Securing Amazon Web Services with Qualys

July 28, 2021

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

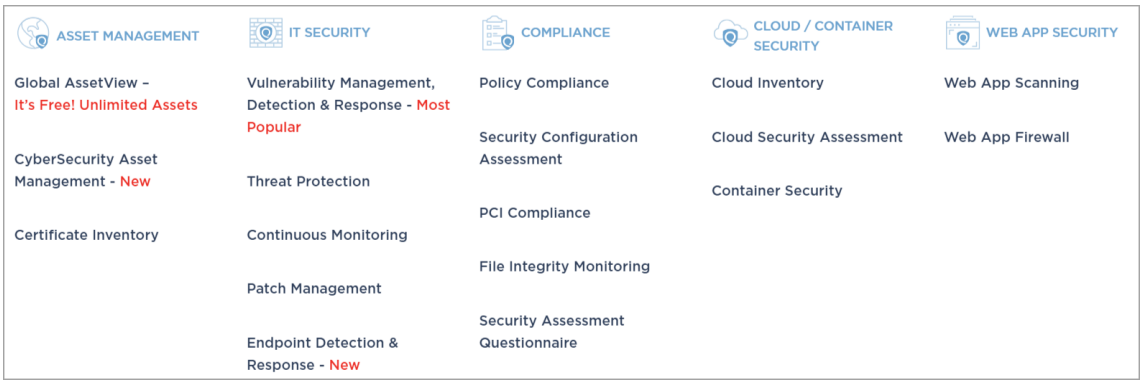
Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at www.qualys.com/support/

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

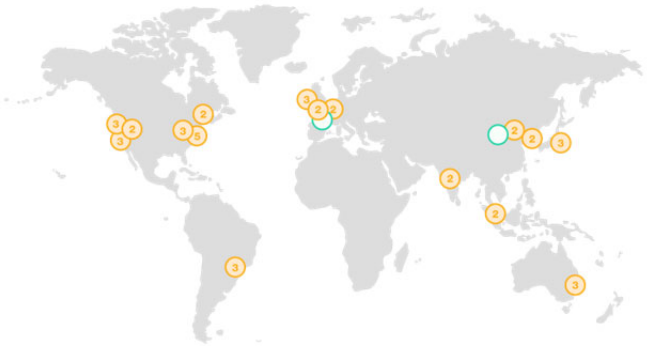
With Qualys Cloud Platform you get a single view of your security and compliance - in real time. If you're new to Qualys we recommend you to visit the Qualys Cloud Platform web page to know more about our cloud platform.



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

- Pre-authorized 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!

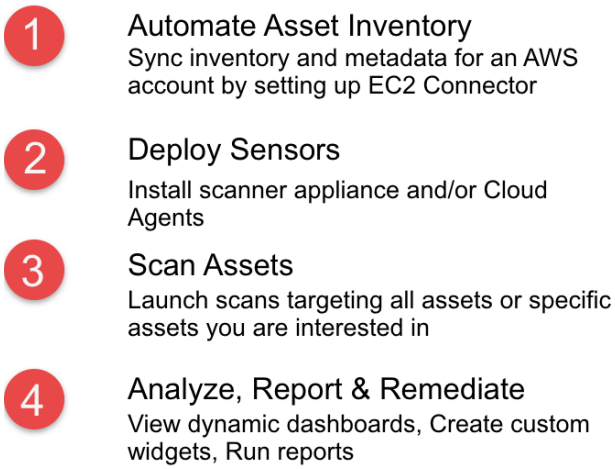
Video Tutorials get you familiar with basics

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.



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 EC2 Connector

This is the first step for securing AWS Infrastructure. In this section we will go through the steps required to setup the EC2 connector. Qualys recommends you setup one EC2 connector per AWS account.

Qualys discovers and syncs asset inventories every 4 hours. Asset inventory is independent of a scan. See AWS APIs used by EC2 Connector to discover assets.

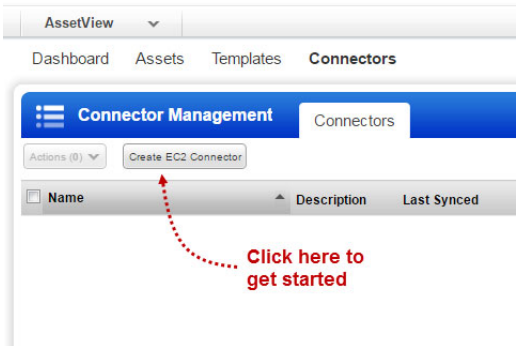
Cross-Account Role Authentication for EC2 Connectors

Cross-account role allows Qualys to access your AWS EC2 instances without the need to share your AWS security credentials. Qualys will access your AWS EC2 instances by assuming the IAM role that you create in your AWS account. This eliminates the overhead of management of IAM user keys in your Qualys subscription.

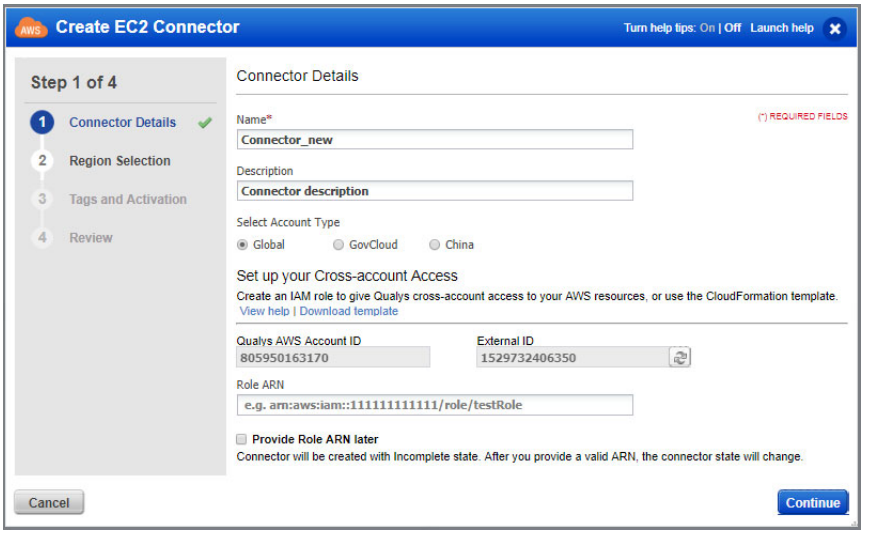
ARN authentication

You can create new EC2 connectors using cross-account role authentication. Let us see the steps to create EC2 connectors using cross-account role authentication.

1) Go to AssetView (AV) > Connectors and click Create EC2 Connector.



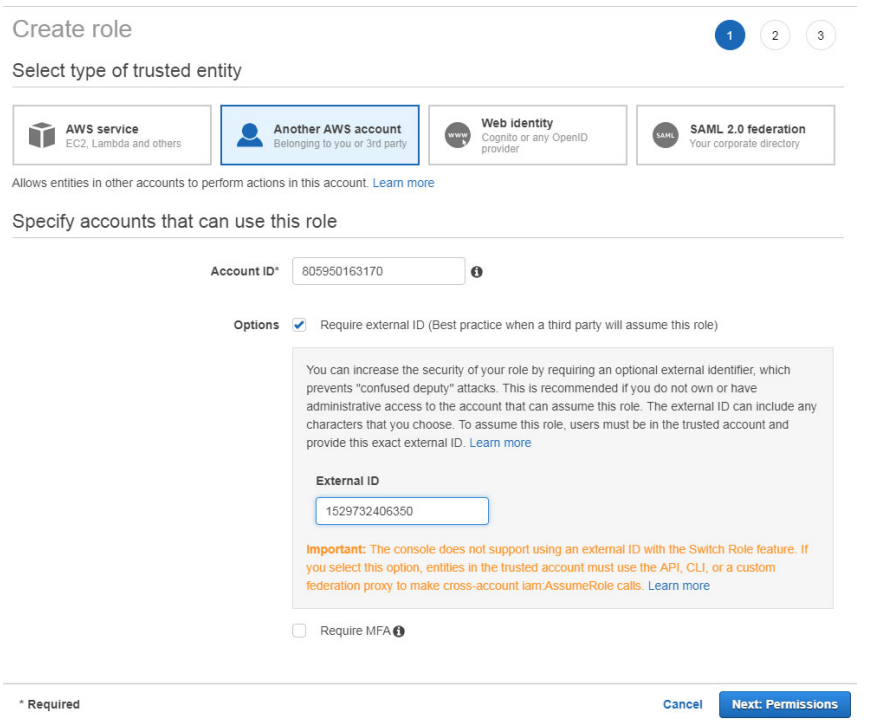
2) Provide a connector name, description (optional) and select the account type.



3) Launch AWS console and navigate to IAM > Roles section. Click Create Role.

4) Add another AWS account.

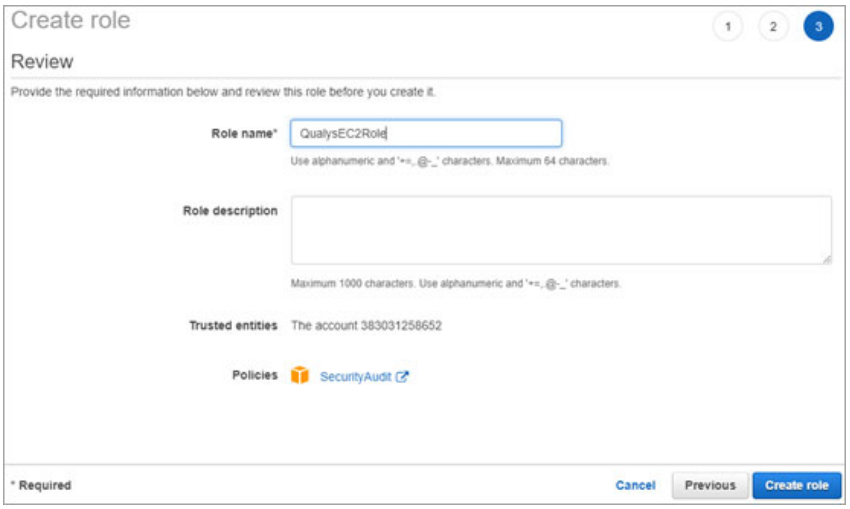
- Choose ‘Another AWS account’. (Use 1 AWS account per connector.)
- Paste in the Account ID (AWS Account ID) and External ID from connector details
- Click ‘Next: Permissions’.



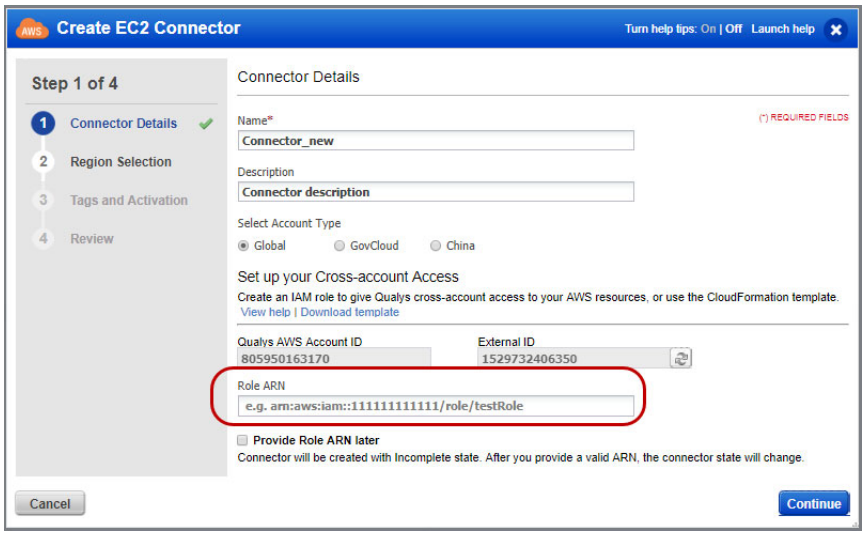
5) Find the policy titled “SecurityAudit” and select the check box next to it. Click Next: Tags.

6) Click ‘Next: Review’.

7) Enter a role name (e.g. QualysEC2Role) and click Create role.



8) Click on the role you just created to view details. Copy the Role ARN value and paste the Role ARN value into your Qualys connector details.



9) Click Continue on the connector creation wizard and complete the remaining steps of region selection, tags & module activation.

CloudFormation Template

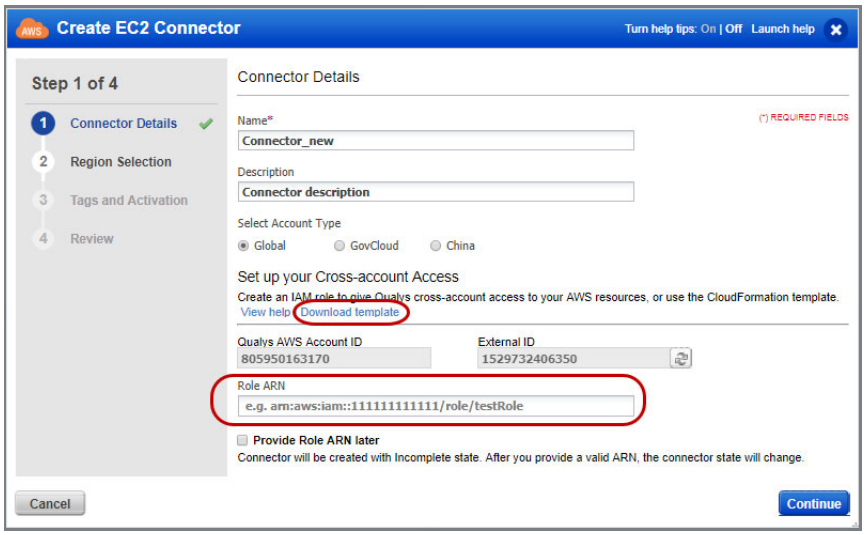
You can automate creation of EC2 connectors using CloudFormation template, which is downloadable directly from the UI.

Let us see the steps to create new EC2 connector by following the UI instructions and manually creating the necessary role in AWS console.

1) Go to AssetView (AV) > Connectors and click Create EC2 Connector.

2) Provide a connector name, description (optional) and select the account type.

3) Click 'Download template' link. This will download the CloudFormation template that you can run in the AWS console that you want to configure.

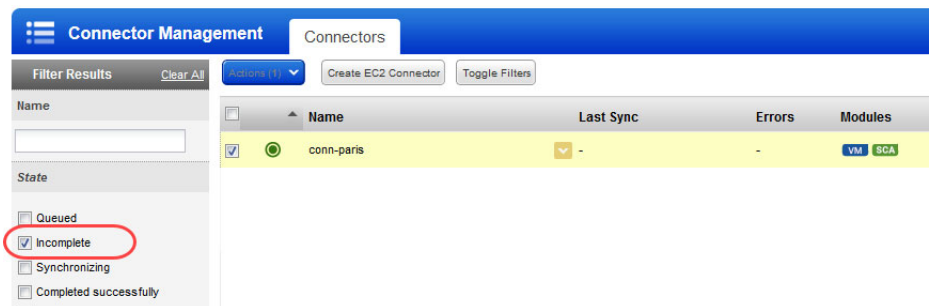


4) Select the 'Provide Role ARN later' option. This will create a connector in Incomplete state and you can edit it later to update the Role ARN. Click 'Continue' to perform the remaining steps and finish creating the connector.

5) Log in to Amazon Web Services (AWS) and go to CloudFormation.

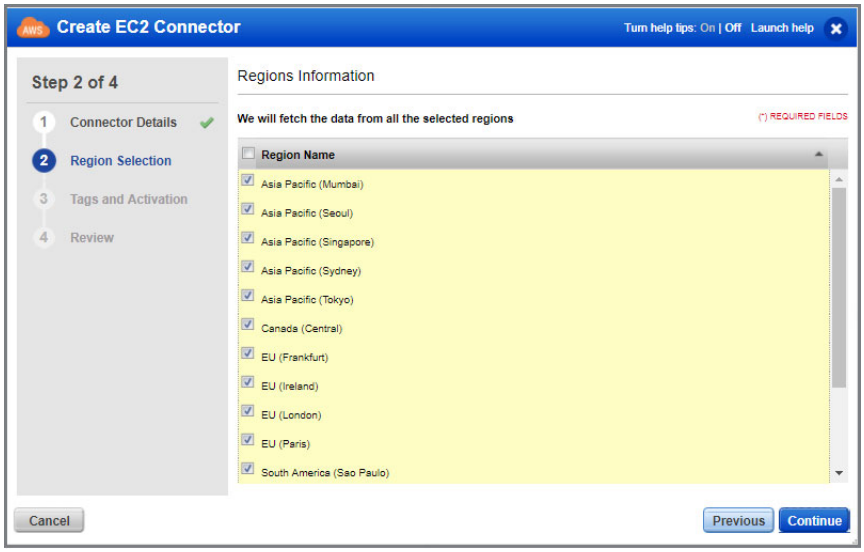
6) Create stack & upload the template downloaded in the step 3. When the stack is complete, copy the Role ARN value from the output.

7) Navigate back to AssetView (AV) > Connectors and locate the connector by filtering on Incomplete state. Then edit the connector and paste the ARN value into the details.



Selecting EC2 regions

Select the regions you want to collect EC2 data from. You can use the Sync Assets button to get the asset count for each region. If you select only a few regions here, you can later modify to add additional regions. We recommend to select all regions. This gives you the visibility whether someone has turned up instance in another region.

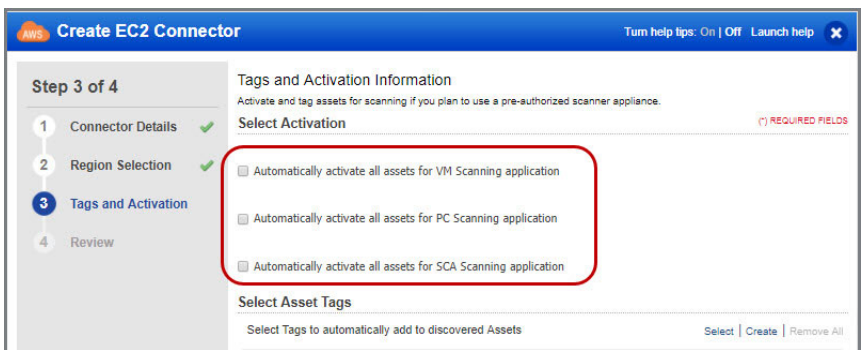


Activating Assets

EC2 assets must be activated for your Qualys license in order to scan them. If you are going to use the Pre-authorized scanner in AWS, you are required to activate your assets here or manually from AssetView. By choosing “Automatically activate” we’ll activate all discovered EC2 assets (size medium and above). This makes them ready for scanning.

By default, assets with instance type m1.small, t1.micro or t2.nano are excluded from activation and cannot be scanned. You can reach out to your Technical Account Manager or Qualys Support to lift this limitation and allow assets with these instance types to be activated.

