Securing Amazon Web Services with Qualys

February 15, 2024

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

Table of Contents

About this guide

Welcome to Qualys Cloud Platform and security scanning in the Cloud! We'll help you get acquainted with the Qualys solutions for scanning your Cloud IT infrastructure using the Qualys Cloud Security Platform.

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

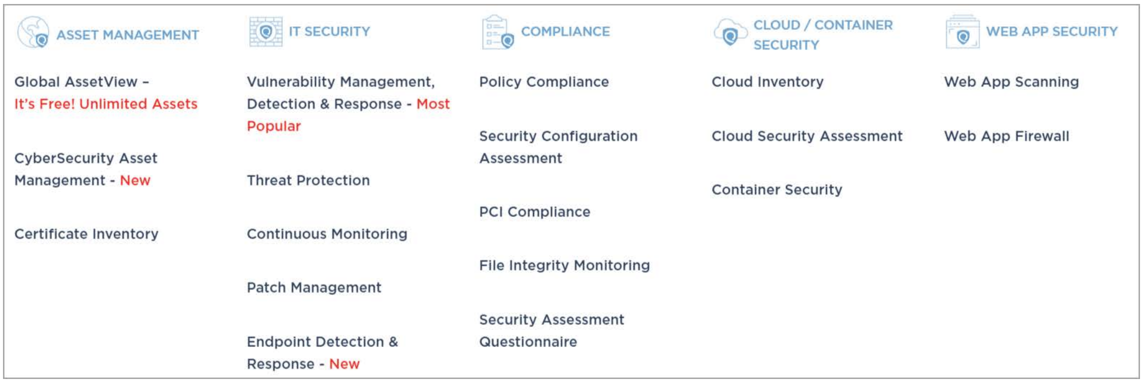
Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at www.qualys.com/support/

Introduction

Welcome to Qualys Cloud Platform that brings you solutions for securing your Cloud IT Infrastructure as well as your traditional IT infrastructure. In this guide we'll be talking about securing your Amazon AWS EC2 infrastructure using Qualys.

Qualys Integrated Security Platform

With Qualys Cloud Platform you get a single view of your security and compliance - in real time. If you're new to Qualys we recommend you to visit the Qualys Cloud Platform web page to know more about our cloud platform.



ASSET MANAGEMENT

Global AssetView – It's Free! Unlimited Assets

CyberSecurity Asset Management - New

Certificate Inventory

IT SECURITY

Vulnerability Management, Detection & Response - Most Popular

Threat Protection

Continuous Monitoring

Patch Management

Endpoint Detection & Response - New

COMPLIANCE

Policy Compliance

Security Configuration Assessment

PCI Compliance

File Integrity Monitoring

Security Assessment Questionnaire

CLOUD / CONTAINER SECURITY

Cloud Inventory

Cloud Security Assessment

Container Security

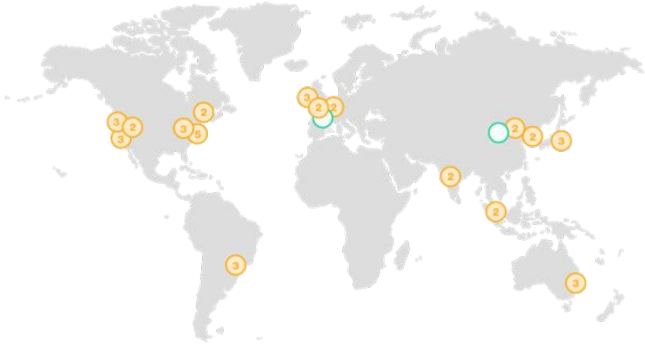
WEB APP SECURITY

Web App Scanning

Web App Firewall

Qualys Support for AWS

Qualys AWS Cloud support provides the following features:



- Secure EC2 Instances (IaaS) from vulnerabilities and check for regulatory compliance on OS and Applications (Database, Middleware)

- Gain continuous security using Cloud Agents, embed them into AMIs to get complete visibility

- Identify vulnerabilities for public facing IPs and URLs

- Secure Application using Application Scanning and Firewall solutions

- Vulnerability Scan

- Supports all AWS global regions including GovCloud

- Supports EC2 instances in Classic and VPC platform

- Qualys Cloud Agents certified to work in EC2

Qualys Sensors

Qualys sensors, a core service of the Qualys Cloud Platform, make it easy to extend your security throughout your global enterprise. These sensors are remotely deployable, centrally managed and self updating. They collect the data and automatically beam it up to the Qualys Cloud Platform, which has the computing power to continuously analyze and correlate the information in order to help you identify threats and eliminate vulnerabilities.

Virtual Scanner Appliances
Remote scan across your networks - hosts and applications

Cloud Agents
Continuous security view and platform for additional security

AWS Cloud Connectors
Sync cloud instances and its metadata

Internet Scanners
Perimeter scan for edge facing IPs and URLs

Web Application Firewalls
Actively defend intrusions and secure applications

Pre-requisites

These options must be enabled for your Qualys user account.

- Qualys Applications: Vulnerability Management (VM/VMDR), Policy Compliance (PC) or Security Configuration Assessment (SCA), Cloud Agent (CA), Web Application Scanning (WAS), Web Application Firewall (WAF).

- Qualys Amazon AWS EC2 Scanning option must be turned ON. If not available, please contact your Qualys Sales representative (TAM) or Support.

- Qualys Sensors: Virtual Scanner Appliances, Cloud Agents, as desired

- Manager or Unit Manager role

It's easy to get started

You might already be familiar with Qualys Cloud Suite, its features and user interface. If you're new to Qualys we recommend these overview tutorials - it just takes a few minutes!

Video Tutorials get you familiar with basics

Vulnerability Management Detection and Response. (3 mins)

Policy Compliance Overview

Quick Steps: Securing AWS

Here's the user flow for securing AWS EC2 using Qualys.

1 **Automate Asset Inventory**
Sync inventory and metadata for an AWS account by setting up EC2 Connector

2 **Deploy Sensors**
Install scanner appliance and/or Cloud Agents

3 **Scan Assets**
Launch scans targeting all assets or specific assets you are interested in

4 **Analyze, Report & Remediate**
View dynamic dashboards, Create custom widgets, Run reports

Helpful resources Always up to date with the information you need

From the Community

Qualys Training | Free self paced classes, video series, online classes

Qualys Documentation | Getting started guides, quick references, API docs

Qualys AWS EC2 Video Series | Learn how to discover and secure AWS assets

Automate Asset Inventory

The Connector for Amazon continuously discovers Amazon EC2 and VPC assets using an Amazon API integration. Connectors may be configured to connect to one or more Amazon accounts so they can automatically detect and synchronize changes to virtual machine instance inventories from all Amazon EC2 Regions and Amazon VPCs.

AWS instances are tracked by their Amazon Instance ID within Qualys, even as their IP addresses change over time. Asset Tags, which can drive or influence policies and reporting throughout Qualys, may be automatically assigned to asset entries as part of the import process. Attributes and contextual metadata about Amazon instances are also captured and available as data points to perform further Dynamic Asset Tagging within Qualys.

For an EC2 instance, you'll see the IP address, tags, private DNS name, EC2 Instance ID.

Setting up Connectors

This is the first step for securing AWS Infrastructure. In this section we will go through the steps required to setup a connector. Qualys recommends you setup one connector per AWS account. Qualys discovers and syncs asset inventories every 4 hours. Asset inventory is independent of a scan.

To learn how to set up a connector for your AWS account, see Connector Online Help.

Merge Existing Connector with Connector App

You can now merge your existing connectors that are created using AssetView or TotalCloud with the centralized Connector application (app). The new connectors are created through the Connector app and not AssetView/TotalCloud app. We recommend you to merge your existing connectors to proceed with securing your assets.

To merge your existing connectors, follow the instructions laid out in Configure Your AWS Connector.

Using Base Account Authentication

The AWS connectors with cross-account role uses Qualys accounts. If you do not wish to use Qualys account, you can use the base account to set up the AWS connectors.

You can configure to use your own AWS account as a base account while setting up the AWS Connectors instead of using Qualys account. You need to map your AWS account ID (in case of multiple AWS accounts, at least one AWS account) with the base account you create.

For example, you have 3 AWS accounts: A1, A2, A3. All the three accounts belong to Global region. If you create a base account for Global region. All the connectors associated with A1, A2, and A3 accounts will use base account.

Create a Base Account

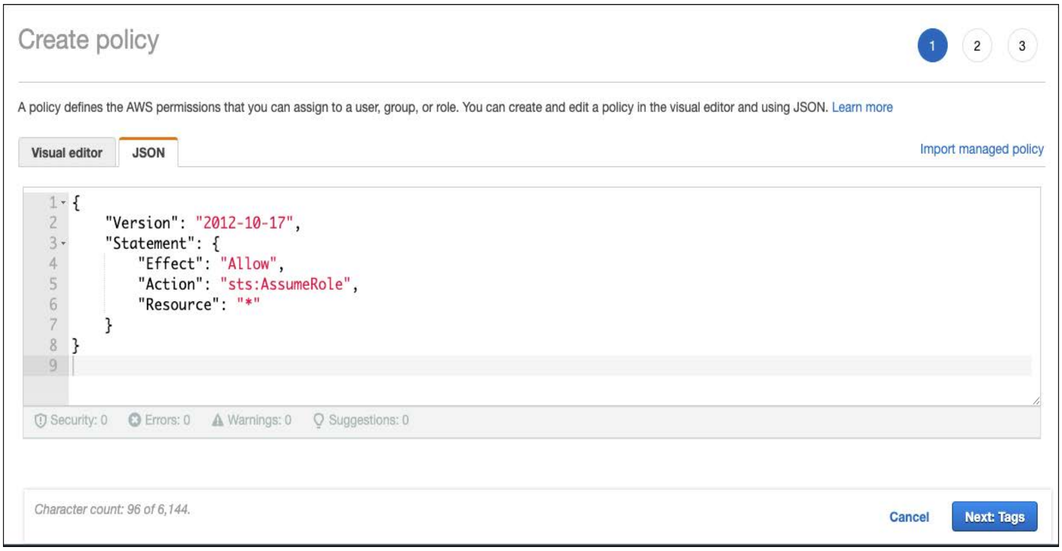
Before you create a new connector, create a base account for the same account type (region). You can still create a connector without a base account. If you plan to use base account for your connectors, there are certain pre-requisites and settings that need to be configured on the AWS console. The detailed steps and configuration required in AWS console for setting up base account is listed below.

Create IAM User and associate policy in AWS

1) Navigate to **AWS>IAM>Policies>Create Policy** to create AssumeRolePolicy

2) Click JSON tab and paste the below policy.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "sts:AssumeRole",
        "Resource": "*"
    }
}
```



A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "sts:AssumeRole",
        "Resource": "*"
    }
}
```

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

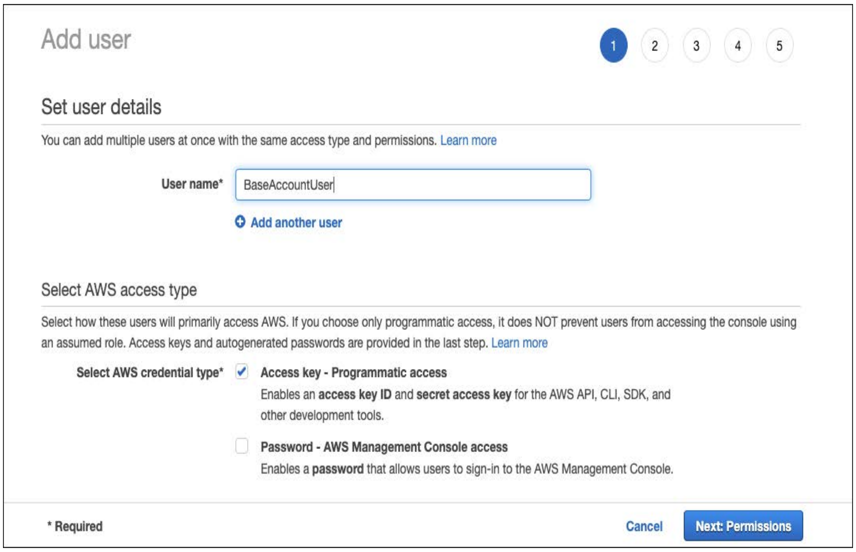
Character count: 96 of 6,144.

3) Click **Next: Tags** > **Next: Review**.

4) Add name and description for the policy and click **Create Policy**.

5) Create IAM User, navigate to **AWS > IAM > Users** and then click **Add user**.

6) Provide a user name and enable Programmatic access for the user. Click **Next: Permissions**.



Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* BaseAccountUser

Select AWS access type

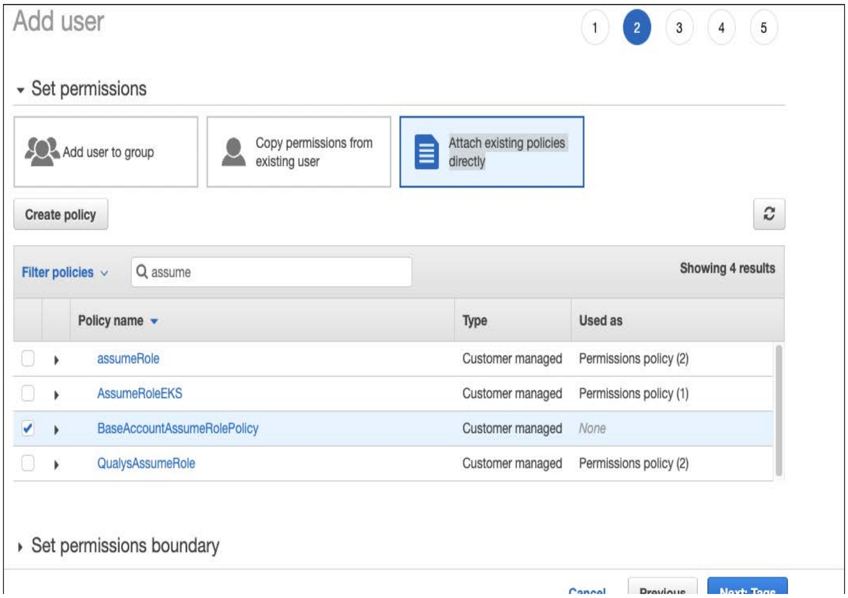
Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. Learn more

Select AWS credential type*

☑ **Access key - Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

□ **Password - AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

7) On Set Permissions, navigate to **Attach existing policies directly**.



Search: assume

Showing 4 results

		Policy name	Type	Used as
□	▸	assumeRole	Customer managed	Permissions policy (2)
□	▸	AssumeRoleEKS	Customer managed	Permissions policy (1)
☑	▸	BaseAccountAssumeRolePolicy	Customer managed	None
□	▸	QualysAssumeRole	Customer managed	Permissions policy (2)

8) Search for the policy name created in step 1-4.

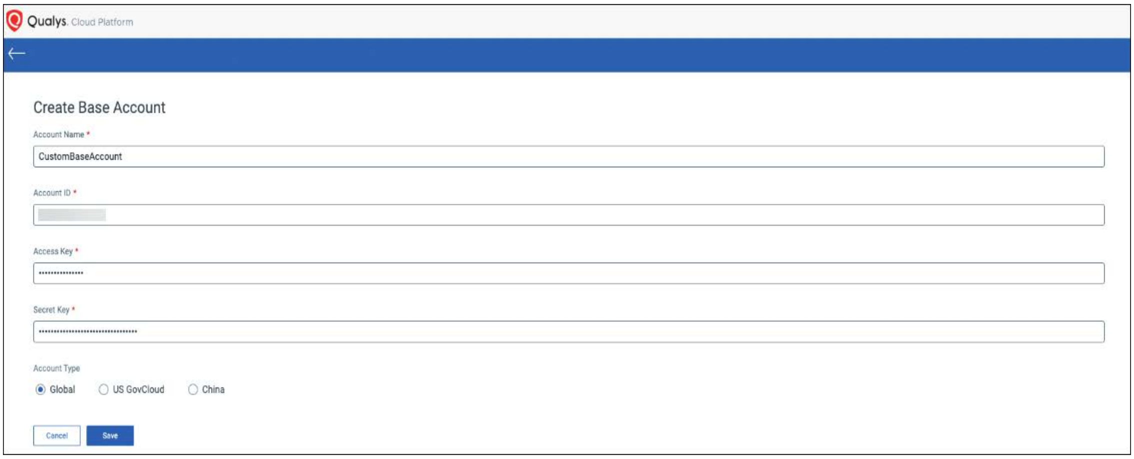
9) Click **Next:Tags** > **Next:Review** > **Create user**.

10) Copy the Access Key Id and Secret access key for later use. Click **Close**.

Base Account Configuration at Connectors Application

1) At the Qualys console, navigate to **Connectors Application > Amazon Web Services Connectors > Base Account**.

2) Paste the Access Key Id and Secret access key for the user that was created as part of AWS configuration and click **Save**.



Create Base Account

Account Name *
CustomBaseAccount

Account ID *
[redacted]

Access Key *
•••••••••••••••

Secret Key *
••••••••••••••••••••••••••••••••••

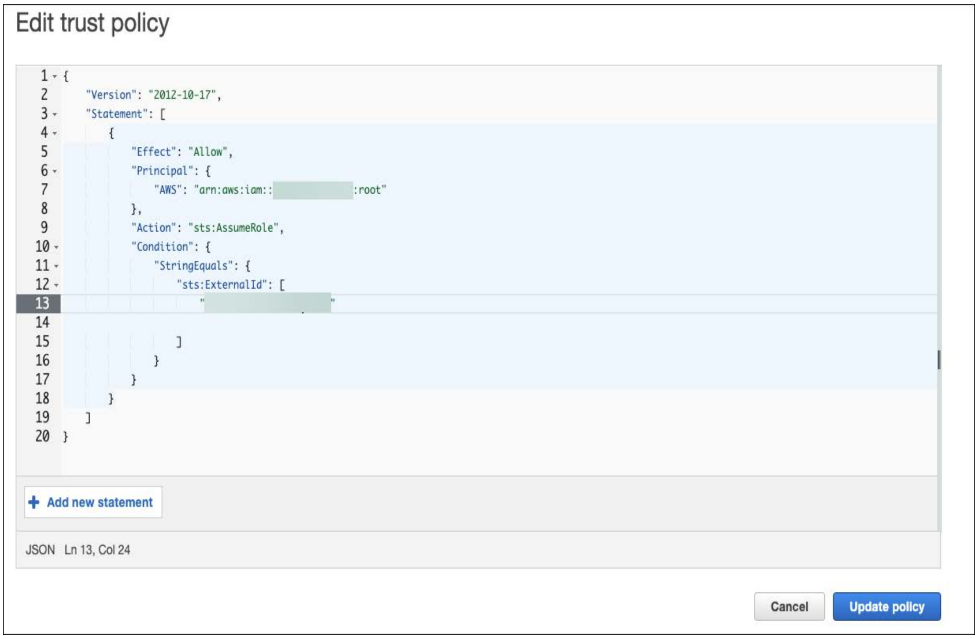
Account Type
● Global ○ US GovCloud ○ China

Using Custom Base Account to existing Connectors

1) To update the existing AWS connectors with cross-account role to base account usage, you need to create a base account using the steps mentioned as part of **Create Custom Base Account**).

2) Navigate to **AWS > IAM > Role > Select the Connector Role**.

3) On the summary page, select **Trust relationships** > **Edit trust policy**.

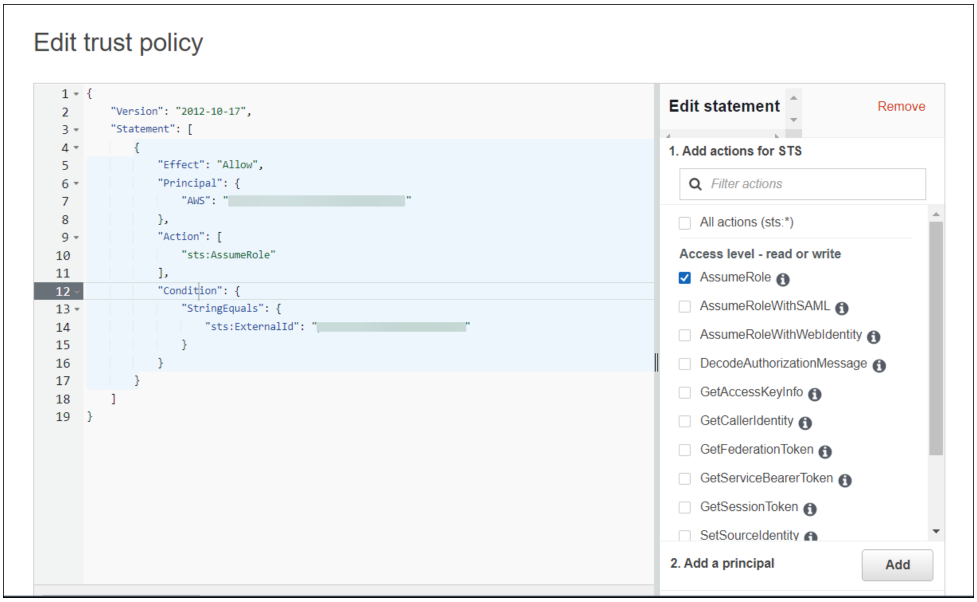


Edit trust policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::[redacted]:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "sts:ExternalId": [
                        "[redacted]"

                    ]
                }
            }
        }
    ]
}
```

4)Update the principal to use the custom base account.



Edit trust policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "[redacted]"
            },
            "Action": [
                "sts:AssumeRole"
            ],
            "Condition": {
                "StringEquals": {
                    "sts:ExternalId": "[redacted]"
                }
            }
        }
    ]
}
```

Edit statement Remove

1. Add actions for STS

Filter actions

□ All actions (sts:*)

Access level - read or write

☑ AssumeRole
□ AssumeRoleWithSAML
□ AssumeRoleWithWebIdentity
□ DecodeAuthorizationMessage
□ GetAccessKeyInfo
□ GetCallerIdentity
□ GetFederationToken
□ GetServiceBearerToken
□ GetSessionToken
□ SetSourceIdentity

2. Add a principal

5) Click **Update Policy**.

How does a Connector work?

Asset Discovery: The connector performs asset discovery for your cloud with its continuous synchronization mechanism. The connector synchronizes every 4 hours with the AWS account and pulls in all instances (including terminated instances).

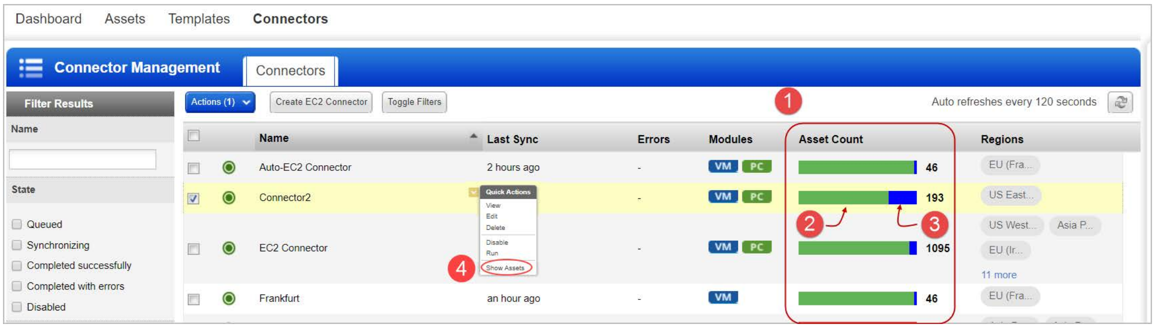
AWS retains the terminated instances for approximately one hour. However, Qualys stores record of all the terminated instances and you can always track the history and details of all such terminated instances.

Synchronization of Assets: Adds the assets to your Qualys account. Except for assets with errors (as such assets are dropped off), all other assets are added to the Qualys account.

Activation: When you plan to execute a scan using scanner appliances, you need to activate Vulnerability Management/Policy Compliance/Security Configuration Assessment licenses for the assets you added to your Qualys account. You can manually activate the assets or enable automatic activation during the connector setup.

Excluded from Activation: Apart from the terminated instances that are excluded from activation, m1.small, t1.micro, t2.nano or t3.nano instances are also excluded from activation. Please reach out to your Technical Account Manager or Qualys Support to lift this limitation and allow assets with these instance types to be auto-activated based on the connector settings. Once activated, you can launch cloud perimeter scan for such instances. Alternately, you could use Cloud Agent on such instances.

Viewing Imported Assets



Name

State

- □ Queued
- □ Synchronizing
- □ Completed successfully
- □ Completed with errors
- □ Disabled

□		Name	Last Sync	Errors	Modules	Asset Count	Regions
□	●	Auto-EC2 Connector	2 hours ago	-	VM PC	46	EU (Fra...
☑	●	Connector2		-	VM PC	193	US East...
□	●	EC2 Connector		-	VM PC	1095	US West... Asia P... EU (Ir... 11 more
□	●	Frankfurt	an hour ago	-	VM	46	EU (Fra...

The connector start pulling the instances once you finish the connector creation. Let's check out the different information we display once the connector run is complete.

1 **Asset Count** - The Asset count column shows the assets discovered and synchronized in the latest connector run.

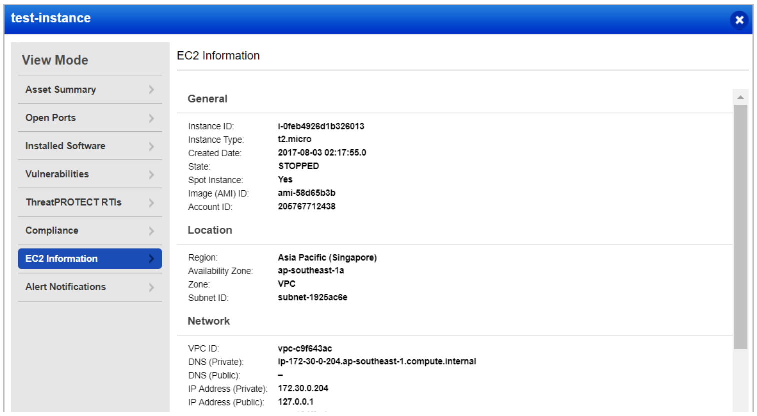
2 **Synchronized Assets** - In the Asset count column, the green portion represents assets synchronized. Synchronized count represents assets that are successfully processed at Qualys.

3 **Excluded Assets** - The blue portion represents the assets which are synchronized but excluded from VM/PC/SCA activation. Excluded assets could be terminated instances or m1.small, t1.micro, t2.nano or t3.nano which cannot be scanned by Qualys scanners. Please reach out to your Technical Account Manager or Qualys Support to lift this limitation and allow assets with these instance types to be auto-activated based on the connector settings. Once activated, you can launch cloud perimeter scan for such instances (m1.small, t1.micro, t2.nano or t3.nano). Excluded assets are subset of synchronized assets.

4 **Show assets** – The total count of assets discovered by the connector over its span of time.

