Cloud Perimeter Scans

User Guide

April 14, 2022

Copyright 2018-2022 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo 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

Thank you for your interest in the Qualys Cloud Platform! This guide tells you how to configure and launch cloud perimeter scans using the UI and API.

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

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/

Configuring Cloud Perimeter Scanning for EC2 Connectors

What you'll need

Cloud Perimeter Scanning must be enabled

You'll need to have these features enabled to run perimeter scans on your cloud environment: 1) Cloud Perimeter Scanning, 2) EC2 Scanning and 3) Scan by Hostname.

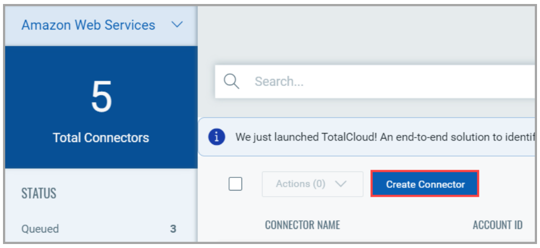
Please contact your Technical Account Manager or Qualys Support to have features enabled. (Not available to Express Lite.)

Manager or Unit Manager privileges

Your account must have a Manager or Unit Manager role.

EC2 connector is required

If this is your first EC2 scan then we recommend you start by creating an EC2 connector. You'll do this within the Connector application. A wizard will walk you through the steps.



We just launched TotalCloud! An end-to-end solution to identif

Want to learn more about setting up connectors? Check out Connector Online Help.

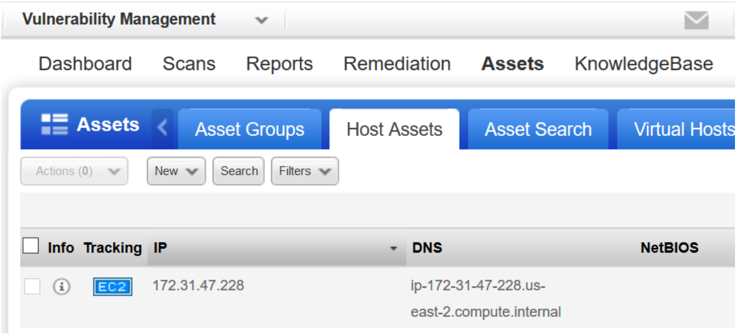
Note: Ensure your existing service control policies do not block the required permissions for EC2 connector runs.

EC2 Scan Checklist

We recommend a few steps before scanning.

Check EC2 Assets are activated

Check that your EC2 hosts are activated and have the EC2 tracking method. You can see this in VM on the Host Assets tab and also in AssetView on the Assets tab.



□	Info	Tracking	IP	DNS	NetBIOS
□	ⓘ	EC2	172.31.47.228	ip-172-31-47-228.us-east-2.compute.internal	

Configure Your New Cloud Perimeter Scan

Good to Know

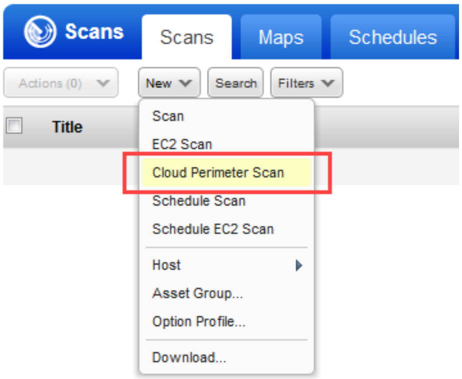
- Cloud perimeter scans use Qualys External Scanners (Internet Remote Scanners), located at the Qualys Cloud Platform. For accounts on Private Cloud Platforms, your account may be configured to allow internal scanners to be used.

- These are DNS or IP -based scans launched using the public DNS or Public IP of the target EC2 instances. If both public DNS and public IP address exist for your EC2 assets, then we will launch a scan on public DNS.

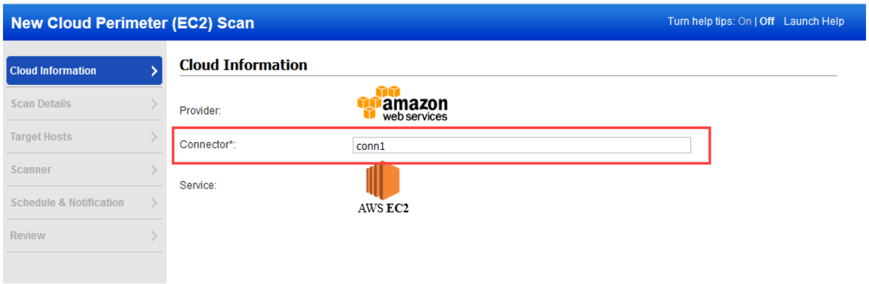
- All cloud perimeter scans are scheduled - either for “now” (essentially a one-time scan) or “recurring”. Once saved, you’ll see the scan job on the Schedules list. When the scan starts it will appear on your Scans list.

Get Started

Go to Scans > Scans > New > Cloud Perimeter Scan (also on the Schedules tab).



Select the EC2 connector you've configured.



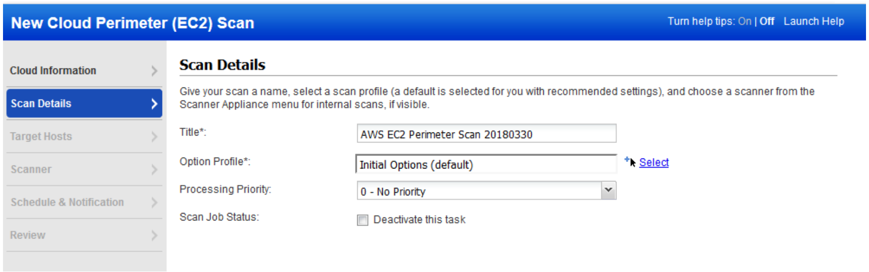
Cloud Information

Provider: amazon web services

Connector*: conn1

Service: AWS EC2

Give your scan a title and select an option profile. Note that cloud perimeter scans typically do not use authentication.



