CloudView

User Guide

March 21, 2019

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

Table of Contents

About this Guide

Welcome to Qualys CloudView! We'll help you get acquainted with the Qualys solutions for securing your AWS resources using the Qualys Cloud Security Platform.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com

Qualys Support

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

CloudView Overview

Qualys CloudView provides visibility and continuous security across all of your cloud environments.

With CloudView you'll get these features:

- Discover and inventory assets and resources across all regions from multiple accounts and multiple cloud platforms

- Search resource metadata, view resource details and show associations across resources

- Out-of-box AWS and Azure policies

- Continuously assess and report on resource misconfigurations by checking against the controls from out-of-box policies

- Ability to view, filter and export misconfigurations.

Qualys Subscription and Modules required

Check that you have these modules available in your subscription:

- CloudView

- Vulnerability Management (only if you want to view host vulnerability information)

- AssetView

- Cloud Agents for VM

If you need access to a module, please contact your Qualys Technical Account Manager (TAM).

Concepts and Terminologies

Get familiar with common terms used in CloudView.

Concept	Description
Policy	A set of configuration checks that will assess different resources collected from your cloud account.
Control	A configuration check. Each check applies to a specific service/resource. Here are some examples: - MFA should be enabled for console user - applies to AWS IAM Service and IAM User Resource - Password policy should have upper case letter enforced - applies to AWS IAM Service - Security group should not allow inbound access on port 22 from 0.0.0.0 - applies to EC2/VPC services and Security Group Resource
Service	A service is the high level grouping by functional area. Each service consists of different entities or resources.

Concept	**Description**
Resource	A resource is an entity that you can work with. Examples include an Amazon EC2 instance, IAM User, Security Group.
Control Passed	Each control is applicable to a specific resource type. For each control, applicable resources are collected. The control checks whether the particular attribute of a resource is configured as per best practices. The control is passed when the attribute that the control is checking is found configured as per the desired configuration for all the applicable resources collected.
Control Failed	Control is considered failed when an attribute of the control being checked is not configured as per the desired configuration for any of the applicable resources collected.
Resource Passed	Resource is considered passed for a control if it’s attribute is configured as per the desired configuration in the control.
Resource Failed	Resource is considered failed for a control if it’s attribute is not configured as per the desired configuration in the control.

Get Started

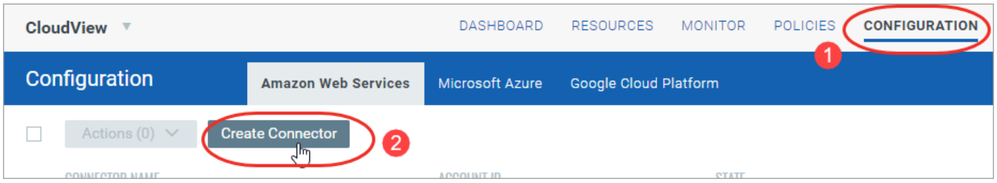
Just set up a connector for your cloud environment and that's it! We'll start discovering resources that are present in your cloud account. You can create AWS, Azure and GCP connectors. We'll walk you through the steps.

AWS

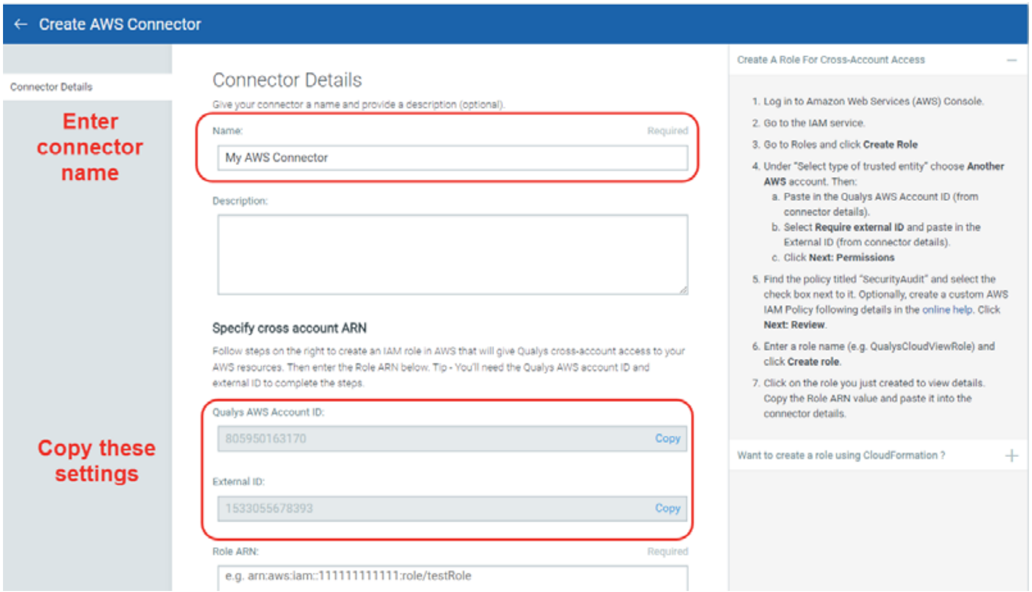
Configure AWS connectors for gathering resource information from your AWS account. It just takes a couple of minutes.

Steps to Create AWS Connector

Go to the Configuration > Amazon Web Services tab and click Create Connector.



Provide a name and description (optional) for your connector. Then copy settings from the connector details: Qualys AWS Account ID and External ID. You'll need these for creating your IAM role in AWS in the next step.



Enter connector name

Copy these settings

Connector Details

Give your connector a name and provide a description (optional).

Name: Required
My AWS Connector

Description:

Specify cross account ARN

Follow steps on the right to create an IAM role in AWS that will give Qualys cross-account access to your AWS resources. Then enter the Role ARN below. Tip - You'll need the Qualys AWS account ID and external ID to complete the steps.

Qualys AWS Account ID:
805950163170 Copy

External ID:
1533055678393 Copy

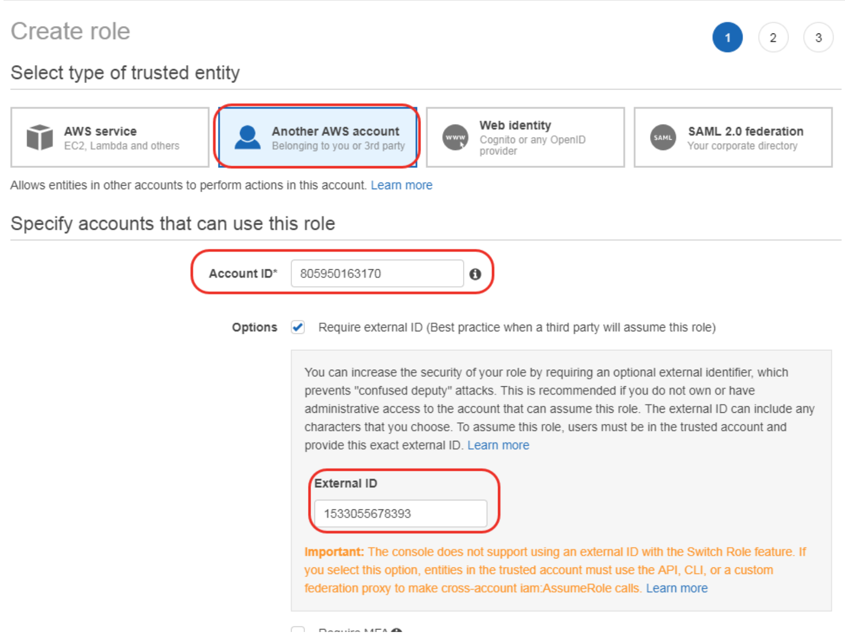
Role ARN: Required
e.g. arn:aws:iam::111111111111:role/testRole

Create A Role For Cross-Account Access —

1. Log in to Amazon Web Services (AWS) Console.
2. Go to the IAM service.
3. Go to Roles and click **Create Role**
4. Under "Select type of trusted entity" choose **Another AWS** account. Then:
   a. Paste in the Qualys AWS Account ID (from connector details).
   b. Select **Require external ID** and paste in the External ID (from connector details).
   c. Click **Next: Permissions**
5. Find the policy titled "SecurityAudit" and select the check box next to it. Optionally, create a custom AWS IAM Policy following details in the online help. Click **Next: Review**.
6. Enter a role name (e.g. QualysCloudViewRole) and click **Create role**.
7. Click on the role you just created to view details. Copy the Role ARN value and paste it into the connector details.

Want to create a role using CloudFormation ? +

Launch your AWS console, and go to IAM > Roles and click Create Role. In the Create role window, choose "Another AWS account". Paste in the Qualys account ID and the External ID that you copied in the previous step. Click Next: Permissions.



Create role

Select type of trusted entity

Allows entities in other accounts to perform actions in this account. Learn more

Specify accounts that can use this role

Account ID* 805950163170

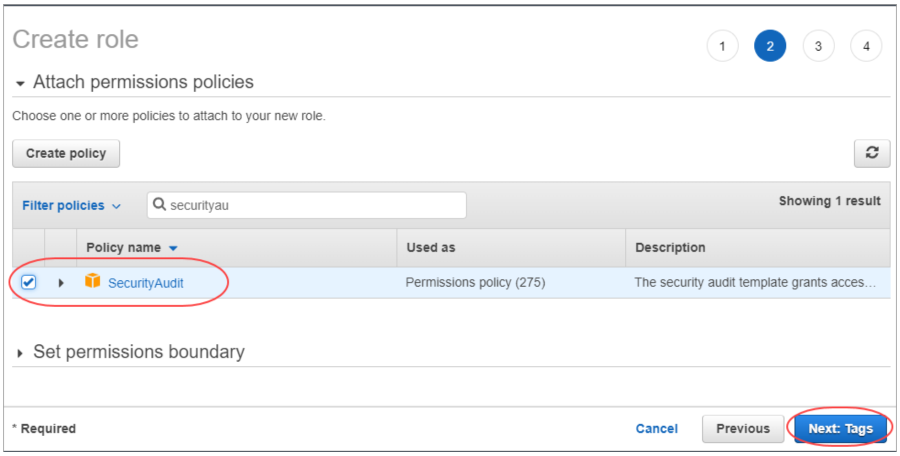
Options ☑ Require external ID (Best practice when a third party will assume this role)

You can increase the security of your role by requiring an optional external identifier, which prevents "confused deputy" attacks. This is recommended if you do not own or have administrative access to the account that can assume this role. The external ID can include any characters that you choose. To assume this role, users must be in the trusted account and provide this exact external ID. Learn more

External ID
1533055678393

Important: The console does not support using an external ID with the Switch Role feature. If you select this option, entities in the trusted account must use the API, CLI, or a custom federation proxy to make cross-account iam:AssumeRole calls. Learn more

Choose AWS policy to attach to role. Find the policy "SecurityAudit" and select the check box next to it. Click Next: Tags.



Create role

Attach permissions policies

Choose one or more policies to attach to your new role.

securityau

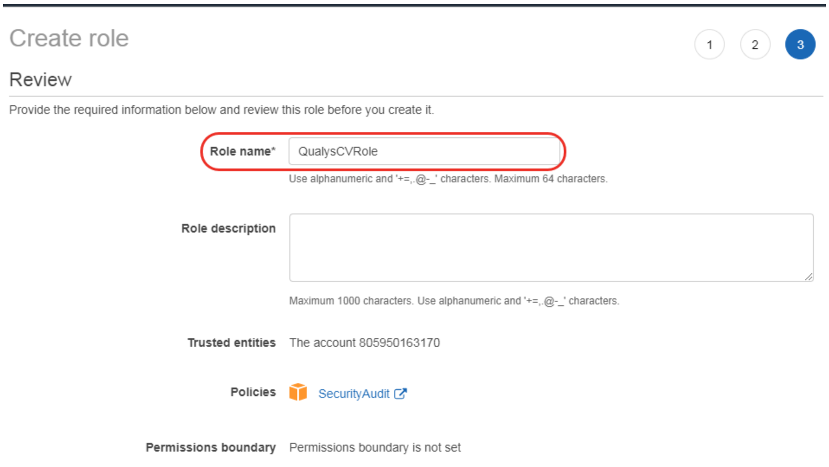
Showing 1 result

		Policy name	Used as	Description
☑	▸	SecurityAudit	Permissions policy (275)	The security audit template grants acces...

Set permissions boundary

* Required

Save AWS role and get the ARN. Enter a role name (e.g. QualysCVRole), click Create role. Then click on the saved role to view role details and copy the ARN value.



Review

Provide the required information below and review this role before you create it.

Role name* QualysCVRole

Use alphanumeric and '+=,.@-_' characters. Maximum 64 characters.