Assets with Error - The Asset count column may also show a portion in red which represents assets with errors. Assets with errors are those which have encountered issues while being processed at Qualys.

You can view the assets that are collected by connector by navigating to AssetView. The EC2 Information tab of Asset details page displays the AWS instance metadata collected. Here is the sample screen shot that displays the information we collect.



EC2 Information

General

Instance ID:	i-0feb4926d1b326013
Instance Type:	t2.micro
Created Date:	2017-08-03 02:17:55.0
State:	STOPPED
Spot Instance:	Yes
Image (AMI) ID:	ami-58d65b3b
Account ID:	205767712438

Location

Region:	Asia Pacific (Singapore)
Availability Zone:	ap-southeast-1a
Zone:	VPC
Subnet ID:	subnet-1925ac6e

Network

VPC ID:	vpc-c9f643ac
DNS (Private):	ip-172-30-0-204.ap-southeast-1.compute.internal
DNS (Public):	–
IP Address (Private):	172.30.0.204
IP Address (Public):	127.0.0.1

Once the EC2 instances are discovered, you are ready to start scanning and securing your Amazon EC2 infrastructure!

AWS Metadata

This section provides information on cloud provider metadata provided by Qualys Cloud Agent, AssetView Connector and Qualys Scanner

AssetView Connector and Cloud Agent

General:

- Reservation ID

- Instance ID

- Instance Type

- Created Date

- Image (AMI) ID

- Account ID

- Instance State (Only Running for QCA data collection)

Location:

- Region

- Availability Zone

- Zone

Network:

- VPC ID

- DNS (Private)

- DNS (Public)

- Local Hostname

- MAC Address

- Subnet ID

- Security Groups

- Security Groups IDs

- IP Address (Private)

- IP Address (Public)

AssetView Connector Only

- AWS Tags

- Instance State Updates (Stopped, Terminated, ...)

QID - 370098 Amazon EC2 Linux Instance Metadata

metadata/

- AMI ID

- AMI Launch Index

- AMI Manifest Path

- Hostname

- Instance Action

- Instance ID

- Instance Type

- Kernel ID

- Local Hostname
- Local Ipv4
- MAC
- Public Hostname
- Public Ipv4
- Reservation ID
- Security Groups
- Ancestor AMI Ids
- Profile

dynamic/instance-identity/document/

- accountId
- availabilityZone
- kernelId
- ramdiskId
- pendingTime
- architecture
- privateIp
- devpayProductCodes
- version
- billingProducts
- instanceId
- imageId
- instanceType
- region

AWS APIs used by EC2 Connector to discover assets

Qualys uses three APIs to discover EC2 instances and identify additional information about those instances from an AWS account. Information about these APIs is available on the Amazon AWS web site locations mentioned below.

DescribeInstances API

https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_DescribeInstances.html

DescribeImages API

https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_DescribeImages.html

DescribeNetworkInterfaces API

https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_DescribeNetworkInterfaces.html

The Discovery job can be run on demand or with the default frequency (every 4 hours). This frequency is currently not configurable.

Qualys APIs for EC2 Connectors

You can perform various EC2 connector operations through API as well. For detailed information on using Qualys APIs related to AWS, see the Asset Management and Tagging API v2 User Guide.

Here are some useful EC2 connector APIs:

Create AWS Connector

https://qualysapi.qualys.com/qps/rest/3.0/create/am/awsassetdataconnector

Run Connector

https://qualysapi.qualys.com/qps/rest/3.0/run/am/assetdataconnector/<id>

Get Host Asset Info (get the metadata of an EC2 instance)

https://qualysapi.qualys.com/qps/rest/2.0/get/am/hostasset/<id>

Scanning in AWS EC2 Environments

Let us get familiar with few terms in networking basics.

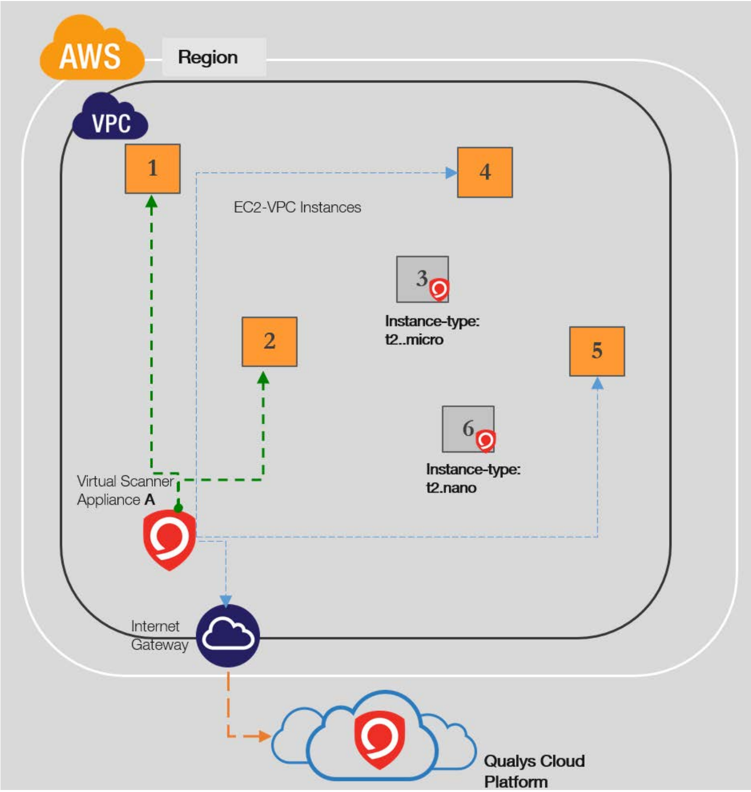
VPC: enables you to launch AWS resources into a virtual network that you've defined. This closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalability of AWS.

VPC Peering: a networking connection between two VPCs that enables you to route traffic between them.

Transit Gateway: A network transit hub, which you can use to interconnect your virtual private clouds (VPC) and on-premises networks.

Let us now see the various scenarios for scanning in AWS EC2 environment.

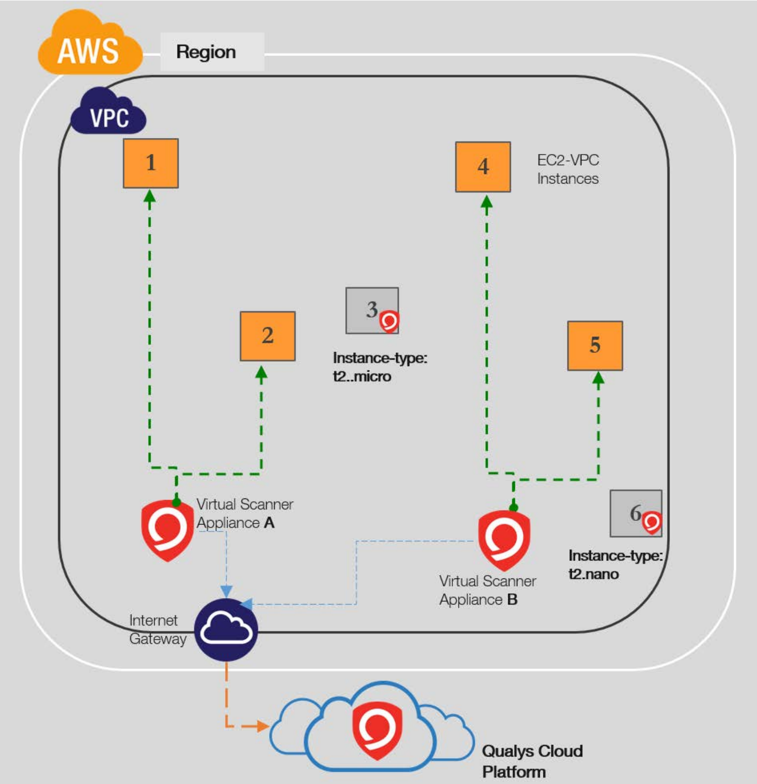
A Single scanner scans MULTIPLE instances in a VPC



Scanners needs to be configured to communicate to Qualys Cloud Platform and AWS EC2 & STS endpoints over https (via security groups and internet gateways)

AWS recommends excluding the following EC2 instance types (T3.nano, T2.nano, T1.micro and M1.small) from your security assessments to minimize potential disruption to your environment.Cloud-agents are preferred method for scanning them.

Multiple scanners to scan MULTIPLE instances in VPC

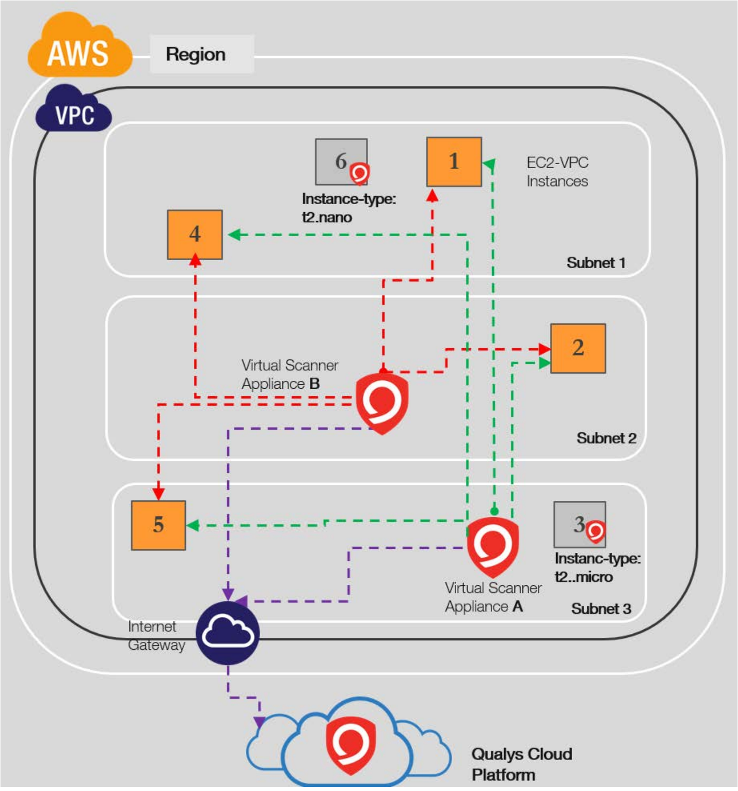


Based on number of instances and scan frequency, multiple scanners might be required to scan MULTIPLE instances in a VPC. Require at least one scanner per VPC. You can add more based on requirements.

Scanners needs to be configured to communicate to Qualys Cloud Platform and AWS EC2 & STS endpoints (via security groups and internet gateways)

AWS recommends excluding the following EC2 instance types (T3.nano, T2.nano, T1.micro and M1.small) from your security assessments to minimize potential disruption to your environment. Cloud-agents are preferred method for scanning them.

A Single scanner scans MULTIPLE instances across the subnets within a VPC

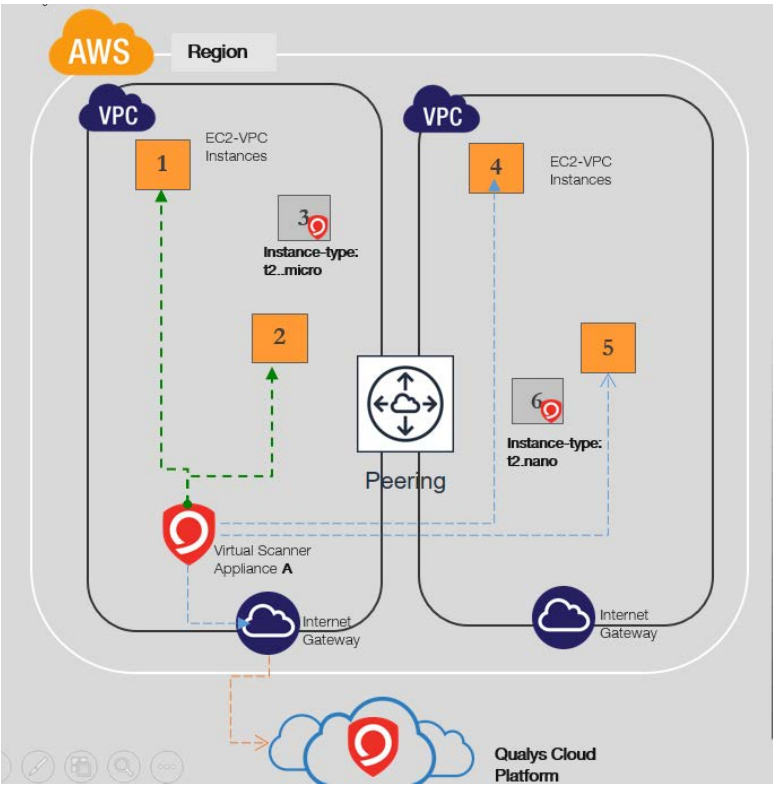


Scanners can typically work across the subnets within a VPC, unless there are restrictions in networks introduced

Scanners needs to be configured to communicate to Qualys Cloud Platform and AWS EC2 & STS endpoints over https (via security groups or internet gateways)

AWS recommends excluding the following EC2 instance types (T3.nano, T2.nano, T1.micro and M1.small) from your security assessments to minimize potential disruption to your environment. Cloud-agents are preferred method for scanning them.

A Single scanner scans MULTIPLE instances across Peered VPCs in a region

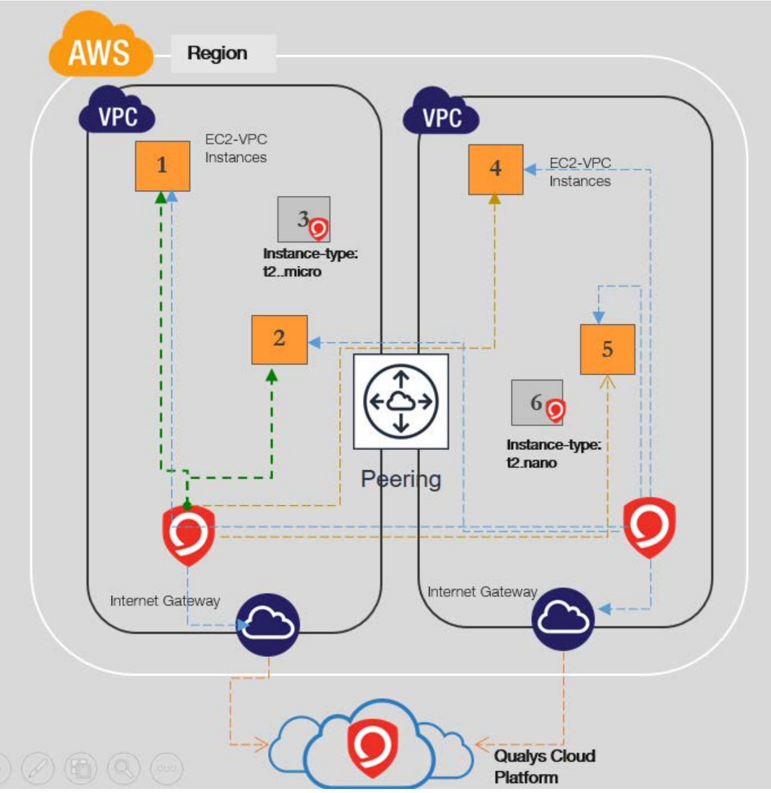


You can add more based on requirements.

Scanners needs to be configured to communicate to Qualys Cloud Platform and AWS EC2 & STS endpoints over https (via security groups and internet gateways)

AWS recommends excluding the following EC2 instance types (T3.nano, T2.nano, T1.micro and M1.small) from your security assessments to minimize potential disruption to your environment. Cloud-agents are preferred method for scanning them.

Multiple scanners might be required to scan MULTIPLE instances across Peered VPCs

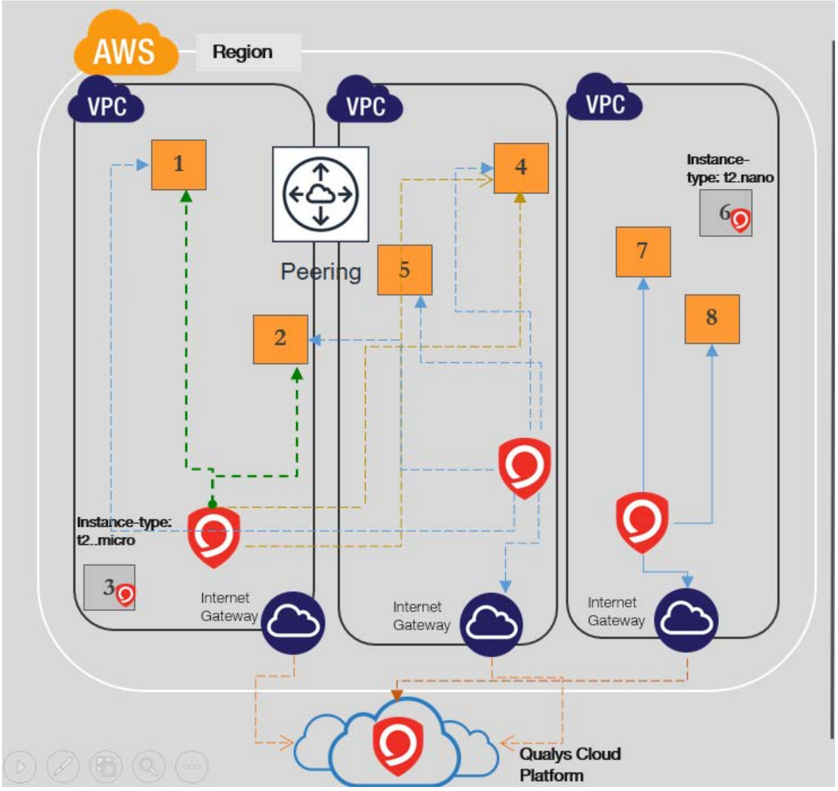


Based on number of instances and scan frequency, multiple scanners might be required to scan MULTIPLE instances across Peered VPCs in a region. You can add more based on requirements to ALLOW Scanning across VPC boundaries.

Scanners need to be configured to communicate to Qualys Cloud Platform and AWS EC2 & STS endpoints over https (via security groups and internet gateways).

AWS recommends excluding the following EC2 instance types (T3.nano, T2.nano, T1.micro and M1.small) from your security assessments to minimize potential disruption to your environment. Cloud-agents are preferred method for scanning them.

Scanner cannot scan instances in non-peered VPCs

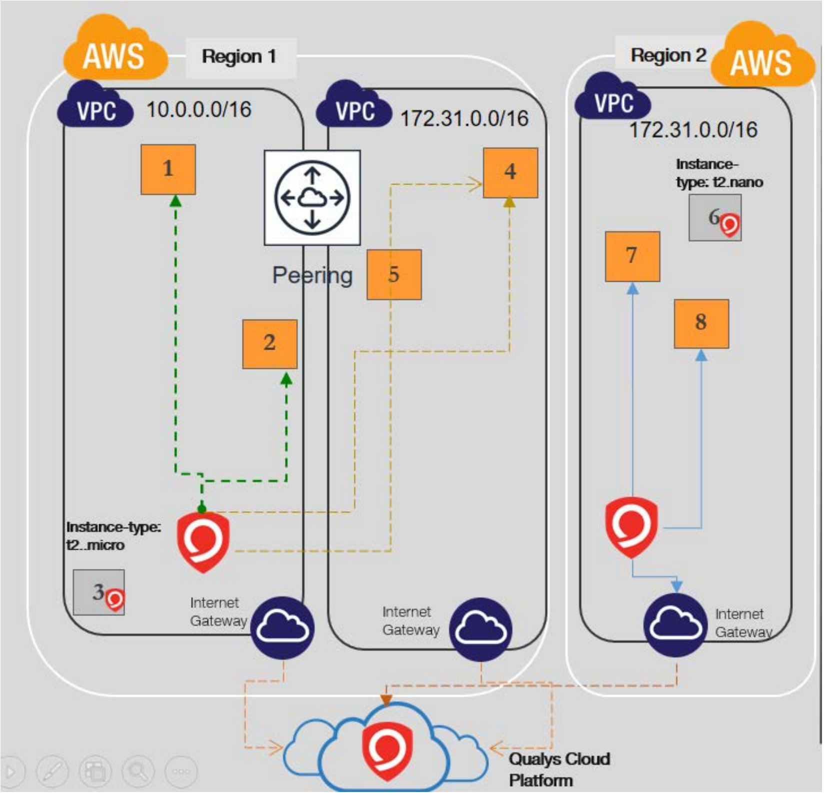


You can add more based on requirements to ALLOW Scanning across VPC boundaries.

Scanners needs to be configured to communicate to Qualys Cloud Platform and AWS EC2 & STS endpoints over https (via security groups and internet gateways)

AWS recommends excluding the following EC2 instance types (T3.nano, T2.nano, T1.micro and M1.small) from your security assessments to minimize potential disruption to your environment. Cloud-agents are preferred method for scanning them.

Scanner cannot scan instances in VPCs with overlapping IP addresses



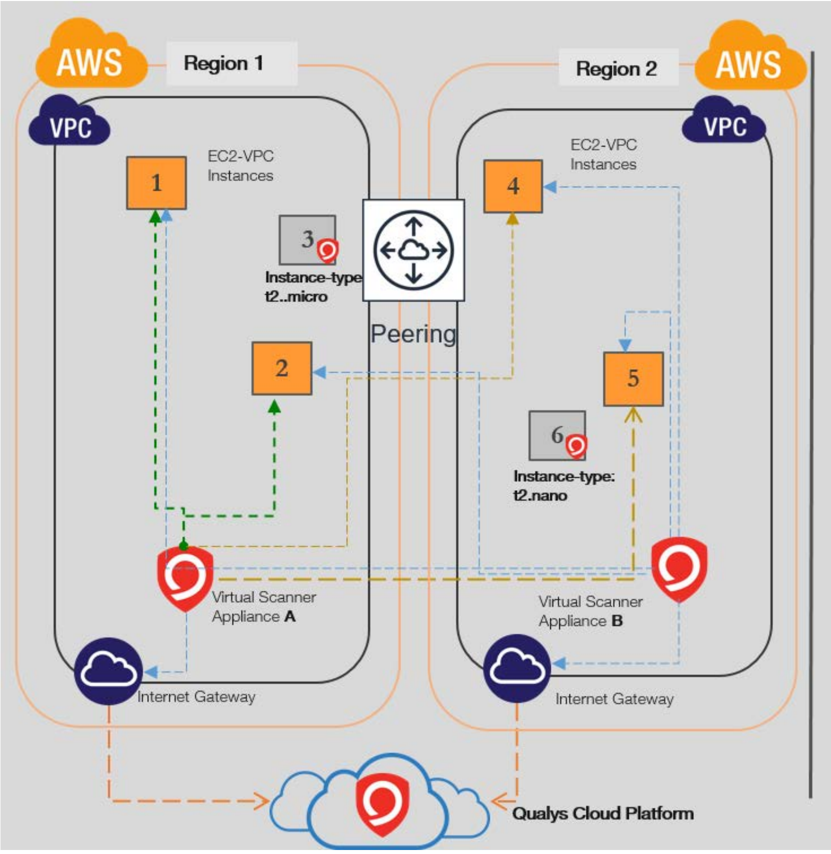
A single scanner cannot scan instances in VPCs with overlapping IP addresses due to reachability to a single subnet. You can add more based on requirements to ALLOW Scanning across VPC boundaries.

Note: Albeit VPC peering can be configured between VPC A & C, due to overlapping subnets between B & C, scanners will only reach one of them based on route table.

Scanners need to be configured to communicate to Qualys Cloud Platform and AWS EC2 & STS endpoints over https (via security groups and internet gateways).

AWS recommends excluding the following EC2 instance types (T3.nano, T2.nano, T1.micro and M1.small) from your security assessments to minimize potential disruption to your environment. Cloud-agents are preferred method for scanning them.

Single scanner scans MULTIPLE instances across Peered VPCs in different regions

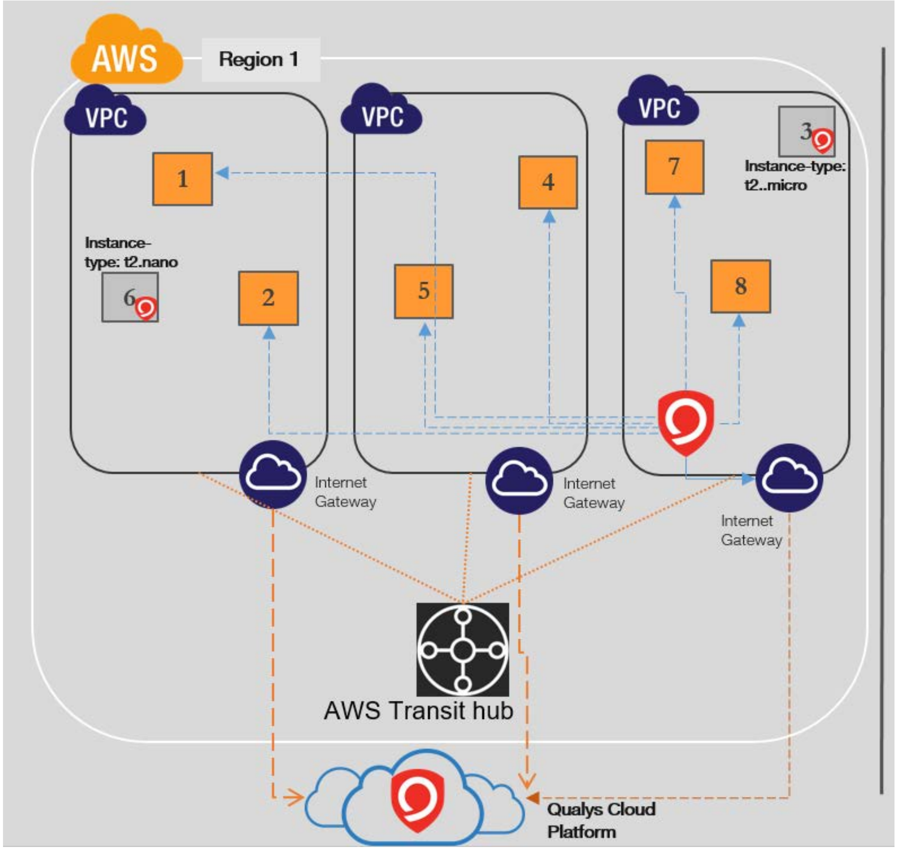


You can add more scanners based on requirements to ALLOW Scanning across Region across VPC boundaries.

Scanners needs to be configured to communicate to Qualys Cloud Platform and AWS EC2 & STS endpoints over https (via security groups and internet gateways)

AWS recommends excluding the following EC2 instance types (T3.nano, T2.nano, T1.micro and M1.small) from your security assessments to minimize potential disruption to your environment. Cloud-agents are preferred method for scanning them.

