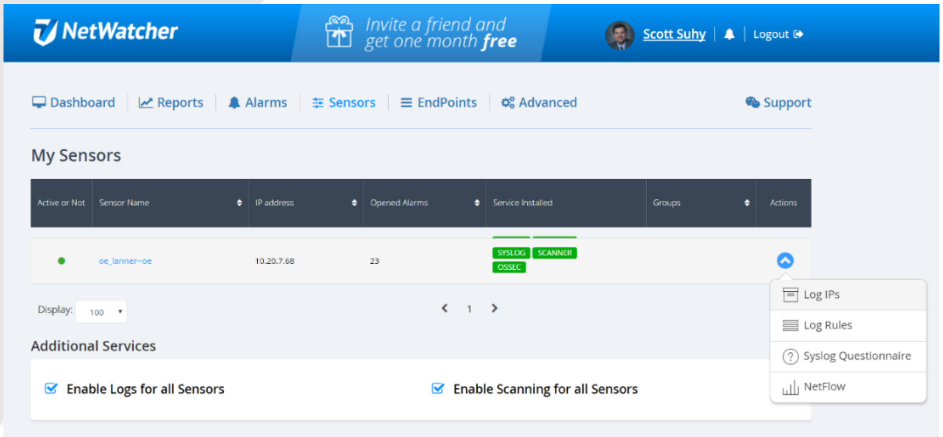
Copyright © 1996–2014 Netgear ®

7. Connect the other LAN port on the sensor to the newly created mirror port.
8. Verify the sensor light turns green on the sensors tab in the Customer Portal

If you are setting up the SIEM for log aggregation this is accomplished in 2 parts (setting up hardware SYSLOGs like firewalls and setting up servers and desktop logs)

Setting up SYSLOG Ingestion

9. Verify the device you want to monitor is on the supported device list found here.
10. In the Customer Portal go to the "Sensors" tab and select the sensor that you want to receive the logs and choose the Actions | Log IPs option.



NetWatcher | Invite a friend and get one month free | Scott Suhy | Logout

Dashboard | Reports | Alarms | Sensors | EndPoints | Advanced | Support

My Sensors

Active or Not	Sensor Name	IP address	Opened Alarms	Service Installed	Groups	Actions
●	oe_lanner--oe	10.20.7.68	23	SYSLOG SCANNER OSSEC		

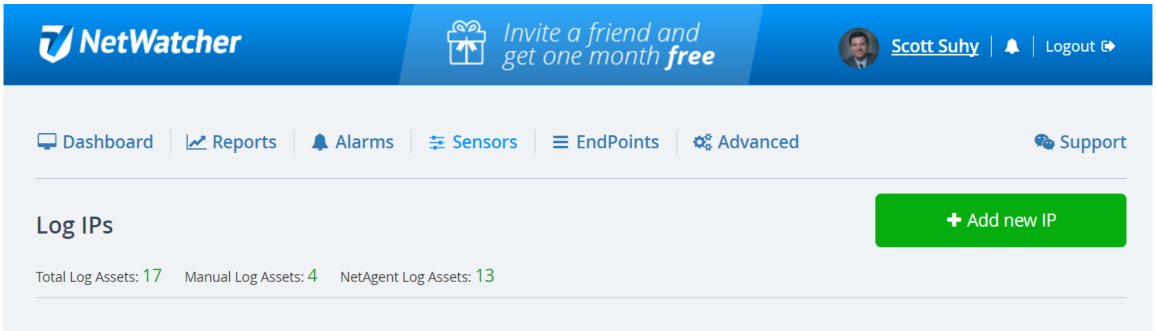
Display: 100 ▾ ‹ 1 ›

Actions menu: Log IPs, Log Rules, Syslog Questionnaire, NetFlow

Additional Services

☑ Enable Logs for all Sensors ☑ Enable Scanning for all Sensors

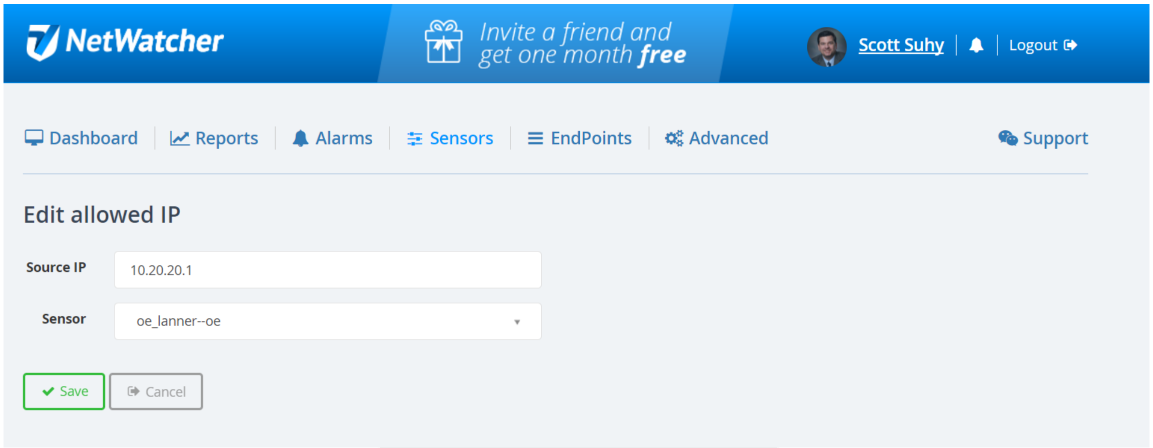
11. Choose “Add new IP”



Log IPs

Total Log Assets: 17 Manual Log Assets: 4 NetAgent Log Assets: 13

12. Add the IP of the Device

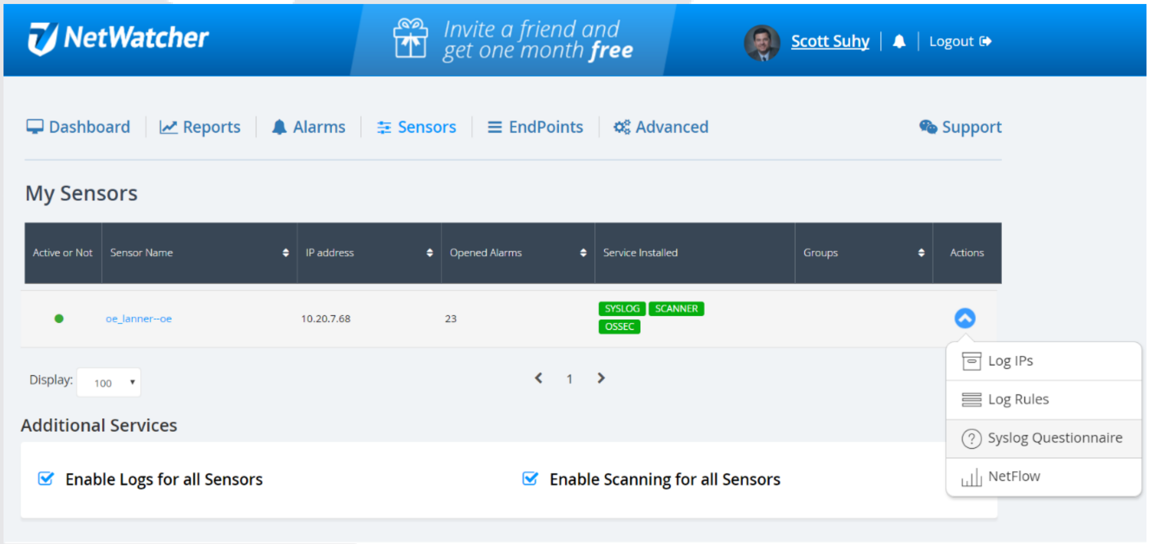


Edit allowed IP

Source IP: 10.20.20.1

Sensor: oe_lanner--oe

13. Go back to the main page under the ‘Sensors’ tab and select Action | Syslog Questionnaire



My Sensors

Active or Not	Sensor Name	IP address	Opened Alarms	Service Installed	Groups	Actions
●	oe_lanner--oe	10.20.7.68	23	SYSLOG SCANNER OSSEC		

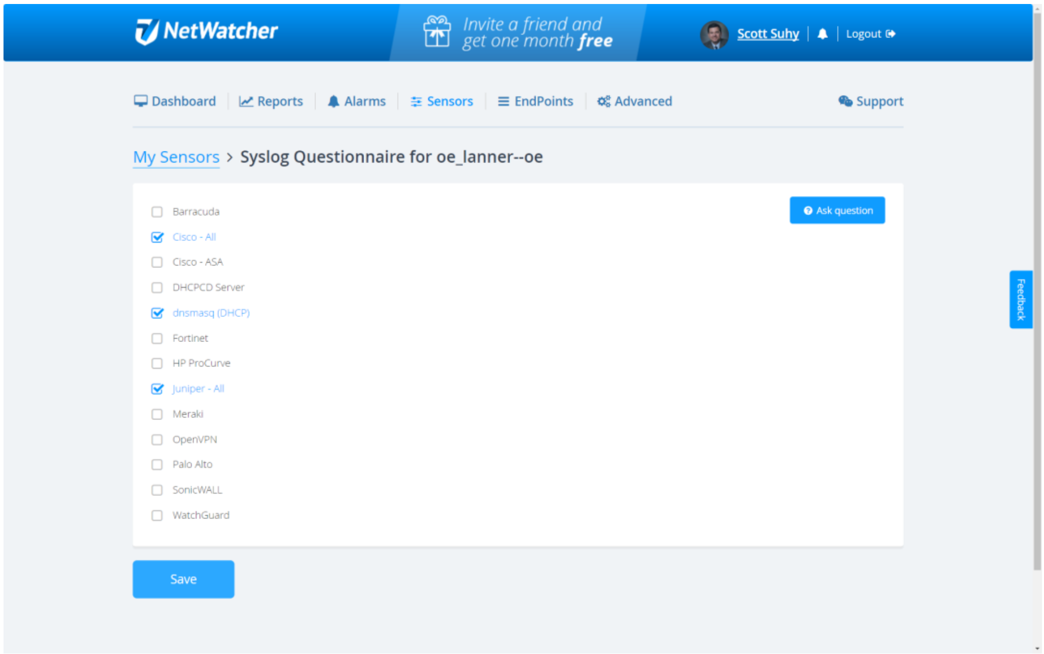
Display: 100

Additional Services

☑ Enable Logs for all Sensors

☑ Enable Scanning for all Sensors

14. Select the device type that is sending the SYSLOG. If it is not on the list, choose ‘Ask Question’ and specify the device and the DevOps team will enable the ruleset manually.

