



# Securing Google Cloud Platform with Qualys

July 28, 2021

Copyright 2021 by Qualys, Inc. All Rights Reserved.

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

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



# Table of Contents

|  |           |
|--|-----------|
| <b>About this guide.....</b>   | <b>5</b>  |
| About Qualys .....   | 5         |
| Qualys Support .....   | 5         |
| <b>Introduction.....</b>   | <b>6</b>  |
| Qualys Cloud Platform .....  | 6         |
| Prerequisites .....  | 7         |
| <b>Scanning in GCP Environments .....</b>                                | <b>10</b> |
| Networking Basics .....  | 10        |
| Use Cases for Scanning GCP environment .....                             | 10        |
| <b>Deploying Sensors.....</b>  | <b>17</b> |
| Deploying Virtual Scanner Appliance in Google Compute Engine (GCP) ..... | 17        |
| Cost and Licenses .....  | 17        |
| Qualys Cost .....  | 17        |
| GCP Cost .....   | 18        |
| Deployment Recommendations for Scanner .....                             | 18        |
| Instance Snapshots or Cloning Not Allowed .....                          | 18        |
| Moving or Exporting Instance Not Allowed .....                           | 18        |
| Virtual Machine Size for Hosting the Scanner .....                       | 18        |
| What Do I Need? .....  | 19        |
| What Is Not Supported? .....   | 19        |
| Generating a Personalization Code .....                                  | 19        |
| Launching Virtual Scanner Appliance .....                                | 21        |
| Deploying Qualys Cloud Agent from Google Cloud Console .....             | 32        |
| <b>Scanning Assets .....</b>   | <b>40</b> |
| GCP Scan Checklist .....   | 40        |
| Internal Scanning using Virtual Scanning Appliance .....                 | 44        |
| Internal Network Scanning by using Qualys Cloud Agent .....              | 46        |
| External Scanning using External Scanner Appliance .....                 | 47        |
| Cloud Inventory and Security Assessment .....                            | 48        |
| Securing Web Applications .....  | 51        |
| Securing Containers .....  | 52        |
| <b>Analysis, Reporting and Remediation .....</b>                         | <b>54</b> |
| Downloading and Exporting Results .....                                  | 55        |
| Creating Widget .....  | 56        |
| Creating Reports .....   | 56        |

|   |           |
|---|-----------|
| Dynamic Tagging by Using GCP Metadata .....           | 57        |
| <b>Organizing Assets in Qualys Subscription .....</b> | <b>60</b> |
| Setting up Qualys Configurations .....                | 60        |
| Uninstalling Agents .....                             | 62        |
| <b>Frequently Asked Questions (FAQs).....</b>         | <b>64</b> |

## 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 by 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, visit [www.qualys.com](http://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/](http://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, let's talk about securing your Google Cloud Platform infrastructure by using Qualys Cloud Platform.

## Qualys Cloud Platform

As a unified architecture that powers more than 15 Qualys security and compliance Cloud Apps, the Qualys Cloud Platform offers you a streamlined solution for avoiding the cost and complexities of managing multiple security vendors. By automatically gathering and analyzing security and compliance data from IT assets anywhere in one single-pane view, the Qualys Cloud Platform gives you the scalability, visibility, accuracy, and breadth of capabilities to fight cyber-attacks and build security into your digital transformation initiatives.

If you're new to Qualys, we recommend you visit the [Qualys Cloud Platform](#) web page to know more about our cloud platform.

| ASSET MANAGEMENT   | IT SECURITY   | COMPLIANCE                           | CLOUD / CONTAINER SECURITY | WEB APP SECURITY |
|--|---|--------------------------------------|----------------------------|------------------|
| Global AssetView -<br><b>It's Free! Unlimited Assets</b> | Vulnerability Management,<br>Detection & Response - <b>Most Popular</b> | Policy Compliance                    | Cloud Inventory            | Web App Scanning |
| CyberSecurity Asset<br>Management - <b>New</b>           | Threat Protection   | Security Configuration<br>Assessment | Cloud Security Assessment  | Web App Firewall |
| Certificate Inventory                                    | Continuous Monitoring   | PCI Compliance                       | Container Security         |                  |
|  | Patch Management  | File Integrity Monitoring            |                            |                  |
|  | Endpoint Detection &<br>Response - <b>New</b>                           | Security Assessment<br>Questionnaire |                            |                  |

## Qualys Integration with Google Cloud Security Command Center: Overview

You can now integrate Qualys Cloud Platform with the Cloud Security Command Center (Cloud SCC) for Google Cloud Platform (GCP), a security and data risk platform helping enterprises to gather data, identify threats, and act on them before they result in business damage or loss.

Cloud SCC provides security teams a single pane for security features, policies, and insights across GCP. Qualys' integration expands on existing data within the Cloud SCC by adding vulnerability management and threat data for compute engine instances within a GCP project.

This capability gives customers visibility of Qualys data within Cloud SCC and allows DevOps and security teams to protect their workloads by gaining full visibility of vulnerability and threat posture at a glance. Users can further drill-down to find details and actionable intelligence for every identified vulnerability and can navigate with a single-click back to their Qualys subscription for additional reports and threat intelligence.

Customers can gain access to Qualys-generated vulnerability and threat posture data within Cloud SCC by deploying Qualys' lightweight Cloud Agents on workload images. This step either bakes the agent within the image or automatically deploys the agent on the compute engine instance.

## Prerequisites

For the Qualys Integration with Google Cloud Security Command Center, the following options must be enabled for your Qualys subscription.

### Active Qualys subscription:

To leverage the Qualys data collection, evaluation, and reporting capabilities for your GCP VM instances, you must first have an active Qualys subscription. For more details, contact [Qualys Support](#) or [sign up for a free trial](#).

### Qualys Applications:

- You must have the [Qualys Vulnerability Management \(VM/VMDR\)](#) and [Qualys Cloud Agent](#) modules enabled in your subscription.
- Cloud Agents must be installed on your GCP VM instances. For more information, see [Deploying Qualys Cloud Agent from Google Cloud Console](#).
- As an alternative to Cloud Agent, you can add Virtual Scanner Appliances and configure them for your GCP instances. GCP VM instance must be able to reach the Qualys Cloud Platform over the HTTPS port 443. You will also need a scanner personalization code (14 digits) which is used to deploy the Virtual Scanner Appliance. For every new virtual scanner appliance, you must generate a new personalization code. For more information, see [Deploying Virtual Scanner Appliance in Google Compute Engine \(GCP\)](#).

### Roles:

- You must have the **Manager** or the **Unit Manager** role in your Qualys subscription.
- You must have the following Cloud Identity and Access Management (Cloud IAM) roles to set up Security Command Center in Google cloud console:

Organization Admin (roles/resourcemanager.organizationAdmin)

Security Center Admin (roles/securitycenter.admin)

Security Center Settings Admin (roles/securitycenter.settingsAdmin)

Security Admin (roles/iam.securityAdmin)

Service Account Creator (roles/iam.serviceAccountCreator)

To learn more, see [Security Command Center roles](#).

### **Google Cloud Security Command Center (SCC):**

Security Command Center must be enabled for your organization. For more details, see [Quickstarts for Security Command Center](#).

### **Security Command Center API:**

You must enable the Security Command Center APIs for the selected project. To know more, see [Enable and disable Google APIs](#).

## **GCP Metadata**

The following cloud provider metadata is provided by Qualys Cloud Agent and Qualys Virtual Scanner Appliance.

### **Metadata provided by Qualys Cloud Agent**

#### **General:**

- Instance ID
- Host Name
- Machine Type
- Zone
- Project Number
- Project ID

#### **Network:**

- Private IP Address
- MAC Address
- VPC Network
- Public IP Address
- Network Interfaces

### **Metadata provided by Qualys Virtual Scanner Appliance**

#### **QID-45465 Google Cloud Platform (GCP) Linux Instance Metadata:**

- CPU-platform
- Description
- Hostname
- ID



- Image
- Machine-type
- Maintenance-event
- Name
- Tags
- Zone

Read more about [Dynamic Tagging by Using GCP Metadata](#).

# Scanning in GCP Environments

In this section, let's take a look at some common use cases for scanning a GCP environment.

## Networking Basics

To start with, let's get familiar with a few terms in networking basics.

### VPC networks

A Virtual Private Cloud (VPC) network provides networking functionality for Google Compute Engine Virtual Machine (VM) instances. This pretty much resembles a traditional network in your own data center, except that it is virtualized within Google cloud. Without a VPC Network, you cannot create VM instances. It is a global resource; but an organization may want to separate their deployment environments, and so, they create VPCs for isolation purposes.

### VPC Peering

This is a networking connection between two VPCs that enables you to connect VM instances hosted in separate VPC networks and route traffic between them.

### Subnets

These are one or more useful IP range partitions in each VPC network. It is a regional resource.

To understand the scanning procedure, see [Scanning Assets](#).

## Use Cases for Scanning GCP environment

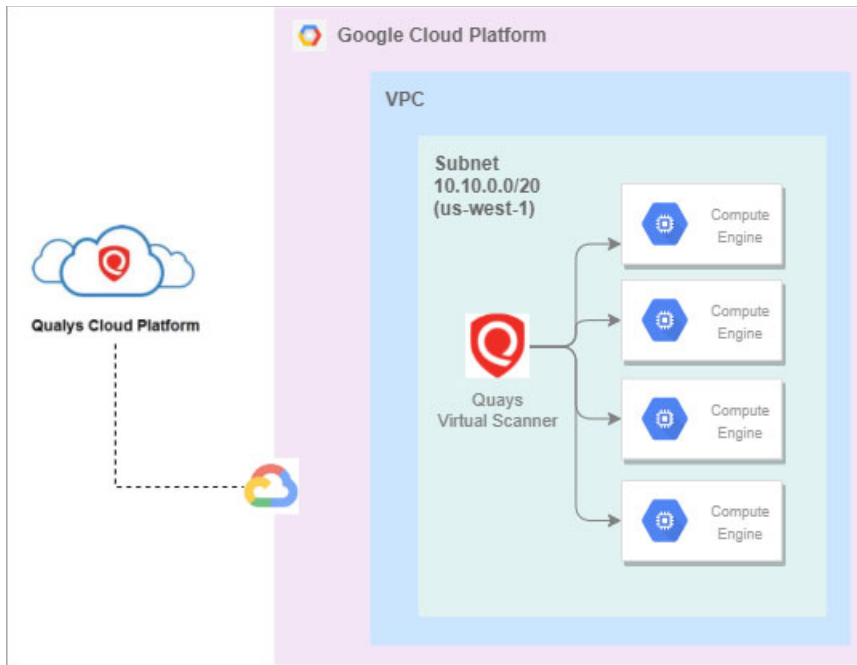
The following are a few common use cases for scanning a GCP environment. You must configure your virtual scanner appliances to communicate to Qualys Cloud Platform over HTTPS (via firewall rules and proper routing).

- [Single scanner to scan multiple instances in a VPC in a single region](#)
- [Multiple scanners to scan multiple instances in a VPC in a single region](#)
- [Single scanner to scan multiple instances across subnets in different regions in a VPC](#)
- [Multiple scanners to scan multiple instances across subnets in different regions in a VPC](#)
- [Single scanner to scan multiple instances across subnets in different regions across peered VPCs](#)
- [Multiple scanners to scan multiple instances across subnets in different regions across peered VPCs](#)
- [Scanner cannot scan instances in non-peered VPC](#)

- Scanner cannot scan instances in VPCs with overlapping IP address

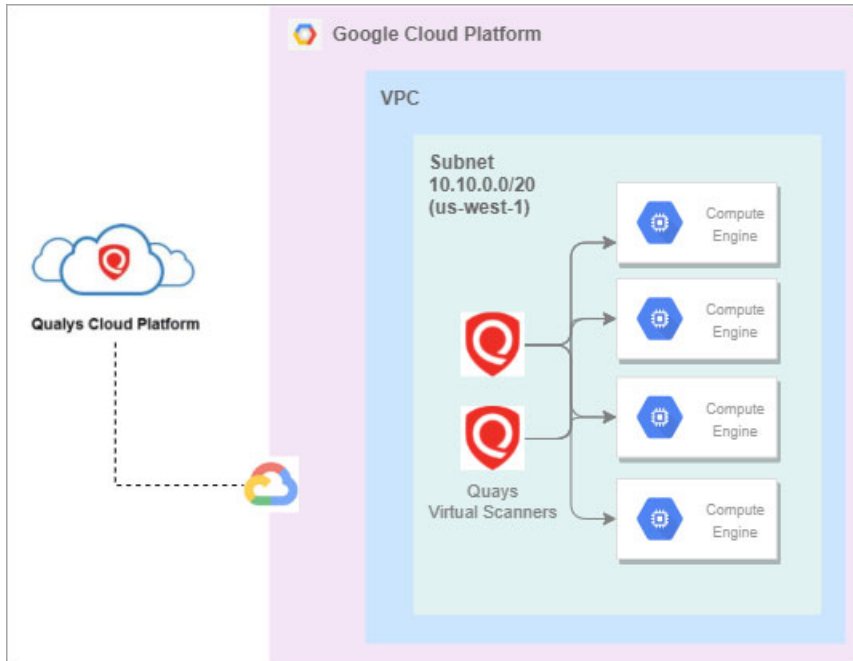
### Single scanner to scan multiple instances in a VPC in a single region

A single Qualys scanner appliance can be configured to scan multiple GCP VM instances running in a single VPC in a single region.



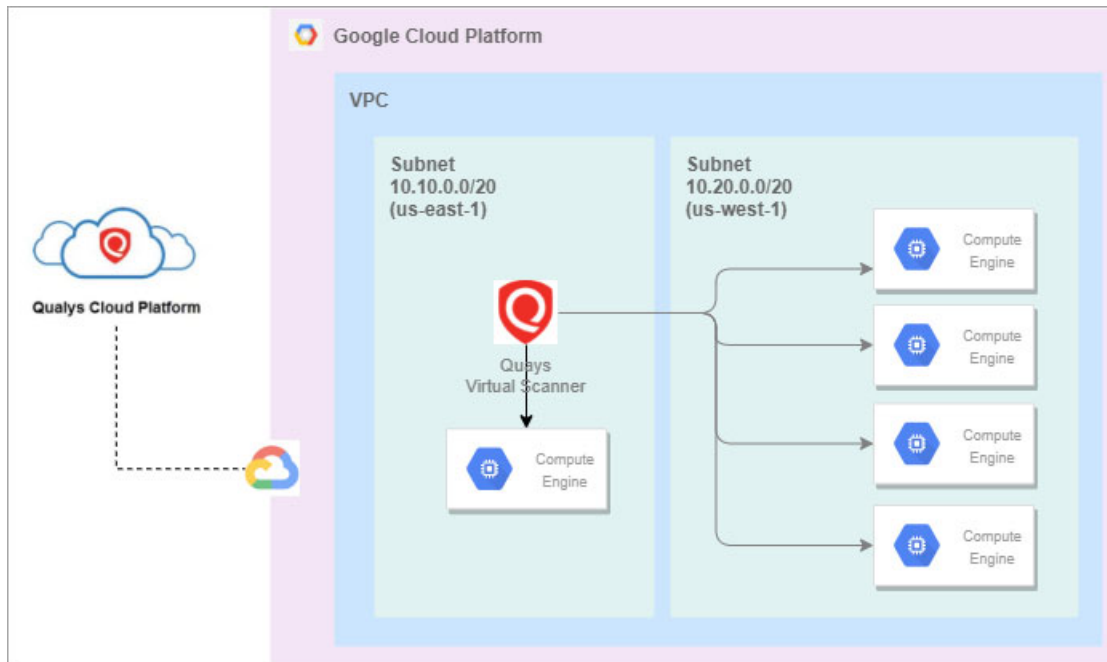
### Multiple scanners to scan multiple instances in a VPC in a single region

Based on the number of VM **instances** and scan frequency, multiple scanners might be required to scan multiple VM Instances in a subnet in a VPC. You can add more scanners based on requirements.