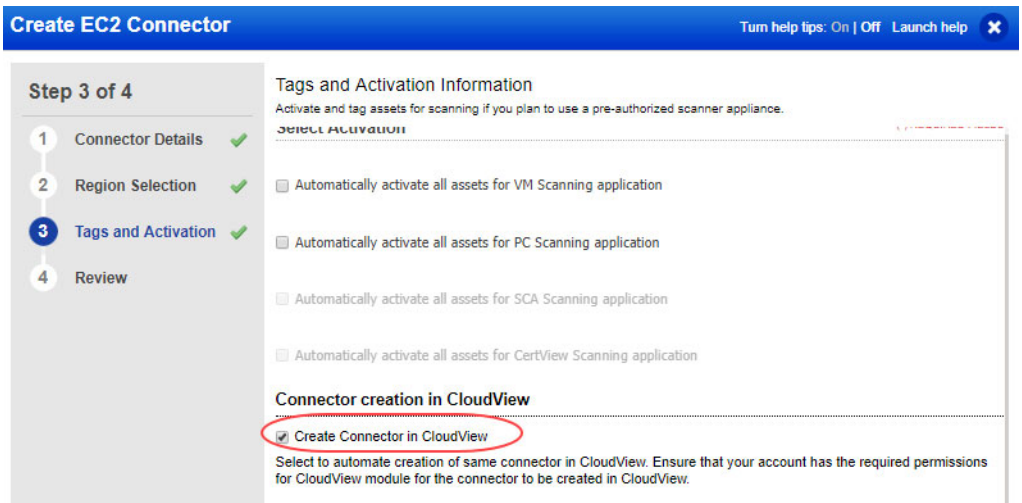
Once this capability is enabled for your subscription, the next time the connector runs assets with m1.small, t1.micro or t2.nano instance types will auto-activate for VM/PC/SCA as configured in the connector settings.



Want to activate later? Just go to the Assets tab in AssetView, select the assets you want to activate, and choose “Activate Assets” from the Actions menu.

Enable AWS connector for CloudView

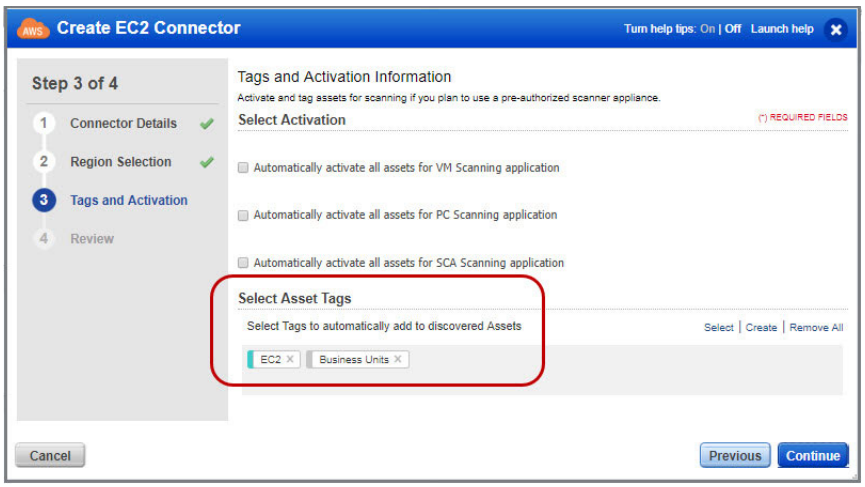
While creating a new AWS connector in AssetView or editing an existing one, you can use the “Create Connector in CloudView” option to enable that AWS connector to be available in the CloudView App as well. This will save you from creating a separate connector in CloudView.



Once enabled in AssetView, disabling this option later will not remove the corresponding connector from CloudView. you need to explicitly remove the connector from the CloudView app.

Assigning Tags

EC2 Scans with Qualys relies upon a “scan-by-tag” workflow. It is a best practice to associate a Qualys tag to all of your EC2 instances. To scan using a pre-authorized scanners use of tags is required. It’s recommended you create at least one generic Asset Tag (for example, "EC2") and have the connector automatically apply the EC2 tag to all imported assets.



You can also create dynamic tags that allow you to tag your EC2 assets automatically based upon the IP address of the discovered EC2 instances & other EC2 attributes.

Click Finish to complete the connector creation.

What’s next

Once you create your connector, we’ll discover EC2 instances, activate them and add them to your Qualys account. You’ll see them in your assets inventory in your Qualys Cloud Suite apps.

App	Asset inventory
VM/VMDR, PC, SCA	Assets > Host Assets tab
AssetView	Assets tab

Upgrade existing connector to cross-account role

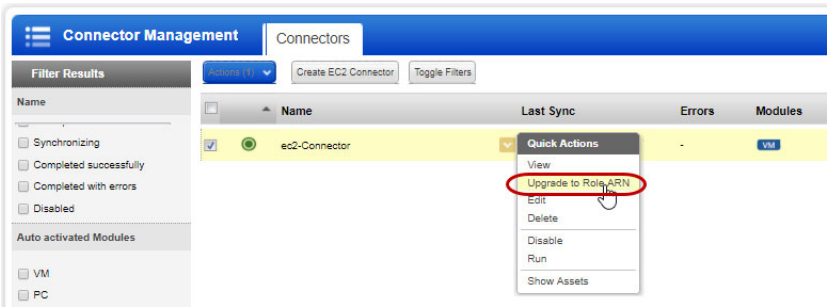
You can now upgrade your existing connectors that are created using access key to cross-account role authentication. The new connectors only support cross-account access roles and not key-based connectors

We'll help you migrate your existing EC2 connectors to now use cross-account access roles. Note that this migration of your existing EC2 connector to cross account role is unidirectional and cannot be reverted.

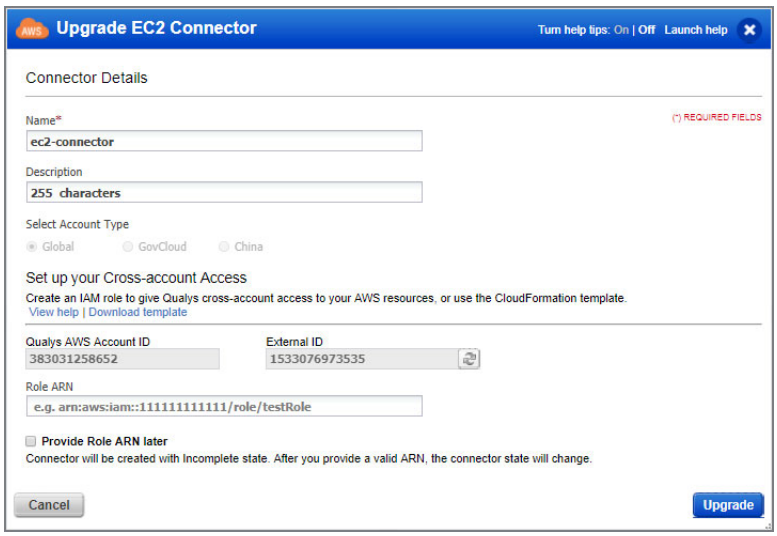
> Support for key-based connectors will be discontinued after 180 days. Ensure that you upgrade your key-based connectors to cross-account role within 180 days.

Steps to upgrade key-based connectors to cross-account role

1) Go to AssetView > Connectors. Identify the EC2 connector you want to upgrade, then right-click and select Upgrade to Role ARN from the quick actions menu.



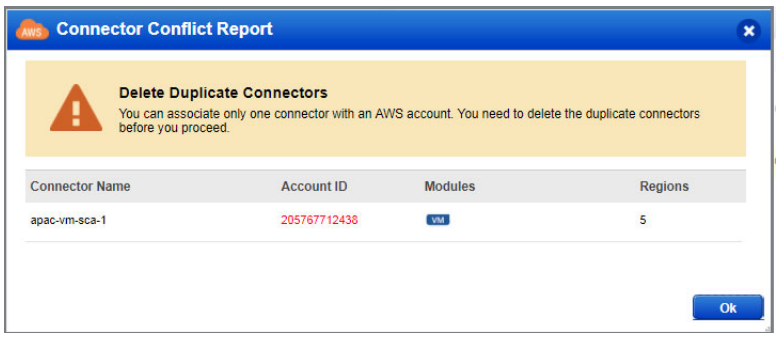
Provide ARN details and click Upgrade.



Upgrade multiple EC2 connectors for same AWS account

You can now create only one connector for each unique AWS account. If you have multiple EC2 connectors for the same AWS account, you need to retain only one of the two connectors. Before you remove one of the connectors, ensure that you add the settings (for example, regions, tags and activation) to the connector you plan to retain and then switch to cross-account role based authentication.

If you have duplicate connectors for the same AWS account and you try to upgrade any one of them you will be provided with a conflict report listing the duplicate connectors.



Delete duplicate connectors and retain only one connector for each AWS account.

Create only one connector for each unique AWS account. It's recommended that you merge multiple EC2 connectors into one by removing duplicate connectors before you upgrade to ARN.

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.

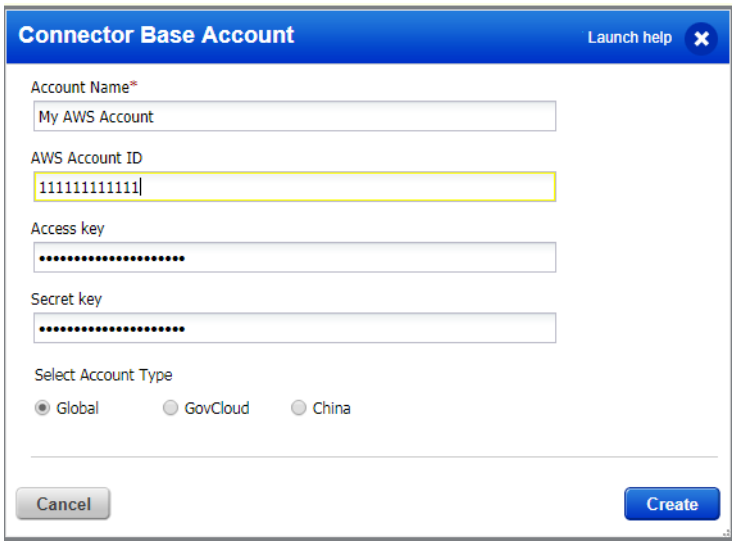
You can configure to use your own AWS account as a base account while setting up the AWS Connectors instead of using Qualys account. You need to map your AWS account ID (in case of multiple AWS accounts, at least one AWS account) with the base account you create.

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). If you do not create a base account, you can still create a connector.

Go to Connectors > Connectors and then click Configure Base Account. Provide name, AWS account ID, access and secret keys and then select the account type.



You can create only one base account per account type. Ensure that the AWS account ID for which you configure that base account has policies associated in the AWS console. To know detailed configuration steps on AWS console, refer to Base Account Configuration in AWS.

Edit a Base Account

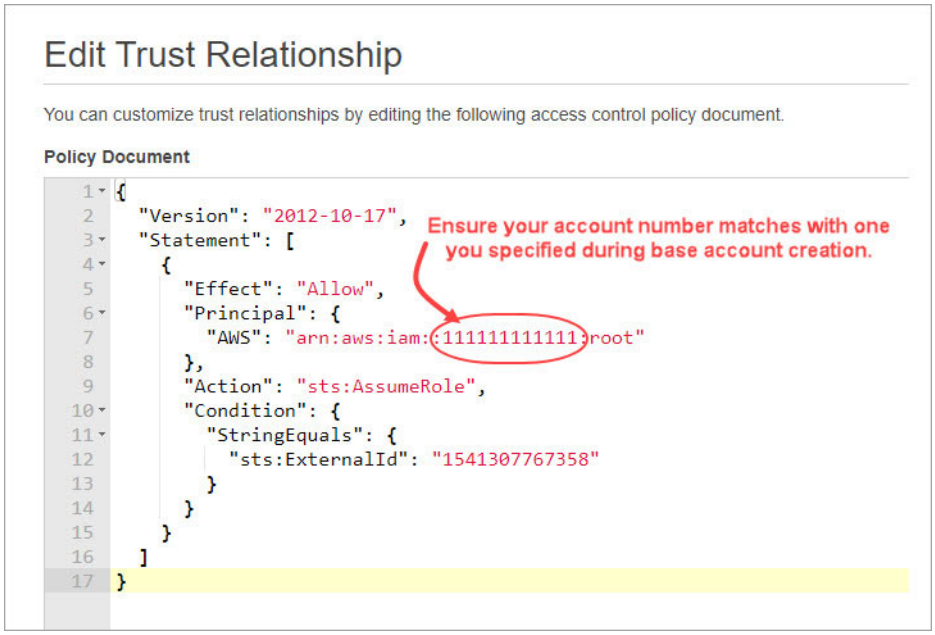
Select the base account you want to edit and click the quick action menu, then select Edit. You can edit name, AWS account ID, access keys and secret keys. You cannot edit the account type.

Updating Existing Connectors to Base Account

To update the existing AWS connectors with cross-account role to base account usage, you need to

-create a base account using AWS account ID (as described in Create a Base Account).

-update the Trust Entities for your IAM Roles: On AWS console, go to IAM role > Trust relationships and then Edit trust relationship. Ensure that the AWS account ID for which you configure that base account matches the account number in trusted relationships of the AWS console. Click Update Trust Policy.



Base Account Configuration in AWS

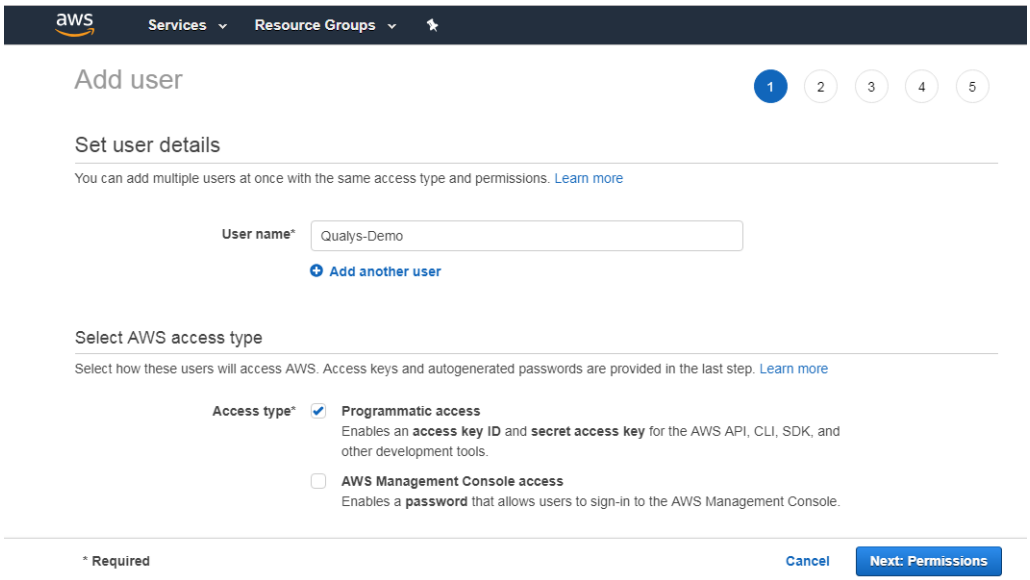
If you plan to use base account for your connectors, there are certain pre-requisites and settings that need to be configured on AWS console. The detailed steps and configuration required in AWS console for setting up base account is listed below.

Create IAM User and associate policy in AWS

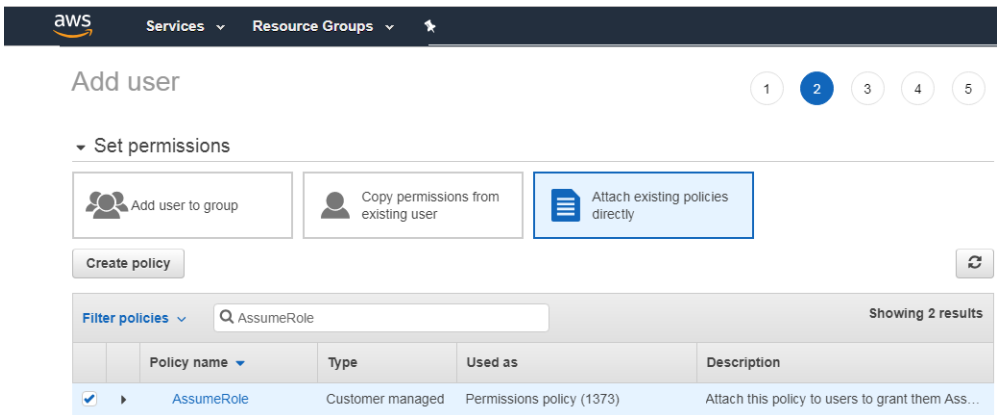
1. On the AWS console, navigate to AWS > Policies and create a policy (for example, AssumeRole) that contains the following JSON content.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1501205548000",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

2. Create IAM User. Navigate to Identity and Access Management > Users and then click Add user.



3. Provide a user name and enable Programmatic access for the user. Click Next: Permissions.



4. Select Attach existing policies directly and then type the name of the policy that you created (AssumeRole) in Filter policies. Select the policy (AssumeRole) you configured and then click Next: Tags.

Add tags if needed (as this is optional). Review the user settings you configured and then click Create user.

How does EC2 Connector work?

Asset Discovery: The EC2 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).

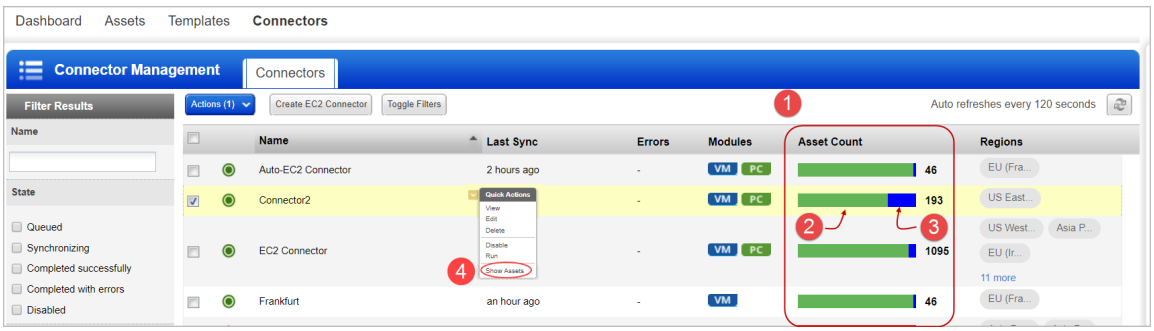
AWS retains the terminated instances for approximately one hour. However, Qualys stores record of all the terminated instances and you can always track the history and details of all such terminated instances.

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 EC2 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



The EC2 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 EC2 connector run.