Single scanner scans multiple instances across VPCs in region connected by Transit

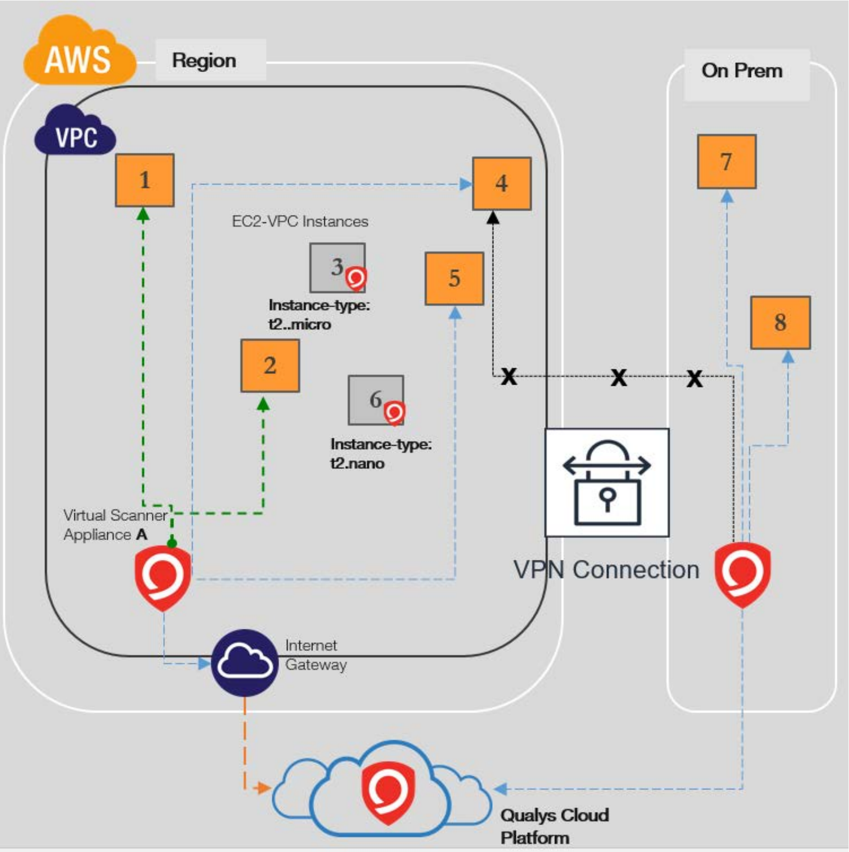


Since a network transit hub allows interconnectivity between virtual private clouds (VPC), a single scanner can be used to scan multiple instances across VPCs in a region connected by Transit gateway.

Scanners needs to be configured to communicate to Qualys Cloud Platform and AWS EC2 & STS endpoints over https (via security groups and internet gateways)

AWS recommends excluding the following EC2 instance types (T3.nano, T2.nano, T1.micro and M1.small) from your security assessments to minimize potential disruption to your environment. Cloud-agents are preferred method for scanning them.

On-premises Scanners not recommended for scans of Cloud Instances



Scanners needs to be configured to communicate to Qualys Cloud Platform and AWS EC2 & STS endpoints over https (via security groups and internet gateways)

Scanners residing on your on-prem network should not be used to scan your cloud instances as they are not cloud aware and has traditional workflow for scanning.

Instance types of t2.micro and t2.nano will NOT be scanned as per AWS pen testing rules. Cloud-agents are preferred method for scanning them.

Deploy Sensors

Qualys sensors, a core service of the Qualys Cloud Platform, make it easy to extend your security throughout your global enterprise. These sensors are remotely deployable, centrally managed and self-updating. They collect the data and automatically beam it up to the Qualys Cloud Platform, which has the computing power to continuously analyze and correlate the information in order to help you identify threats and eliminate vulnerabilities. For AWS, the sensors come as virtual appliances in the form of AMI & lightweight agents.

Prior to scan, you need to deploy sensors. Depending on your preference, you could deploy virtual scanner appliance or Qualys Cloud Agent. Let's go through the steps involved in deploying these sensors.

Deploying Virtual Scanner Appliance
Deploying Qualys Cloud Agent

Deploying Virtual Scanner Appliance

Before we go through the actual steps involved in the virtual scanner deployment let's understand the licensing/cost aspect and the deployment recommendations.

Cost and Licenses

Qualys Virtual Scanner Appliance is available as an Amazon Machine Image (AMI) at AWS Marketplace, ready for customers to launch onto Amazon EC2-Classic and EC2-VPC.

There are two aspects to consider:

- Qualys costs for the virtual scanner license subscription

- AWS costs for the computing resources to run the appliance as an EC2 Instance

Qualys Cost

You will need to acquire a Qualys license for each virtual scanner appliance Instance you would like to run. This license is acquired from Qualys, not from AWS, and our scanner appliances are listed at AWS Marketplace with a BYOL (i.e., "bring your own license") model accordingly. Each Qualys Virtual Scanner Appliance profile that you define in the Qualys Cloud Platform UI will consume a single virtual scanner appliance license. If you delete a virtual scanner appliance profile from your Qualys subscription, that license is freed up and immediately available for re-use.

Contact your Qualys technical account manager or Qualys reseller for a pricing quotation or to request an evaluation.

AWS Cost

Each virtual scanner appliance Instance will be launched into one of your own AWS accounts. You will be responsible for paying AWS for the costs of running the appliance.

Those costs include:

- Compute Capacity based upon instances type
- Storage
- Data transfer IN/OUT

The compute capacity charges (i.e., CPU, RAM) are overwhelmingly the largest part of the costs to run an Instance. Note that you are not required to keep your scanner appliance(s) running at all times. Any hours during which your Instance is Stopped will incur only per-GB provisioned storage charges. However, scanners should be turned on for at least several hours per week in order to ensure that they stay up-to-date with software and signatures.

Deployment recommendations for scanner

Following are some recommendations from Qualys for deploying scanners based on the network topology and the size of the EC2 instance for hosting the scanner appliance.

Instance size for hosting the scanner

To host the Qualys Virtual Scanner Appliance, the maximum supported size for a scanner instance by Qualys is 8 CPUs and 16 GB RAM. In addition, we do not support scanner deployment on ARM-based architecture instance types such as A1, c6g, m6g, t4g, and r6g instance families. Based on the number of EC2 instances being scanned, and the number of times the instances are scanned, you can scale up to 8 CPUs and 16 GB RAM.

To select an instance type based on its scanning capacity (applicable only to versions up to 2.7.45), refer to https://success.qualys.com/discussions/s/article/000006880.

To learn more about the scanner appliance capacity required for various scan jobs, refer to https://success.qualys.com/support/s/article/000003491.

Support for ENA instances

Qualys Virtual Scanner Appliance can also be deployed on instance types that support enhanced networking (ENA) and NVMe SSD Volumes. Please refer to the following table for networking and storage features supported by AWS in their current generation instance types:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-types.html#instance-type-summary-table

Please note that Qualys Virtual Scanner Appliance can only be deployed on instance types that have a maximum of 16 CPUs and 16 GB RAM.

Limitations on scanning targets

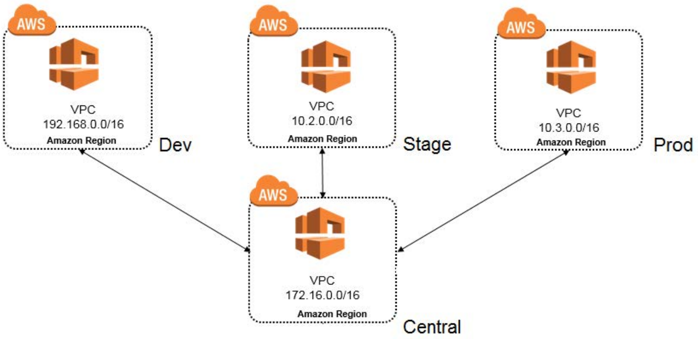
Scans cannot be launched on targets using t1.micro, m1.small, t2.nano instance types.

Scanner placement based on the network topology

Amazon Virtual Private Cloud (Amazon VPC) offers a comprehensive set of virtual networking capabilities that provide AWS customers with many options for designing and implementing networks on the AWS cloud. With Amazon VPC, customers can provision logically isolated virtual networks to host their AWS resources. Based upon how you have setup you AWS network, here are some recommendations on how you can place your scanner.

- Non peered VPCs in a region - Qualys recommends to have one or more scanners per VPC per region if the VPCs are non peered.

- Peered VPCs in a region - you can have one or more scanners in the central VPC which is peered to other VPC in a region (hub 'n' spoke model). Here is an example for the same.



- VPCs across regions - you can have one or more scanners in a VPC which has VPN or VPC-transit to other regions.

Instance Snapshots/Cloning Not Allowed

Using a snapshot or clone of a virtual scanner instance to create a new instance is strictly prohibited. The new instance will not function as a scanner. All configuration settings and platform registration information will be lost. This could also lead to scans failing and errors for the original scanner.

Moving/Exporting Instance Not Allowed

Moving or exporting a registered scanner instance from a virtualization platform (HyperV, VMware, XenServer) in any file format to the AWS cloud platform is strictly prohibited. This will break scanner functionality & the scanner will permanently lose all its settings.

What do I need?

The Virtual Scanner option must be turned on for your account. Contact Qualys Support or your Technical Account Manager if you would like us to turn on this option for you.

You must be a Manager or a sub-user with the “Manage virtual scanner appliances” permission. This permission may be granted to Unit Managers. Your subscription may be configured to allow this permission to be granted to Scanners.

Scanner Deployment

The scanner deployment involves configuration in Qualys as well as AWS.

Some things to consider...

The following features are not supported and are disabled in all cloud (private and public) platforms:

- WAN/Split network SETTINGS - “WAN Interface” option for split network settings is not available from Scanner UI/console. Only LAN/single network settings from Cloud UI, used for both scanning and connecting to Qualys servers, are supported

- NATIVE VLAN - “VLAN on LAN” option for configuring Native VLAN is not available from scanner UI/console

- STATIC VLAN (IPV4 AND IPV6) - "VLANs" option for configuring static VLANs is not available from Qualys UI

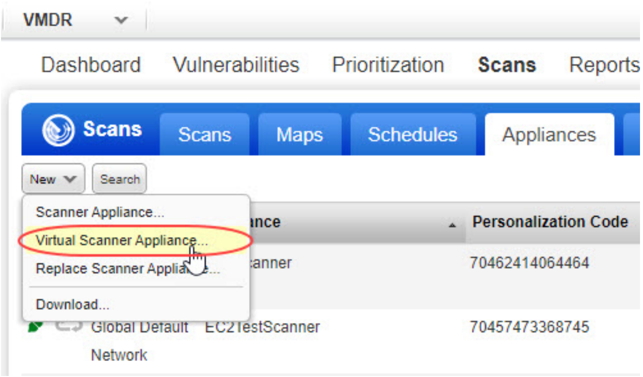
- STATIC ROUTES (IPV4 AND IPV6) - Option to configure “Static Routes” is not available from Qualys UI

- IPV6 ON LAN - Option to configure “IPv6 on LAN” is not available from Qualys UI

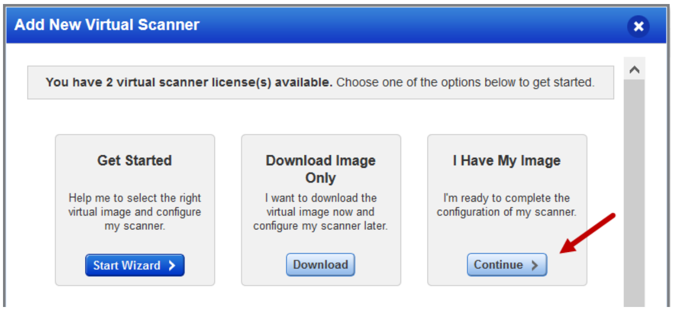
Configuration in Qualys

Setting up Virtual Appliance - Get Personalization Code

Select VM/VMDR or PC from the Qualys app picker. Then navigate to Scans > Appliances and select New > Virtual Scanner Appliance.



Choose “I have My Image” and click Continue.



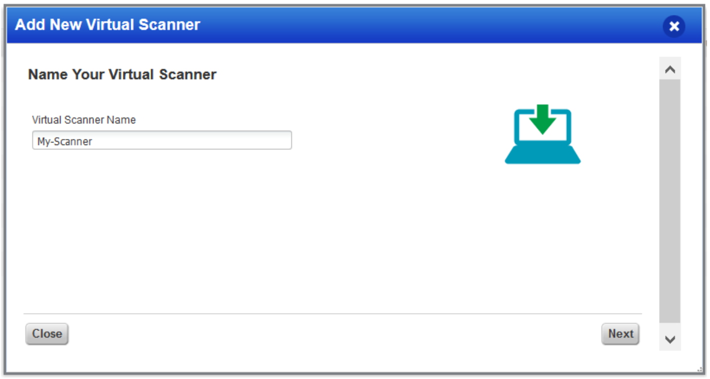
You have 2 virtual scanner license(s) available. Choose one of the options below to get started.

Get Started
Help me to select the right virtual image and configure my scanner.
Start Wizard

Download Image Only
I want to download the virtual image now and configure my scanner later.
Download

I Have My Image
I'm ready to complete the configuration of my scanner.
Continue

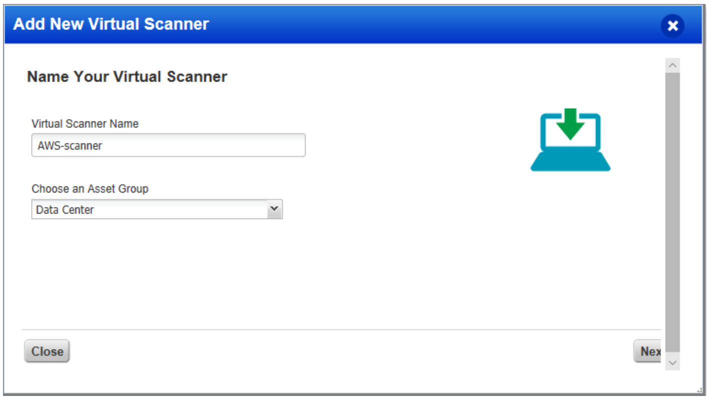
Provide a name and click Next.



Name Your Virtual Scanner

Virtual Scanner Name: My-Scanner

If you’re a sub-user then you’ll need to pick an asset group that has been assigned to your business unit by a Manager user. Not seeing any asset groups? Please ask a Manager to assign an asset group (other than the All group) to your business unit.

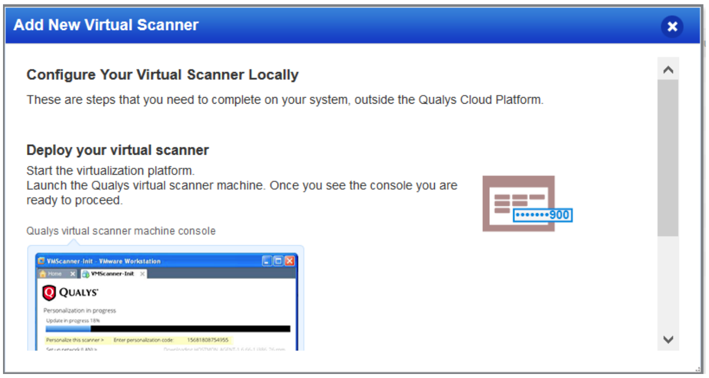


Name Your Virtual Scanner

Virtual Scanner Name: AWS-scanner

Choose an Asset Group: Data Center

Follow the on-screen instructions to configure your virtual scanner. Click Next.



Configure Your Virtual Scanner Locally

These are steps that you need to complete on your system, outside the Qualys Cloud Platform.

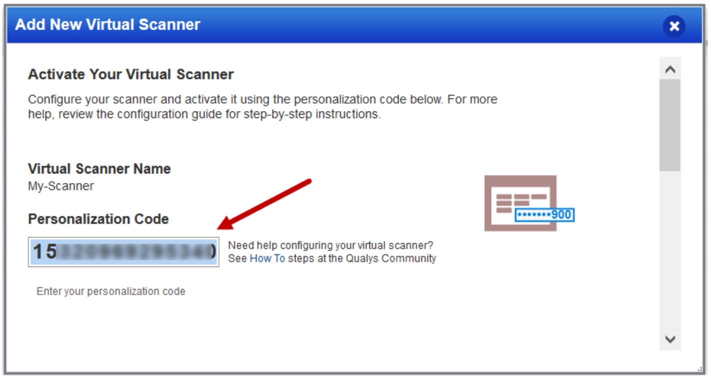
Deploy your virtual scanner

Start the virtualization platform.
Launch the Qualys virtual scanner machine. Once you see the console you are ready to proceed.

Qualys virtual scanner machine console

Personalization in progress
Update in progress 18%
Personalize this scanner > Enter personalization code: 15681808754955

Get your personalization code. You'll need this to launch your AMI instance.



Add New Virtual Scanner

Activate Your Virtual Scanner

Configure your scanner and activate it using the personalization code below. For more help, review the configuration guide for step-by-step instructions.

Virtual Scanner Name
My-Scanner

Personalization Code
15[redacted]

Need help configuring your virtual scanner?
See How To steps at the Qualys Community

Enter your personalization code

Configuration in AWS

Launch an AMI instance in the Amazon AWS

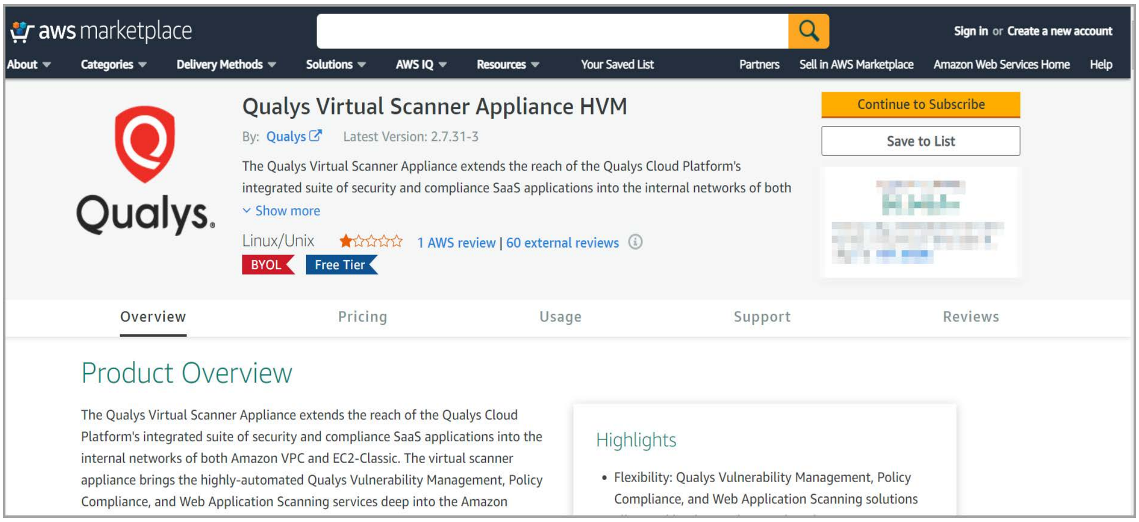
Qualys virtual scanners can be launched from the AWS marketplace or from a custom AMI that has been shared with your AWS account. You can also launch an AMI instance using the AWS Management Console (i.e. sign in to the console, go to Services > EC2 and enter AMI settings per below).

1) Deploy the Qualys Virtual Scanner Appliance.

To Launch from the AWS Marketplace

Go to Qualys Virtual Scanner Appliance page at AWS Marketplace and login to your AWS account.

Qualys Virtual Scanner Appliance HVM on AWS Marketplace



Qualys Virtual Scanner Appliance HVM

By: Qualys Latest Version: 2.7.31-3

The Qualys Virtual Scanner Appliance extends the reach of the Qualys Cloud Platform's integrated suite of security and compliance SaaS applications into the internal networks of both

Show more

Linux/Unix ★☆☆☆☆ 1 AWS review | 60 external reviews

BYOL Free Tier

Product Overview

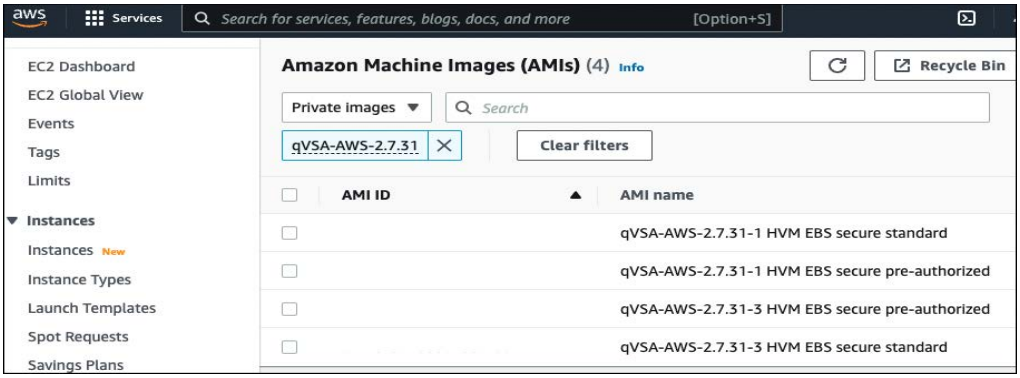
The Qualys Virtual Scanner Appliance extends the reach of the Qualys Cloud Platform's integrated suite of security and compliance SaaS applications into the internal networks of both Amazon VPC and EC2-Classic. The virtual scanner appliance brings the highly-automated Qualys Vulnerability Management, Policy Compliance, and Web Application Scanning services deep into the Amazon

Highlights

- Flexibility: Qualys Vulnerability Management, Policy Compliance, and Web Application Scanning solutions

To Launch Custom AMI from AWS Console

To launch from a custom AMI that has been shared with your AWS account, login to your AWS console and go to Images - AMI – Private Images – enter ‘qVSA’ in the search box and you should see all Qualys virtual scanner images shared with your account:



Amazon Machine Images (AMIs) (4) Info

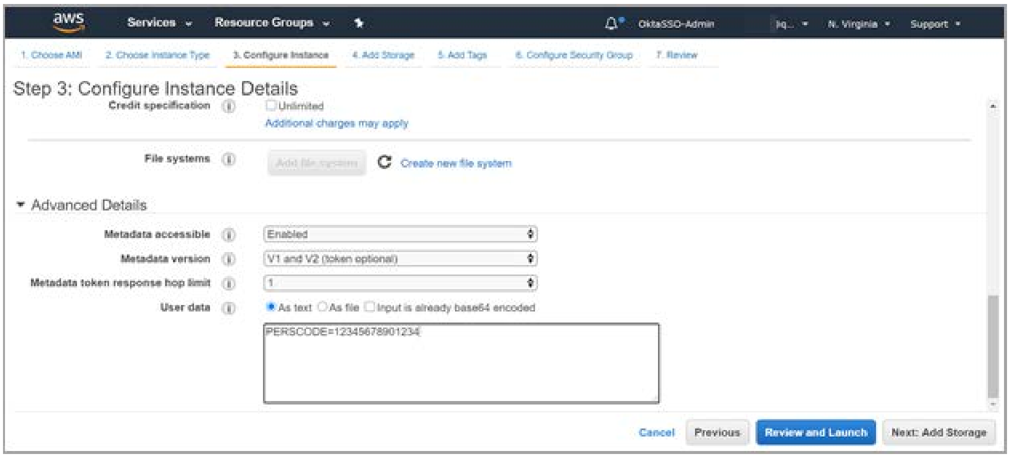
Private images ▼ | Search

qVSA-AWS-2.7.31 ✕

□	AMI ID ▲	AMI name
□		qVSA-AWS-2.7.31-1 HVM EBS secure standard
□		qVSA-AWS-2.7.31-1 HVM EBS secure pre-authorized
□		qVSA-AWS-2.7.31-3 HVM EBS secure pre-authorized
□		qVSA-AWS-2.7.31-3 HVM EBS secure standard

2) Launch the virtual scanner AMI in a region.

3)Use the wizard to enter AMI settings. Qualys now also supports V2(token required) version. In the Advance Details section, select Metadata version accordingly. So, in the User data field, you must enter the personalization code you obtained from the Qualys user interface and optionally proxy server (if used).



Step 3: Configure Instance Details

Credit specification: □ Unlimited
Additional charges may apply

File systems

Advanced Details

Metadata accessible: Enabled
Metadata version: V1 and V2 (token optional)
Metadata token response hop limit: 1
User data: ● As text ○ As file □ Input is already base64 encoded

```
PERSCODE=12345678901234
```

Personalization Code - Enter the personalization code that you obtained from Qualys preceded by PERSCODE=

Proxy Server (Optional) - Enter Proxy Server information, on a separate line from the personalization code, preceded by PROXY_URL. A proxy server is used when your scanner does not have direct connectivity to the Qualys Cloud Platform.

Enter proxy information in the format username:password@proxyhost:port
If you have a domain user, the format is domain\username:password@proxyhost:port
If authentication is not used, the format is proxyhost:port

where proxyhost is the IPv4 address or the FQDN of the proxy server, port is the port the proxy server is running on.

Example:

```
PERSCODE=12345678901234
PROXY_URL=jdoe:abc12345@10.40.1.123:3128
```

> If you use a proxy server, ensure that you configure the Amazon EC2 API Proxy server settings in Qualys UI. To know more refer to Define Amazon EC2 API Proxy settings in Qualys UI.

Deploy a Qualys Virtual Scanner Appliance in AWS cloud via cloud shell

The following AWS CLI command will create an instance in AWS cloud infrastructure. Please note that the “user-data” option is where PERSCODE and Proxy server configuration, if any, should be specified in base64 encoded format.

Use this command:

aws ec2 run-instances [OPTIONS]

Required Parameters:

--image-id (string)

The ID of the AMI. An AMI ID is required to launch an instance and must be specified here or in a launch template.

--instance-type (string)

The instance type. For more information, see Instance types in the Amazon EC2 User Guide

--key-name (string)

The name of the key pair. You can create a key pair using CreateKeyPair or ImportKeyPair .

NOTE:- If you do not specify a key pair, you can’t connect to the instance unless you choose an AMI that is configured to allow users another way to log in.

--security-group-ids (list)

The IDs of the security groups. You can create a security group using CreateSecurityGroup.

--subnet-id (string)

[EC2-VPC] The ID of the subnet to launch the instance into.

If you specify a network interface, you must specify any subnets as part of the network interface.

--user-data (string)

The user data script to make available to the instance. For more information, see Run commands on your Linux instance at launch and Run commands on your Windows instance at launch. If you are using a command line tool, base64-encoding is performed for you, and you can load the text from a file. Otherwise, you must provide base64-encoded text. User data is limited to 16 KB.

Example of launching a Qualys Scanner via AWS CLI:

```
aws ec2 run-instances --image-id ami-07581f2a1fbf34f4f --count 1 --instance-type t1.micro --key-name vScanner --subnet-id subnet-81e1e5da --security-group-ids sg-0e6a6c4c16488fd6f --user-data UEVSU0NPREU9MTIzNDU2Nzg5MDEyMzQKUFJPWFlfVVJMPWFiYzp4eWRAMS4xLjEuMTo4MDgw
```

More information regarding launching instances on AWS cloud infrastructure can be found here: https://awscli.amazonaws.com/v2/documentation/api/latest/reference/ec2/run-instances.html

Once launched, Virtual Appliance connects to Qualys Cloud Platform

This step registers the Virtual Scanner Appliance with your Qualys account. Also, your appliance will download all the latest software updates right away, so it's ready for scanning.