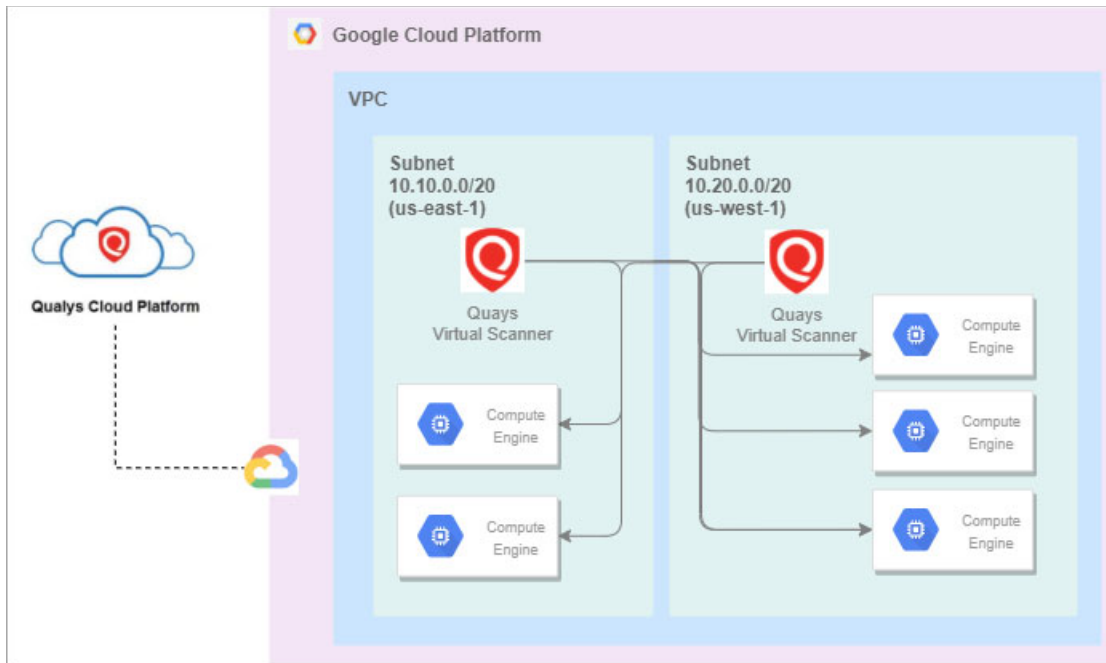
### Single scanner to scan multiple instances across subnets in different regions in a VPC

A single scanner can reach multiple VM instances across different subnetworks in different regions within a single VPC.



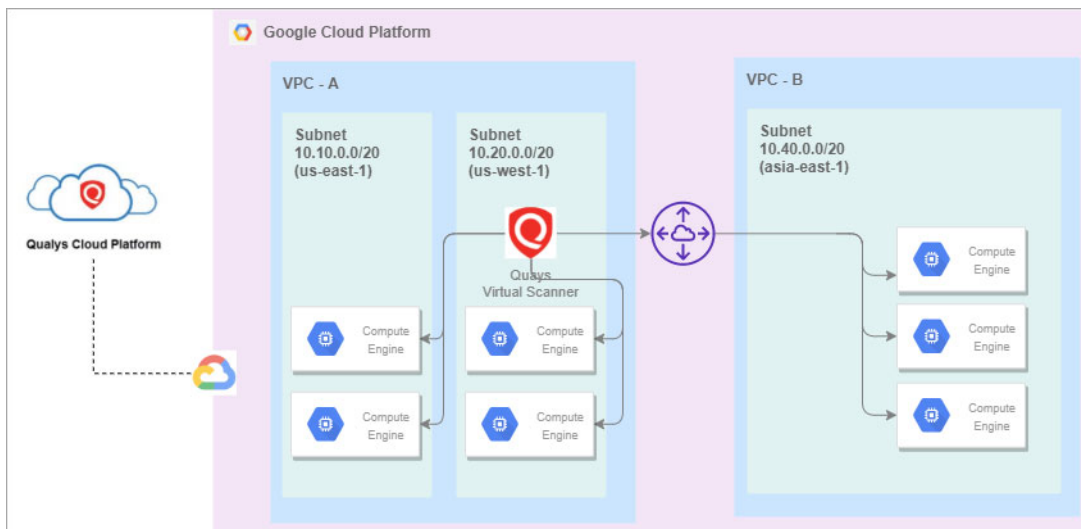
### Multiple scanners to scan multiple instances across subnets in different regions in a VPC

Based on the number of VM instances and scan frequency, multiple scanners might be required to scan multiple VM instances across subnets in different regions in a VPC. You can add more scanners based on requirements.



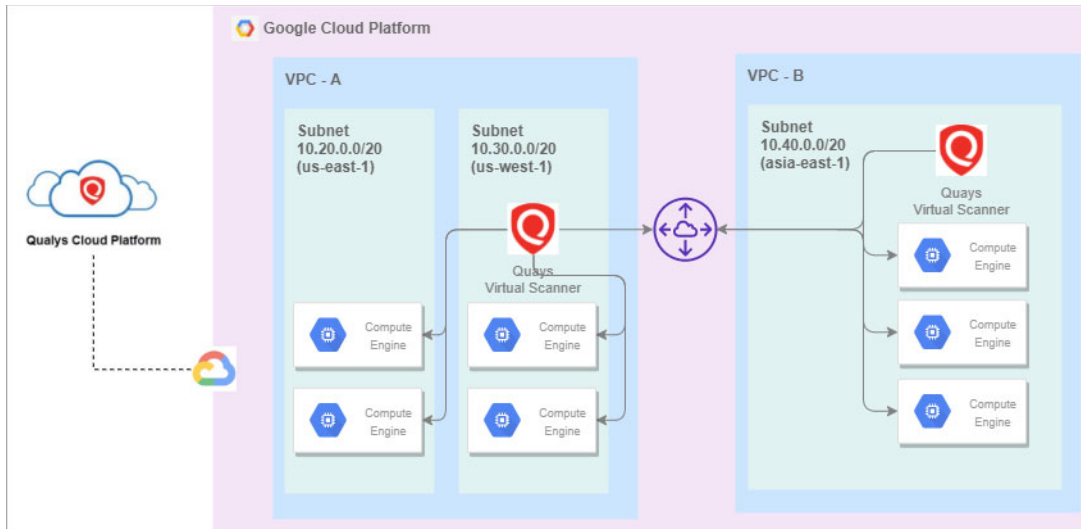
### Single scanner to scan multiple instances across subnets in different regions across peered VPCs

A single scanner can reach multiple VM instances in different regions and subnets in a peered VPC.



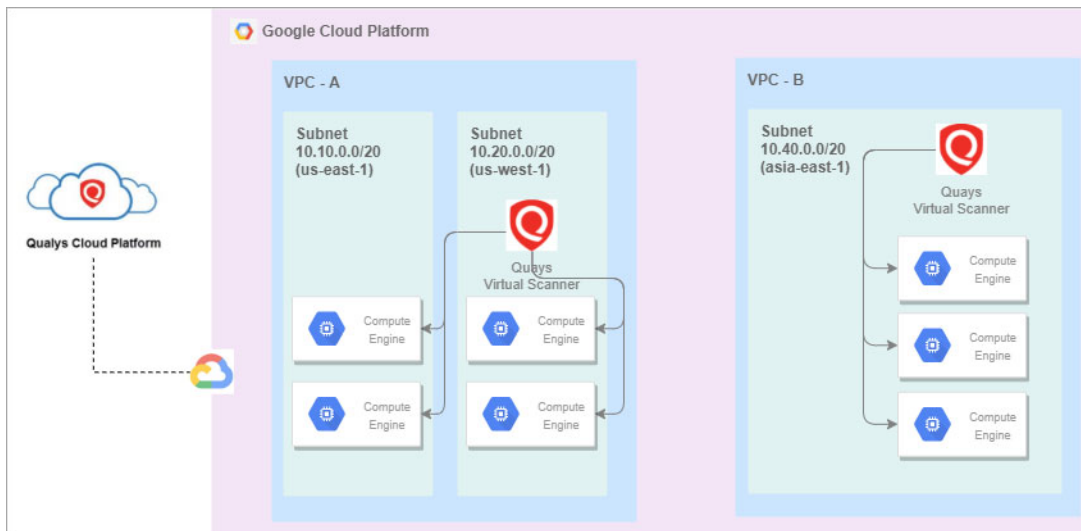
## Multiple scanners to scan multiple instances across subnets in different regions across peered VPCs

Based on the number of machines and scan frequency, multiple scanners might be required to scan multiple VM instances across peered VPCs in different regions.

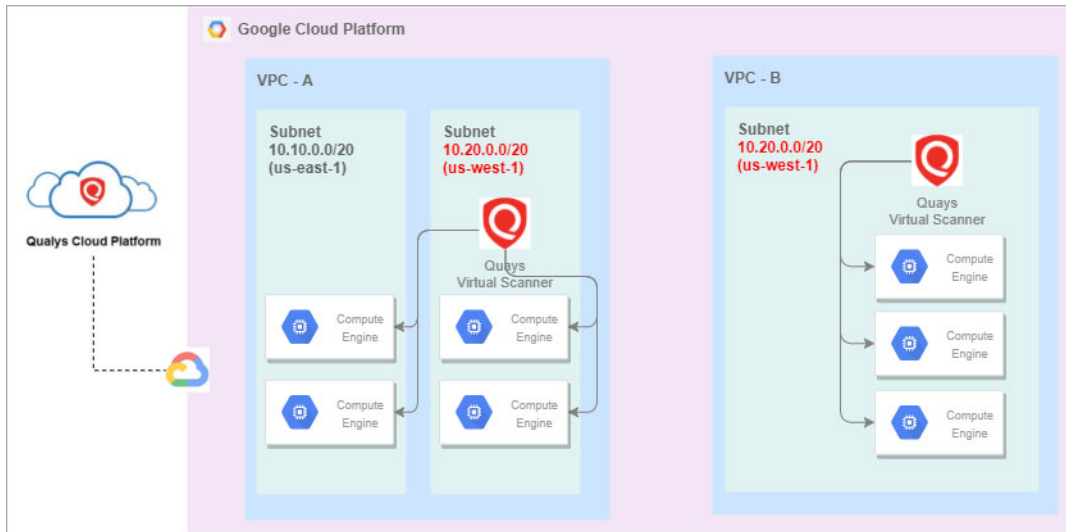


## Scanner cannot scan instances in non-peered VPC

Scanner's reachability is curtailed if the VPCs are not peered. In non-peered VPCs, scanners cannot reach the VM instances to launch a scan.



## Scanner cannot scan instances in VPCs with overlapping IP address



A single scanner cannot scan VM instances in VPCs with overlapping IP addresses due to reachability issues. Add more scanner appliances based on your requirements to allow scanning across VPC boundaries.

In case of regions displayed in the sample screenshot, VPC peering cannot be configured between VPC-A and VPC-B. So, in this case, scanner in VPC-A cannot reach VM instances in VPC-B as VPC-A and VPC-B have one overlapping IP Address (10.20.0.0/20).

To understand the scanning procedure, see [Scanning Assets](#).



## Deploying 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.

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

- [Deploying Virtual Scanner Appliance in Google Compute Engine \(GCP\)](#)
- [Deploying Qualys Cloud Agent from Google Cloud Console](#)

### Deploying Virtual Scanner Appliance in Google Compute Engine (GCP)

You can scan your Google Cloud Compute Engine instances along with all other global elastic cloud and on-premise assets from within the Qualys Cloud Platform. Qualys Virtual Scanner Appliance can be directly deployed from the Google Marketplace.

Scanner deployment involves configuration in Qualys Cloud Platform as well as GCP.

Before we know the steps to deploy a virtual scanner, let's understand the licensing/cost aspect and the deployment recommendations.

#### Cost and Licenses

Qualys Virtual Scanner Appliance is available as an image at Google Cloud Marketplace, ready for customers to launch onto GCP Virtual Machines. There are two aspects to consider:

- Qualys costs for the virtual scanner license subscription.
- GCP costs for the computing resources to run the appliance as a virtual machine.

**Note:** Ensure that you use the image available at Google Cloud Marketplace or the Signed URL provided by Qualys for downloadable GCP-specific images. Using images downloaded from Qualys UI are not recommended to be used on GCP.

#### Qualys Cost

You need to acquire a Qualys license for each virtual scanner appliance instance that you would like to run. This license is acquired from Qualys, not from GCP, and our scanner appliances are listed at Google Cloud Marketplace with a Bring Your Own License (BYOL) 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. However, the personalization code that you generate to register a scanner appliance can be used only once. For every new virtual scanner appliance, you must generate a new personalization code.

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

## **GCP Cost**

For each virtual scanner appliance, virtual machine is launched into one of your own GCP accounts. You are responsible for paying Google for the costs of running the appliance. Those costs include:

- Compute Capacity based upon size
- 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 may not need to keep your scanner appliances running at all times. Any hours during which your virtual machine is stopped, only per-GB-provisioned storage charges are incurred. For those able to spend a little more upfront, GCP virtual machines can be reserved by financially committing for one or three years to save. 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 GCP instance for hosting the scanner appliance.

### **Instance Snapshots or Cloning Not Allowed**

Using a snapshot or clone of a virtual scanner instance to create a new instance is strictly prohibited. The new instance does 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 or Exporting Instance Not Allowed**

Moving or exporting a registered scanner instance from a virtualization platform (HyperV, VMware, XenServer) in any file format to the Google Cloud Platform is strictly prohibited. This breaks scanner functionality and the scanner permanently loses all its settings.

### **Virtual Machine Size for Hosting the Scanner**

The default sizing for a Qualys Virtual Scanner Appliance is 2 vCPU and 7.5 GB memory and can be customized. The maximum supported limit by Qualys is 16 CPUs and 16 GB RAM. Based on the frequency of scanning, and the number of GCP Virtual machines that are being scanned, you can scale up to machine t16 CPUs and 16 GB RAM. For customization, choose core to memory in the ratio of 1:3.5.