Scan Details

Give your scan a name, select a scan profile (a default is selected for you with recommended settings), and choose a scanner from the Scanner Appliance menu for internal scans, if visible.

Title*: AWS EC2 Perimeter Scan 20180330

Option Profile*: Initial Options (default)

Processing Priority: 0 - No Priority

Scan Job Status: □ Deactivate this task

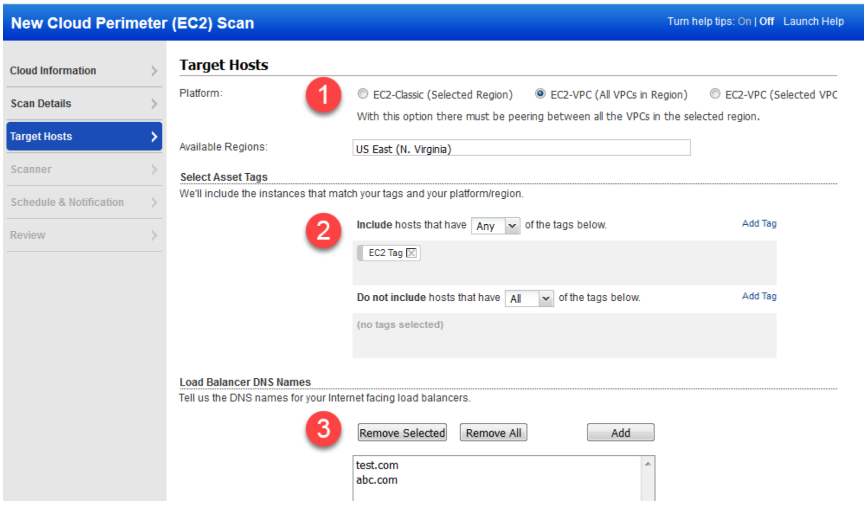
Now it's time to pick your target hosts. Selecting target hosts is an optional step. If you do not specify the platform, region code, vpc id or asset tags, we will create the new cloud perimeter scan job using only the connector.

1) Choose a platform option: EC2 Classic, EC2 VPC (All VPCs in region) or EC2 VPC (Selected VPC). Based on your selection you'll select region(s).

2) Select asset tags - these are assets activated for your connector.

3) Enter the DNS names for your load balancers to include them in the scan.

Note that if no assets are resolved from the connector and for the optional "platform" and "asset tags" selections, the scan is launched on the load balancer DNS names. If no load balancer DNS names are specified, then the scan will fail and get terminated.



Target Hosts

Platform: ○ EC2-Classic (Selected Region) ● EC2-VPC (All VPCs in Region) ○ EC2-VPC (Selected VPC

With this option there must be peering between all the VPCs in the selected region.

Available Regions: US East (N. Virginia)

Select Asset Tags

We'll include the instances that match your tags and your platform/region.

Include hosts that have Any of the tags below.

EC2 Tag ☒

Do not include hosts that have All of the tags below.

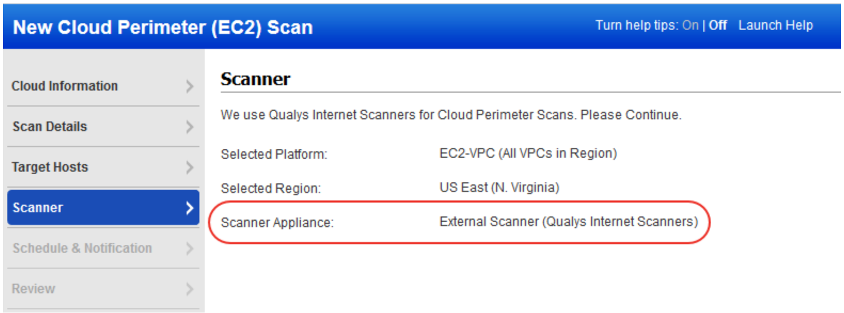
(no tags selected)

Load Balancer DNS Names

Tell us the DNS names for your Internet facing load balancers.

test.com
abc.com

By default cloud perimeter scans use Qualys External Scanners.



Scanner

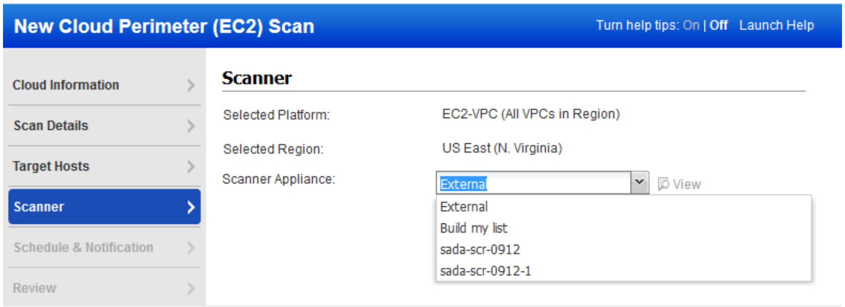
We use Qualys Internet Scanners for Cloud Perimeter Scans. Please Continue.

Selected Platform: EC2-VPC (All VPCs in Region)

Selected Region: US East (N. Virginia)

Scanner Appliance: External Scanner (Qualys Internet Scanners)

For Private Cloud Platforms - Your account may be configured to allow scanner appliances to be used. In this case, choose one or more scanner appliances from the list (use the Build my list option).