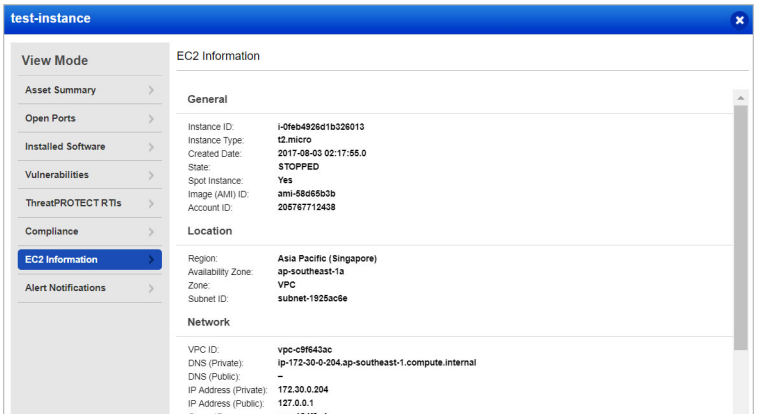
2. **Synchronized Assets** - In the Asset count column, the green portion represents assets synchronized. Synchronized count represents assets that are successfully processed at Qualys.

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.



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/2.0/create/am/awsassetdataconnector

Run Connector

https://qualysapi.qualys.com/qps/rest/2.0/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.

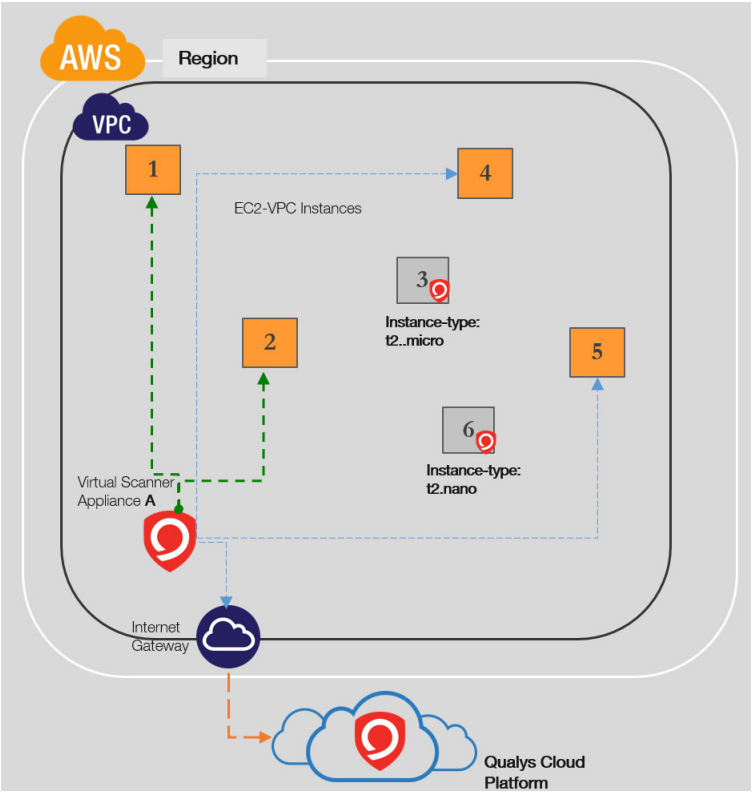
VPC: enables you to launch AWS resources into a virtual network that you've defined. This closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalability of AWS.

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.

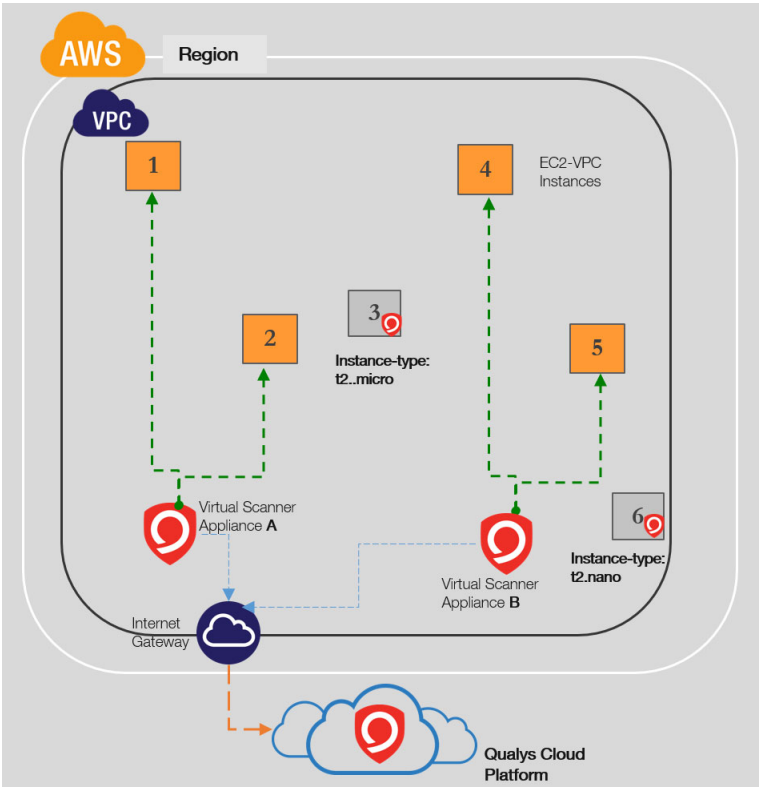
A Single scanner scans MULTIPLE instances in a VPC



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

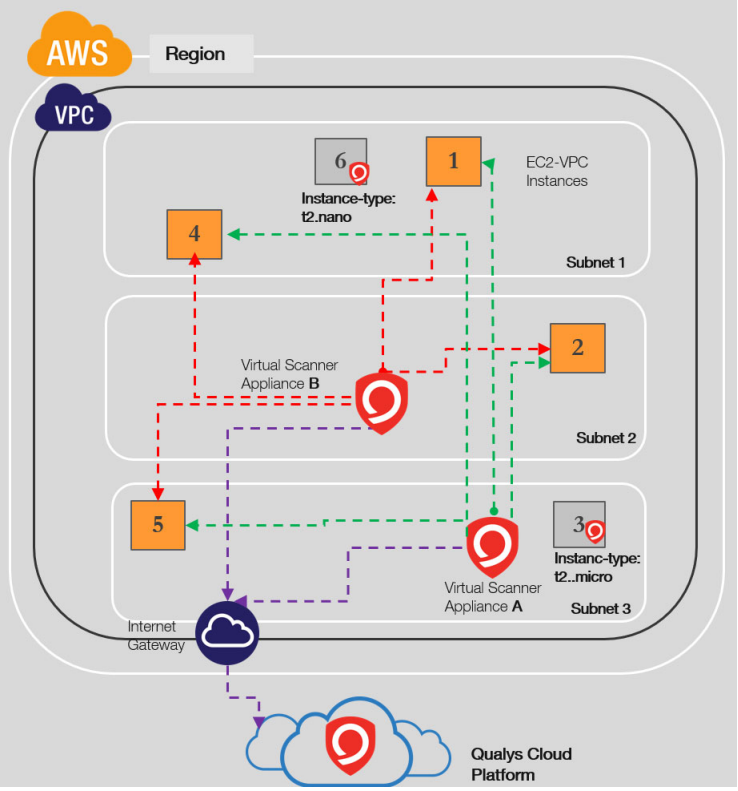


Based on number of instances and scan frequency, multiple scanners might be required to scan MULTIPLE instances in a VPC. Require at least one scanner per VPC. You can add more based on requirements.

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

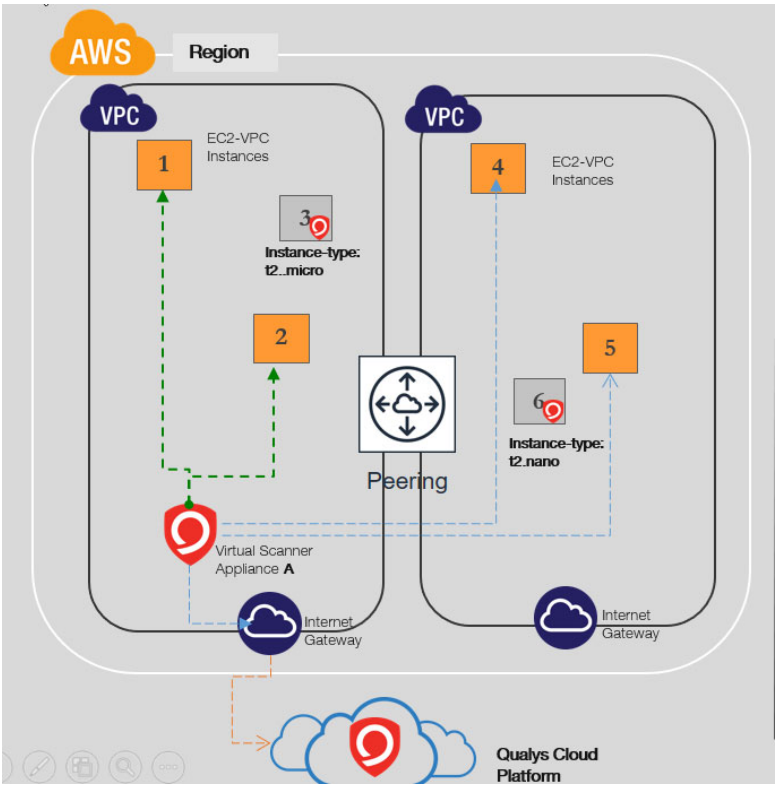


Scanners can typically work across the subnets within a VPC, unless there are restrictions in networks introduced

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

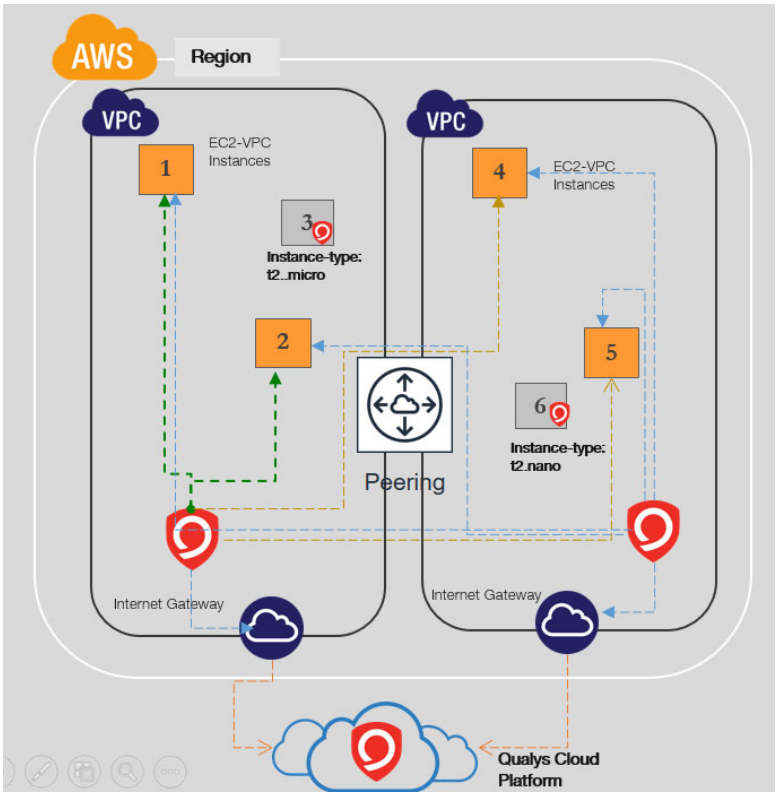


You can add more based on requirements.

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

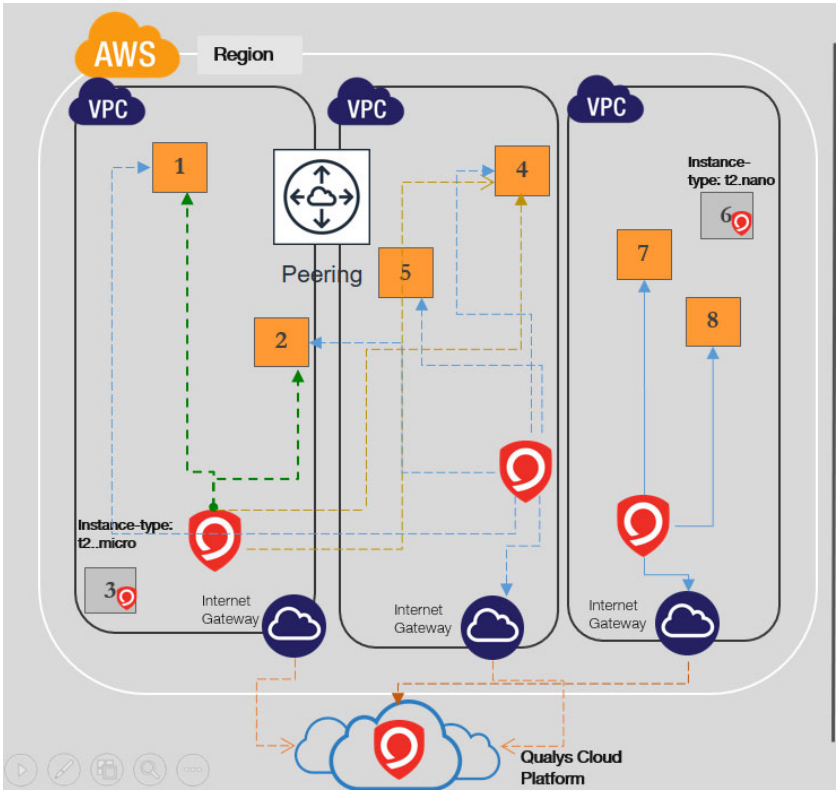


Based on number of instances and scan frequency, multiple scanners might be required to scan MULTIPLE instances across Peered VPCs in a region. You can add more based on requirements to ALLOW Scanning across VPC boundaries.

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

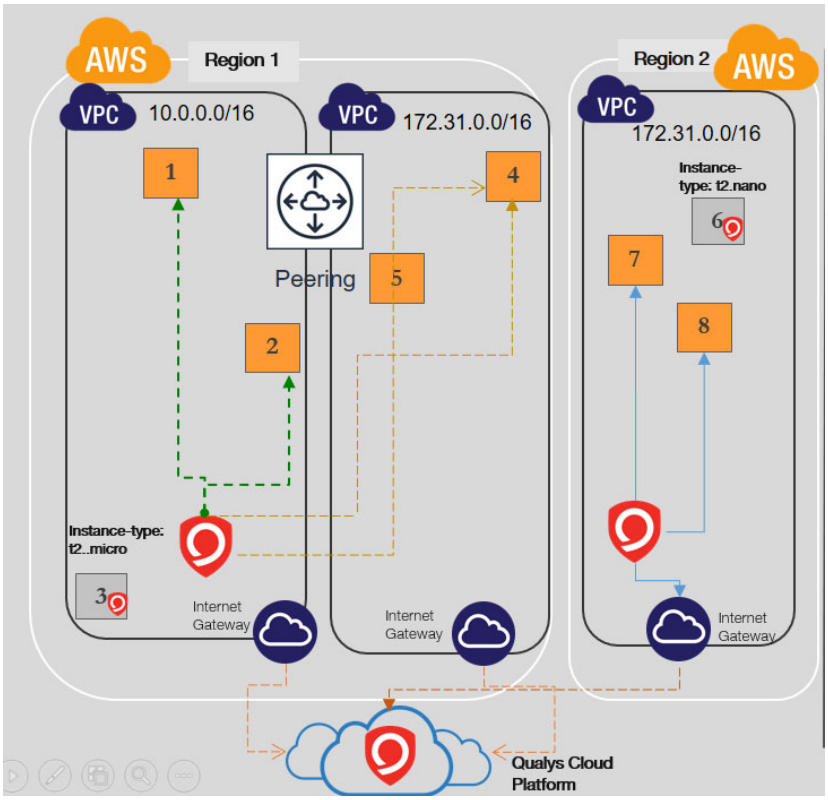


You can add more based on requirements to ALLOW Scanning across VPC boundaries.

Scanners needs to be configured to communicate to Qualys Cloud Platform and AWS EC2 & STS endpoints ove https (via security group 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 minimiz potential disruption to your environment. Cloud-agents are preferred method for scanning them.

Scanner cannot scan instances in VPCs with overlapping IP addresses



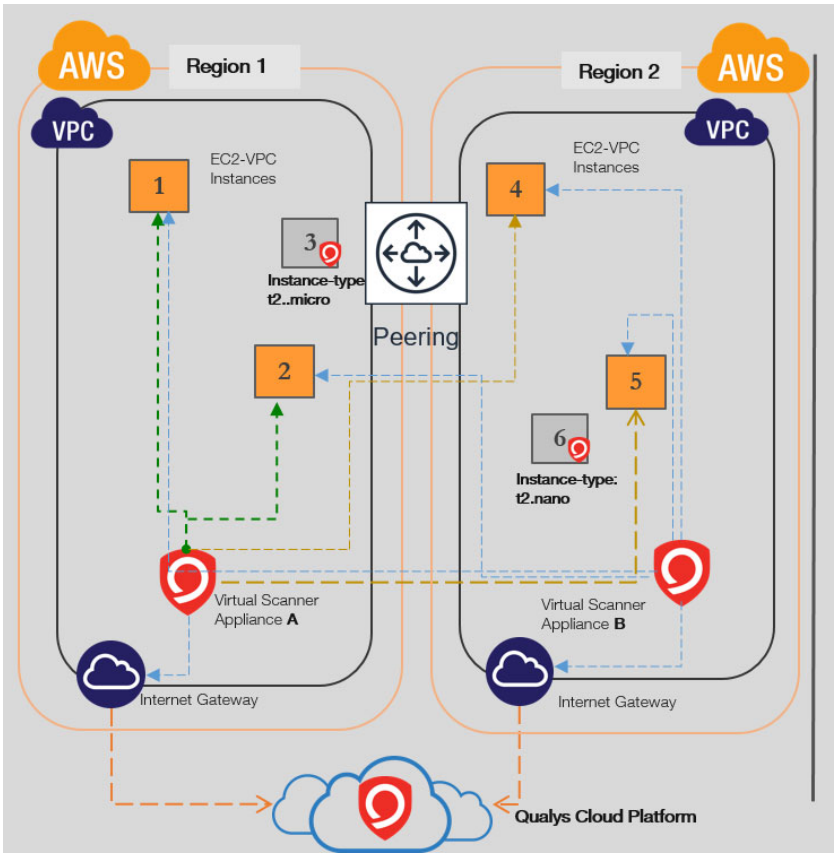
A single scanner cannot scan instances in VPCs with overlapping IP addresses due to reach-ability to a single subnet. You can add more based on requirements to ALLOW Scanning across VPC boundaries.