## 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.

## What Is Not Supported?

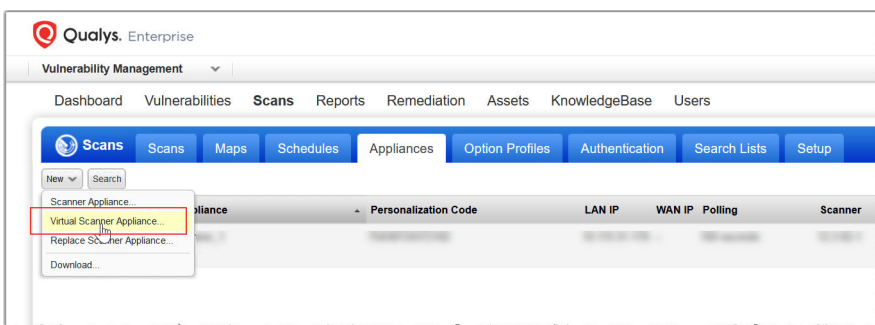
The following features are not supported and are disabled in all cloud (private and public) platforms:

- 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.

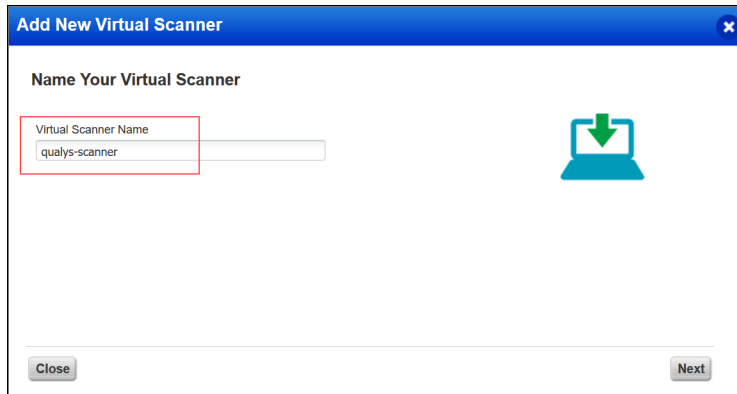
## Generating a Personalization Code

Get a personalization code from your Qualys Cloud Platform subscription to register every new appliance instance. To get the code, do the following:

1. Log in to the Qualys UI.
2. From the module picker in the left, choose **Vulnerability Management** or **Policy Compliance**, depending on your scanning needs.
3. Go to **Scans > Appliances** and select **New > Virtual Scanner Appliance**.

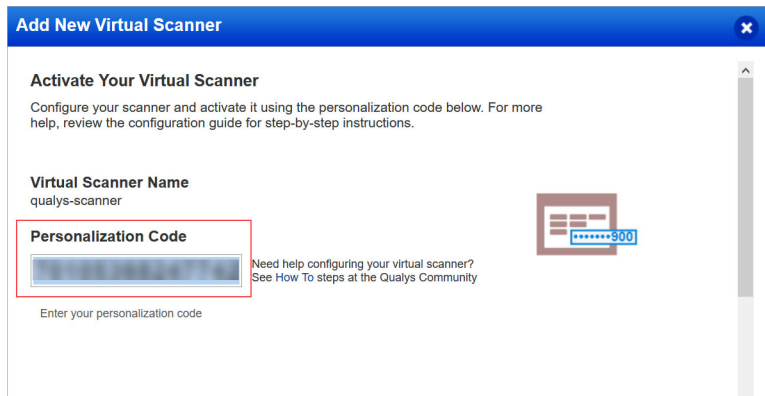


4. In the **Add New Virtual Scanner** dialog box, click **Continue** in the **I Have My Image** section. Give your virtual scanner a name. As per the GCP naming conventions, you can use lowercase letters, numbers, and hyphens in the scanner name.



The screenshot shows a dialog box titled "Add New Virtual Scanner" with a close button (X) in the top right corner. The main heading is "Name Your Virtual Scanner". Below it, there is a text input field labeled "Virtual Scanner Name" containing the text "qualys-scanner". To the right of the input field is a blue icon of a laptop with a green arrow pointing down into it. At the bottom of the dialog, there are two buttons: "Close" on the left and "Next" on the right.

5. Click **Next** to walk through the wizard. Copy the personalization code.



The screenshot shows the same dialog box, now at the "Activate Your Virtual Scanner" section. The heading is "Activate Your Virtual Scanner" with a subtext: "Configure your scanner and activate it using the personalization code below. For more help, review the configuration guide for step-by-step instructions." Below this, the "Virtual Scanner Name" field still shows "qualys-scanner". To the right is a red icon of a document with a blue box containing a personalization code. Below the name field, there is a "Personalization Code" label and a text input field containing a blurred code. To the right of the input field is a link: "Need help configuring your virtual scanner? See [How To](#) steps at the Qualys Community". At the bottom, there is a prompt: "Enter your personalization code".

6. Keep this window open and switch to your Google Cloud Portal to launch the appliance. You can check for activation status in the same window after deployment.

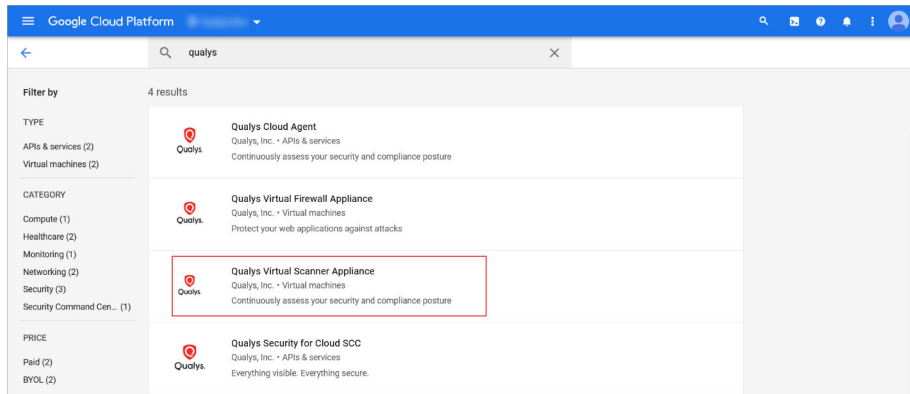
## Launching Virtual Scanner Appliance

You can deploy a Qualys Virtual Scanner Appliance by either of the following ways:

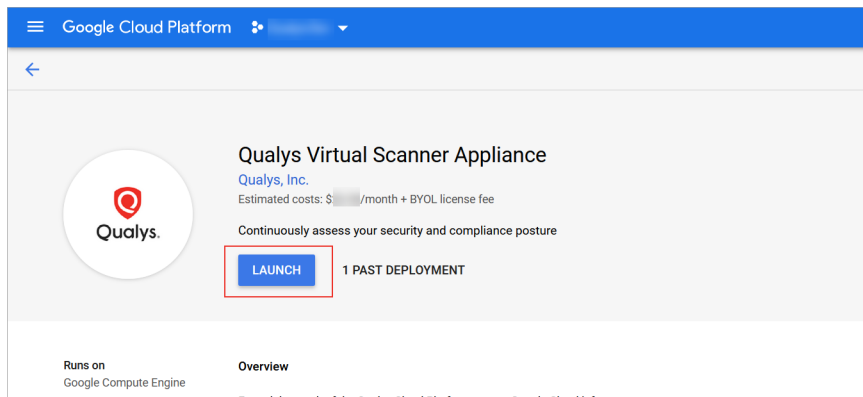
- [Deploying scanner from Google Cloud Marketplace](#)
- [Deploying Custom Image on Private Cloud Platforms](#)

### Deploying scanner from Google Cloud Marketplace

1. Sign in to Google Cloud Platform and navigate to **Marketplace**.
2. In the **Search** box, type Qualys, and then from the search results, click **Qualys Virtual Scanner Appliance**.



3. Click **Launch**.



4. Provide the following details for the virtual scanner appliance instance:

**Deployment name:** It is advised to specify the same name that you use on the Qualys Cloud Platform while generating a personalization code.

**Zone:** Select a zone that co-locates the scanner instance with scan target instances. For the scanner to reach other zones, setup connectivity with appropriate network configurations is needed.

**Machine type:** The default pre-set is 2 vCPU and 7.5 GB memory and can be customized.

Note: The appliance supports a maximum of 16 cores and 16GB memory. For customization, choose core to memory in the ratio of 1:3.5.

**Personalization code:** Provide the 14-digit personalization code generated from Qualys Cloud Platform. This is a one-time use code only. To register every new virtual scanner appliance instance, you must generate a fresh personalization code.

**Proxy URL** (Optional): Add the proxy server URL to communicate with Qualys Cloud Platform via SSL tunneling proxy. We support both IP and FQDN for the proxy server configuration. Specify the proxy server URL as username:password@proxyhost:port

|                      |  |
|----------------------|--|
| Syntax for proxy URL | <ul style="list-style-type: none"> <li>• If you have a domain user, use this syntax:<br/>domain\username:password@proxyhost:port</li> <li>• If authentication is not used, use this syntax:<br/>proxyhost:port</li> </ul> <p>where proxyhost is the IP address or the FQDN of the proxy server and port is the proxy port.</p> |
| Examples             | <ul style="list-style-type: none"> <li>• doe:abc12345@10.40.1.123:3128</li> <li>• jdoe:abc12345@myproxy.qualys.com:3128</li> </ul>   |

## Boot Disk

Do not change the following values unless instructed by Qualys Support:

**Boot disk type:** Standard Persistent Disk

**Book disk size in GB:** 56

Google Cloud Platform

Deploy Qualys Virtual Scanner Appliance to Google Compute Engine

Select or create a project 2 Configure & deploy

New Qualys Virtual Scanner Appliance deployment

Deployment name  
qualys-virtual-scanner-appliance-1

Zone  
us-west2-a

Machine type  
1 vCPU 3.75 GB memory Customize

Personalization Code

Proxy URL  
proxy\_user.proxy\_pass@proxyhost:port

Boot Disk  
Boot disk type  
Standard Persistent Disk

Boot disk size in GB  
56

Networking  
Network interfaces  
default default

+ Add network interface

You have reached the maximum number of one network interface

More

Deploy

Qualys Virtual Scanner Appliance overview

Qualys Solution provided by Qualys, Inc.

\$ per month estimated  
Effective hourly rate \$0.044 (730 hours per month)

Details

Software  
Operating System Qualys Appliance Linux (QAL-2.0-3)

Launching a BYOL solution

Qualys Virtual Scanner Appliance is a BYOL (Bring Your Own License) solution. Marketplace will deploy this solution, but you are responsible for purchasing and managing the license directly from the provider.

Terms of Service

By deploying the software or accessing the service you are agreeing to comply with the Qualys, Inc. terms of service, GCP Marketplace terms of service and the terms of applicable open source software licenses bundled with the software or service. Please review these terms and licenses carefully for details about any obligations you may have related to the software or service. To the limited extent an open source software license related to the software or service expressly supersedes the GCP Marketplace Terms of Service, that open source software license governs your use of that software or service.

By using this product, you understand that certain account and usage information may be shared with Qualys, Inc. for the purposes of sales attribution, performance analysis, and support.

Google is providing this software or service "as-is" and any support for this software or service will be provided by Qualys, Inc. under their terms of service.

5. Click **Deploy** and follow to the section [Post-deployment Progress and Monitoring](#).

## Deploying Custom Image on Private Cloud Platforms

Here you are expected to build a Qualys scanner image specific to your private cloud platform. Do the following:

1. Download the qVSA image file (tar.gz) by using the SAS link provided by Qualys Operations. For more details, contact Qualys Support.
2. Create a Google Storage Bucket.
3. Upload the downloaded qVSA image file to your storage bucket.
4. Create the Qualys Scanner Image by using the uploaded QVSA Image file (tar.gz) file.
5. Provide the following details for the virtual scanner appliance instance custom image:

**Name:** Provide a unique name to identify the Qualys Scanner appliance image.

**Source:** Select **Cloud Storage File** which allows you to select the Qualys Scanner image file stored in the Storage Bucket. In the following image, qualys-scanner is a bucket name and qVSA-GCE-xxxxxxx.tar.gz is the Qualys scanner image file.

**Create an image**

**Name** ⓘ  
Name is permanent  
qvs-a-gce-

**Source** ⓘ  
Cloud Storage file

**Cloud Storage file** ⓘ  
Your image source must use the .tar.gz extension and the file inside the archive must be named disk.raw. [Learn more](#)  
☒ qualys-scanner/qVSA-GCE- .tar.gz [Browse](#)

**Location** ⓘ  
☐ Multi-regional  
☒ Regional  
us-east1 (South Carolina)

**Family** (Optional) ⓘ

**Description** (Optional)

**Labels** ⓘ (Optional)  
[+ Add label](#)

**Encryption**  
Data is encrypted automatically. Select an encryption key management solution.  
☒ Google-managed key  
No configuration required  
☐ Customer-managed key  
Manage via Google Cloud Key Management Service  
☐ Customer-supplied key  
Manage outside of Google Cloud

You will be billed for this image. [Compute Engine pricing](#) ⓘ

[Create](#) [Cancel](#)

6. Generate a personalization code. (Generating a Personalization Code)

7. Provide the following details for the Virtual Scanner Appliance instance:

**Deployment name:** It is advised to specify the same name that you use on the Qualys Cloud Platform while generating a personalization code.



**Zone:** Select a zone that co-locates the scanner instance with scan target instances. For the scanner to reach other zones, setup connectivity with appropriate network configurations is needed.

**Machine type:** The default pre-set is 2 vCPU and 7.5 GB memory and can be customized.

**Note:** The appliance supports a maximum of 16 cores and 16GB memory. For customization, choose core to memory in the ratio of 1:3.5.

### **Boot Disk**

Change the boot disk to the newly created Qualys Scanner Appliance image disk.

Do not change the following values unless instructed by Qualys Support:

**Boot disk type:** Standard Persistent Disk

Book disk size in GB: 56

Name ?  
Name is permanent

Labels ? (Optional)  

+ Add label

Region ?  
Region is permanent  

us-central1 (Iowa)

Zone ?  
Zone is permanent  

us-central1-a

Machine configuration

Machine family  

General-purpose

Memory-optimized

Compute-optimized

  
Machine types for common workloads, optimized for cost and flexibility


Series  

N1

  
Powered by Intel Skylake CPU platform or one of its predecessors

Machine type  

n1-standard-2 (2 vCPU, 7.5 GB memory)



vCPU

2


Memory

7.5 GB

< CPU platform and GPU

Container ?  
☐ Deploy a container image to this VM instance. [Learn more](#)

Boot disk ?  



New 56 GB standard persistent disk

Image

qvs-a-gce-

Change

### Metadata (Optional)

You can set custom metadata for an instance or project outside of the server-defined metadata. This is useful in passing in arbitrary values to your project or instance that can be queried by your code on the instance.

**PERSCODE:** Provide the 14-digit personalization code generated from Qualys Cloud Platform.

26

See [Generating a Personalization Code](#).