Scanner

Selected Platform: EC2-VPC (All VPCs in Region)

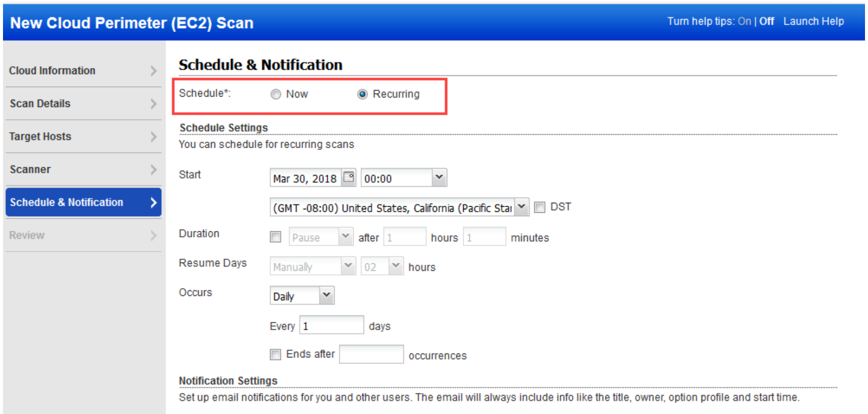
Selected Region: US East (N. Virginia)

Scanner Appliance: External

Tell us when you want the scan to run - Now or Recurring.

Note that when you choose Now your scan may not start immediately. We'll check for new scan requests every few minutes. If a scanner is available and you haven't reached your concurrent scan limit then we'll launch the scan. If scanners are not available or you have reached your limit then the scan will be launched at the next opportunity.

When you choose Recurring you'll also set scheduling and notification options. These are the same settings as other scan schedules so they should look familiar.



Schedule & Notification

Schedule*: ○ Now ● Recurring

Schedule Settings
You can schedule for recurring scans

Start: Mar 30, 2018 00:00
(GMT -08:00) United States, California (Pacific Stai □ DST

Duration: □ Pause after 1 hours 1 minutes

Resume Days: Manually 02 hours

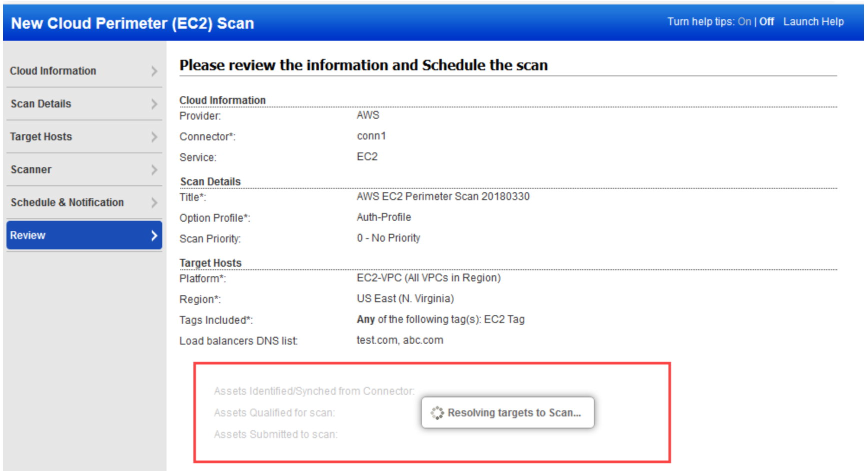
Occurs: Daily

Every 1 days

□ Ends after occurrences

Notification Settings
Set up email notifications for you and other users. The email will always include info like the title, owner, option profile and start time.

We'll identify the assets to scan based on your settings.



Please review the information and Schedule the scan

Cloud Information
Provider: AWS
Connector*: conn1
Service: EC2

Scan Details
Title*: AWS EC2 Perimeter Scan 20180330
Option Profile*: Auth-Profile
Scan Priority: 0 - No Priority

Target Hosts
Platform*: EC2-VPC (All VPCs in Region)
Region*: US East (N. Virginia)
Tags Included*: **Any** of the following tag(s): EC2 Tag
Load balancers DNS list: test.com, abc.com

Assets Identified/Synched from Connector:
Assets Qualified for scan:
Assets Submitted to scan:

You'll see these asset counts:

Assets Identified / Synced - The number of assets discovered by the connector.

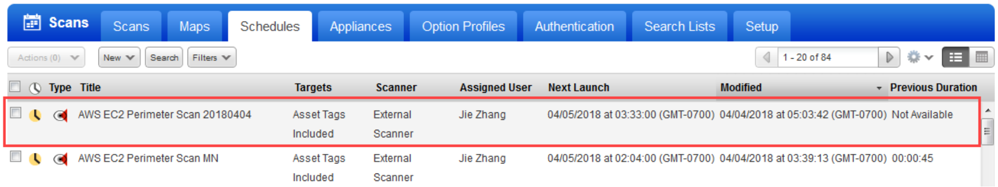
Assets Qualified for scan - The number of assets discovered by the connector that also match the selected platform, region, asset tags. We'll take out the Terminated instances.

Assets Submitted to scan - The number of assets that we'll submit in the scan job. We start with the qualified assets (previous count) and filter out assets that are not activated for VM (for vulnerability scan) or not activated for PC (for compliance scan).

When you're ready, click Submit Scan Job.

What happens next

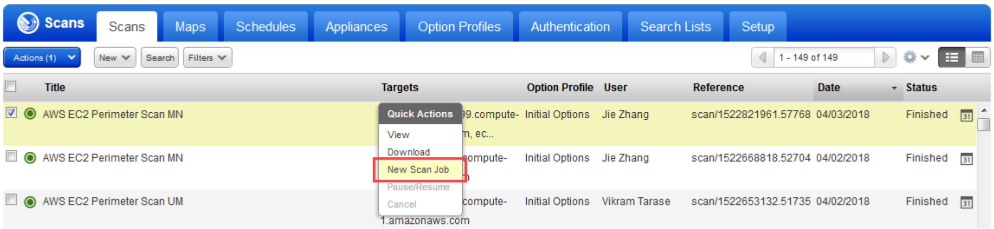
Your new scan will appear on the Schedules list (even if you started it from the Scans tab).