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

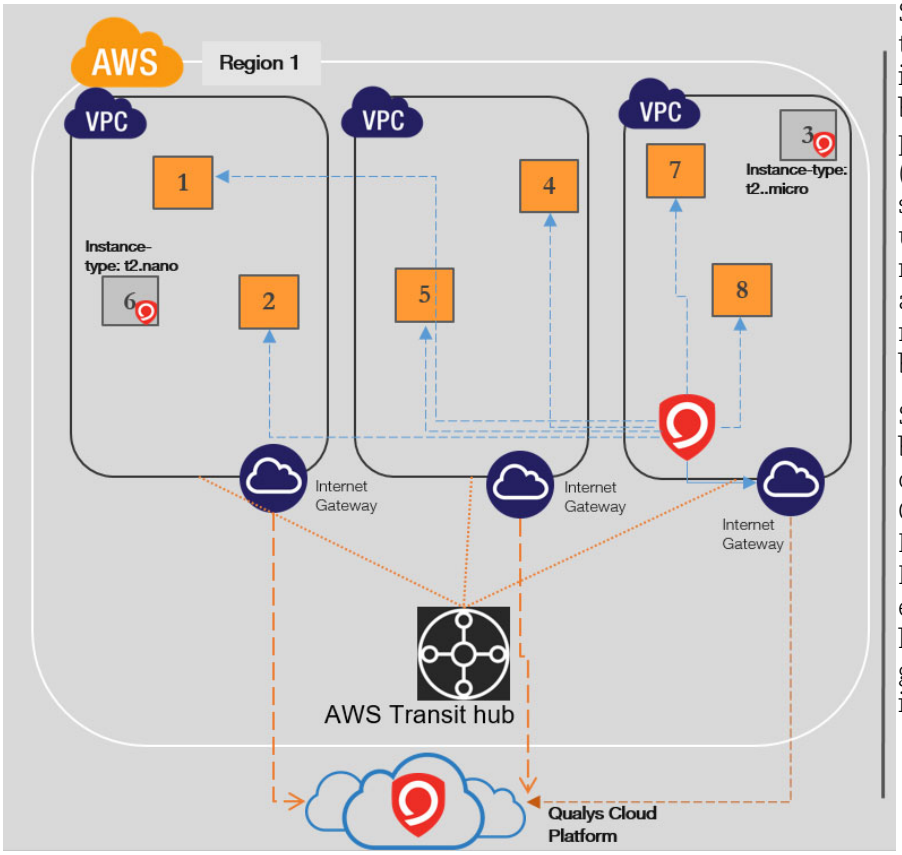


You can add more scanners based on requirements to ALLOW Scanning across Region across VPC boundaries.

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

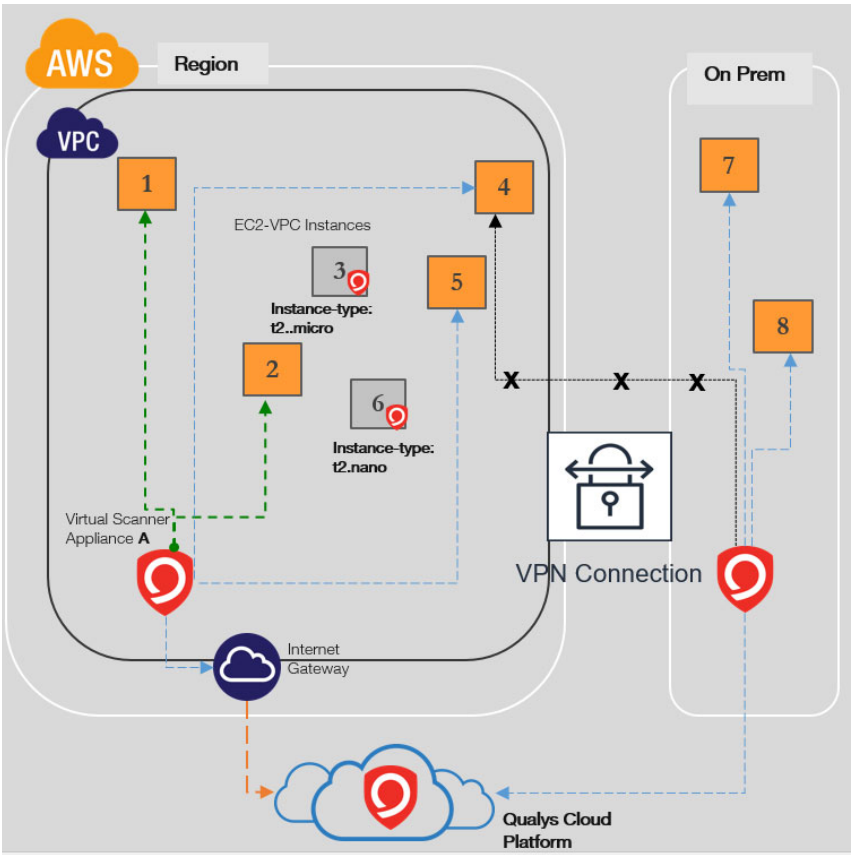


Since a network transit hub allows interconnectivity between virtual private clouds (VPC), a single scanner can be used to scan multiple instances across VPCs in a region connected by Transit gateway.

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 pre-authorized scanner appliance or Qualys Cloud Agent. Let's go through the steps involved in deploying these sensors.

Deploying Pre-authorized Virtual Scanner Appliance
Deploying Qualys Cloud Agent

Deploying Pre-authorized Virtual Scanner Appliance

Before we go through the actual steps involved in the pre-authorized 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 16 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 16 CPUs and 16 GB RAM.

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

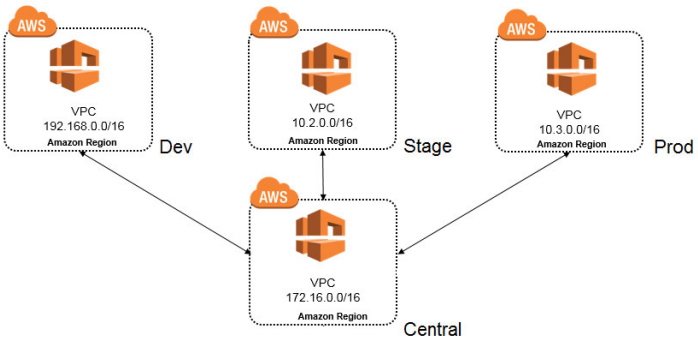
Scans cannot be launched on targets using t1.micro, m1.small, t2.nano instance types.

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

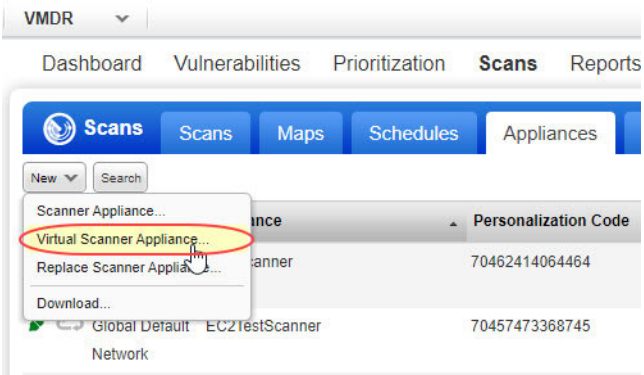
- STATIC ROUTES (IPV4 AND IPV6) - Option to configure “Static Routes” is not available from Qualys UI

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

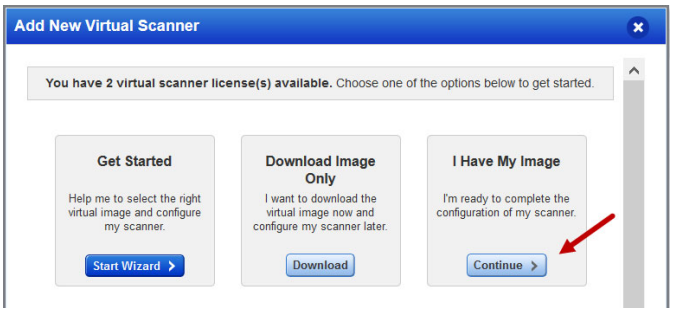
Configuration in Qualys

Setting up Virtual Appliance - Get Personalization Code

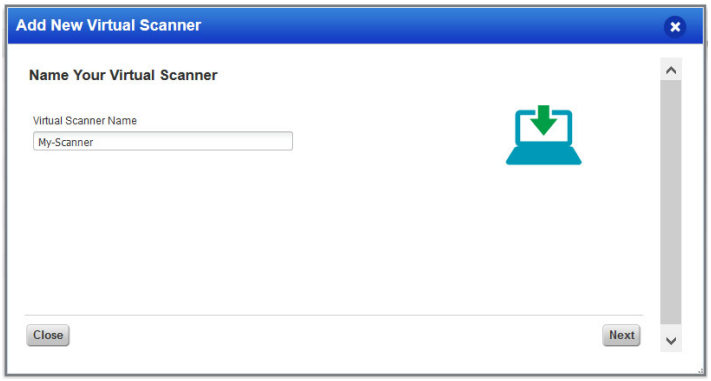
Select VM/VMDR or PC from the Qualys app picker. Then navigate to Scans > Appliances and select New > Virtual Scanner Appliance.



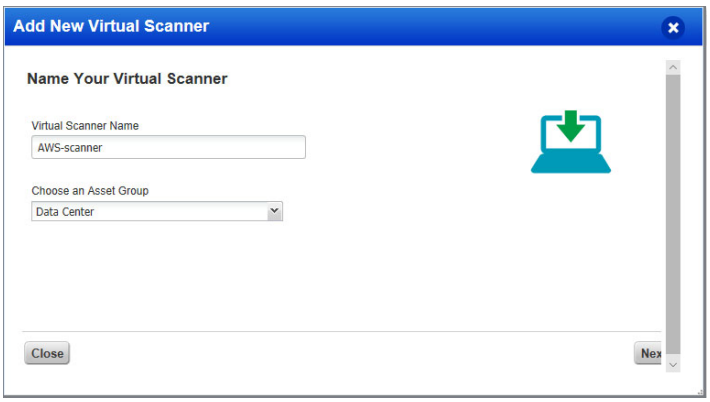
Choose “I have My Image” and click Continue.



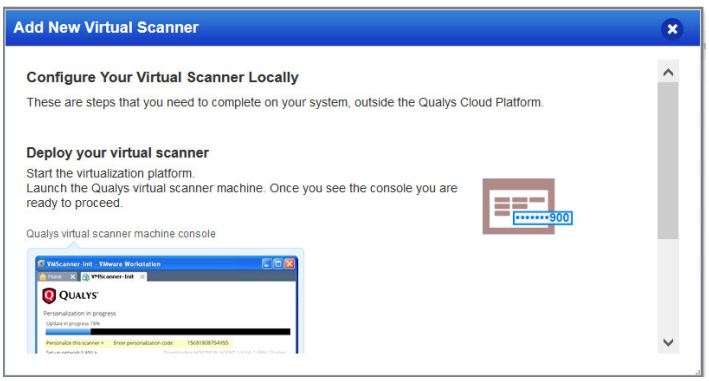
Provide a name and click Next.



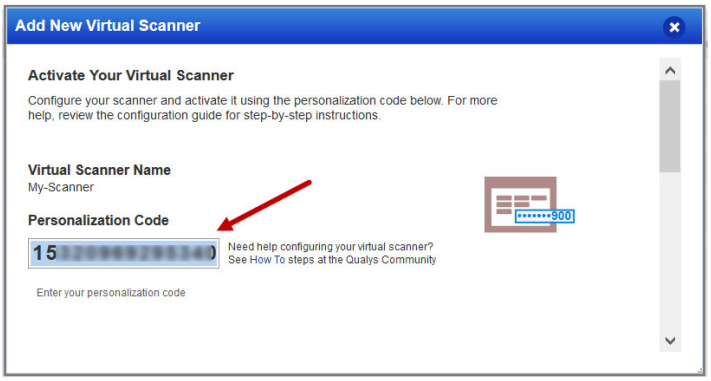
If you're a sub-user then you'll need to pick an asset group that has been assigned to your business unit by a Manager user. Not seeing any asset groups? Please ask a Manager to assign an asset group (other than the All group) to your business unit.



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



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



Configuration in AWS

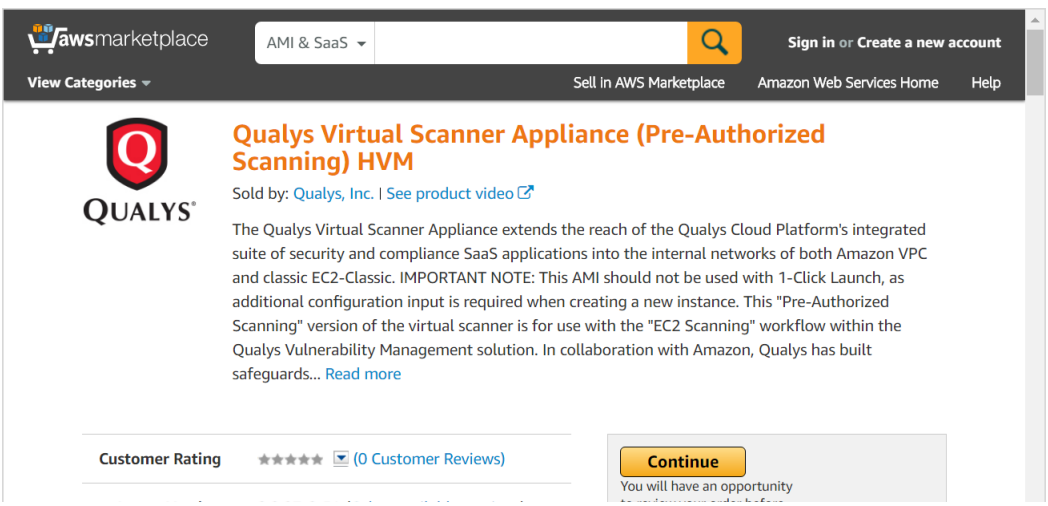
Launch an AMI instance in the Amazon AWS

These steps tell you how to launch an AMI instance from the Amazon AWS Marketplace. 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).

Note: Ensure that you only use the image available at AWS marketplace or the Signed URL provided by Qualys for downloadable AWS specific images. Using images downloaded from Qualys UI are not recommended to be used on AWS.

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

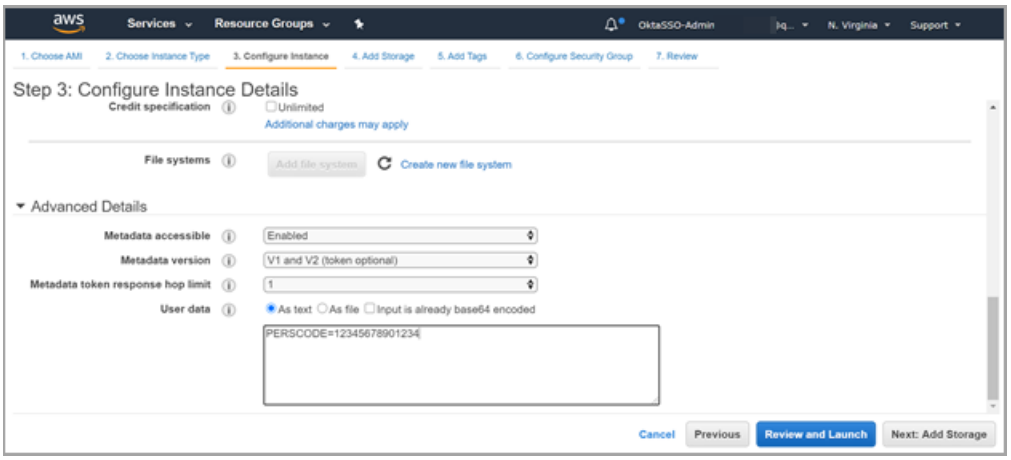
Qualys Virtual Scanner Appliance (Pre-Authorized Scanning) HVM on AWS Marketplace



The AWS marketplace lists two virtual scanner appliances - A Pre-Authorized scanner appliance and a Standard scanner appliance. The Standard appliance performs IP based scanning and Qualys recommends you to use the Pre-Authorized scanner appliance. If you cannot use the Pre-Authorized scanner appliance it is recommended to contact Qualys Support before choosing the Standard scanner appliance.

2) Launch the virtual scanner AMI in a region.

3) Use the wizard to enter AMI settings. In the Advance Details section, use "V1 and V2 (token optional)" as Metadata version. Currently, Qualys does not support V2 (token required). 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).



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.

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.

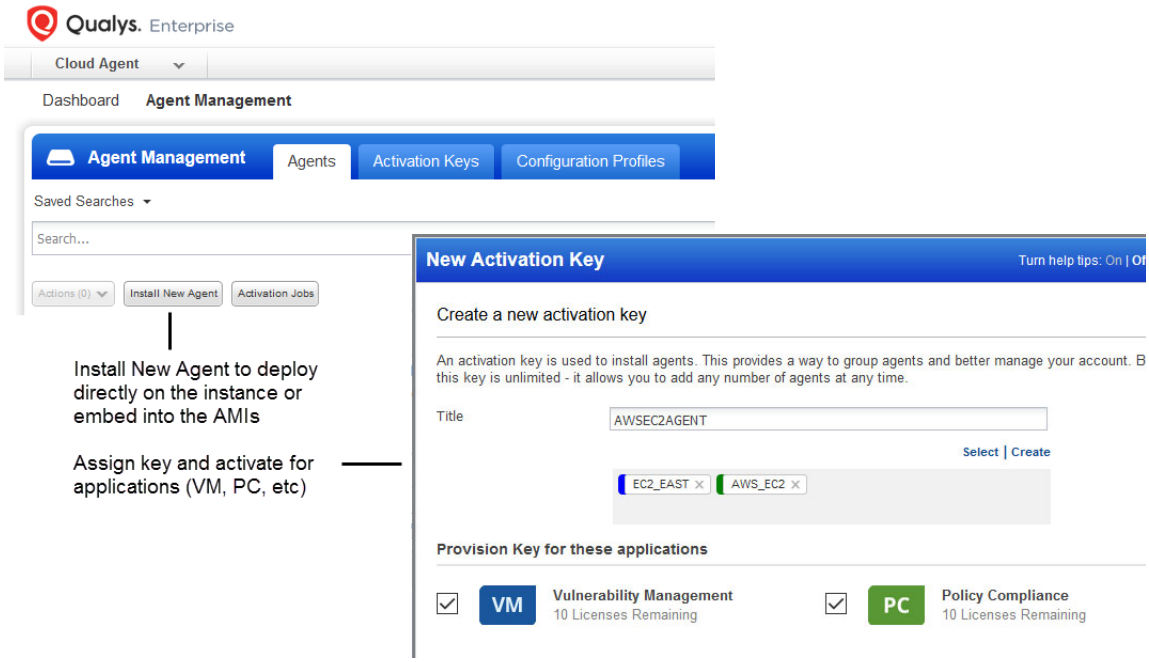
- Deployable directly on the EC2 instances or embed in the AMIs. Works well for cloud burst and ephemeral instances

- 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.



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.

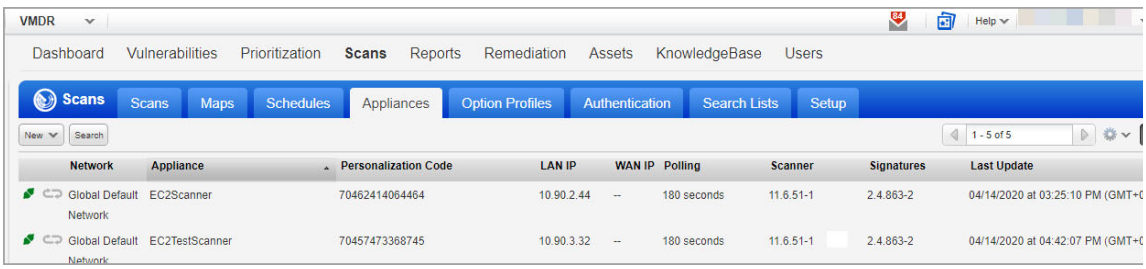
EC2 Scan checklist

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.