**PROXY\_URL** (Optional): Add the proxy server URL to communicate with Qualys Cloud Platform via SSL tunneling proxy. We support both IP and FQDN for the proxy server configuration. Specify the proxy server URL as username:password@proxyhost:port

|                           |  |
|---------------------------|--|
| ProxySyntax for proxy URL | <ul style="list-style-type: none"><li>• If you have a domain user, use this syntax:<br/>domain\username:password@proxyhost:port</li><li>• If authentication is not used, use this syntax:<br/>proxyhost:port</li><li>• Where proxyhost is the IP address or the FQDN of the proxy server and port is the proxy port.</li></ul> |
| Examples                  | <ul style="list-style-type: none"><li>• doe:abc12345@10.40.1.123:3128</li><li>• jdoe:abc12345@myproxy.qualys.com:3128</li></ul>  |

**Metadata** (Optional)  
You can set custom metadata for an instance or project outside of the server-defined metadata. This is useful for passing in arbitrary values to your project or instance that can be queried by your code on the instance. [Learn more](#)

PERSCODE

×

PROXY\_URL

×

+ Add item

**Availability policy**

**Preemptibility**  
A preemptible VM costs much less, but lasts only 24 hours. It can be terminated sooner due to system demands. [Learn more](#)

Off (recommended)

▼

**On host maintenance**  
When Compute Engine performs periodic infrastructure maintenance it can migrate your VM instances to other hardware without downtime

Migrate VM instance (recommended)

▼

**Automatic restart**  
Compute Engine can automatically restart VM instances if they are terminated for non-user-initiated reasons (maintenance event, hardware failure, software failure and so on)

On (recommended)

▼

[^](#) Less

You will be billed for this instance. [Compute Engine pricing](#) [↗](#)

Create

Cancel

8. Click **Create**.

## Post-deployment Progress and Monitoring

Deployment of the Qualys Virtual Scanner Appliance can take up to 10 minutes. Upon deployment, the appliance connects with the Qualys Cloud Platform to complete registration. The appliance also downloads the latest software and vulnerability signatures.

You can monitor the progress of the instance creation in the GCE VM instances.

To view further progress of the appliance configuration or to diagnose any issues, look at the serial console output. Click 'Serial port 1 (console)' in the logs section.

## Logs

Cloud Logging

Serial port 1 (console)

Serial port 2

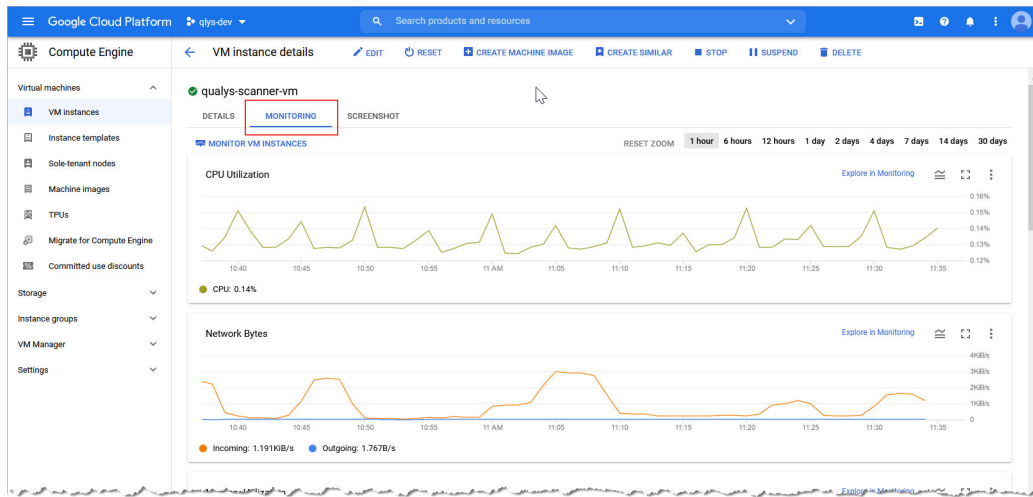
Serial port 3

Serial port 4

⬆ Less

The screenshot shows the Google Cloud Platform console interface. On the left sidebar, the 'Compute Engine' section is expanded, and 'VM instances' is selected. The main panel displays the 'Serial port 1' console output for a VM instance. The output shows the boot process of a Debian-based system, including kernel boot messages, hardware detection (CPU, memory, disk), and the GRUB bootloader. The system is identified as 'srdqualys-scanner-vm' and is running kernel '4.19.0-1000-000'. The console output is truncated with a '...' in the middle, indicating more logs are available.

In Google Compute Engine (GCE), you can also check VM status graphs for instance resources such as CPU Utilization, Disk IO and Network status:



From the Qualys Cloud Platform UI, you can check the activation status of your Qualys Virtual Scanner Appliance. Click **Check Activation** in the **Add New Virtual Scanner** dialog from where you copied the personalization code.

Learn more about [Generating a Personalization Code](#).

Add New Virtual Scanner

Activate Your Virtual Scanner

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

Virtual Scanner Name

qualys-scanner

Personalization Code

\*\*\*\*\*900

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

Enter your personalization code

Enter your personalization code

VMScanner - VMScanner Workstation

QUALYS

Personalization in progress

Update in progress 100%

Personalize this scanner > Enter personalization code: \*\*\*\*\*900 > Download VMScanner\_AGENT\_3.0.0-1.085\_2019.msi

Set up network LAN2 >

Change network interface >

Disable firewall >

Restart network config >

System shutdown >

System reboot >

Version info: 3.12.27.5.11.0



Exit this menu >

Check Activation



Indicators of Scanner Appliance Statuses


You can check the status of the virtual scanner appliance in the Qualys Cloud Platform UI. Go to Scans > Appliances and search for your appliance in the list. It can take several minutes for the Qualys user interface to get updated after you add a new appliance. Refresh your browser periodically to ensure that you see the most up-to-date details.

The following table lists the various indicators and the respective appliance status that they denote:

| Indicator   | Meaning   |
|---|---|
|  | The appliance is connected to Qualys Cloud Platform and is ready to perform scans.  |
|  | The appliance is not connected to Qualys Cloud Platform and it's not ready to perform scans. Check to be sure your appliance is properly configured and can access Qualys Cloud Platform. |

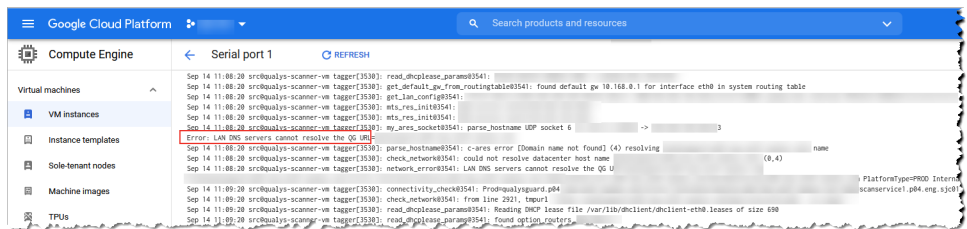
31

| Indicator   | Meaning   |
|---|---|
|  | The scanner is currently busy with a scan job. See preview pane for available capacity. |
|  | The scanner is not busy with any scan job.  |

After you see the  indicator, start your internal scans. After this, you'll see the busy icon is grayed out until you launch a scan using this scanner.

### Diagnosing Common Errors in Scanner Deployment

Check for errors in the output in the Serial Port 1 (console).



If you find issues with the personalization code, shut down the VM, fix the Metadata PERSCODE value and start the VM again. If the problem persists and the appliances are not communicating with Qualys Cloud Platform, contact [Qualys Support](#). Include your Qualys portal URL, username and attach the serial output logs to the support ticket.

For more information about the errors and the troubleshooting tips related to Qualys Virtual Scanner Appliance, see [Scanner Appliance Troubleshooting and FAQs](#).

You can install Qualys Cloud Agents (Windows and Linux) for GCP VM Instances via seamless integration of Qualys Cloud Agent solution in GCP Marketplace. This integration is a Bring Your Own License (BYOL) where only Qualys customers can use it as it requires them to use Cloud Agent Customer ID and Activation ID to configure the integration.

### Deploying Qualys Cloud Agent from Google Cloud Console

Using this solution, you can configure deployment of the Qualys Cloud Agent on specified compute instances on Google Cloud Platform. Using the Cloud Agent, you can activate multiple applications on the Qualys Cloud Platform (for example, Vulnerability Management, Policy Compliance, File Integrity Monitoring) as supported for each operating system. Additionally, you can integrate these Qualys security findings (like Vulnerabilities) directly into GCP by leveraging the Qualys Integration with Google Cloud Security Command Center, which pushes these findings in Google Security Command Center.



## Prerequisites For Deploying Cloud Agent From Google Cloud Console

You must have an active Qualys subscription. To buy a subscription, contact [Support](#) or [Sign up](#) from the Qualys website.

Ensure that you have the **Cloud Agent** module available and enabled in your subscription. The appropriate Customer ID and Activation ID are required to configure the installation.

Application modules such as Vulnerability Management, Policy Compliance, File Integrity Monitoring, among others, must be available and enabled.

Enable the following APIs from the Google Cloud Platform:

[Cloud OS Conf API](#)

[Compute Engine API](#)

And then, [install the OS Configuration agent](#) on your virtual machine. To know more, check the documentation for [Deploying Security Software Agents from Google Cloud Marketplace and Enabling an API](#). You can enable the OS Config and Compute APIs also by using gcloud commands through Google Cloud SDK shell.

Enable the OSConfig Agent in your project metadata. To enable this, use either of the following gcloud commands:

```
"gcloud compute project-info add-metadata --metadata=enable-osconfig=true"
```

```
"gcloud compute project-info add-metadata --metadata=enable-osconfig=true,enable-os-inventory=true,enable-guest-attributes=true,os-package-enabled=true,enable-os-config-debug=true,os-debug-enabled=true".
```

You can enable the OSConfig Agent also by using Google cloud console: [Compute Engine Metadata through GCP console](#). Setting metadata values enables OS inventory management, OS patch management and OS Configuration management, which is a prerequisite for this solution as this integration works on Google's OS configuration management feature.

Ensure that you have the following IAM permissions. If you don't, create a custom role including the following permissions. To know more, see [Creating and managing custom roles](#).

- osconfig.guestPolicies.create
- osconfig.guestPolicies.delete
- osconfig.guestPolicies.get
- osconfig.guestPolicies.list
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.objects.delete

Make sure that all the VM instances that you include in the deployment process have outbound connectivity to reach Qualys Cloud Platform. Check out the [GCP support page](#) to learn more.

## Getting Started with the Deployment

To start with, subscribe and configure Qualys Cloud Agent solution available on the GCP Marketplace to quickly deploy and install agents on multiple Google VM Instances with no software to maintain.

The configuration workflow follows a two-step process:

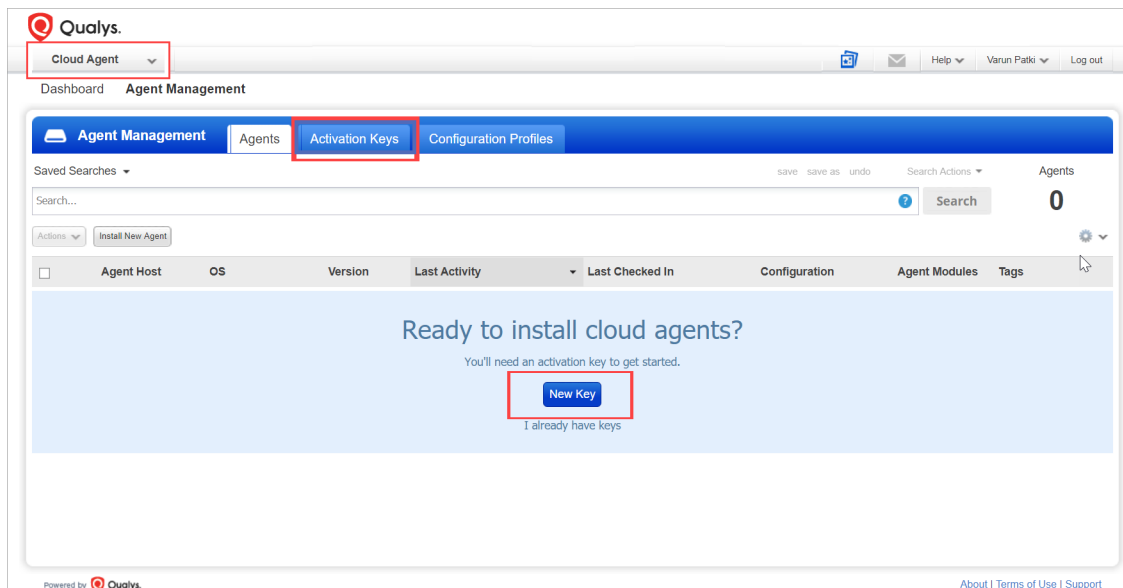
1. [Retrieving Customer ID, Activation ID and Platform Information from Qualys Subscription](#)
2. [Configuring Qualys Cloud Agent solution on GCP Console](#)

## Retrieving Customer ID, Activation ID and Platform Information from Qualys Subscription

The Qualys Customer ID, Activation Id, and platform information are the required fields for configuring a Qualys Cloud Agent solution available on Google Cloud Console.

Follow the steps to retrieve Qualys Customer ID and Activation ID:

1. Log in to your Qualys subscription. Navigate to "Cloud Agent" application module from the module picker in the left, and then click the **Activation Keys** tab.



2. Click **New Key** and generate an activation key. Specify a unique name to identify the key (for example, GCP Cloud Agent) and select Vulnerability Management and/or other cloud-agent-supported modules depending on your licenses.

**New Activation Key** Turn help tips: On | Off

Create a new activation key

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

Title:  [Select](#) [Create](#)

(no tags selected)

Provision Key for these applications

|  |  |
|--|--|
| <input type="checkbox"/> <b>GAV</b> Global Asset View<br>Activations managed by GAV            | <input type="checkbox"/> <b>PM</b> Patch Management<br>0 Activations Remaining                 |
| <input type="checkbox"/> <b>VM</b> Vulnerability Management<br>9997 Activations Remaining      | <input type="checkbox"/> <b>PC</b> Policy Compliance<br>97 Activations Remaining               |
| <input type="checkbox"/> <b>EDR</b> Endpoint Detection and Response<br>2 Activations Remaining | <input type="checkbox"/> <b>FIM</b> File Integrity Monitoring<br>9999999 Activations Remaining |
| <input type="checkbox"/> <b>SCA</b> Secure Config Assessment<br>9999 Activations Remaining     |  |

Select the Network

[Set limits](#)

[Close](#) [Generate](#)

We recommend that you create a Tag for GCP key and use that tag to be dynamically associated with the assets identified via the key.

You will get an acknowledgment as **New activation key generated successfully** with the Activation Key.

**New Activation Key** Turn help tips: On | Off

New activation key generated successfully

Give your key a name and add tags to easily find agents installed using this key. We'll associate the tags to the agent hosts.