□	Type	Title	Targets	Scanner	Assigned User	Next Launch	Modified	Previous Duration
□		AWS EC2 Perimeter Scan 20180404	Asset Tags Included	External Scanner	Jie Zhang	04/05/2018 at 03:33:00 (GMT-0700)	04/04/2018 at 05:03:42 (GMT-0700)	Not Available
□		AWS EC2 Perimeter Scan MN	Asset Tags Included	External Scanner	Jie Zhang	04/05/2018 at 02:04:00 (GMT-0700)	04/04/2018 at 03:39:13 (GMT-0700)	00:00:45

When your scan starts it will appear on the Scans list. Like with other scans you can take actions like cancel or pause the scan, view the scan status and download the results.

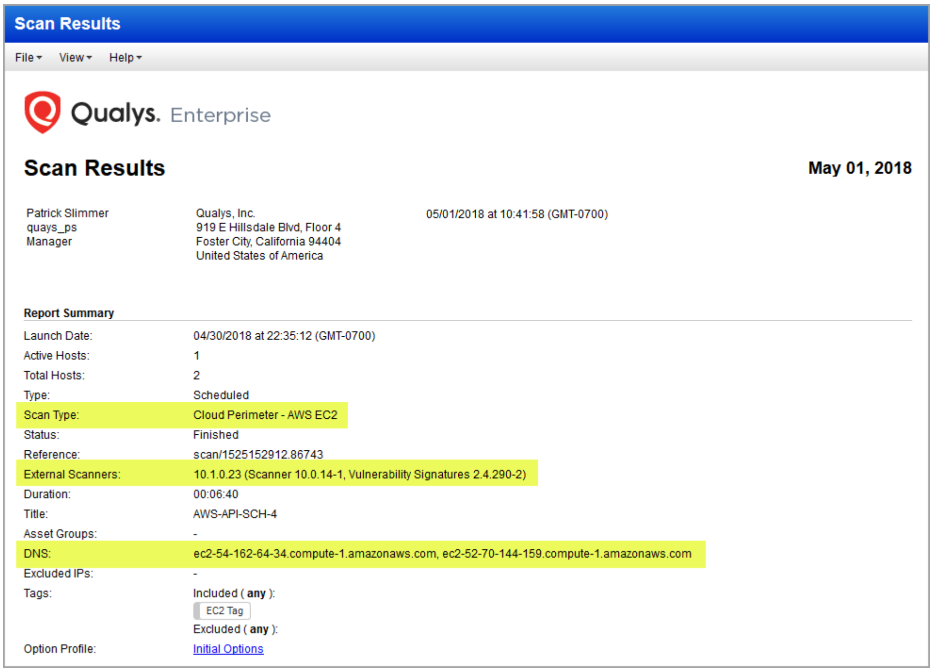
Want to run the scan again? Choose New Scan Job from the Quick Actions menu. We'll retain certain scan settings from the original scan job and schedule the scan to run Now.



□	Title	Targets	Option Profile	User	Reference	Date	Status
☑	AWS EC2 Perimeter Scan MN	9.compute- n, ec...	Initial Options	Jie Zhang	scan/1522821961.57768	04/03/2018	Finished
□	AWS EC2 Perimeter Scan MN	ompute- n	Initial Options	Jie Zhang	scan/1522668818.52704	04/02/2018	Finished
□	AWS EC2 Perimeter Scan UM	compute- 1.amazonaws.com	Initial Options	Vikram Tarase	scan/1522653132.51735	04/02/2018	Finished

View Scan Results

Choose View from the Quick Actions menu for any finished scan in your list to see the scan results. You'll notice the scan type is "Cloud Perimeter - AWS EC2", you'll see that Qualys External Scanners were used for the scan, and you'll see the target DNS names for the assets submitted in the scan job.



Scan Results

May 01, 2018

Patrick Slimmer
quays_ps
Manager

Qualys, Inc.
919 E Hillsdale Blvd, Floor 4
Foster City, California 94404
United States of America

05/01/2018 at 10:41:58 (GMT-0700)

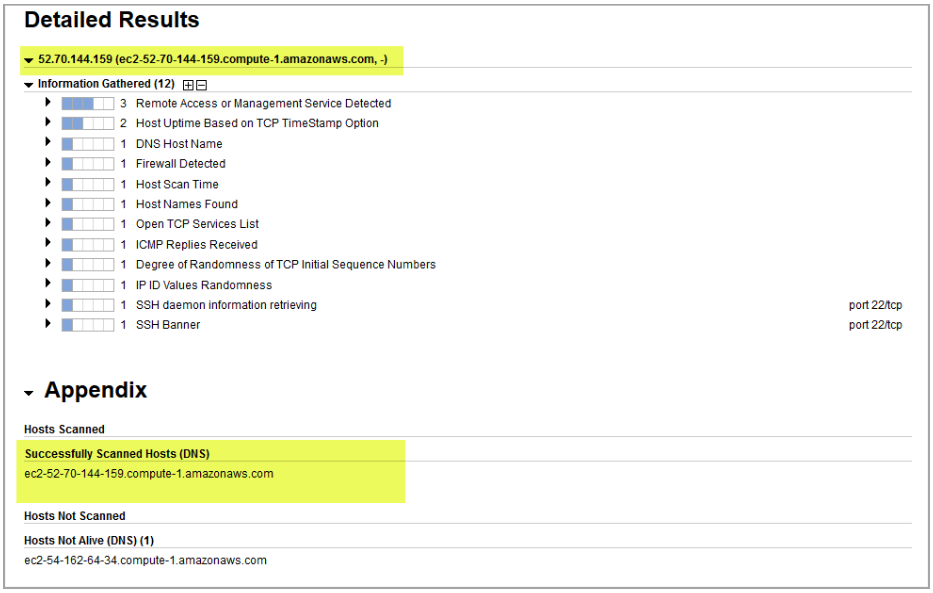
Report Summary

Launch Date:	04/30/2018 at 22:35:12 (GMT-0700)
Active Hosts:	1
Total Hosts:	2
Type:	Scheduled
Scan Type:	Cloud Perimeter - AWS EC2
Status:	Finished
Reference:	scan/1525152912.86743
External Scanners:	10.1.0.23 (Scanner 10.0.14-1, Vulnerability Signatures 2.4.290-2)
Duration:	00:06:40
Title:	AWS-API-SCH-4
Asset Groups:	-
DNS:	ec2-54-162-64-34.compute-1.amazonaws.com, ec2-52-70-144-159.compute-1.amazonaws.com
Excluded IPs:	-