Configuring security groups for your Virtual Scanner Appliance

Setup following outbound rule in security group assigned to scanner appliance.

- Connectivity to Qualys Cloud Platform

The scanner appliance must have connectivity to Qualys Cloud Platform. If the scanner appliance has direct internet connectivity, ensure that the outbound rule allows access on port 443 to Qualys Security Operations Center (SOC) IP address. You can get the SOC IP address range by logging in to Qualys Portal and navigating to Help > About option. If you are using proxy server, ensure you have outbound rule that allows communication to proxy server and the proxy server can reach the Qualys Cloud Platform.

- Connectivity to Amazon EC2 API endpoints

The scanner appliance must have connectivity to the Amazon EC2 and STS API endpoints. For authorization, scanners must reach STS endpoints to assume role and get tokens to make EC2 API calls. The communication to the EC2 and STS API will not be routed through the proxy server that you may have configured for appliance management communications with the Qualys Cloud Platform (see above). The scanner appliance must communicate directly to the EC2 and STS API or through a fully transparent proxy or filtering technology.

If the scanner appliance has direct internet connectivity, ensure that the outbound rule allows access on port 443 to Amazon EC2 and STS API endpoints. If you have configured Amazon EC2 API proxy server in Qualys UI then ensure you have outbound rule that allows communication to proxy server and proxy server can reach Amazon EC2 API endpoints.

The scanner appliance must have connectivity to the Amazon EC2 API endpoints. If the appliance cannot reach the Amazon EC2 API endpoint, then any EC2 Scan job you initiate will not be able to succeed. Your scan will conclude without scanning any of the EC2 instance targets, because the appliance will not be able to resolve the list of target instance IDs to IP addresses with potential error "No Hosts alive".

Go here to learn about regions & endpoints:
http://docs.aws.amazon.com/general/latest/gr/rande.html#ec2_region

- Connectivity to target instances

Scanner should be able to reach out to all the target instances for running the scan. It is recommended to configure outbound rule that allows access to all ports and subnets of the EC2 instances that the scanner is going to scan.

Support for Qualys Private Cloud Platform

If you are using Qualys Private Cloud Platform (PCP) to scan EC2 instances, please contact your Qualys Sales representative (TAM) or Support to generate a Virtual Scanner Appliance AMI for AWS. Provide the following information:

- The AWS regions in which you want to deploy the scanner appliance

- The AWS account you want to use for scanner deployment

Ensure that the security groups allow communication from the scanner appliance to your Qualys PCP on port 443. You may need to provide the IP address of your Qualys PCP to Support.

Deploying Qualys Cloud Agent

Using our revolutionary Qualys Cloud Agent platform you can deploy lightweight cloud agents to continuously assess your AWS infrastructure for security and compliance.

Cloud Agent features

- Communicates to the Qualys Cloud Platform over port 443 and supports Proxy configurations.

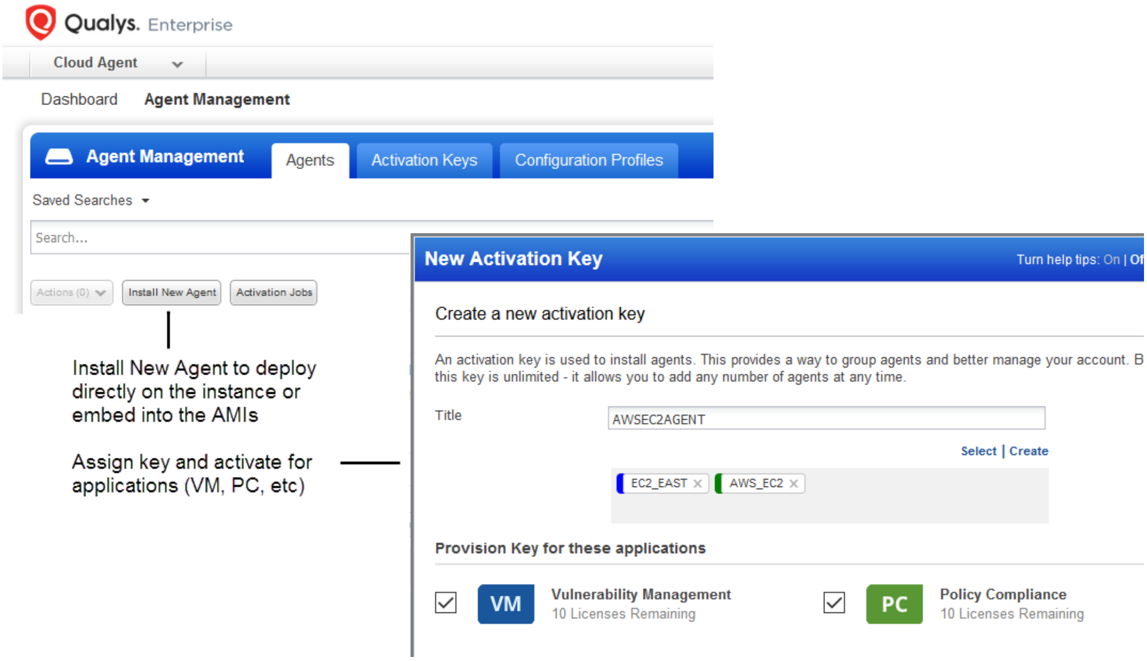
- Deployable directly on the EC2 instances or embed in the AMIs. Works well for cloud burst and ephemeral instances

- Supports scanning a range of Linux and Windows OS versions

- Supports scanning EC2 instance OS vulnerabilities

What are the steps?

Navigate to the Cloud Agent (CA) app and install the Cloud Agent in minutes.



Create a new activation key

An activation key is used to install agents. This provides a way to group agents and better manage your account. B
this key is unlimited - it allows you to add any number of agents at any time.

Title: AWSEC2AGENT

Select | Create

EC2_EAST × AWS_EC2 ×

Provision Key for these applications

☑ VM Vulnerability Management
10 Licenses Remaining

☑ PC Policy Compliance
10 Licenses Remaining

Install New Agent to deploy directly on the instance or embed into the AMIs

Assign key and activate for applications (VM, PC, etc)

We recommend these resources

Qualys Cloud Platform

Qualys Cloud Agent Getting Started Guide

Scan Assets

We will see the steps to scan your network. Before you initiate your scan, you must ensure few check points/pre-configurations.

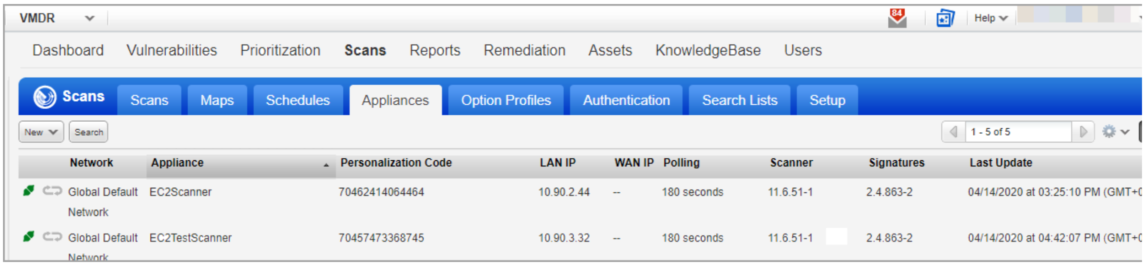
EC2 Scan checklist

Go to Qualys VM/VMDR or Qualys PC - We recommend these steps before scanning.

- Check Appliance Status
- Define Amazon EC2 API Proxy settings in Qualys UI (only if you've defined Proxy Server)
- Check EC2 Assets are activated
- Configure security groups for the EC2 instances to be scanned
- Configure OS Authentication

Check Appliance Status

Go to Scans > Appliances - Be sure the new Scanner Appliance is connected to the Qualys Cloud Platform. means your appliance is connected and ready for scanning.



Network	Appliance	Personalization Code	LAN IP	WAN IP	Polling	Scanner	Signatures	Last Update
Global Default Network	EC2Scanner	70462414064464	10.90.2.44	--	180 seconds	11.6.51-1	2.4.863-2	04/14/2020 at 03:25:10 PM (GMT+0
Global Default Network	EC2TestScanner	70457473368745	10.90.3.32	--	180 seconds	11.6.51-1	2.4.863-2	04/14/2020 at 04:42:07 PM (GMT+0

Define Amazon EC2 API Proxy settings in Qualys UI

This step is required if you have defined Proxy Server in User Data field during the virtual scanner deployment. Your EC2 scan won't work if you do not perform this step.

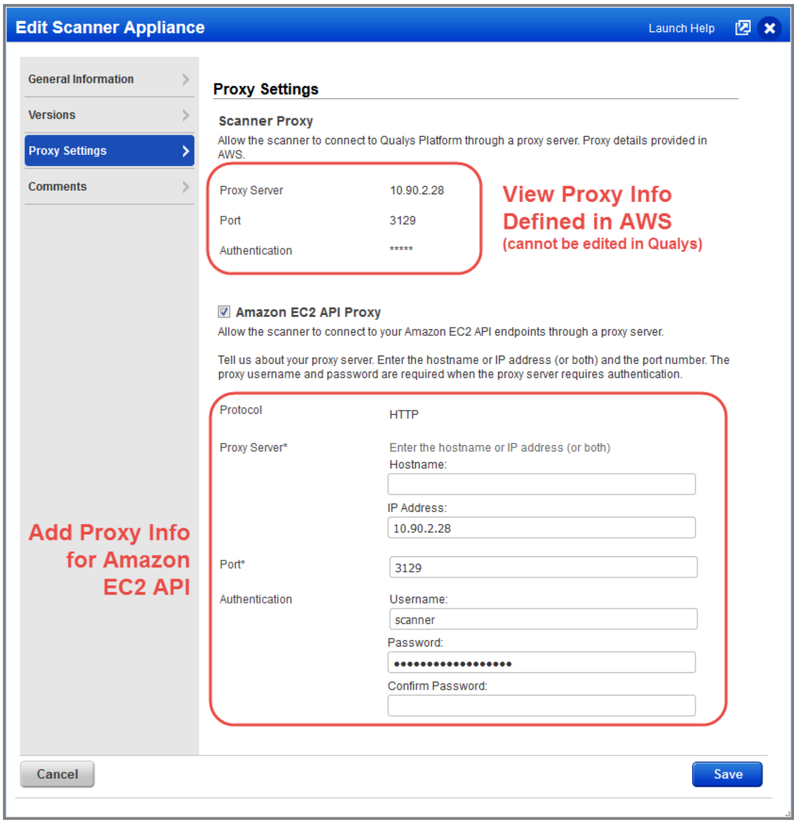
Go to Scans > Appliances - Edit your EC2 Virtual Scanner Appliance. Go to the Proxy Settings tab, select the Amazon EC2 API Proxy check box and tell us about your proxy server (i.e. hostname and/or IP address, port and proxy credentials (if required by the proxy server).

Good to Know - The settings you enter here allow the Virtual Appliance to connect to your Amazon EC2 API endpoints. The Virtual Appliance makes API calls to the AWS Gateway through the proxy server that you specify. For example, it calls the DescribeInstance API to get the current IP address for each EC2 instance you want to scan.

Sample Scanner Appliance Proxy Settings

You can view all proxy settings on the Scanner Appliance Information page. Just go to Scans > Appliances hover over your appliance and choose Info from the Quick Actions menu. Click Edit to make changes to the Amazon EC2 API Proxy settings.

The Scanner Proxy section shows Proxy Server info currently defined in AWS AMI settings (credentials are masked with ***) during its deployment.



Proxy Settings

Scanner Proxy

Allow the scanner to connect to Qualys Platform through a proxy server. Proxy details provided in AWS.

Proxy Server	10.90.2.28
Port	3129
Authentication	*****

View Proxy Info Defined in AWS
(cannot be edited in Qualys)

☑ Amazon EC2 API Proxy

Allow the scanner to connect to your Amazon EC2 API endpoints through a proxy server.

Tell us about your proxy server. Enter the hostname or IP address (or both) and the port number. The proxy username and password are required when the proxy server requires authentication.

Protocol: HTTP

Proxy Server*: Enter the hostname or IP address (or both)
Hostname:
IP Address: 10.90.2.28

Port*: 3129

Authentication: Username: scanner
Password: ••••••••••••••••••
Confirm Password:

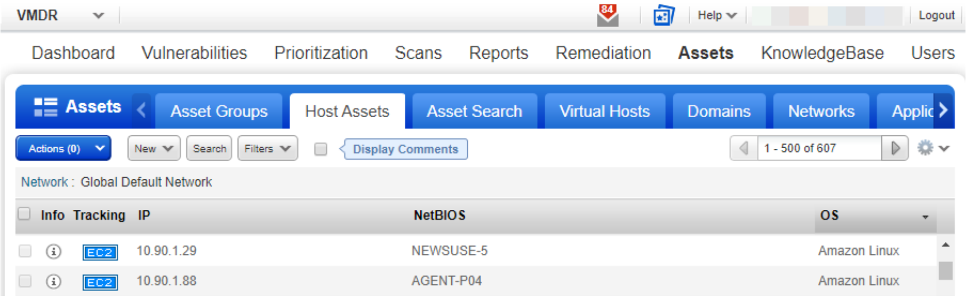
Add Proxy Info for Amazon EC2 API

You must allow the EC2 Region endpoints to be accessible via the proxy.

Identify the URL to an endpoint from here - http://docs.aws.amazon.com/general/latest/gr/rande.html#ec2_region

Check EC2 Assets are activated

Go to Assets > Host Assets or Qualys AssetView (AV) - Check that your EC2 hosts are activated. Activated assets are assigned the EC2 tracking method.



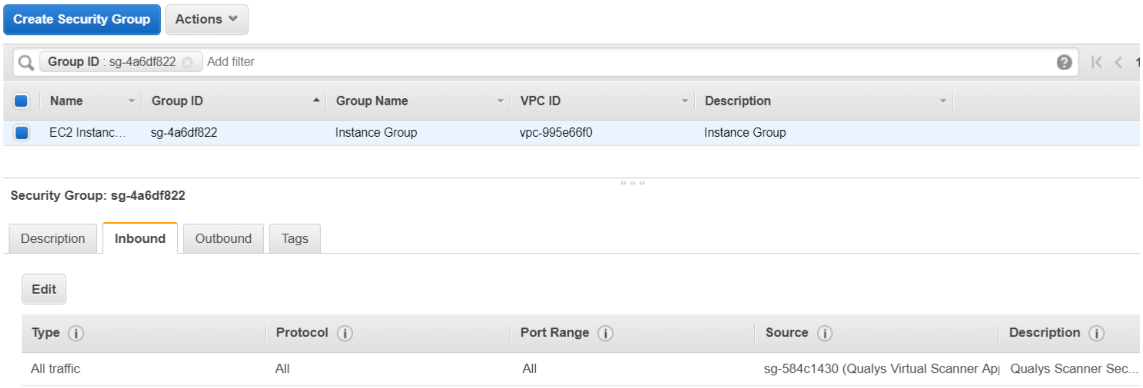
Network : Global Default Network

Info	Tracking	IP	NetBIOS	OS
ⓘ	EC2	10.90.1.29	NEWSUSE-5	Amazon Linux
ⓘ	EC2	10.90.1.88	AGENT-P04	Amazon Linux

Configure security groups for the EC2 instances to be scanned

In AWS, you must associate a security group that allows inbound access on all ports for the IP address of the scanner appliance or the security group of the scanner appliance.

Here is the sample security group assigned to EC2 instance allowing inbound access on all the ports for the security group of Qualys Virtual Scanner Appliance.



Name	Group ID	Group Name	VPC ID	Description
EC2 Instanc...	sg-4a6df822	Instance Group	vpc-995e66f0	Instance Group

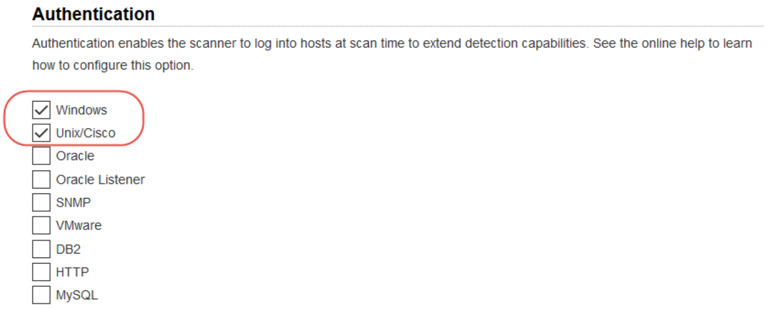
Security Group: sg-4a6df822

Type	Protocol	Port Range	Source	Description
All traffic	All	All	sg-584c1430 (Qualys Virtual Scanner Ap	Qualys Scanner Sec...

Configure OS Authentication

Using host OS authentication (trusted scanning) allows our service to log in to each target system during scanning. Running authenticated scans gives you the most accurate results with fewer false positives.

Go to Scans > Option Profiles. Edit the profile Initial Options, use Save As to save a copy with another name. In your new profile enable the authentication types you'll need.

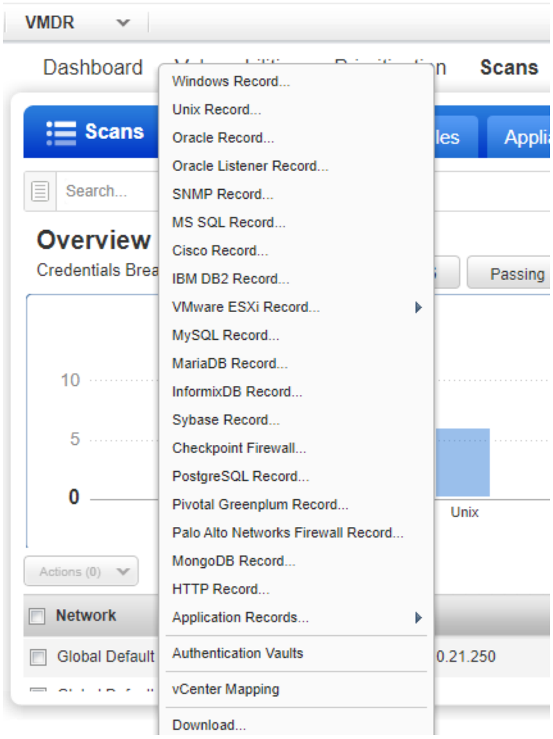


Authentication

Authentication enables the scanner to log into hosts at scan time to extend detection capabilities. See the online help to learn how to configure this option.

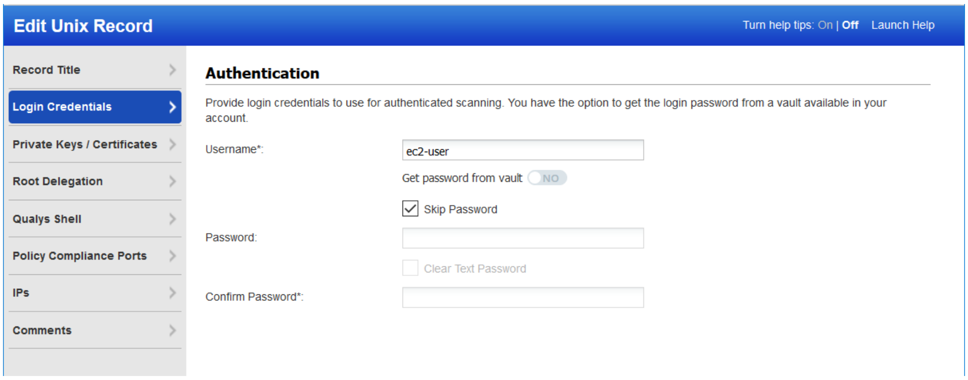
☑ Windows
☑ Unix/Cisco
☐ Oracle
☐ Oracle Listener
☐ SNMP
☐ VMware
☐ DB2
☐ HTTP
☐ MySQL

Go to Scans > Authentication. Add authentication records for the EC2 instances you'll be scanning - Unix and/or Windows. In the record you'll need to add credentials for the account to be used for authentication - this is an account for OS user (not the AIM user). We recommend you create a dedicated account for authentication on target systems.



Sample Unix Record

1) Login Credentials - Provide OS user name and select Skip Password



Authentication

Provide login credentials to use for authenticated scanning. You have the option to get the login password from a vault available in your account.

Username*: ec2-user

Get password from vault: NO

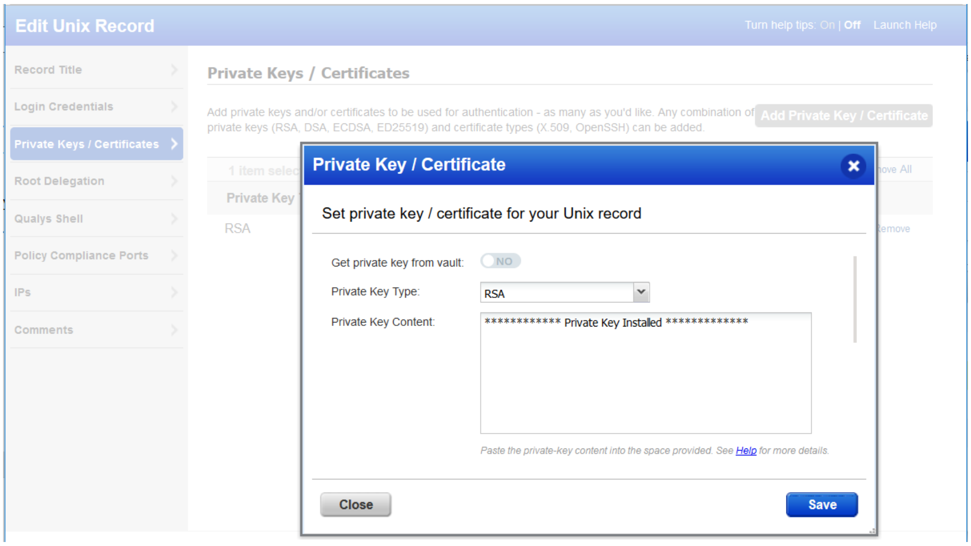
☑ Skip Password

Password:

□ Clear Text Password

Confirm Password*:

2) Private Keys - Key authentication recommended. Select key type (RSA, DSA, ECDSA, ED25519) and enter your private key content.



Private Keys / Certificates

Add private keys and/or certificates to be used for authentication - as many as you'd like. Any combination of private keys (RSA, DSA, ECDSA, ED25519) and certificate types (X.509, OpenSSH) can be added.

Private Key / Certificate

Set private key / certificate for your Unix record

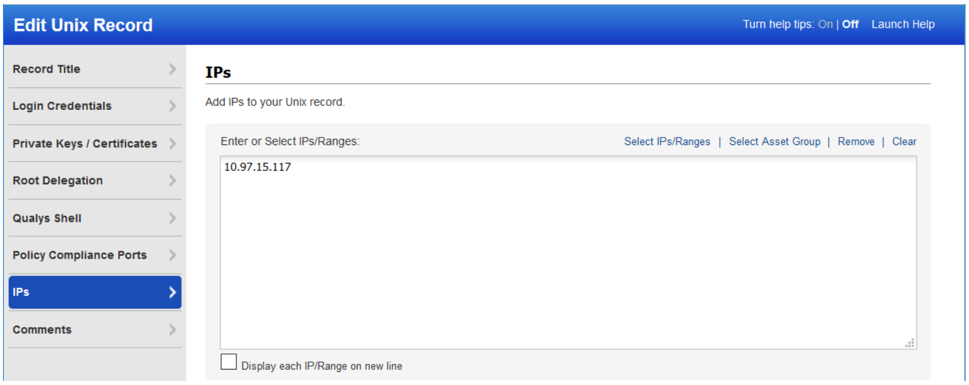
Get private key from vault: NO

Private Key Type: RSA

Private Key Content: ************ Private Key Installed *************

Paste the private-key content into the space provided. See Help for more details.

3) IPs - Select Unix IP addresses/ranges of your EC2 instances for this record. Credentials in this record will be used to scan these assets.



IPs

Add IPs to your Unix record.

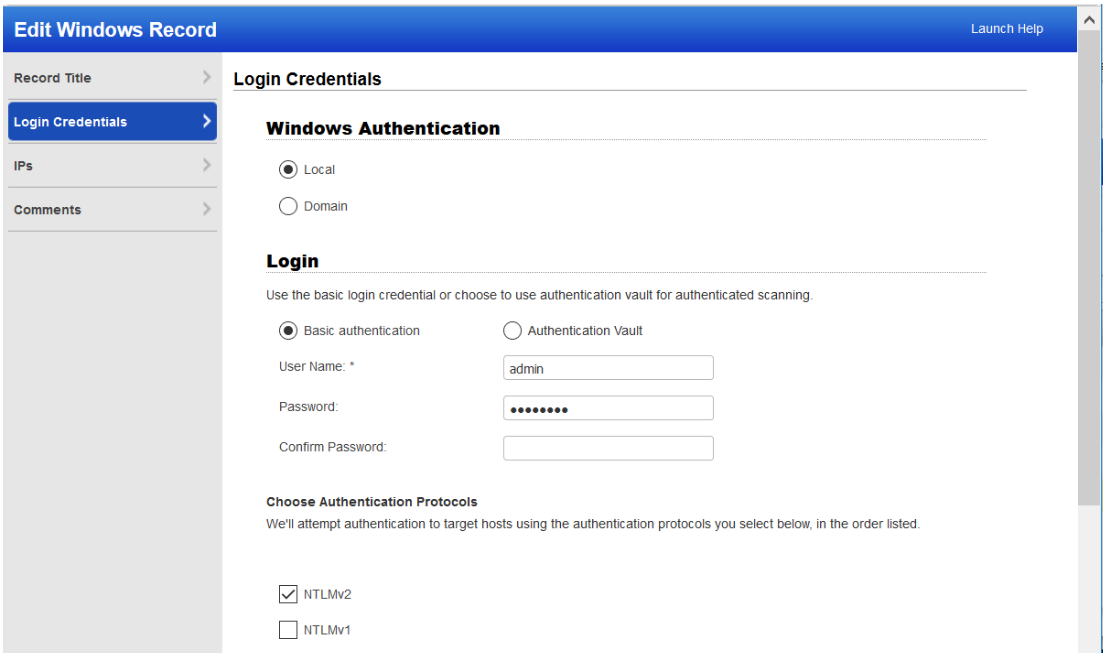
Enter or Select IPs/Ranges:

10.97.15.117

□ Display each IP/Range on new line

Sample Windows Record

1) Login Credentials - Provide OS user name and select Skip Password



Login Credentials

Windows Authentication

● Local

○ Domain

Login

Use the basic login credential or choose to use authentication vault for authenticated scanning.