Role description

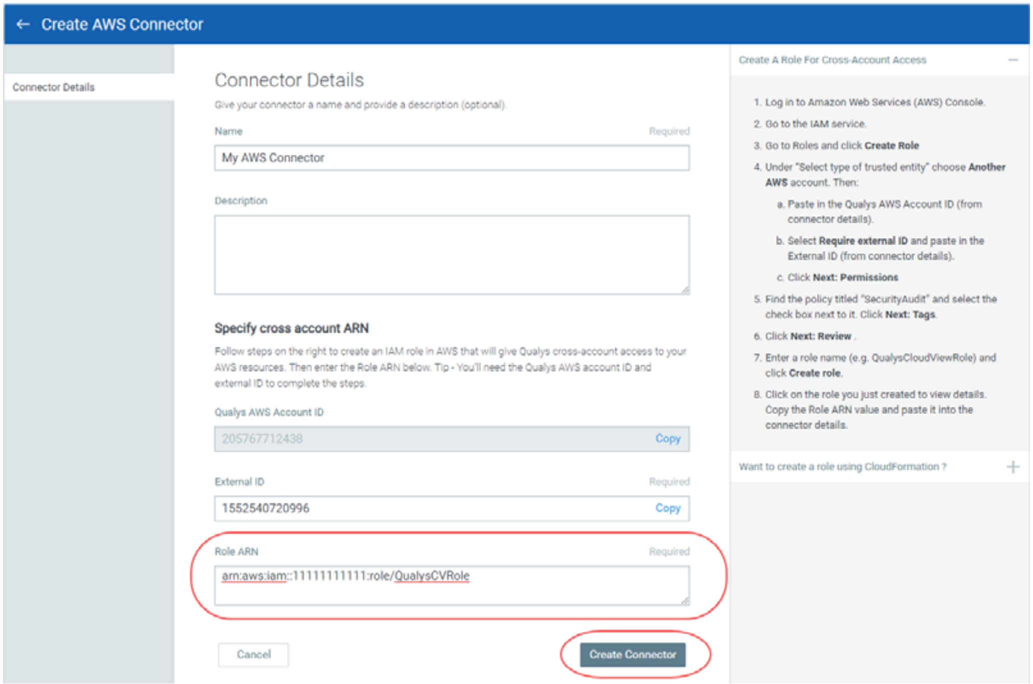
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Trusted entities: The account 805950163170

Policies: SecurityAudit

Permissions boundary: Permissions boundary is not set

Go back to your AWS connector in Qualys CloudView and paste the Role ARN value into the connector details. Then click Create Connector.



Connector Details

Give your connector a name and provide a description (optional).

Name (Required): My AWS Connector

Description

Specify cross account ARN

Follow steps on the right to create an IAM role in AWS that will give Qualys cross-account access to your AWS resources. Then enter the Role ARN below. Tip - You'll need the Qualys AWS account ID and external ID to complete the steps.

Qualys AWS Account ID: 205767712438 Copy

External ID (Required): 1552540720996 Copy

Role ARN (Required): arn:aws:iam::11111111111:role/QualysCVRole

Create A Role For Cross-Account Access

1. Log in to Amazon Web Services (AWS) Console.
2. Go to the IAM service.
3. Go to Roles and click **Create Role**
4. Under "Select type of trusted entity" choose **Another AWS** account. Then:
   a. Paste in the Qualys AWS Account ID (from connector details).
   b. Select **Require external ID** and paste in the External ID (from connector details).
   c. Click **Next: Permissions**
5. Find the policy titled "SecurityAudit" and select the check box next to it. Click **Next: Tags**.
6. Click **Next: Review** .
7. Enter a role name (e.g. QualysCloudViewRole) and click **Create role**.
8. Click on the role you just created to view details. Copy the Role ARN value and paste it into the connector details.

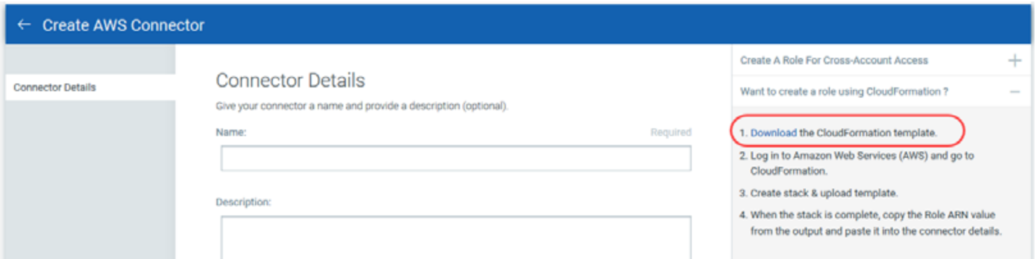
Want to create a role using CloudFormation ?

That's it! The connector will establish a connection with AWS to start discovering resources from each region and evaluate them against policies..

> A unique external ID gets generated during connector creation. If you want to use your own external ID, use API to create the connector. For more details, refer to Example 4: Create AWS connector.

Want to create a role using CloudFormation?

Download the CloudFormation template from the Create AWS Connector window.


Create AWS Connector
Connector Details
Create A Role For Cross-Account Access
Want to create a role using CloudFormation ?

Connector Details

Give your connector a name and provide a description (optional).

Name: Required

Description:

1. Download the CloudFormation template.
2. Log in to Amazon Web Services (AWS) and go to CloudFormation.
3. Create stack & upload template.
4. When the stack is complete, copy the Role ARN value from the output and paste it into the connector details.

Follow the steps on the screen to create a stack and upload the template. When the stack is complete, copy the Role ARN from the output and paste it into the connector details.

AWS Resource Inventory

Upon setting up the AWS connector, it starts discovering the resources that are present in your AWS account. The inventory and the metadata of the resources is pushed to Qualys portal. For list of the resources that are getting collected, refer Resources List. To fetch the updated resources, you need to select Run from the quick actions menu for the AWS connector.

What do you achieve?

- Get centralized visibility of services/resources across your multiple AWS accounts.

- Identify services/resources running your AWS account. For list of resources getting collected, refer Resources List.

- Identify the number of resources that are non-compliant.

- View resource details and their associations with other resources.

- Locate the resources by querying the resource attributed, account & region etc.

- Search tagged/untagged resources using AWS tags.

- Trend chart and time range will help you understand the how the resources are varied over the past 7, 30 days. You can also specify the custom range.

Resources List

CloudView will discover and fetch following AWS resources and their corresponding attributes.

- Subnet
- Network ACL
- Internet Gateway
- Load Balancer
- Instance
- Route Table
- S3 Bucket
- IAM User
- VPC
- Auto Scaling Group
- Security Group
- RDS
- EBS Volume

Microsoft Azure

Configure Microsoft Azure connectors for gathering resource information from your Microsoft Azure account. It just takes a couple of minutes.

Let us see what permissions are needed to create Azure connector.

Pre-requisites

Before you create an Azure connector, ensure that you have the following permissions:

- Assign Azure Active Directory permissions to register an application with your Azure Active Directory

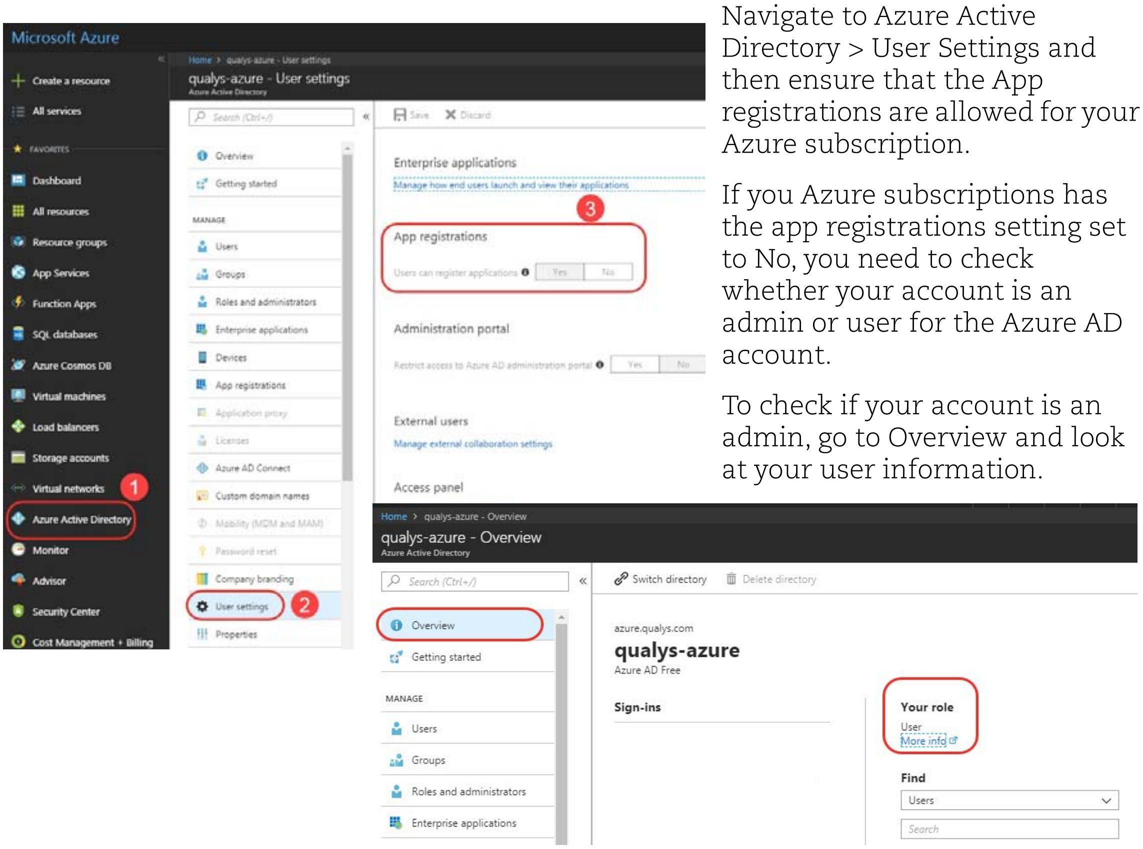
- Check Azure Subscription permissions to assign the application to a role in your Azure subscription

Assign Azure Active Directory permissions

Navigate to Azure Active Directory > User Settings and then ensure that the App registrations are allowed for your Azure subscription.

If you Azure subscriptions has the app registrations setting set to No, you need to check whether your account is an admin or user for the Azure AD account.

To check if your account is an admin, go to Overview and look at your user information.

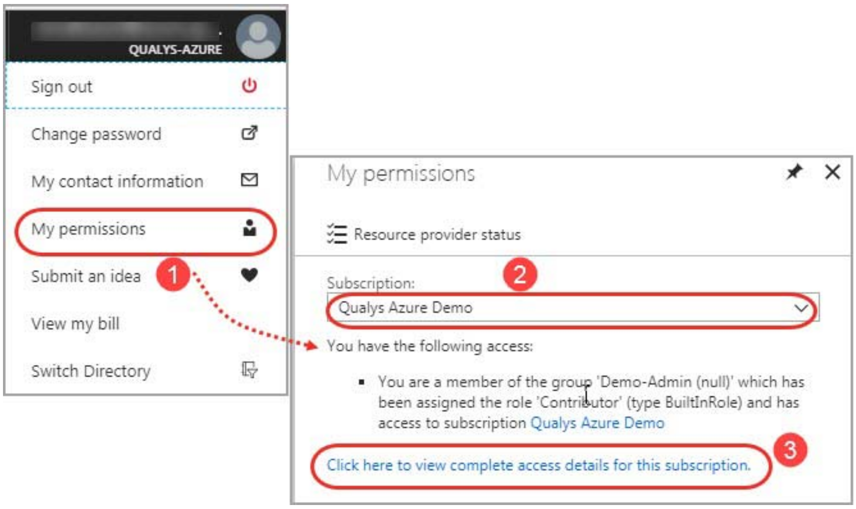


If your account is assigned to the User role, but the app registration setting is restricted to admin users, you will not be permitted to register new apps. In such case, ask your administrator to either assign you to the global administrator role, or to enable users to register apps.

Check Azure Subscription permissions

In your azure subscription, your account must have Owner access role to assign an AD app to a reader role. If your account is assigned to the Contributor role, you do not have adequate permission and will receive an error when attempting to assign the service principal to a role.

To know the role assigned to you, select your account (refer image) and select My permissions. From the Subscription drop-down list, select the subscription for which you would want to check permissions and then click the "Click here to view complete access details for this subscription" link.



