Securing Amazon Web Services with Qualys

January 20, 2018
Table of Contents

**About this guide** .......................................................................................................................... 3
  About Qualys ................................................................................................................................. 3
  Qualys Support .............................................................................................................................. 3

**Introduction** .............................................................................................................................. 4
  Qualys Integrated Security Platform .......................................................................................... 4
  Pre-requisites ............................................................................................................................... 6

**Automate Asset Inventory** ........................................................................................................ 8
  Setting up EC2 Connector ............................................................................................................. 8
    Enabling GovCloud .................................................................................................................... 10
    Selecting EC2 regions ................................................................................................................ 10
    Activating Assets ...................................................................................................................... 11
    Assigning Tags .......................................................................................................................... 12
  How does EC2 Connector work? .................................................................................................... 13
  Viewing Imported Assets ............................................................................................................. 13
  AWS APIs used by EC2 Connector to discover assets ................................................................ 14
  Qualys APIs for EC2 Connectors ............................................................................................... 15

**Deploy Sensors** ........................................................................................................................ 16
  Deploying Pre-authorized Virtual Scanner Appliance ................................................................. 16
    Cost and Licenses ....................................................................................................................... 16
    Deployment recommendations for scanner ............................................................................. 17
    About managing instances ....................................................................................................... 18
    Scanner Deployment ................................................................................................................ 18
    Support for Qualys Private Cloud Platform ........................................................................... 22
  Deploying Qualys Cloud Agent .................................................................................................... 23

**Scan Assets** .............................................................................................................................. 25
  EC2 Scan checklist ....................................................................................................................... 25
  Scan Using Pre-authorized Virtual Scanner Appliance ............................................................... 31
    EC2 Scan workflow ................................................................................................................... 31
    Scanning EC2 Classic instances ............................................................................................... 33
    Scanning VPC instances ........................................................................................................... 33
    Scanning instances using VPC Peering .................................................................................... 33
    Scanning EC2 Instances in GovCloud ....................................................................................... 34
  Internal Network Scanning using Qualys Cloud Agent .............................................................. 35
  Perimeter Scanning using Qualys External Scanners ................................................................. 36
  Securing Web Applications ......................................................................................................... 39

**Analyze, Report & Remediate** ................................................................................................. 40
  How to Query EC2 Assets .......................................................................................................... 40
  Dynamic Tagging Using EC2 Attributes ..................................................................................... 43
Securing AWS with Qualys

Contents

Generate Reports ................................................................................................................................................................. 43

Manage Assets using Qualys ................................................................................................................................................. 46

Setting up Qualys configurations ................................................................................................................................. 46

Use Cases for scanning your AWS environment .......................................................................................................... 49

  Use Case 1 - Scanning multiple VPCs with No Overlapping IPs ............................................................................. 49

  Use Case 2 - Scanning multiple VPCs with Overlapping IPs ..................................................................................... 50

  Use Case 3 - Automate scanning into DevOps process to harden the AMI ......................................................... 51

Common Questions ............................................................................................................................................................... 53
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 with over 9,300 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. The Qualys Cloud Platform and integrated suite of solutions help organizations 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, Fujitsu, HCL Comnet, HPE, 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 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 without penetration form sign ups

--- Supports all AWS global regions including GovCloud

--- Supports EC2 instances in Classic and VPC platform

--- Qualys Cloud Agents certified to work in EC2
Securing AWS with Qualys

Introduction

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
Applications: VM, PC, SCA, WAS

Cloud Agents
Continuous security view and platform for additional security solutions
Applications: CA (required), VM, PC

AWS Cloud Connectors
Sync cloud instances and its metadata
Applications: VM, PC

Internet Scanners
Perimeter scan for edge facing IPs and URLs
Applications: VM, PC, WAS

Web Application Firewalls
Actively defend intrusions and secure applications
Applications: WAF

Pre-requisites

These options must be enabled for your Qualys user account.

- Qualys Applications: Vulnerability Management (VM), 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, it’s features and user interface. If you are new to Qualys we recommend these overview tutorials - it just takes a few minutes!

Video Tutorials get you familiar with basics

Vulnerability Management Overview (8 mins)
Policy Compliance Overview (14 mins)
Quick Steps: Securing AWS

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

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

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

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

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

Helpful resources Always up to date with the information you need

From the Community

Qualys Training | Free self paced classes, video series, online classes
Qualys Documentation | Getting started guides, quick references, API docs
Qualys AWS EC2 Video Series | Video series on 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 will see the IP address, tags, private DNS name and 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.

Go to Qualys AssetView (AV) - Just select AV from the app picker. Then navigate to the Connectors tab, and click the Create EC2 Connector button.