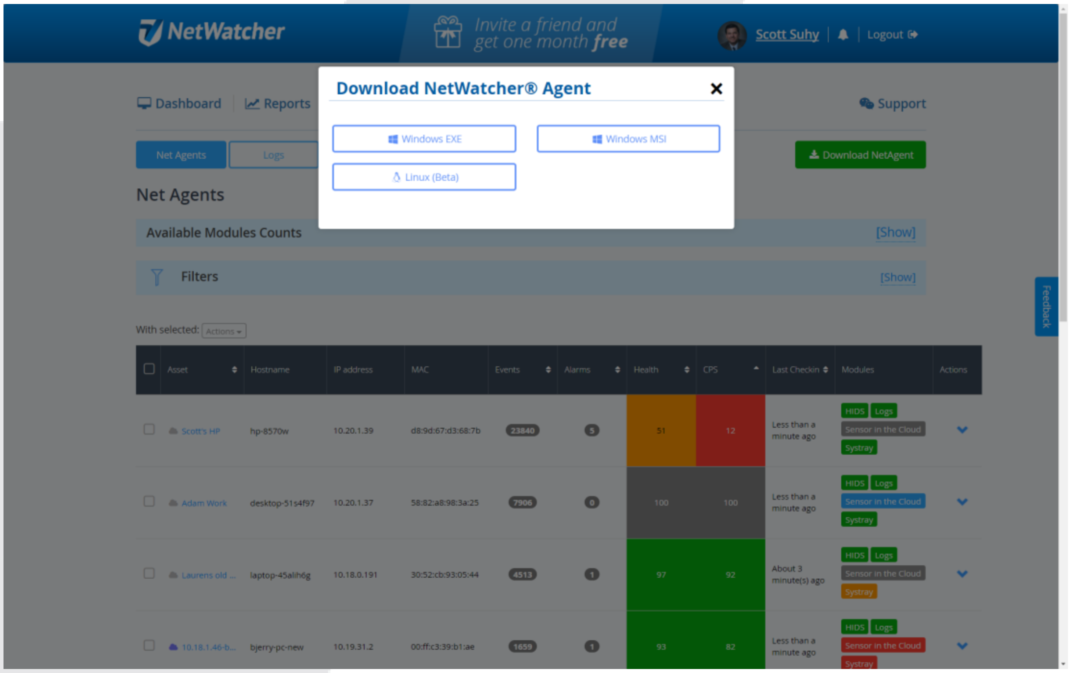

NetWatcher
Invite a friend and get one month free
Scott Suhy | Logout
Dashboard | Reports | Alarms | Sensors | EndPoints | Advanced
Support
Ask question
Feedback
Save

My Sensors > Syslog Questionnaire for oe_lanner--oe

- □ Barracuda
- ☑ Cisco - All
- □ Cisco - ASA
- □ DHCPCD Server
- ☑ dnsmasq (DHCP)
- □ Fortinet
- □ HP ProCurve
- ☑ Juniper - All
- □ Meraki
- □ OpenVPN
- □ Palo Alto
- □ SonicWALL
- □ WatchGuard

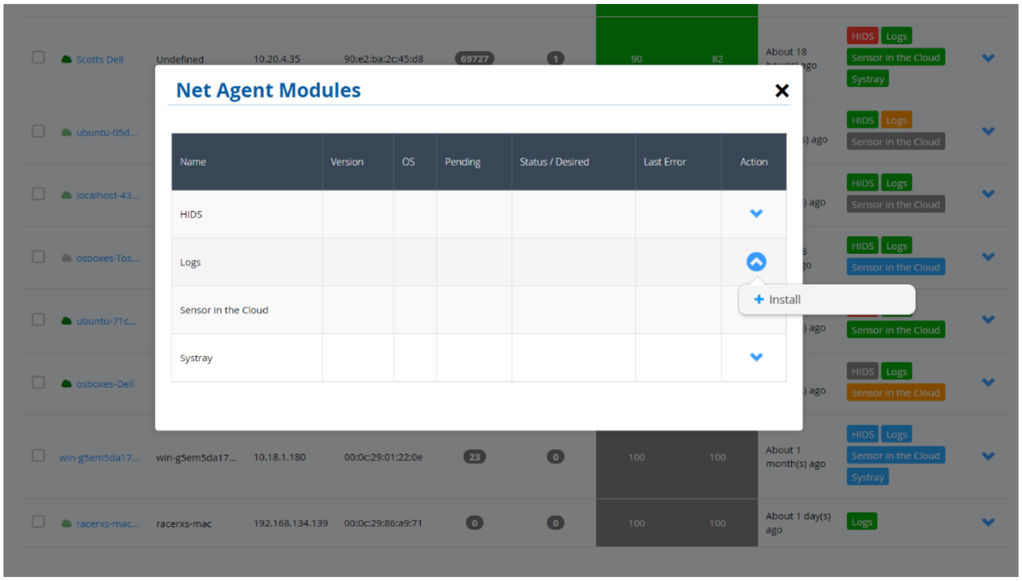
Setting up Server / Desktop / Laptop LOGS

15. Got to the ‘Endpoints’ tab and choose the green ‘Download NetAgents’ button. Remember that the NetAgent is free and can be run on any supported Windows or Ubuntu/Redhat Linux asset.



□	Asset	Hostname	IP address	MAC	Events	Alarms	Health	CPS	Last Checkin	Modules	Actions
□	Scott's HP	hp-8570w	10.20.1.39	d8:9d:67:d3:68:7b	23840	5	51	12	Less than a minute ago	HIDS Logs Sensor in the Cloud Systray	⌄
□	Adam Work	desktop-51s4f97	10.20.1.37	58:82:a8:98:3a:25	7906	0	100	100	Less than a minute ago	HIDS Logs Sensor in the Cloud Systray	⌄
□	Laurens old ...	laptop-45alih6g	10.18.0.191	30:52:cb:93:05:44	4513	1	97	92	About 3 minute(s) ago	HIDS Logs Sensor in the Cloud Systray	⌄
□	10.18.1.46-b...	bjerry-pc-new	10.19.31.2	00:ff:c3:39:b1:ae	1659	1	93	82	Less than a minute ago	HIDS Logs Sensor in the Cloud Systray	⌄

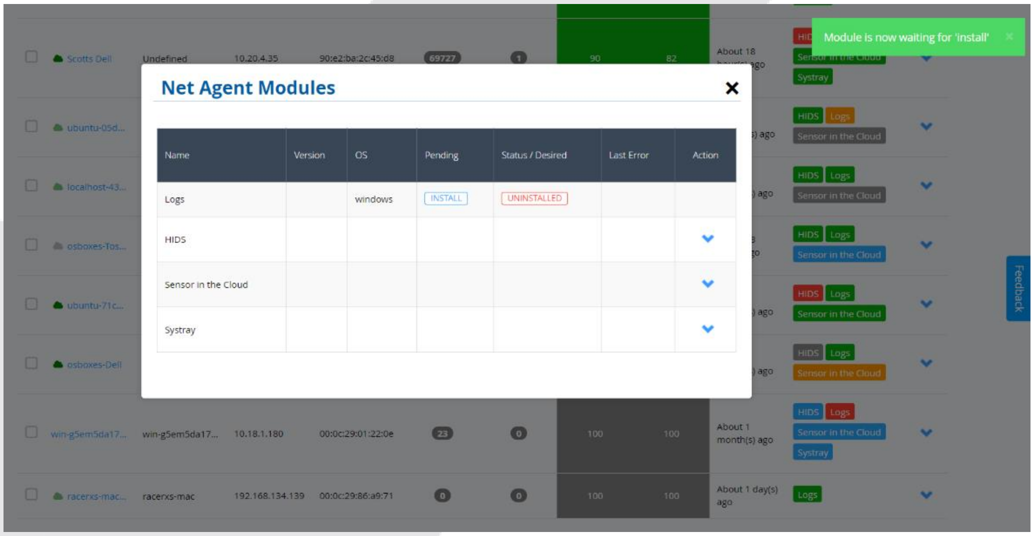
16. Once the NetAgent has been deployed the asset will show up on the list (may take a few minutes). Select 'LOGS' and the following dialog box will appear—choose Action 'Install' for LOGS. Repeat for HIDS if you want to install the Host Intrusion Detection Logs as well.



Net Agent Modules

Name	Version	OS	Pending	Status / Desired	Last Error	Action
HIDS						⌄
Logs						⌃
Sensor in the Cloud						
Systray						⌄

17. The Dialog box will reflect a Pending Install and in a minute or so the Logs will begin to send to the sensor. If the sensor is not live, the Logs will go directly to the cloud over a secure VPN until the sensor goes live again.