Tags:	Included (**any**):
	EC2 Tag
	Excluded (**any**):

Option Profile:	Initial Options

The Detailed Results and Appendix sections of your scan results show the public DNS name for each scanned asset since cloud perimeter scans are DNS-based.



Detailed Results

52.70.144.159 (ec2-52-70-144-159.compute-1.amazonaws.com, -)

Information Gathered (12)

3	Remote Access or Management Service Detected	
2	Host Uptime Based on TCP TimeStamp Option	
1	DNS Host Name	
1	Firewall Detected	
1	Host Scan Time	
1	Host Names Found	
1	Open TCP Services List	
1	ICMP Replies Received	
1	Degree of Randomness of TCP Initial Sequence Numbers	
1	IP ID Values Randomness	
1	SSH daemon information retrieving	port 22/tcp
1	SSH Banner	port 22/tcp

Appendix

Hosts Scanned

Successfully Scanned Hosts (DNS)

ec2-52-70-144-159.compute-1.amazonaws.com

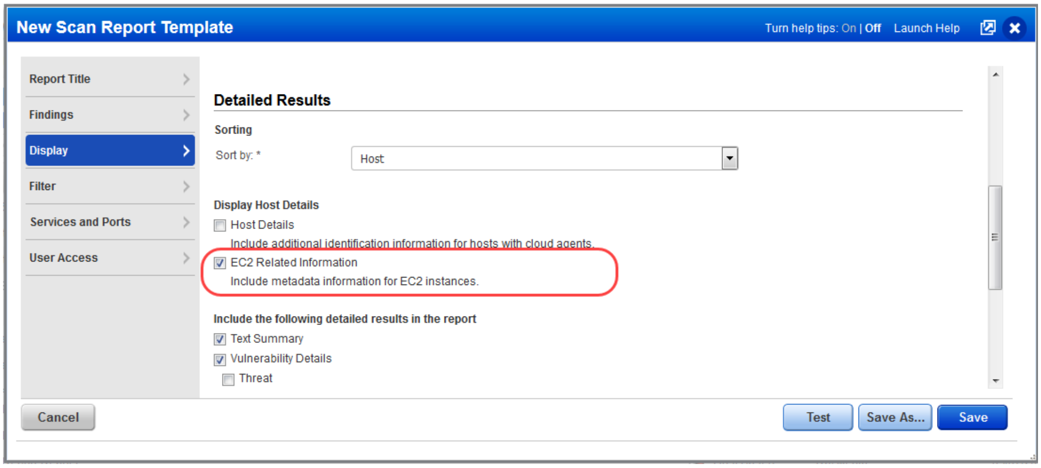
Hosts Not Scanned

Hosts Not Alive (DNS) (1)

ec2-54-162-64-34.compute-1.amazonaws.com

Run Scan Reports

In your scan report template select the EC2 Related Information option on the Display tab. This lets you see EC2 details for each asset in your report, including the public DNS name.



Detailed Results

Sorting

Sort by: * Host

Display Host Details

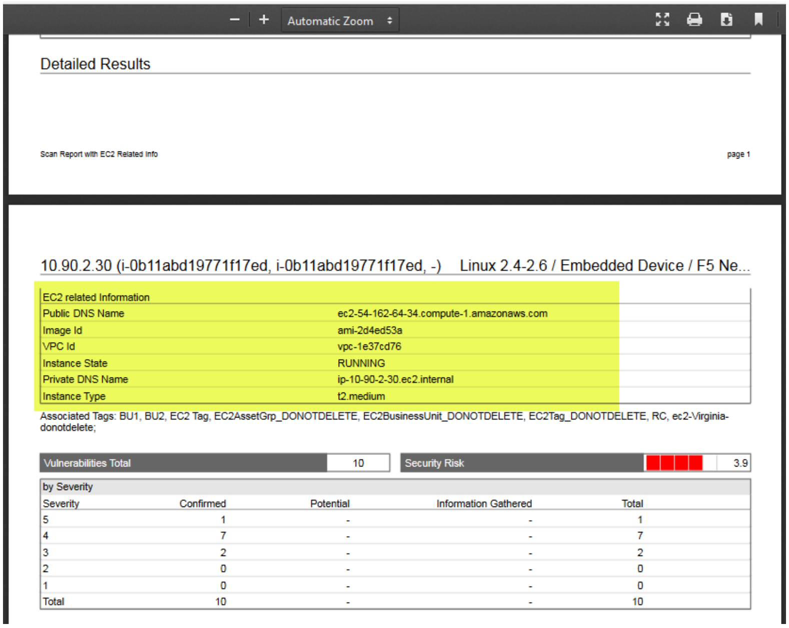
☐ Host Details
Include additional identification information for hosts with cloud agents.

☑ EC2 Related Information
Include metadata information for EC2 instances.

Include the following detailed results in the report

☑ Text Summary
☑ Vulnerability Details
☐ Threat

Check out this sample report with EC2 related information.



Detailed Results

Scan Report with EC2 Related Info page 1

10.90.2.30 (i-0b11abd19771f17ed, i-0b11abd19771f17ed, -) Linux 2.4-2.6 / Embedded Device / F5 Ne...