Activation Key:  [Install instructions](#)

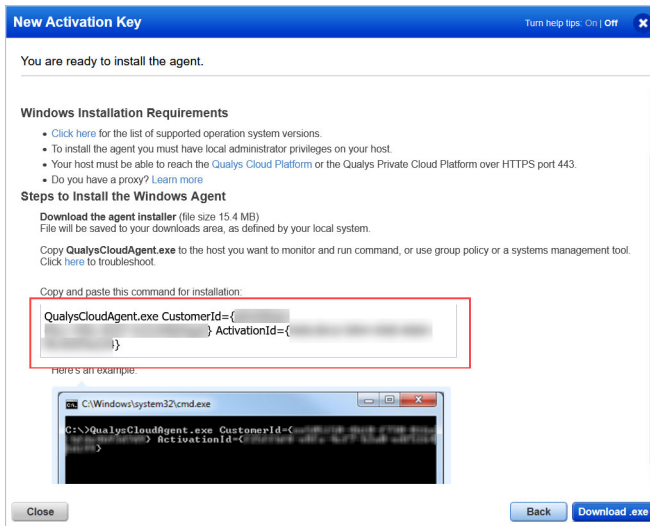
Key Type: ☒ Unlimited key

Installation Requirements

|                |           |  |                                      |
|----------------|-----------|--|--------------------------------------|
| Windows (.exe) | x86-32/64 | Microsoft Windows Client<br>Microsoft Windows Server   | <a href="#">Install instructions</a> |
| Linux (.rpm)   | x64       | Red Hat Enterprise Linux<br>CentOS<br>Fedora<br>OpenSUSE<br>SUSE Enterprise Linux<br>Amazon Linux<br>Oracle Enterprise Linux | <a href="#">Install instructions</a> |
| Linux (.rpm)   | ARM64     | Red Hat Enterprise Linux<br>CentOS<br>Amazon Linux   | <a href="#">Install instructions</a> |
| Linux (.deb)   | x64       | Debian<br>Ubuntu   | <a href="#">Install instructions</a> |
| Linux (.deb)   | ARM64     | Debian<br>Ubuntu   | <a href="#">Install instructions</a> |

[Close](#)

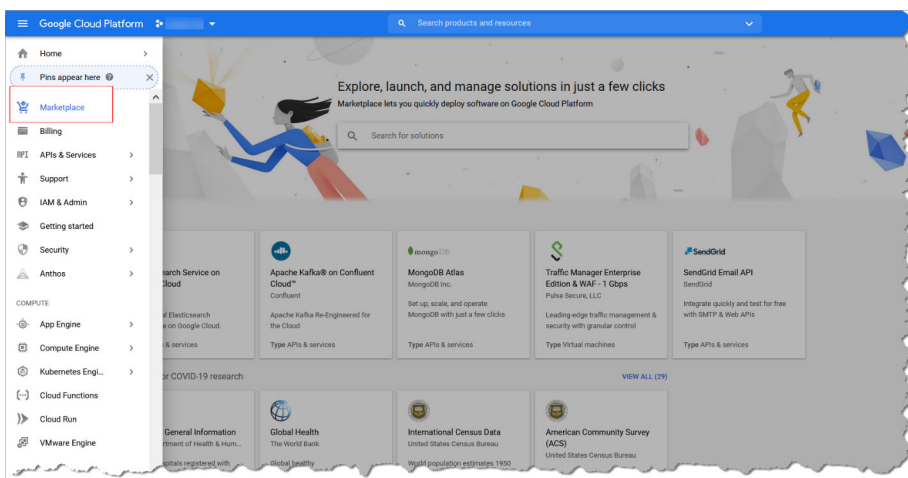
3. Currently, this integrated deployment supports only Windows and Linux agents . In the **Installation Requirements** section, click **Install Instructions** within Windows or Linux to retrieve your **Customer ID** and the **Activation ID**.



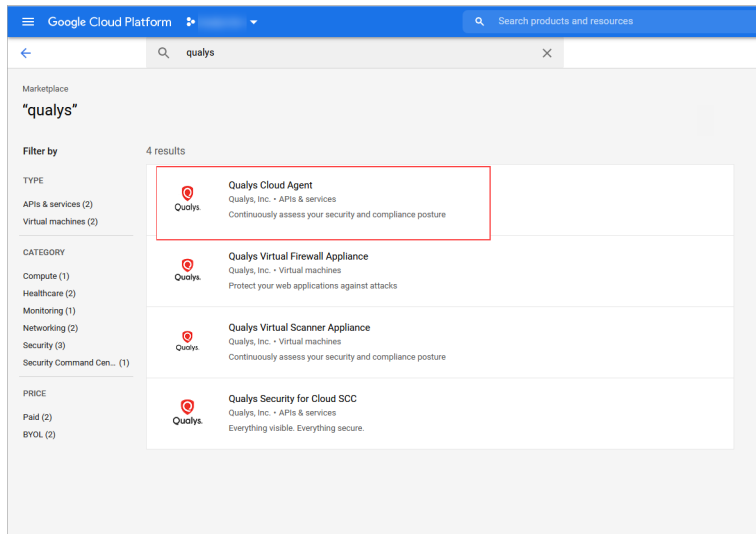
## Configuring Qualys Cloud Agent solution on GCP Console

The Qualys-GCP integration leverages telemetry from the Qualys cloud agent and security findings from other Qualys apps including Vulnerability Management, Policy Compliance, FIM, IOC, Patch Management and Global Asset IT Inventory. To configure the Qualys Cloud Agent solution available in the GCP Marketplace, follow the process as mentioned below. Ensure you have completed the [Prerequisites For Deploying Cloud Agent From Google Cloud Console](#) before proceeding with the following process.

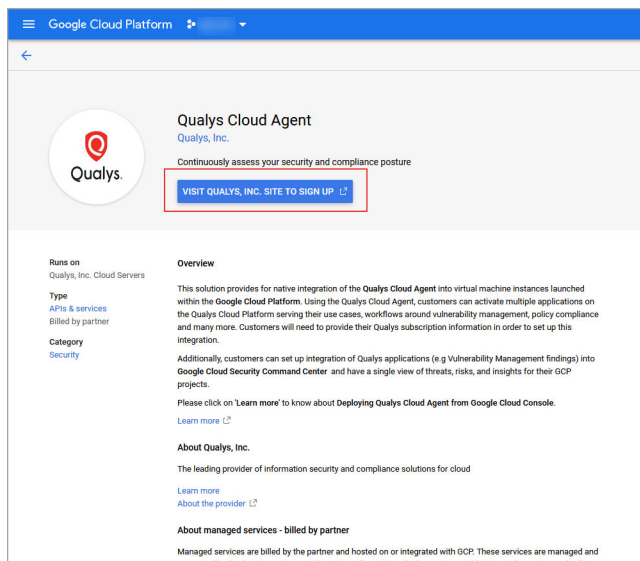
1. Go to GCP Marketplace and search for **Qualys**.



2. Click **Qualys Cloud Agent**. Another sign-up page is displayed.

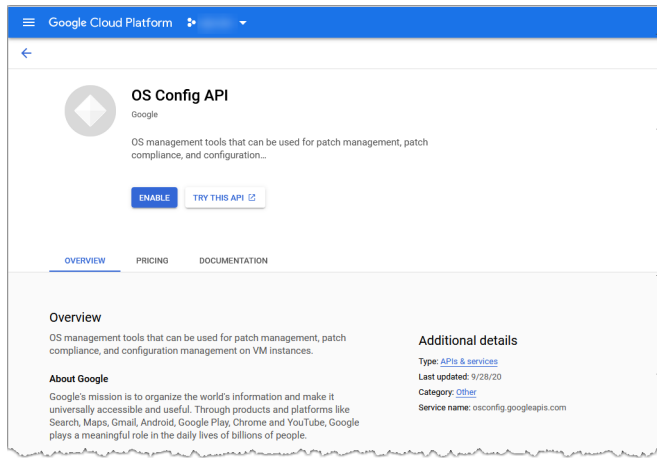


3. Click **VISIT QUALYS, INC. SITE TO SIGN UP**.

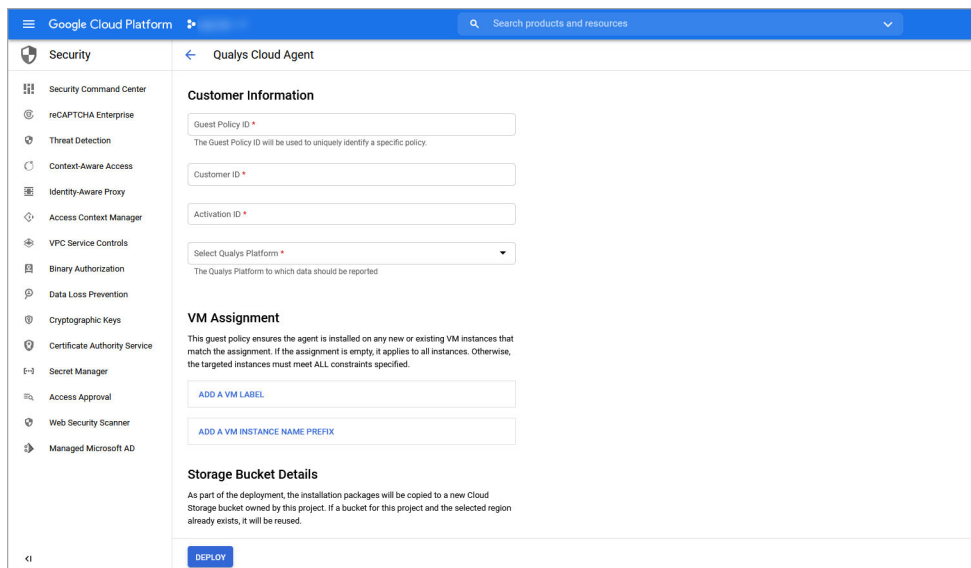


4. If you have already enabled **Cloud OS Config API**, you are redirected to the main configuration page.

5. If you haven't enabled the OS Config API, you are redirected to the **Cloud OS Config API** library page on the GCP console. To enable the OS Config API, click '**ENABLE**.' Also, make sure, you [install the OS Configuration Agent](#) as mentioned in the prerequisites.



You are redirected to the main **Qualys Cloud Agent** configuration page.



6. Specify an appropriate name as **Guest Policy ID**. For example, **qualys-demo**. Guest policy ID is used to uniquely identify a specific policy.

**Note:** Guest Policy ID must contain only lowercase letters, numbers and dashes.

Guest policies are created automatically.

7. Enter the **Customer ID** and the **Activation ID** retrieved from the Qualys portal.
8. From the Select Qualys Platform list, select the desired platform to which the data must be reported. Click [What's your Qualys Platform?](#) to verify your Qualys platform.
9. Select **VM Assignment**. By selecting this, the guest policy gets updated and ensures that the agent is installed on any new or existing VM instances that match the assignment. If no assignments are added, it applies to all instances. Here, you can add a label for VM instances or a VM Instance name prefix. To add a VM label, click **ADD A VM LABEL** and to add a VM Instance name prefix, click **ADD A VM INSTANCE NAME PREFIX**. After the assignment is configured, the guest policy ensures that Qualys cloud agent is installed on all those VM instances with specified labels or name prefix.
10. Select the region for the Cloud storage bucket in the **Storage Bucket Details** section and click **DEPLOY**. This deploys the Qualys cloud agent on the VM instances that match the VM assignment. A cloud storage bucket is automatically created in your project. This bucket is created to reduce the load on original source of installers. The storage buckets that are created as a part of this configuration, are synced with the original source of installers. The installers are copied automatically into this storage bucket from original source so that they are available to all the VM instances within the project. Only one storage bucket is created in the specified region (the regional parameter is a legal requirement to satisfy regulations on data localization) and can be reused to launch subsequent deployments.

## Storage Bucket Details

As part of the deployment, the installation packages will be copied to a new Cloud Storage bucket owned by this project. If a bucket for this project and the selected region already exists, it will be reused.

[Learn more about bucket regions](#) 

Select region for the Cloud Storage bucket \*

us

The created Cloud Storage bucket will have a name of the form: **security-agents-us-\***

This completes the Qualys Cloud Agent deployment and configuration procedure.

# Scanning Assets


This section helps you understand the steps to scan your network. Before you initiate your scan, you must ensure the following check points or configurations in your setup:

## GCP Scan Checklist

We recommend these steps before scanning.

- [Check Appliance Status](#)
- [Configure OS Authentication](#)

## Check Appliance Status

Qualys VMMDR or Policy Compliance subscription, go to **Scans > Appliances** - Be sure the new Scanner Appliance is connected to the Qualys Cloud Platform. The  icon means your appliance is connected and ready for scanning.

## Tips and Best Practices

### Has Qualys Defined Networks? Move your Virtual Scanner 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 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.

## 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. In your Qualys VMMDR subscription, go to **Scans > Option Profiles**. Edit the **Initial Options** profile, click **Save As** to save a copy with another name. In your new profile, on the **Scan** tab, enable the authentication types that you need.

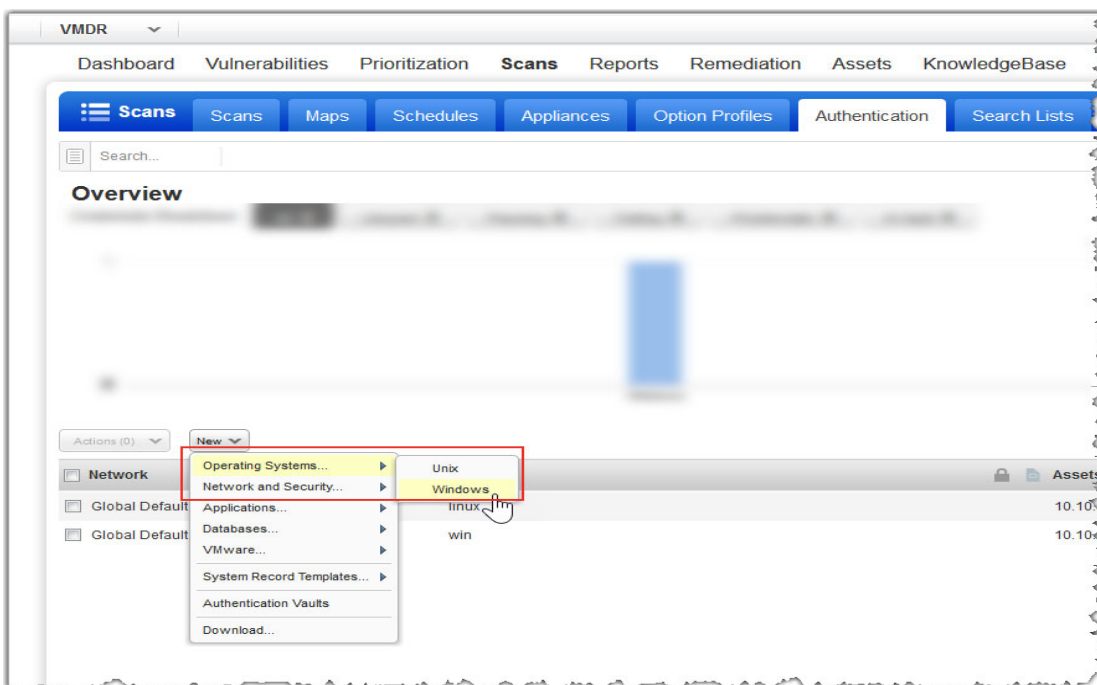


### Authentication

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

- ☒ Windows
- ☒ Unix/Cisco
- ☐ Oracle
- ☐ Oracle Listener
- ☐ SNMP
- ☐ VMware
- ☐ DB2
- ☐ HTTP
- ☐ MySQL
- ☐ Tomcat Server
- ☐ MongoDB
- ☐ Palo Alto Networks Firewall
- ☐ Oracle WebLogic Server
- ☐ Jboss Server
- ☐ Sybase