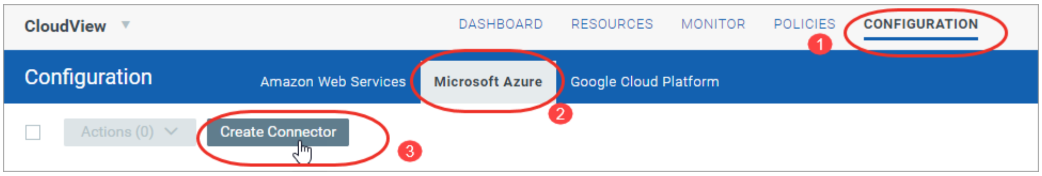
You have the following access:

- You are a member of the group 'Demo-Admin (null)' which has been assigned the role 'Contributor' (type BuiltInRole) and has access to subscription Qualys Azure Demo

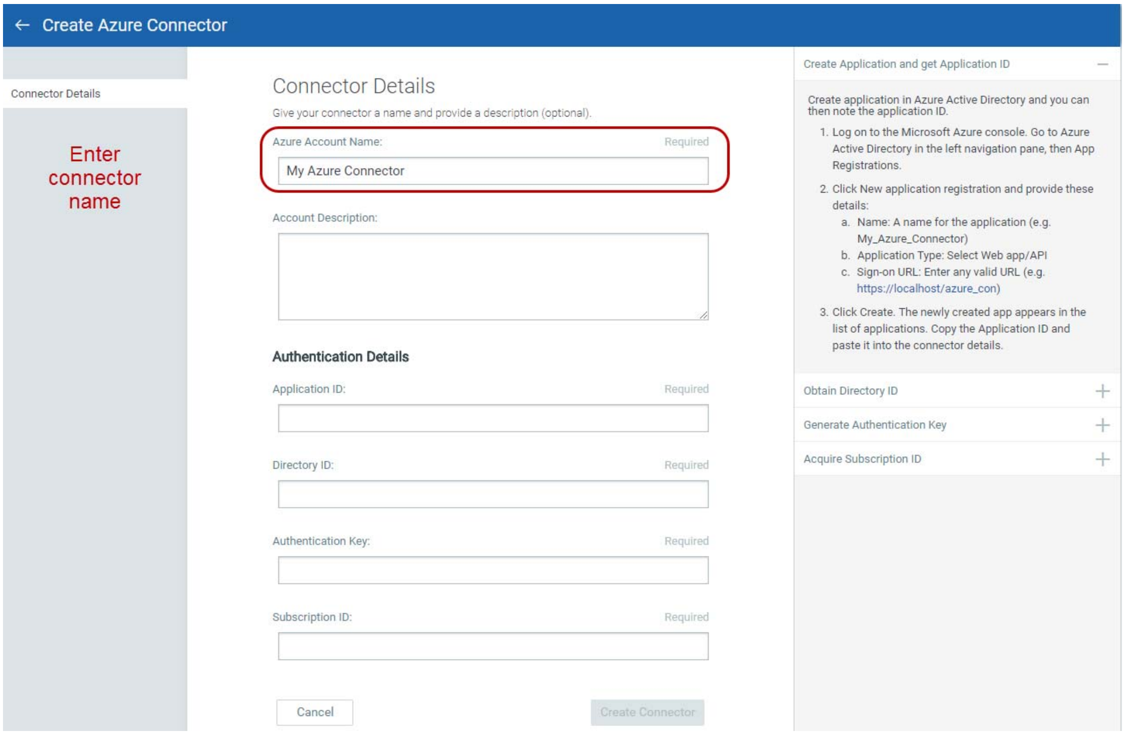
Click here to view complete access details for this subscription.

Steps to Create Azure Connector

On the Configuration tab, select Create Connector > Microsoft Azure.



Provide a name and description (optional) for your connector.



Enter connector name

Connector Details

Give your connector a name and provide a description (optional).

Azure Account Name: Required
My Azure Connector

Account Description:

Authentication Details

Application ID: Required

Directory ID: Required

Authentication Key: Required

Subscription ID: Required

Create Application and get Application ID

Create application in Azure Active Directory and you can then note the application ID.

1. Log on to the Microsoft Azure console. Go to Azure Active Directory in the left navigation pane, then App Registrations.
2. Click New application registration and provide these details:
   a. Name: A name for the application (e.g. My_Azure_Connector)
   b. Application Type: Select Web app/API
   c. Sign-on URL: Enter any valid URL (e.g. https://localhost/azure_con)
3. Click Create. The newly created app appears in the list of applications. Copy the Application ID and paste it into the connector details.

Obtain Directory ID

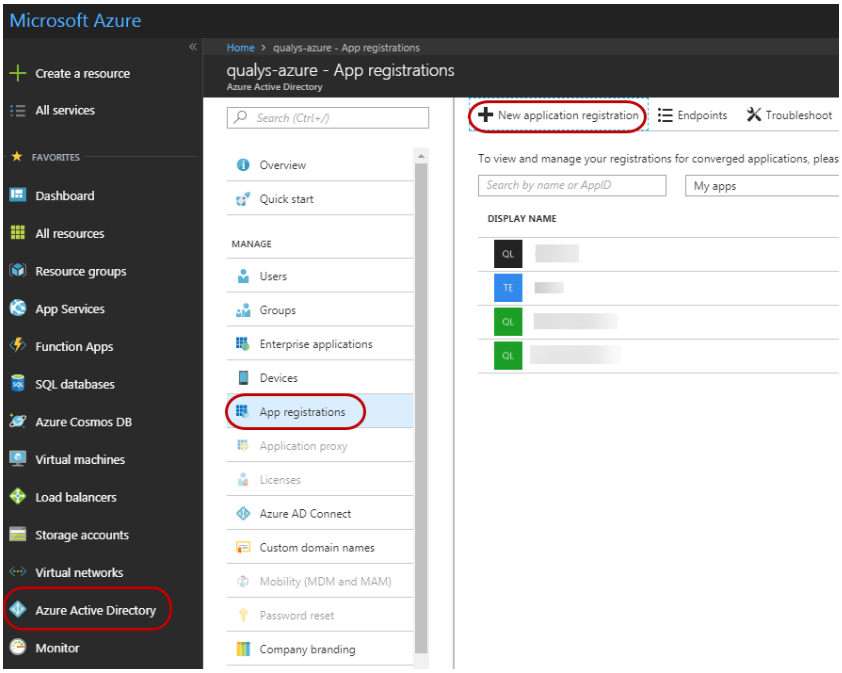
Generate Authentication Key

Acquire Subscription ID

Next we'll describe how to configure the application ID, directory ID, authentication key and subscription ID from the Microsoft Azure console to paste into your connector details.

Application ID

Create an application in Azure Active Directory. Log on to the Microsoft Azure console and go to Azure Active Directory in the left navigation pane, then App registrations. Click New application registration.



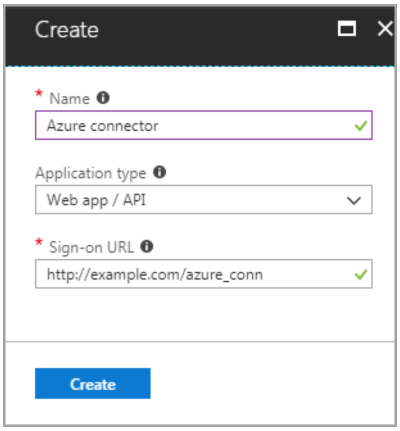
To view and manage your registrations for converged applications, pleas

Provide these details:

Name: A name for the application (e.g. Azure connector)

Application type: Select Web app/API

Sign-on URL: Enter any valid URL. You can enter a URL that does not exist, but it must be in valid format.



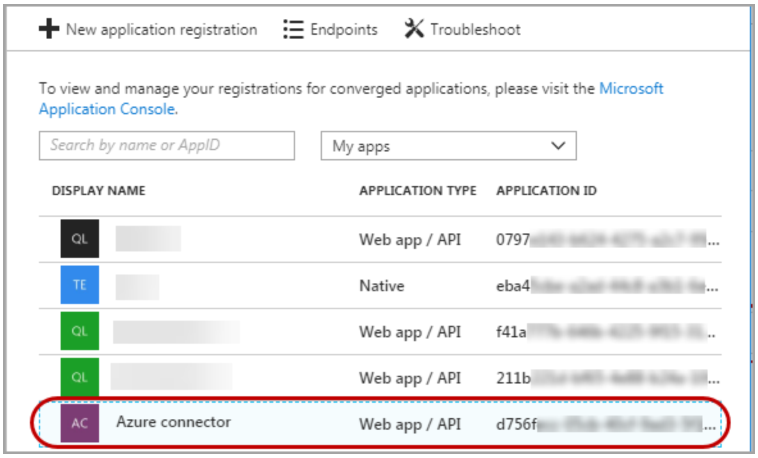
* Name: Azure connector

Application type: Web app / API

* Sign-on URL: http://example.com/azure_conn

Click Create. The newly created app is displayed in the list of applications.

Copy the Application ID and paste it into the connector details.

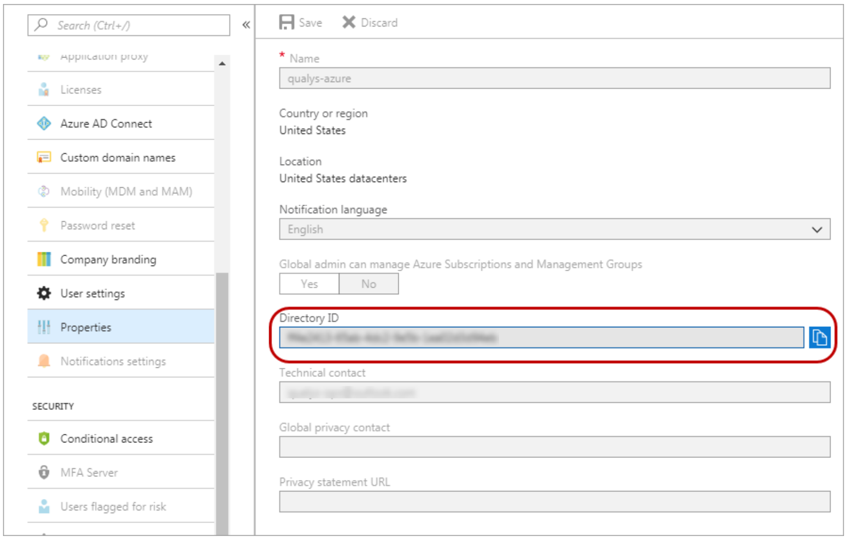


To view and manage your registrations for converged applications, please visit the Microsoft Application Console.

DISPLAY NAME	APPLICATION TYPE	APPLICATION ID
QL [redacted]	Web app / API	0797[redacted]...
TE [redacted]	Native	eba4[redacted]...
QL [redacted]	Web app / API	f41a[redacted]..
QL [redacted]	Web app / API	211b[redacted]...
AC Azure connector	Web app / API	d756f[redacted]...

Directory ID

This is the unique identifier of your Azure Active Directory. In the Azure Active Directory blade, go to Properties. Copy the Directory ID and paste it into the connector details.



* Name
qualys-azure

Country or region
United States

Location
United States datacenters

Notification language
English

Global admin can manage Azure Subscriptions and Management Groups
Yes No

Directory ID
[redacted]

Technical contact
[redacted]

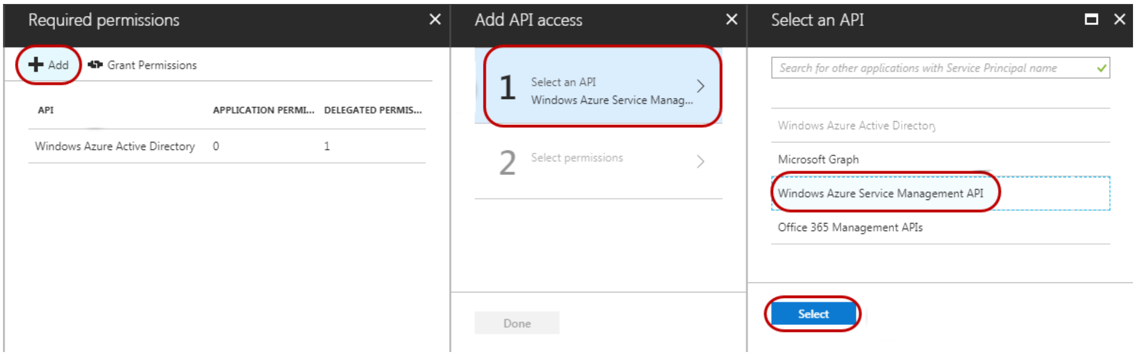
Global privacy contact

Privacy statement URL

Authentication Key

You must provide permission to the new application to access the Windows Azure Service Management API and create a secret key.

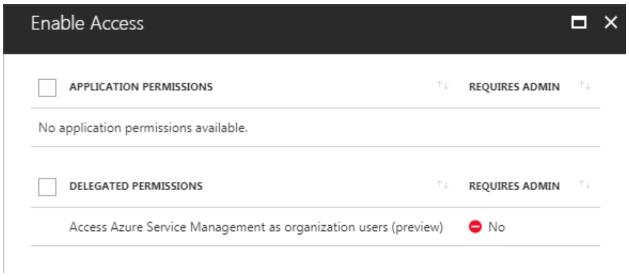
Provide permission: Select the application that you created and go to Settings > Required permissions. Click Add > Select an API > Windows Azure Service Management API, and click Select.