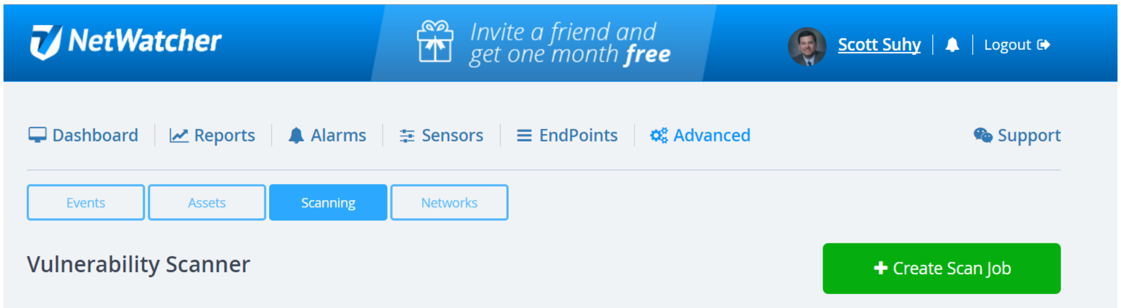
Module is now waiting for 'install'

Net Agent Modules

Name	Version	OS	Pending	Status / Desired	Last Error	Action
Logs		windows	INSTALL	UNINSTALLED		
HIDS						⌄
Sensor in the Cloud						⌄
Systray						⌄

Setting Up Reoccurring Vulnerability Scans

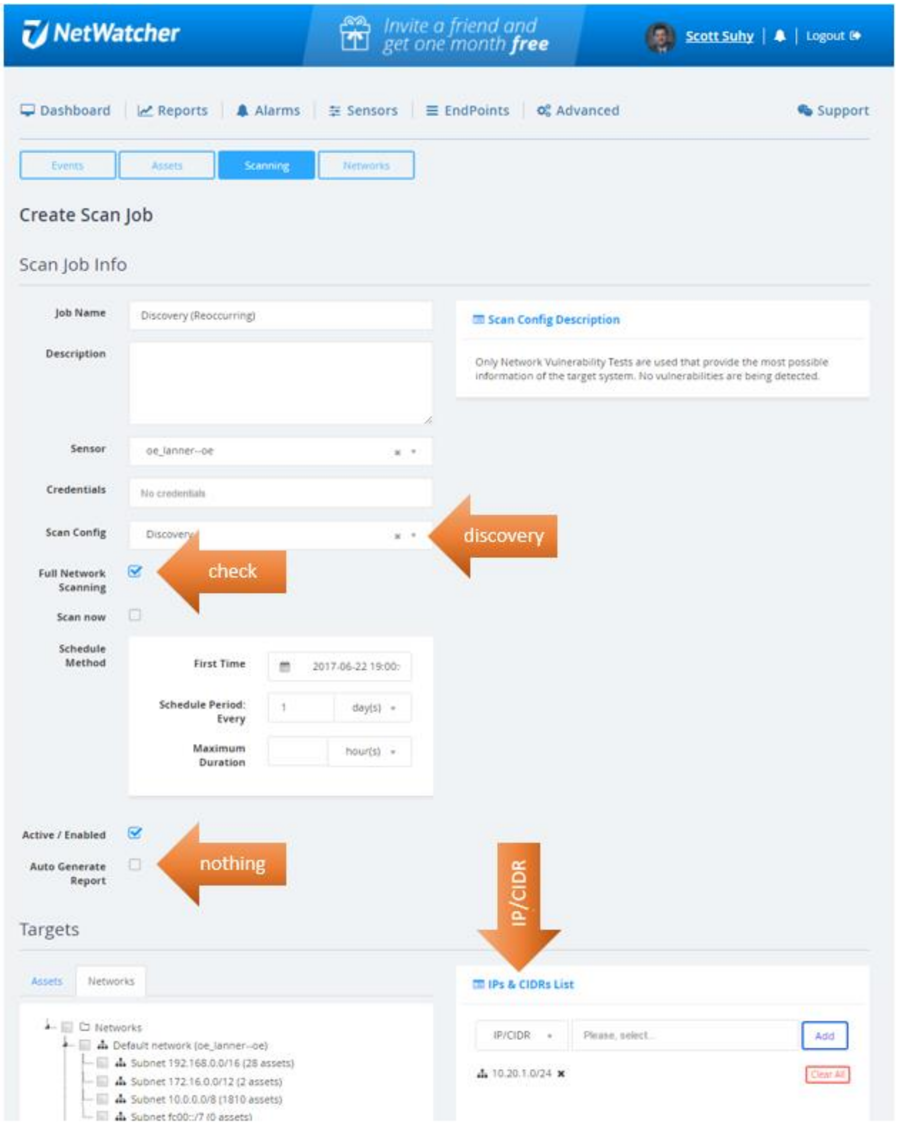
18. Got to the ‘Advanced’ tab (you need to have ‘Intermediate’ checked in your user profile to see the ‘Advanced’ tab) and choose the ‘Scanning’ button and then choose the ‘Create Scan Job’ button.



19. We want to setup 2 scans (Discovery daily and a Full and Fast on a Weekend)

Step 1: Setup the Discovery scan.

Note how the 'full network scanning' checkbox is checked. This ensures we see every IP in the range provided. Don't generate a report from the Discovery scan as it is not necessary.



Create Scan Job

Scan Job Info

Job Name: Discovery (Reoccurring)

Description:

Sensor: oe_lanner--oe

Credentials: No credentials

Scan Config: Discovery

Full Network Scanning ☑

Scan now ☐

Schedule Method: First Time 2017-06-22 19:00; Schedule Period: Every 1 day(s); Maximum Duration hour(s)

Active / Enabled ☑

Auto Generate Report ☐

Scan Config Description

Only Network Vulnerability Tests are used that provide the most possible information of the target system. No vulnerabilities are being detected.

discovery

check

nothing

IP/CIDR

Targets

Assets | Networks

- Networks
  - Default network (oe_lanner--oe)
    - Subnet 192.168.0.0/16 (28 assets)
    - Subnet 172.16.0.0/12 (2 assets)
    - Subnet 10.0.0.0/8 (1810 assets)
    - Subnet fc00::/7 (0 assets)

IPs & CIDRs List

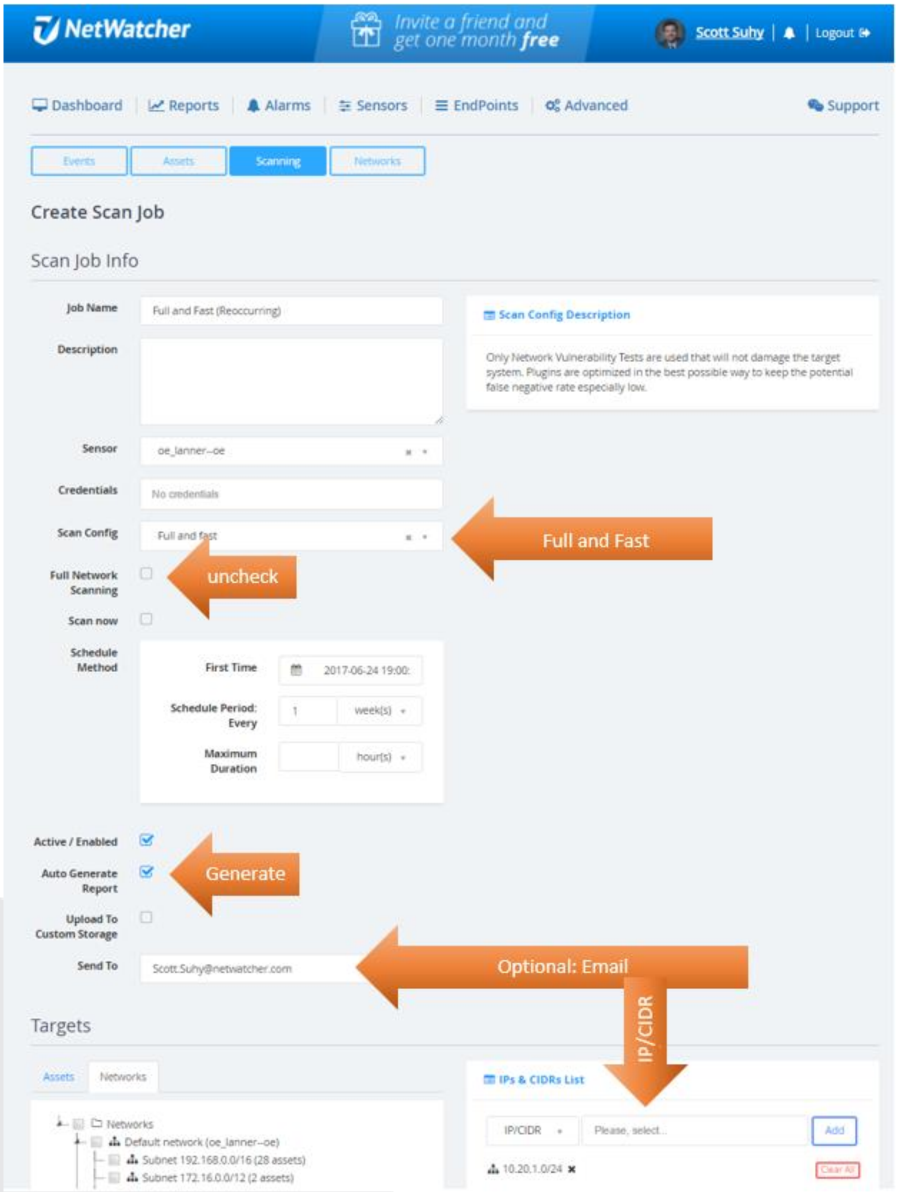
IP/CIDR | Please, select... | Add

10.20.1.0/24 ✖ | Clear All

Step 2: Create the Full and Fast Scan

For this scan, you will not need to check the 'Full Network Scanning' because the Discovery scan already found all the assets. This will greatly shorten the time the "Full and Fast" scan runs. You also might want to generate a report and have it sent to an email address. To add credentials, go to https://portal.netwatcher.com/account and choose the ‘credentials button’.

