

Network Passive Sensor

Virtual Appliance User Guide

November 24, 2023

Copyright 2022-23 by Qualys, Inc. All Rights Reserved.

Qualys, the Qualys logo and QualysGuard are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

Qualys, Inc. 919 E Hillsdale Blvd 4th Floor Foster City, CA 94404 1 (650) 801 6100

Table of Contents

About this Guide	4
Welcome to Qualys Network Passive Sensor	5
Network requirements / configuration Get Started Mirror the traffic Step 1 - Download Virtualization Image Step 2 - Generate Personalization Code Step 3 - Deploy Virtualization Image Step 4 - Register the Virtual Appliance Step 5 - Check the Status Manage Sensors	
Network Configurations	19 27
Configure Static IP Address Proxy Configuration	27 28
Appendix	29
Virtual Network Passive Sensor (PS) Appliance Packet Throughput Based on Resc Virtual Network Passive Sensor (PS) Throughput Capacity Based on Hardware Adding/Removing Sniffing Interfaces from Virtual Appliance Classification of Assets in Passive Sensor	ources 29 29 33 37
Best Practices	43

About this Guide

Welcome to Qualys Cloud Platform! In this guide, we'll show you how to set up your virtual appliance for Qualys Network Passive Sensor.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA).

For more information, please visit www.qualys.com.

Contact Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at www.qualys.com/support/.

Welcome to Qualys Network Passive Sensor

With Qualys Network Passive Sensor (PS), you can automatically detect, and profile devices connected to your network, eliminating blind spots across your IT environment. Network Passive Sensor monitors network activity without any active probing of devices in order to detect active assets in your network.

Virtual Appliance supports a maximum throughput of 2Gbps. It can be scaled up or down depending on the resources allocated to it. Refer to the Appendix section for more details.

It's easy to set up a virtual appliance. We'll help you with the steps.

Bandwidth	Minimum recommended bandwidth connection of 1 Megabits per second (Mbps) to the Qualys Cloud Platform for a network containing around 10,000 assets.
Appliance Access	The Network Passive Sensor must be able to reach certain infrastructure located on the Qualys Cloud Platform where your Qualys account is located. The local network must be configured to allow outbound HTTPS (port 443) access to the Internet, so that the Network Passive Sensor can communicate with the Qualys Cloud Platform. Tip - Log into your account and go to Help > About to see the Qualys Cloud Platform URLs.
DHCP or Static IP	By default the Network Passive Sensor is pre-configured with DHCP. If configured with a static IP address, be sure you have the IP address, netmask, default gateway and primary DNS.
Proxy Support	The Network Passive Sensor includes Proxy support with or without authentication. Proxy-level termination (as implemented in SSL bridging, for example) is not supported. SOCKS proxies are not supported.

Network requirements / configuration

Get Started

Network Passive Sensor will start discovering assets on your network once you complete the setup. It takes just a couple of minutes. It's important that you complete the steps in the order shown.

Mirror the traffic

You need to feed traffic to the appliance by mirroring the traffic (using physical tap or mirror port). Connect the mirrored port to the sniffing interface of the appliance. This step is required in order to see discovered assets.

Network Passive Sensor supports mirror traffic of SPAN, RSPAN, and ERSPAN methods. For more information, refer to the Deployment Guide.

Step 1 - Download Virtualization Image

1) Log in to the Qualys UI and select **Network Passive Sensor** from the app picker.

2) On the Home tab, scroll down and click Deploy Network Sensor.

3) From the **Sensors** tab, go to **New Sensor** > **Virtual Sensor** and then click **Download** link from Deploy Image step of the New Virtual Sensor wizard. For VMWare ESXi, you can download the image (OVA file) to your local system. For Hyper-V, you can download zip file of the Hyper-V image. Click **I Agree** from **Review and Agree to Virtual Scanner License** popup. The image download will start.

Step 2 - Generate Personalization Code

You'll need a unique personalization code to register your appliance with the Qualys Cloud Platform. Follow these steps to generate a personalization code:

1) Log in to the Qualys UI and select **Network Passive Sensor** from the app picker.

2) On the Sensors tab, go to **New Sensor** > **Virtual Sensor** to register a new sensor.

3) In the **New Virtual Sensor** wizard, provide a name for your sensor and the location. Click the **Generate Code** button. **Copy the code and keep it handy. You'll need it later.**

4) Click **Next** to go to the Installation screen. If you have not downloaded image from Home screen, you'll be able to download it form there.

5) Click **Next** to go to the Define Internal Assets screen. Here, you'll define the IP ranges within your network you want to monitor. The assets discovered for these IP addresses will be individually inventoried and tracked for traffic analysis. You can use default IP ranges or use customized IP ranges. Select **Inventory these assets** check box for marking inventoried assets. You'll be able to apply existing tags to these assets. To configure internal, external and excluded type of assets, refer Configure Assets.

6) Click **Finish** to complete the registration steps. A pop up will be shown with Sensor not connected text. Now complete the next steps and the sensor status will change once registration is successful in Step 4 - Register the Virtual Appliance.

Step 3 - Deploy Virtualization Image

You can deploy the image on the VMware ESXi or Microsoft Hyper-V. VMware ESXi or Microsoft Hyper-V monitors the network activity without any active probing of the device in order to detect the active assets on the network. It identifies the key device attributes that help the web services on the cloud to catalog the devices into operating system/hardware.

Deployment on VMware ESXi

ESXi server requirements: VMware ESXi 6.0 or later, 50 GB HDD, 16 GB Memory, Octa-Core Processor

Follow these steps to deploy an image on ESXi server:

1) Login to your ESXi Server, and go to **Virtual Machines** > **Create/Register VM**. It will open New Virtual Machine wizard.

2) For creation type, choose **Deploy a virtual machine from an OVF or OVA file**.

1 Select creation type 2 Select OVF and VMDK files 3 Select storage	Select creation type How would you like to create a Virtual Machine?	
4 License agreements 5 Deployment options 6 Additional settings	Create a new virtual machine Deploy a virtual machine from an OVF or OVA file	This option guides you through the process of creating a virtual machine from an OVF and VMDK files.
7 Ready to complete	Register an existing virtual machine	
vm ware [®]		

3) Click **Next** and enter a name for your virtual machine. Select or drag/drop the virtual sensor image you downloaded in Step 1 - Download Virtualization Image.

1 Select creation type 2 Select OVF and VMDK files 3 Select storage	Select OVF and VMDK files Select the OVF and VMDK files or OVA for the VM you would like to deploy
4 License agreements 5 Deployment options 6 Additional settings 7 Ready to complete	Enter a name for the virtual machine. Network_Passive_Sensor_VM Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance. * m qPS-1.3.0-11.ova
vm ware	

4. Click **Next** and select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Select OVF and VMDK files Select storage	Select storage Select the storage type and dat	astore						
License agreements Deployment options Additional settings Ready to complete	Standard Persistent Men Select a datastore for the virtu	nory Ial machine's I	configuration file	es and all of its'	virtual disks.			
	Name	~	Capacity 🗸	Free 🗸	Type 🗸 🗸	Thin pro 🗸	Access	`
	Datastore-2_5.69		4.31 TB	2.75 TB	VMFS6	Supported	Single	
	datastore1_5.69		42.5 GB	33.71 GB	VMFS6	Supported	Single	
							2 it	en
vm ware [®]								

5. Click **Next** to go to the **Deployment Options** page. The OVA file creates a VM with two interfaces - Management and Sniffing.

 1 Select creation type 2 Select OVF and VMDK files 3 Select storage 	Deployment options Select deployment options	
 4 Deployment options 5 Ready to complete 	Network mappings	Management VM Network Sniffing Interface My_Port_Group
	Disk provisioning Power on automatically	
vm ware [®]		
		Back Next Finish Car

The Management interface is required to connect the virtual appliance to the Qualys Cloud Platform. Make sure the Management interface is connected to the preconfigured port group having WAN or Internet connectivity. The Sniffing interface is used by the appliance to inspect the traffic. Make sure the Sniffing interface is connected to the pre-configured port group having TAP/TUN interface. Also make sure that "Promiscuous Mode" is enabled on respective vSwitch and port group.

Following screen shows typical vSwitch topology with port group settings.

✓ Edit settings ✓ Refresh			
▼ vSwitch topology	* Security policy		
	Allow promiscuous mode	Yes	
My_Port_Group Physical adapters	Allow forged transmits	Yes	
VLAN ID: 4095	Allow MAC changes	Yes	
Network_Passive_Senso	✓ NIC teaming policy		
	Notify switches	Yes	
	Policy	Route based on originating port ID	
	Reverse policy	Yes	
	Failback	Yes	
	 Shaping policy 		
	Enabled	No	

6. Click **Next** and review the settings configured earlier. Click **Finish** and wait for some time to complete the virtual appliance deployment using OVA.

7. Once the deployment is complete, open the virtual appliance console by selecting the VM and navigating to **Console** > Open browser console. Wait while the VM boots up.