EC2 related Information	
Public DNS Name	ec2-54-162-64-34.compute-1.amazonaws.com
Image Id	ami-2d4ed53a
VPC Id	vpc-1e37cd76
Instance State	RUNNING
Private DNS Name	ip-10-90-2-30.ec2.internal
Instance Type	t2.medium

Associated Tags: BU1, BU2, EC2 Tag, EC2AssetGrp_DONOTDELETE, EC2BusinessUnit_DONOTDELETE, EC2Tag_DONOTDELETE, RC, ec2-Virginia-donotdelete;

Vulnerabilities Total 10
Security Risk 3.9

by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	1	-	-	1
4	7	-	-	7
3	2	-	-	2
2	0	-	-	0
1	0	-	-	0
Total	10	-	-	10

Configuring Cloud Perimeter Scanning for Azure Connectors

We provide the ability to scan public facing virtual machines in your Azure cloud environment using Cloud Perimeter Scanning for VM and PC.

Qualys External Scanners (Internet Remote Scanners), located at the Qualys Cloud Platform are used for Perimeter Scanning of Azure virtual machines. For subscriptions on Private Cloud Platforms, your account may be configured to allow internal scanners to be used.

These are DNS or IP -based scans launched using the public DNS or Public IP of the target virtual machines. If both public DNS and public IP address exist for your virtual machines, then we will launch a scan on public DNS.

What you'll need

- The "Cloud Perimeter Azure VM Scan" feature must be enabled for your subscription. Please reach out to your Technical Account Manager or Qualys Support to enable this feature. You'll also need these features enabled: Cloud Perimeter Scanning, EC2 Scanning, Scan by Hostname.
- Cloud perimeter scans are available for VM and PC modules. Only Managers and Unit Managers have permission to configure cloud perimeter scans.
- We allow you to create/update a cloud perimeter scan job through Cloud Perimeter Scan API even if no scan targets are resolved from the provided details. At the time of scan, if no scan targets are resolved from the provided details, the scan will not be launched, and we add the error in the Activity log and Run history of the schedule scan job.

Configure Cloud Perimeter Scan

All cloud perimeter scans are scheduled - either for "now" (a one-time scan job) or "recurring". Once saved, you'll see the scan job on the Schedules list. When the scan job starts it will appear on your Scans list.

1) Create a dynamic tag with Cloud Asset Search filters under "AssetView" app based on your requirements.

For example:

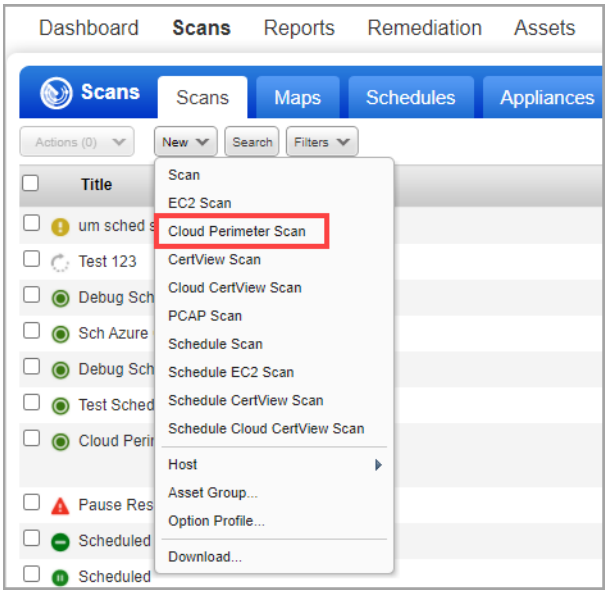
All running public VMs in your Qualys Subscription: **`not azure.vm.publicIpAddress is null and azure.vm.state:"RUNNING"`**

All running public VMs in your Azure Subscription: **`not azure.vm.publicIpAddress is null and azure.vm.subscriptionId: and azure.vm.state:"RUNNING"`**

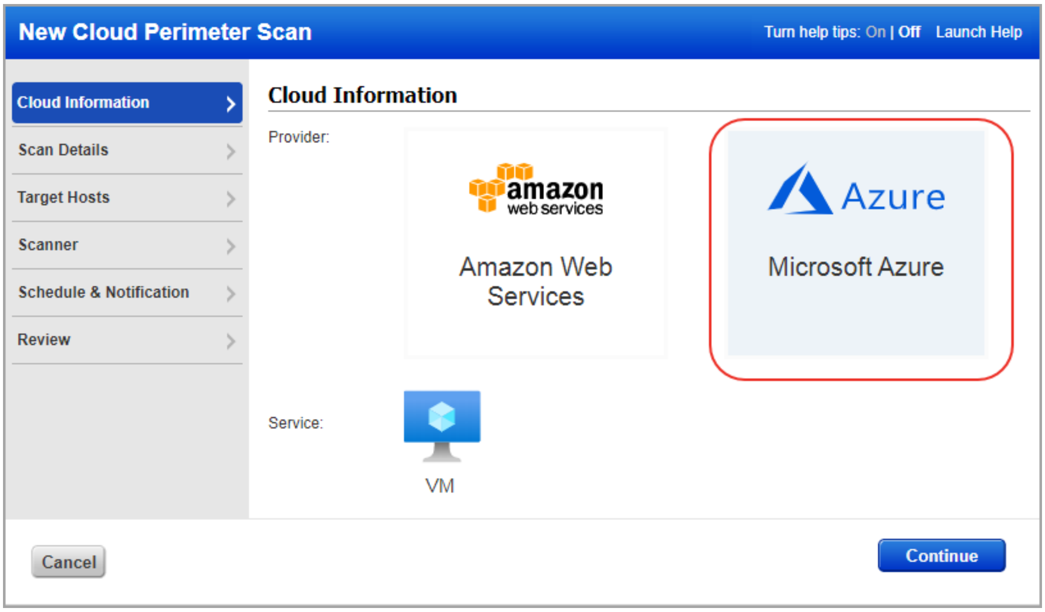
All running public VMs in a location: **`not azure.vm.publicIpAddress is null and azure.vm.state:"RUNNING" and azure.vm.location:westus`**

All running public VMs in a resource group: **`not azure.vm.publicIpAddress is null and azure.vm.state:"RUNNING" and azure.vm.resourceGroupName:testRG`**

2) Now, lets start scanning. Go to VM/VMDR for a vulnerability scan (or PC for a compliance scan) and choose New > Cloud Perimeter Scan. You'll also see this option on the Schedules tab.