● Basic authentication ○ Authentication Vault

User Name: * admin

Password: ••••••••

Confirm Password:

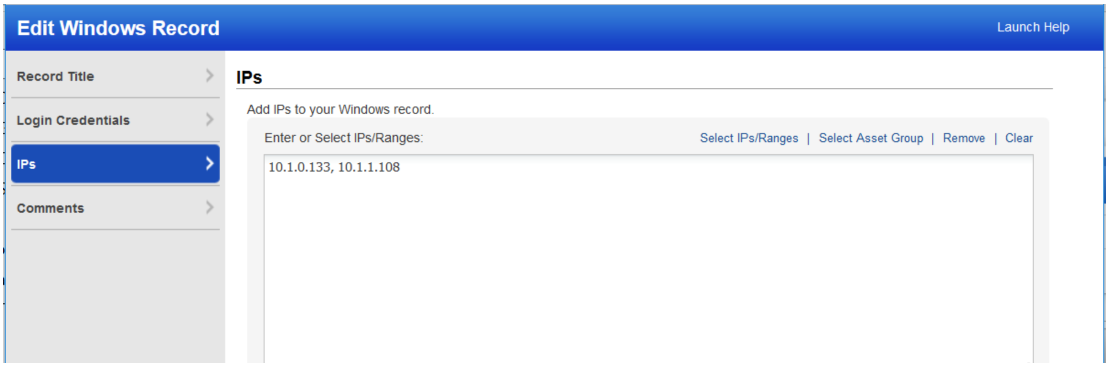
Choose Authentication Protocols

We'll attempt authentication to target hosts using the authentication protocols you select below, in the order listed.

☑ NTLMv2

□ NTLMv1

2) IPs - Select Windows IP addresses/ranges of your EC2 instances for this record. Credentials in this record will be used to scan these assets.



IPs

Add IPs to your Windows record.

Enter or Select IPs/Ranges:

10.1.0.133, 10.1.1.108

Learn more about OS authentication

Online help within the authentication record workflows provides detailed instructions and guidance on all available options. These documents are good resources

Qualys Windows Authentication Guide (pdf)

Qualys Unix Authentication Guide (pdf)

Have Qualys Defined Networks? Move your Virtual Appliance

This step is recommended if you've defined custom networks in your Qualys account.

By default a new Virtual Scanner Appliance is placed in the Global Default Network and when a scan is performed host scan data is added to that network. We recommend you move this Virtual Appliance to the desired network before scanning - the Global EC2 Network or a custom network.

Go to Assets > Networks, edit the network you want to move the Virtual Appliance to and add the appliance to that network.

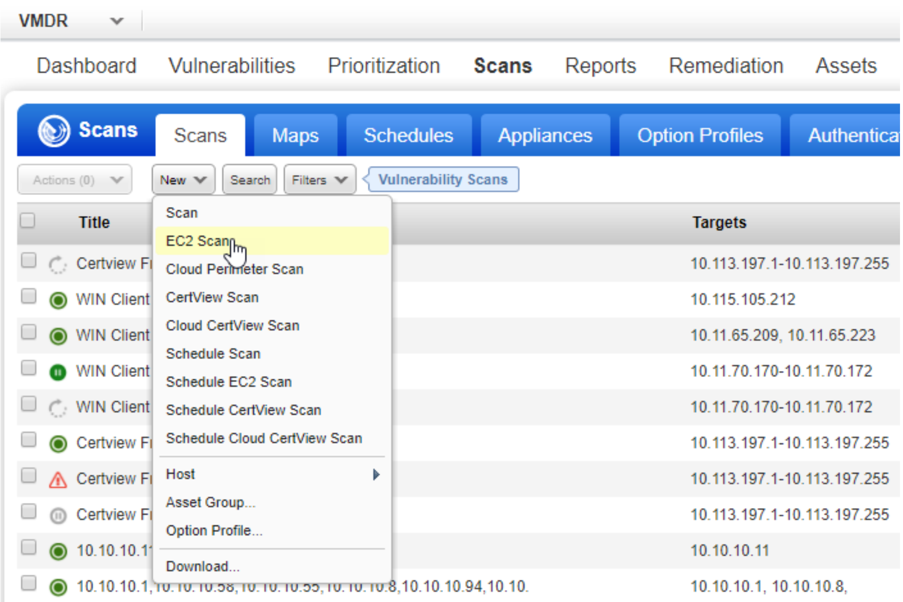
Scan Using Virtual Scanner Appliance

Scanning with virtual scanner appliance involves following sequence of steps.

EC2 Scan workflow

Qualys provides a special EC2 Scan (and Schedule EC2 Scan) workflow which only works in collaboration with an instance of the scanning virtual appliance AMI. This solution allows on-demand and scheduled scanning in Amazon EC2-Classic and EC2-VPC, without the need for the customer to manually request scanning permission from AWS.

Qualys Community: AWS Acceptable Use Guidance For Scanning



☐	Title	Targets
☐	Certview Fi	10.113.197.1-10.113.197.255
☐	WIN Client	10.115.105.212
☐	WIN Client	10.11.65.209, 10.11.65.223
☐	WIN Client	10.11.70.170-10.11.70.172
☐	WIN Client	10.11.70.170-10.11.70.172
☐	Certview Fi	10.113.197.1-10.113.197.255
☐	Certview Fi	10.113.197.1-10.113.197.255
☐	Certview Fi	10.113.197.1-10.113.197.255
☐	10.10.10.1	10.10.10.11
☐	10.10.10.1,10.10.10.58,10.10.10.55,10.10.10.8,10.10.10.94,10.10.	10.10.10.1, 10.10.10.8,

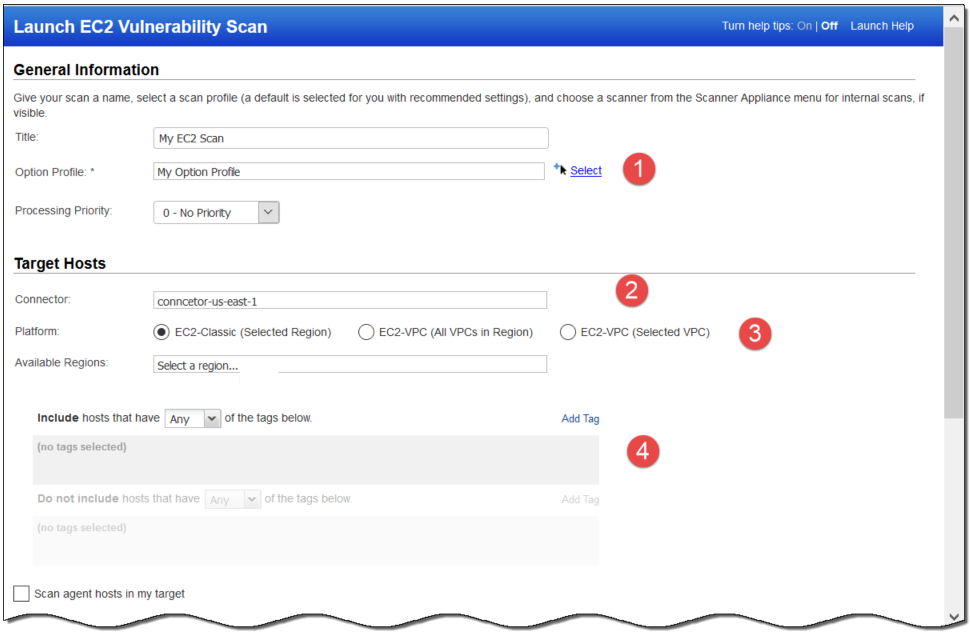
Provide scan settings:

1) Give your scan a title and select the option profile you configured with authentication (required for vulnerability scan).

2) Select the EC2 connector name you configured.

3) For Platform choose one of EC2 Classic, EC2 VPC (All VPCs in region) or EC2 VPC (Selected VPC). Based on your selection you'll select region(s).

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



Launch EC2 Vulnerability Scan

Turn help tips: On | **Off** Launch Help

General Information

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: My EC2 Scan

Option Profile: * My Option Profile Select

Processing Priority: 0 - No Priority

Target Hosts

Connector: conncetor-us-east-1

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

Available Regions: Select a region...

Include hosts that have Any of the tags below. Add Tag

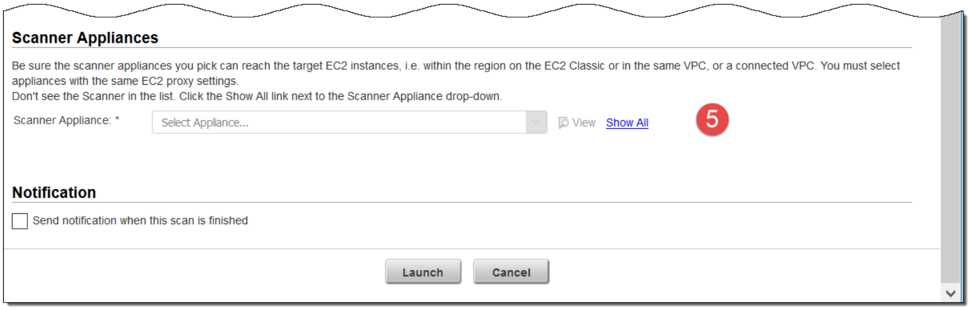
(no tags selected)

Do not include hosts that have Any of the tags below. Add Tag

(no tags selected)

□ Scan agent hosts in my target

5) Choose the Virtual Scanner Appliance AMI you've launched in Amazon EC2.



Scanner Appliances

Be sure the scanner appliances you pick can reach the target EC2 instances, i.e. within the region on the EC2 Classic or in the same VPC, or a connected VPC. You must select appliances with the same EC2 proxy settings.
Don't see the Scanner in the list. Click the Show All link next to the Scanner Appliance drop-down.

Scanner Appliance: * Select Appliance... View Show All

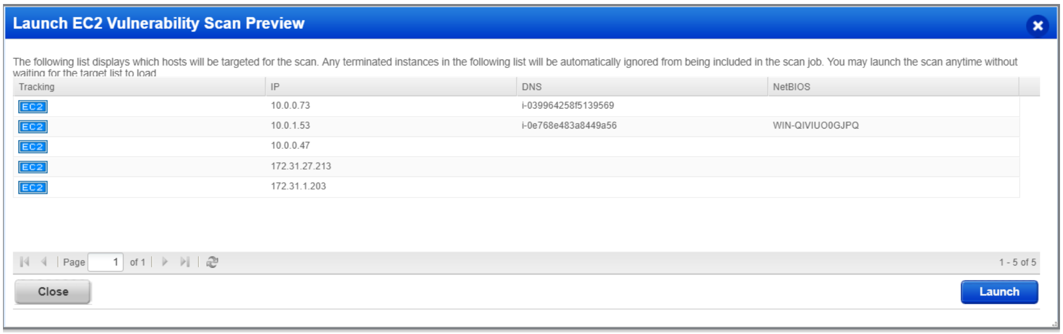
Notification

□ Send notification when this scan is finished

Launch Cancel

Click Launch and start scanning and securing your Amazon EC2 infrastructure.

Before you launch the scan, the EC2 Vulnerability Scan Preview lists all the instances (including terminated instances). However, during the scan all such terminated instances will be ignored from the scan.



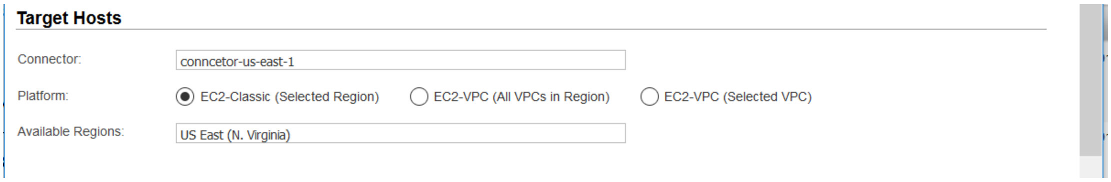
Launch EC2 Vulnerability Scan Preview

The following list displays which hosts will be targeted for the scan. Any terminated instances in the following list will be automatically ignored from being included in the scan job. You may launch the scan anytime without waiting for the target list to load

Tracking	IP	DNS	NetBIOS
EC2	10.0.0.73	i-039964258f5139569	
EC2	10.0.1.53	i-0e768e483a8449a56	WIN-QIVIUO0GJPQ
EC2	10.0.0.47		
EC2	172.31.27.213		
EC2	172.31.1.203		

Scanning EC2 Classic instances

Choose **EC2 Classic (Selected Region)** to scan EC2 classic hosts in a region. When selected we'll only scan EC2 Classic instances in the region.



Target Hosts

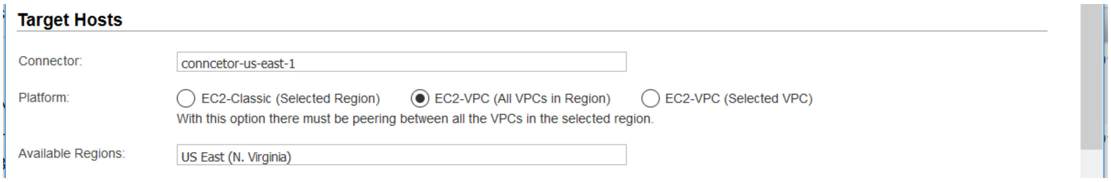
Connector: conncetor-us-east-1

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

Available Regions: US East (N. Virginia)

Scanning VPC instances

Choose **EC2-VPC (Selected VPC)** to scan only a VPC you select.



Target Hosts

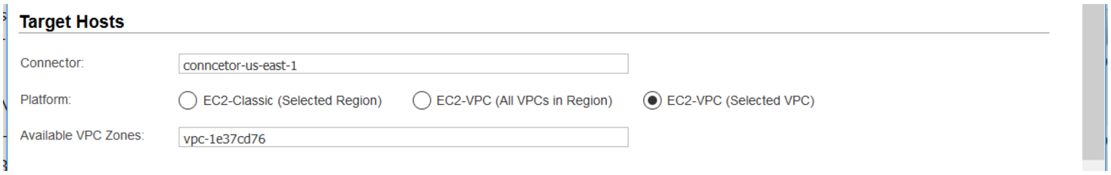
Connector: conncetor-us-east-1

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)

Scanning instances using VPC Peering

Choose **EC2-VPC (All VPCs in Region)** to scan all VPCs in a region. Select this option ONLY if there is peering between all the VPCs in the region, or you could end up with Host not found errors for instances where your Virtual Scanner Appliances cannot reach them.



Target Hosts

Connector: conncetor-us-east-1

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

Available VPC Zones: vpc-1e37cd76

Scanning EC2 Instances in GovCloud

Follow the instructions below to get started with securing your AWS GovCloud using Qualys Virtual Scanner Appliance (qVSA).

1) Contact your Qualys TAM or Qualys Support requesting access to a) GovCloud Feature and b) Qualys Virtual Scanner Appliance AMI.

2) Include your AWS Account ID under which you would be running the scanner, access to the AMI is enabled by Qualys support for specific Account IDs.

3) Qualys Support will send you a mail with approval and access information.

4) Create a Qualys Virtual Scanner Instance with the “qVSA”AMI, which will now be available under MyImages section in the Create Instance wizard. (If you need to search, use the keyword “qVSA” to find the Qualys scanner).

5) Configure the Virtual Scanner Instance as described in Scanner Deployment

6) You’re ready to start scanning! Just follow the steps in Scan Using Virtual Scanner Appliance

Internal Network Scanning using Qualys Cloud Agent

Using our revolutionary Qualys Cloud Agent platform you can deploy lightweight cloud agents to continuously assess your AWS infrastructure for security and compliance.

Cloud Agent features

- Communicates to the Qualys Cloud Platform over port 443 and supports Proxy configurations.

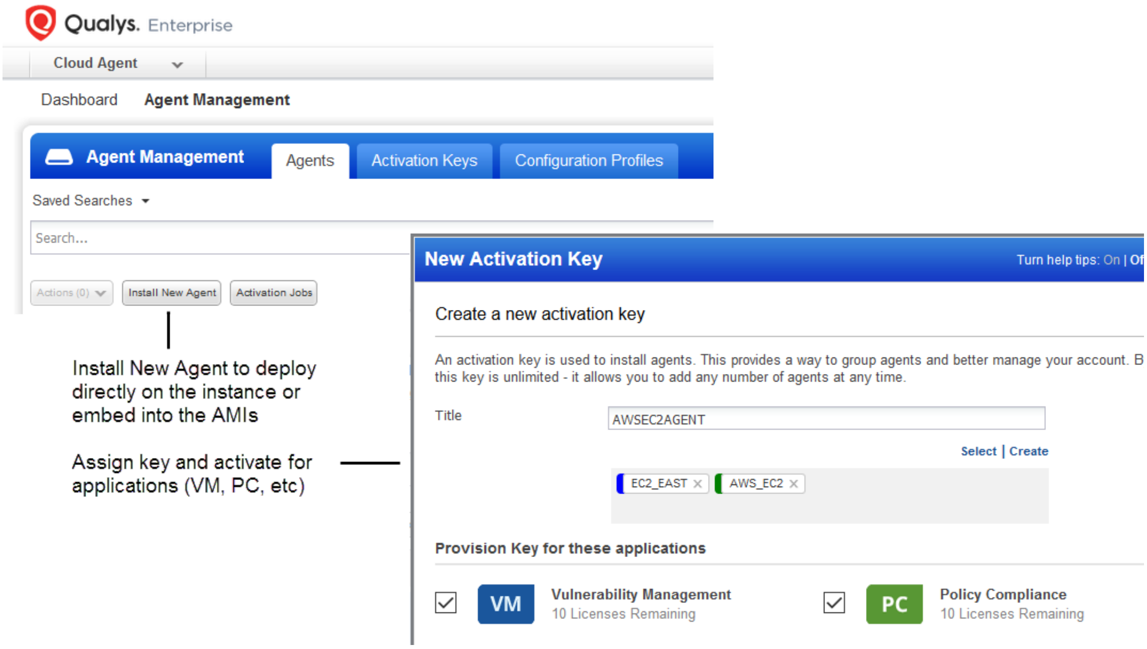
- Deployable directly on the EC2 instances or embed in the AMIs. Works well for cloud burst and ephemeral instances

- Supports scanning a range of Linux and Windows OS versions

- Supports scanning EC2 instance OS vulnerabilities

Get Started

Navigate to the Cloud Agent (CA) app and install the Cloud Agent in minutes



Install New Agent to deploy directly on the instance or embed into the AMIs

Assign key and activate for applications (VM, PC, etc)

Create a new activation key

An activation key is used to install agents. This provides a way to group agents and better manage your account. B this key is unlimited - it allows you to add any number of agents at any time.

Title: AWSEC2AGENT

Provision Key for these applications

☑ Vulnerability Management
10 Licenses Remaining

☑ Policy Compliance
10 Licenses Remaining

We recommend these resources

Qualys Cloud Platform

Qualys Cloud Agent Getting Started Guide

Perimeter Scanning using Qualys Scanners

Qualys Scanners (Internet Remote Scanners), located at the Qualys Cloud Platform, may be used for Perimeter Scanning of EC2 instances.

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 EC2 instances. If both public DNS and public IP address exist for your EC2 assets, then we will launch a scan on public DNS.

Requirements

You'll get Cloud Perimeter Scanning when these features are enabled for your account:

1) EC2 Scanning and 2) Scan by Hostname.

Your account must have a Manager or Unit Manager role with following permissions assigned to your account.

- Enable Cloud Perimeter Scans (to launch scan using external scanners).

- Enable Internal Scanners for Cloud Perimeter Scans (to launch scan using internal scanners).

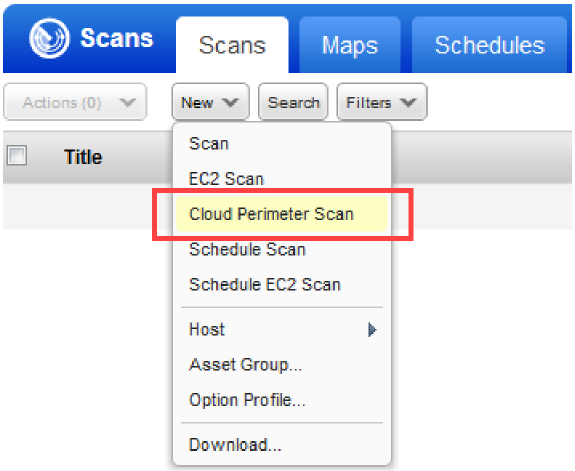
EC2 connector is required. Configure this same EC2 connector in your TotalCloud account if you wish to “include public load balancers from the connector” in the scan. To create the connector, your account must have TotalCloud subscription and your platform has access to TotalCloud base URL “qweb_cloud_view_base_url”. See “Configure Your AWS Connector” in TotalCloud Online help.

If you wish to include micro, nano and small instance types in the scan, these instance types should be activated for your account.

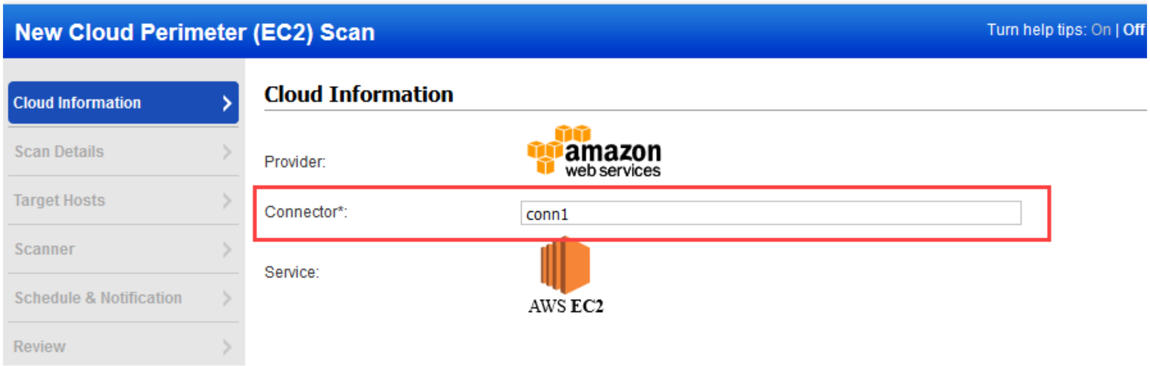
Get Started

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.

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.



The first thing you'll do is select the EC2 connector you've configured.



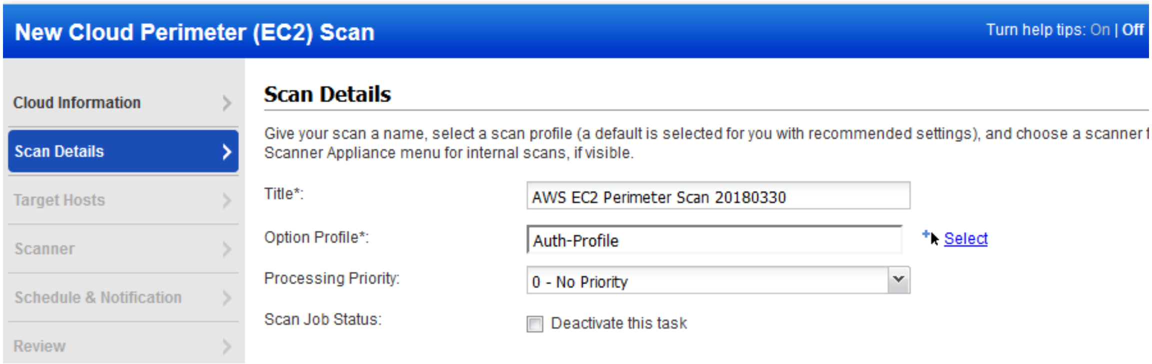
Cloud Information

Provider:

Connector*: conn1

Service: AWS EC2

Give your scan a title and select the option profile you configured with authentication. You can launch either unauthenticated or authenticated Cloud Perimeter scans.



Scan Details

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

Title*: AWS EC2 Perimeter Scan 20180330

Option Profile*: Auth-Profile

Processing Priority: 0 - No Priority

Scan Job Status: □ Deactivate this task

Now it's time to pick your target hosts. If you do not specify the platform, region code, vpc id, asset tags or load balancers DNS names then we will launch scan on the assets resolved from the connector.

1) (Optional) 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).

You also have the option to include assets with instance types t2.nano, t3.nano, t1.micro and m1.small in the scan. When you select this option, we will show you a warning message recommending you to perform no authentication, light port scanning for these instances types. Note that to include micro, nano and small instance types in the scan, these instance types should be activated for your account.

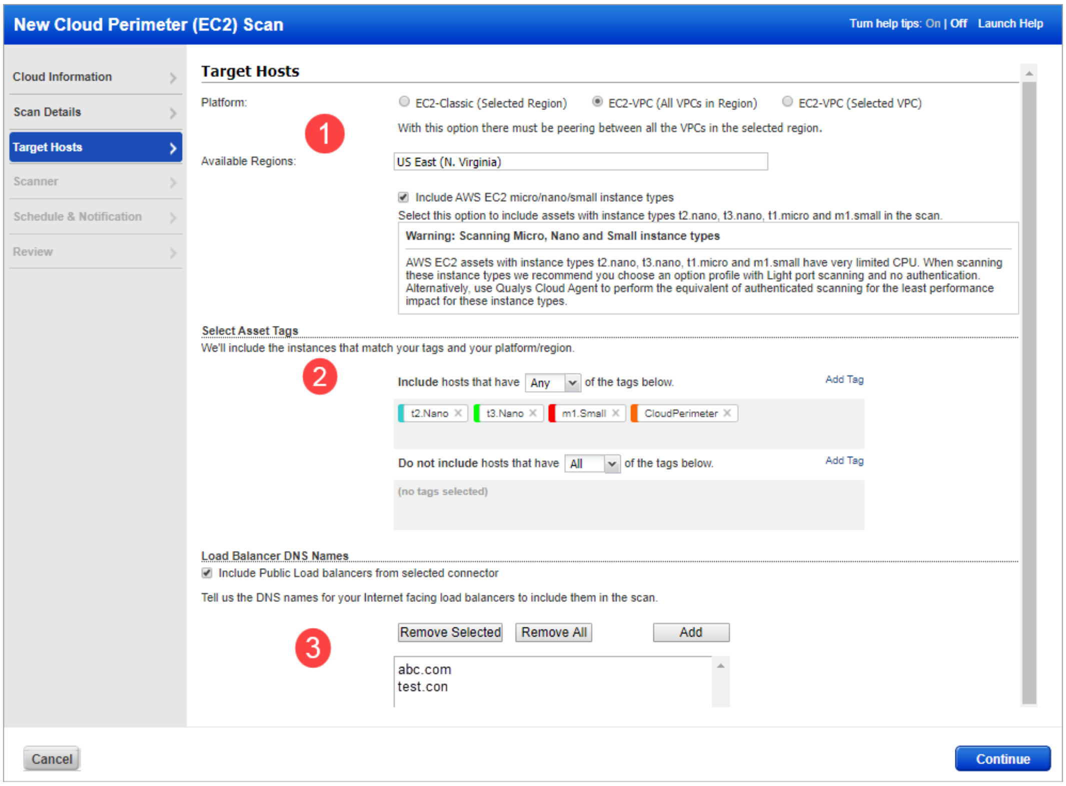
2) (Optional) Select asset tags - these are assets activated for your connector.