Console 🌆 Monitor	Power on Power off II Suspend Reset	🥖 Edit 🕴 🧲 Refresh 🕴 🏠 Actio	ons		сри 86 MHz
	Guest OS Red Hat Enterprise L Compatibility ESXI 6.0 and later (V VMware Tools No	inux 7 (64-bit) M version 11)			MEMORY 10 936 MB
	Memory 16 GB			K	18.56 GB
- General Information			+ Hardware Configuration		
Networking	No network information		F 🔲 CPU	8 vCPUs	
Mware Tools	Not installed	Actions	Memory	16 GB	
Storage	1 disk		Hard disk 1	50 GB	
Notes	QualysGuard(R) Virtual Passive Scanner Applian	nce, build:qPS- 🥖 Edit notes	Ima Network adapter 1	VM Network (Connected)	
	1.3.0-11		Network adapter 2	My_Port_Group (Connected)	
Performance summary las	st hour		Video card	8 MB	
	Consumed host CPU	Ready	Others	Additional Hardware	
100.	 Consumed host memory 	y	* Resource Consumption		
2		15	Consumed host CPU	86 MHz	
£ 80		onsu	Consumed host memory	936 MB	
8 60		10	Kative guest memory	163 MB	
E CE		host			
g 40		me m	Provisioned	50 GB	
20		5 By	Uncommitted	47.55 GB	
12 20		GB	Not-shared	18.56 GB	
0					

8) There are some network configuration settings (static IP, proxy) you'll need to set before proceeding to the next step. Complete Network Configurations.

Deployment on Microsoft Hyper-V

Hyper-V server requirements: Microsoft Hyper-V 2012 R2 or later, 50 GB HDD, 16 GB Memory, Octa-Core with total 14 GHz dedicated CPU Clock Processor

Follow these steps to deploy an image on Hyper-V server:

1) Login to your Hyper-V Server and go to **Start** > **Server Manager** > **Tools** > **Hyper-V Manager**. Right-click your Hyper-V host and select New > Virtual Machine.

2) For Specify Name and Location, provide the name that will be displayed on Hyper-V Manager and select the location where virtual machine will be stored.

3) For Specify Generation, select the appropriate generation(recommended - Generation 1) for the virtual machine.

4) For Assign Memory, provide appropriate memory (RAM) for the virtual machine. Minimum recommended RAM is 16384 MB.

5) For Configure Networking, select appropriate virtual switch with Internet connectivity so that the network adapter on the sensor can use a virtual network for communication with Qualys cloud platform.

6) For Connect Virtual Hard Disk, select "Use an existing virtual hard disk" and provide the location of the .vhdx file (Unzip the zip file downloaded in Step 1 - Download Virtualization Image to obtain the virtual hard disk file. As an example, unzip qPS-1.0.0-1-vhdx.zip to obtain the virtual hard disk qPS-1.0.0-1-disk1.vhdx).

7) Click **Next** and review Summary. Click **Finish** and your virtual machine is ready. Following screen shows the deployment configurations.

Setore You Begin	A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.
Specify Generation	O Create a virtual hard disk
Assign Memory	Use this option to create a VHDX dynamically expanding virtual hard disk.
Configure Networking	Name: New Virtual Machine.vhdx
onnect Virtual Hard Disk	Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\ Browse
ummary	Size: 127 GB (Maximum: 64 TB)
	Use an existing virtual hard disk Use this exists a statute with all hard disk
	Use this option to attach an existing virtual hard disk, either VHD or VHDX format.
	Location: Divers Administrator Downloads QPS-1.0.0-1-vhdx QPS-1.0.0-1- Browse
	Attach a virtual bard disk later
	Use this option to skip this step now and attach an existing virtual hard disk later.

8) Select the virtual machine (just created) and navigate to Settings. Change default number of virtual processors to 8.

Qua	lys Network Passive Sensor qPS-1.	
	Hardware Add Hardware BIOS Boot from CD Security Key Storage Drive disabled Memory	Processor You can modify the number of virtual processors based on the number of processors on the physical computer. You can also modify other resource control settings. Number of virtual processors: 8 Resource control
• [16384 MB Processor 8 Virtual processors	You can use resource controls to balance resources among virtual machines. Virtual machine reserve (percentage): 0
	IDE Controller 0 IDE Controller 0 IDE Controller 1 DUD Drive None	Percent of total system resources: 0 Virtual machine limit (percentage): 100 Percent of total system resources: 80 Relative weight: 100
	SISI Controller Network Adapter LAN-Network-vSwitch COM 1 None COM 2 None None None None None None None None	This virtual machine is configured with the following: Sockets: 2 NUMA nodes per socket: 1 Virtual processors per NUMA node: 10 Memory per NUMA node: 13318 MB

9) Make sure that "Automatic Stop Action" the VM is set to "Turn off the virtual machine" and apply changes.



10) Navigate to **Virtual Switch Manager** and create a new virtual network switch > Select type of switch as **External**.

Virtual Switches	💒 Create virtual switch
New virtual network switch	What type of virtual switch do you want to create?
Intel(R) Gigabit 4P I350-t rNDC #2 PS-Test-Nic2 Intel(R) Gigabit 4P I350-t rNDC #3	External Internal Private
I perf_nic4 Intel(R) Gigabit 4P I350-t rNDC #4	
Global Network Settings MAC Address Range 00-15-5D-68-38-00 to 00-15-5D-6	Create Virtual Switch
	creates a virtual switch that binds to the physical network adapter so that virtual machines can access a physical network.

11) Give a name to the virtual switch, e.g., "test_switch".

12) Select the appropriate external physical **NIC** interface to connect the virtual switch from the drop-down menu.

13) Uncheck the option Allow management operating system to share the network adapter.

14) Click OK.

Virtual Switch Manager for NAC-HYPERV-2	016 — 🗆	\times
 Virtual Switch Manager for NAC-HYPERV-2 Virtual Switches New virtual network switch Regnt Intel(R) Gigabit 4P I350-trNDC #2 PS-Test-Nc2 Intel(R) Gigabit 4P I350-trNDC #3 Perf_nic4 Intel(R) Gigabit 4P I350-trNDC #4 TateI(R) Gigabit 4P I350-trNDC #4 A test_switch Intel(R) Gigabit 4P I350-trNDC #4 MAC Address Range 00-15-50-68-38-00 to 00-15-50-6 	016	×
	private switch. OK Cancel Apply	~

15) In Powershell, execute the following commands:

- Set the port feature property to the virtual switch created.

```
$portFeature = Get-VMSystemSwitchExtensionPortFeature -
FeatureName "Ethernet Switch Port Security Settings"
```

- Configure the port monitor mode.

\$portFeature.SettingData.MonitorMode = 2

- Use the same switch name as defined earlier

Add-VMSwitchExtensionPortFeature -ExternalPort -SwitchName test_switch -VMSwitchExtensionFeature \$portFeature

16) Select the virtual machine and go to **Settings**.

17) Go to **Add Hardware** > Select **Network Adapter** > Click **Add** > Click **OK** to add new network adapter in Hyper-V.



18) Select the second Network Adapter tab from the drop-down > Select the newly created virtual switch (**test_switch**).



19) Go to **Advanced Features** > Select **Destination** from Mirroring Mode drop-down in Port Mirroring Section.



20) Power on the VM.

21) There are some network configuration settings (static IP, proxy) you'll need to set before proceeding to the next step. Complete Network Configurations.

Step 4 - Register the Virtual Appliance

1) Open the Virtual Appliance console by selecting the VM and then navigating to **Console** > Open browser console.

2) Choose the **Personalize this scanner** option.

3) Enter your 14 digit personalization code which you generated in Step 2 - Generate Personalization Code.

Enter	the	14 d	ligit	Personalization Code:
	-			
		CSub	mit	(Cancel)

4) Click **Submit** and wait for the confirmation message **Appliance registration completed successfully**. Check that the status on the console is Registered.



5) Once your appliance successfully registers to the Qualys Cloud Platform, you'll start seeing appliance with status as paused.

Step 5 - Check the Status

Log in to the Qualys UI and select **Network Passive Sensor** from the application picker. Navigate to the **SENSORS** tab to view list of sensors in your account and their status.

Sens	sors						
	4 Active Assets (7days)	0 New Discoveries (24hrs)					
\bigtriangledown	Filters 🗸 New Sensor 🗸					1 - 3 of 3	< D C 🕸
	SENSOR	DEPLOY LOCATION	ACTIVE ASSETS (1 HOUR)	NETWORK UTILIZATION	CPU	RAM	HDD
X	PS-AutoPhysical Unregistered	Pune -	0	0	0	0	0
Ê	PS-AutoVirtual QPS-01G-0100-VM 1.3.2-12 Sensing	Pune 10.113.231.61 / fe80::20c:29ff:febb:fd03 00:0c:29:bb:fd:03	73	0.0 Gbps/1.0 Gbps	20%	22%	4%
ê	PS-Virtual_deploy QPS-01G-0100-VM 1.3.2-12 Deregistered	wifi 10.113.231.61 / fe80::20c:29ff:febb:fd03 00:0c:29:bb:fd:03	0	0/1.0 Gbps	0	0	0

You'll see the status for each appliance in the list: Paused, Sensing or Not Connected.

If the status is **Unregistered**, you can view details for the sensor and deregister.

If the status is **Sensing**, you can view details and pause the sensing.

If the status is **Deregistered**, you can view details for the sensor and delete Sensor.

Manage Sensors

You can easily manage your physical or virtual sensors from the Sensors tab.

Simply, navigate to the **Sensors** tab and from the Quick Actions menu you can perform actions like view details, deregister sensor, delete assets discovered by the sensor, delete sensor, etc.

Ó	PS-Automation Unregistered	Quick Actions 🗸	wifi -	0	0	0	0	0
H	PS-AutoPhysical Unregistered	View Details	Pune -	0	0	0	0	0
6	PS-AutoVirtual	Reboot	Pune	75	0.0 Gbps/1.0 Gbps	19%	22%	4%
	Sensing	Delete Assets	0.000					
۵	PS-Virtual_deploy QPS-01G-0100-VM 1	Deregister	wifi	0	0/1.0 Gbps	0	0	0
	Deregistered		10 M					

For more detailed information about the **Sensors** tab, refer to online help.