Note: Always schedule the "Discovery" scan at least 2 hours ahead of the "Full and Fast" scan so they don't overlap.



Create Scan Job

Scan Job Info

Job Name: Full and Fast (Reoccurring)

Description:

Sensor: oe_lanner--oe

Credentials: No credentials

Scan Config: Full and fast

Full Network Scanning: □

Scan now: □

Schedule Method:
First Time: 2017-06-24 19:00:
Schedule Period: Every: 1 week(s)
Maximum Duration: hour(s)

Active / Enabled: ☑

Auto Generate Report: ☑

Upload To Custom Storage: □

Send To: Scott.Suhy@netwatcher.com

Scan Config Description

Only Network Vulnerability Tests are used that will not damage the target system. Plugins are optimized in the best possible way to keep the potential false negative rate especially low.

Targets

Assets
Networks
Networks
Default network (oe_lanner--oe)
Subnet 192.168.0.0/16 (28 assets)
Subnet 172.16.0.0/12 (2 assets)
IPs & CIDRs List
IP/CIDR
Please, select...
Add
10.20.1.0/24
Clear All

Full and Fast

uncheck

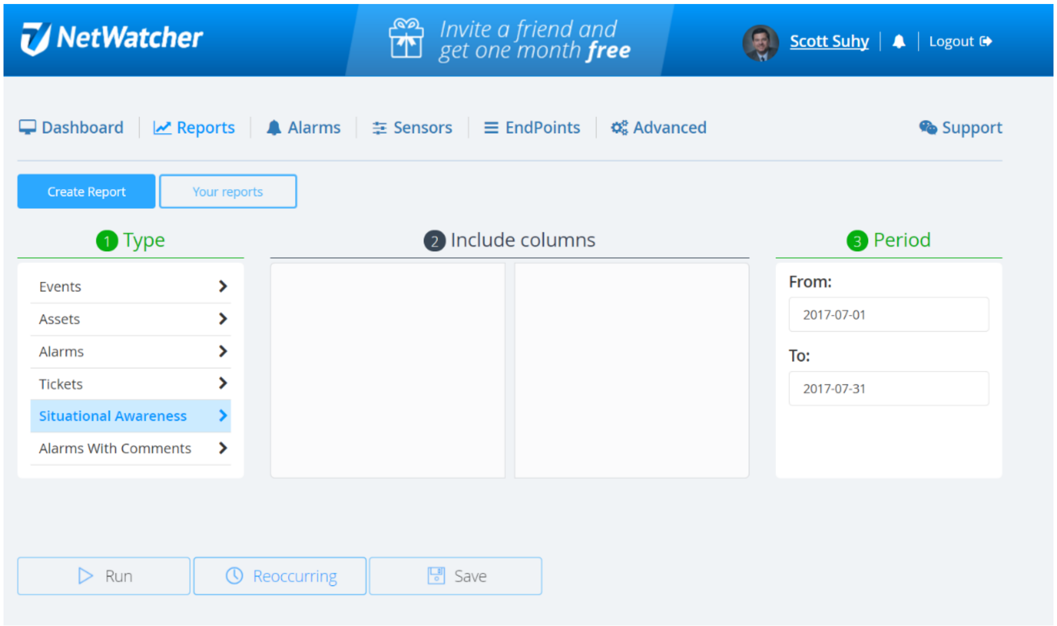
Generate

Optional: Email

IP/CIDR

Setup Reoccurring Reports

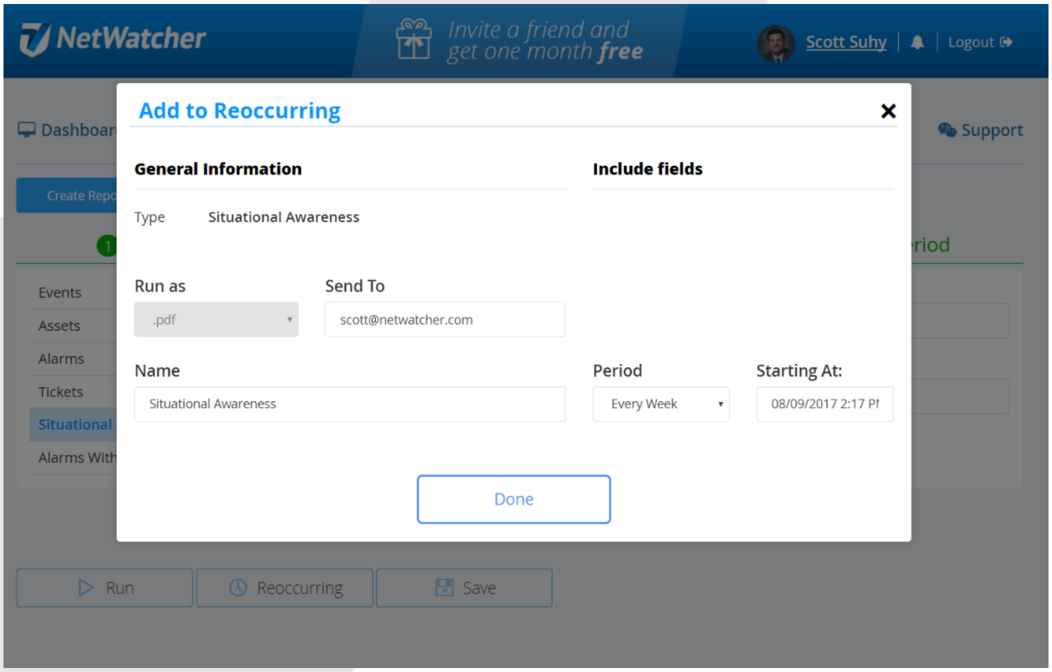
20. Go to the ‘Reports’ tab in the Customer Portal and choose the ‘Situational Awareness’ report. This gives you an overview of the entire landscape. Create the report from the beginning of a month to the end of a month.



From: 2017-07-01

To: 2017-07-31

21. Choose where to send the report to (email address, but it will also store it on the portal for you to download in the future) and choose how often you want to receive the report.



Add to Reoccurring

General Information

Include fields

Type Situational Awareness

Run as .pdf

Send To scott@netwatcher.com

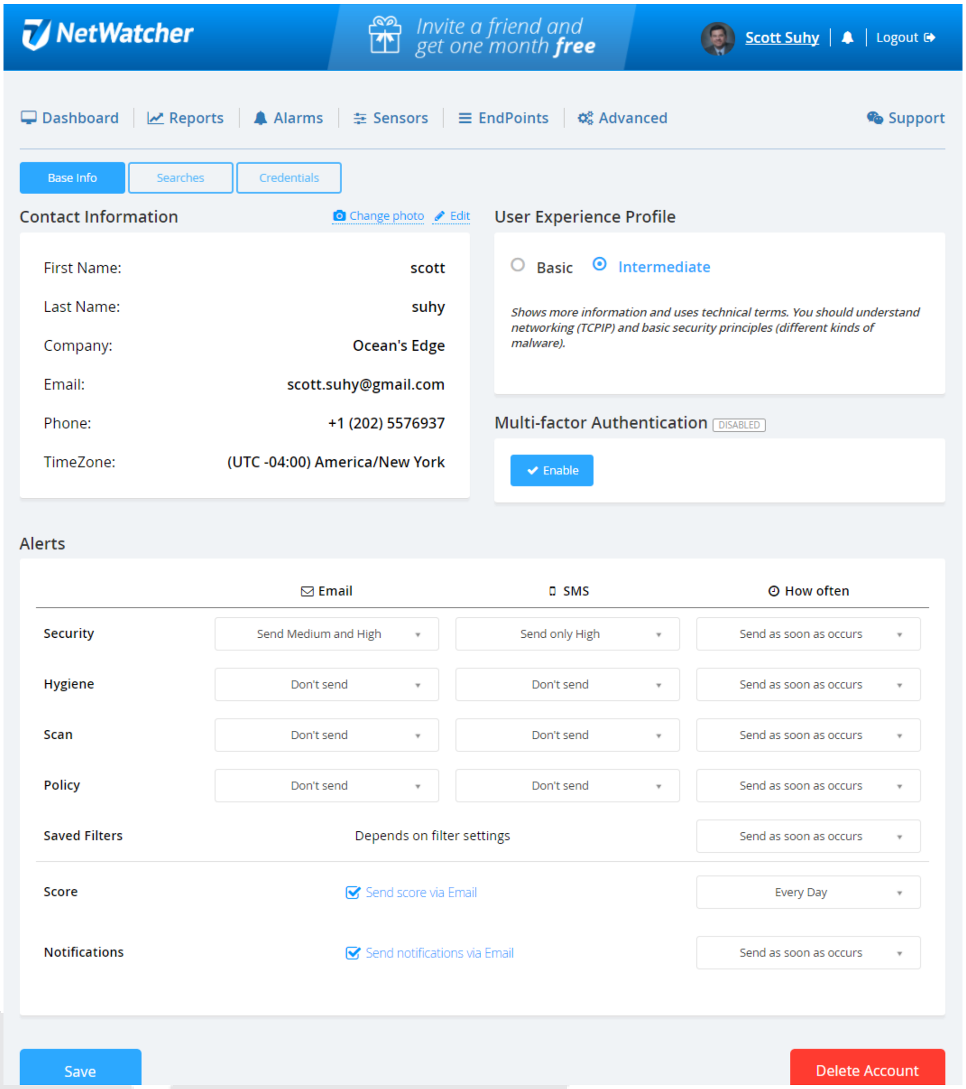
Name Situational Awareness

Period Every Week

Starting At: 08/09/2017 2:17 PI

Setup Notifications

22. Setup your notifications by choosing your name in the upper right corner of the screen.



Contact Information

First Name:	scott
Last Name:	suhy
Company:	Ocean's Edge
Email:	scott.suhy@gmail.com
Phone:	+1 (202) 5576937
TimeZone:	(UTC -04:00) America/New York

User Experience Profile

○ Basic ● Intermediate

Shows more information and uses technical terms. You should understand networking (TCPIP) and basic security principles (different kinds of malware).