Required permissions
Add
Grant Permissions

API	APPLICATION PERMI...	DELEGATED PERMIS...
Windows Azure Active Directory	0	1

Add API access
1 Select an API
Windows Azure Service Manag...
2 Select permissions
Done
Select an API
Search for other applications with Service Principal name
Windows Azure Active Directory
Microsoft Graph
Windows Azure Service Management API
Office 365 Management APIs
Select

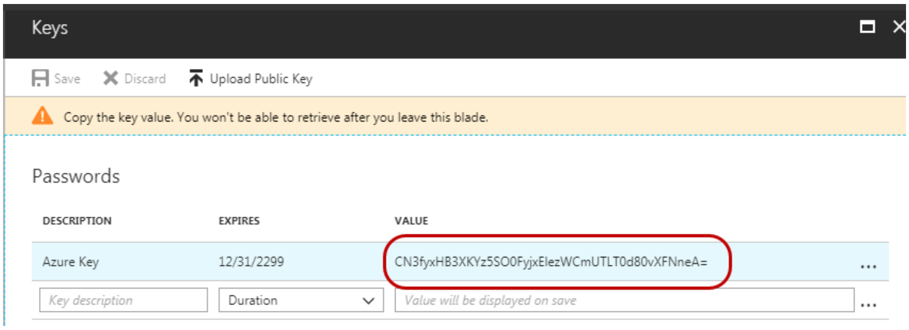
Select required Delegated Permissions, click Select and then click Done.



□ APPLICATION PERMISSIONS	REQUIRES ADMIN
No application permissions available.	

□ DELEGATED PERMISSIONS	REQUIRES ADMIN
Access Azure Service Management as organization users (preview)	⛔ No

Create secret key: Select the application that you created and go to Settings > Keys. Add a description and expiry duration for the new key and click Save. The value of the key appears in the Value field.



Copy the key value. You won't be able to retrieve after you leave this blade.

Passwords

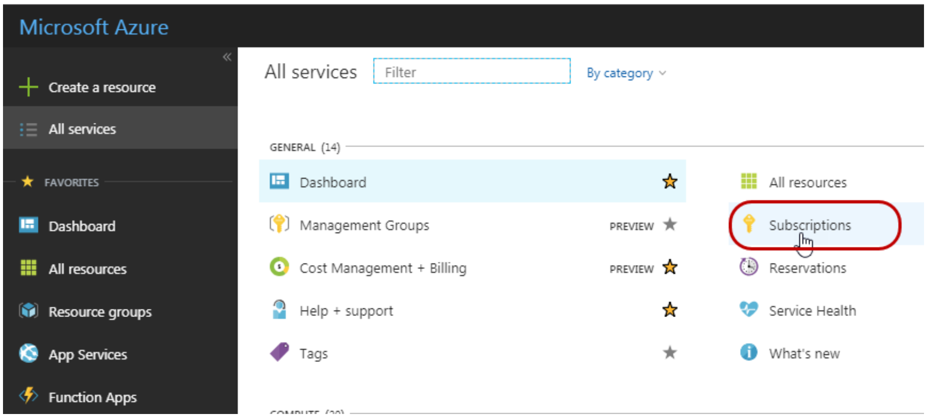
DESCRIPTION	EXPIRES	VALUE
Azure Key	12/31/2299	CN3fyxHB3XKYz5SO0FyjxElezWCmUTLT0d80vXFNneA=
Key description	Duration	Value will be displayed on save

Copy the key value at this time. You won’t be able to retrieve the key later. Note down the secret key and store it securely with you. You’ll need to provide the key value with the application ID to log on as the application.

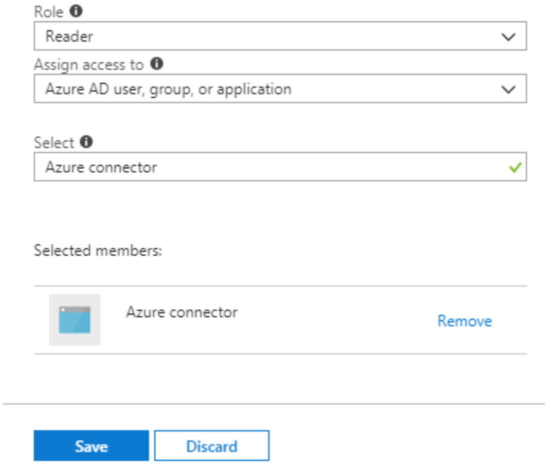
Subscription ID

Grant permission for the application to access subscriptions. Assign a role to the new application. The role defines the permissions for the new application to access subscriptions. Repeat these steps to add more subscriptions.

On the Microsoft Azure portal, navigate to Subscriptions.



Select the subscription for which you want to grant permission to the application, and choose Access Control (IAM). Go to Add > Select a role. Pick the role you want to give to the user. For example, the Reader role. A Reader can view everything, but cannot make any changes to the resources of a subscription.


Role: Reader

Assign access to: Azure AD user, group, or application

Select: Azure connector

Selected members:

Azure connector

Select Azure AD user, group, or application in Assign Access to drop-down. Search for your application, and select it. Then click Save to finish assigning the role. You'll see your application in the list of users assigned to a role for that scope.

Copy the subscription ID you noted and paste it into the connector details in the Qualys Azure Connector screen and then click Create Connector.

Azure Resource Inventory

Upon setting up the Azure connector, it starts discovering the resources that are present in your Azure account. The inventory and the metadata of the resources is pushed to Qualys portal. For list of the resources that are getting collected, refer Resources List. To fetch the updated resources, you need to select Run from the quick actions menu for the Azure connector.

Resources List

CloudView will discover and fetch following Azure resources and their corresponding attributes.

- SQL Server

- SQL Server Database

- Resource Group

- Virtual Network

- Virtual Machine

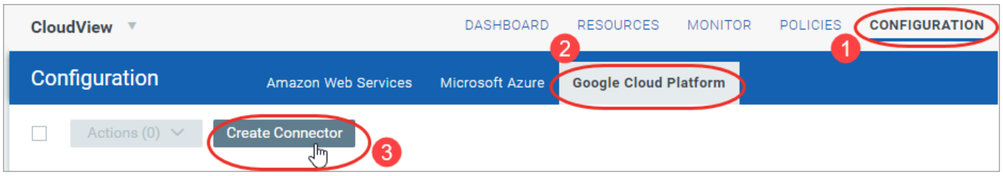
- Network Security Group

Google Cloud Platform

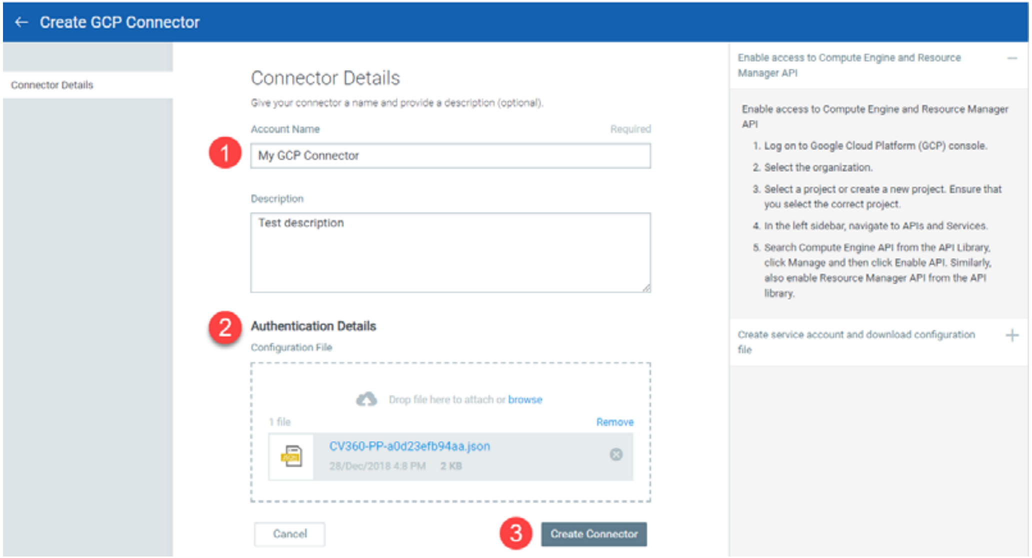
Configure a Google Cloud Platform (GCP) connector for gathering resource information from your Google Cloud Platform project. It just takes a couple of minutes.

Steps to Create GCP Connector

Go to the Configuration > Google Cloud Platform and then click Create Connector.



(1) Provide a name and description (optional) for your connector.



← Create GCP Connector

Connector Details

Give your connector a name and provide a description (optional).

Account Name Required: My GCP Connector

Description: Test description

Authentication Details

Configuration File

CV360-PP-a0d23efb94aa.json
28/Dec/2018 4:8 PM 2 KB

Enable access to Compute Engine and Resource Manager API —

Enable access to Compute Engine and Resource Manager API

1. Log on to Google Cloud Platform (GCP) console.
2. Select the organization.
3. Select a project or create a new project. Ensure that you select the correct project.
4. In the left sidebar, navigate to APIs and Services.
5. Search Compute Engine API from the API Library, click Manage and then click Enable API. Similarly, also enable Resource Manager API from the API library.

Create service account and download configuration file +

(2) You need to download the configuration file from the GCP console and then upload it to Qualys Cloud Platform to complete GCP connector creation.

(3)Click Create Connector.

That’s it! The connector will establish a connection with GCP to start discovering resources from each region.

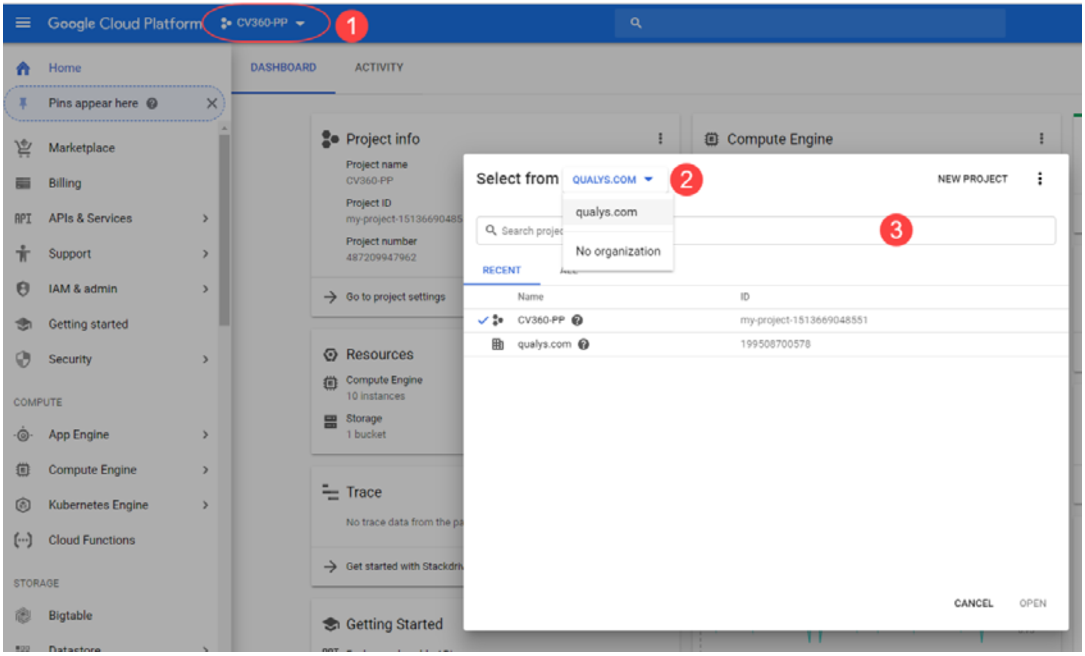
Let us see the steps to download the configuration (JSON) file from GCP console and set up the required authentication details. You need to enable access to the necessary APIs from the API library.

Enable Access to Compute Engine and Resource Manager API

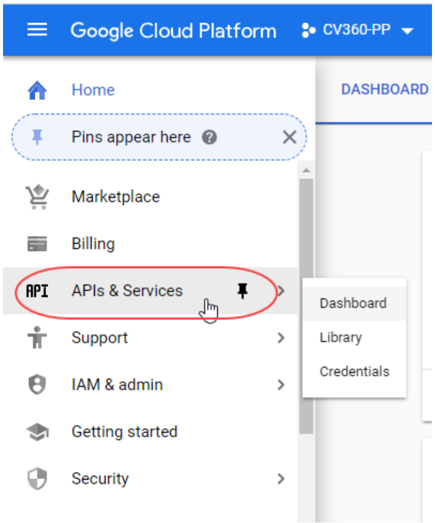
(1) Navigate to Google Cloud Platform (GCP) console.

(2) Select the organization.

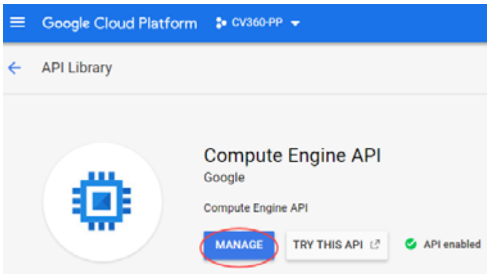
(3) Select a project or create a new project. Ensure that you select the correct project.