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 pre-authorized scanner deployment. Your EC2 scan won't work if you do not perform this step.

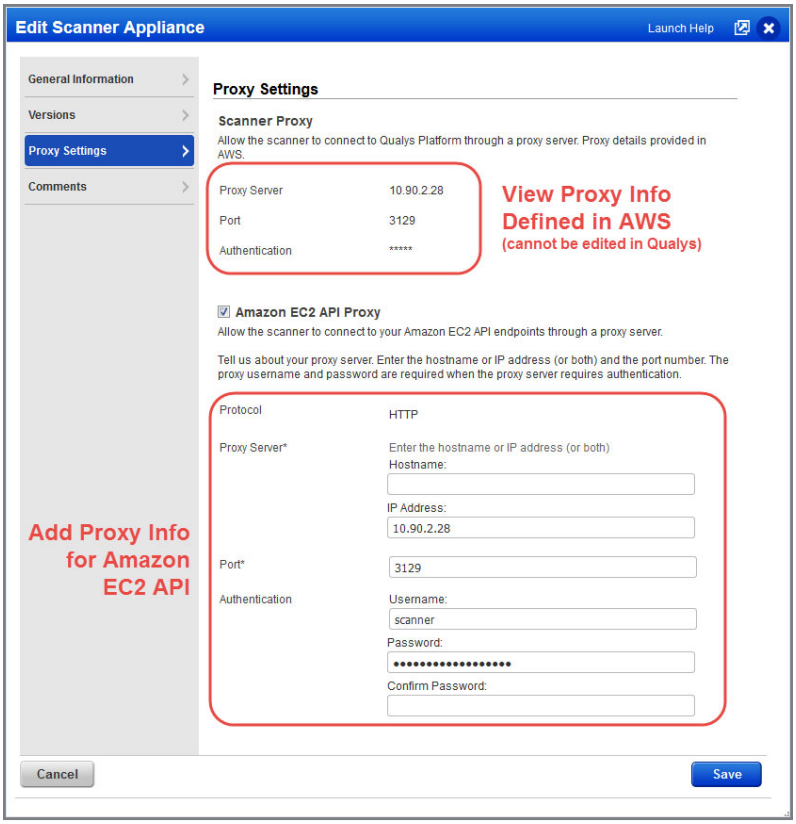
Go to Scans > Appliances - Edit your EC2 Virtual Scanner Appliance. Go to the Proxy Settings tab, select the Amazon EC2 API Proxy check box and tell us about your proxy server (i.e. hostname and/or IP address, port and proxy credentials (if required by the proxy server).

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.

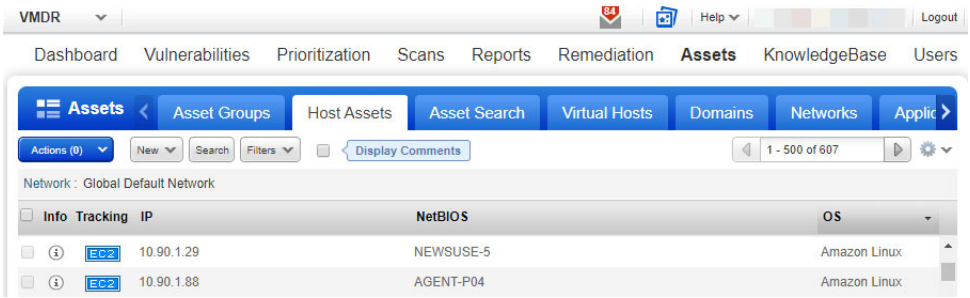


You must allow the EC2 Region endpoints to be accessible via the proxy.

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

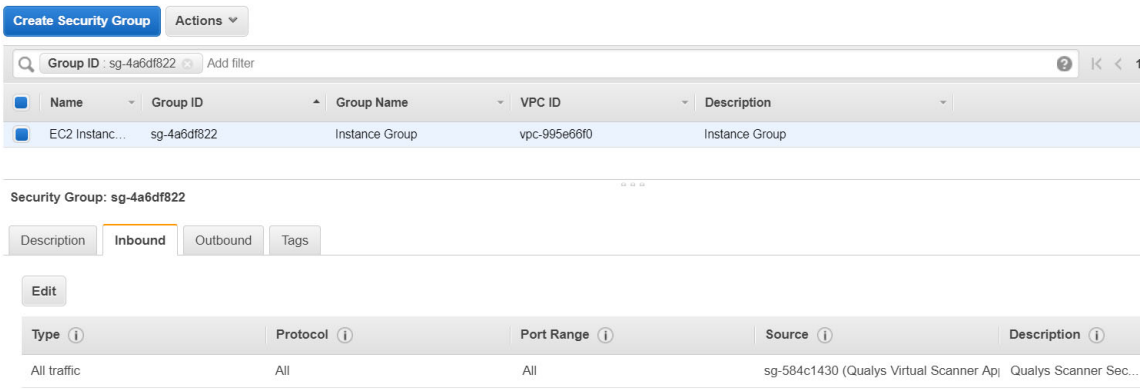
Go to Assets > Host Assets or Qualys AssetView (AV) - Check that your EC2 hosts are activated. Activated assets are assigned the EC2 tracking method.



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.

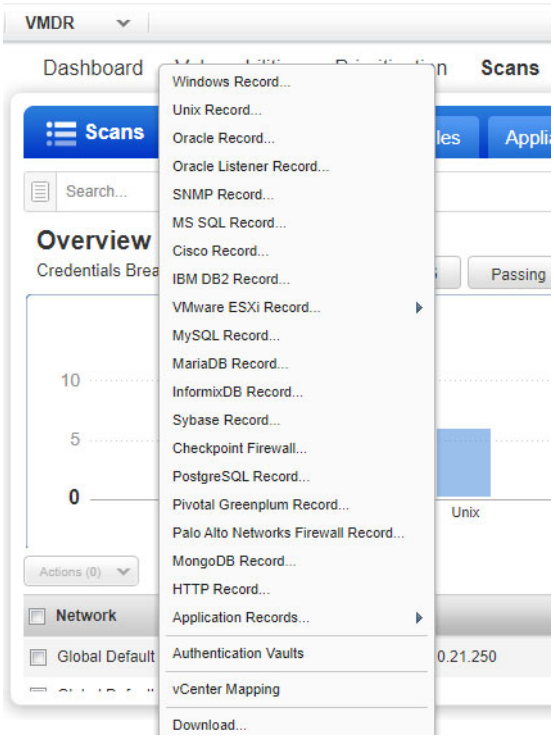


Configure OS Authentication

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.

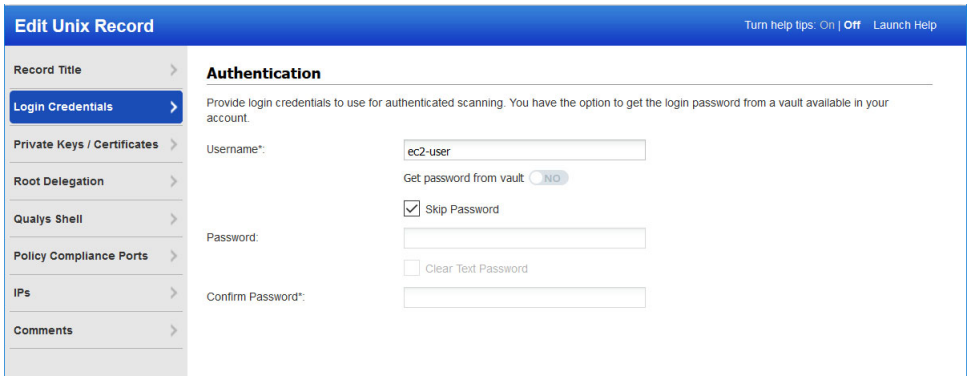
Go to Scans > Option Profiles. Edit the profile Initial Options, use Save As to save a copy with another name. In your new profile enable the authentication types you'll need.

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.

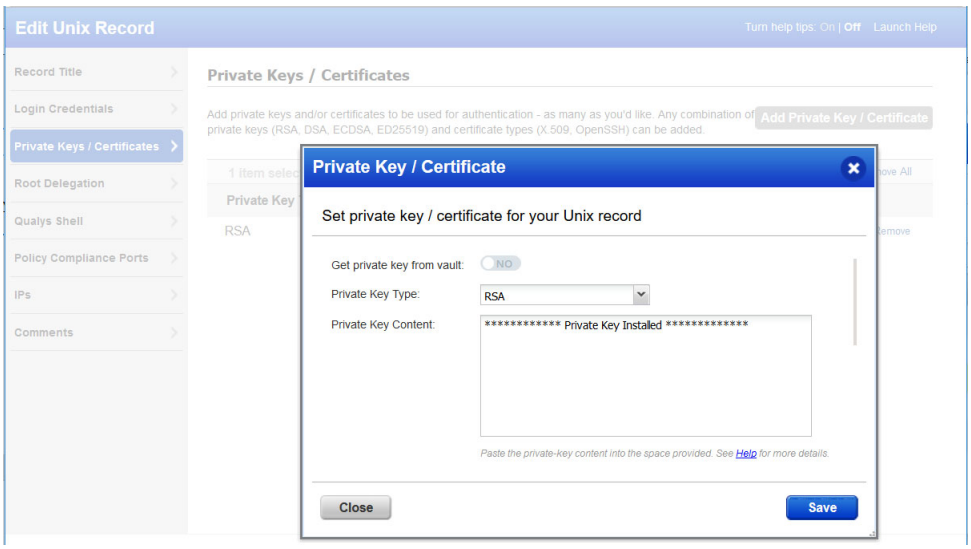


Sample Unix Record

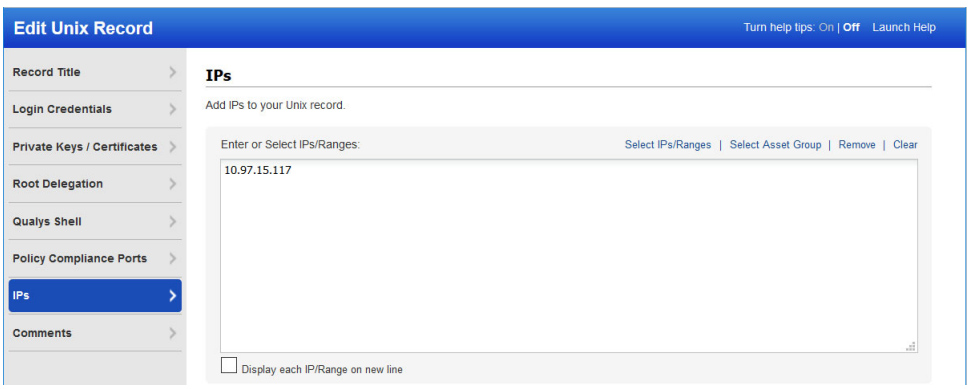
1) Login Credentials - Provide OS user name and select Skip Password



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

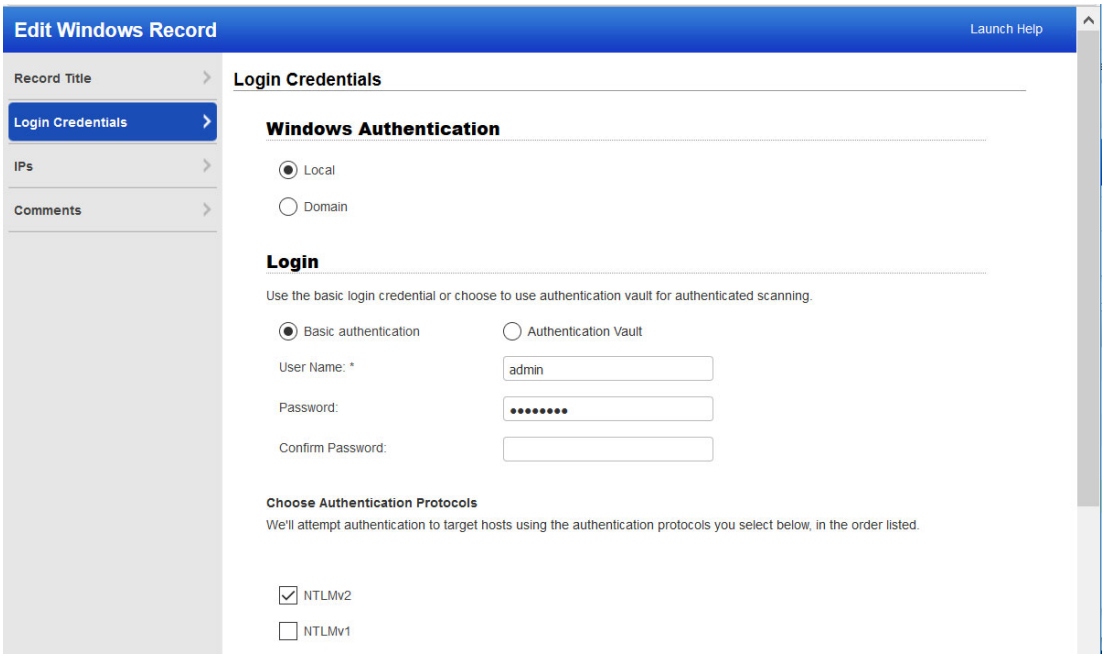


3) IPs - Select Unix IP addresses/ranges of your EC2 instances for this record. Credentials in this record will be used to scan these assets.

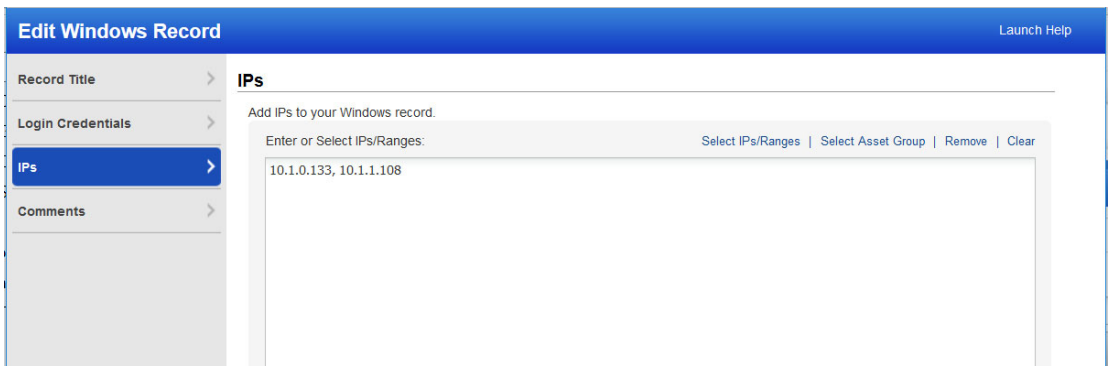


Sample Windows Record

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



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.



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.

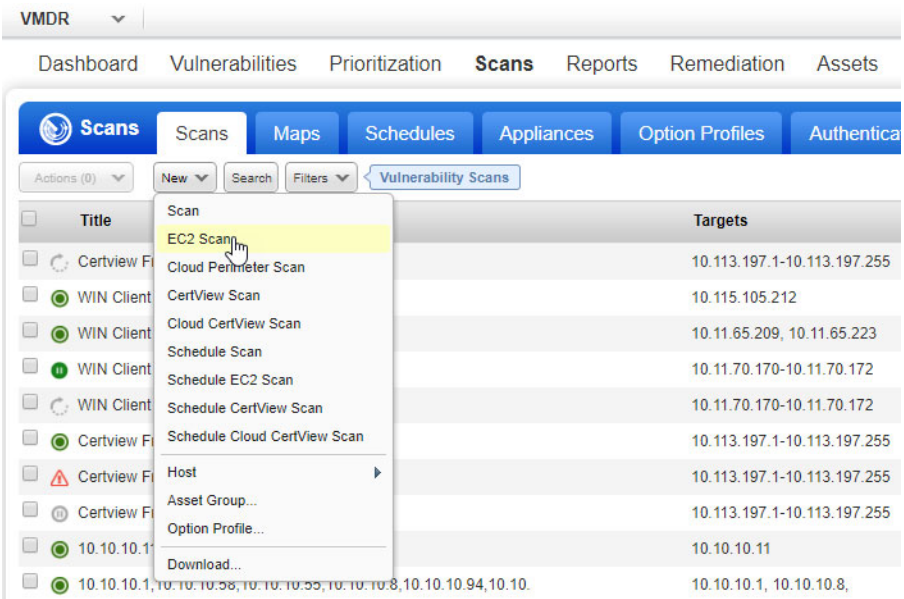
Scan Using Pre-authorized Virtual Scanner Appliance

Scanning with pre-authorized 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 Pre-Authorized 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



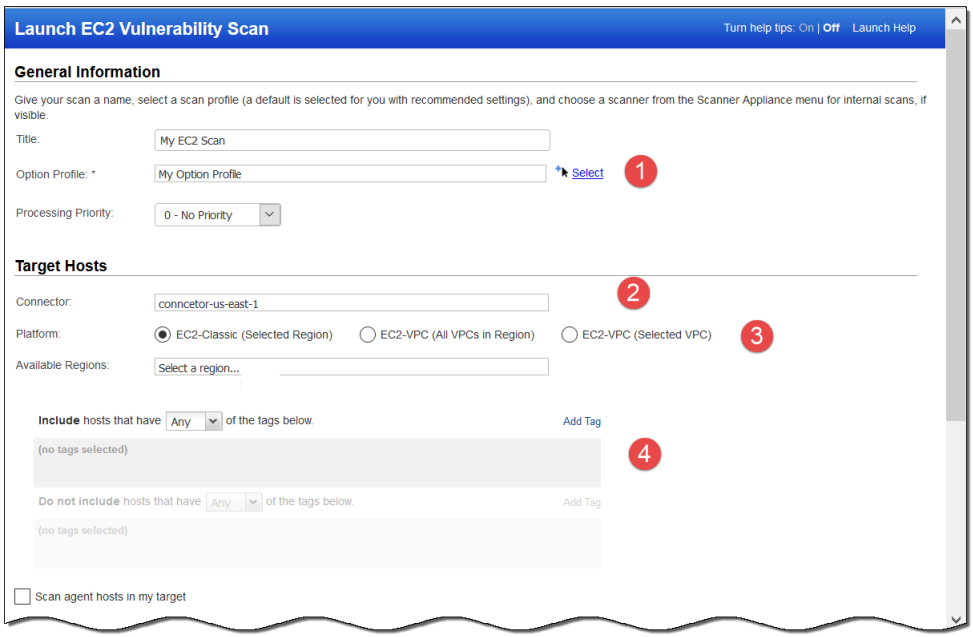
Provide scan settings:

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

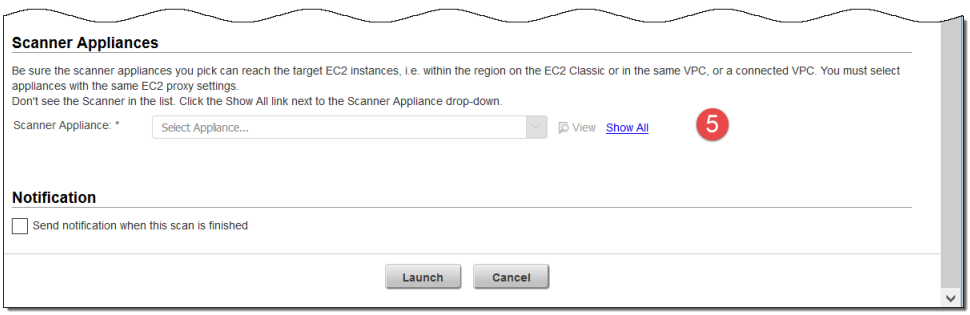
2) Select the EC2 connector name you configured.