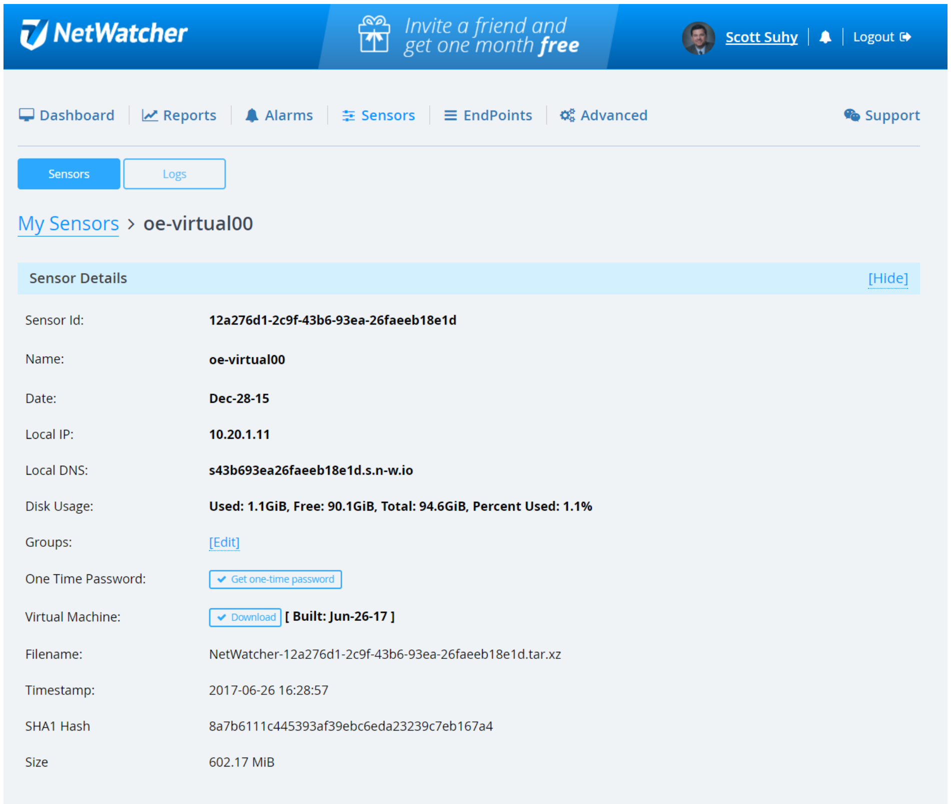
Multi-factor Authentication DISABLED

Alerts

	Email	SMS	How often
Security	Send Medium and High	Send only High	Send as soon as occurs
Hygiene	Don't send	Don't send	Send as soon as occurs
Scan	Don't send	Don't send	Send as soon as occurs
Policy	Don't send	Don't send	Send as soon as occurs
Saved Filters	Depends on filter settings		Send as soon as occurs
Score	☑ Send score via Email		Every Day
Notifications	☑ Send notifications via Email		Send as soon as occurs

Connecting Virtual Sensor to NetWatcher Cloud – VSphere

1. The NetWatcher team should have sent you an Activate email that will allow you to create your Customer Portal account. If you didn't get this send a note to info@netwatcher.com and someone will assist you.
2. Ensure you are not blocking any of the following ports OUTBOUND. These ports are what the sensor uses to communicate back to the NetWatcher cloud.
    - TCP 22 => portal.netwatcher.com
    - TCP 8443 => p.netwatcher.com
    - UDP 443 => vpn.netwatcher.com
    - TCP 443 => vpn-tcp.netwatcher.com
    - TCP 443 => index.docker.io
    - TCP 443 => registry-1.docker.io
    - TCP 443 => public.update.core-os.net
    - TCP 80 to google.com => Used to test internet/DNS connectivity
3. Log in to https://portal.netwatcher.com/login navigate to https://portal.netwatcher.com/sensor/sensors , click on your sensor, and press the download button next to the Virtual Machine. 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. Compare the SHA1 hash.



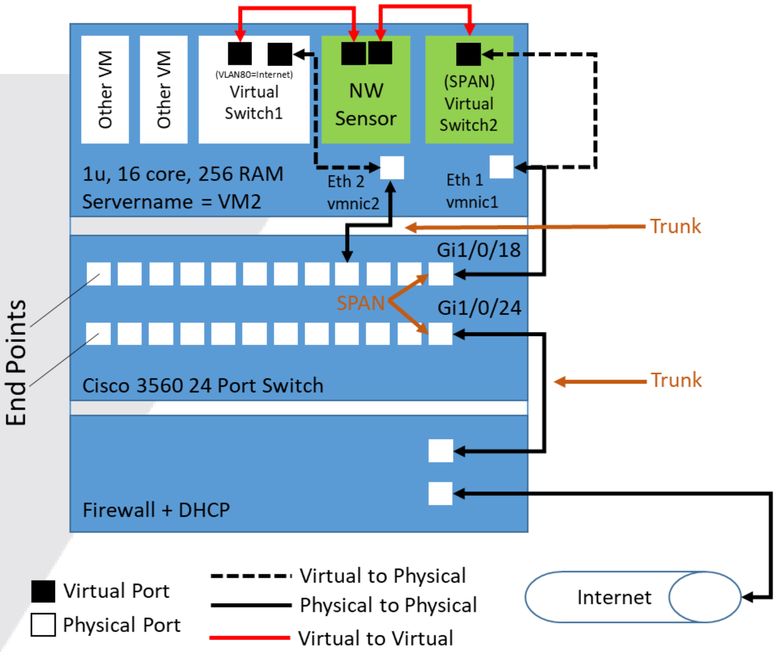
NetWatcher | Invite a friend and get one month *free* | Scott Suhy | Logout

My Sensors > oe-virtual00

Sensor Details [Hide]

Sensor Id:	**12a276d1-2c9f-43b6-93ea-26faeeb18e1d**
Name:	**oe-virtual00**
Date:	**Dec-28-15**
Local IP:	**10.20.1.11**
Local DNS:	**s43b693ea26faeeb18e1d.s.n-w.io**
Disk Usage:	**Used: 1.1GiB, Free: 90.1GiB, Total: 94.6GiB, Percent Used: 1.1%**
Groups:	[Edit]
One Time Password:	✓ Get one-time password
Virtual Machine:	✓ Download **[Built: Jun-26-17]**
Filename:	NetWatcher-12a276d1-2c9f-43b6-93ea-26faeeb18e1d.tar.xz
Timestamp:	2017-06-26 16:28:57
SHA1 Hash	8a7b6111c445393af39ebc6eda23239c7eb167a4
Size	602.17 MiB

4. Understand your current VM architecture and map out how you will setup your sensor VM. Here is a typical setup:



5. Create a mirror of the firewall traffic for the Network Intrusion Detection (NIDS)

Example on a Cisco device: See https://learningnetwork.cisco.com/docs/DOC-26018

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
```

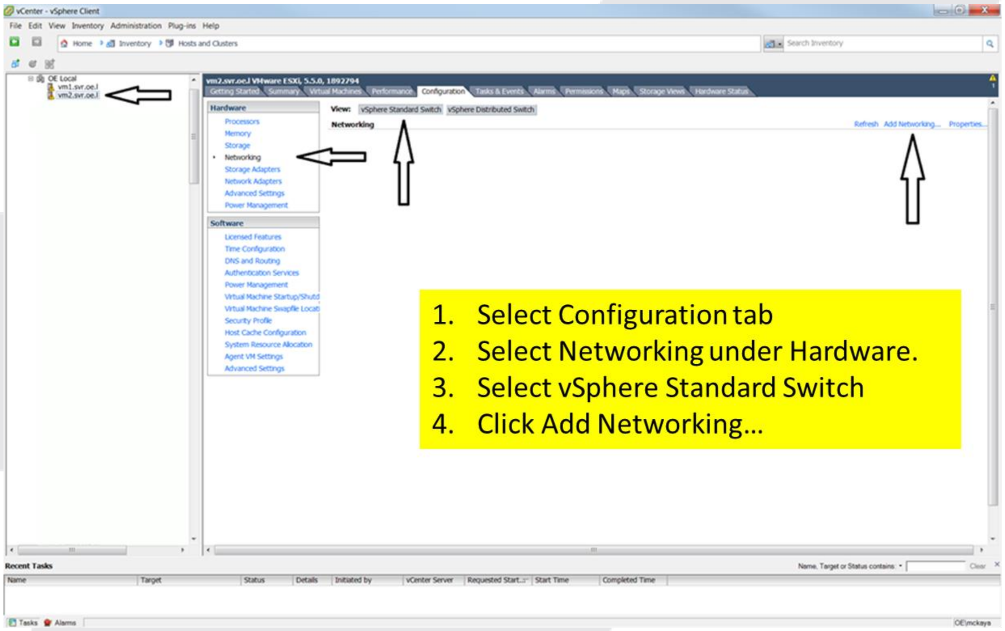
Identify Destination port for SPAN