3) In the Cloud Information tab, select the Azure icon to scan the Azure VM machines and click **Continue**.



Note: While updating the scan, you cannot change the Provider. We populate the values you selected at the time of creating the scan in Scan option profile settings.

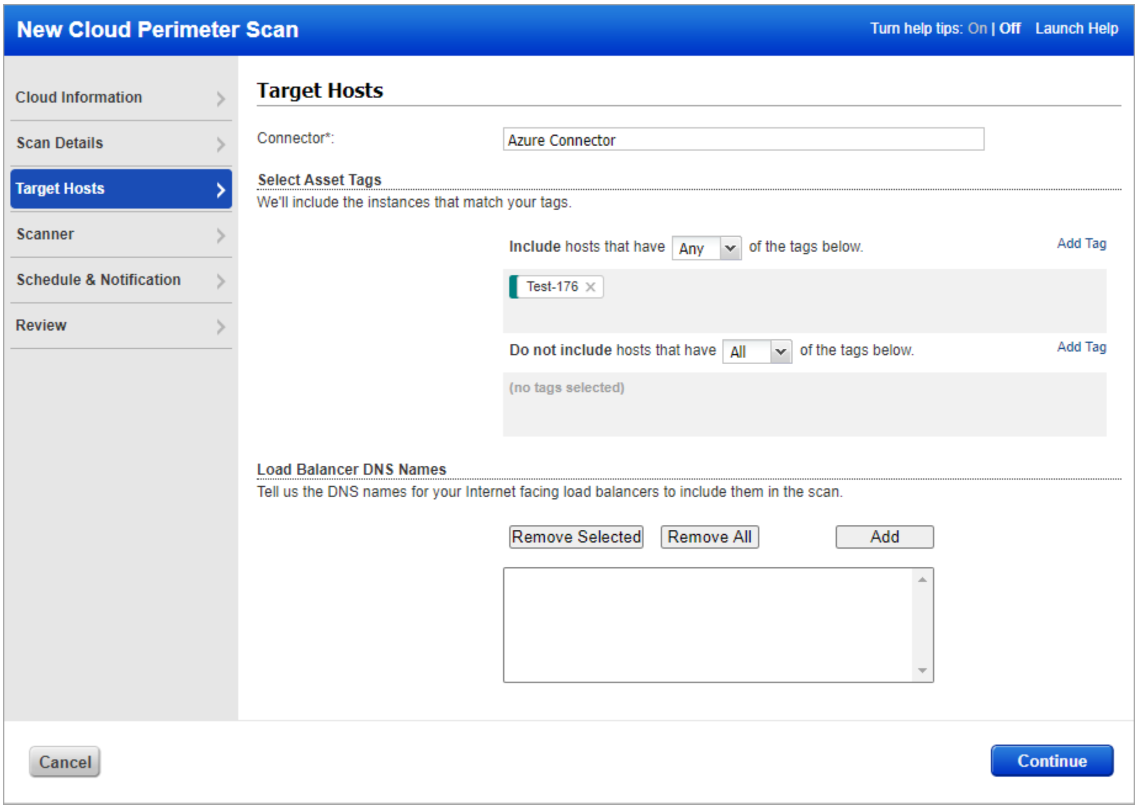
4) Go to the **Scan Details** tab and give the scan a name and select the option profile and priority.

5) Go to the **Target Hosts** tab to select the public facing Azure VM machines on which you want to run the Cloud Perimeter scan. From the **Connectors** drop-down, select an Azure connector.

The Connector drop-down lists the connectors that you have configured in Connectors Application. Select asset tags to further filter the Azure VM assets fetched from the Azure connector.

Note: The selected asset tag will scope the selected connectors assets and will not scan assets from under other connectors or non-connector based assets.

For load balancers, manually add the DNS names of internet facing load balancers. For Azure VM scan, we do not support pulling load balancer DNS names from the CloudView module.



Target Hosts

Connector*: Azure Connector

Select Asset Tags

We'll include the instances that match your tags.

Include hosts that have Any of the tags below.

Test-176 ×

Do not include hosts that have All of the tags below.

(no tags selected)

Load Balancer DNS Names

Tell us the DNS names for your Internet facing load balancers to include them in the scan.

6) Go to the Scanner and Schedule & Notification tabs to select the External/Internal scanner and schedule the scans.