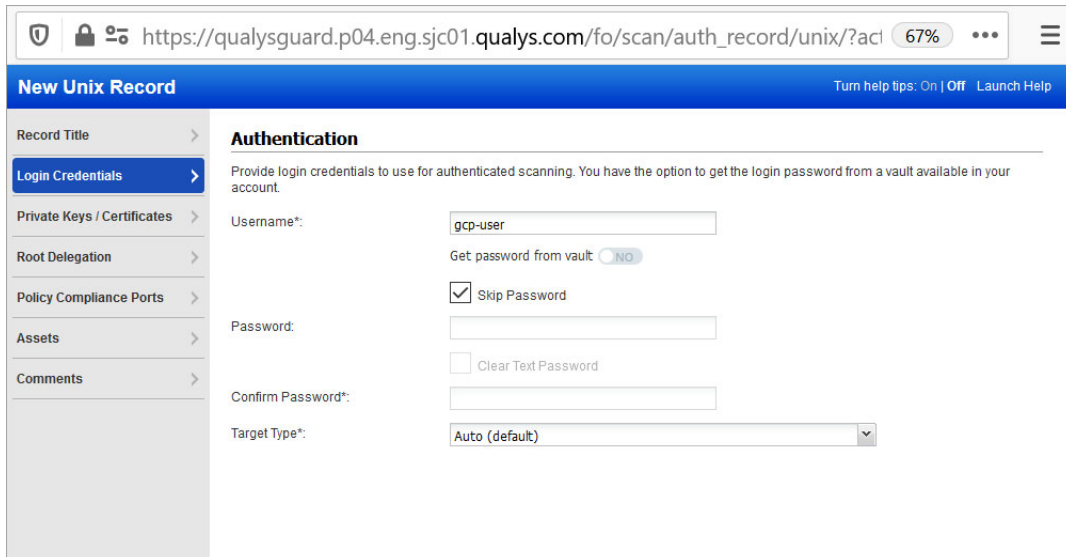
In VMDR, go to **Scans > Authentication**. Add OS authentication records for the GCP instances that you'll be scanning - Unix and/or Windows. In the record, add credentials for the account to be used for authentication - this is an account for OS user (not the AIM user). We recommend you create a dedicated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



The following are the sample UNIX and Windows records for your reference:

### Sample UNIX Record

1. In the **New Unix Record wizard**, on the **Record Title** screen, give a name to your record and select the network.
2. On the **Login Credentials** screen, provide the username, select **Skip Password**, and select the target type.



The screenshot shows the 'New Unix Record' wizard in the Qualys interface. The browser address bar shows the URL: [https://qualysguard.p04.eng.sjc01.qualys.com/fo/scan/auth\\_record/unix/?act](https://qualysguard.p04.eng.sjc01.qualys.com/fo/scan/auth_record/unix/?act). The page has a blue header with 'New Unix Record' and 'Turn help tips: On | Off Launch Help'. A left sidebar contains a list of steps: 'Record Title', 'Login Credentials' (selected), 'Private Keys / Certificates', 'Root Delegation', 'Policy Compliance Ports', 'Assets', and 'Comments'. The main content area is titled 'Authentication' and contains the following fields: 'Username\*' with the value 'gcp-user', 'Get password from vault' with a 'NO' toggle, a checked 'Skip Password' checkbox, an empty 'Password\*' field, an unchecked 'Clear Text Password' checkbox, an empty 'Confirm Password\*' field, and 'Target Type\*' with a dropdown menu set to 'Auto (default)'.

3. On the **Private Keys/ Certificates** screen, click **Add Private Key/Certificate** and then in the **Private Key / Certificate** dialog box, select the key type (RSA, DSA, ECDSA, ED25519) and enter your private key content.



The screenshot shows the 'Private Key / Certificate' dialog box. The title bar is blue with the text 'Private Key / Certificate' and a close button. The main content area is titled 'Set private key / certificate for your Unix record'. It contains the following fields: 'Get private key from vault' with a 'NO' toggle, 'Private Key Type' with a dropdown menu set to 'RSA', and 'Private Key Content' with a large text area. The text area contains the text '\*\*\*\*\*Private Key Installed\*\*\*\*\*'. At the bottom, there is a 'Close' button and a 'Save' button. A small note at the bottom of the text area says: 'Paste the private-key content into the space provided. See [Help](#) for more details'.

4. On the **Assets** screen, enter the Unix IP addresses or ranges of your GCP virtual machines for this record. Credentials in this record are used to scan these assets.

**New Unix Record** Turn help tips: On | Off Launch Help

**Record Title** > **Assets**

**Login Credentials** > Select the asset type for creating authentication record.

**Private Keys / Certificates** > Asset Type: ☒ IPs/Ranges ☐ IP Range in Tag Rule ☐ Asset Tags

**Root Delegation** > Select IP addresses/ranges to include in this record.

**Policy Compliance Ports** > Enter or Select IPs/Ranges: Select IPs/Ranges | Select Asset Group | Remove | Clear

**Assets** > 10.97.15.117

**Comments** >

☐ Display each IP/Range on new line

Cancel Create

## Sample Windows Record

1. In the **New Windows Record** wizard, on the **Record Title** screen, give a name to your record and select the network.

2. On the **Login Credentials** screen, enter the username and password.

**New Windows Record** Launch Help

Record Title > **Login Credentials**

**Login Credentials** >

Assets >

Comments >

---

**Windows Authentication**

☒ Local

☐ Domain

**Login**

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

☒ Basic authentication ☐ Authentication Vault

User Name: \*

Password:

Confirm Password:

**Choose Authentication Protocols**

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

☒ NTLMv2

☐ NTLMv1

**SMB**

☐ SMB signing required

Minimum SMB version:

3. On the **Assets** screen, enter the Windows IP addresses or ranges of your GCP virtual machines for this record. Credentials in this record are 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 \(pdf\)](#)

## Internal Scanning using Virtual Scanning Appliance

Scanning with virtual scanner appliance involves the following sequence of steps:

1. Based on your requirements, create a dynamic tag with Cloud Asset Search filters under the Qualys AssetView module.

For example: All running VM instances in your Qualys Subscription:

**gcp.compute.state:"RUNNING"**

All running VM instances in your GCP Project: **gcp.compute.projectId:<your GCP Project ID> and gcp.compute.state:"RUNNING"**

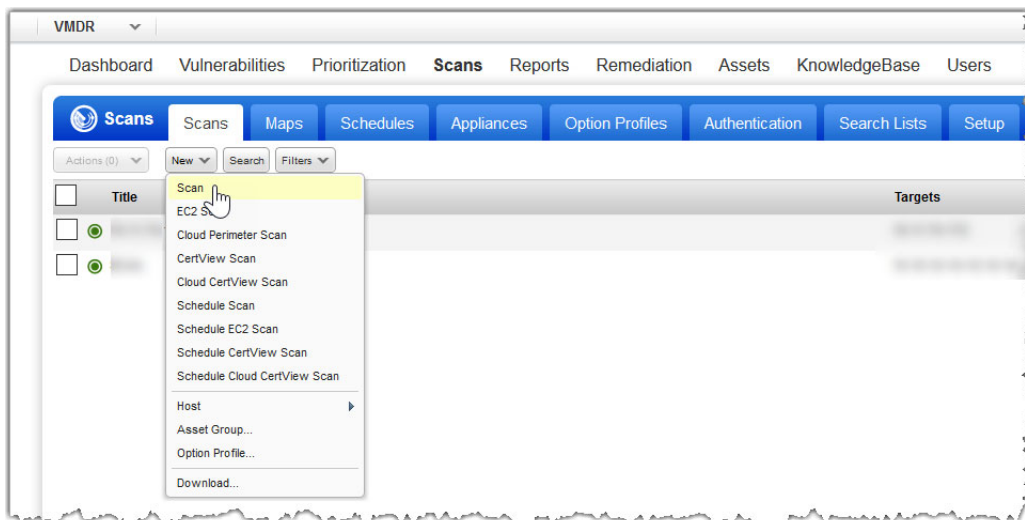
All running VM Instances in US East 1 zone: **gcp.compute.state:"RUNNING" and gcp.compute.zone: us-east1-b**

2. Extract IP addresses of machines returned by tags created in step 1. You can extract it by using Download or API Query to Host Assets.

3. Add these IP addresses grouped as Asset Groups or individually as Host Assets under Assets tab in VM or VMDR.

4. Configure OS Authentication.

5. Now, let's start scanning. Go to VM or VMDR > **Scans > Scans > New > Scan** (or **Schedule Scan**).



6. Identify your scan target. Click **Assets** to select a combination of asset groups and IP addresses to scan or click **Tags** to select one or more asset tags to scan.

**Launch Vulnerability Scan** Turn help tips On | Off

---

**General Information**

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

Title:

Option Profile: \*  [Select](#)

Processing Priority:

Network:

Scanner Appliance:  [View](#)

---

**Choose Target Hosts from**

Tell us which hosts (IP addresses) you want to scan.

☒ Assets ☐ Tags

Asset Groups:  [Select](#)

IPs/Ranges:  [Select](#)

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

Exclude IPs/Ranges:  [Select](#)

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

☐ Temporarily add agent addresses  
Select this option to add the IP addresses of any agents in your target when those IPs are not already in your subscription. They'll be added for this scan only

---

**Notification**

☐ Send notification when this scan is finished

7. Click **Launch**, and you're done!

## Internal Network Scanning by using Qualys Cloud Agent

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

### Cloud Agent features

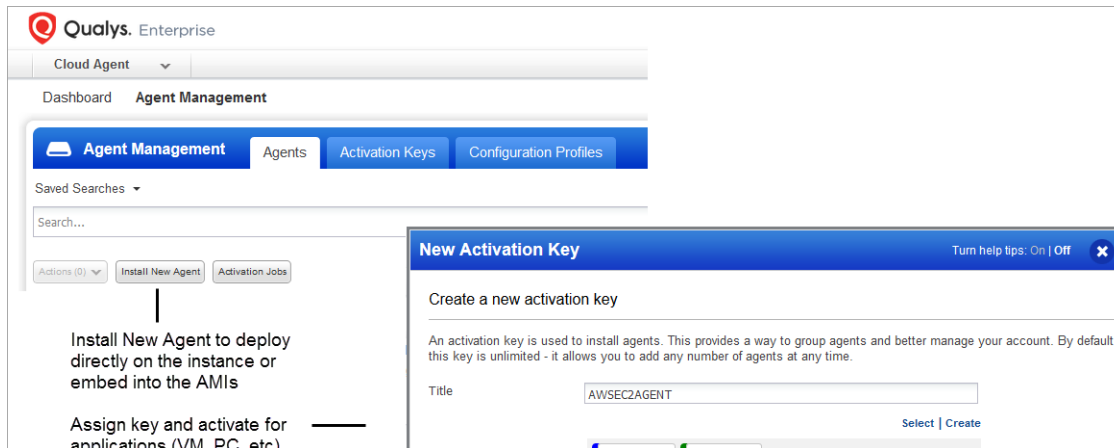
- Communicates to the Qualys Cloud Platform over port 443 and supports Proxy configurations.
- Deployable directly on the GCP VM instances or embed in the workload images. Works well for cloud burst and ephemeral instances
- Supports scanning a range of Linux and Windows OS versions
- Supports scanning GCP instance OS vulnerabilities

For more information on Qualys Cloud Platform and Qualys Cloud Agent, we recommend the following resources:

- [Qualys Cloud Platform](#)
- [Qualys Cloud Agent Getting Started Guide](#)

## Get Started

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



## External Scanning using External Scanner Appliance

We provide the ability to scan public-facing virtual machines in your GCP cloud environment. You must use the standard scan workflow to scan your public-facing GCP VM instances. Create a tag for your GCP instances having a publicly assigned IP, specify IPs to be used in an standard scan workflow, select the external scanners in the scan setup and launch the scan. Also ensure that you those external IPs are activated in your Qualys subscription.

Qualys External Scanners (Internet Remote Scanners) located at the Qualys Cloud Platform are used for external scanning of GCP VM instances. For subscriptions on Private Cloud Platforms, your account may be configured to allow internal scanners to be used.

## Get Started

You can run an external scan immediately or All cloud perimeter scans are scheduled - either for "now" (a one-time scan job) or "recurring". After saved, you see the scan job on the Schedules list. When the scan job starts, it appears on your Scans list.

1. Based on your requirements, create a dynamic tag with Cloud Asset Search filters under "AssetView" app.

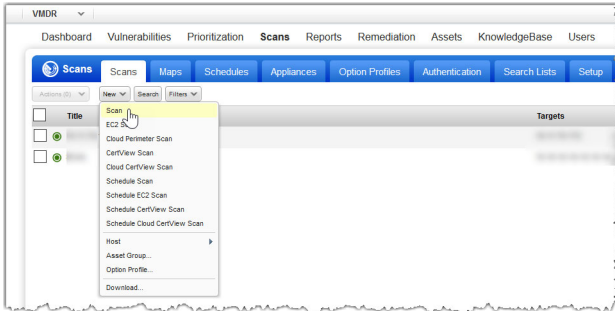
For example,

All running public VM instances in your Qualys Subscription: **not gcp.compute.publicIpAddress is null and gcp.compute.state:"RUNNING"**

All running public VM instances in your GCP Project: **not gcp.compute.publicIpAddress is null and gcp.compute.projectId: and gcp.compute.state:"RUNNING"**

All running public VM instances in a zone: **not gcp.compute.publicIpAddress is null and gcp.compute.state:"RUNNING" and gcp.compute.zone:westus**

2. Extract IP addresses of machines returned by tags created in step 1. You can extract it by using Download or API Query to Host Assets.
3. Add these IP addresses grouped as Asset Groups or individually as host assets under the Assets tab in VM or VMDR.
4. Configure OS Authentication.
5. Now, let's start scanning. Go to VM or VMDR > **Scans** > **Scans** > **New** > **Scan** (or **Schedule Scan**).



6. In the Launch Vulnerability Scan window, provide the required details like scan title, option profile, and network, among others. Select the **External** scanner appliance type from the dropdown list.
7. Identify your scan targets. You can either add the exported list of IPs to an asset group or directly list the IP addresses to scan.
8. Click **Launch** and you're done!

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.

For more details on vulnerability scans, see [Scan for Vulnerabilities](#).

## Cloud Inventory and Security Assessment

This section describes the discovery of cloud inventory such as cloud assets and resources. It also describes the security assessment giving full visibility into the public cloud security posture of all assets and resources.