```
#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
```

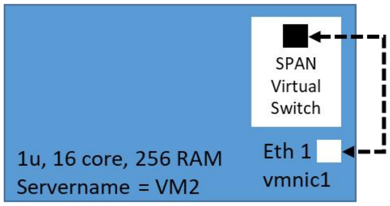
Configure SPAN:

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

6. Create a Virtual Switch w/Virtual SPAN Port & Map it to a Physical Port

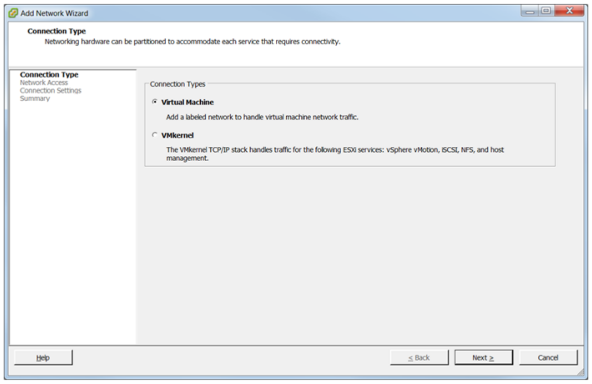


1. Select Configuration tab
2. Select Networking under Hardware.
3. Select vSphere Standard Switch
4. Click Add Networking…



7. Create a Virtual Switch w/Virtual SPAN Port & Map it to a Physical Port--Create the SPAN Port to mirror all traffic. Set VLAN ID to 4095 (Step 3) to ensure proper handling of VLAN tags.

1



Add Network Wizard

Connection Type

Networking hardware can be partitioned to accommodate each service that requires connectivity.

Connection Type
Network Access
Connection Settings
Summary

Connection Types

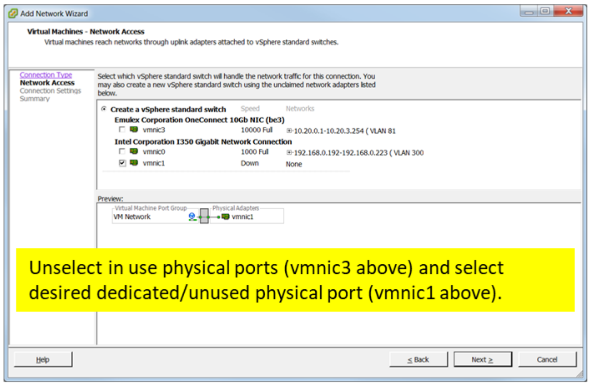
● **Virtual Machine**

Add a labeled network to handle virtual machine network traffic.

○ **VMkernel**

The VMkernel TCP/IP stack handles traffic for the following ESXi services: vSphere vMotion, iSCSI, NFS, and host management.

2



Add Network Wizard

Virtual Machines - Network Access

Virtual machines reach networks through uplink adapters attached to vSphere standard switches.

Connection Type
Network Access
Connection Settings
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**

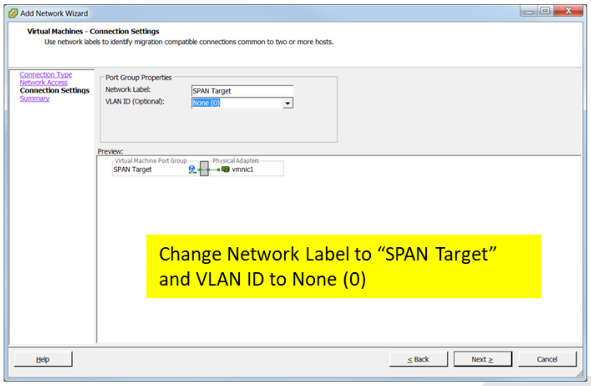
	Speed	Networks
Emulex Corporation OneConnect 10Gb NIC (be3)		
□ vmnic3	10000 Full	10.20.0.1-10.20.3.254 (VLAN 81
Intel Corporation I350 Gigabit Network Connection		
□ vmnic0	1000 Full	192.168.0.192-192.168.0.223 (VLAN 300
☑ vmnic1	Down	None

Preview:

Virtual Machine Port Group	Physical Adapters
VM Network	vmnic1

Unselect in use physical ports (vmnic3 above) and select desired dedicated/unused physical port (vmnic1 above).

3



Add Network Wizard

Virtual Machines - Connection Settings

Use network labels to identify migration compatible connections common to two or more hosts.

Connection Type
Network Access
Connection Settings
Summary

Port Group Properties

Network Label: SPAN Target

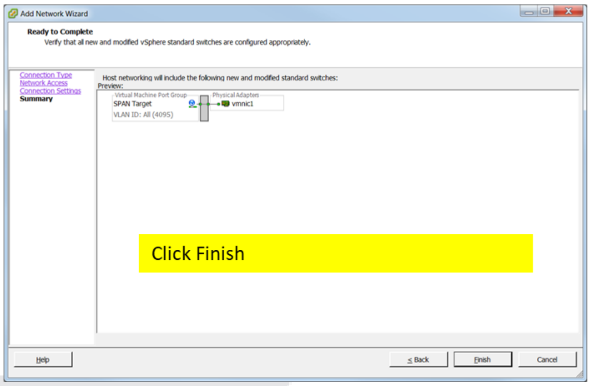
VLAN ID (Optional): None (0)

Preview:

Virtual Machine Port Group	Physical Adapters
SPAN Target	vmnic1

Change Network Label to “SPAN Target” and VLAN ID to None (0)

4



Add Network Wizard

Ready to Complete

Verify that all new and modified vSphere standard switches are configured appropriately.

Connection Type
Network Access
Connection Settings
Summary

Host networking will include the following new and modified standard switches:

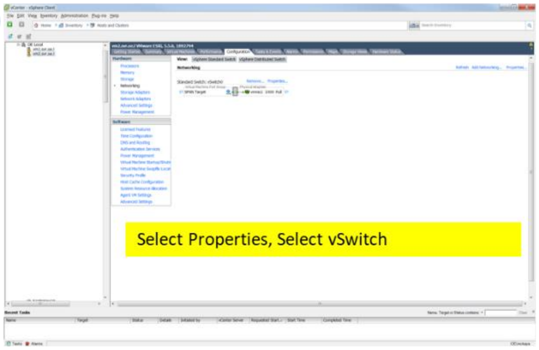
Preview:

Virtual Machine Port Group	Physical Adapters
SPAN Target VLAN ID: All (4095)	vmnic1

Click Finish

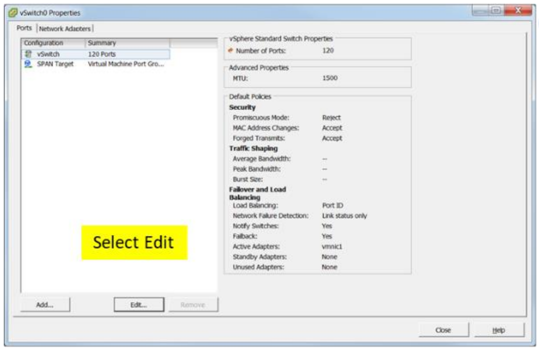
8. Create a Virtual Switch w/Virtual SPAN Port & Map it to a Physical Port--Enable Promiscuous Mode

1



Select Properties, Select vSwitch

2



vSwitch0 Properties

Ports | Network Adapters |

Configuration	Summary
vSwitch	120 Ports
SPAN Target	Virtual Machine Port Gro...

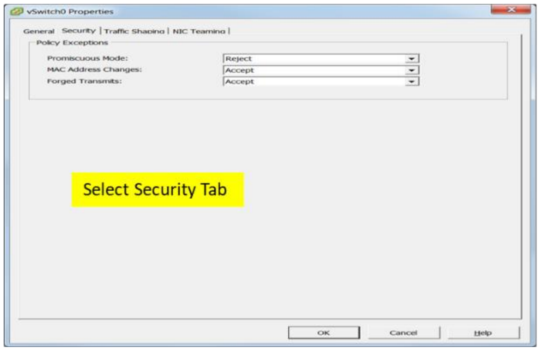
vSphere Standard Switch Properties
Number of Ports: 120

Advanced Properties
MTU: 1500

Default Policies
Security
Promiscuous Mode: Reject
MAC Address Changes: Accept
Forged Transmits: Accept
Traffic Shaping
Average Bandwidth: --
Peak Bandwidth: --
Burst Size: --
Failover and Load Balancing
Load Balancing: Port ID
Network Failure Detection: Link status only
Notify Switches: Yes
Failback: Yes
Active Adapters: vmnic1
Standby Adapters: None
Unused Adapters: None

Select Edit

3



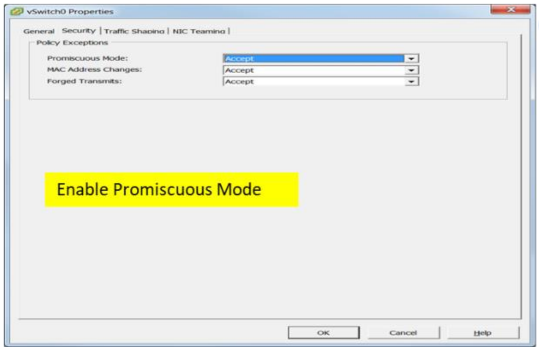
vSwitch0 Properties

General Security | Traffic Shaping | NIC Teaming |

Policy Exceptions
Promiscuous Mode: Reject
MAC Address Changes: Accept
Forged Transmits: Accept

Select Security Tab

4



vSwitch0 Properties

General Security | Traffic Shaping | NIC Teaming |

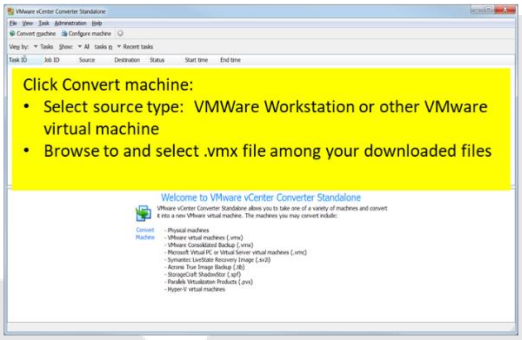
Policy Exceptions
Promiscuous Mode: Accept
MAC Address Changes: Accept
Forged Transmits: Accept

Enable Promiscuous Mode

9. Import NetWatcher Sensor VM

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

1



VMware vCenter Converter Standalone

Click Convert machine:

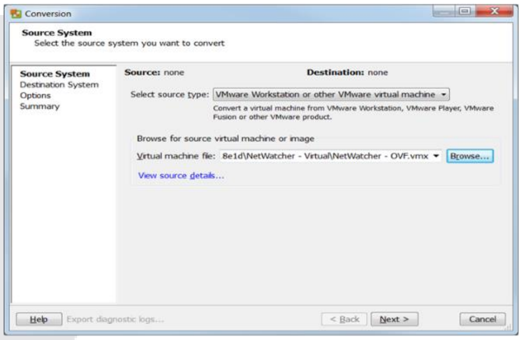
- Select source type: VMWare Workstation or other VMware virtual machine
- Browse to and select .vmx file among your downloaded files

Welcome to VMware vCenter Converter Standalone

VMware vCenter Converter Standalone allows you to take one of a variety of machines and convert it into a new VMware virtual machine. The machines you may convert include:

- Physical machines
- VMware virtual machines (.vmx)
- VMware Consolidated Backup (.vmx)
- Microsoft Virtual PC or Virtual Server virtual machines (.vmc)
- Symantec LiveState Recovery Image (.sv2i)
- Acronis True Image Backup (.tib)
- StorageCraft ShadowStor (.spf)
- Parallels Virtualization Products (.pvs)
- Hyper-V virtual machines

2



Conversion