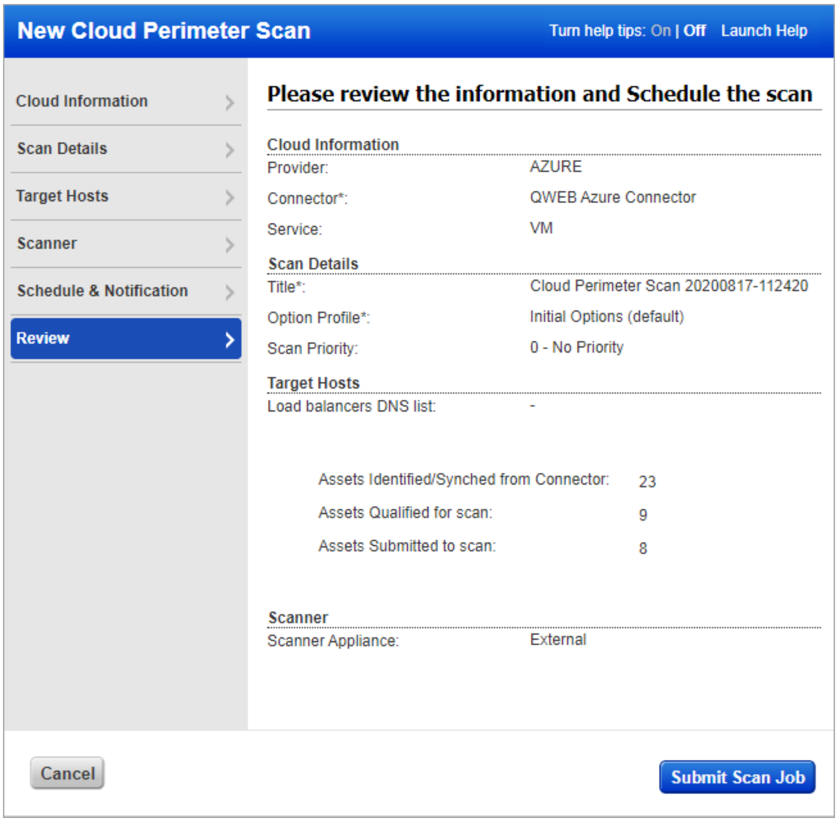
Note: By default, the external scanner appliance is selected. If internal scanner is enabled for cloud perimeter scan in your subscription, only then we allow you to select an internal scanner for the scan.

7) Go to the Review tab. In the Target Hosts section, we will show you:

- how many public facing Azure VM assets are fetched from the connector,

- assets that are qualified for the scan and

- out of the qualified assets, how many assets are activated in VM on which the scan will be launched.



Please review the information and Schedule the scan

Cloud Information

Provider:	AZURE
Connector*:	QWEB Azure Connector
Service:	VM

Scan Details

Title*:	Cloud Perimeter Scan 20200817-112420
Option Profile*:	Initial Options (default)
Scan Priority:	0 - No Priority

Target Hosts

Load balancers DNS list:	-

Assets Identified/Synched from Connector:	23
Assets Qualified for scan:	9
Assets Submitted to scan:	8

Scanner

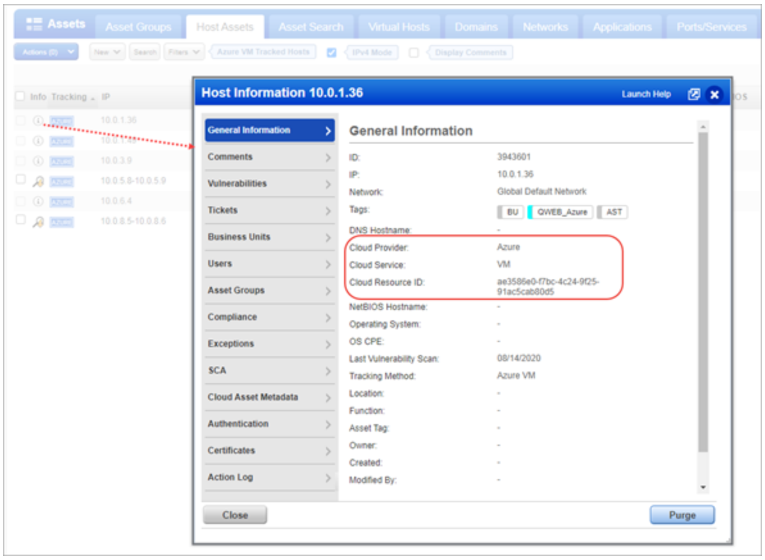
Scanner Appliance:	External

8) Finally, submit the scan job.

The VM assessment results from Azure perimeter scans will be tracked to the virtual machine ID tracked asset. As a part of the scan option profile, the scanner tries to reach out the IPs and try to get to the virtual machines.

View Azure VM Tracked Host Assets in Host Assets

Go to Assets > Host Assets > Filters to search for the Azure VM tracked assets.



Host Information 10.0.1.36

General Information

ID: 3943601
IP: 10.0.1.36
Network: Global Default Network
Tags: BU QWEB_Azure AST
DNS Hostname: -
Cloud Provider: Azure
Cloud Service: VM
Cloud Resource ID: ae3586e0-f7bc-4c24-9f25-91ac5cab80d5
NetBIOS Hostname: -
Operating System: -
OS CPE: -
Last Vulnerability Scan: 08/14/2020
Tracking Method: Azure VM
Location: -
Function: -
Asset Tag: -
Owner: -
Created: -
Modified By: -

Click the info button to view the cloud provider name (which is Azure for Azure VM assets), cloud service name (VM for Azure VM assets), and resource ID for the Azure Virtual Machine in the Host Information screen. The Cloud Asset Metadata tab shows the metadata information for the host.

Qualys API Support

The Qualys API provides support for cloud perimeter scan jobs in these ways:

- Use the Cloud Perimeter Scans API (/api/2.0/fo/scan/cloud/perimeter/job) to create and update scan perimeter scan jobs. You can schedule a scan for now or schedule it to start at a later time or on a recurring basis. Cloud perimeter scans are available for VM and PC modules. Only Managers and Unit Managers have permission to configure cloud perimeter scans.

- Use the Schedule Scan List API (/api/2.0/fo/schedule/scan/?action=list) to show cloud perimeter scan jobs. When you include cloud details in the XML output, the cloud details will show scan type "Cloud Perimeter" for cloud perimeter scans.

- Use the Fetch Scan Results API (/api/2.0/fo/scan/?action=fetch) to fetch scan results for cloud perimeter scan jobs using the API.

Refer to the Qualys API (VM, PC) User Guide to learn more about these APIs, including available input parameters and API samples.