Our wizard will walk you through the steps for configuring a working connection to the EC2 APIs.
You will need to provide AWS Access Keys with read access as part of the Connector configuration.

**Configuration to acquire AWS Access Credentials**

You must associate valid AWS IAM (Identity and Access Management) credentials with sufficient privileges to read from your AWS account through the EC2 APIs. This credential comes in the form of an AWS IAM Access Key pair, which must be created by your AWS administrator and then typed/pasted into your Qualys EC2 Connector configuration.

AWS provides various out-of-the-box “read only” permission policy templates, many of which would allow our EC2 Connector to work. As of this writing, these three templates are known to include sufficient access for the Qualys EC2 Connector:

- Read Only Access
- Amazon EC2 Read Only Access
- Security Audit.

If you wish to provide absolute minimum permissions by creating a custom AWS permission policy, note that only the following Amazon EC2 API permissions are actually needed by the Qualys EC2 Connector as of this writing:

- DescribeInstances
- DescribeImages
- DescribeNetworkInterfaces

You can associate these permissions at the User level or Group level in AWS IAM.

Qualys discovers and syncs asset inventories every hour. Asset inventory is independent of a scan. See [AWS APIs used by EC2 Connector to discover assets](#)
Enabling GovCloud

The Qualys solution is also available for users of AWS GovCloud in addition to the global AWS regions.

Create a new Authentication record for an IAM user of your GovCloud AWS account. Select the newly created authentication record and select the checkbox at the bottom for “Set the connector only for AWS GovCloud (US) region”.

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 automatically activate all discovered EC2 assets (size medium and above). This makes them ready for scanning.

Note that assets of type m1.small, t1.micro or t2.nano instances are excluded from activation. These assets will be imported into the Qualys however they won’t be activated for VM, PC or SCA. The AWS acceptable scanning policy prevents us from scanning the m1.small, t1.micro or t2.nano instances.

Want to activate later? Sure you can do it manually anytime with Qualys AssetView. Just go to the Assets tab, select the assets you want to activate, then choose “Activate Assets” from the Actions menu.
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.

<table>
<thead>
<tr>
<th>App</th>
<th>Asset inventory</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM, PC, SCA</td>
<td>Assets &gt; Host Assets tab</td>
</tr>
<tr>
<td>AssetView</td>
<td>Assets tab</td>
</tr>
</tbody>
</table>
How does EC2 Connector work?

Let us quickly see how EC2 connector works.

**Asset Discovery**: The EC2 connector performs the asset discovery for your cloud with its continuous synchronization mechanism. The EC2 connector synchronizes every hour with the AWS account and pulls in all the instances (including terminated instances) from your account.

AWS retains the terminated instances for only about 15 minutes. 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 the scanner appliances, you need to activate Vulnerability Management/Policy Compliance/Security Configuration Assessment licenses for the assets you added to your Qualys account. You could opt to 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 or t2.nano instances are also excluded from activation. The AWS acceptable scanning policy prevents us from scanning the m1.small, t1.micro or t2.nano instances. 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 or t2.nano, which cannot be scanned by Qualys scanners as per AWS Acceptable Use Guidance for Scanning. Excluded assets are subset of synchronized assets.
Securing AWS with Qualys
Automate Asset Inventory

**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 AssetsView. The EC2 Information tab of Asset details page displays the AWS instance metadata collected. Here is the sample screen shot that display the information we collect.

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

**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 of an hour. 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:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create AWS Auth Record</td>
<td>This API creates the AWS Authentication Record</td>
<td><a href="https://qualysapi.qualys.com/qps/rest/2.0/create/am/awauthrecord">https://qualysapi.qualys.com/qps/rest/2.0/create/am/awauthrecord</a></td>
</tr>
<tr>
<td>Create AWS Connector</td>
<td>This API creates the EC2 connector</td>
<td><a href="https://qualysapi.qualys.com/qps/rest/2.0/create/am/awsassetdataconnector">https://qualysapi.qualys.com/qps/rest/2.0/create/am/awsassetdataconnector</a></td>
</tr>
<tr>
<td>Run Connector</td>
<td>This API runs the EC2 connector</td>
<td><a href="https://qualysapi.qualys.com/qps/rest/2.0/run/am/assetdataconnector/">https://qualysapi.qualys.com/qps/rest/2.0/run/am/assetdataconnector/</a>&lt;id&gt;</td>
</tr>
<tr>
<td>Get Host Asset Info</td>
<td>This API gets the metadata of an EC2 instance</td>
<td><a href="https://qualysapi.qualys.com/qps/rest/2.0/get/am/hostasset/">https://qualysapi.qualys.com/qps/rest/2.0/get/am/hostasset/</a>&lt;id&gt;</td>
</tr>
</tbody>
</table>
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 reuse.