Source System
Select the source system you want to convert

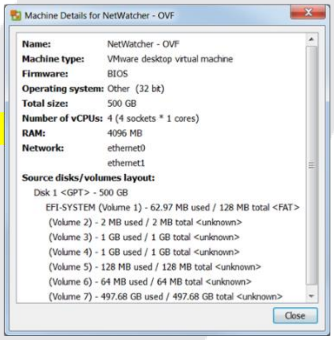
Source: none **Destination:** none

Select source type: VMware Workstation or other VMware virtual machine
Convert a virtual machine from VMware Workstation, VMware Player, VMware Fusion or other VMware product.

Browse for source virtual machine or image
Virtual machine file: 8e1d\NetWatcher - Virtual\NetWatcher - OVF.vmx

3

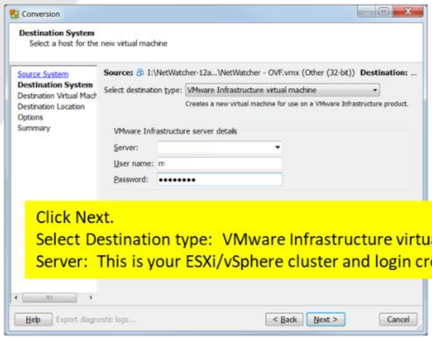
Click on source details and it should look like this:



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>

4



Conversion

Destination System
Select a host for the new virtual machine

Source: I:\NetWatcher-12a...\NetWatcher - OVF.vmx (Other (32-bit)) **Destination:** ...

Select destination type: VMware Infrastructure virtual machine
Creates a new virtual machine for use on a VMware Infrastructure product.

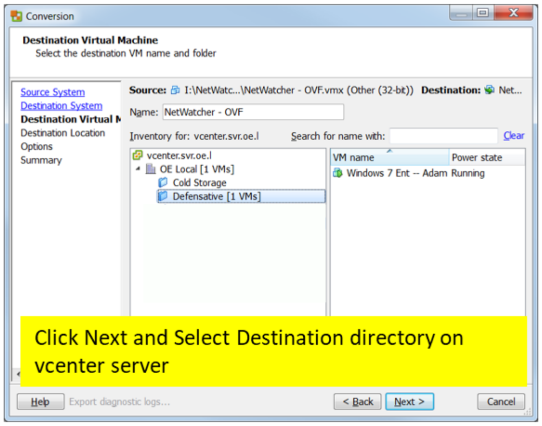
VMware Infrastructure server details
Server:
User name: m
Password: ••••••••

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

NW Sensor

10. Import NetWatcher Sensor VM

1



Conversion

Destination Virtual Machine
Select the destination VM name and folder

Source System
Destination System
Destination Virtual M
Destination Location
Options
Summary

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

Name: NetWatcher - OVF

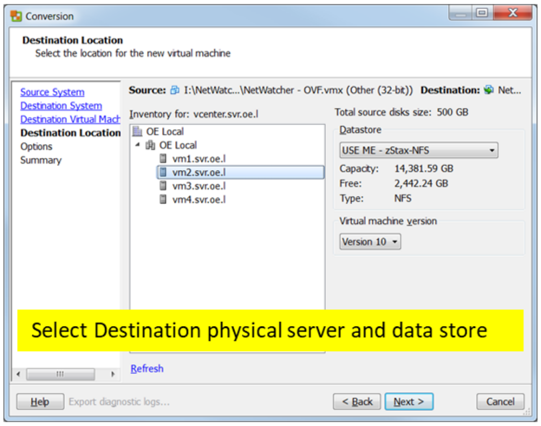
Inventory for: vcenter.svr.oe.l   Search for name with: Clear

- vcenter.svr.oe.l
  - OE Local [1 VMs]
    - Cold Storage
    - Defensative [1 VMs]

VM name	Power state
Windows 7 Ent -- Adam	Running

Click Next and Select Destination directory on vcenter server

2



Conversion

Destination Location
Select the location for the new virtual machine

Source System
Destination System
Destination Virtual Mach
Destination Location
Options
Summary

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

Inventory for: vcenter.svr.oe.l

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

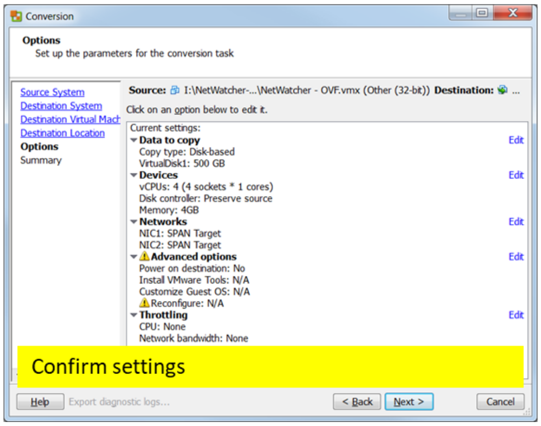
Total source disks size: 500 GB

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



Conversion

Options
Set up the parameters for the conversion task

Source System
Destination System
Destination Virtual Mach
Destination Location
Options
Summary

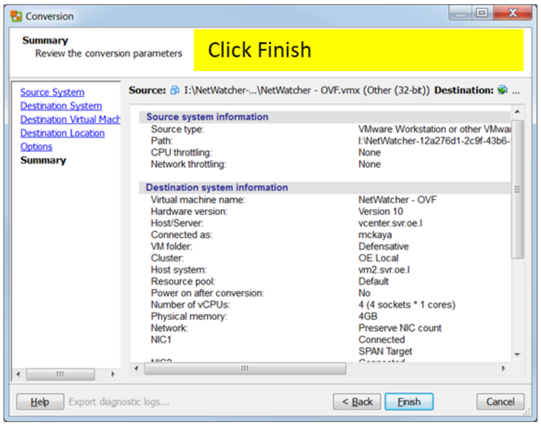
Source: I:\NetWatcher-...\NetWatcher - OVF.vmx (Other (32-bit)) **Destination:** ...

Click on an option below to edit it.

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

Confirm settings

4



Conversion

Summary
Review the conversion parameters

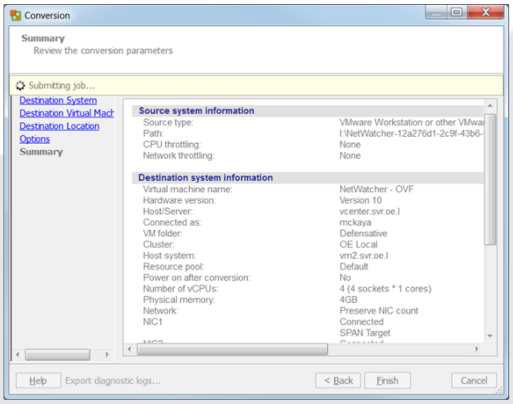
Click Finish

Source System
Destination System
Destination Virtual Mach
Destination Location
Options
Summary

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

Source system information	
Source type:	VMware Workstation or other VMwar
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

11. Import NetWatcher Sensor VM



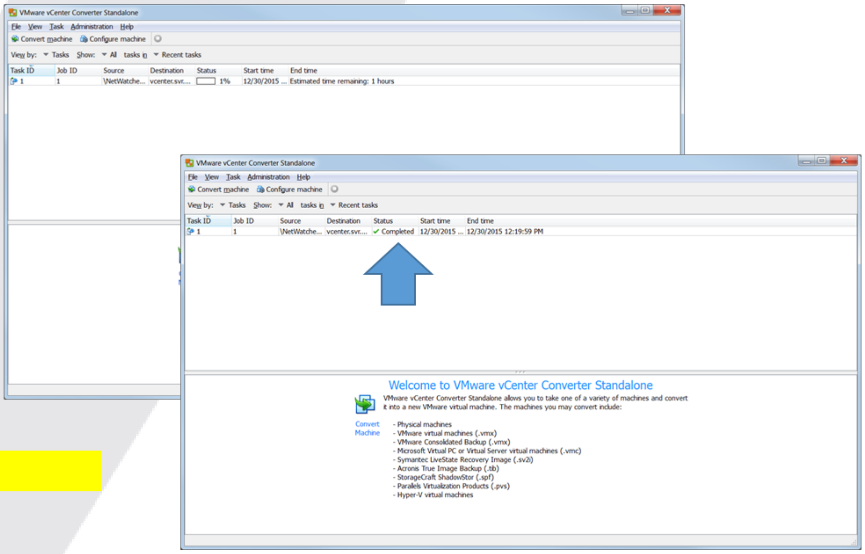
Conversion

Summary
Review the conversion parameters

Submitting job...

Destination System
Destination Virtual Mach
Destination Location
Options
Summary

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



VMware vCenter Converter Standalone

Task ID	Job ID	Source	Destination	Status	Start time	End time
1	1	\NetWatche...	vcenter.svr....	1%	12/30/2015 ...	Estimated time remaining: 1 hours

VMware vCenter Converter Standalone

Task ID	Job ID	Source	Destination	Status	Start time	End time
1	1	\NetWatche...	vcenter.svr....	✓ Completed	12/30/2015 ...	12/30/2015 12:19:59 PM

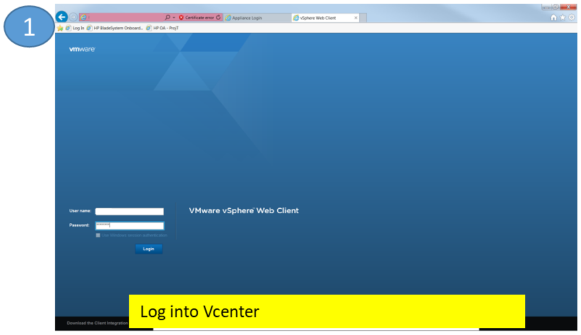
Welcome to VMware vCenter Converter Standalone

VMware vCenter Converter Standalone allows you to take one of a variety of machines and convert it into a new VMware virtual machine. The machines you may convert include:

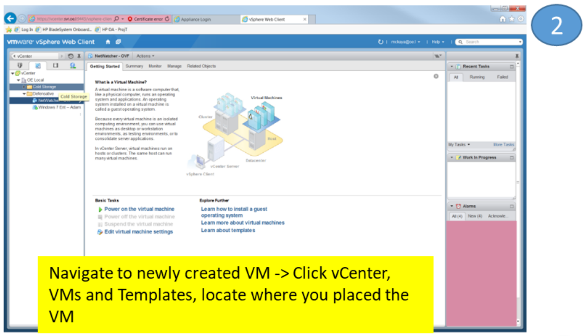
- Physical machines
- VMware virtual machines (.vmx)
- VMware Consolidated Backup (.vmx)
- Microsoft Virtual PC or Virtual Server virtual machines (.vmc)
- Symantec LiveState Recovery Image (.sv2i)
- Acronis True Image Backup (.tib)
- StorageCraft ShadowStor (.spf)
- Parallels Virtualization Products (.pvs)
- Hyper-V virtual machines

Let it build.

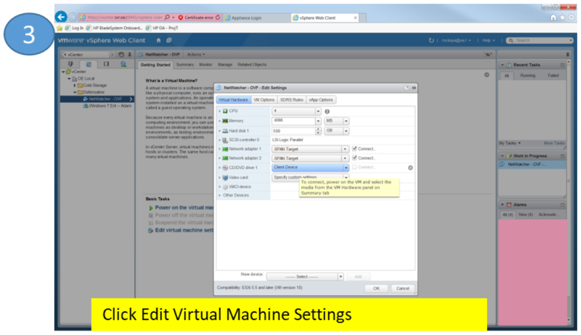
12. Map NetWatcher Sensors Network Adapter 1 and Network Adapter 2



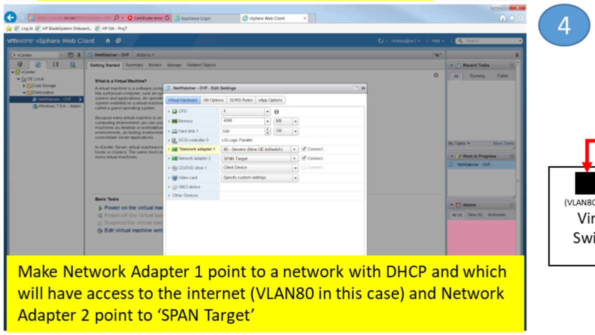
Log into Vcenter



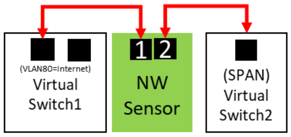
Navigate to newly created VM -> Click vCenter, VMs and Templates, locate where you placed the VM



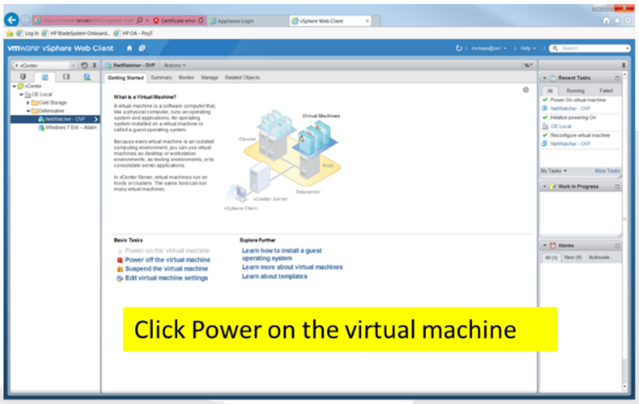
Click Edit Virtual Machine Settings



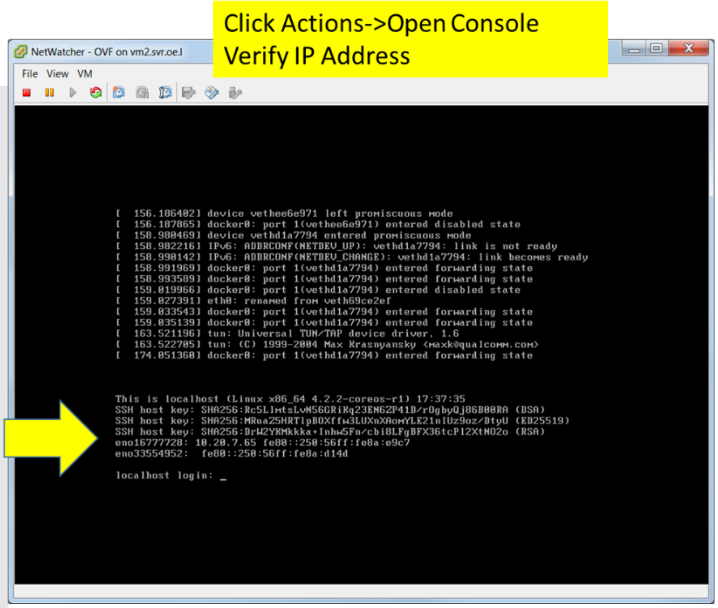
Make Network Adapter 1 point to a network with DHCP and which will have access to the internet (VLAN80 in this case) and Network Adapter 2 point to 'SPAN Target'



13. Open NetWatcher Sensor Console



Click Power on the virtual machine



Click Actions->Open Console
Verify IP Address