(4) In the left sidebar, navigate to APIs and Services.



(5) Search Compute Engine API from the API library, click Manage and then click Enable API.

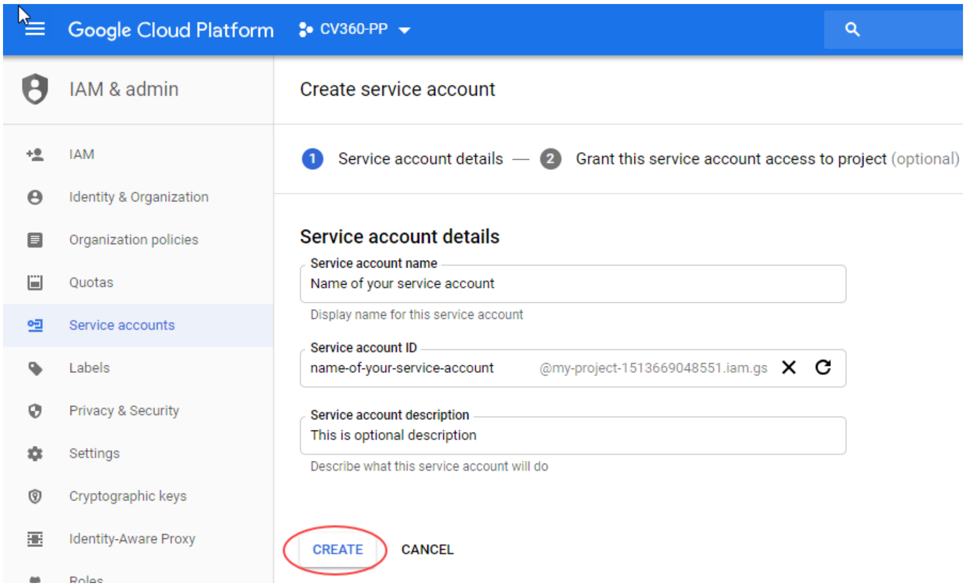


Similarly, enable Cloud Resource Manager API from the API library.

Create Service Account and Download Configuration File

(1) Login to the GCP console and select a project.

(2) From the left sidebar, navigate to IAM & admin > Service accounts and click CREATE SERVICE ACCOUNT. Provide a name and description (optional) for the service account and click Create.



Service account details

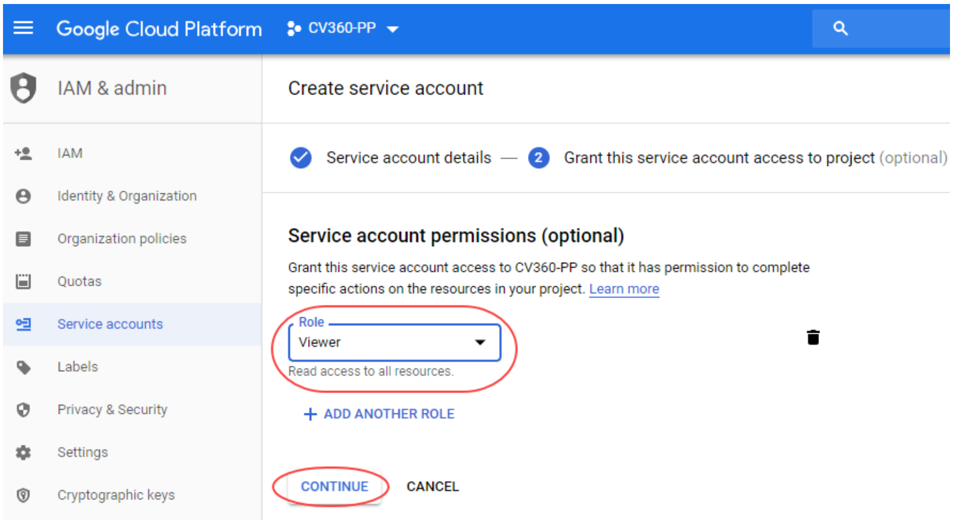
Service account name: Name of your service account
Display name for this service account

Service account ID: name-of-your-service-account @my-project-1513669048551.iam.gs

Service account description: This is optional description
Describe what this service account will do

CREATE CANCEL

(3) Choose Viewer role to assign at least reader permissions to the service account and click Continue.



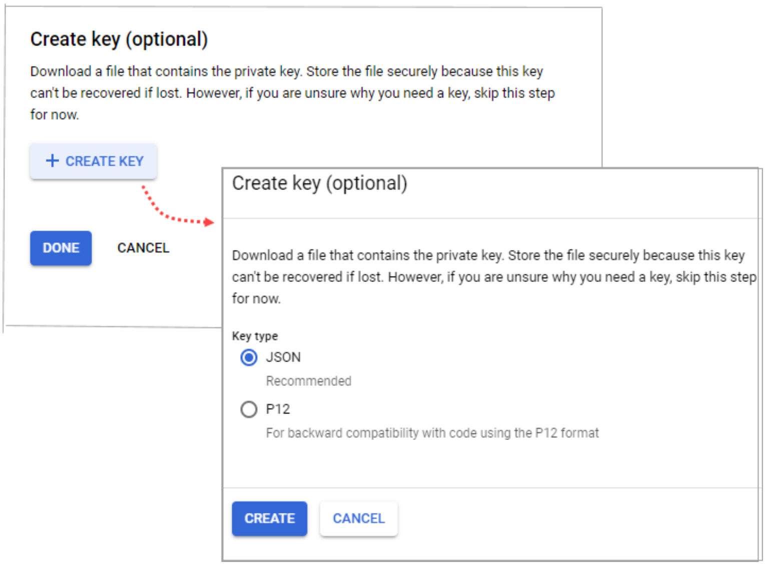
Service account permissions (optional)

Grant this service account access to CV360-PP so that it has permission to complete specific actions on the resources in your project. Learn more

Role: Viewer

Read access to all resources.

(4) Click CREATE KEY and select JSON as Key type and click Create.



Create key (optional)

Download a file that contains the private key. Store the file securely because this key can't be recovered if lost. However, if you are unsure why you need a key, skip this step for now.

Create key (optional)

Download a file that contains the private key. Store the file securely because this key can't be recovered if lost. However, if you are unsure why you need a key, skip this step for now.

Key type

● JSON
Recommended

○ P12
For backward compatibility with code using the P12 format

A message saying “Private key saved to your computer” is displayed and the JSON file is downloaded to your computer. Click Close and then click Done.

Upload the configuration (JSON) file and click Create Connector to complete GCP connector creation in Qualys Cloud Platform.

GCP Resource Inventory

Upon setting up the Google Cloud Platform (GCP) connector, it starts discovering the resources that are present in your GCP account. The inventory and the metadata of the resources is pushed to Qualys portal. For list of the resources that are getting collected, refer Resources List. To fetch the updated resources, you need to select Run from the quick actions menu for the GCP connector.

Resources List

CloudView will discover and fetch following GCP resources and their corresponding attributes.

- VM Instances
- Networks
- Firewall Rules
- Subnetworks

Securing Cloud Resources

Upon setting up your connector, it starts discovering the resources that are present in your cloud account. The resources inventory and the metadata of the resources is pushed to Qualys portal. You can navigate to the Resources tab to view the resources getting collected along with their details.

Dashboard

The Qualys CloudView application provides out-of-the box default AWS Dashboard providing a summary of inventory and security posture across resources.

The default dashboard provides:

- Resource inventory - Route Tables, EC2 Instances, VPC, Subnets, IAM Users, etc

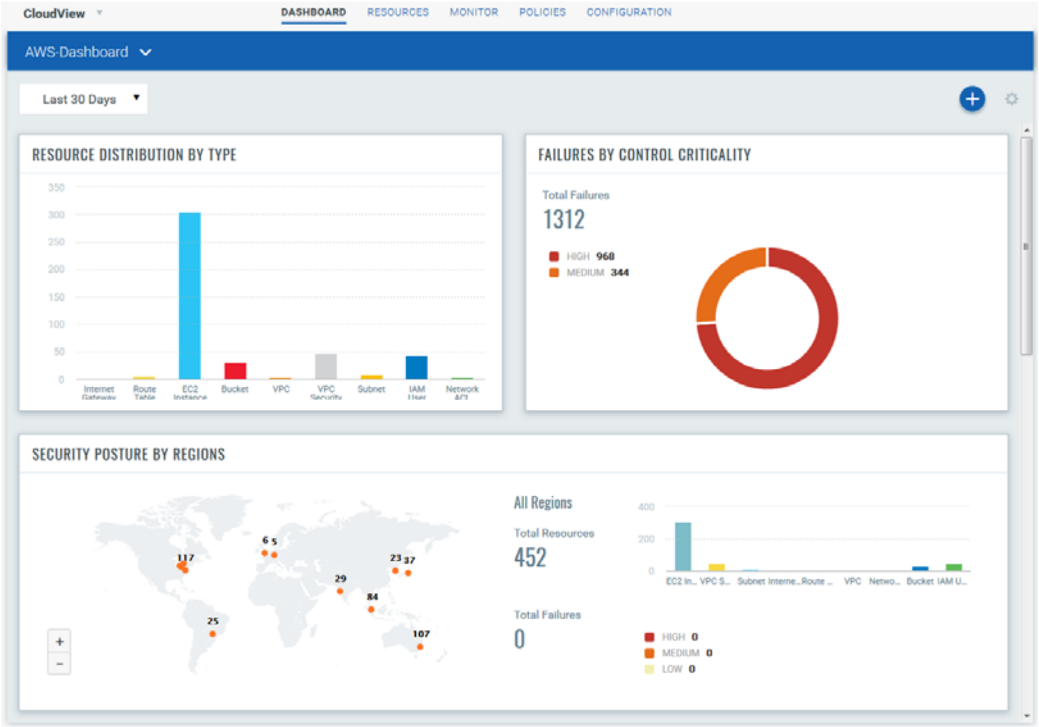
- Total evaluation failures i.e. the resources misconfigurations by control criticality

- Security posture at each region level showing resources and failures

- Top 5 Accounts with maximum control failures

- Top 5 Failed controls

Check out this sample dashboard

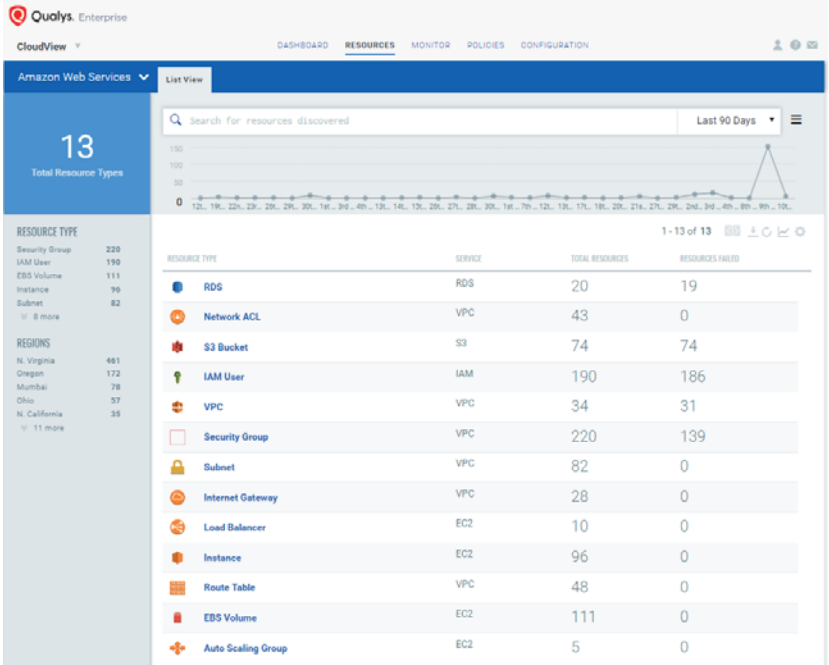


Resources Details

The Resources tab displays the information about various resources collected. It helps you to identify the number of resources for each type and the number of resources that have one or more control failures. You can click on a row to view the number of resources of a specific type. You can click on an individual resource to view the details. For each resource you will view the following information.

Resources Summary

The List View provides a summary of your resources, including the total resources and the number of failed resources for each resource type.