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.

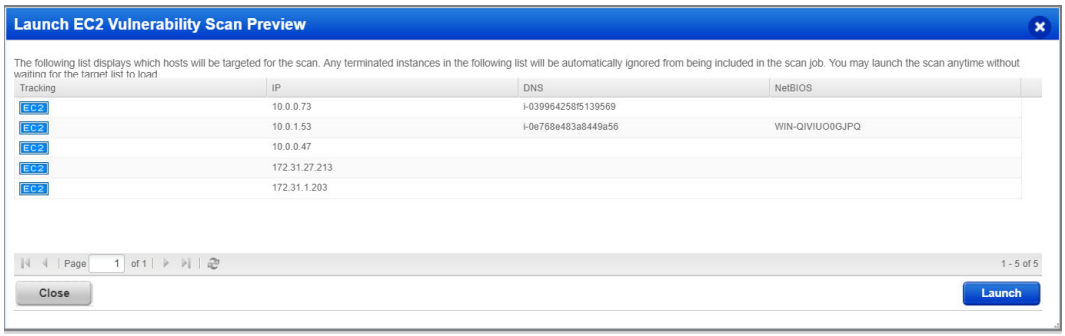


5) Choose the Virtual Scanner Appliance AMI you've launched in Amazon EC2.



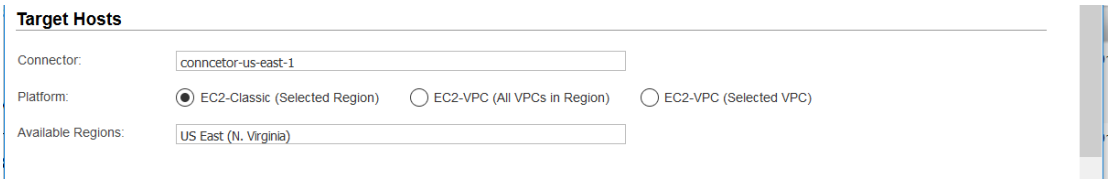
Click Launch and start scanning and securing your Amazon EC2 infrastructure.

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.



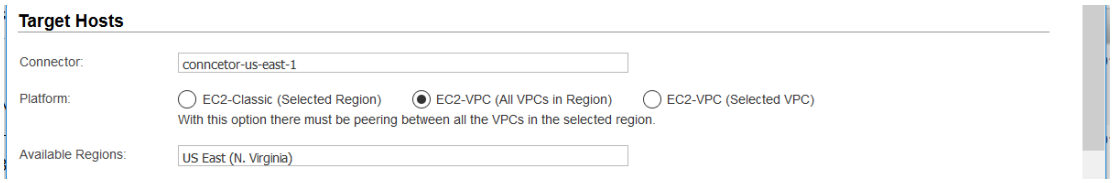
Scanning EC2 Classic instances

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.



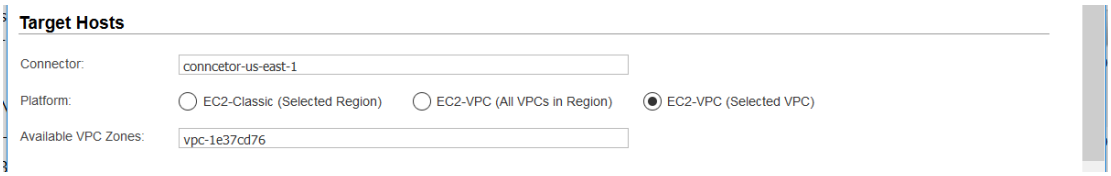
Scanning VPC instances

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



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.



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 Scanner Appliance Pre-Authorized 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 Pre-authorized 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.

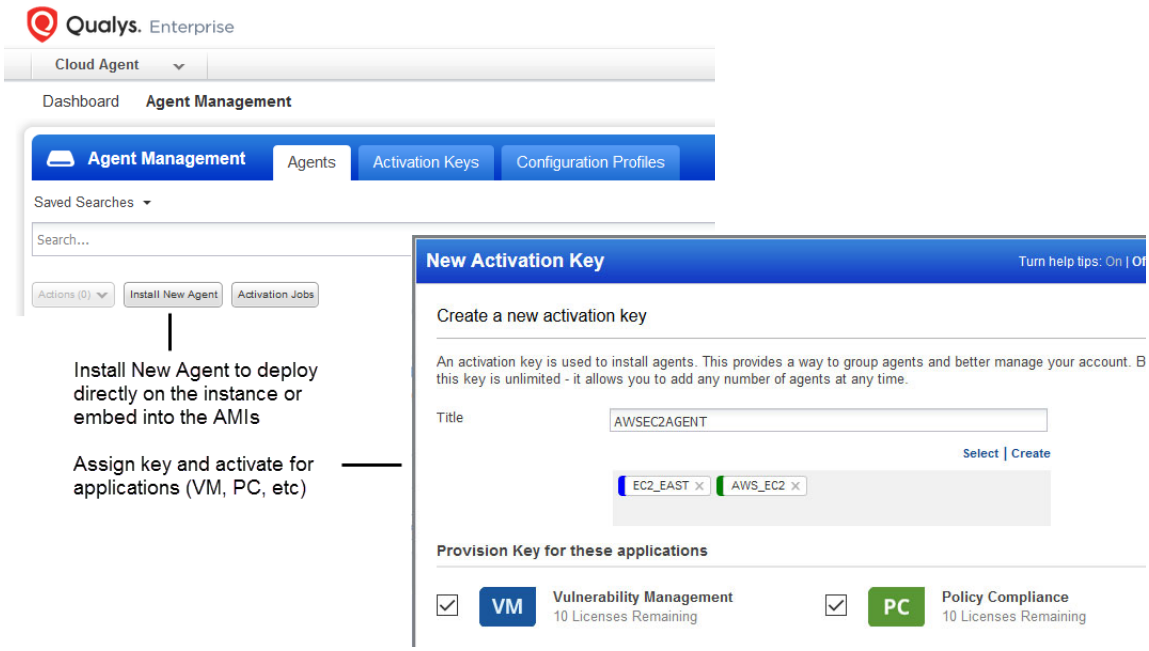
- Deployable directly on the EC2 instances or embed in the AMIs. Works well for cloud burst and ephemeral instances

- 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



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).

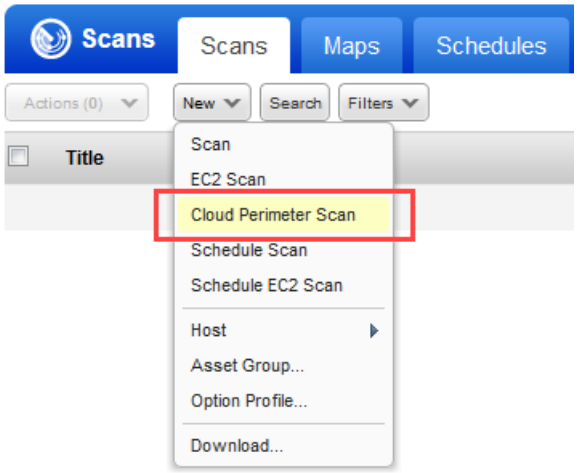
EC2 connector is required. Configure this same EC2 connector in your CloudView account if you wish to “include public load balancers from the connector” in the scan. To create the connector, your account must have CloudView subscription and your platform has access to CloudView base URL “qweb_cloud_view_base_url”.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

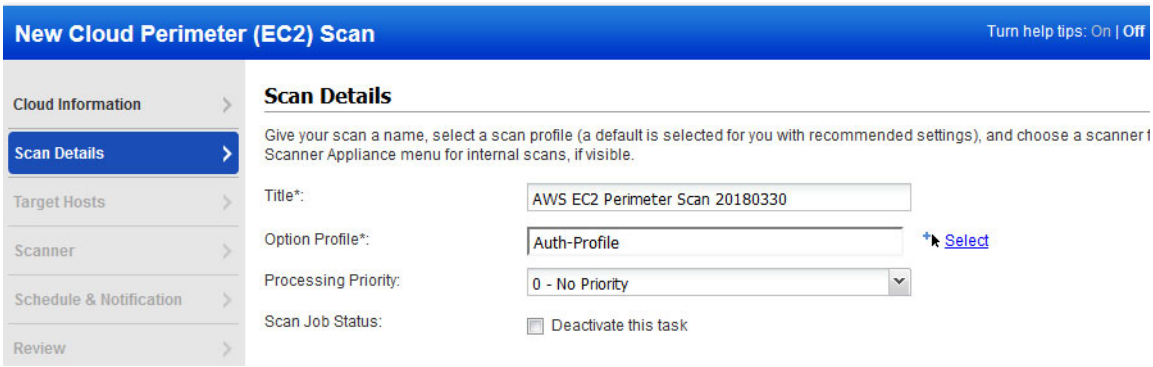
All cloud perimeter scans are scheduled - either for “now” (a one-time scan job) or “recurring”. Once saved, you’ll see the scan job on the Schedules list. When the scan job starts it will appear on your Scans list.

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.

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



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.

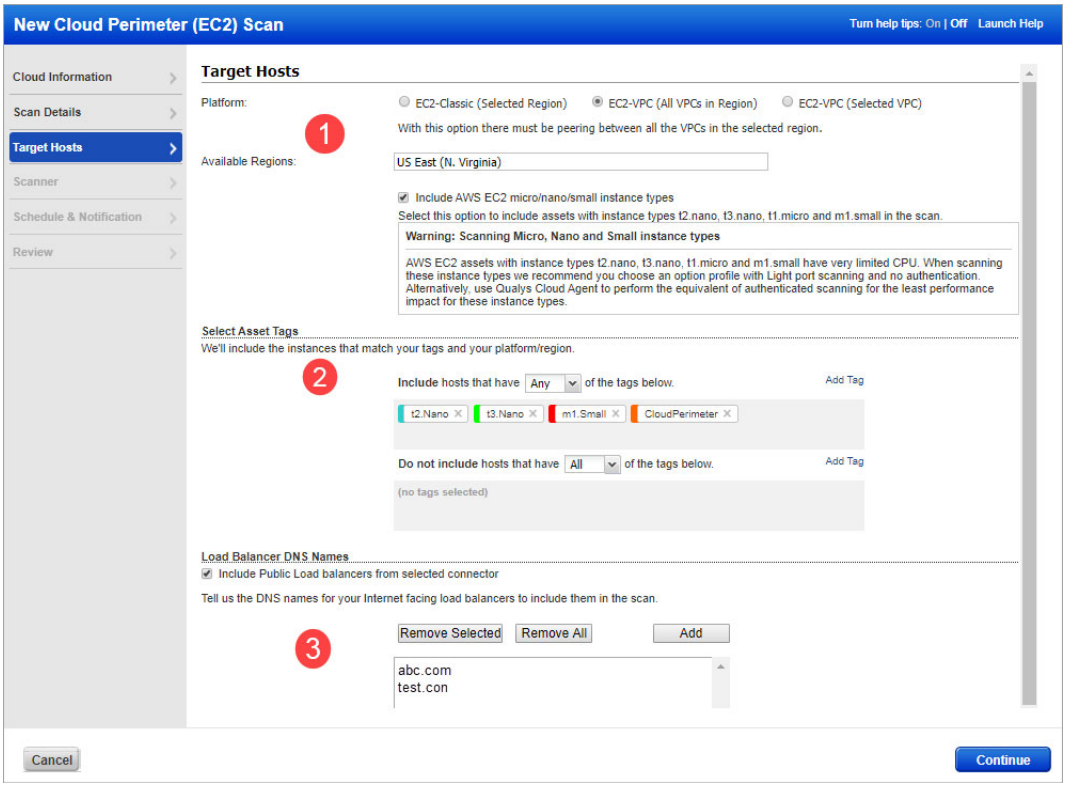
2) (Optional) Select asset tags - these are assets activated for your connector.

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 CloudView 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 CloudView account with a configuration similar to that of the selected connector. If the connector in CloudView is not found, then selecting this option won't fetch any public load balancers. See "Configure Your AWS Connector" in CloudView 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.

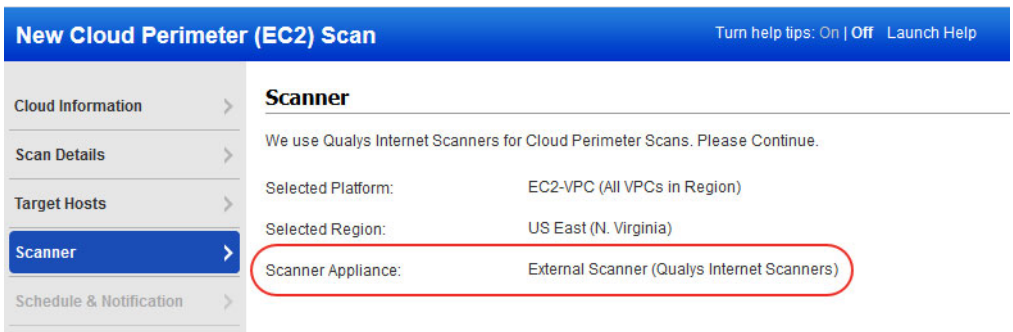


DNS-based scans

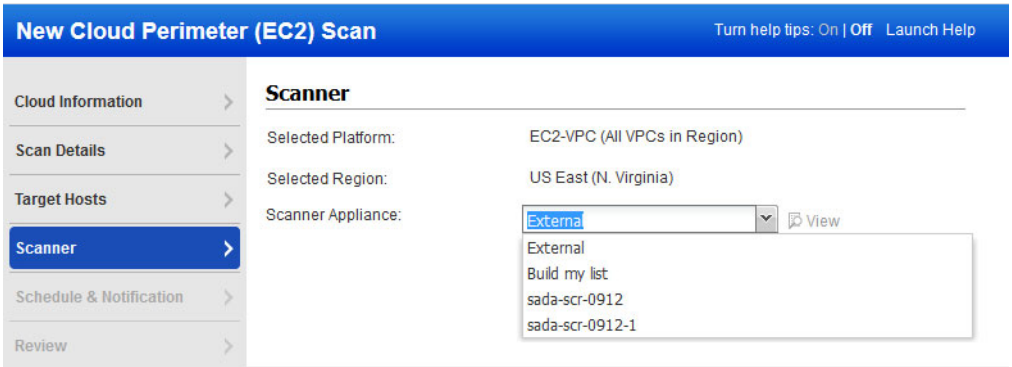
This feature needs to be turned ON for your subscription. Please contact Qualys Support if you would like to enable this feature.

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.



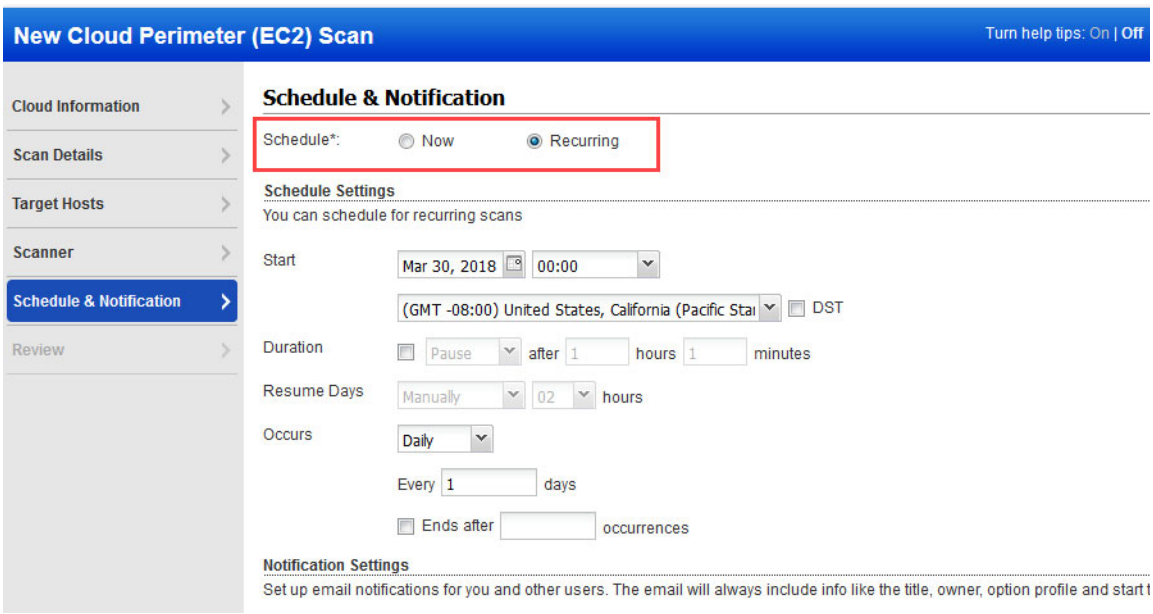
For Private Cloud Platforms - Your subscription may be configured to allow scanner appliances to be used for cloud perimeter scan jobs. In this case, choose one or more scanner appliances from the list (use the Build my list option).