Assigning/Removing IP Addresses to the Appliance Sniffing Interfaces

To assign or remove the IP address from the appliance sniffing interface, go to the **Sensors** tab and from the Quick Actions menu of a sensor, click **View Details** > **Interface Settings**. Alternatively, you can click on the sensor to go directly to the sensor view details page.

Click the **edit** icon of the desired sniffing interface, as shown in the following screenshot.

← Sensor Details: PS-:	243-10G					
VEW KODE Summary General Settings Natasak Interface Settings Events	Interface Settings			pplance		8007
		Fort Active Link Up	Port in Active Link Up	Port Active Link Down	Port in Active Link Down	
	Interface Group 1					C. Update
	INTERFACE PORT	PORT STATE	(INC.12 ⁹	IP ANDRESS ())	WINE	
	10/1	Active	Down		DEFAULT	0
	15/2	Active	Up		DEMACT	0
	10/3	Active	Down		DEFAULT	0
	15/4	Active	Up		DEFAULT	Ø
	106/1	Inective	Down		DISNUS	0
	106/2	inactive	Dove		ODMUCT	0
	Interface Group 2					
	INTERFACE PORT	PORT STATE	UNKUP	IF ADDRESS 💬	NUDF	
	100/3	macSve	Down		DEFAULT	0

DEFAULT

NOX DEFAULT

Select **ERSPAN** mode and assign IP to the interface along with subnet mask.

← Sensor Details:	PS-243-10G					
VEW MODE	Interface Settings					
Summary'	interface settings		106	Anniance		LOW
General Settings						
Network						
Interface Settings				-		
Contra			16/1 16/3 15/3 16/4 186/1 196/3	100/3 100/4		
		Port Active Link Up	Port In Active Link Up	Port Active Link Down	Port in Active Link Down	
	Interface Group 1					C. Update
	INTERNACE PORT	PORT STATE	LINK UP	IP AECHESS (0)	WOR	
	16/1	Active	Down	2	DEFAULT	3 0
	10/2	Active	tap	10.20.30.40/30	ERSPAN V	Dk Genoel
					ECRANT	
	10/3	Active	Down		ERSPAN	0

Click **Ok** > Click **Update** to save the configuration. Refer to the following screenshot.

To remove the IP Address from the sniffing interface, click the edit icon of the desired sniffing interface. As shown in the above screenshot.

LINK U

Select **DEFAULT** mode, click **Ok** > Click **Update** to save the configuration. Refer to the following screenshot.

← Sensor Details: PS-	243-10G					
VEW MODE Barmery Conneal Barmery Network Interface Settings Events	Interface Settings	(100 A	pplance		ROY
		Port Active Link Up	Portie-Active Link Up	Port Active Link Down	Port In-Active Link Down	
	Interface Group 1					3 C. Updana
	INTERFACE PORT	PORT STATE	UNK (P	IF ADDRESS (C)	14036	
	16/1	Active	Down		DEHAULT 1	2 0
	16/2	Active	tāp	10.20.30.40/30	DEFAULT ~	Ok Cancel
	10/3	Active	Down		EPISPAN	0
	16/4	Active	Up		DEFAULT	0
	105/1	Inective	Down		DEHAULT	0
	109/2	Inactive	Down		DEFAULT	0
	Interface Group 2					
	NICHAGE PORT	PORT STATE	CHK (P	IF ADDRESS ©	ant) a	
	166/3	Inactive	Down		DEFAULT	0
	100/4	Active	Up		DEFAULT	0

Important:

- The Network Passive Sensor (NPS) appliance will reboot once after adding/editing/deleting the IP address of the sniffing interface.

Note: The Network Passive Sensor (NPS) appliance version 1.3.6-12 supports assigning IP addresses on the sniffing interface. So before assigning an IP address to the sniffing interface, ensure that the NPS appliance version is 1.3.6-12 or above.

Configure Assets

Network Passive Sensor can see traffic flows between two types of IP addresses. These IP addresses can be internal (within your network) or external (outside your network).

You can configure how you want to categorize your assets discovered by the sensors while monitoring traffics flow. All these assets are listed in the **Assets** tab of **Global AssetView/CyberSecurity Asset Management**.

Assets can be defined as Internal Assets, Excluded Assets, and External Assets.

Internal Assets

To add internal assets, simply go to **Configuration** > **Internal Assets** > **Add**.

Internal Assets	
Define the IP ranges within your network that you want to monitor. These IP addres	ses will be individually tracked for traffic analysis.
The passive sensor senses all the traffic that you have mirrored. However, by defini monitor and report on.	ng internal asset ranges, you choose the assets you want to
☆ Internal Asset Group/Network	
Name *	
ICS_test_group	
Include the Following Sensors	Select Sensor
1 SENSOR SELECTED	Remove All
Test_Sensor	×
Do you want to inventory the assets? (?)	
● Yes ◯ No	
Internal Asset IP Range	
Default IP Ranges	~
 ✓ 192.168.0.0/16 ✓ 173.16.0.0/12 	
 ○ 172.10.0.0/12 ○ 10.0.0.0/8 	
Туре	
DHCP V	

Here, you define the IP ranges within your network you want to monitor. The assets discovered for these IP addresses will be individually inventoried and tracked for traffic analysis. You can use default IP ranges, IP range tags, or customized IP ranges options to define range of internal assets. NPS will inventory assets for the IP ranges configured in the Internal Asset IP Range when default option under Do you want to Inventory the assets is set to **Yes**.

Select **No** if you want to just monitor the traffic flows to/from the configured IP ranges but do not want to track them in asset inventory. You can always edit the sensor configuration later to add assets for the IP ranges to the inventory if you have selected No while registering virtual sensors.

To complete the sensor setup and to start sensing assets you must define Internal Asset ranges. The passive sensor senses all the traffic that you have mirrored. However, by defining internal asset ranges, you choose the assets you want to monitor and report on.

1 - Default IP Ranges

This option defines internal assets discovered within default internal ranges for your network. Click **Select Sensors** to select sensor from the list of sensors for which you want to define internal asset.

Include the Following Sensors	Select Sensors
1 SENSOR SELECTED	Remove All
Test_Sensor	×
Do you want to inventory the assets? ⑦ ● Yes ○ No	
Internal Asset IP Range	
Default IP Ranges	\sim
 ⊘ 192.168.0.0/16 ⊘ 172.16.0.0/12 ⊘ 10.0.0.0/8 	
Type DHCP	
Cancel	

2 - IP-Range Tags

This option defines internal assets discovered with IP range tags. These are the dynamic tags created with 'IP Address In Range(s)' rule engine. Click **Select Sensors** to select sensor from the list of sensors for which you want to define internal asset.

Click **Select IP Ranges** to select IP tags from the list of tags for which you want to define internal asset.

Include the Following Sensors		Select Sensors
1 SENSOR SELECTED		Remove All
PS-Automation		×
Do you want to inventory the assets? 🧿		
● Yes ◯ No		
Internal Asset IP Range		
IP Range Tags		~
Include the Following IP Tags		Select IP Ranges
TAGS	IP RANGES	
IP_tag1	1 mar hannan hannan harran k	Х
Туре		

3- Custom IP Ranges

This option defines internal assets discovered with custom IP ranges. You can provide IP ranges for monitoring. Click **Select Sensors** to select sensor from the list of sensors for which you want to define internal asset.

Include the Following Sensors	Select Sensors
1 SENSOR SELECTED	Remove All
PS-Automation	×
Do you want to inventory the assets? (?)	
● Yes ◯ No	
Internal Asset IP Range	
Custom IP Ranges	~
IP Ranges •	
10.10.10.0/12	±
Type	

Excluded Assets

Here, you define the IP ranges or MAC addresses to be excluded from the inventory. The assets discovered for these addresses are masked as Excluded in the traffic summary.

To add excluded assets, simply go to **Configuration** > **Excluded Assets** > **Add**.

\leftarrow Excluded Assets	
	Excluded Assets Define the IP or MAC addresses to be excluded from the inventory. The assets discovered for these addresses will be masked as "Excluded" in traffic summary. Name * Asset Type * Define Type * Define Type * Enter an IP Range
	Cancel Save

Monitor External Assets

Here, you define the external sites you want to monitor. These sites are reported individually for traffic summary however these will not be inventoried like the internal assets.

To add external assets, simply go to **Configuration** > **Monitor External Assets** > **Add**.

\leftarrow External Assets	
	External Assets Define the external sites you want to monitor. These sites will be reported individually for traffic summary however, these will not be inventoried like the internal assets.
	Details • Enter an IP Address or a domain name Add
	Cancel Save

General Settings

- You can help Qualys NPS to enhance the operating system and device prediction of the asset by providing fingerprint data.

- You can set up notifications for events like Driver Change Required, Reboot Required,

and Asset Reporting Stopped to be sent to your email address.

You can see the latest events generated in the events section of the sensor details page.

← Sensor Details: NP	S_1.				
VIEW MODE					Last 2 Dave
Summary					Lust 2 Days
General Settings					
Network					1-2 of 2 🔇 🜔 🖒 🔞
Interface Settings	EVENTS	COU	INT MODUL	E TYPE	TIMESTAMP RANGE
Events	Uriver Change Required	1	AU	Moderate	07 Sep 2022 08:56 am
	Reboot Required	1	AU	Moderate	07 Sep 2022 08:52 am

Exclusion

You can exclude specific hostnames when merging unmanaged assets or merging them into managed assets.