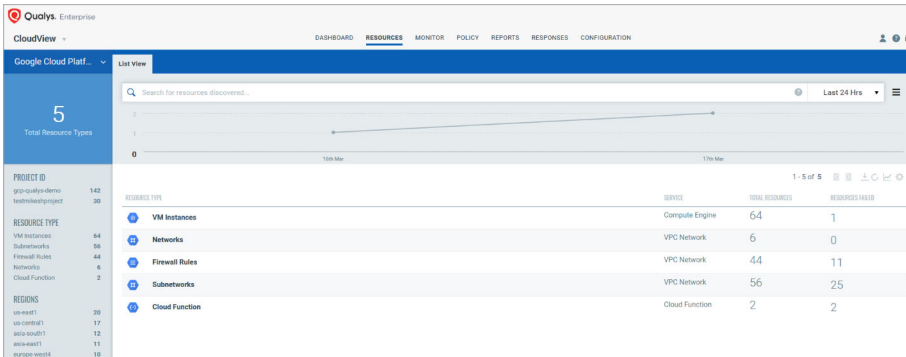
### Cloud Inventory

Qualys Cloud Inventory continuously discovers and tracks assets and resources such as VM Instances, Networks, Firewall Rules, Subnetworks, and Cloud Function across all regions and multiple projects in Google Cloud Platform and gives you an "at-a-glance" comprehensive picture of your cloud inventory and the location of assets across global regions. You can view all this information in one central place.



## Features

- Provides a quick overview of inventory via pre-built dashboards, and lets you personalize or build your own dashboard with custom widgets.
- Collects rich metadata for every resource and shows associations across resources, so you can understand scenarios such as which firewall rules are potentially public and unprotected, and which related assets this is impacting.



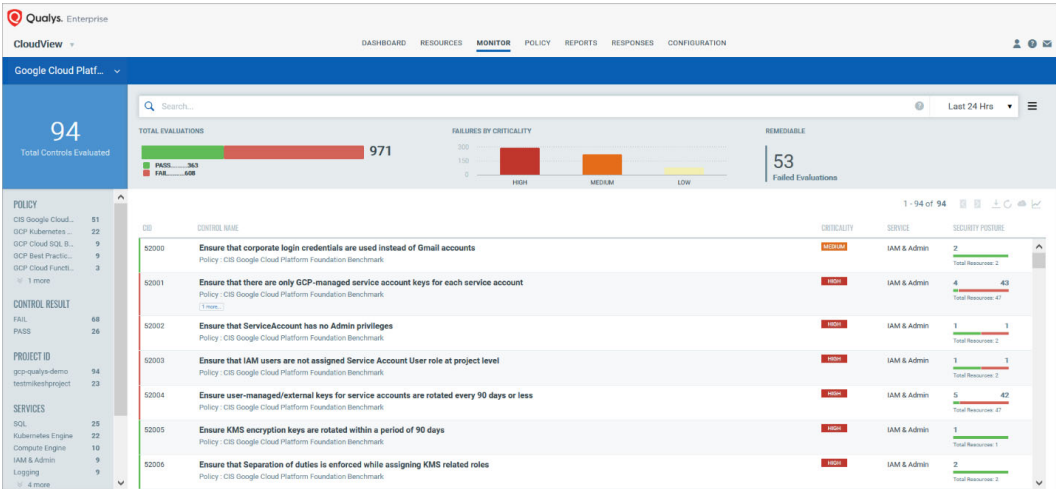
## Cloud Security Assessment

Qualys Cloud Security Assessment gives full visibility into the compliance posture of your cloud infrastructure against regional, industry, and government mandates by using reports and dashboards.

Refer to the [CloudView User Guide](#) for more details.

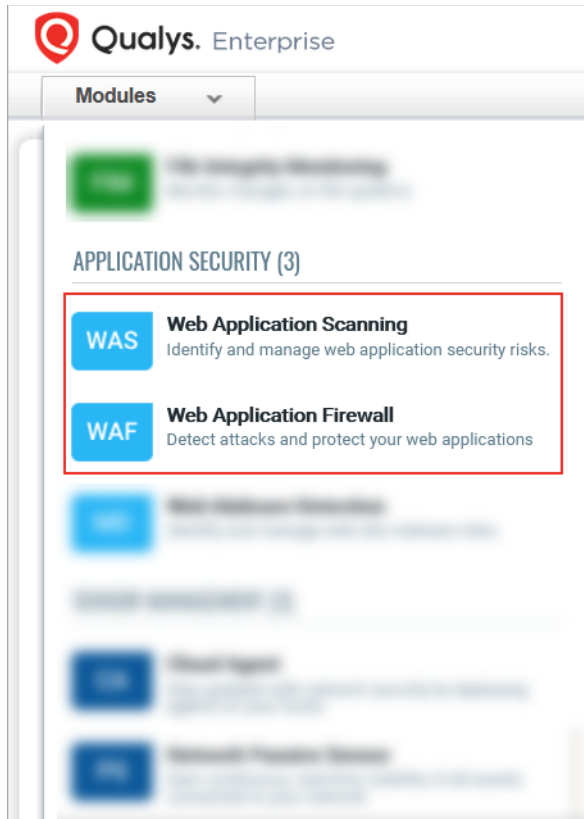
Features:

- Provides a quick overview of inventory and security posture via dashboards
- Lets you personalize or build your own with custom widgets based on queries or on other criteria, such as "Top 10 accounts based on failures" and "Top 10 controls that are failing"
- Out-of-box GCP policies like CIS Google Cloud Platform Foundation Benchmark and GCP Best Practices Policy
- Continuously assess and report on resource mis-configurations by checking against the controls from out-of-box policies
- Build your own policies and customize controls to suit your need
- Ability to view, filter, and export misconfigurations



## Securing Web Applications

You can secure your applications by using the Qualys Web Application Scanning and Web Application Firewall solutions.



### Qualys WAS

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

### How do i get started?

- Follow the steps in You can scan your Google Cloud Compute Engine instances along with all other global elastic cloud and on-premise assets from within the Qualys Cloud Platform. Qualys Virtual Scanner Appliance can be directly deployed from the Google Marketplace.
- Then review instructions in [Qualys Web Application Scanning Getting Started Guide](#).

## Qualys WAF

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

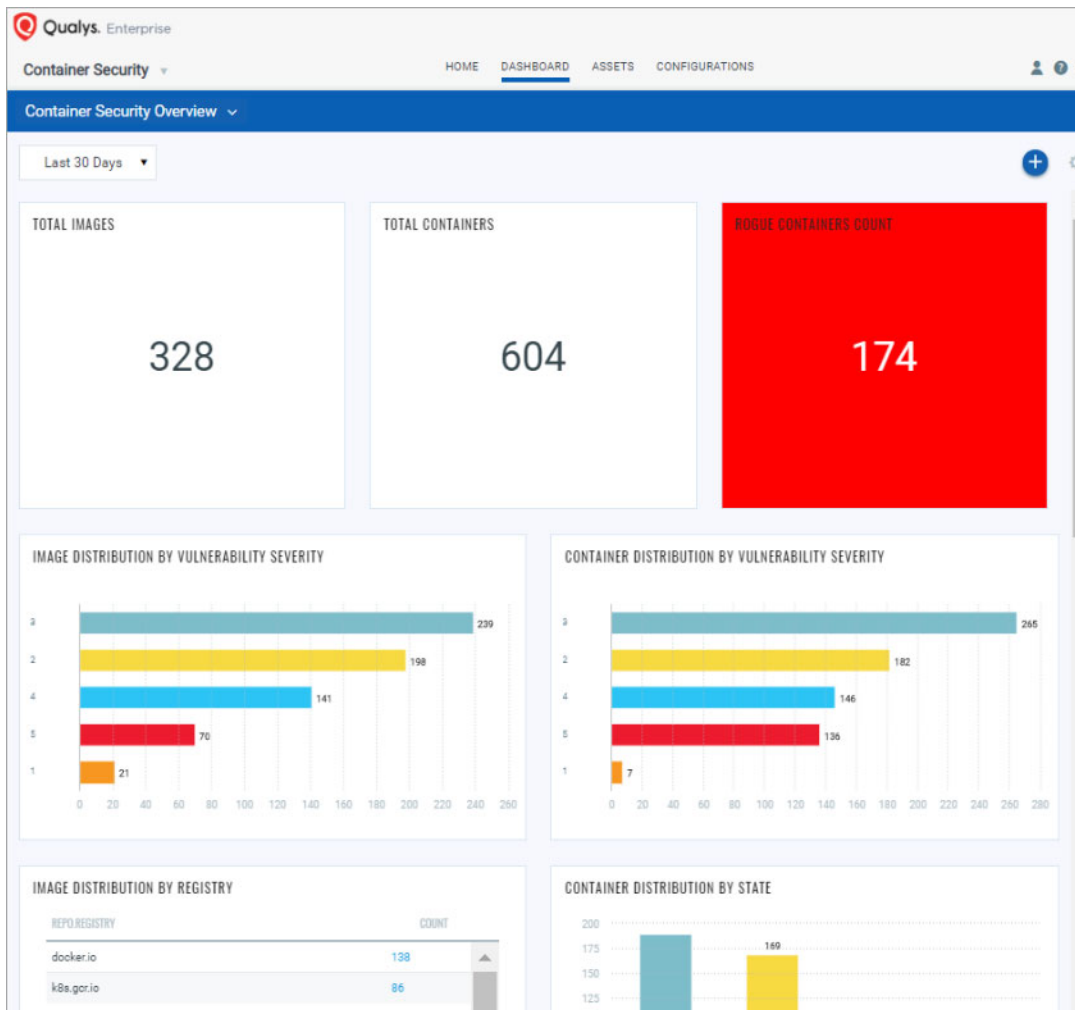
### How do i get started?

- Install the Web Application Firewall Appliance available on the GCP.
- Then review instructions in Qualys Web Application Firewall Getting Started Guide.

## Securing Containers

Qualys Container Security provides discovery, tracking and continuously protection to container environments. This addresses vulnerability management for images and containers in their DevOps pipeline and deployments across cloud and on-premise environments. Qualys Container Security supports:

- Discovery, inventory and near-real-time tracking of container environments
- Vulnerability analysis for images and containers
- Vulnerability analysis for registries
- Integration with CI/CD pipeline using Jenkins/Bamboo Plugins or REST APIs (DevOps flow)
- Support for GKE deployments
- Support for Google Container Registry (GCR) and Google Artifactory Registries



For more details, refer to the [Qualys Container Security User Guide](#).

## Deploying Container Sensor

The sensor from Qualys is designed for native support of Docker environments. Sensor is packaged and delivered as a Docker Image. Download the image and deploy it as a Container alongside with other application containers on the host. Since they are docker based, the sensor can be deployed into orchestration tool environments such as Kubernetes, Mesos or Docker Swarm just like any other application container.

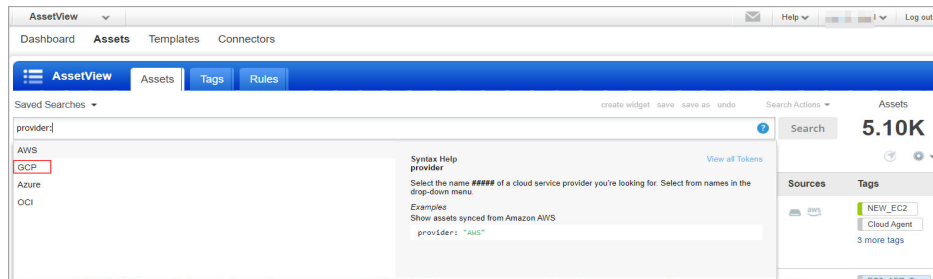
For more details, refer to the [Qualys Container Security Deployment Guide](#).

# Analysis, Reporting and Remediation

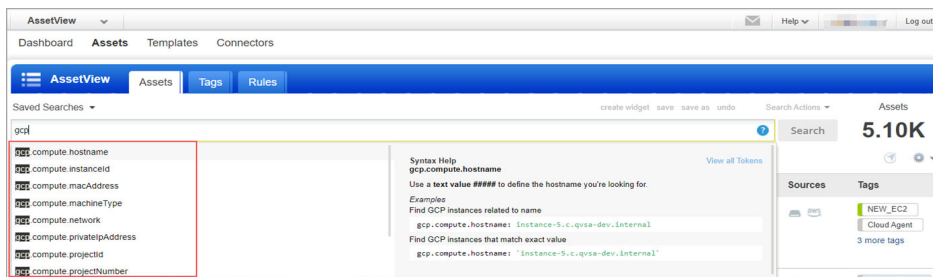
This section covers - how to query assets, build widgets and dashboards, and then how to generate vulnerability reports on GCP assets.

## Using Qualys Search Tokens

Our advanced search capabilities help you quickly find your asset data all in one place. In your Qualys subscription, in the module picker, choose the Qualys AssetView app and go to the Assets tab. This is where you see an inventory of all your scanned assets. Say you want to find all your GCP assets. Type provider and select GCP from the drop-down menu.

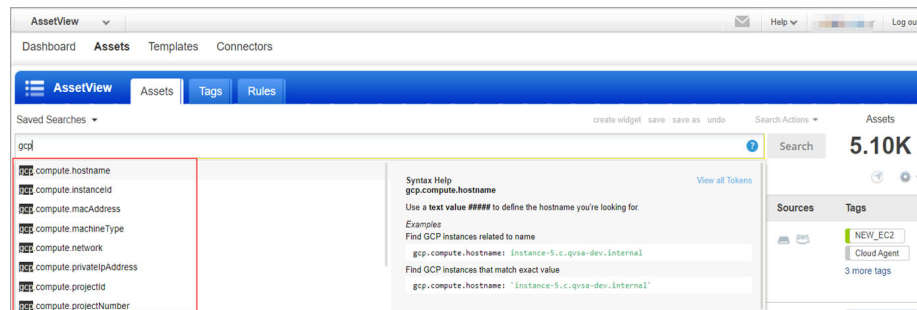


You can search many GCP asset properties. Start typing gcp and you see a list of GCP asset properties (tokens) that you can use to search. Hover over the token name and see the syntax help to the right.



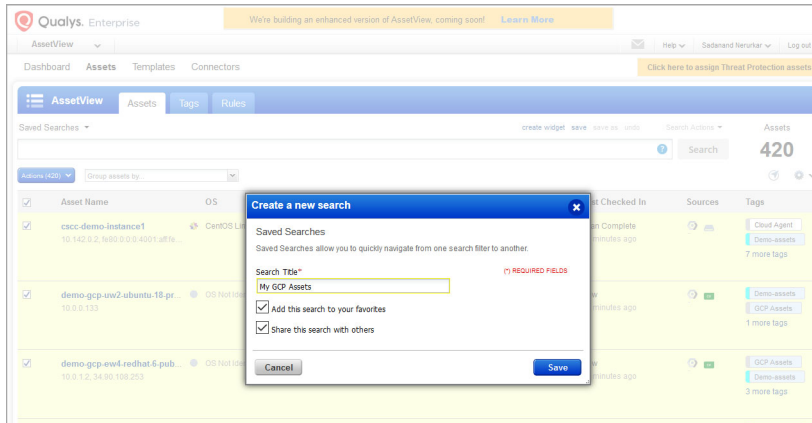
## Viewing Asset Details

The latest vulnerability and compliance data is always available in your assets inventory. Just select the asset and choose View Asset Details from the quick actions menu.