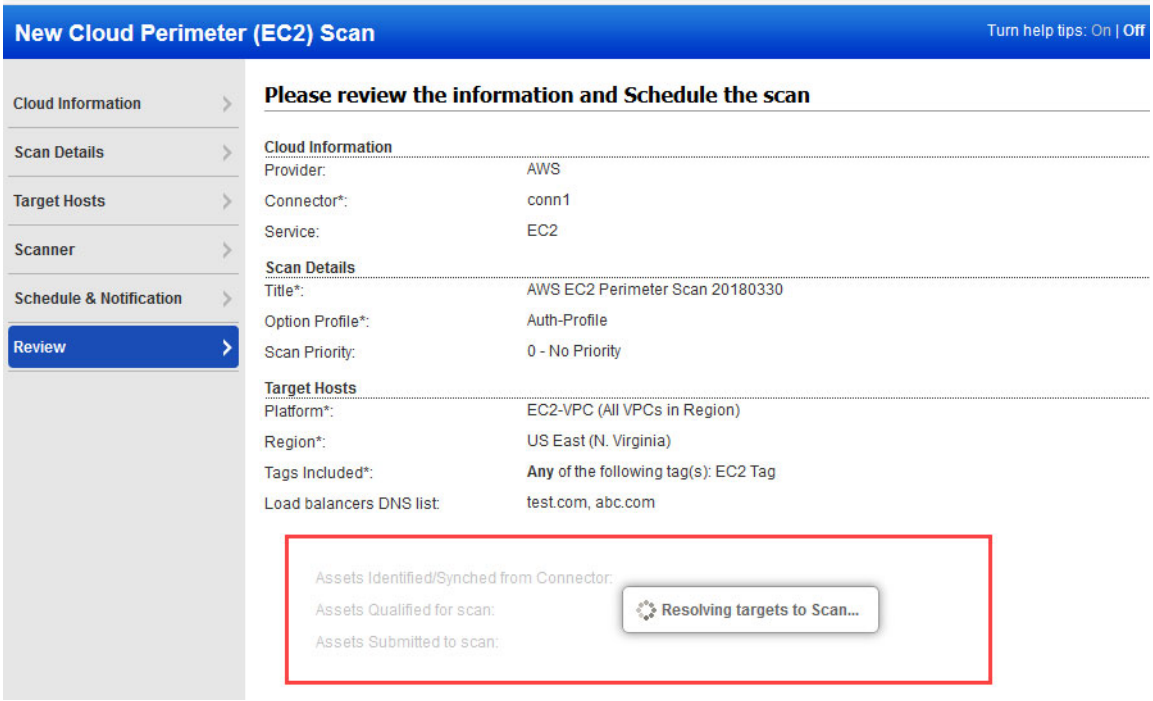
Tell us when you want the scan to run - Now or Recurring.

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.



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



You'll see these asset counts:

Assets Identified / Synced - The number of assets discovered by the connector that you selected for this scan job.

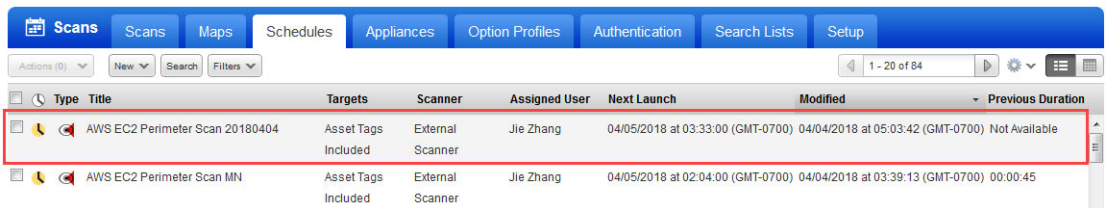
Assets Qualified for scan - The number of assets discovered by the connector that also match the selected platform, region, asset tags. We'll remove the Terminated instances.

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.

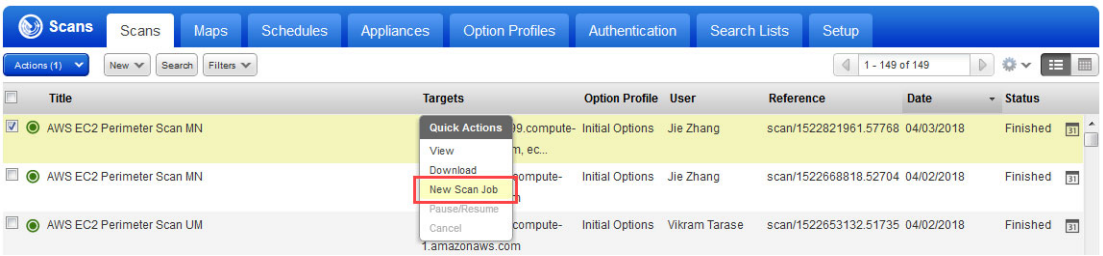
What Happens Next

Your new scan job will appear on the Schedules list.



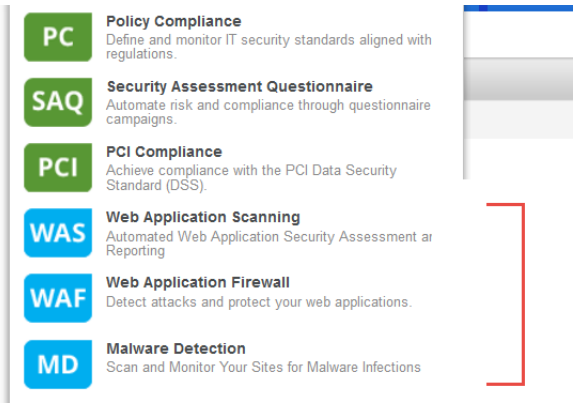
When your scan starts it will appear on the Scans list. Like with other scans you can take actions like cancel or pause the scan, view the scan status and download the results.

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".



Securing Web Applications

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



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 that's pre-authorized by AWS. 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.

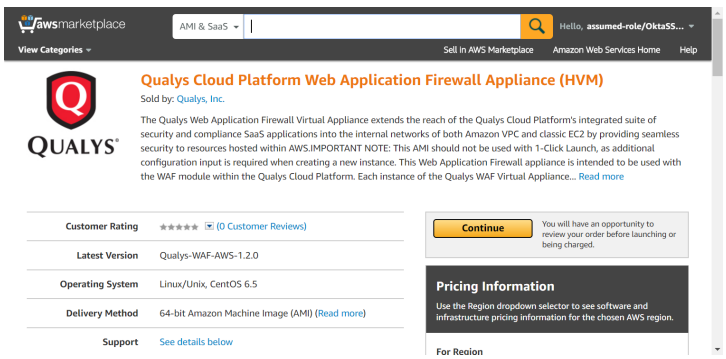
Qualys WAF

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

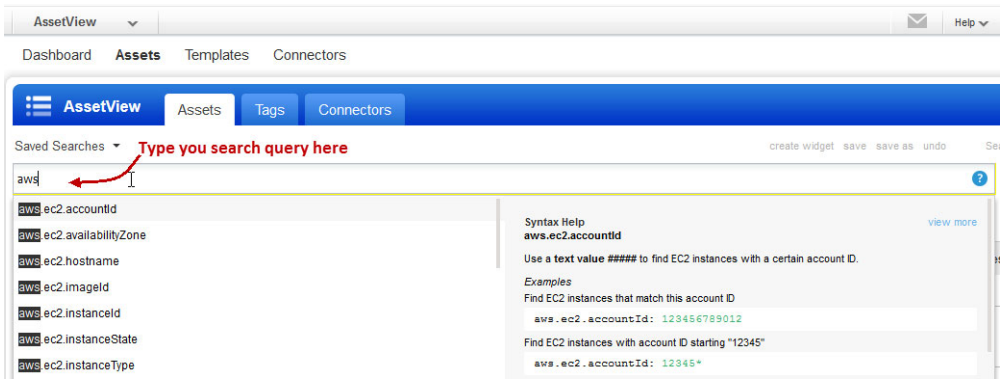


Analyze, Report & Remediate

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.

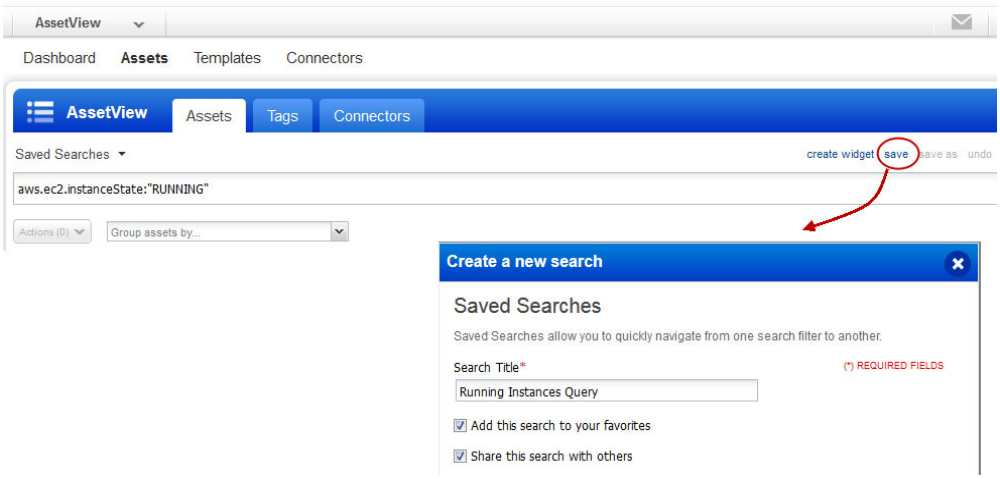
How to Query EC2 Assets

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.



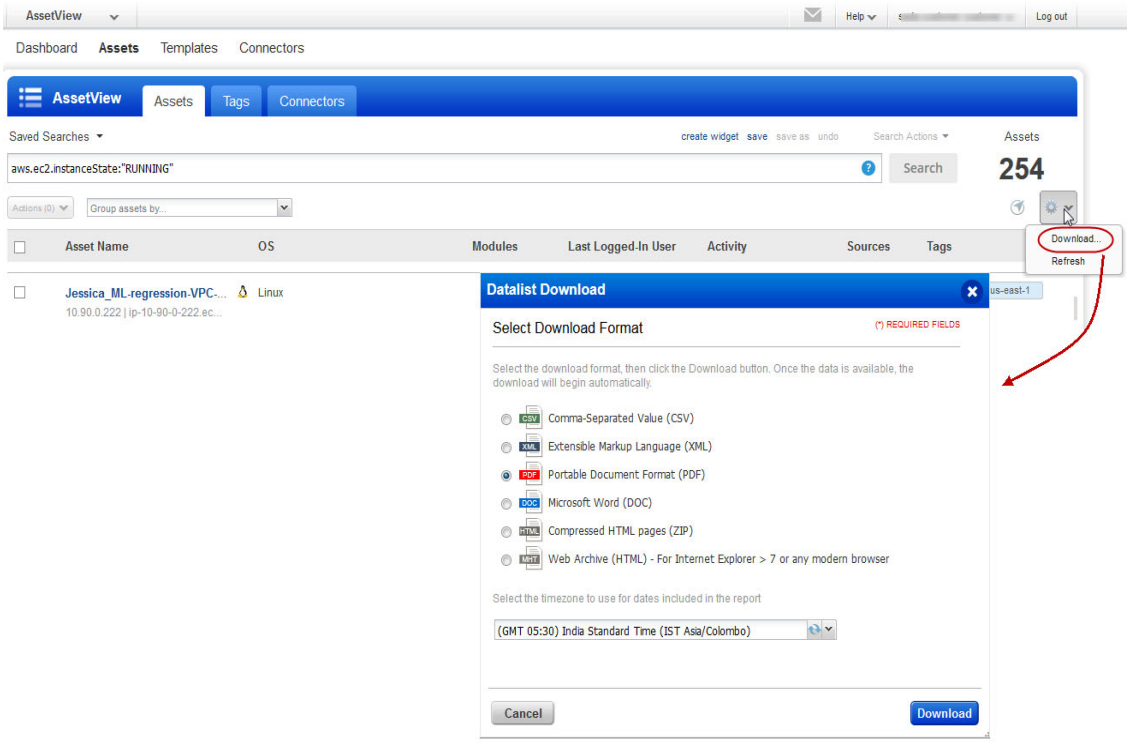
Save Query

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



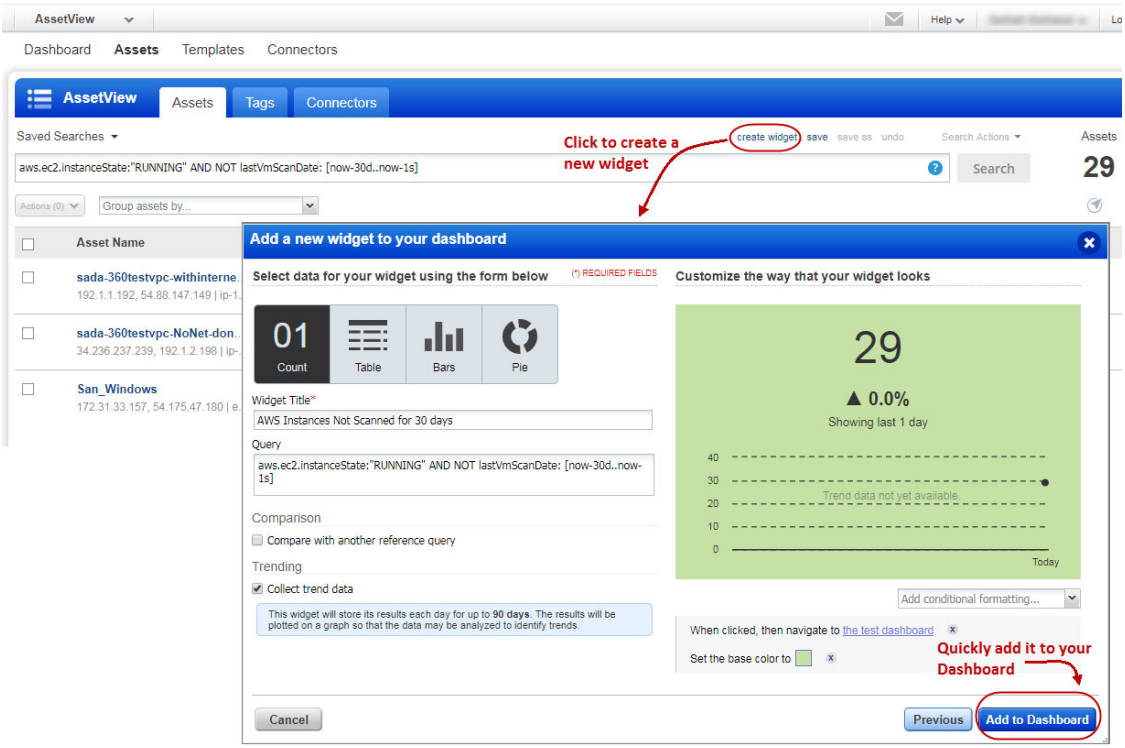
Download and export results

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).



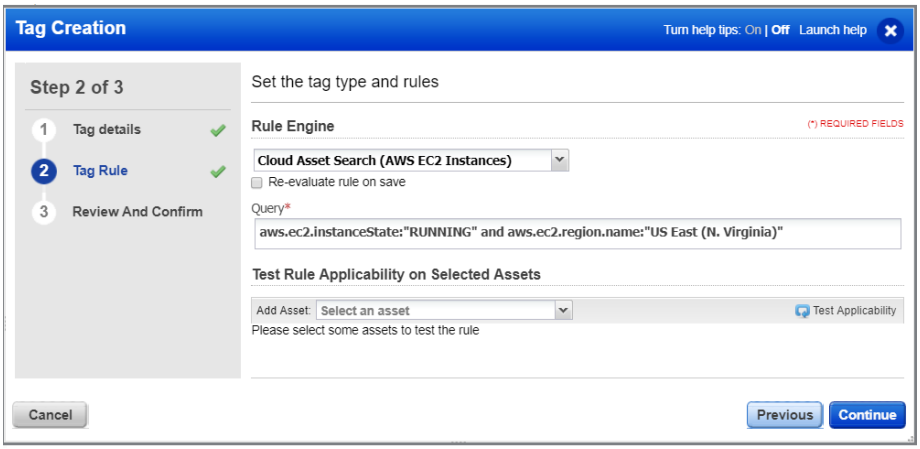
Create widget

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.



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.



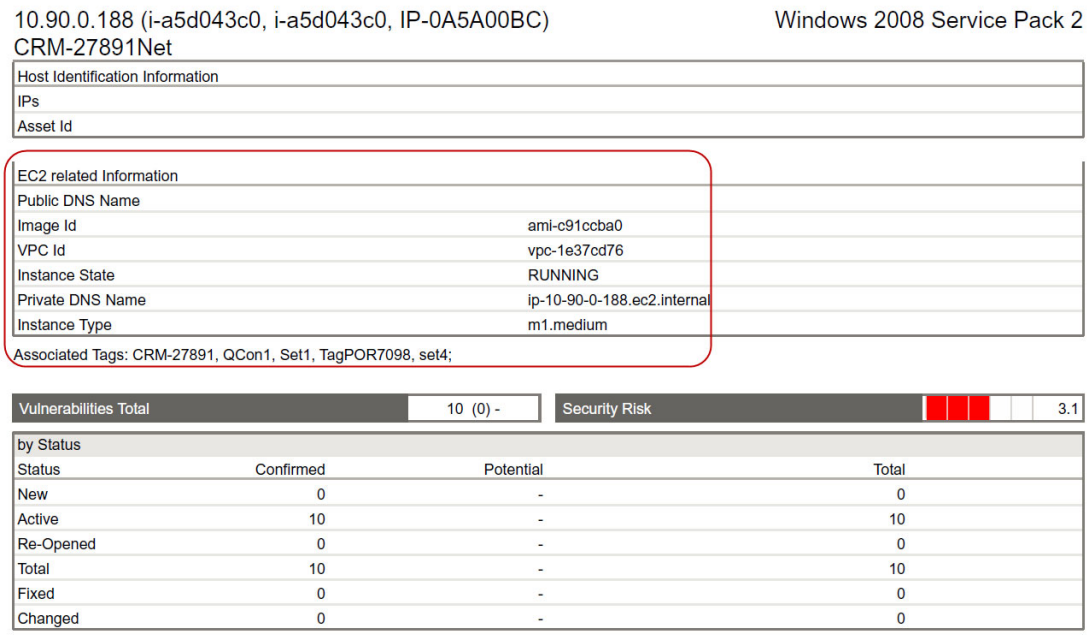
Generate Reports

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

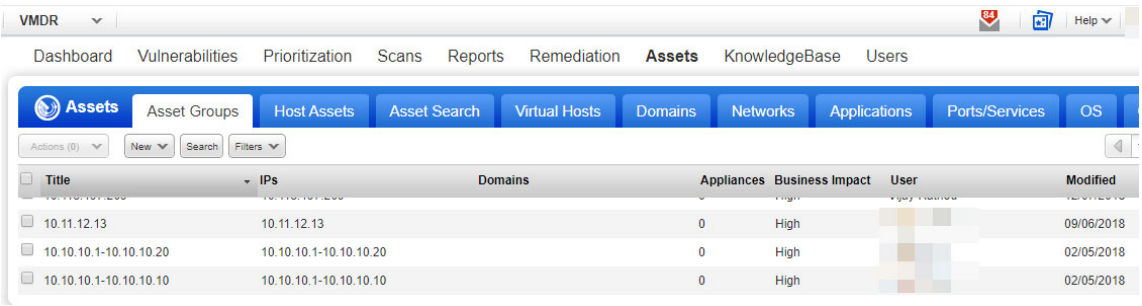
Status	Confirmed	Potential	Total
New	0	-	0
Active	10	-	10
Re-Opened	0	-	0
Total	10	-	10
Fixed	0	-	0
Changed	0	-	0

Manage Assets using Qualys

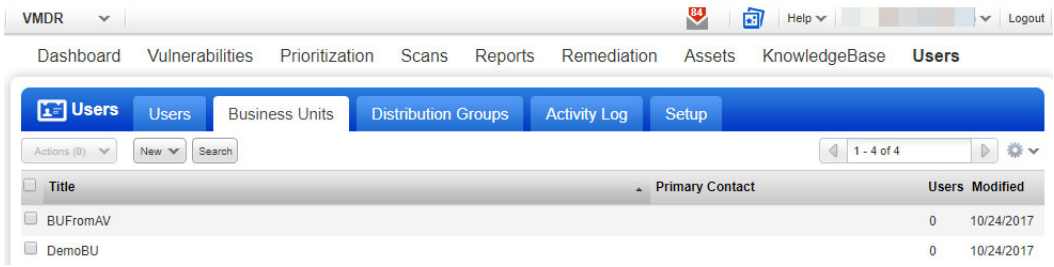
Here's some best practices and tips for organizing assets to help you secure AWS EC2 infrastructure using Qualys.