3) (Optional) Select public load balancer check box to include public load balancers from the selected connector. EC2 Classic platform does not support public load balancers.

You also have the option to enter DNS names for your load balancers to include them in the scan along with public load balancers. Click Add to enter the DNS names.

Note that when you select the "Include Public Load balancers from selected connector" check box, we fetch public load balancers from the AWS connector in TotalCloud that has the same configuration as that of the selected connector. If you select this option, ensure that you have the connector created in your TotalCloud account with a configuration similar to that of the selected connector. If the connector in TotalCloud is not found, then selecting this option won't fetch any public load balancers. See "Configure Your AWS Connector" in TotalCloud Online help.

When resolving the assets and load balancers, if no assets or public load balancers 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.



New Cloud Perimeter (EC2) Scan

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)

☑ Include AWS EC2 micro/nano/small instance types

Select this option to include assets with instance types t2.nano, t3.nano, t1.micro and m1.small in the scan.

Warning: Scanning Micro, Nano and Small instance types

AWS EC2 assets with instance types t2.nano, t3.nano, t1.micro and m1.small have very limited CPU. When scanning these instance types we recommend you choose an option profile with Light port scanning and no authentication. Alternatively, use Qualys Cloud Agent to perform the equivalent of authenticated scanning for the least performance impact for these instance types.

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.

t2.Nano t3.Nano m1.Small CloudPerimeter

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

(no tags selected)

Load Balancer DNS Names

☑ Include Public Load balancers from selected connector

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

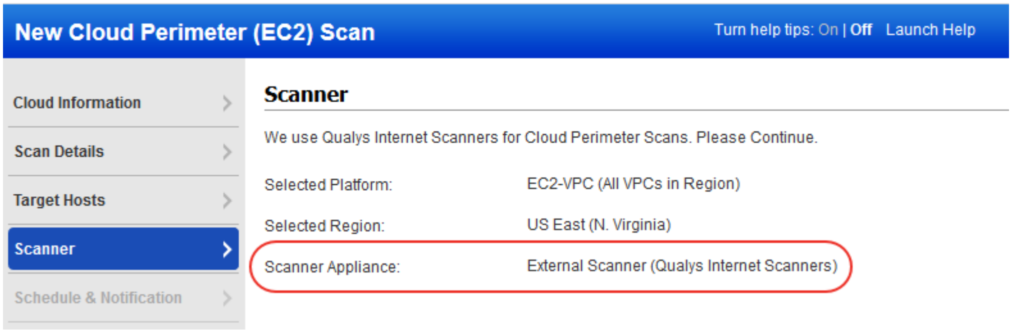
abc.com
test.con

DNS-based scans

This feature needs to be turned ON for your subscription. Please contact Qualys Support if you would like to enable this feature.

How DNS-based scans work: Users submit scans on the DNS for ELB and the rest. The IPs are resolved in realtime and then scanned for.

By default cloud perimeter scans use Qualys External Scanners.



New Cloud Perimeter (EC2) Scan

Scanner

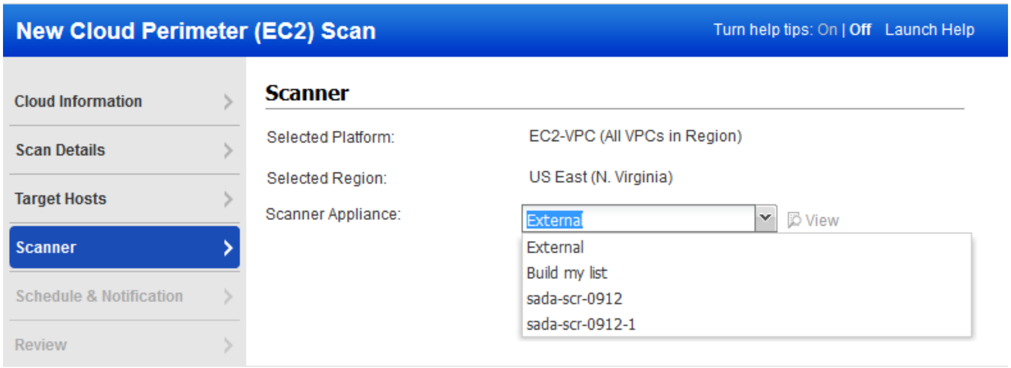
We use Qualys Internet Scanners for Cloud Perimeter Scans. Please Continue.

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 subscription may be configured to allow scanner appliances to be used for cloud perimeter scan jobs. 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)

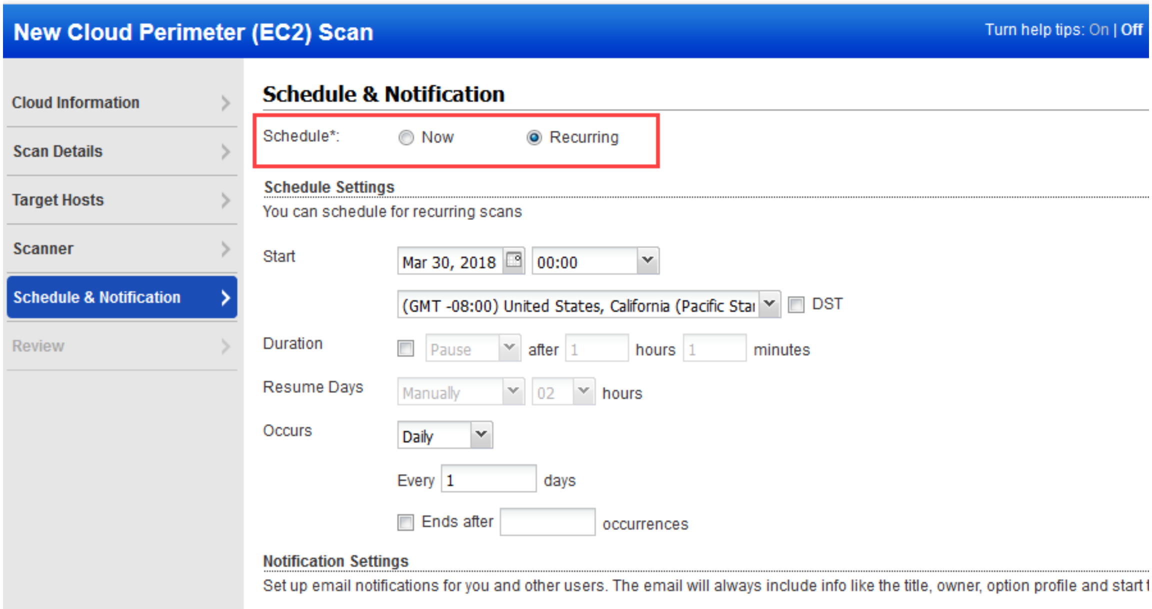
Scanner Appliance: External

- External
- Build my list
- sada-scr-0912
- sada-scr-0912-1

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 Star □ DST

Duration: □ Pause after 1 hours 1 minutes

Resume Days: Manually 02 hours

Occurs: Daily

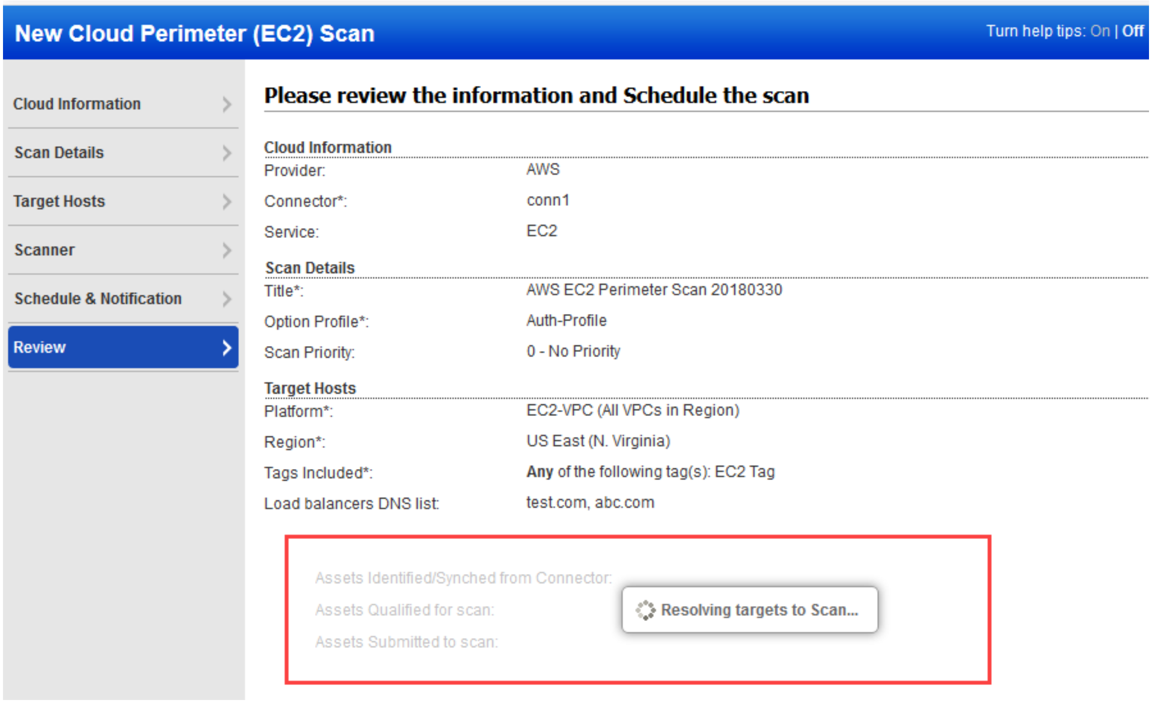
Every 1 days

□ 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 t

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 that you selected for this scan job.

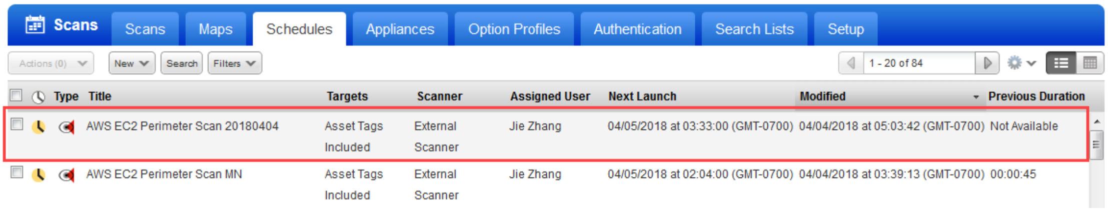
Assets Qualified for scan - The number of assets discovered by the connector that also match the selected platform, region, asset tags. We'll remove the Terminated instances.

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

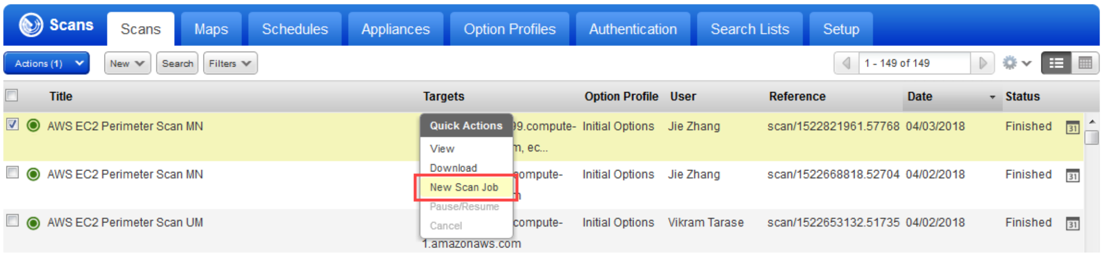
Your new scan job will appear on the Schedules list.



□	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.

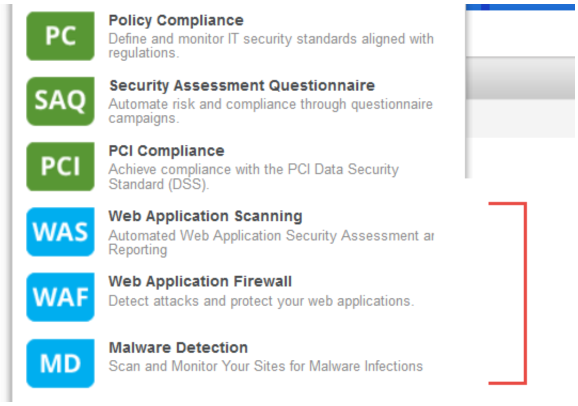
Want to run the scan again? Choose New Scan Job from the Quick Actions menu. We'll retain certain scan settings from the original scan job and schedule the scan to run "Now".



□	Title	Targets	Option Profile	User	Reference	Date	Status
☑	AWS EC2 Perimeter Scan MN	9.compute- m, 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

Securing Web Applications

Using Qualys you can secure Applications using Application Scanning and Firewall solutions.



Policy Compliance
Define and monitor IT security standards aligned with regulations.

Security Assessment Questionnaire
Automate risk and compliance through questionnaire campaigns.

PCI Compliance
Achieve compliance with the PCI Data Security Standard (DSS).

Web Application Scanning
Automated Web Application Security Assessment ar Reporting

Web Application Firewall
Detect attacks and protect your web applications.

Malware Detection
Scan and Monitor Your Sites for Malware Infections

Qualys WAS

Qualys Web Application Scanning (WAS) provides automated crawling and testing of custom web applications to identify application and RESTAPI vulnerabilities including cross site scripting (XSS) and SQL injection. To get started install the Qualys Virtual Scanner Appliance. This is the same appliance used to scan for vulnerabilities and compliance checks.

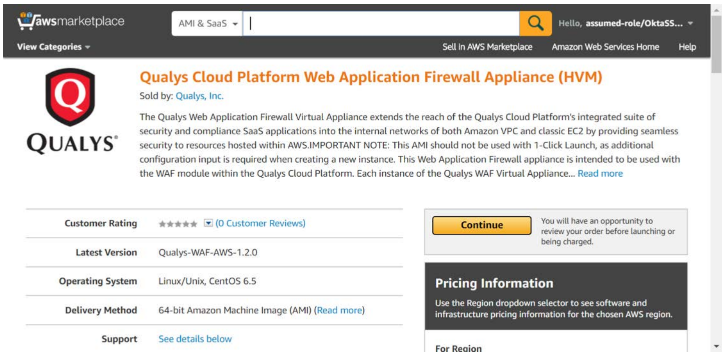
How do I get started?
- Follow the steps in Scanner Deployment
- Then review instructions in Qualys Web Application Scanning Getting Started Guide.

Qualys WAF

Protect applications with firewall rules and instant virtual patches using Qualys Web Application Firewall (WAF).

How do I get started?
- Install the Web Application Firewall Appliance available on the AWS Marketplace
- Then review instructions in Qualys Web Application Firewall Getting Started Guide.

Qualys Cloud Platform Web Application Firewall Appliance (HVM) on AWS Marketplace



Qualys Cloud Platform Web Application Firewall Appliance (HVM)

Sold by: Qualys, Inc.

The Qualys Web Application Firewall Virtual Appliance extends the reach of the Qualys Cloud Platform's integrated suite of security and compliance SaaS applications into the internal networks of both Amazon VPC and classic EC2 by providing seamless security to resources hosted within AWS.IMPORTANT NOTE: This AMI should not be used with 1-Click Launch, as additional configuration input is required when creating a new instance. This Web Application Firewall appliance is intended to be used with the WAF module within the Qualys Cloud Platform. Each instance of the Qualys WAF Virtual Appliance... Read more

Customer Rating	★★★★★ (0 Customer Reviews)
Latest Version	Qualys-WAF-AWS-1.2.0
Operating System	Linux/Unix, CentOS 6.5
Delivery Method	64-bit Amazon Machine Image (AMI) (Read more)
Support	See details below

You will have an opportunity to review your order before launching or being charged.

Pricing Information

Use the Region dropdown selector to see software and infrastructure pricing information for the chosen AWS region.

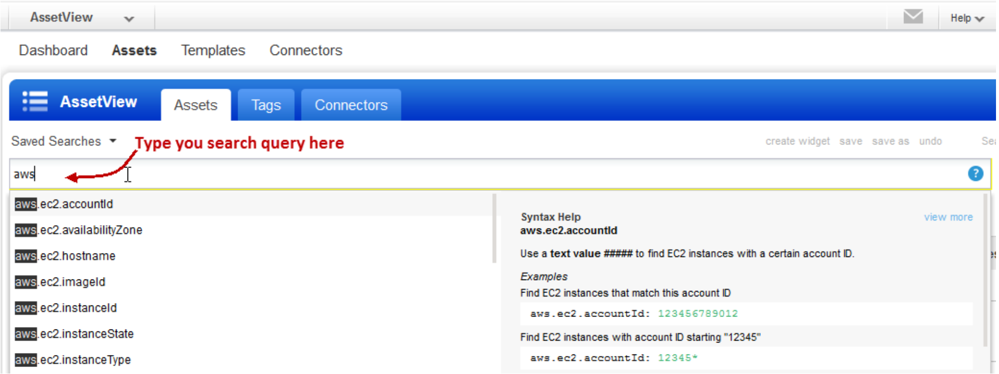
For Region

Analyze, Report & Remediate

In this section we will cover how to query assets, build widgets and dashboards, and then how to generate reports on AWS hosts in vulnerability management.

How to Query EC2 Assets

Our search capabilities give you the ability to quickly find all about your assets all in one place. Go to Assets tab in AssetView app. Start typing AWS and we'll show you the asset properties you can search like accountId, instanceType, hostname, etc. Select the one you're interested in.



Type you search query here

aws

- aws.ec2.accountId
- aws.ec2.availabilityZone
- aws.ec2.hostname
- aws.ec2.imageId
- aws.ec2.instanceId
- aws.ec2.instanceState
- aws.ec2.instanceType

Syntax Help
aws.ec2.accountId

Use a **text value #####** to find EC2 instances with a certain account ID.

Examples
Find EC2 instances that match this account ID

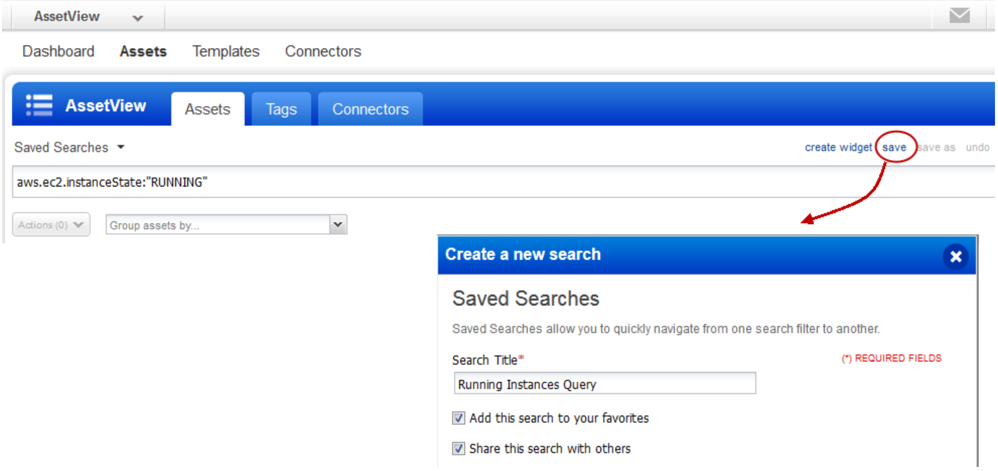
```
aws.ec2.accountId: 123456789012
```

Find EC2 instances with account ID starting "12345"

```
aws.ec2.accountId: 12345*
```

Save Query

You can easily save your searches for reuse and share them with other users.



aws.ec2.instanceState:"RUNNING"

Create a new search

Saved Searches

Saved Searches allow you to quickly navigate from one search filter to another.

Search Title* (*) REQUIRED FIELDS

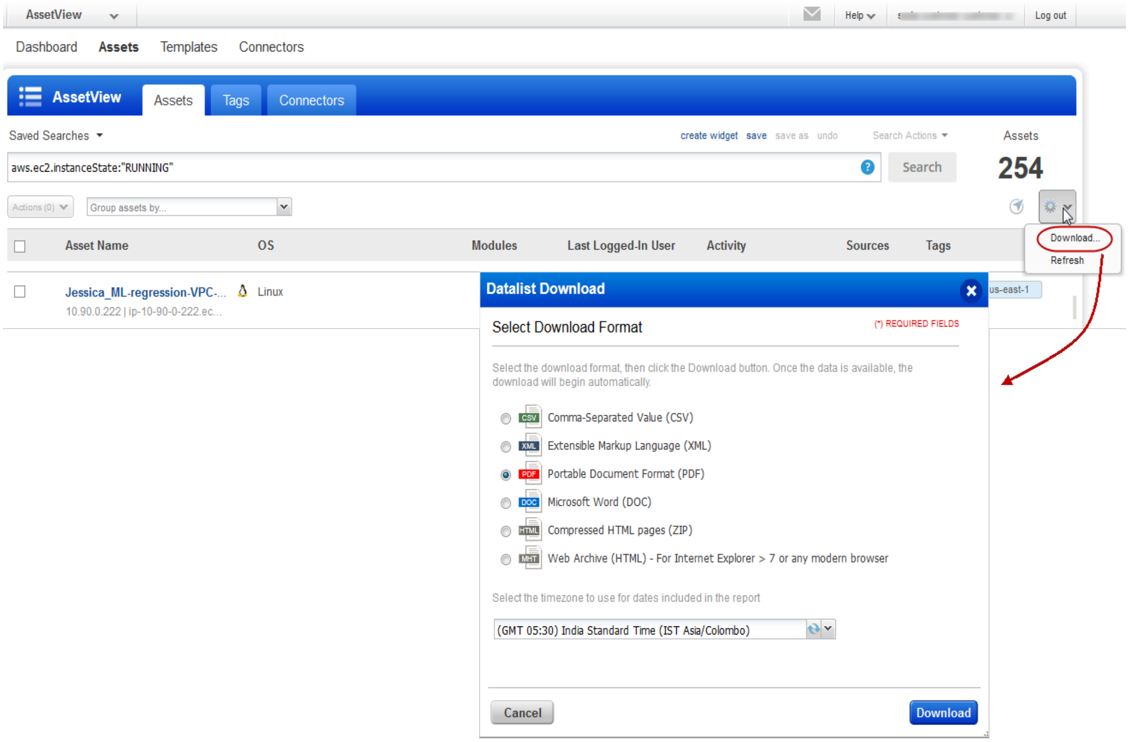
Running Instances Query

☑ Add this search to your favorites

☑ Share this search with others

Download and export results

It just takes a minute to export search results. Select Download from the Tools menu. Next, choose an export format and click Download. You can export results in multiple formats (CSV, XML, PDF, DOC, HTML, etc).



aws.ec2.instanceState:"RUNNING"

□ Jessica_ML-regression-VPC-... Linux
10.90.0.222 | ip-10-90-0-222.ec...

Datalist Download

Select Download Format

(*) REQUIRED FIELDS

Select the download format, then click the Download button. Once the data is available, the download will begin automatically.

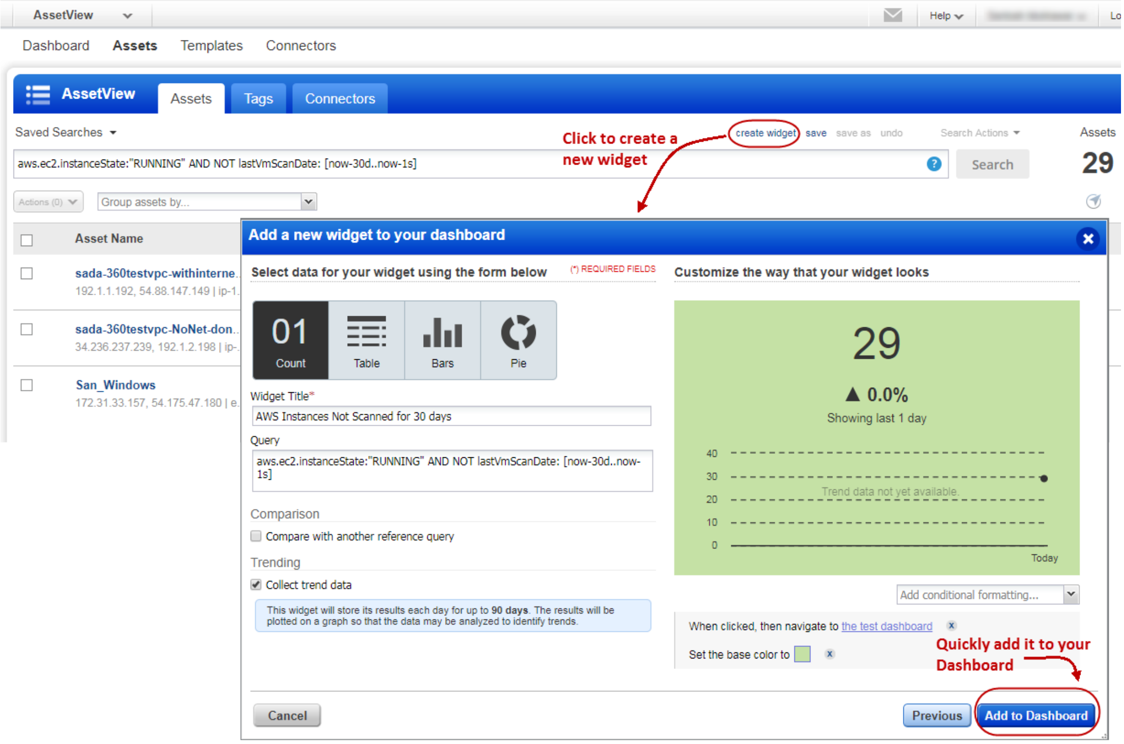
○ Comma-Separated Value (CSV)
○ Extensible Markup Language (XML)
● Portable Document Format (PDF)
○ Microsoft Word (DOC)
○ Compressed HTML pages (ZIP)
○ Web Archive (HTML) - For Internet Explorer > 7 or any modern browser

Select the timezone to use for dates included in the report

(GMT 05:30) India Standard Time (IST Asia/Colombo)

Create widget

Run a query for your assets to create a widget and add it to your dashboard. For example, search for AWS assets that are in running state and have not been scanned for a month. Type your query and click Create a widget. Then add the widget to your dashboard.



aws.ec2.instanceState:"RUNNING" AND NOT lastVmScanDate: [now-30d..now-1s]

Click to create a new widget

Add a new widget to your dashboard

Select data for your widget using the form below (*) REQUIRED FIELDS

Widget Title*: AWS Instances Not Scanned for 30 days

Query: aws.ec2.instanceState:"RUNNING" AND NOT lastVmScanDate: [now-30d..now-1s]

Comparison

☐ Compare with another reference query

Trending

☑ Collect trend data

This widget will store its results each day for up to **90 days**. The results will be plotted on a graph so that the data may be analyzed to identify trends.