General Configuration

Qualys NPS service utilizes the data gathered from traffic flows to predict the OS and hardware. NPS does not collect any user-specific sensitive data. It collects the protocolspecific data gathered from packet headers, which are transparently displayed to the customer in the asset's Raw Discovery Data (in the CSAM/GAV > Asset Details > System Information > View Raw Information Data section).

NPS service identifies patterns in this data to predict OS and device models. There is always a scope for improving pattern recognition to detect more OS and device models.

Once consent is given, Qualys can collect the asset's metadata and utilize it to enhance predictions of OS and device models in future releases.

Follow these steps to configure the general settings.

- Navigate to Configuration > General Settings > General configuration.

- To give consent to Qualys to access the metadata, toggle Access to Fingerprint Data to allow access.

Go to the Recipients text box and add the e-mail. You can add multiple e-mails using comma separated.

Click Save.

Once you add the recipients, they receive the events in their e-mail inbox.

Network Passive Sensor	V HOME SENSORS CONFIGURATION
Configuration	Internal Assets Excluded Assets Monitor External Assets General Settings
	General Configuration
General Configuration	Access to Fingerprint Data Allow Qualys to collect asset fingerprint data By enabling this option you permit Qualys to collect fingerprints of assets. This will help improve Operating System and Device prediction of the assets. Please note that fingerprints do not include any sensitive data. They consist of metadata related to the assets, which can be viewed in the CSAM/QAV > Asset Details > System Information -> View Raw Information exciton.
	Mail ID Recipients ① Add recipients to receive email notifications for specific events Recipients
	Separate emails using commas () between addresses
	Save

Exclusion

You can configure hostnames that need to be excluded while merging unmanaged assets or merging unmanaged assets into managed assets.

The hostnames provided here are case-insensitive. When a new hostname is added to the exclusion list, make sure first to purge the asset created for that hostname. Refer the following screenshot for configuring excluded hostnames.

Also, you can configure hostnames that need to be excluded while de-duplicating unmanaged assets or de-duplicating unmanaged assets into managed assets. The hostnames provided here are case-insensitive. When a new hostname is added to the exclusion list, make sure first to purge the asset created for that hostname. Refer to the following screenshot for configuring excluded hostnames.

Network Passive Sensor	V HOME SENSORS CONFIGURATION	DN
Configuration	Internal Assets Excluded Assets Monitor External Assets General Settings	
General Configuration	Exclusions	
Exclusion	Configure names that Qualys should exclude from hostname based asset de-duplication	
	Add Hostnames ()	
	Enter Hostname	Add
	Clear Selection Remove Selected	Q
	hostnames	
	ASD	$\mathrel{\oslash} \times$
	QWE	\diamond ×
	example	\diamond \times
	Save	

Note: Contact Qualys Customer Support to get them deleted to avoid deduplication in the future.

Network Configurations

You'll need to complete certain network configuration settings under Set up Network. This is where you'll enable and configure the management interface of the appliance.

These configurations are described:

Configure Static IP Address

Proxy Configuration

Configure Static IP Address

If the core group to which Management interface is connected has DHCP server, then you can view the Management Network Configurations with **Show** option. If DHCP is not on your network, you must enable the Virtual Sensor with a static IP address using the **STATIC IP** option. One of these configurations is required.

To enable a static IP address, follow these steps:

1) Go to the **Set up Network** menu option and press **Enter** to continue.

2) Press Space Bar to select Static IP option and choose OK.

3) Provide parameters for Static IP configuration:

- IP address - Enter the static IP address.

- **Netmask** Enter the desired netmask value.
- Gateway Enter the gateway IP address.

- DNS1 - Enter the IP address for the primary DNS server.

- DNS2 - Enter the IP address for the secondary DNS server. This entry is optional.

4) Choose **Submit** and press **Enter**. Wait for some time and you'll see a confirmation message for successful configuration of network settings.

Proxy Configuration

If the Virtual Sensor is behind a Proxy server, you need to enable a Proxy configuration using the **Enable Proxy** menu option. Authentication (Basic) of the Virtual Sensor connection to your Proxy server can be enabled by configuring the Proxy user and password fields.

The Virtual Sensor uses Secure Sockets Layer (SSL) protocol (HTTPS) to secure its connection to the Qualys web application, in a similar way that a web browser does to a secure web server. If the Qualys connection must pass through a Proxy server, then you must enable the Proxy option on the Virtual Sensor. This configuration re-directs Qualys outbound connections through the Proxy server.

Your Proxy server must be configured to tunnel or pass through the SSL session to the Qualys web application. This ensures a secured end-to-end connection. SSL bridging or tunnel termination must not be configured in your Proxy server when supporting the Virtual Sensor.

To configure Proxy support, follow these steps:

- 1) Go to the **Set up Network** menu option.
- 2) Choose Proxy Configuration and press Enter to continue.
- 3) Select Enable Proxy and click OK.

4) When the **Enter the proxy server details** prompt appears, provide the proxy server parameters:

- Proxy IP Address - Enter the Proxy server's IP address.

- Proxy Port - Enter the port number assigned to the Proxy server.

5) Click **Next** to select the authentication type from **NoAuth**, **BasicAuth** and **NTLMAuth**. If you select authentication type as **BasicAuth** or **NTLMAuth**, you need to provide user name and password.

- **Proxy User** - Enter the user name for Proxy authentication. If authentication is not enabled at the Proxy level, leave the entry field blank.

- **Proxy Password** - Enter the password for Proxy authentication. If authentication is not enabled at the Proxy level, leave the entry field blank.

Appendix

Virtual Network Passive Sensor (PS) Appliance Packet Throughput Based on Resources

The Virtual Network Passive Sensor (PS) appliances auto-scaling capability starts automatically at the boot time to calculate how much packet throughput it can handle.

The delta increase in the throughput depends on the additional dedicated resources made available to the appliance. The resources include the CPU clock, the type of CPU, and the type of RAM in the VM appliance system.

To handle continuous traffic, the CPU GHz must be allocated in a dedicated manner. The estimated maximum throughput is visible on the sensor details page. The throughput may vary depending on the dedicated nature of the resources and the type of traffic visible to the sensor.

Virtual Network Passive Sensor (PS) Throughput Capacity Based on Hardware

The throughput of the VM appliance is directly dependent on the CPU resources allocated to the VM. In addition, it is strongly advised to increase memory as well. Use the following comparison chart as a guideline for resource allocation for the desired throughput.

Comparison Chart

The throughput is dependent on multiple factors, such as

a) The composition of the data fed to sniffing interface: Example number of flows in the traffic, few flows having heavy traffic volume as compared to the rest, the constitution of application data within a flow, etc.

b) Resources allocated to the VM: number of CPU cores, frequency of the CPU core, and the type of memory.

The following is the throughput as measured in the Qualys lab on hardware with the following specifications and with reasonable well-conditioned test data.

Hardware Specifications:

CPU core: Intel(R) Xeon(R) CPU @ 2.30GHz

RAM: RAM DDR4 2133

Virtualization Platform: VMware ESXi 6.7.0

Capacity (MBps)	RAM (GB)	CPU Core
500	8	4
750	12	6
1000	16	8
1250	18	10
1500	20	12
1750	22	14
2000	24	16

Notes :

- For the desired throughput above 1000Mbps, Qualys strongly advises to add 4 GB RAM (if not possible, a minimum of 2 GB RAM) with every addition of 2 CPU cores to ensure smooth functionality of PS appliances.

- The throughput achieved with a single core by varying the CPU core frequency were as: 150 MBps (CPU core frequency < 1.5 GHz), 200 MBps (1.5 GHz > CPU core frequency > 2 GHz), and 250 Mbps (CPU core frequency > 2 GHz).

How to Modify Hardware Resources for VM Deployed on the ESXi Server

1. Go to **System Shutdown** option and press **Enter** to shutdown the appliance via console.



2. Click **Edit**.

3. Increase the **CPU** cores and **Memory** as per your throughput requirements and click **Save** to save your configuration.