Setting up Qualys configurations

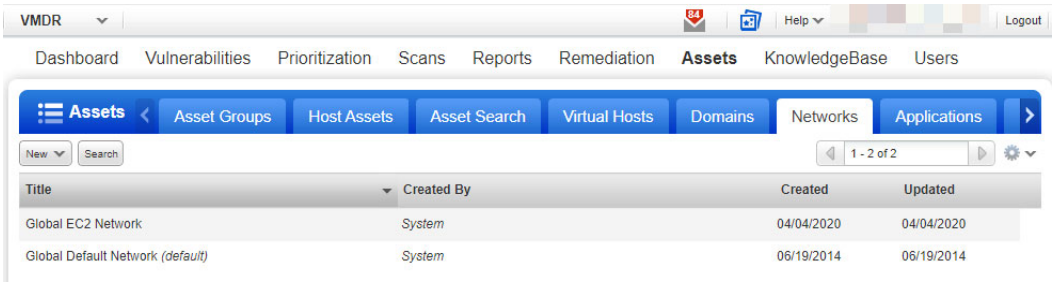
Asset Groups - Organize assets into meaningful groups and assign them to sub-users. Asset groups are required when you have multiple users i.e. Scanner, Reader, Unit Manager (if business units are defined). The same IP address can be included in multiple asset groups.



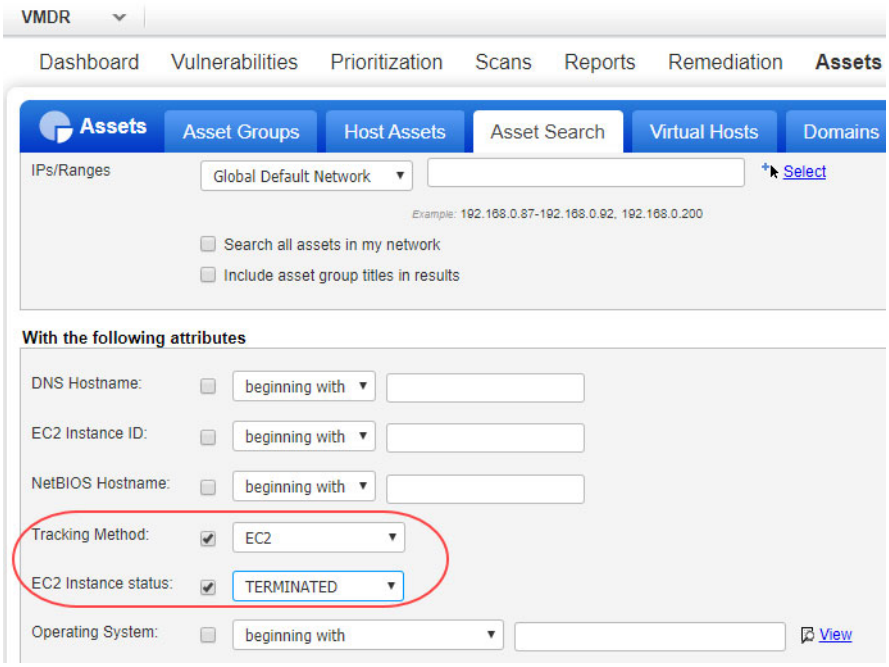
Business Units - Organize users and assets into business units in a way that matches your organization. This gives Managers the ability to grant users role-based permissions in the context of their assigned business unit. The same IP address can be included in multiple business units.



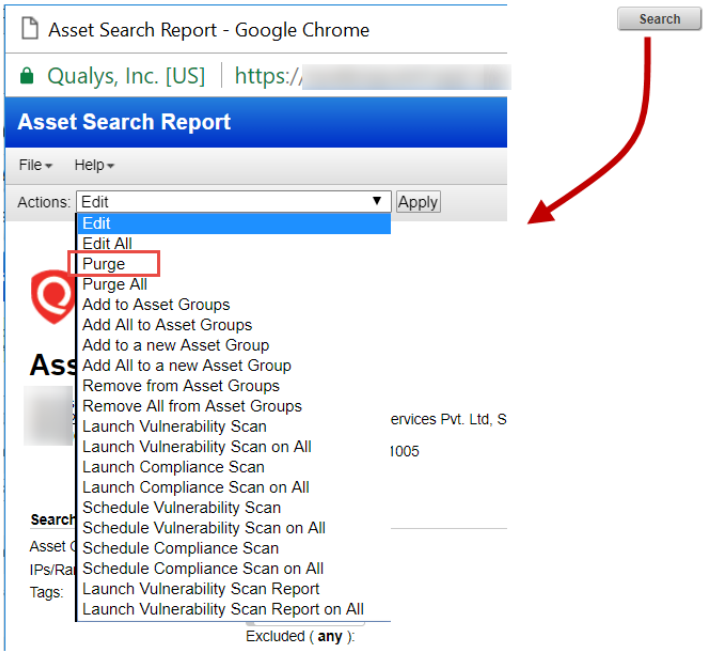
Networks - Organize discrete private IP networks to keep overlapping IP blocks separate. When configured Qualys tracks IPs by network and IP address. Keep in mind... An IP address must be unique to your subscription or a single network.



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.



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



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.

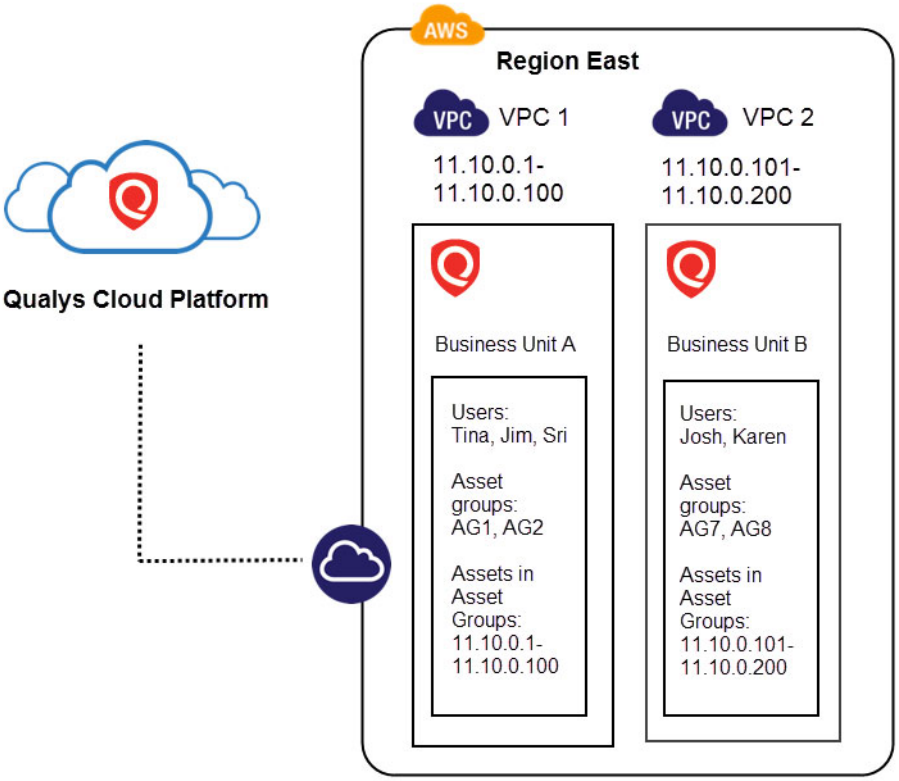
Use Cases for scanning your AWS environment

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.



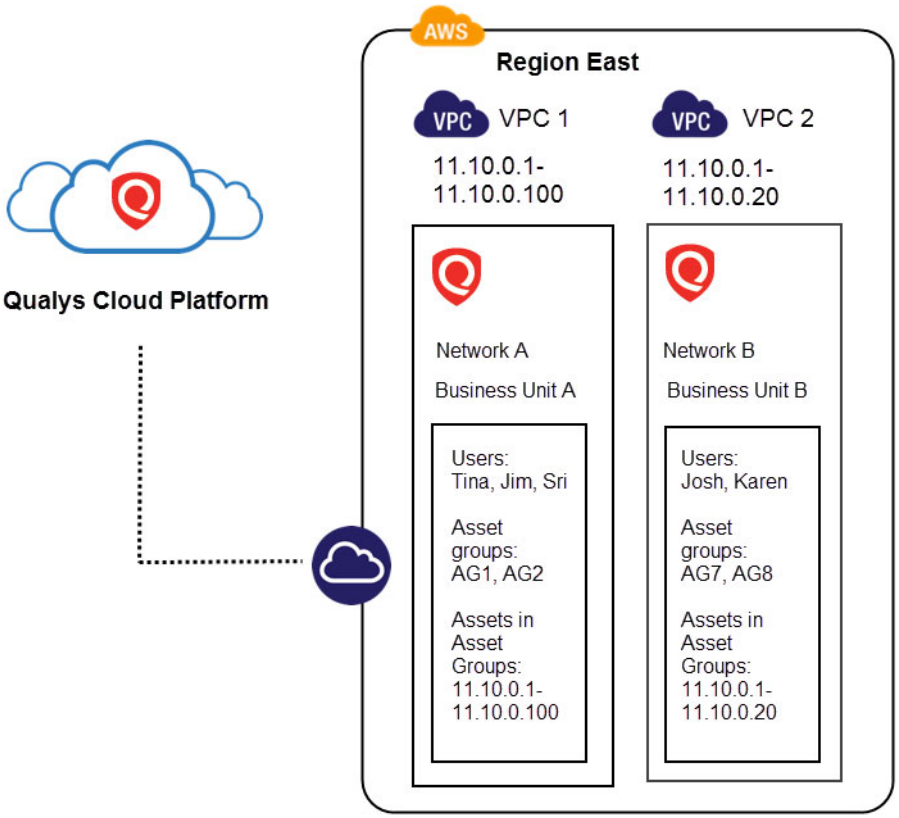
Use Case 2 - Scanning multiple VPCs with Overlapping IPs

- 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

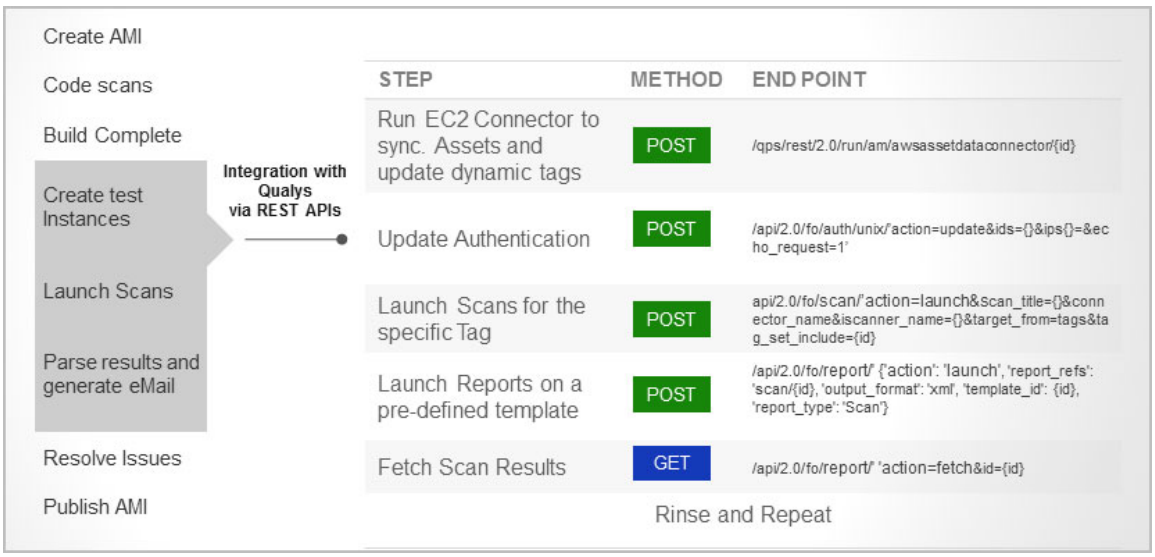
Automate VM scanning of host and EC2 cloud instance from Jenkins

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.

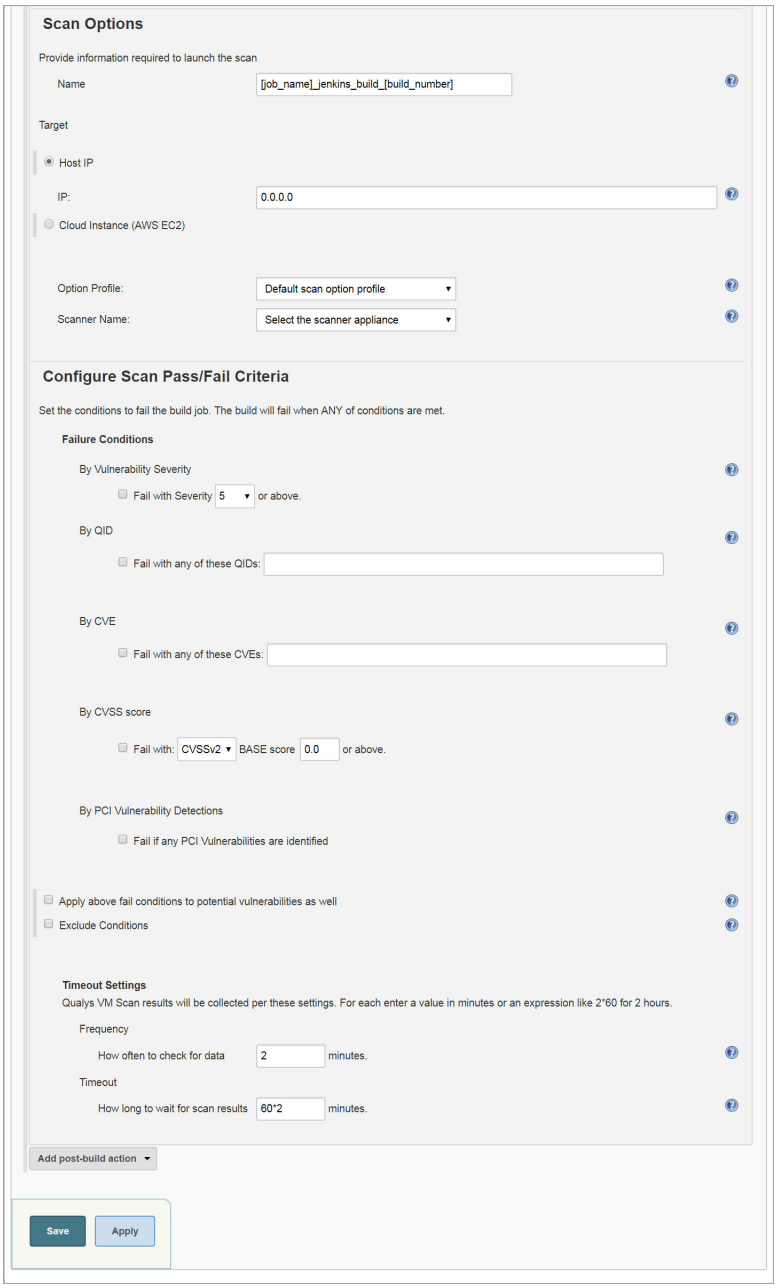
For example here are the typical steps involved in AMI creation and how Qualys APIs can be used for hardening the AMI.



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

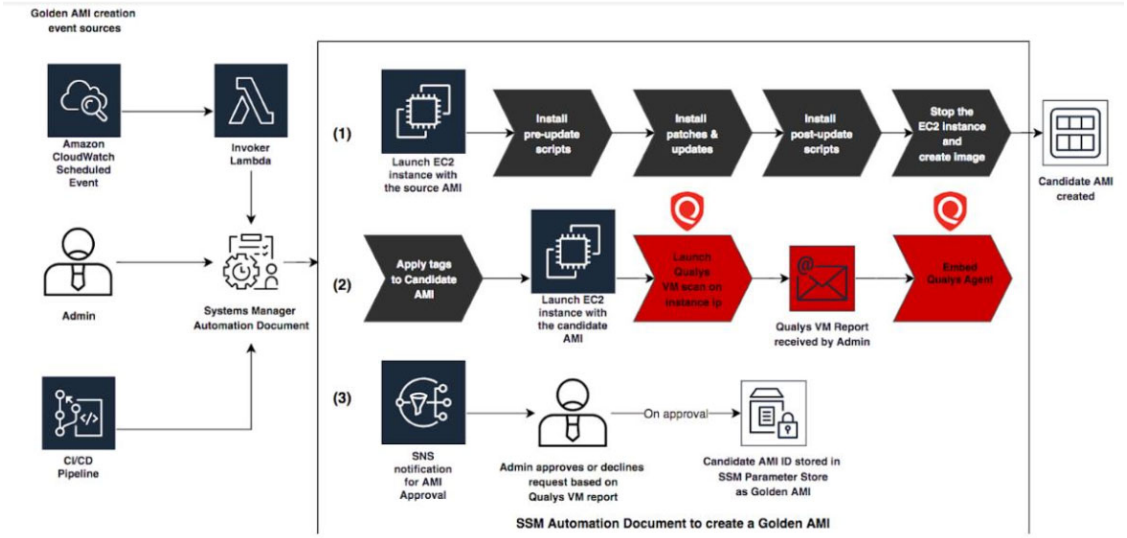
Automate VM scanning of host and EC2 cloud instance from Jenkins

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.



Golden AMIs Pipeline

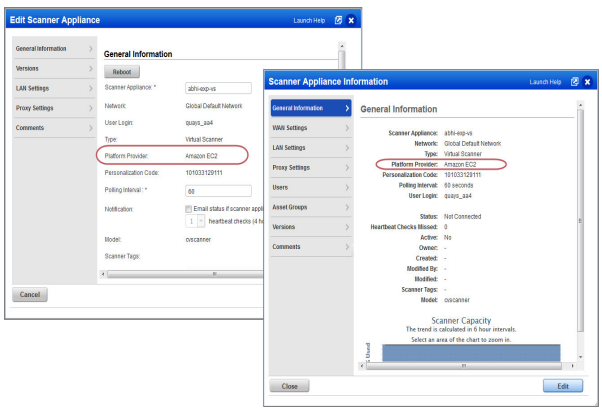
When developing golden Amazon Machine Images (AMIs), DevOps teams should run continuous and automated checks to eliminate vulnerabilities and misconfigurations in them. Qualys collaborated with Amazon to integrate the AWS Golden Amazon Machine Image Pipeline reference architecture with Qualys scanners 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.



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). 

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.