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**
Qualys recommends to host the Qualys Virtual Scanner Appliance on a t2.medium instance. You can then scale up based on the number of EC2 instances being scanned, and the number of times the instances are scanned. XScanner 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.

![Diagram of VPCs](image)

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

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 and the scanner will permanently lose all of its settings.

Scanner Deployment
The scanner deployment involves configuration in Qualys account as well as AWS configuration.

Scanner Deployment - Configuration in Qualys
Let us see the configuration steps needed in Qualys account during scanner deployment.

Setting up Virtual Appliance - Get Personalization Code
Go to Qualys Vulnerability Management (VM) or Policy Compliance (PC) - Just select VM or PC from the Qualys app picker.

Navigate to Scans > Appliances and select New > Virtual Scanner Appliance.
Choose “I have my image” and click Continue.

Provide a name and click Next.

Follow the onscreen instructions to configure your virtual scanner. Click Next.
Get your personalization code. You’ll need this to launch your AMI instance.

Scanner Deployment - 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).

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

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 it needs penetration testing forms to be submitted. 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 User data field you must enter the personalization code you obtained from the Qualys user interface and optionally proxy server (if used).

![Screenshot of AWS Console showing user data entry](image)

**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.

Important: The proxy server needs to allow access to AWS region-specific endpoints. Go here to learn about regions & endpoints: [http://docs.aws.amazon.com/general/latest/gr/region#ec2_region](http://docs.aws.amazon.com/general/latest/gr/region#ec2_region)

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 (FQDN is supported for virtual scanners only), `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.

--If you are using proxy server then ensure you have outbound rule allowing access on port 443 and the port used to communicate with proxy server.

--If scanner appliance has direct internet connectivity, then ensure that out bound 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.

--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.

Quick links We recommend these resources s

- 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 or Qualys PC - We recommend these steps before scanning.

---Check Appliance Status

--Define Amazon EC2 API Proxy settings in Qualys UI (only if you have 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.

![Image of Vulnerability Management screen with an appliance listed](image)

**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 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.

The General 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 End points to be accessible via that proxy. Identify the URL to an end point from here - http://docs.aws.amazon.com/general/latest/gr/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 (default), 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 option

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 option

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](#)
Securing AWS with Qualys
Scan Assets

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

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

Quick links We recommend these resources

Qualys Cloud Platform
Qualys Cloud Agent Getting Started Guide
Securing AWS with Qualys

Scan Assets

Perimeter Scanning using Qualys External Scanners

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

- You’ll use the Standard Scan workflow in Qualys
- Customers need to add the Public IPs of the Instances to your account.
- Qualys External Scanners support both IP-based scans and DNS-based scans

You will have to take prior approval from AWS (by filling in [AWS Vulnerability Testing Request](#)) if you are planning to use Qualys external scanners for scanning AWS instances. You can refer to [AWS Acceptable Use Guidance For Scanning](#) for more details on AWS approval.

What are the steps

Go to Qualys VM for a vulnerability scan - Use the Scan workflow in Qualys to launch scans.

For Option Profile we recommend Initial Options to get started, for Scanner Appliance select the External scanner, for scan target choose IP addresses, asset groups containing IP addresses, asset tags defined using Qualys AssetView (AV).

Go to Qualys PC for a compliance scan. You’ll use similar Scan workflow to launch scans.

Scanning profile options

As a part of the Scanning option profile, you can turn ON the Load balancer check and also if you have special HTTP header that can be defined too. In this case, the scanner will try to reach out the IPs and wherever the IPs are getting directed to say ELB (Elastic Load Balancer) and try to get to the instances behind it as allowed or routed by the ELB. Ensure that you enable authentication for Windows and/or Unix. See [Configure OS Authentication](#).
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.

Adding IPs to scan: Users normally resolve the IPs outside Qualys and then add the IPs for scanning.

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.

AWS Vulnerability Testing Request

The main objective of vulnerability testing is to determine exploitable vulnerabilities and security weakness. AWS considers Vulnerability testing as malicious behavior and thus blocks the source IP address. Before performing running a scan against your AWS infrastructure using Qualys External Scanner you need to inform the AWS about the test.

You can request authorization for vulnerability testing by signing in with your root account credentials and filling out the AWS Vulnerability Testing Request Form.