4. Click **Power ON** to start your appliance.

							Q Search
Navigator	B PS_Demo						
Host	Conside III Monitor I Prove	non Bouwer off 11 Surround		sh 🗌 🙃 Actions			
Manage	Secondar Emonal 1 5 1 010	PS Demo		an 1 M Honora			
Monitor		Guest OS Red Hat E	interprise Linux 7 (64-bit)				0 MHz
and the second sec		VMware Tools No	xi 6.0 and later (VM version 11)		han		MEMORY NEED
		CPUs 8 Memory 16	68				0 B
the state of the s					1.1.1		STORAGE
		-			MM_r		2.15 66
	VMware Tools is not installed in	this virtual machine. VMware Tool	is allows detailed guest information	to be displayed as well as allo	wing you to perform operations on th	e quest OS, e.g.	araceful ×
the second se	shutdown, reboot, etc. You sho	uld install VMware Tools. 🏠 Actio	ons				
Access (E)							
-	- General Information			* Hardware Configuration			
	Networking	No network information	A Antina		B VCPUs		
	Init VMware Tools	Not installed	Actions	Memory	16 08		
	Notes	QualysGuard(R) Virtual Passive S	icapper / Edit poter	IN Network adapter 1	VM Network (Connected)		
	and the second se		Controlog				
	ID PS Demo						
	Conscier Monade Dewer	on Terrer of Terrerio 6	🕼 Reset 🕴 🥒 Edit 🕴 🙋 Refresh	Actions			
	🔂 Edit settings -	PS_Demo (ESXi 6.0 virtual machine	e)				
							0 MHz
	Virtual Hardwar	e VM Options			N N		
	Add hard d	sk 🛤 Add network adapter 🛛 🚍 A	Add other device				0 B
	• 🖬 CPU 🇥		0			<u> </u>	
		0 ·	U				2.15 GB
	Memory	16384	MB 🔻				
	Low and Low and						
	shutdown, rec	50	GB 🔻		n operations on the guildent of the guilden		
	SCSI Cor	troller 0	Parallel				
	(manual states)						
	General Informa > MI Network	Adapter 1 VM Netwo	ork	 Connect 	0		
	Networking	Manter 2			18		
	Whyare Tools	tcp_repla	ıy_controller	Connect	0		
	 Storage Video Ca 	rd Specify c	ustom settings	•			
	Notes				vork (Connected)		
	And the other design of the second						
	Recent tasks						
	Recent tasks						ompietea • •
	Task Update Child Resource Cord				replated successfully	~ 0	5/12/2021 14:53:36
	Task Task Updas Child Resource Cont Peaver On VM			Save	Cancel moleted successfully	~ C 0 0	8/12/2021 14:53:36 8/12/2021 14:53:18
	Recent tasks Task Update Child Resource Cont Perver On VM Records VM	B PS_Dane	Root 06/12/2021 14	Save 08/12/20271 - 51 13	Cancel moleted successfully moleted successfully Completed successfully	~ C 0 0 0	0000000000 0 0 0 0 0 0 0 0 0 0 0 0 0 0
	Recent tasks Task Update Child Resource Corl Power Co VM Records VM	B PS_Dane	root @8122021144	06/12/02/11/4/53:13	Cancel moleceastical processing of the successing of the successin	~ 0 0 0	01122021 14 53 36 8122021 14 53 16 8122021 14 53 18
	II. Recent tasks Task Dpdat OMR Resource Cont Perior Co VII Records VII	2 Po Dente	root @0122021144	Save (h) 06/12/02/10/06/13	Cancel moleceastury moleceastury completed accessfully	~ C 0 0	ompeted * 5 9/12/2021 14:53:35 9/12/2021 14:53:18 9/12/2021 14:53:13
ware: ESXI"	Recent tasks Task Update Child Records Cont Records VM	2 10 feet	reel 00122021141	Spre 	Cancel modeled successfully modeled successfully completed successfully	- C 0 0 0	Compared V V 12/2021 14/53 36 512/2021 14/53 15 b12/2021 14/53 13 Q Search
ware [,] ESXi [*]	Recent tasks Task Dak Da	B Hijbew	.0014202114	Sine Sine Is	Cancel poster accessfully Cancel poster accessfully Compared accessfully	- C 0 0	Q Search
Ware: ESXI Virtual machine PS_Demo was s	Recent tasks Task	B SJan	.eet161232114	513 SOLOUTINSIS	ngeneratury manufactures and accessfully Completed accessfully	- C 0 0 1 1 1 1 1 1 1 1 1 1	0 mppela 1 0 11/2/22/14/53/6 11/2/22/14/53/16 11/2/22/14/53/13 Q. Search
Ware ESXI [®] Virtual machine P5_Demo was su Hoss	Construction C	0 10 Dawn	vei studdi 14	Actions	ngelet ausseaduly mgelet ausseaduly gelet ausseaduly dispond successful	~ 0 0 1 1 Help ~ 1	omposed * 0 5122021 1453 15 5122021 1453 15 3122021 1453 13 9 9 Search x
Ware: ESXI" Virtual machine PS_Demo was su Vess Manage	Recent task Task	an Power of Powerson Powerson Powerson the visual machine	ner entstatt för	Street Actions	Cancel - myself accessibly myself accessibly	~ 0 0 0	omposed * • • • • • • • • • • • • • • • • • •
Worke' ESXI' Vintual machine PS_Demo was su ji lest Manage Montar	Recent tasks Task Task Task Dala Manara (Ser Task Dala) Recently Vite Configured - domes.	on Disease of Disease of Posterior of Posterior of Disease of Dise	veit 0012021114 Q Resett ✓ Edst ♥ Refeat keptine Linux 7 (64:00)	s u second det	patient aussessiuly patient aussessiuly mathef aussessiuly admentiate aussessiuly	~ 0 0 1 Help + 1 1	omposed * • • • • • • • • • • • • • • • • • •
Ware' ESXI' Vintui mashine PS_Demo was su Vintui mashine PS_Demo was su Manage Monaor	Construction Cons	a) II Poer of II Sussed Poer of the Vital Institute Over 0 By Restrict Computing Exc	See Line () € Edst € Refeat Septie Line 7 (64 a) Line 7 (64 a)	Actions	Cancel Market Accessive	- 0 0 1 Help - 1 1	CPU
Ware' ESXi" Virtual machine PS_Demo was su Host Manage Montor	Prevent task Tok Uptin BoldMoncers Cur Records UN Records Record	Constant and the Statement	Net USID227144	sto sepont ett	Annell Annell Annell Annell Annell Annell Annell Annell	- 0 0 1 1 Help - 1 0	C Search C Search C Search C MHz UNIX 1443 13 C Search C Search
WBICE ESXI" Virtual machine PS_Demo was su Host Monaor	Construction C	or Prover of Subjects Power on the visual machine Generating Competition National Competition National Chara B Memory 16 G	ver en bland i Ar Q Reset ✓ Eds. € Refesi Herging Line 7 (64.6) i.6.9 ard later (Mi verson 11) 16	a transministration	Company accountly Company accountly Company accountly Company accountly	- 0 0 1 1 Help - 1 1	Q, Search CPU 2013 H4 53 H P120201 H4 53 H P120201 H4 53 H P120201 H4 53 H CPU 2013 H4 53 H K CPU 2013 H4 53 H K CPU 2013 H4 54 H K CPU 2013 H CPU 2013 H
Ware: ESXi" Virtual machine PS_Demo was su Hest Manage Montor	Recent task Task Task Task Task Task Task Task T	an a Power of a Support Power on the visual machine Course of the visual machine Course of a set relation Visuale Tools No Comparison No Compa	Rest (✓ Edt) C Reheat Perset (✓ Edt) C Reheat herpite Lnux 7 (64 at) 6.0 and ther (M version 11)	stu Sport Seturat Arto I Actore	Cancel Manual Annual Annua	- C 1 0 0 0	CPU CALL CPU CA
Warter ESX1" Virtual machine P5_Demo was su Host Montor	Recent table Tak Tak Tak Tak Chall Back of the Annual Processfully reconfigured downs.	All Characterial Annovation of the Statement Annovation of the visual machine Competitive Competitive Competitive Competitive Competitive Competitive Statement Statement Statement	ent et al Mariel Me Parter V Edit et al Parter Reprise Lines 7 (6-64) 6.0 and later (M. version 11) 6.0	Actions	Annell Annell Annell Annell Annell Annell	- C 0 0 1 1 1 Help - 1 1	Q, Search Q, Search O, MHz O, MHz O, MHz S, Search CPU O, MHz CPU CPU CPU CPU CPU CPU CPU CPU CPU CPU
Mare' ESXI' Vintui machine PS_Demo waa su Host Montor	Recent table Taol Taol Taol Taol Taol Taol Taol Taol	or Power of Powerson Power on the visual muchine Over on the visual muchine Over 05 Res Hat Ex Vehane Stock No Congression No	net et blact t ki Q Reset [✔ Edt] € Refusi leptite Linux 7 (64-86) S de letter (Mi version 11) 8	a u Seriever her u	Cancer Make Accessive	 C B B	Q Search Q Search x C 0 MHz x C 0 MHz x C x
Ware: ESX;" Virtual machine PS_Demo was su Manage Montor	Resert task Tex T	an and the second	Image: Section 1 Image: Section 2 Image: Section 2 Image: Section 2	ST Strong	Cancel Partial accessibly myskel accessibly Cancel Partial accessibly Cancel Cancel Partial accessibly Cancel Cance	- C 8 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	Q Search Q Search C Sear
Warter ESXI [®] Vintual machine PS_Demo was su Nost Montor	State Output Level by Under Patient Score If at room If the house a sage it Wit followsh (Construint) State If at room If a	Opposed					
Ware' ESXI' Virtual machine PS_Demo was su Manage Montor	Resert task Tok Tok Tok Tok Tok Tok Tok Tok Tok To	Arian Statement Arian Statement Arian Statement Areas Statement Areas Areas Areas Areas Areas Areas Areas Areas	Rest:	a u Spre	Cancel Market accessed Market accessed Compared accessed	- C 0 0 0 1 1 1 1 2 2 2 2 2 2 2 2 2 2 2 2 2	Opplexed * Standard 14 45 39 Standard 14 45 39 Standard 14 45 39 Standard 14 45 39 O, Search O, MHz USUBONY Standard 14 45 39 O, MHz Standard 14 45 39
Warter ESXI [®] Virtual machine PS_Demo was su Hest Manage Monitor		Power of B Magazat Constant of B Magazat Constant of B Magazat Constant of B Magazat Constant of B Magazat Magazat Magazat Magazat Magazat Magazat Magazat	ent allows dealled guest information to s	a ta se traver la dese e displayed as well as allow + Mardware Configuration	Compared Automaticly Compared Automaticly Compared Automaticly In a second s	- C - 0 - 0 - 0 - 0 - 0 - 0 - 0 - 0	Opposed 1 45.35 Statuti 14.53 55.35 Statuti 14.53 55.35 O MH12 0 O MH12 0 Usebory 10 Statuti 14.53 10 O MH12 1 Usebory 10 2,15 06 cetu K
Ware' ESXI' Virtual machine PS_Demo was to Host Montor Nontor	Constant table Tool T	Ar a James Ar a James at a James a	net (Briddet 14) (Constant of the second o	a u Sectors	Cancel Masked Jackson J.	- (() 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Q. Sharch Q. Sharch C.PU 0.MHz 0.BHZ 0.BHZ 0.
Ware' ESXI Vitual machine PS_Dence was su I test Montor Montor		an an anna an anna an an an an an an	ont (■ 14401 M Press ✓ Edt @ Release Reprise Lines 7 (6-64) 8.8 and terr (M version 11) 8 allows detailed guest information 1 9 C Actions	Actions Actions Hardware Configuration Hardware Configuration Monory	Cancel Partial accessibly madel accessibly water accessibly Carpoint accessibly the partial accessible	- C (0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	00000001 H4 53 90 9702021 H4 53 93 9702021 H4 53 93 90020221 H4 53 93 90 Search × 0 MHz ■ ULLORY ¥ 3109A0E 2.15 GB eeful ×
Ware' ESXi' Vitual machine PS_Demo was us Host Montor	Constant lask Tex Tex Tex Tex Tex Tex Tex Te	A Constant of the Subsection of the Volume Handwork of the Subsection of the Volume Handwork of the Subsection of the Volume Handwork of the Subsection	Antimeter Actions	a ta se tanto her ta a ta se tanto her ta Actions • displayed as well as allow • Hardware Configuration • Hardware Configuration • Hardware Configuration • Hardware Configuration	Cancel Make Jaccastly Corpored Jaccastly Corpored Jaccastly Corpored Jaccastly Sources Sources Sources Sources Sources Sources Sources	- C 0 0 0 1 1 2 2 2 2 2 0 0 0 0 0 0 0 0 0 0	Q. Search Criv C. Search C. Sea
Ware' ESXI' Virtual machine PS_Demo was su Nanape Mantar	Beart task Tax Ta	An and a second se	Image: Control of the second secon	a u Section the section of the secti	B VCPUs B VCPUs B VCPUs UN Network (Connected)	- (()) () () () () () () () (onguezes * • • • • • • • • • • • • • • • • • •
Ware ESXI Virtual machine PS_Damo was a Intest Manage Montor		Present of Statement Comparison Compar	(a) March M (a) Rest Cat (b) Rest Cat (c) Rest (c) Reheat (c) Rehat (c) Reheat (c) Rehat (c) Reheat (c) Rehat (c) Rehat (c) Rehat (c) Rehat <	Actions	B VCPUs B VCPUs B VCPUs UN Network (Connected)	- () -	Q, Search Q, Search Q, Search CHU UNLYZ 2,15 GB Ceful X Ceful X X X
Ware ESXI Virtual machine PS_Demo was su Manage Monitor	Revert table	An and Power of a Conception An and a conception of the visual machine Normation Normation Normation Added	Not Statute 1 M Image: Statute of Statute	Contract better	Compared accession Provide accession Compared accession	- (()) () () () () () () () (Opplement K Opplement K Standard K Opplement K
Ware ESXI Virtual machine PS_Demo was su Hest Manage Monor	Constitution Record table Tex Tex Tex Tex Tex Tex Tex T	An and a second se	ent (Bilder) M Prest (Cat (Prest) 16 Prest (Cat (Prest) 16 Prest (Cat (Prest) 16 Prest (Prest) 16 Prest) 16 Prest)	Actions	Comment Secondly Comment Secondly Comment Secondly Sec	- C C C C C C C C C C C C C C C C C C C	Opposed 1 45 30 D020211 44 53 30 3000000000000000000000000000000000000
Watre ESXI Virtual machine PS_Demo was su Henst Mondor	Record table	Ar a James Ar a James and a Jame	Not Balance 144 Image: Preser Edit Image: Preser Image: Preser Edit Image: Preser Image: Preser Edit Preser	Actions	Cancel Make Jaccasely Corpored Jaccasely C	- (1965 -) (Q. Search Q. Search C.FU 0.H.FU 0.B.R 310AGA 310AGA 310AGA 140
Watre: ESXi Vitual machine PS_Dence was su from Manage Monter	Construction C	Ar an endown formation Ar and a statement Ar and a stat	Image: Control of the second secon	Actions Actions Hardware Configuration Hardware Sontiguration Hardware Sontiguration Hardware Sontiguration Hardware Sontiguration Hardware Sontiguration Monony	Concell Provided accessed of maked accessed of maked accessed of respective acces	- (C 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	ongenerati strandingenerations on