Customize the way that your widget looks

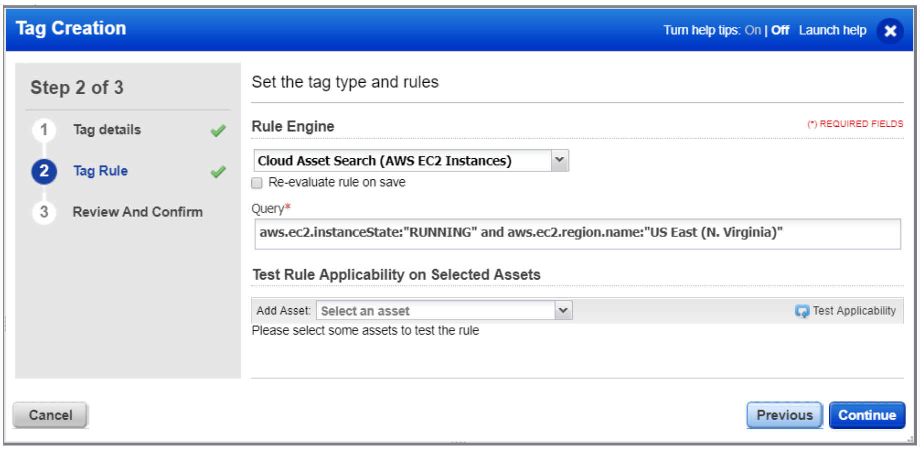
When clicked, then navigate to the test dashboard

Set the base color to 🟩

Quickly add it to your Dashboard

Dynamic Tagging Using EC2 Attributes

Create dynamic tags using EC2 metadata attributes for assets as collected by the EC2 connector. Then use dynamic tags as the scope for your EC2 scans. Go to AssetView > Assets > Tags and create a tag using the Cloud Asset Search (AWS EC2 Instances) tag rule.



Set the tag type and rules

Rule Engine (*) REQUIRED FIELDS

Cloud Asset Search (AWS EC2 Instances)

☐ Re-evaluate rule on save

Query*: aws.ec2.instanceState:"RUNNING" and aws.ec2.region.name:"US East (N. Virginia)"

Test Rule Applicability on Selected Assets

Add Asset: Select an asset

Please select some assets to test the rule

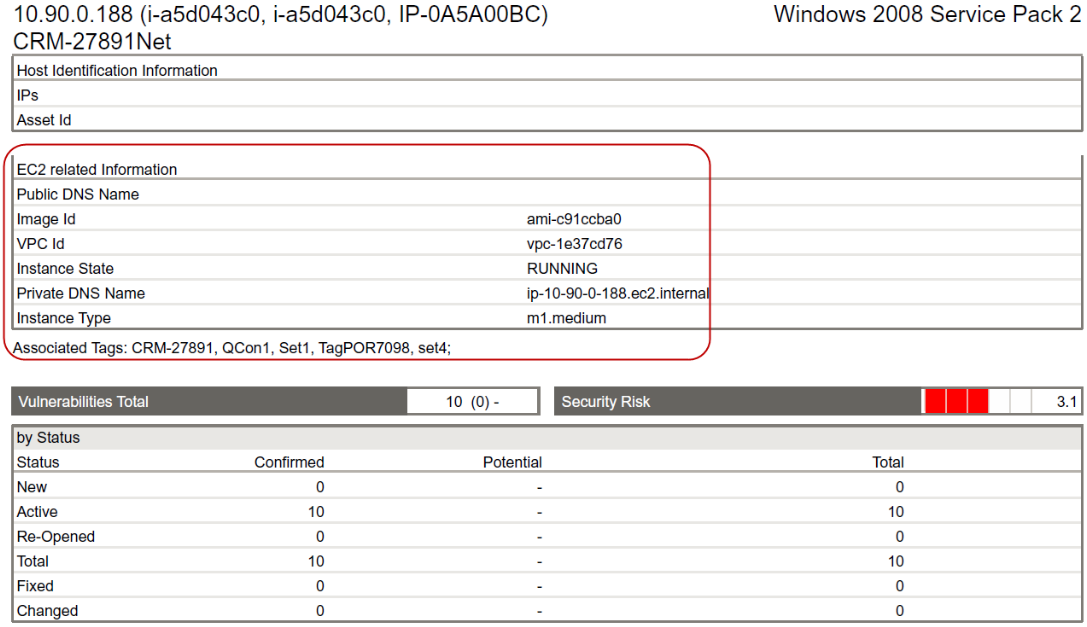
Generate Reports

You can create a report to identify the vulnerability of your EC2 assets. Simply go to Reports > Reports > New > Scan Report. You can then choose a pre-configured template or customized template.

Give the report a title, choose the template, report format, hosts (IP address or tags) and then generate the report.

Depending on your template customization, your report could include graphs, charts depicting vulnerability information and EC2 instance information such as Image Id, VPC Id, Instance state and type so on. You could use the instance information for remediation and fix the vulnerability on the host.

Here is the sample of report on EC2 assets.



10.90.0.188 (i-a5d043c0, i-a5d043c0, IP-0A5A00BC) Windows 2008 Service Pack 2
CRM-27891Net

Host Identification Information
IPs
Asset Id

EC2 related Information	
Public DNS Name	
Image Id	ami-c91ccba0
VPC Id	vpc-1e37cd76
Instance State	RUNNING
Private DNS Name	ip-10-90-0-188.ec2.internal
Instance Type	m1.medium

Associated Tags: CRM-27891, QCon1, Set1, TagPOR7098, set4;

Vulnerabilities Total	10 (0) -	Security Risk	🟥🟥🟥□□	3.1

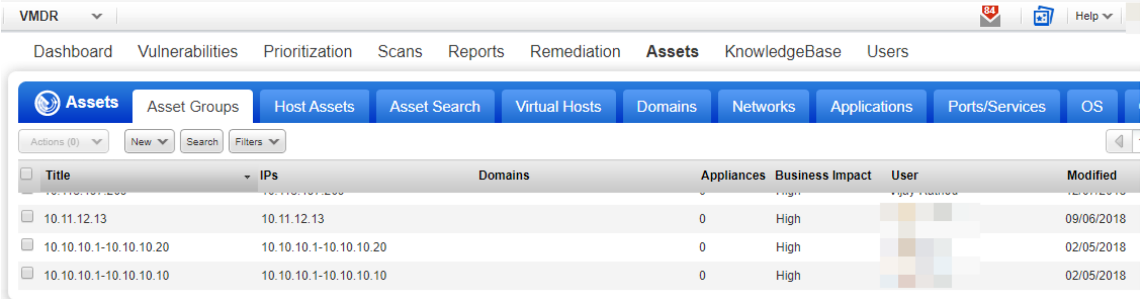
by Status			
Status	Confirmed	Potential	Total
New	0	-	0
Active	10	-	10
Re-Opened	0	-	0
Total	10	-	10
Fixed	0	-	0
Changed	0	-	0

Manage Assets using Qualys

Here's some best practices and tips for organizing assets to help you secure AWS EC2 infrastructure using Qualys.

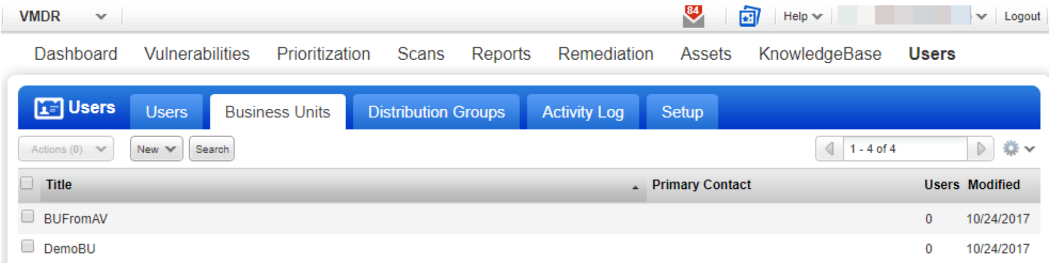
Setting up Qualys configurations

Asset Groups - Organize assets into meaningful groups and assign them to sub-users. Asset groups are required when you have multiple users i.e. Scanner, Reader, Unit Manager (if business units are defined). The same IP address can be included in multiple asset groups.



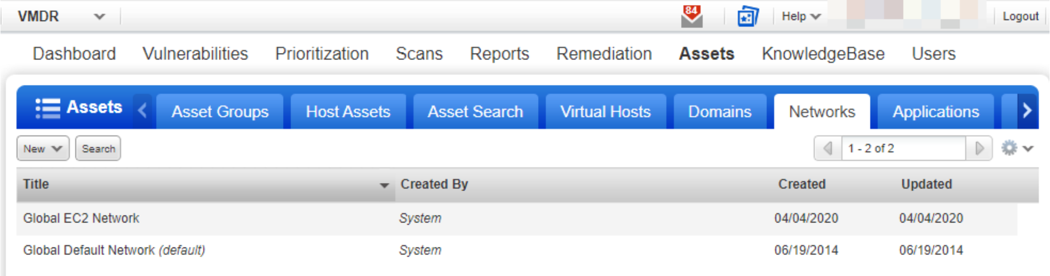
□	Title	IPs	Domains	Appliances	Business Impact	User	Modified
□	10.11.12.13	10.11.12.13		0	High	[redacted]	09/06/2018
□	10.10.10.1-10.10.10.20	10.10.10.1-10.10.10.20		0	High	[redacted]	02/05/2018
□	10.10.10.1-10.10.10.10	10.10.10.1-10.10.10.10		0	High	[redacted]	02/05/2018

Business Units - Organize users and assets into business units in a way that matches your organization. This gives Managers the ability to grant users role-based permissions in the context of their assigned business unit. The same IP address can be included in multiple business units.



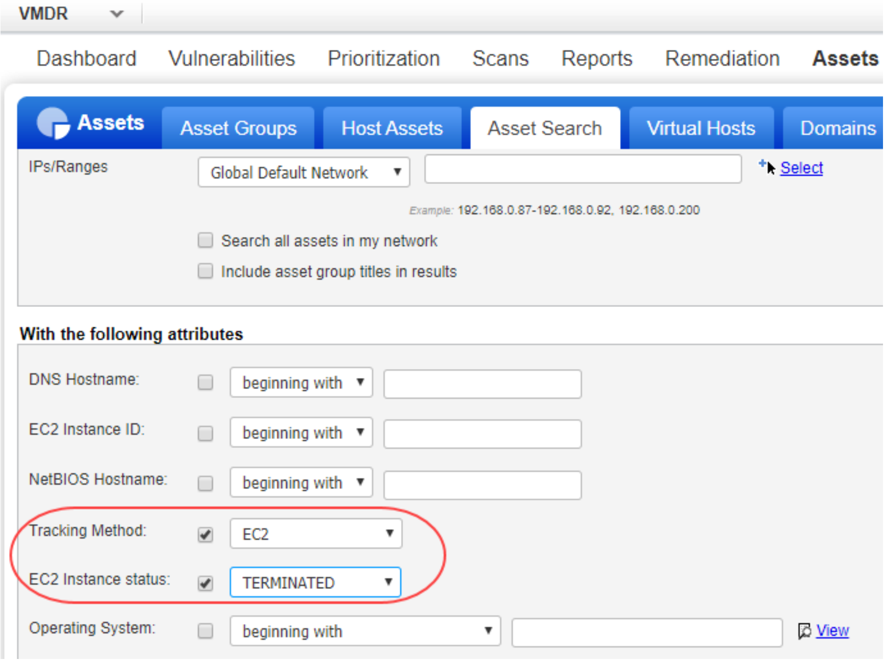
□	Title	Primary Contact	Users	Modified
□	BUFromAV		0	10/24/2017
□	DemoBU		0	10/24/2017

Networks - Organize discrete private IP networks to keep overlapping IP blocks separate. When configured Qualys tracks IPs by network and IP address. Keep in mind... An IP address must be unique to your subscription or a single network.



Title	Created By	Created	Updated
Global EC2 Network	*System*	04/04/2020	04/04/2020
Global Default Network *(default)*	*System*	06/19/2014	06/19/2014

Removing Terminated Instances - You can remove terminated instances from your Qualys account. Go to Vulnerability Management or Policy Compliance > Hosts > Asset Search and select the assets with tracking method as EC2. You could also add more parameters to refine your such as Last Scan Data not within x days and so on.



IPs/Ranges: Global Default Network

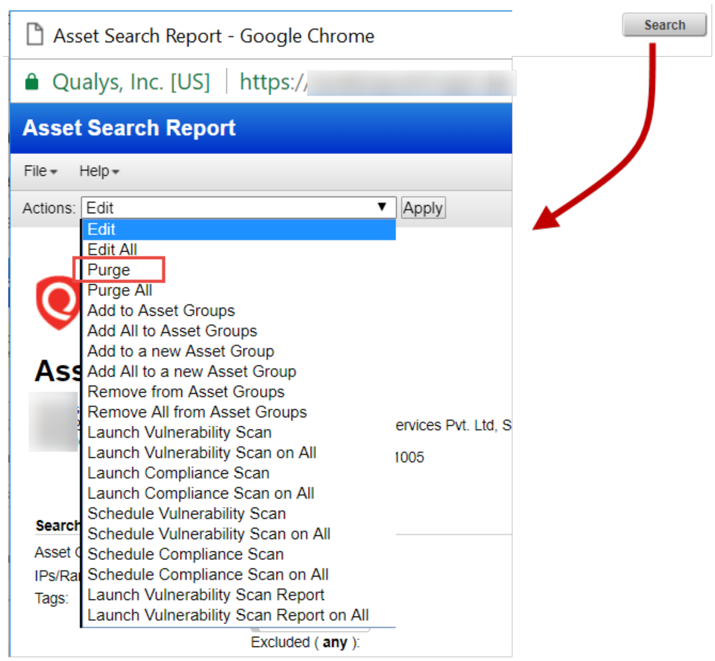
Example: 192.168.0.87-192.168.0.92, 192.168.0.200

□ Search all assets in my network
□ Include asset group titles in results

With the following attributes

DNS Hostname: □ beginning with
EC2 Instance ID: □ beginning with
NetBIOS Hostname: □ beginning with
Tracking Method: ☑ EC2
EC2 Instance status: ☑ TERMINATED
Operating System: □ beginning with

Click Search and then from the Actions menu, select Purge. This results in removal of assets along with its associated data from the module.


Asset Search Report - Google Chrome
Qualys, Inc. [US] | https:/[redacted]
Search
Asset Search Report
File
Help
Actions: Edit
Apply
Edit
Edit All
Purge
Purge All
Add to Asset Groups
Add All to Asset Groups
Add to a new Asset Group
Add All to a new Asset Group
Remove from Asset Groups
Remove All from Asset Groups
Launch Vulnerability Scan
Launch Vulnerability Scan on All
Launch Compliance Scan
Launch Compliance Scan on All
Schedule Vulnerability Scan
Schedule Vulnerability Scan on All
Schedule Compliance Scan
Schedule Compliance Scan on All
Launch Vulnerability Scan Report
Launch Vulnerability Scan Report on All
Ass
Search
Asset
IPs/Ra
Tags:
ervices Pvt. Ltd, S
1005
Excluded (any):

Consider a scenario where you have deployed cloud agents on your EC2 assets and you want to uninstall agents not checked-in for last N days, you can use the API call.

Request:

```
curl -u "USERNAME:PASSWORD" -X "POST" -H "Content-Type: text/xml"
-H
"Cache-Control: no-cache" --data-binary
@uninstall_agents_not_checkedin.xml
"https://qualysapi.qualys.com/qps/rest/2.0/uninstall/am/asset/"
```

Contents of uninstall_agents_not_checkedin.xml:

```
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
<filters>
<Criteria field="tagName" operator="EQUALS">Cloud Agent</Criteria>
<Criteria field="updated" operator="LESSER">2016-08-
25T00:00:01Z</Criteria>
</filters>
</ServiceRequest>
```

For more information on Cloud Agent APIs, refer to our Cloud Agent API User Guide.

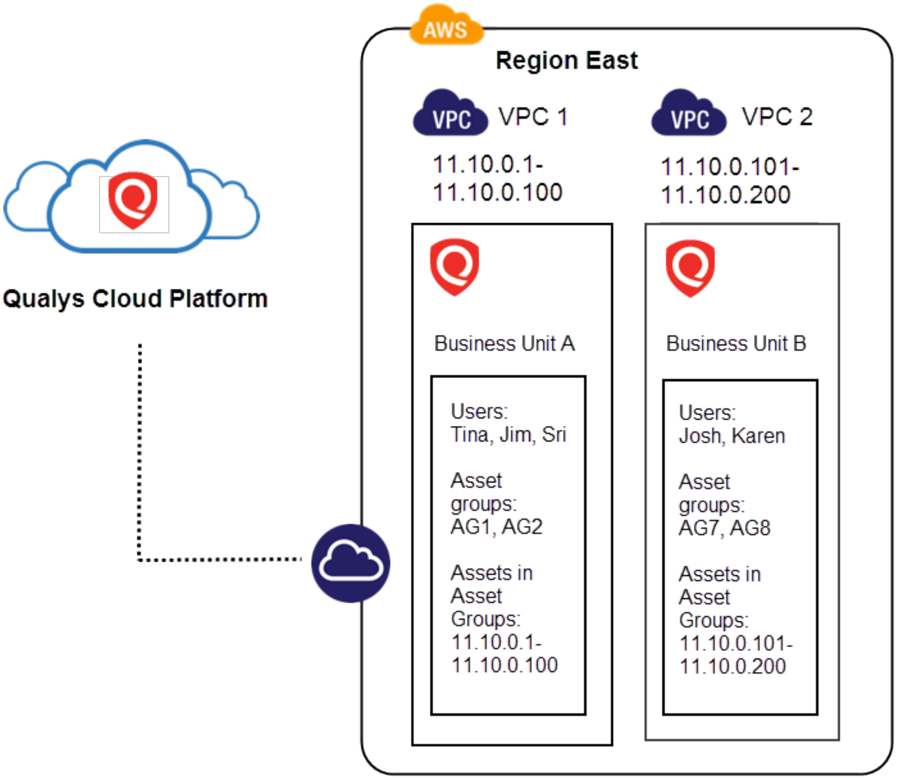
Use Cases for scanning your AWS environment

Use Case 1 - Scanning multiple VPCs with No Overlapping IPs

- Need to define Asset Groups, Business Units are optional

- When defined business Units restrict user access to assets within their own business unit. Users in Business Unit A can't access assets in Business Unit B.

- Solution for when there's no overlapping IP addresses in groups AG1, AG2, AG7, AG8.



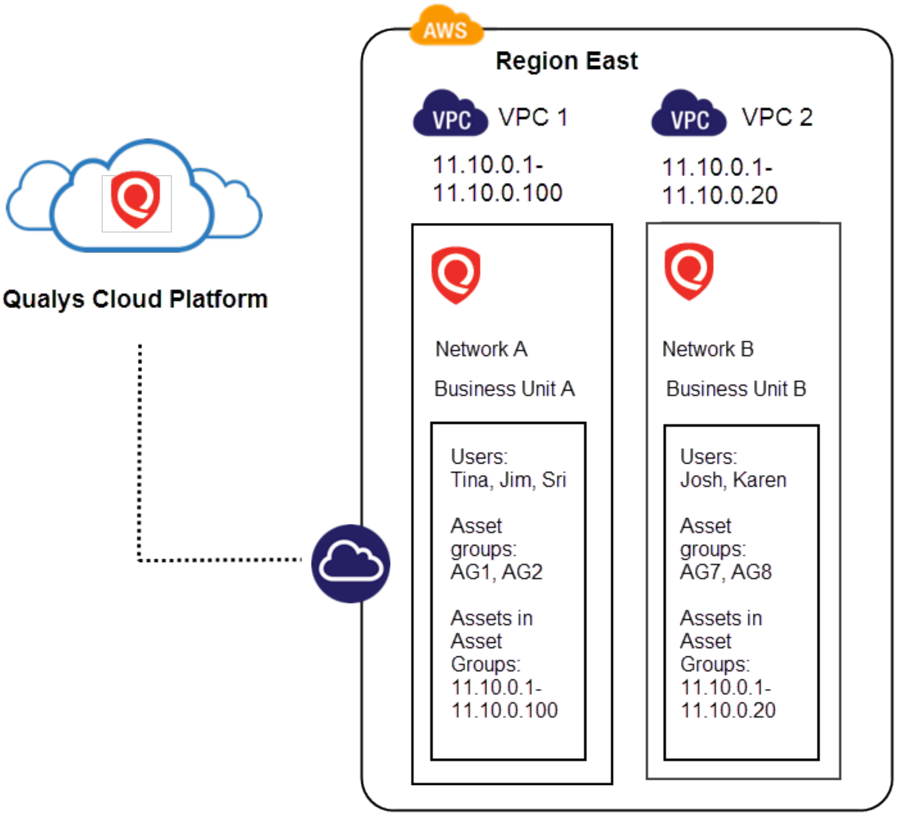
Use Case 2 - Scanning multiple VPCs with Overlapping IPs

- Need to define Networks, Business Units, Asset Groups

- Business Units restrict user access to assets within their own business unit. Users in Business Unit A can't access assets in Business Unit B.

- Solution for when there's overlapping IP addresses in Network A (asset groups AG1, AG2) and Network B (AG7, AG8)

Note: The networks can also be within the same business unit.



DevOps Security

Let us see the various method you could integrate DevOps and fasten the process of scan automation.

Automate scanning into DevOps process to harden the AMI

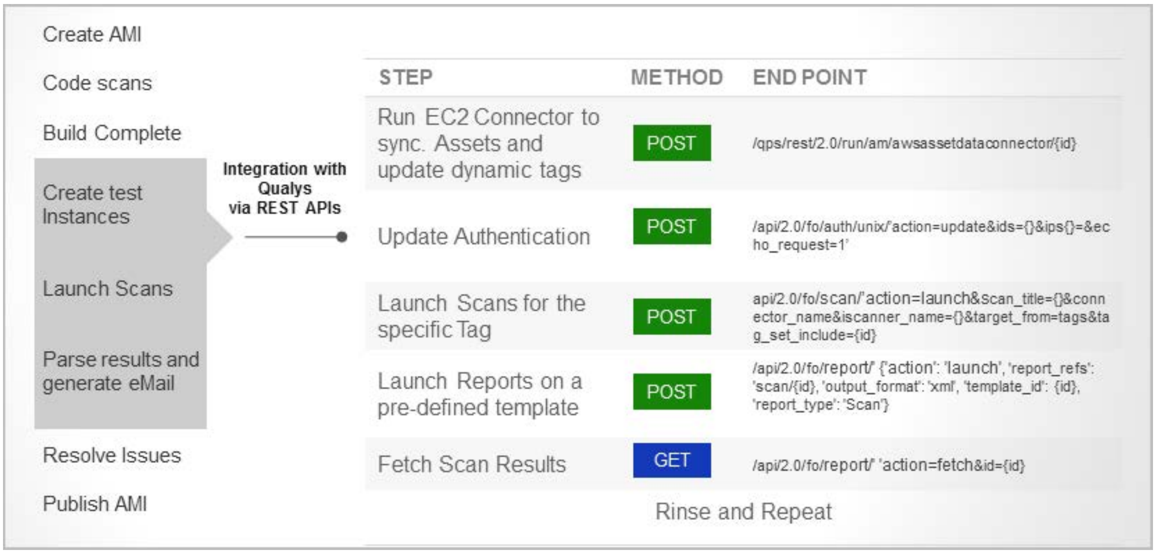
Automate VM scanning of host and EC2 cloud instance from Jenkins

Golden AMIs Pipeline

Automate scanning into DevOps process to harden the AMI

In AWS, it is a best practice to create your own custom Amazon Machine Images (AMIs) using the publicly available AMI. You can then customize the pre-configured OS & software to run your application. However, you should comprehensively test such custom AMI before using it for production workload. You should also run a vulnerability scan against the AMI to assess applications for vulnerabilities or deviations from the best practices. Qualys provides out-of-box API's to integrate into your DevOps process for scanning the AMI images.

For example here are the typical steps involved in AMI creation and how Qualys APIs can be used for hardening the AMI.



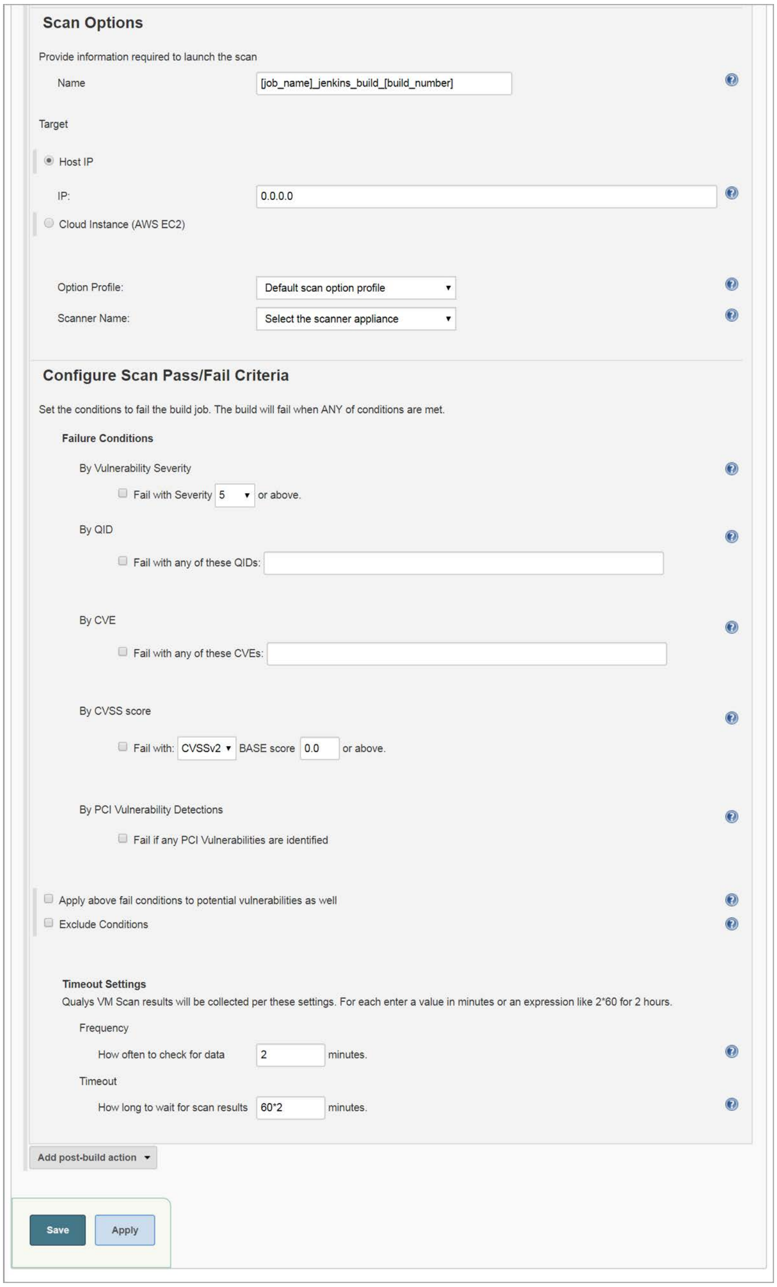
STEP	METHOD	END POINT
Run EC2 Connector to sync. Assets and update dynamic tags	POST	/qps/rest/2.0/run/am/awsassetdataconnector/{id}
Update Authentication	POST	/api/2.0/fo/auth/unix/'action=update&ids={}&ips{}=&echo_request=1'
Launch Scans for the specific Tag	POST	api/2.0/fo/scan/'action=launch&scan_title={}&connector_name&iscanner_name={}&target_from=tags&tag_set_include={id}
Launch Reports on a pre-defined template	POST	/api/2.0/fo/report/' {'action': 'launch', 'report_refs': 'scan/{id}, 'output_format': 'xml', 'template_id': {id}, 'report_type': 'Scan'}
Fetch Scan Results	GET	/api/2.0/fo/report/' 'action=fetch&id={id}

Rinse and Repeat

For detailed information on using Qualys APIs related to AWS, see the Asset Management and Tagging API v2 User Guide.