You need to agree to the terms and conditions and AWS policy Regarding the Use of Security Assessment Tools and Services Agreement. You also need to provide the following information in the request form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Recommended Settings and description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Information</td>
<td>Provide your company contact information such as name, email address, and other required details.</td>
</tr>
<tr>
<td>Target Data</td>
<td>Provide the instance ID &amp; IP address of the EC2 instances that will be targeted in the scan.</td>
</tr>
<tr>
<td>DNS Zone Walking</td>
<td>Provide DNS server details such as name of the server, domain name, and IP address.</td>
</tr>
<tr>
<td>Source Data</td>
<td>Specify source of the scan as Qualys external scanners. You can get the IP address range by logging in to Qualys Portal and navigating to Help &gt; About option.</td>
</tr>
</tbody>
</table>

Testing Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Recommended Settings and description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expected peak bandwidth (Gbps)</td>
<td>Typically, its few MBs to 10s of MBs depending on the system. Since external scanning is primarily unauthorized (unless you configure the authentication record) the file size per instance being scanned is less.</td>
</tr>
</tbody>
</table>
Securing AWS with Qualys
Scan Assets

<table>
<thead>
<tr>
<th>Field</th>
<th>Recommended Settings and description</th>
</tr>
</thead>
</table>
| Expected peak requests per second (RPS)    | Depends on the number of hosts being scanned, as well as the Performance settings of the option profile in use. Here is the formula to calculate the same:  
  **Formula:**  
  \[(H \times P)/(D+1)\]  
  **Legend:**  
  H = Number of hosts being scanned.  
  P = Number of processes specified to run in parallel.  
  D = Packet (Burst Delay in Seconds).  
  If you are using the Initial Options Profile, and there are 15 hosts, then the estimated value could be 75. Here’s the calculation:  
  \[15[H] \times 10[P] = 150/(2[D]) = 75\] |
| Expected peak Queries per second (QPS) for DNS Zone Walking | Typically, this should be between 4 and 8 DNS queries per host scanned. |
| Start Date and Time                        | Provide the start date of your scan. |
| End Date and Time                          | Provide an end date for your scan depending on the option profile in use, as well as the number of hosts being scanned. |
| Additional testing details and why this testing is needed | Provide any other details on purpose of the test. |
| What criteria/metrics will you monitor to ensure the success of this test? | Qualys scan is to be marked as Finished on the Qualys platform. |
| Do you a way to immediately stop the traffic if we/your discover any issue | Yes |
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 chapter 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

You could simply run a query for your assets and create a widget and add it to your dashboard. For example, let us search for AWS assets that are in running state and have not been scanned for a month. Type your query and then click Create a widget. You could then add the widget to the dashboard.
Dynamic Tagging Using EC2 Attributes

You can create dynamic tags using EC2 metadata attributes for assets as collected by the EC2 connector. You can use this dynamic tag as the scope for your EC2 scans. Go to AssetView > Assets > Tags and then create dynamic tag by using 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.

<table>
<thead>
<tr>
<th>Vulnerabilities Total</th>
<th>Security Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>By Status</th>
<th>Confirmed</th>
<th>Potential</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>0</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>Active</td>
<td>10</td>
<td>-</td>
<td>10</td>
</tr>
<tr>
<td>Re-Opened</td>
<td>0</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>10</td>
<td>-</td>
<td>10</td>
</tr>
<tr>
<td>Fixed</td>
<td>0</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>Changed</td>
<td>0</td>
<td>-</td>
<td>0</td>
</tr>
</tbody>
</table>
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 in 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 asset 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.
Use Case 3 - Automate scanning into DevOps process to harden the AMI

In AWS, it is a best practice to create your own custom AMI 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](#).
Securing AWS with Qualys
Manage Assets using Qualys
# Common Questions

<table>
<thead>
<tr>
<th>Queries</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Results and EC2 Instance ID</td>
<td>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.</td>
</tr>
<tr>
<td>How does EC2 scan job handles Terminated EC2 instances?</td>
<td>We’ll automatically filter out all EC2 instances with a Terminated status from EC2 scans, launched from Qualys VM 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.</td>
</tr>
<tr>
<td>What User Permissions are needed for EC2 Scans?</td>
<td>Managers and Unit Managers can start, schedule and manage EC2 scans using Qualys VM and Qualys PC as per their Qualys license. Qualys VM - 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 an asset group in the Unit Manager’s business unit by a Manager.</td>
</tr>
</tbody>
</table>
## Queries

<table>
<thead>
<tr>
<th><strong>How to view platform provider info on virtual scanner appliances?</strong></th>
<th><strong>Solutions</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>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 &gt; Appliances).</td>
<td></td>
</tr>
</tbody>
</table>

![Edit Scanner Appliance](image)

## 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.