How to Modify Hardware Resources for VM Deployed on the HyperV Server

1. Follow Step 1 same as mentioned above.

2. Select the virtual machine and go to **Settings**. Modify the **CPU** cores and **Memory** as per your throughput requirements > Click **Apply** to apply the changes > Click **OK** to save your configuration.

ps.	_demo	~	4 > 0	
*	Hardware	^	Processor	
	Add Hardware BIOS Boot from CD		You can modify the number of virtual processors based on the number of processor the physical computer. You can also modify other resource control settings.	rs on
	Security Key Storage Drive disabled		Number of virtual processors: 16 🜩	
	Memory		Resource control	
	8192 MB		You can use resource controls to balance resources among virtual machines.	
Ξ	Processor 16 Virtual processors		Virtual machine reserve (percentage): 0	
	Compatibility		Percent of total system resources: 0	
Ξ	IDE Controller 0		Virtual machine limit (percentage): 100	
	Hard Drive		Percent of total system resources: 80	
-	IDE Controller 1		Relative weight:	
	DVD Drive		Reduct negre	
	SCSI Controller			
ŧ	Network Adapter mgmt			
+	Network Adapter test_switch			
	COM 1 None			
	COM 2 None	1		
	Diskette Drive			
*	Management			
	Name ps_demo			
	Integration Services	~		



3. Power ON the VM.

Adding/Removing Sniffing Interfaces from Virtual Appliance

Network Passive Sensor (PS) now supports an aggregated/bonded sniffing interface. A virtual interface aggregates multiple physical interfaces allow the appliance to add one or more sniffing interfaces.

How to Add Sniffing Interface to the PS Appliance Deployed on the ESXi Server

1. Go to the **System Shutdown** option and press **Enter** to shutdown the appliance via console.



2. Click **Edit**

10 m m m	Memory	8 16 GB	-		MEMORY 0 B STORAGE 2 15 GB
• Gene	vare Tools is not installed in this virtual machin down, reboot, etc. You should install VMware 1 ral Information brocking No network inform	n. VNIware Tools allows detailed guest information Tools. 🎲 Actions	Hardware Configuration GPU	g you to perform operations on the guest OS	S, e.g. graceful ×
> (in Vi	tware Tools Not installed	Actions	Memory .	16 GB	
• 🗐 Str	orage 1 disk	-	Hard disk 1	50 GB	
C No	tes QualysGuard(R)	Virtual Passive Scanner / Edit notes	IN Network adapter 1	VM Network (Connected)	

						Q Search
PS_Demo						
	tor Power on Power off	19 Suspend 👩 Reset 🚺 Z Edit 🗋 📿 Refre	sh 🕹 Actions			
	Edit settings - PS_Demo (ESXi 6.0	0 virtual machine)		_		
						0 MHz
1	Virtual Hardware VM Options					MEMORY WERE
	Add hard disk ME Add network	k adapter Add other device				0 B
	• 🖬 CPU 🧘	Add a network adapter to the virtual machine				STORAGE
	• 🛲 Memory 🛕	16384 MB *				2.15 GB
VMware Tools shutdown ret	+ 🔜 Hard disk 1 🛕	50 GB •		0	n operations on the guest OS, e.g.	graceful 🙁
	SCSI Controller 0	LSI Logic Parallel		0		
- General Informa	IN Network Adapter 1	VM Network	▼ Z Connect	0		
Willware Tools	INIE Network Adapter 2	tcp_replay_controller	▼ Z Connect	0		
• 🗐 Storage	• 🕎 Video Card	Specify custom settings	•			
Notes:					vork (Connected)	
Recent tasks						
Task					•	Completed *
Update Child Resource Confi-			Cau	Canad	bieled successfully	08/10/2021 11:54:39

3. Click **Add Network Adapter** for adding new sniffing interface.

4. Select appropriate port group > Select the adapter type ${\bf VMXNET}~{\bf 3}$ > Click ${\bf Save}$ to save your configuration.

						Search
PS_Demo						
90 N 80	ace 📙 🕨 Power on 🔳 Power off	😝 Suspendi 😰 Reset 🥒 Edit 💆 R	efresh 📗 🏠 Actions			
	Edit settings - PS_Demo (ESXi 6	.0 virtual machine)				CPU PT
	Memory 🛕	16384 MB *				0 MHz
	• 🖾 Hard disk 1 🛕	50 GB ¥		0		MEMORY ALE
	SCSI Controller 0	LSI Logic Parallel	×	0		STORAGE
	RM Network Adapter 1	VM Network	• Connect	0	CONTRACTOR OF CONTRACTOR	
William VMware Tools shutdown, ret	INI Network Adapter 2	tcp_replay_controller	🔹 🗹 Connect	0	n operations on the guest OS, e.g. gracel	
Concernance of	• Mil New Network Adapter	tcp_replay_controller_2	•	0		
General Informa	Status	Connect at power on				
VIAware Tools	Adapter Type	VMXNET 3	•			
Notes	MAC Address	Automatic • 00.00:00:00:00.00			vark (Connected)	
Recent tasks	Video Card	Specify custom settions	•			
Task		opecity custom setungs			v ⊂ Com	pleted *
Update Child Resource Confi					plefed auccessfully 08/10/	2021 11:54 39
Power On VM			(all a	e Cancel	sketed auccessfully 08/10/	2021 11:54 12
Power On VM	TO PO UND	1000 US 19770	1113723	25	uprofileted successfully 08/10/	

5. **Power on** the VM.