Qualys. Enterprise
CloudView
DASHBOARD
RESOURCES
MONITOR
POLICIES
CONFIGURATION
Amazon Web Services
List View
Search for resources discovered
Last 90 Days
13
Total Resource Types
150
100
50
0
12t... 19t... 22n... 23r... 26t... 29t... 30t... 1st ... 3rd ... 4th ... 13t... 14t... 15t... 26t... 27t... 28t... 30t... 1st ... 7th ... 12t... 13t... 17t... 18t... 20t... 21s... 27t... 29t... 2nd... 3rd ... 4th ... 8th ... 9th ... 10t...
1 - 13 of 13

RESOURCE TYPE	
Security Group	220
IAM User	190
EBS Volume	111
Instance	96
Subnet	82
8 more	

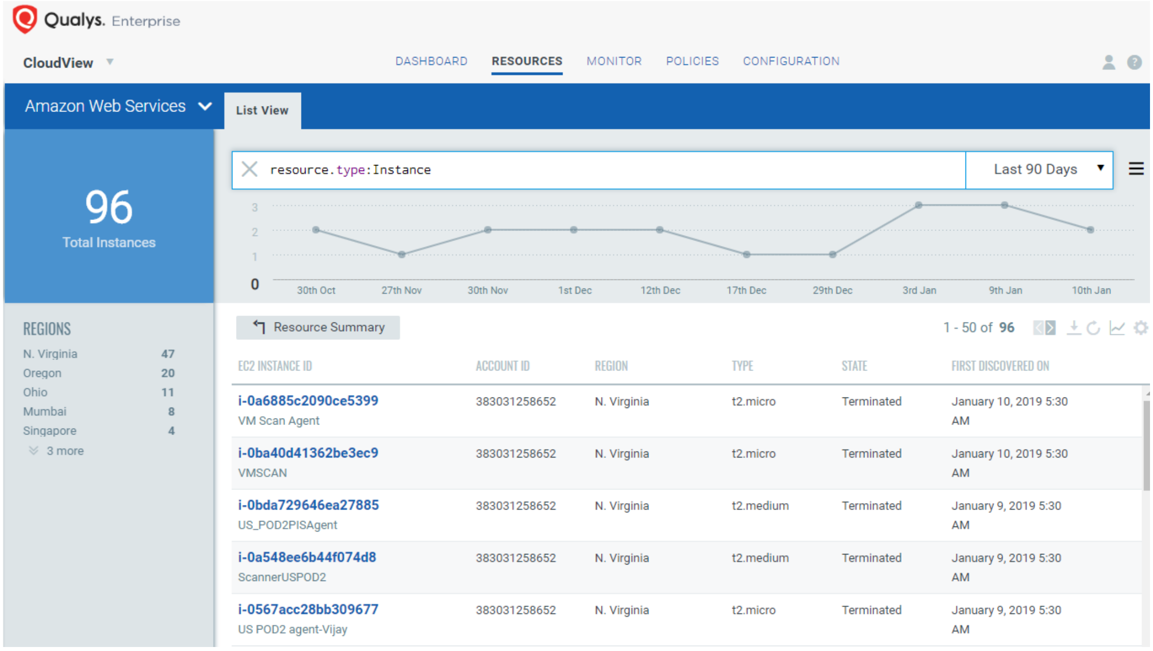
REGIONS	
N. Virginia	461
Oregon	172
Mumbai	78
Ohio	57
N. California	35
11 more	

RESOURCE TYPE	SERVICE	TOTAL RESOURCES	RESOURCES FAILED
RDS	RDS	20	19
Network ACL	VPC	43	0
S3 Bucket	S3	74	74
IAM User	IAM	190	186
VPC	VPC	34	31
Security Group	VPC	220	139
Subnet	VPC	82	0
Internet Gateway	VPC	28	0
Load Balancer	EC2	10	0
Instance	EC2	96	0
Route Table	VPC	48	0
EBS Volume	EC2	111	0
Auto Scaling Group	EC2	5	0

Let us consider an example of Instance (EC2 Instance) and Security Group resource type to view the resource details and information.

Instance Details

Click Instance type to drill-down into your AWS EC2 instances. You could also use the filters in the left pane to narrow down resources per region or account.



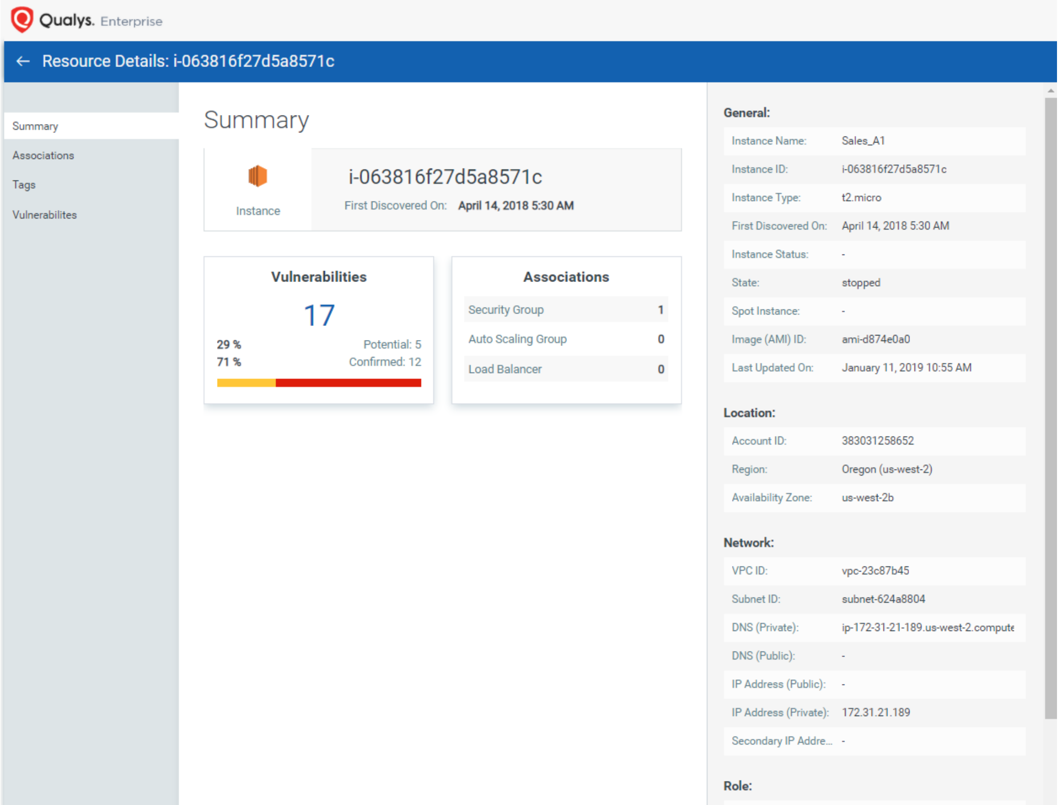
```
resource.type:Instance
```

REGIONS

N. Virginia	47
Oregon	20
Ohio	11
Mumbai	8
Singapore	4

EC2 INSTANCE ID	ACCOUNT ID	REGION	TYPE	STATE	FIRST DISCOVERED ON
i-0a6885c2090ce5399 VM Scan Agent	383031258652	N. Virginia	t2.micro	Terminated	January 10, 2019 5:30 AM
i-0ba40d41362be3ec9 VMSCAN	383031258652	N. Virginia	t2.micro	Terminated	January 10, 2019 5:30 AM
i-0bda729646ea27885 US_POD2PISAgent	383031258652	N. Virginia	t2.medium	Terminated	January 9, 2019 5:30 AM
i-0a548ee6b44f074d8 ScannerUSPOD2	383031258652	N. Virginia	t2.medium	Terminated	January 9, 2019 5:30 AM
i-0567acc28bb309677 US POD2 agent-Vijay	383031258652	N. Virginia	t2.micro	Terminated	January 9, 2019 5:30 AM

Then click on any EC2 Instance ID to see the number of detected vulnerabilities, resource associations, location and network information.



Summary

i-063816f27d5a8571c

First Discovered On: **April 14, 2018 5:30 AM**

Vulnerabilities

17

29 % Potential: 5
71 % Confirmed: 12

Associations

Security Group	**1**
Auto Scaling Group	**0**
Load Balancer	**0**

General:

Instance Name:	Sales_A1
Instance ID:	i-063816f27d5a8571c
Instance Type:	t2.micro
First Discovered On:	April 14, 2018 5:30 AM
Instance Status:	-
State:	stopped
Spot Instance:	-
Image (AMI) ID:	ami-d874e0a0
Last Updated On:	January 11, 2019 10:55 AM

Location:

Account ID:	383031258652
Region:	Oregon (us-west-2)
Availability Zone:	us-west-2b

Network:

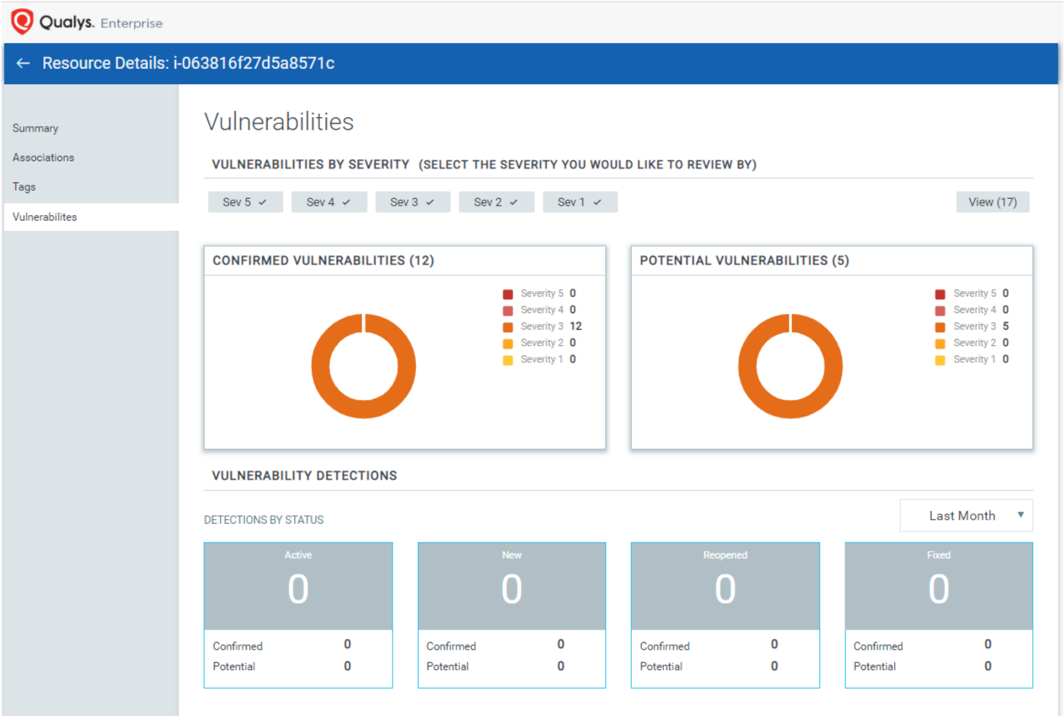
VPC ID:	vpc-23c87b45
Subnet ID:	subnet-624a8804
DNS (Private):	ip-172-31-21-189.us-west-2.compute
DNS (Public):	-
IP Address (Public):	-
IP Address (Private):	172.31.21.189
Secondary IP Addre...	-

Role:

Vulnerability Details

Click on the Vulnerabilities count to get information about detected vulnerabilities.

> The vulnerability related data is populated only if you are using a scanner appliance or Cloud Agent.