Automate VM scanning of host and EC2 cloud instance from Jenkins

DevOps teams can use the 'Qualys VM Jenkins plugin' to automate the VM scanning of host and EC2 cloud instance from Jenkins. By integrating scans in this manner, Host or Cloud instance security testing is accomplished to discover and eliminate security flaws. See Jenkins Plugin for VM User Guide.



Scan Options

Provide information required to launch the scan

Name: [job_name]_jenkins_build_[build_number]

Target

● Host IP

IP: 0.0.0.0

○ Cloud Instance (AWS EC2)

Option Profile: Default scan option profile ▾

Scanner Name: Select the scanner appliance ▾

Configure Scan Pass/Fail Criteria

Set the conditions to fail the build job. The build will fail when ANY of conditions are met.

Failure Conditions

By Vulnerability Severity

□ Fail with Severity 5 ▾ or above.

By QID

□ Fail with any of these QIDs:

By CVE

□ Fail with any of these CVEs:

By CVSS score

□ Fail with: CVSSv2 ▾ BASE score 0.0 or above.

By PCI Vulnerability Detections

□ Fail if any PCI Vulnerabilities are identified

□ Apply above fail conditions to potential vulnerabilities as well

□ Exclude Conditions

Timeout Settings

Qualys VM Scan results will be collected per these settings. For each enter a value in minutes or an expression like 2*60 for 2 hours.

Frequency

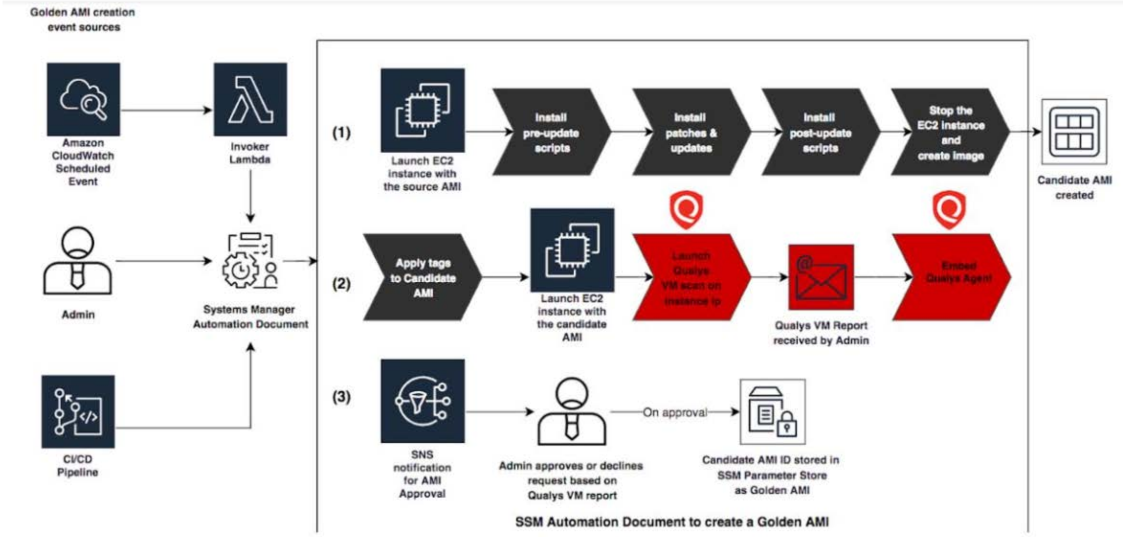
How often to check for data: 2 minutes.

Timeout

How long to wait for scan results: 60*2 minutes.

Golden AMIs Pipeline

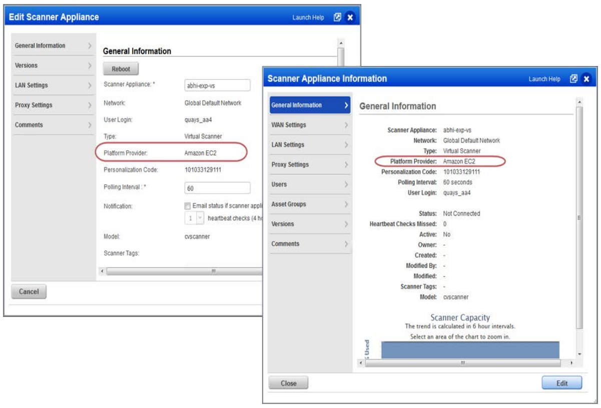
When developing golden Amazon Machine Images (AMIs), DevOps teams should run continuous and automated checks to eliminate vulnerabilities and misconfigurations in them. Qualys collaborated with Amazon to integrate the AWS Golden Amazon Machine Image Pipeline reference architecture with Qualys scanners to perform continuous assessments on the portfolio of hardened AMIs existing in your AWS environment. This will help you detect and fix critical vulnerabilities and compliance issues in the image creation pipeline, before they reach production environments.


Golden AMI creation event sources
Amazon CloudWatch Scheduled Event
Invoker Lambda
Admin
Systems Manager Automation Document
CI/CD Pipeline
(1)
Launch EC2 instance with the source AMI
Install pre-update scripts
Install patches & updates
Install post-update scripts
Stop the EC2 instance and create image
Candidate AMI created
(2)
Apply tags to Candidate AMI
Launch EC2 instance with the candidate AMI
Launch Qualys VM scan on instance ip
Qualys VM Report received by Admin
Embed Qualys Agent
(3)
SNS notification for AMI Approval
Admin approves or declines request based on Qualys VM report
On approval
Candidate AMI ID stored in SSM Parameter Store as Golden AMI
SSM Automation Document to create a Golden AMI

To learn more about the integration of Qualys with Amazon's Golden AMI, refer to the references: AWS Golden AMI Pipelines, video series.

We also provide scripts that can be used for the Golden AMI Pipeline integration with a Qualys Scanner for vulnerability assessments. Learn more.

Common Questions

Queries	Solutions
Scan Results and EC2 Instance ID	EC2 scan results are indexed by EC2 Instance ID. This way we continue to track your assets even when IP address changes occur. When an IP address change is found during a scan you'll see the new IP address in your scan results, scan reports and in your AssetView asset inventory, once scan results are processed.
How does EC2 scan job handle Terminated EC2 instances?	We'll automatically filter out all EC2 instances with a Terminated status from EC2 scans, launched from Qualys VM/VMDR or Qualys PC. This way we don't attempt to scan dead EC2 instances. Note that the Launch EC2 Scan Preview, which appears after you launch an on demand EC2 scan, will list Terminated instances since the filtering happens after the scan job is submitted to the Scanner Appliance.
What User Permissions are needed for EC2 Scans?	Managers and Unit Managers can start, schedule and manage EC2 scans using Qualys VM/VMDR and Qualys PC as per their Qualys license. Qualys VM/VMDR -Perform vulnerability scans on EC2 assets -Configure Virtual Scanner Appliance (AMI instance) -Create/manage EC2 connectors using Qualys AssetView (AV) Qualys PC -Perform compliance scans on EC2 assets -Configure Virtual Scanner Appliance (AMI instance) -Create/manage EC2 connectors using Qualys AssetView (AV) Unit Manager requirements: IPs for the EC2 environment must be added to the Unit Manager's business unit by a Manager via asset group. An appliance configured by a Unit Manager must be added to at asset group in the Unit Manager's business unit by a Manager.
How to view platform provider info on virtual scanner appliances?	You'll see the platform provider info for a virtual scanner appliance that's been deployed on Amazon EC2 (or another cloud platform) within your Qualys account. You'll see this info in the General Information section when you view or edit the appliance (from Scans > Appliances).  Edit Scanner Appliance General Information Scanner Appliance: * abhi-exp-vs Network: Global Default Network User Login: quays_aa4 Type: Virtual Scanner Platform Provider: Amazon EC2 Personalization Code: 101033129111 Polling Interval : * 60 Notification: ☐ Email status if scanner appli 1 heartbeat checks (4 h Model: cvscanner Scanner Tags: Scanner Appliance Information General Information Scanner Appliance: abhi-exp-vs Network: Global Default Network Type: Virtual Scanner Platform Provider: Amazon EC2 Personalization Code: 101033129111 Polling Interval: 60 seconds User Login: quays_aa4 Status: Not Connected Heartbeat Checks Missed: 0 Active: No Owner: - Created: - Modified By: - Modified: - Scanner Tags: - Model: cvscanner Scanner Capacity The trend is calculated in 6 hour intervals. Select an area of the chart to zoom in. Launch Help General Information Versions LAN Settings Proxy Settings Comments Reboot Cancel Launch Help General Information WAN Settings LAN Settings Proxy Settings Users Asset Groups Versions Comments Used Close Edit

Queries	Solutions
Troubleshooting connectivity	Qualys Scanner Appliance must make regular connections to the Qualys Cloud Platform over HTTPS. Please be sure to resolve connectivity issues to ensure proper functioning of your appliance. The Communication Failure message appears if there is a network breakdown between the scanner and the Qualys Cloud Platform. The communication failure may be due to one of these reasons: the local network goes down, Internet connectivity is lost for some reason, or any of the network devices between the scanner and the Qualys Cloud Platform goes down. The Network Error message indicates the Scanner Appliance attempted to connect to the Qualys Cloud Platform and failed. You'll see an error code and description to help you with troubleshooting. Errors can be related to the proxy server and connection errors with Qualys Cloud Platform. The Qualys Cloud Platform logs results of connectivity checks and overall personalization process on the Amazon EC2 System Console. If you see "No connectivity to qualysguard.qualys.com - please fix." messages, please verify that your VPN Network ACLs and Security Groups allow outbound HTTPS (TCP port 443) access. If you are using a proxy server, ensure that the scanner can reach the proxy server, and that the proxy server can access the Qualys cloud platform.

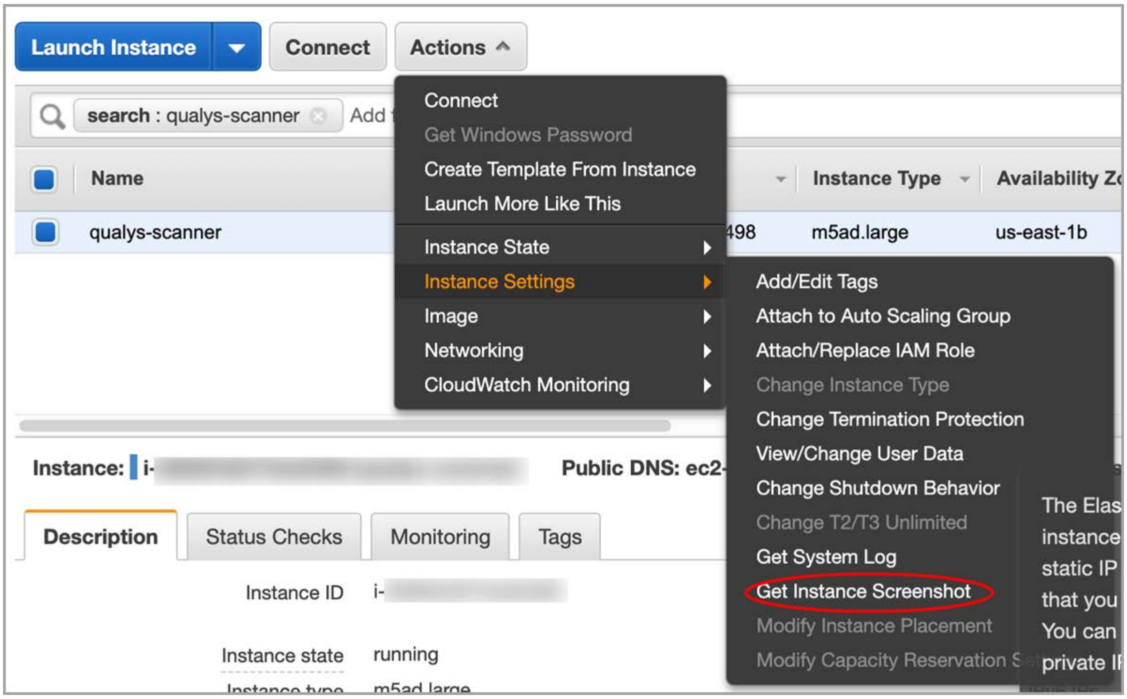
Troubleshooting

To troubleshoot or identify errors with your Qualys Virtual Scanner Appliance, you can access the system logs from **Get Instance Screenshot** and **Get System Log** features within the AWS EC2.

Get Instance Screenshot

To generate the scanner instance console screenshot, log into the EC2 console GUI and locate your scanner instance.

Click **Actions** > **Instance Settings** > **Get Instance Screenshot**.



qualys-scanner 498 m5ad.large us-east-1b

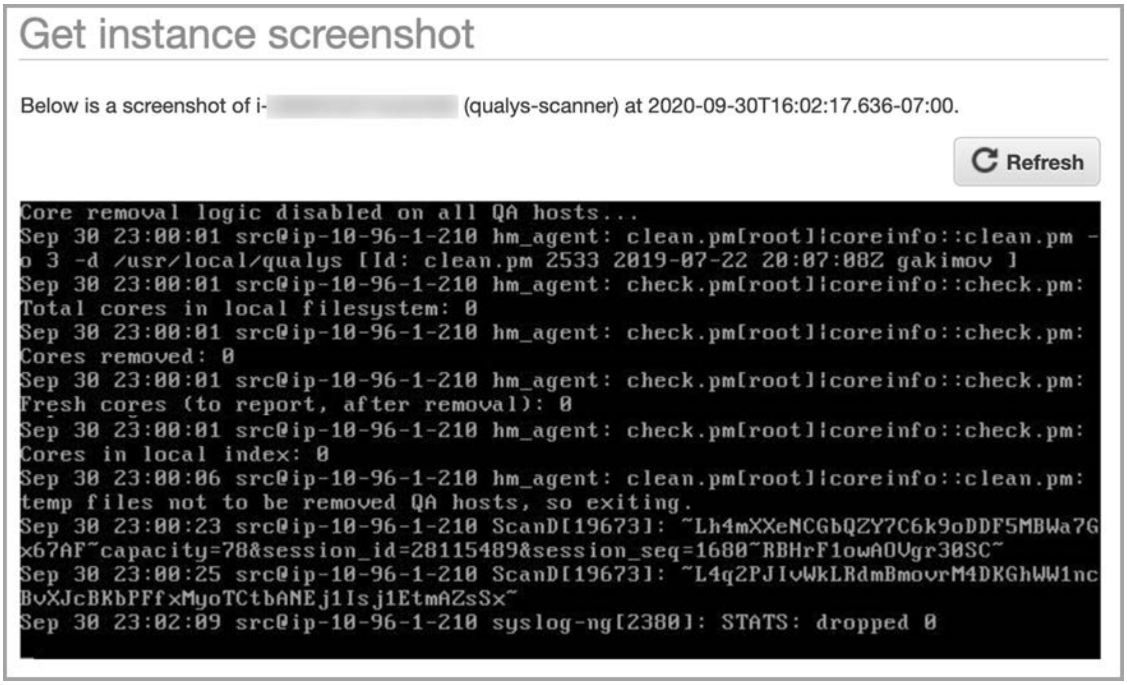
Instance: i-[redacted] Public DNS: ec2-

Instance ID i-[redacted]

Instance state running

Instance type m5ad.large

Click **Refresh** to fetch the latest set of logs.



Get instance screenshot

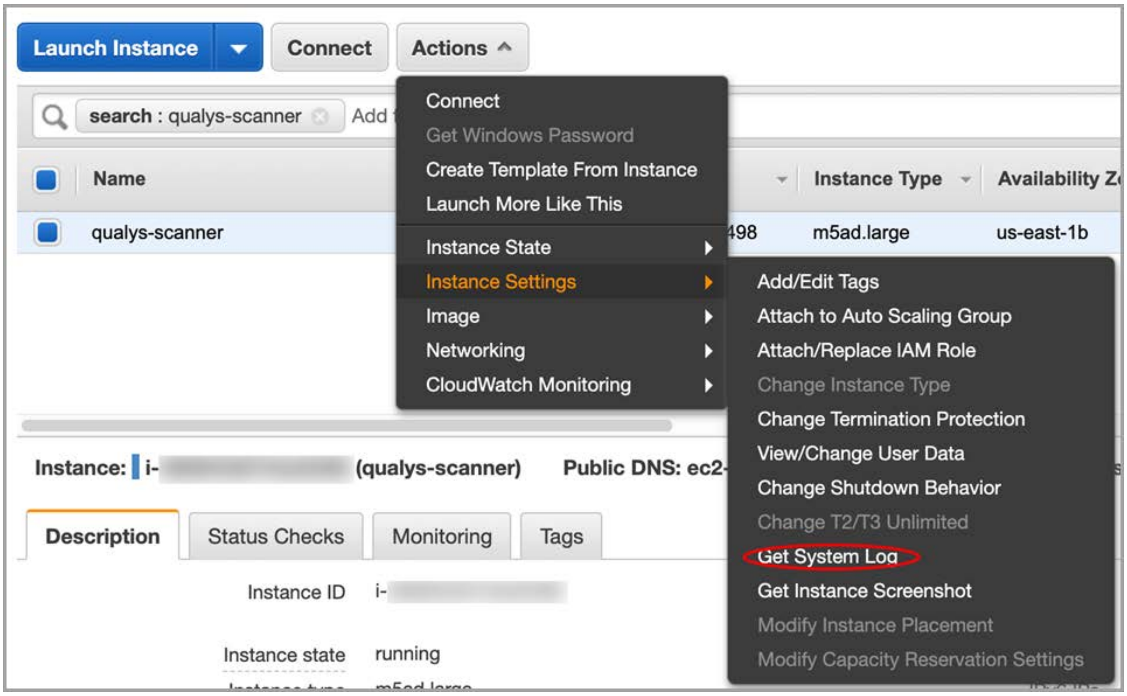
Below is a screenshot of i-[redacted] (qualys-scanner) at 2020-09-30T16:02:17.636-07:00.

```
Core removal logic disabled on all QA hosts...
Sep 30 23:00:01 src@ip-10-96-1-210 hm_agent: clean.pm[root]¦coreinfo::clean.pm -
o 3 -d /usr/local/qualys [Id: clean.pm 2533 2019-07-22 20:07:08Z gakimov ]
Sep 30 23:00:01 src@ip-10-96-1-210 hm_agent: check.pm[root]¦coreinfo::check.pm:
Total cores in local filesystem: 0
Sep 30 23:00:01 src@ip-10-96-1-210 hm_agent: check.pm[root]¦coreinfo::check.pm:
Cores removed: 0
Sep 30 23:00:01 src@ip-10-96-1-210 hm_agent: check.pm[root]¦coreinfo::check.pm:
Fresh cores (to report, after removal): 0
Sep 30 23:00:01 src@ip-10-96-1-210 hm_agent: check.pm[root]¦coreinfo::check.pm:
Cores in local index: 0
Sep 30 23:00:06 src@ip-10-96-1-210 hm_agent: clean.pm[root]¦coreinfo::clean.pm:
temp files not to be removed QA hosts, so exiting.
Sep 30 23:00:23 src@ip-10-96-1-210 ScanD[19673]: ~Lh4mXXeNCGbQZY7C6k9oDDF5MBWa7G
x67AF~capacity=78&session_id=28115489&session_seq=1680~RBHrF1owAOVgr30SC~
Sep 30 23:00:25 src@ip-10-96-1-210 ScanD[19673]: ~L4q2PJIvWkLRdmBmovrM4DKGhWW1nc
BvXJcBKbPFfxMyoTCtbANEj1Isj1EtmAZsSx~
Sep 30 23:02:09 src@ip-10-96-1-210 syslog-ng[2380]: STATS: dropped 0
_
```

Get System Logs

The **Get System Log** feature displays the serial console output, providing buffered information posted shortly after an instance state transition (start, stop, reboot, and terminate).

To generate the serial console output logs, log into the EC2 console GUI and select your scanner instance. Click **Actions** > **Instance Settings** > **Get System Log**.

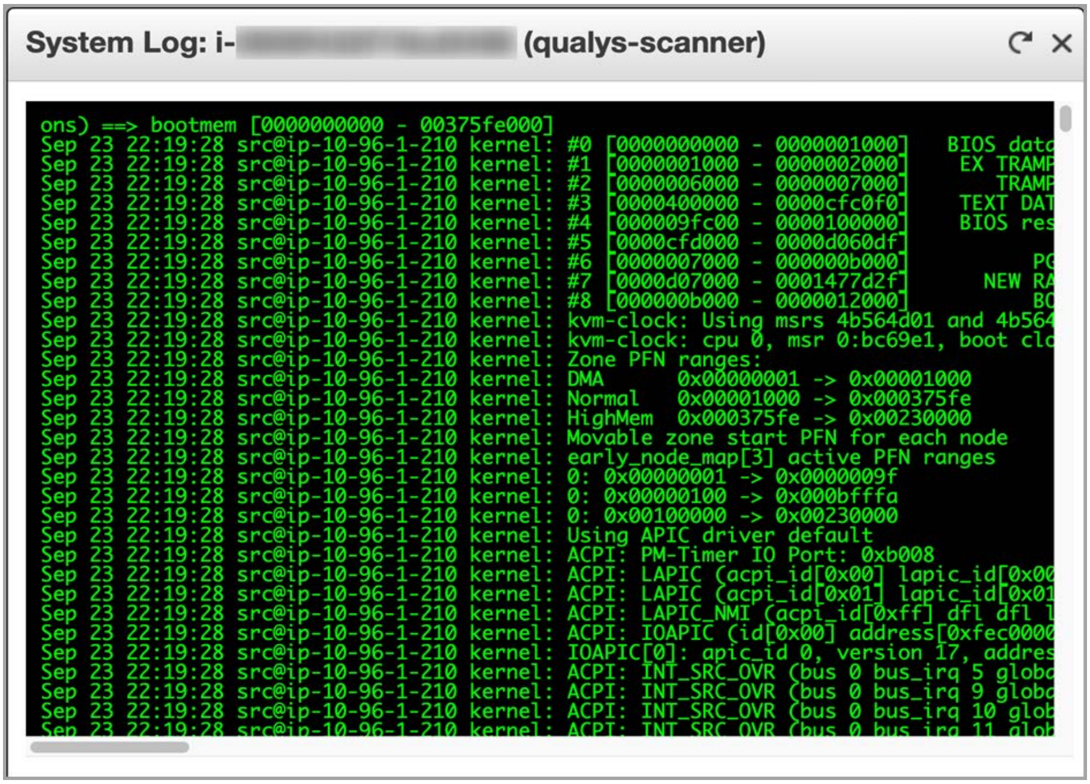


Instance: i-[redacted] (qualys-scanner) Public DNS: ec2-

Instance ID i-[redacted]

Instance state running

The system log is displayed.



System Log: i-[redacted] (qualys-scanner)

```
ons) ==> bootmem [0000000000 - 00375fe000]
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: #0 [0000000000 - 0000001000]   BIOS data
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: #1 [0000001000 - 0000002000]    EX TRAMP
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: #2 [0000006000 - 0000007000]       TRAMP
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: #3 [0000400000 - 0000cfc0f0]    TEXT DAT
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: #4 [000009fc00 - 0000100000]    BIOS res
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: #5 [0000cfd000 - 0000d060df]
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: #6 [0000007000 - 000000b000]          PG
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: #7 [0000d07000 - 0001477d2f]      NEW RA
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: #8 [000000b000 - 0000012000]          BO
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: kvm-clock: Using msrs 4b564d01 and 4b564
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: kvm-clock: cpu 0, msr 0:bc69e1, boot clo
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: Zone PFN ranges:
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: DMA      0x00000001 -> 0x00001000
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: Normal   0x00001000 -> 0x000375fe
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: HighMem  0x000375fe -> 0x00230000
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: Movable zone start PFN for each node
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: early_node_map[3] active PFN ranges
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: 0: 0x00000001 -> 0x0000009f
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: 0: 0x00000100 -> 0x000bfffa
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: 0: 0x00100000 -> 0x00230000
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: Using APIC driver default
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: ACPI: PM-Timer IO Port: 0xb008
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: ACPI: LAPIC (acpi_id[0x00] lapic_id[0x00
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: ACPI: LAPIC (acpi_id[0x01] lapic_id[0x01
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: ACPI: LAPIC_NMI (acpi_id[0xff] dfl dfl l
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: ACPI: IOAPIC (id[0x00] address[0xfec0000
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: IOAPIC[0]: apic_id 0, version 17, addres
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: ACPI: INT_SRC_OVR (bus 0 bus_irq 5 globa
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: ACPI: INT_SRC_OVR (bus 0 bus_irq 9 globa
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: ACPI: INT_SRC_OVR (bus 0 bus_irq 10 glob
Sep 23 22:19:28 src@ip-10-96-1-210 kernel: ACPI: INT_SRC_OVR (bus 0 bus_irq 11 glob
```

Note: From the EC2 console GUI, the posted output is not continuously updated and has a limit of displaying the first 64 KB console output.

To retrieve the latest 64 KB of serial console output via AWS CLI, the scanner instance needs to be deployed on a Nitro-based hypervisor.

For a list of instance types built on the Nitro System, see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-types.html#ec2-nitro-instances.

Get System Log via AWS CLI

By default, the serial console output returns buffered information that was posted shortly after an instance transition state (start, stop, reboot or terminate). This information is available for at least one hour after the most recent post. Only the most recent 64 KB of serial console output is available.

You can optionally retrieve the latest serial console output at any time during the instance lifecycle using the '--latest' option. This option is supported on instance types that use the Nitro hypervisor.

To fetch the serial console logs via CLI, do the following.

1) Set up and configure your AWS CLI environment using AWS latest CLI version, https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-install.html

2) Run the following AWS CLI command:

```
aws ec2 get-console-output --instance-id <instance id> --latest --
output text
```

Note: '--latest' option is only supported on instance types that use the Nitro Hypervisor.

For any errors and troubleshooting tips, visit Scanner Appliance Troubleshooting and FAQs.