How to Remove Sniffing Interface to the PS Appliance Deployed on the ESXi Server

- 1. Follow the Step 1 and Step 2 same as mentioned above.
- 2. Remove the newly added interface and click **Save** to save the configuration.

vmware ESXi						Help + Q Search	*
or Management	PS_Demo						
-	Gonsole: Et Monit	or Power on Bower of	IN Suspend @ Restart / Edt C	Refresh 🛟 Actions			
	6	Edit settings - PS_Demo (ESXi 6.0	0 virtual machine)		_	CPU	
and succession of the		Virtual Hardware VM Options				0 MHz	
E 5.86		Add hard disk 🛤 Add network	k adapter 🛛 昌 Add other device			0 B	MR
and a		• 🖬 CPU 🛕	10 🔻 📵			STORAGE 2.15 GB	8
		• 🎟 Memory 🔔	16384 MB ¥				
and the second division of the second divisio	VMware Tools shutdown, ret	+ 🖾 Hard disk 1 🛕	50 GB •		0	n operations on the guest OS, e.g. graceful	
Anna R	- General Informa	SCSI Controller 0	LSI Logic Parallel	•	0		
A REAL PROPERTY.	• Q Networking	Retwork Adapter 1	VM Network	 Connect 	0	ls	
Second Second	Whware Tools	Retwork Adapter 2	tcp_replay_controller	🔹 🗹 Connect	0		
	Notes	Retwork Adapter 3	tcp_replay_controller_2	🗸 🗹 Connect	g.	work (Connected)	
	Recent tasks	Video Card	Specify custom settings	•	~		10
	Task					Completed	
				Save	Cancel		
		_	_			,	

3. **Power on** the VM.

How to add Sniffing Interface to the PS Appliance Deployed on the HyperV Server

1. Go to the **System Shutdown** option and press **Enter** to shutdown the appliance via console.



Note: A virtual switch that views the mirrored network traffic should be connected to the newly created interface.

Click here to follow steps 10 to 20 in the Deployment on Microsoft Hyper-V section to create a virtual switch and add a new sniffing interface to it.

How to Remove Sniffing Interface to the PS Appliance Deployed on the HyperV Server

1. Go to the **System Shutdown** option and press **Enter** to shutdown the appliance via console.



2. Select the virtual machine and go to **Settings** > Select the Network Adapter tab that needs to be removed > Click **Remove** > Click **Apply** > Click **OK** to remove the network adapter.

s_demo	~	< ►				
Hardware Add Hardware BIOS Boot from CD	^	Network Adapter Specify the configuration of the Virtual switch:	network adapt	er or remove the ne	twork ada	pter.
Security		new_sniff_switch			~	
Memory 8192 MB		VLAN ID	ication			
8 Virtual processors		The VLAN identifier specifies	the virtual LAN	that this virtual mac	hine will us	e for all
IDE Controller 0 Hard Drive aPS-1.3.0-7-open-disk	1.vhdx	2	ugn this networ	K adapter :		
IDE Controller 1	45 11 100	Bandwidth Management				
DVD Drive None		Enable bandwidth manag	ement			
SCSI Controller		Specify how this network ada Bandwidth and Maximum Ban	pter utilizes net dwidth are mea	work bandwidth. Be sured in Megabits p	oth Minimur er second.	n
Network Adapter mgmt		Minimum bandwidth:	0	Mbps		
Network Adapter		Maximum bandwidth:	0	Mbps		
Network Adapter new_sniff_switch		To leave the minimum or	maximum unre	stricted, specify 0 a	s the value	2.
COM 1		To remove the network adapter	from this virtua	al machine, click Ren	nove.	
COM 2					-	Reirove
None Diskette Drive None Management		Use a legacy network adap network-based installation services are not installed in	ter instead of t of the guest op the guest oper	his network adapter erating system or w ating system.	r to perforr /hen integr	n a ation
Name ps_demo Integration Services						

ps_demo	~	4 Þ Ö			
* Hardware	^	Network Adapter			
Add Hardware		Canality they can fin unit on a films	makenally adapt	as as compute they work as	la malambas
BIOS		Speary the configuration of the	network adapt	er or remove the networ	K adapter .
Security		new criff cwitch			
Key Storage Drive disabled		inen_ann_ameri			
Memory		VLAN ID			
8192 MB		Enable virtual LAN Identiti	ication		
Processor S Virtual processors		The VLAN identifier specifies t	the virtual LAN	that this virtual machine	will use for a
E IDE Controller 0		network communications thro	ugh this netwo	rk adapter.	
Hard Drive		2			
qPS-1.3.0-7-open-disk1.vh	dx				
E IDE Controller 1		Bandwidth Management			
OVD Drive		Enable bandwidth manag	ement		
None SCSI Controller		Specify how this network ada	pter utilizes ne	twork bandwidth. Both M	linimum
Network Adapter		Bandwidth and Maximum Ban	dwidth are mea	sured in Megabits per se	cond.
mgmt		Minimum bandwidth:	0	Mbps	
🖭 📮 Network Adapter		Maximum handwidth-	0	Mhose	
test_switch		Maximum parlowidory.		Mups	
Wetwork Adapter		To leave the minimum or	maximum unre	stricted, specify 0 as the	value.
COM 1		To remove the network adapter	from this with the	d machina click Damaua	
None		To remove the memory daupter	in carrie and an eas	a machine, clourenove	and the second s
COM 2					Remov
None		Use a legacy network adap	iter instead of t	his network adapter to p	erform a
None		network-based installation services are not installed in	of the guest operation	erating system or when	integration
* Management	L	and there are they introduce in	are guest ope	ideng system.	
I Name					
ps_demo					
The second state of the se					

Classification of Assets in Passive Sensor

Passive sensor classifies IPs as internal and external for the purpose of asset inventory and traffic monitoring.

The area labelled "Internal" in the diagram below is the universe of IP ranges that exists within an enterprise and therefore worth building an asset inventory. Everything outside this range is "External" and not worth inventorying.

From a traffic monitoring perspective, PS tracks flows between assets in the inventoried IP range by 4-tuple. PS does not track individual IPs in the "External" range and attributes all external IPs to a single asset named "External".



Following is a detailed explanation of how PS treats each class of IPs.

What is Inventory

PS uses IP addresses in this range to

a) Create assets and inventory various asset attributes such as hostname, MAC address, protocol specific attributes, etc.

b) Track traffic flows to/from these IPs to other all other IPs outside this range.

Assets with IPs in this range are listed under the CSAM inventory.

PS aggregates the traffic flows from an IP in the internal range to another IP in the internal range by 4-tuple of Source IP, Destination IP, Destination port, and TCP or UCP protocol. Appliance reports traffic flows at an interval of 5 minutes for new assets and at 30 minutes for asset updates.

The appliance aggregates multiple flows of the same tuple into one flow when reporting it in the 5 or 30-minutes reporting interval.

For example, if Asset A1 initiated HTTP flow to a webserver A2 multiple times within the 30 minutes interval, PS aggregates these flows and reports a single HTTP flow from A1 to A2 at reporting time.

How to Configure Inventoried IP Range

To configure an IP range/subnet as internal inventoried, select the appliance from the Passive Sensor Module listing and navigate to its details to edit the internal asset configuration. Here add the IP range and set the radio button under "Do you want to inventory these assets?" to Yes.

\leftarrow Internal Ass	iets	
	Internal Ascets	
	Define the IP ranges within your network that you want to monitor. These IP addresses will be individually tracked for traffic analy	sis.
	The passive sensor senses all the traffic that you have mirrored. However, by defining internal asset ranges, you choose the asset monitor and report on.	s you want to
	Internal Asset Group/Network	
	Name *	
	Subnet-A	
	Include the Following Sensors	Select Sensors
	1 SENSOR SELECTED	Remove All
	NPS-A	×
	Do you want to inventory the assets? (?) (Yes No	
	Internal Asset IP Range	
	Custom IP Ranges	\sim
	IP Ranges •	
	10.10.0/24	±
	Type DHCP V	
	Cancel Save	

What is Non-Inventory

PS uses IP addresses in this range only for tracking traffic flows to other IPs in the inventory range and NOT for inventory purpose. Assets in this IP range do not show in the CSAM inventory. However, traffic flows to/from these assets are listed in the Network tab of CSAM and under the inventoried asset-centric traffic tab of CSAM.

How to Configure Non-Inventoried IP Ranges

To configure an IP range/subnet as internal non-inventoried, select the appliance from the Passive Sensor Module listing and navigate to its details to edit the internal asset configuration. Here add the IP range and set the radio button under "Do you want to inventory these assets?" to No.