```
[  156.186402] device vethee6e971 left promiscuous mode
[  156.187865] docker0: port 1(vethee6e971) entered disabled state
[  158.980469] device vethd1a7794 entered promiscuous mode
[  158.982216] IPv6: ADDRCONF(NETDEV_UP): vethd1a7794: link is not ready
[  158.990142] IPv6: ADDRCONF(NETDEV_CHANGE): vethd1a7794: link becomes ready
[  158.991969] docker0: port 1(vethd1a7794) entered forwarding state
[  158.993589] docker0: port 1(vethd1a7794) entered forwarding state
[  159.019966] docker0: port 1(vethd1a7794) entered disabled state
[  159.027391] eth0: renamed from veth69ce2ef
[  159.033543] docker0: port 1(vethd1a7794) entered forwarding state
[  159.035139] docker0: port 1(vethd1a7794) entered forwarding state
[  163.521196] tun: Universal TUN/TAP device driver, 1.6
[  163.522705] tun: (C) 1999-2004 Max Krasnyansky <maxk@qualcomm.com>
[  174.051360] docker0: port 1(vethd1a7794) entered forwarding state


This is localhost (Linux x86_64 4.2.2-coreos-r1) 17:37:35
SSH host key: SHA256:Rc5LlmtsLvN56GRiKq23EN6ZP41D/rOgbyQj86B00RA (DSA)
SSH host key: SHA256:MRuaZ5HRTlpBOXffw3LUXnXAomYLE21nIUz9oz/DtyU (ED25519)
SSH host key: SHA256:DrW2YKMkkka+Inhw5Fn/cbi8LFgBFX36tcPl2XtNO2o (RSA)
eno16777728: 10.20.7.65 fe80::250:56ff:fe8a:e9c7
eno33554952:  fe80::250:56ff:fe8a:d14d

localhost login: _
```

14. If you need to setup a static IP address see this article.

15. Login to the Customer Portal to Verify Sensor is Live (Sensor will turn amber if it can connect to the NetWatcher cloud; Sensor will turn green if it can also see the mirror/SPAN traffic)

Installing the Virtual Sensor on Other Virtual Machine Platforms

- For VMWare workstation (for testing only, not production) find details here
- For Hyper-V find details here

We hope you enjoy the NetWatcher service. We've designed the service to be useful for managers, help desk techs and for advanced security analysts. We've tried to make the User Interface (UI) intuitive and easy to use as well as powerful. If you have any questions don't hesitate to contact us at info@netwatcher.com

Follow us on Twitter @netwatcher.

https://netwatcher.com