Qualys. Enterprise

← Resource Details: i-063816f27d5a8571c

Vulnerabilities

VULNERABILITIES BY SEVERITY (SELECT THE SEVERITY YOU WOULD LIKE TO REVIEW BY)

Sev 5 ✓ Sev 4 ✓ Sev 3 ✓ Sev 2 ✓ Sev 1 ✓ View (17)

CONFIRMED VULNERABILITIES (12)

Severity 5	0
Severity 4	0
Severity 3	12
Severity 2	0
Severity 1	0

POTENTIAL VULNERABILITIES (5)

Severity 5	0
Severity 4	0
Severity 3	5
Severity 2	0
Severity 1	0

VULNERABILITY DETECTIONS

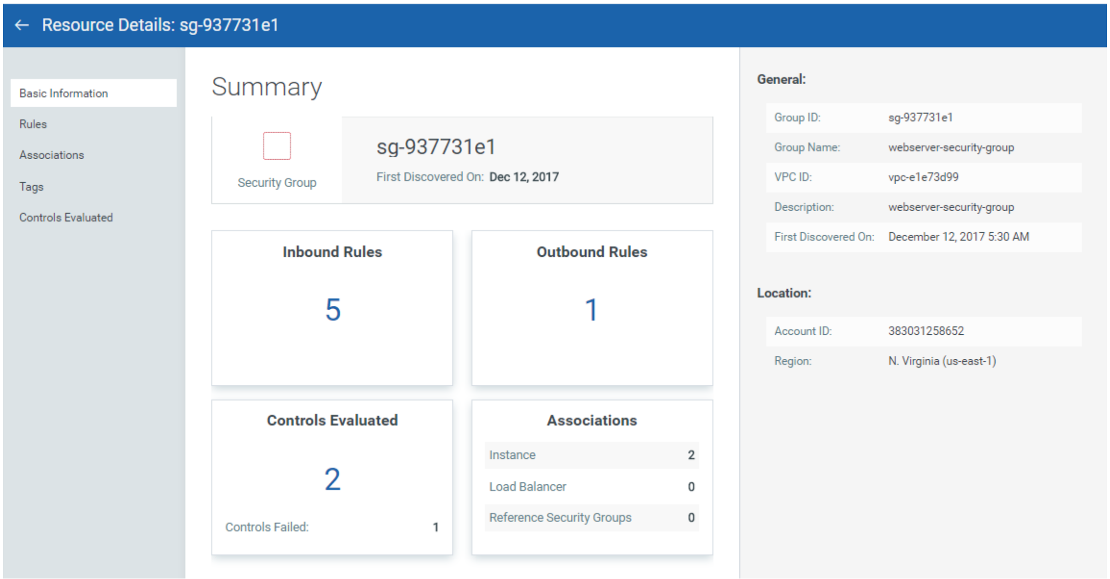
DETECTIONS BY STATUS

Last Month ▾

	Active	New	Reopened	Fixed
	0	0	0	0
Confirmed	0	0	0	0
Potential	0	0	0	0

View Security Group Information

You could view more details about a security group resource. Go to Resources > Security Group, and then click the security group ID to view additional details about it.



sg-937731e1
First Discovered On: Dec 12, 2017

Inbound Rules: 5

Outbound Rules: 1

Controls Evaluated: 2
Controls Failed: 1

Associations	
Instance	2
Load Balancer	0
Reference Security Groups	0

General:

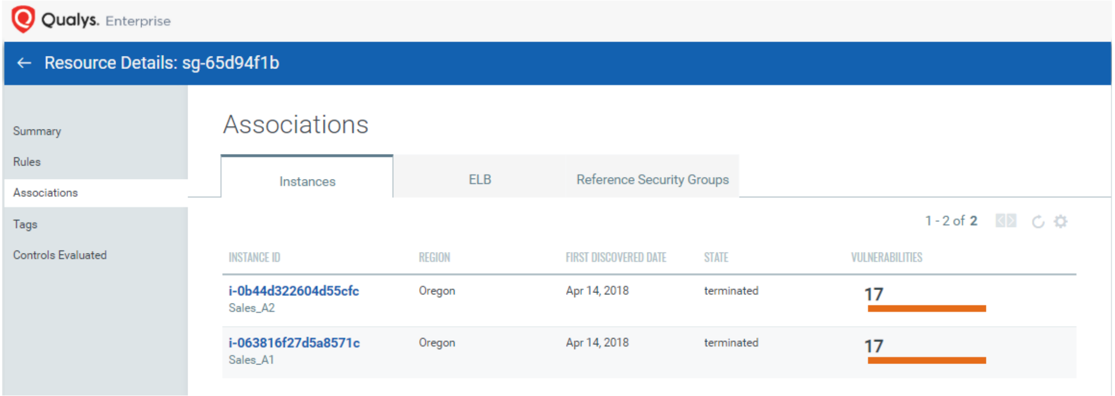
Group ID:	sg-937731e1
Group Name:	webserver-security-group
VPC ID:	vpc-e1e73d99
Description:	webserver-security-group
First Discovered On:	December 12, 2017 5:30 AM

Location:

Account ID:	383031258652
Region:	N. Virginia (us-east-1)

View Security Group Associations

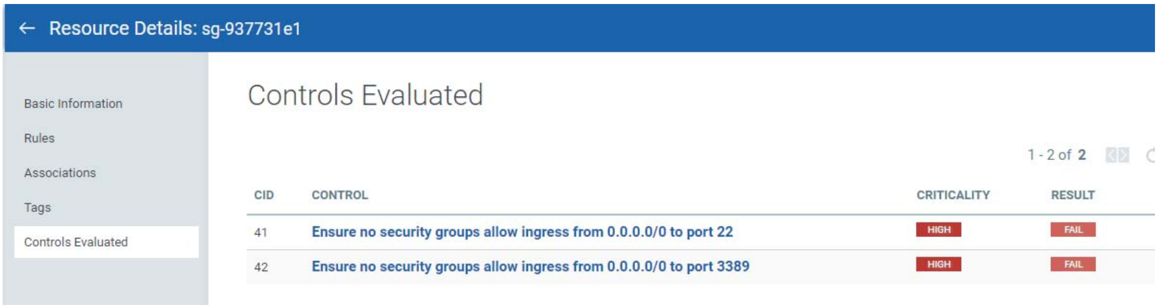
You can view various details about the associations such as the ID, region, state and so on.



INSTANCE ID	REGION	FIRST DISCOVERED DATE	STATE	VULNERABILITIES
i-0b44d322604d55cfc Sales_A2	Oregon	Apr 14, 2018	terminated	17
i-063816f27d5a8571c Sales_A1	Oregon	Apr 14, 2018	terminated	17

View Controls Evaluated

You can view the controls that are evaluated for the resource and if the controls have passed or failed.



Resource Details: sg-937731e1

Controls Evaluated

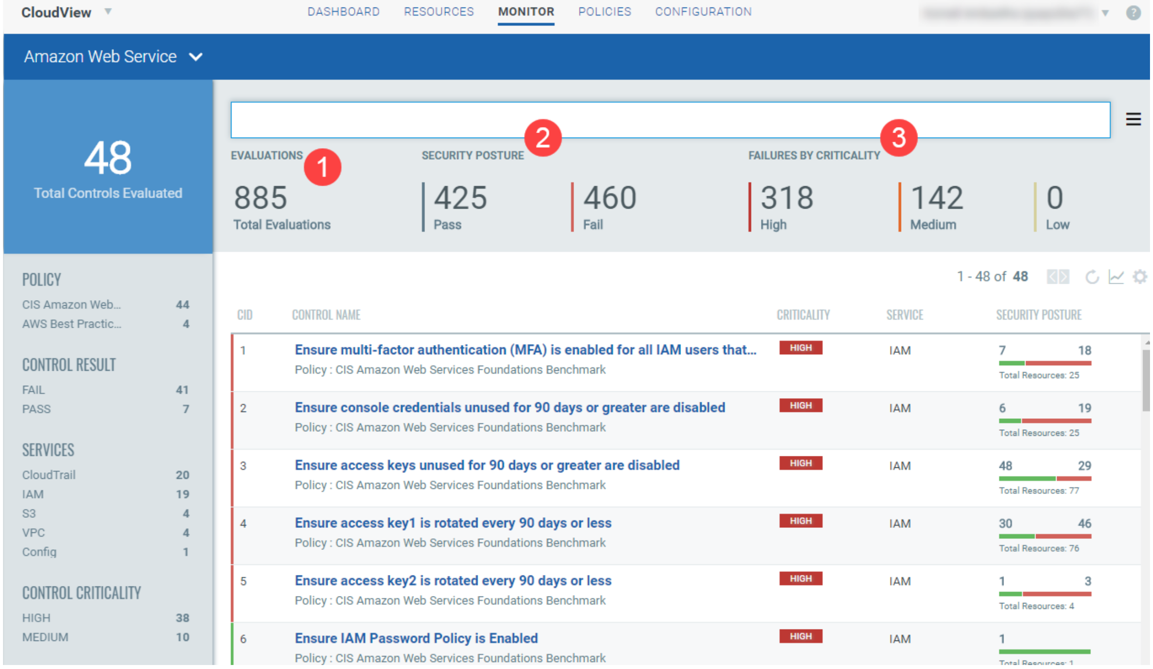
1 - 2 of 2

CID	CONTROL	CRITICALITY	RESULT
41	Ensure no security groups allow ingress from 0.0.0.0/0 to port 22	HIGH	FAIL
42	Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389	HIGH	FAIL

Resources Misconfigurations

CloudView compares controls from the out-of-box policies that define the desired configuration of a resource against the current configuration of the resource. If it finds a difference, then it marks the resource as failed for that particular control. Each control is evaluated against the applicable resources. If all the applicable resources are configured as per the desired configuration of the control, then the control is marked as Pass. If at least one of the applicable controls doesn't comply with the control, then it is marked as failed. The Monitor tab will display all such misconfigurations.

Controls Evaluation View



48
Total Controls Evaluated

EVALUATIONS
885 Total Evaluations

SECURITY POSTURE
425 Pass
460 Fail

FAILURES BY CRITICALITY
318 High
142 Medium
0 Low

POLICY	
CIS Amazon Web...	44
AWS Best Practic...	4
CONTROL RESULT	
FAIL	41
PASS	7
SERVICES	
CloudTrail	20
IAM	19
S3	4
VPC	4
Config	1
CONTROL CRITICALITY	
HIGH	38
MEDIUM	10

1 - 48 of 48

CID	CONTROL NAME	CRITICALITY	SERVICE	SECURITY POSTURE
1	Ensure multi-factor authentication (MFA) is enabled for all IAM users that... Policy : CIS Amazon Web Services Foundations Benchmark	HIGH	IAM	7 18 Total Resources: 25
2	Ensure console credentials unused for 90 days or greater are disabled Policy : CIS Amazon Web Services Foundations Benchmark	HIGH	IAM	6 19 Total Resources: 25
3	Ensure access keys unused for 90 days or greater are disabled Policy : CIS Amazon Web Services Foundations Benchmark	HIGH	IAM	48 29 Total Resources: 77
4	Ensure access key1 is rotated every 90 days or less Policy : CIS Amazon Web Services Foundations Benchmark	HIGH	IAM	30 46 Total Resources: 76
5	Ensure access key2 is rotated every 90 days or less Policy : CIS Amazon Web Services Foundations Benchmark	HIGH	IAM	1 3 Total Resources: 4
6	Ensure IAM Password Policy is Enabled Policy : CIS Amazon Web Services Foundations Benchmark	HIGH	IAM	1 Total Resources: 1

(1) Total Resources - The unique number of resources evaluated against all the controls.

(2) Security Posture - How many control evaluations have passed and failed.

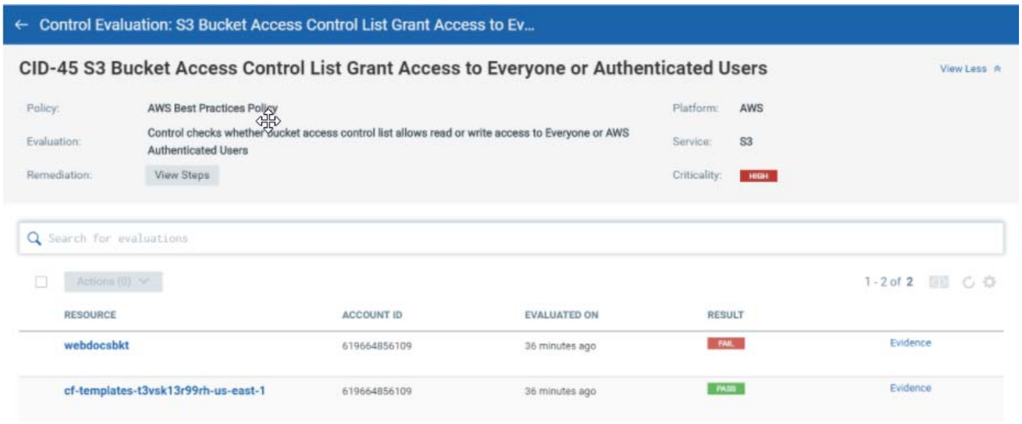
(3) Failures By Critically - Control evaluation failures by control criticality.

Each control is evaluated against the applicable resources which is represented by Total Resources. Number represented by green represents the number of pass resources that have the desired configuration as per the control. Number represented by red represents the number of failed resources.

Click on any control to get details of all the resources evaluated against the control.

Control Evaluation Details

Control details screen shows the number of resources evaluated against the control. For each resource it shows Unique Resource ID, Account ID, Region, etc. You can use the search filter to view pass/failed resources.



← Control Evaluation: S3 Bucket Access Control List Grant Access to Ev...