Internal Assets	
Define the IP ranges within your network that you want to monitor. These IP addresses wi	II be individually tracked for traffic analysis.
The passive sensor senses all the traffic that you have mirrored. However, by defining inte monitor and report on.	ernal asset ranges, you choose the assets you want to
Reference internal Asset Group/Network	
Name •	
Subnet-B	
Include the Following Sensors	Select Sensors
1 SENSOR SELECTED	Remove All
NPS-A	×
Do you want to inventory the assets? ⑦ ○ Yes ● No	
Internal Asset IP Range	
Custom IP Ranges	~
IP Ranges *	
10.20.20.0/24	+
Type DHCP	
Cancel Save	

To review the configuration, check the last column "Inventoried"

Configuration Internal Assets Excluded	Assets Monitor External Assets General Settings		
Actions (0) V Add			1 - 13 of 13 🔇 🕑 💍 🔅
NAME	IP RANGE	SENSOR	TYPE INVENTORIED
Subnet-A	1(NPS-B	DHCP No
Subnet-A	1(- NPS-A	DHCP Yes
Subnet-B	10.000.000000	NPS-A	DHCP No
Subnet-B	11	NPS-B	DHCP Yes

What is Excluded

If there is a need to not see some sensitive or confidential assets listed in the inventory, then the passive sensor allows the user to specify configuring IPs and/or MACs in the Excluded range.

PS excludes gathering all inventory information of the IPs/MACs added in this category/group. These assets do not show in the CSAM asset listing. In the traffic flows to/from these assets as seen in the traffic listing, the asset is seen as Excluded without any IP-address.

How to Configure Excluded IPs/MACs

To configure an IP / MAC as excluded, select the appliance from the Passive Sensor Module listing and navigate to its details to edit the Excluded Assets configuration.

Netwo	ork Passive Sensor	~				
Соп	figuration	internal Assets	Excluded Assets	Monitor External Assets	General Settings	
	Actions (0) 🗸	Add				
	NAME				TYPE	IP RANGE
	exclude-test-dns				IP	10.1
	test-exclude				IP	10.1

Traffic summary representation for Excluded Assets:

curl 7 29 0	curl 7 29 0	Client	4	3.75 KB	12.98 KB	56.73 KB	
TIMESTAMP	THIS ASSET (CLIENT)	FROM/TO	PROTOCOL	PORT	INGRESS	EGRESS	TOTAL
Mar 02 2022 13:42	10.	Excluded	tcp	3128	6.06 KB	1.88 KB	7.94 KB
Mar 02 2022 13:42	10.	Excluded	top	3128	37.69 KB	11.1 KB	48.79 KB

What is Monitored External

PS does not track IPs outside the inventoried and non-inventoried range and attributes them to one asset named External as explained earlier. However, the user may want to monitor traffic flows from internal assets to certain external IPs/FQDNs. For example, monitor the volume of traffic from internal assets to social media sites such as Facebook, Twitter, etc. PS provides a "Monitored External" configuration and uses FQDNs or IPs specified therein, to track traffic flows destined to an asset created per group. These assets do not show in the CSAM asset listing. If Monitor External FQDNs or IPs are configured, then traffic flows of Monitor External assets will be tracked with the actual IP address. i.e., Traffic flows between inventoried assets & Monitor External assets will be shown with the actual IP address of Monitor External IP's/FQDNs assets in the traffic listing of inventoried assets.

How to Configure Monitor External FQDNs or IPs

Select the appliance from the Passive Sensor Module listing and navigate to its details to edit the External Assets configuration to add FQDN / IP in a group. The following screenshots shows 2 groups, each one with a unique name. PS will track traffic flows going to one of the 2 assets that represents each group.

Configuration	Internal Assets	Excluded Assets	Monitor External Assets	General Settings
Actions (0)	Add			
NAME			DETAILS	
social-media			31	www.facebook.com
yahoo-website			www.yahoo	o.com

Traffic summary representation of Monitor External Assets & External Assets:

	FAMILY	APP/SERVICE		CLIENT/SERVER	INGRESS	EGRESS	TOTAL	
2	Web Services	HTTPs		Client	10.59 MB	996.19 KB	11.57 MB	
	TIMESTAMP	THIS ASSET (CLIENT)	FROM/TO	PROTOCO	L PORT	INGRESS	EGRESS	TOTAL
	Mar 02 2022 19:01	10.1	External	top	443	8.51 MB	109.11 KB	8.62 MB
	Mar 02 2022 19:01	10.1	External	top	443	15.06 KB	2.14 KB	17.2 KB
	Mar 02 2022 19:00	10.1	External	tcp	443	6.29 KB	1.04 KB	7.33 KB
	Mar 02 2022 18:57	10.1	98.137.11.1	165 tcp	443	4 KB	3.22 KB	7.23 KB
	Mar 02 2022 18:55	10.1	31.13.65.30	6 udp	443	40.9 KB	28.5 KB	69.4 KB

Best Practices

This section contains certain best practices to follow when configuring the internal assets in PS appliances.

1. Avoid configuring overlapping subnets as internal (inventoried) assets on more than one sensor appliance

In deployments that have more than one passive network sensor appliances registered with the same Qualys cloud account, it is recommended that the configuration of internal inventory network ranges should not overlap between the sensors.

To explain this better, let us consider a sample deployment that has 2 sensors deployed in different locations registered to the same account.



The enterprise network in the above scenario has 2 branches A and B. There are 2 sensors deployed one each in branch A and B. For the enterprise network subnets A and B together make up the range on IPs for internal assets that have to be inventoried. Assets A.1, A.2, and A.3 belong to subnet A and B.1, B.2, and B.3 belong to subnet B.

Now consider a case where there is intra branch traffic. Each of the sensors in branch A and B will "see" traffic flows from/to assets in subnets A to B.

For example, if A.1 were to initiate a flow to B.1, both sensors would sense this flow. If both sensors are configured with subnet A and B as the internal (inventoried) range, then both sensors will report assets A.1 and B.1 causing the same assets to be reported twice to Qualys cloud. This causes additional workload on the cloud services and this may result in delayed or missed updates of the assets or traffic flows as seen in the asset or traffic listing.

This workload multiplies if there are flows from each one of the assets in subnet A to B.1, such as A.1 to B.1, A.2 to B.1, and A.3 to B.1.

So, adding the same subnet into multiple sensors is inefficient and not a recommended configuration.

Desired/Recommended configuration: Detect assets in location specific subnets and provision a "non-inventoried" asset category

A recommended configuration to avoid duplicate processing on the cloud is to configure each sensor with a unique subnet as its inventoried range and add the other subnets internal to the organization as its internal non-inventoried range.

So in the above example, the sensor deployed in Branch A would only consider IPs of subnet A as the internal IPs and treat everything else as external. This means even subnet B which belongs to the universe on internal IPs of the organization would be considered external to the sensor in branch A. However, to track the inter-branch traffic flows so to know which asset in subnet A was talking to which asset in subnet B and vice-versa, it is recommended to add subnet B as internal (non-inventoried) range in sensor of location A. The passive sensor uses the non-inventoried range or IP to create assets whose attributes are not collected just as in the case of External assets but with a difference that its IP is recorded.

Similarly for the sensor in location B, configure subnet B as its internal inventoried range and subnet A as its internal non-inventoried range.

With the above configuration sensor in location A would report A.1, A.2, and A.3 as internal inventoried assets and B.1 as the non-inventoried assets. Similarly, the sensor in location B would report B.1 as its internal inventoried asset and A.1, A.2, and A.3 as its non-inventoried asset.

This configuration saves the PS services from the burden of additional processing. This also conserves the WAN bandwidth needed by sensors to report metadata to Qualys cloud as only one sensor reports the inventoried assets.

To summarize, the configuration of both passive sensors is as follows:

Passive Sensor Appliance Location	Internal (inventoried)	Internal (non-inventoried)
Branch A	Subnet A	Subnet B
Branch B	Subnet B	Subnet A

2. Avoid mirroring replicated IPs to a single appliance

In topologies, more common in OT networks, multiple smaller networks can have the same IP subnet. Each such replicated IP subnets has to be mirrored to a separate PS appliance. Avoid mirroring multiple such subnets to one appliance.

For example, consider a site with a yard having many cranes and each crane is a small network having exactly the same type of devices with the same IPs configured.

The overlapping IP address space in each crane can be handled by the Network feature which the customer can subscribe to. This feature allows the same subscription to uniquely identify IP within a network.

The Network feature is already supported in VM and PC modules and is part of the PS 1.4.0.0 release. PS uses the network feature by de-duplicating passively sensed Unmanaged IPs/assets with managed assets belonging to the same Network. PS exercises the network-based merge to de-duplicate assets only when it has neither MAC nor hostname information to uniquely identify the assets for de-duplication.

So here is what the configuration of PS appliance in each crane would look like

Crane #1

- Add Crane#1 IP range R1 in Asset Group AG1 in Network N1 in VM module

- Run policy compliance scan for the asset group AG1 in N1 in VM module

- Add NPS1 to Network N1 and configure NPS 1 to sense IP range R1 in N1

Crane #2

- Add Crane#2 IP range R2 in Asset Group AG2 in Network N2 in VM modules

- Run policy compliance scan for the asset group AG2 in N2 in the VM module
- Add NPS2 to Network N2 and configure NPS 2 to sense IP range R2 in N2

3. Add NATed IPs in the excluded list

PS does not yet support the capability to detect NATed devices. All assets behind NAT devices get masqueraded by the NATed IP and if PS sees this NATed IP, it will associate meta-data/attributes of all such devices to a single asset which has the Nated IP, making the asset very large, and these slow down the processing pipeline on the cloud. So, it is recommended to add such IPs as internal assets to be excluded.

4. Do not feed multiple copies of the same packet to the sensor

It is important that the TAPs or SPAN ports that feed the traffic copy to PS do not contain duplicate copies of the same packet. This will result in PS reporting incorrect volumes of traffic flow.

5. Backup and restore of PS VM image

It is not recommended to backup PS VM images to be restored later. In case the VM fails to boot due to corruption, contact Qualys support instead of re-deploying the PS VM. The PS services on Qualys cloud account retains the sensor configuration and applies it to the appliance on reboot.