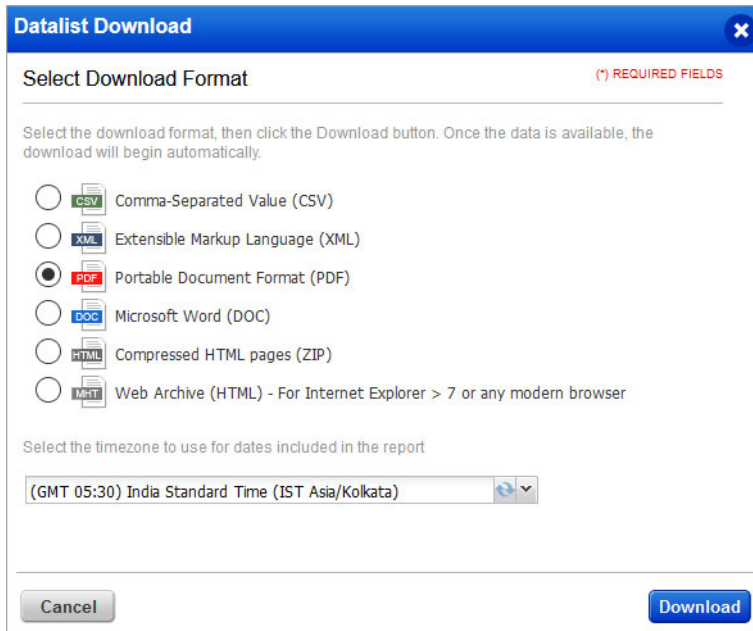
## Saving Search Query

Easily save your searches for reuse and share them with other users.



## Downloading and Exporting Results

It just takes a minute to export search results. Select Download from the Tools menu, choose an export format, and click Download - choose from multiple formats.



## Creating Widget

You can create a widget based on your query, and add it to your dashboard. For example, first search for GCP assets on which vulnerabilities were last found within past 30 days. Here's your query:

```
provider:"GCP" and vulnerabilities.lastFound>now-30d
```

Then choose Create widget. Give a title to your widget. Your query is populated for you. You can add this widget to your dashboard.

**Add a new widget to your dashboard**

Select data for your widget using the form below (1 REQUIRED FIELDS) Customize the way that your widget looks

01 Count Table Bars Pie

Widget Title\*  
GCP Vul within last month

Query  
provider:"GCP" and vulnerabilities.lastFound>now-30d

Categories\*\*  
tags.name

Sort by  
count

Sort direction\*  
Ascending

Limit to\*  
TOP 10

Filters  
Add one or more filters to narrow down your results for the selected group.  
Add filter

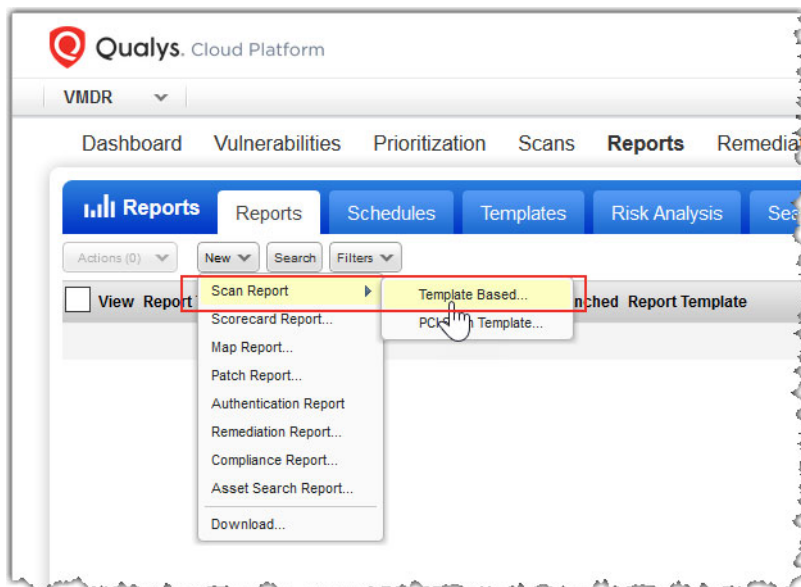
Extras  
☐ Show Legend ☒ Show Labels

Layout  
☒ Vertical Columns ☐ Horizontal Bars

Cancel Previous **Add to Dashboard**

## Creating Reports

You can create various reports on vulnerabilities in the Qualys VM module. Go to VM or VMMDR > Reports > New > Scan Report > Template Based. You can choose from the default report templates and customize them, or create your own. Try the Technical Report to see full vulnerability details in your report.





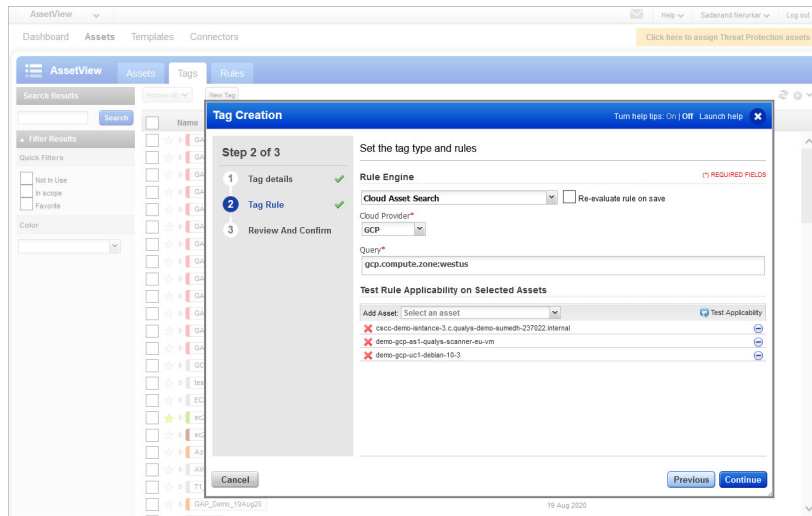
Want to report on compliance data? Choose PC from the module picker. Then go to Reports > New > Compliance Report, and pick the report you're interested in.

## Dynamic Tagging by Using GCP Metadata

Create dynamic tag rules to tag your GCP virtual machine instances based on GCP metadata as collected by the Qualys Cloud Agent and Qualys Virtual Scanner Appliance. For each tag rule, you must provide a search query with GCP instance information.

It's easy to get started!

- 1) Go to AssetView > **Assets > Tags > New Tag**.
- 2) Choose the Cloud Asset Search tag rule.
- 3) Select the cloud provider.
- 4) Enter your query. Start typing in the Query field and we'll show you the GCP attributes that you can search.



## Sample queries

Refer to the following sample queries:

Find GCP VM Instances located in US East 1 zone: **gcp.compute.zone:us-east1-b**

Find GCP instances that match exact value: **gcp.compute.hostname:`instance-5.c.qvsa-dev.internal`**

Find GCP VM instances within a specific GCP Project Id: **"gcp.compute.projectId:gcp-qualys-demo"**

Find GCP VM instances of specific machine type: **"gcp.compute.machineType:n1-standard-1"**

Find GCP VM instances based on IP address (comma-separated list or range):

**gcp.compute.privateIpAddress:10.128.15.234**

**gcp.compute.publicIpAddress:335.232.131.27**

Find GCP instances based on a GCP project number:

**gcp.compute.projectNumber:525006500856**

To know what metadata is collected by Qualys Cloud Agent and Qualys Virtual Scanner Appliance, see [GCP Metadata](#).

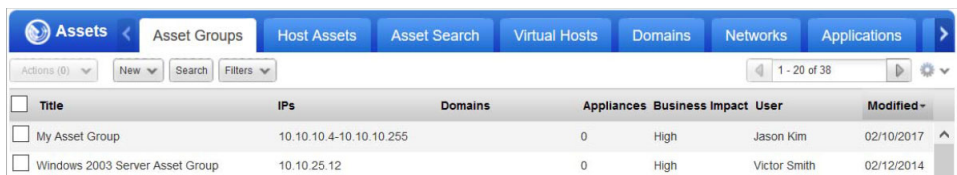


# Organizing Assets in Qualys Subscription

Here are some best practices and tips for organizing assets and thereby securing your GCP infrastructure by using Qualys applications.

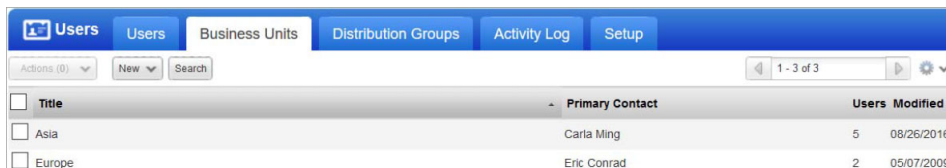
## Setting up Qualys Configurations

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



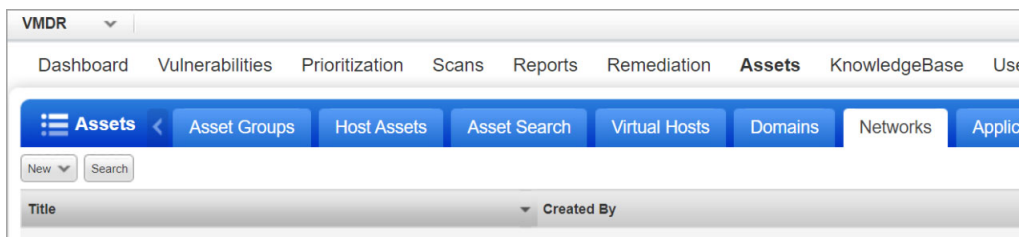
| Title                           | IPs                     | Domains | Appliances | Business Impact | User         | Modified   |
|---------------------------------|-------------------------|---------|------------|-----------------|--------------|------------|
| My Asset Group                  | 10.10.10.4-10.10.10.255 |         | 0          | High            | Jason Kim    | 02/10/2017 |
| Windows 2003 Server Asset Group | 10.10.25.12             |         | 0          | High            | Victor Smith | 02/12/2014 |

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



| Title  | Primary Contact | Users | Modified   |
|--------|-----------------|-------|------------|
| Asia   | Carla Ming      | 5     | 08/26/2016 |
| Europe | Eric Conrad     | 2     | 05/07/2009 |

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



| Title                            | Created By |
|----------------------------------|------------|
| Global Default Network (default) | System     |

**Removing Terminated Virtual Machines**- You can remove terminated virtual machines from your Qualys account. Go to VM/VMDR or Policy Compliance > Assets > Asset Search and select the assets with tracking method as IP address. You could also add more parameters to refine your search such as Last Scan Data not within the past <value> days and so on.

Qualys. Enterprise

Vulnerability Management

Help

Sadanand Nerurkar (quays2mg08)

Logout

Dashboard

Scans

Reports

Remediation

Assets

KnowledgeBase

Users

Assets

Asset Groups

Host Assets

Asset Search

Virtual Hosts

Domains

Networks

Applications

Ports/Services

DNS Hostname:

☐

beginning with

EC2 Instance ID:

☐

beginning with

Azure VM ID:

☐

beginning with

NetBIOS Hostname:

☐

beginning with

Tracking Method:

☐

IP address

EC2 Instance status:

☐

RUNNING

Azure VM state:

☐

STARTING

Operating System:

☐

beginning with

[View](#)

OS CPE:

☐

beginning with

Open Ports:

☐

Running Services:

☐

[Select](#)

QID:

☐

[Select](#)

☐

with results

beginning with

Last Scan Date:

☒

not within

the past

days

Last Scan Date (PC):

☐

within

the past

days

Last Scan Date (SCA):

☐

within

the past

days

Last Scan Date (SCAP):

☐

within

the past

days

First Found Date:

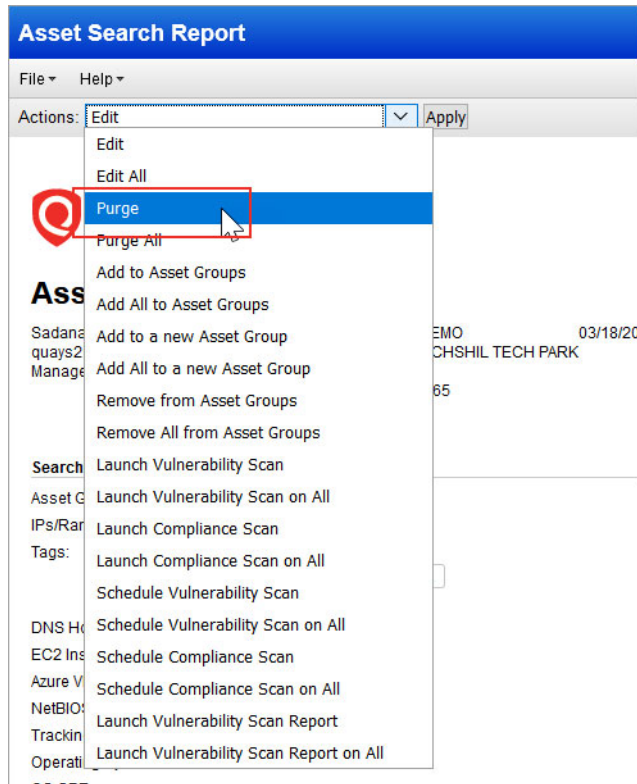
☐

within

the next

days

Click **Search** and then select the assets from the results. From the **Actions** drop-down, select **Purge**. This results in removal of assets along with their associated data from the module.



## Uninstalling Agents

Consider a scenario where you have deployed Qualys Cloud Agents on your GCP VM instances and you want to uninstall agents that haven't checked-in for the last N days, you can use the API call.

Sample API 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 the [Qualys Cloud Agent API User Guide](#).

## Frequently Asked Questions (FAQs)

| Queries  | Solutions   |
|--|---|
| Which organizations can leverage Qualys Integration with Google Cloud Security Command Center? | Only the organizations that already have an existing Qualys subscription that uses a Bring Your Own (Qualys) License can use this integration.  |
| Can I activate other Qualys modules for assets?  | <p>Yes, you can activate multiple applications on Qualys Cloud Platform including:</p> <ul style="list-style-type: none"><li>- Global AssetView/CyberSecurity Asset Management</li><li>- Vulnerability Management</li><li>- Endpoint Detection and Response (EDR)</li><li>- Secure Config Assessment</li><li>- Patch Management</li><li>- Policy Compliance</li><li>- File Integrity Monitoring</li></ul> <p>However, only Vulnerability Management security findings are available in the Security Command Center in Google Cloud, after you configure the Qualys Integration with Google Cloud Security Command Center.</p> |
| Which Operating Systems are supported by this integration?                                     | Qualys Integration supports Windows and Linux OS. For the complete list of supported Windows and Linux platforms, see the Cloud Agent Platform Availability Matrix for Windows and Linux in the <a href="#">Cloud Agent Getting Started Guide</a> .   |
| How are agent installer upgrades handled in this integration?                                  | Qualys updates agent installers in the original source which is available to customer-specific storage buckets that are created during the Qualys Cloud Agent configuration. Even though customer-specific buckets are synced with the original source, Qualys needs to inform Google for any upgrades or updates in the original source, for Google to trigger manual sync to update customer storage buckets with the updated Qualys installers.  |
| Does this integration and deployment model support proxy or Cloud Agent Gateway Service?       | Proxy configuration or Cloud Agent Gateway Service is not included as a part of this deployment model. However, proxy configuration can be set after the agent has been installed.  |
| Does this deployment model support a Qualys PCP?   | No, this deployment model only supports utilization of the Qualys Cloud Shared Platform.  |

For more details on this integration, see the [Qualys Integration with Google Cloud Security Command Center: Overview](#) section.