CID-45 S3 Bucket Access Control List Grant Access to Everyone or Authenticated Users

View Less

Policy:	AWS Best Practices Policy	Platform:	AWS
Evaluation:	Control checks whether bucket access control list allows read or write access to Everyone or AWS Authenticated Users	Service:	S3
Remediation:	View Steps	Criticality:	HIGH

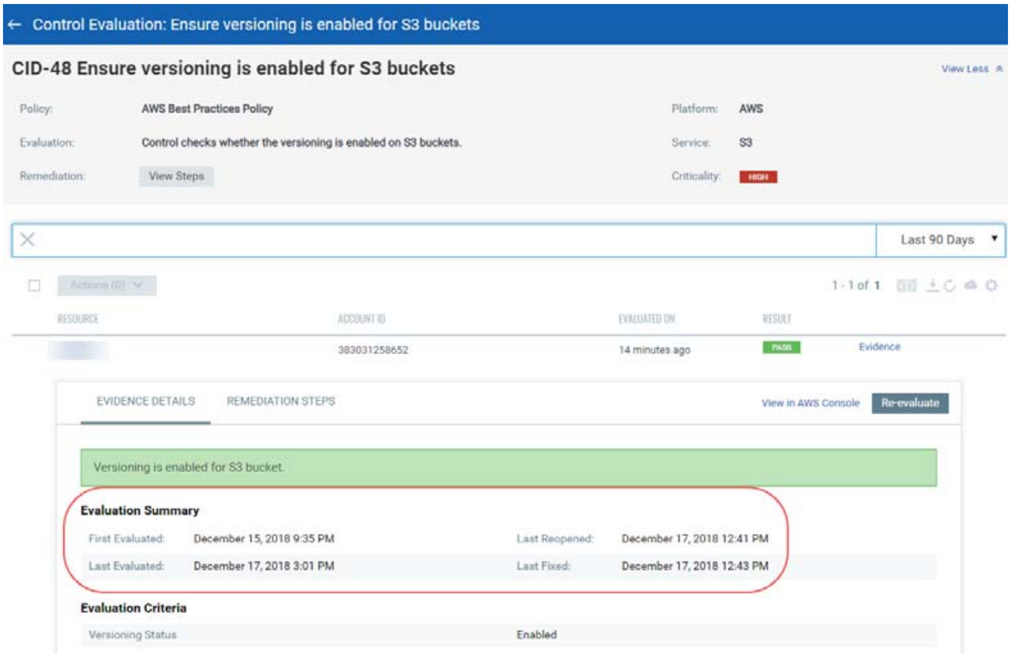
Search for evaluations

□ Actions (0)　　1 - 2 of 2

RESOURCE	ACCOUNT ID	EVALUATED ON	RESULT	
webdocsbkt	619664856109	36 minutes ago	FAIL	Evidence
cf-templates-t3vsk13r99rh-us-east-1	619664856109	36 minutes ago	PASS	Evidence

Resource Evidence

To get more details on why a resource failed, click the Evidence link to see actual values for the resource attributes.



← Control Evaluation: Ensure versioning is enabled for S3 buckets

CID-48 Ensure versioning is enabled for S3 buckets

View Less

Policy:	AWS Best Practices Policy	Platform:	AWS
Evaluation:	Control checks whether the versioning is enabled on S3 buckets.	Service:	S3
Remediation:	View Steps	Criticality:	HIGH

Last 90 Days

□ Actions (0)　　1 - 1 of 1

RESOURCE	ACCOUNT ID	EVALUATED ON	RESULT	
[redacted]	383031258652	14 minutes ago	PASS	Evidence

EVIDENCE DETAILS　REMEDIATION STEPS　　View in AWS Console　Re-evaluate

Versioning is enabled for S3 bucket.

Evaluation Summary

First Evaluated:	December 15, 2018 9:35 PM	Last Reopened:	December 17, 2018 12:41 PM
Last Evaluated:	December 17, 2018 3:01 PM	Last Fixed:	December 17, 2018 12:43 PM

Evaluation Criteria

Versioning Status	Enabled

The Evaluation Summary tells you the following facts as well:

-First Evaluated: The date when the control was evaluated for the first time.

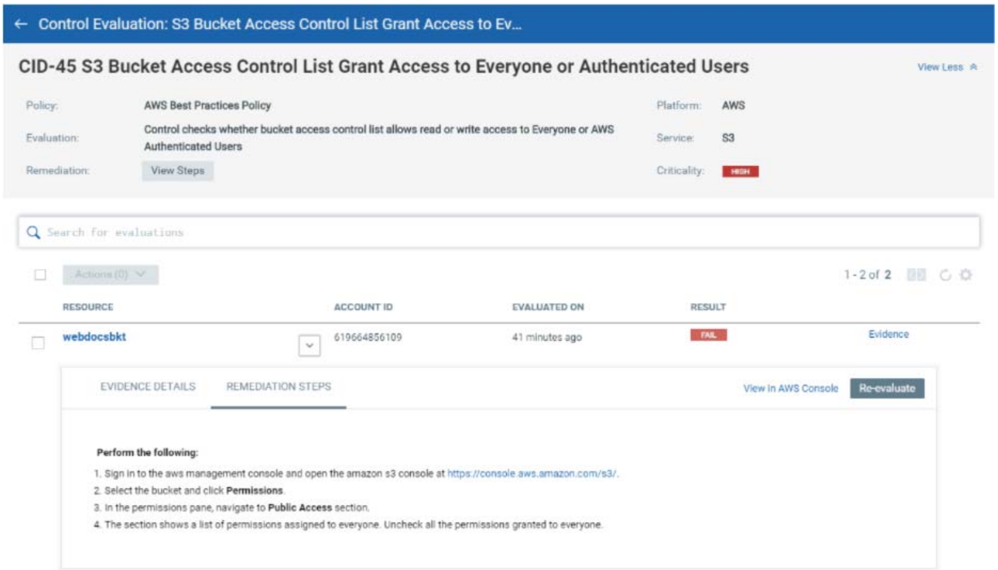
-Last Evaluated: The latest date when the control was evaluated.

-Last Reopened: The latest date when the control evaluation result is changed from pass to fail.

-Last Fixed: The latest date when the control evaluation control result is changed from fail to pass.

View Remediation Steps

Click the Remediation Steps tab to learn the steps needed to fix the failure.



CID-45 S3 Bucket Access Control List Grant Access to Everyone or Authenticated Users

Policy:	AWS Best Practices Policy	Platform:	AWS
Evaluation:	Control checks whether bucket access control list allows read or write access to Everyone or AWS Authenticated Users	Service:	S3
Remediation:	View Steps	Criticality:	HIGH

Search for evaluations

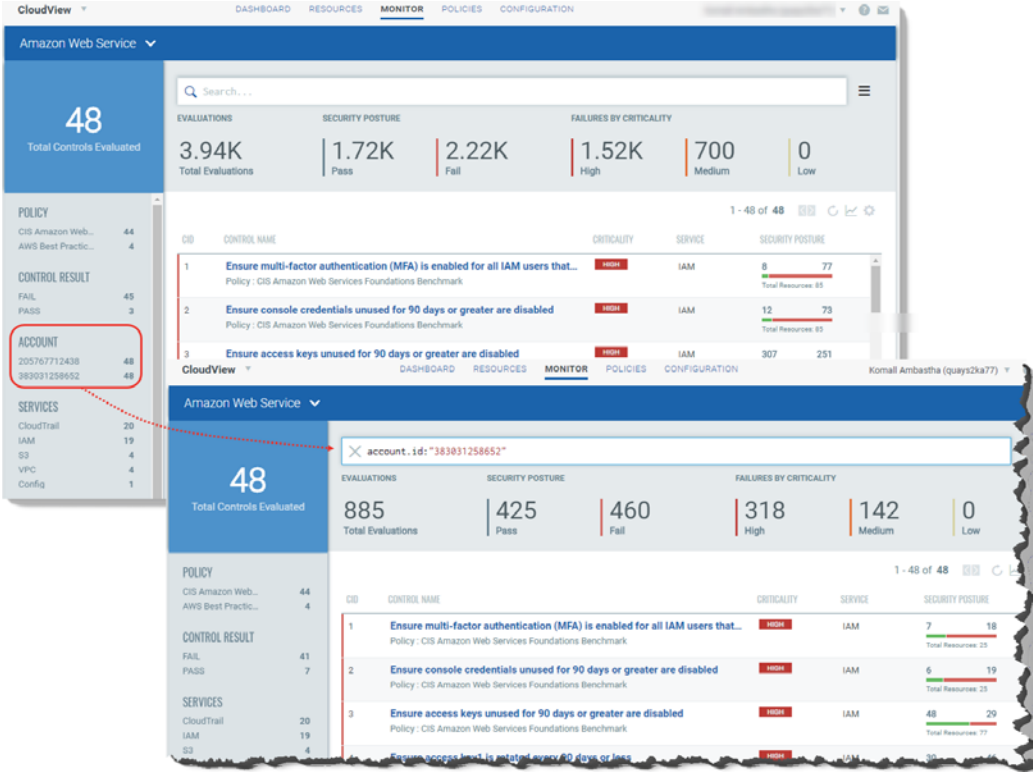
	RESOURCE	ACCOUNT ID	EVALUATED ON	RESULT	
□	webdocsbkt	619664856109	41 minutes ago	FAIL	Evidence

Perform the following:

1. Sign in to the aws management console and open the amazon s3 console at https://console.aws.amazon.com/s3/.
2. Select the bucket and click **Permissions**.
3. In the permissions pane, navigate to **Public Access** section.
4. The section shows a list of permissions assigned to everyone. Uncheck all the permissions granted to everyone.

View Control Evaluation Results per Account

Quickly view how many controls are passed/failed by clicking the account filter.



[redacted]

48
Total Controls Evaluated

EVALUATIONS	SECURITY POSTURE		FAILURES BY CRITICALITY		
3.94K Total Evaluations	1.72K Pass	2.22K Fail	1.52K High	700 Medium	0 Low

POLICY	
CIS Amazon Web...	44
AWS Best Practic...	4
CONTROL RESULT	
FAIL	45
PASS	3
ACCOUNT	
205767712438	48
383031258652	48
SERVICES	
CloudTrail	20
IAM	19
S3	4
VPC	4
Config	1

1 - 48 of 48

CID	CONTROL NAME	CRITICALITY	SERVICE	SECURITY POSTURE
1	Ensure multi-factor authentication (MFA) is enabled for all IAM users that... Policy : CIS Amazon Web Services Foundations Benchmark	HIGH	IAM	8 77 Total Resources: 85
2	Ensure console credentials unused for 90 days or greater are disabled Policy : CIS Amazon Web Services Foundations Benchmark	HIGH	IAM	12 73 Total Resources: 85
3	Ensure access keys unused for 90 days or greater are disabled	HIGH	IAM	307 251

account.id:"383031258652"

48
Total Controls Evaluated

EVALUATIONS	SECURITY POSTURE		FAILURES BY CRITICALITY		
885 Total Evaluations	425 Pass	460 Fail	318 High	142 Medium	0 Low

POLICY	
CIS Amazon Web...	44
AWS Best Practic...	4
CONTROL RESULT	
FAIL	41
PASS	7
SERVICES	
CloudTrail	20
IAM	19
S3	4

1 - 48 of 48

CID	CONTROL NAME	CRITICALITY	SERVICE	SECURITY POSTURE
1	Ensure multi-factor authentication (MFA) is enabled for all IAM users that... Policy : CIS Amazon Web Services Foundations Benchmark	HIGH	IAM	7 18 Total Resources: 25
2	Ensure console credentials unused for 90 days or greater are disabled Policy : CIS Amazon Web Services Foundations Benchmark	HIGH	IAM	6 19 Total Resources: 25
3	Ensure access keys unused for 90 days or greater are disabled Policy : CIS Amazon Web Services Foundations Benchmark	HIGH	IAM	48 29 Total Resources: 77
	Ensure access key1 is rotated every 90 days or less	HIGH	IAM	

Policies and Controls

CloudView continuously discovers resources and ensures resources are compliant in relation to respective Benchmark & Best Practices policy provided out-of box.

The Policies tab lists the policies we currently support.

AWS Best Practices Policy

CIS Amazon Web Services Foundations Benchmark

CIS Microsoft Azure Foundations Benchmark

AWS Best Practices Policy

We support controls for following AWS resources:

S3 Controls

RDS Controls

S3 Controls

CID 45: S3 Bucket Access Control List Grant Access to Everyone or Authenticated Users

CID 46: Ensure S3 Bucket Policy does not allow anonymous (public) access to S3 bucket

CID 47: Ensure access logging is enabled for S3 buckets

CID 48: Ensure versioning is enabled for S3 buckets

CID 57: Ensure that bucket policy enforces encryption in transit

RDS Controls

CID 51: Ensure that Public Accessibility is set to No for Database Instances

CID 52: Ensure DB snapshot is not publicly visible

CID 53: Ensure Encryption is enabled for the database Instance

CID 54: Ensure database Instance snapshot is encrypted

CID 55: Ensure auto minor version upgrade is enabled for a Database Instance

CID 56: Ensure database Instance is not listening on to a standard/default port

CIS Amazon Web Services Foundations Benchmark

We support controls for following AWS resources:

Identity and Access Management (IAM) Controls

CloudTrail Controls

VPC Controls

Config Controls

Identity and Access Management (IAM) Controls

CID 1: Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password

CID 2: Ensure console credentials unused for 90 days or greater are disabled

CID 3: Ensure access keys unused for 90 days or greater are disabled

CID 4: Ensure access key1 is rotated every 90 days or less

CID 5: Ensure access key2 is rotated every 90 days or less

CID 6: Ensure IAM Password Policy is Enabled

CID 7: Ensure IAM password policy requires at least one uppercase letter

CID 8: Ensure IAM password policy require at least one lowercase letter

CID 9: Ensure IAM password policy require at least one symbol

CID 10: Ensure IAM password policy require at least one number

CID 11: Ensure IAM password policy requires minimum length of 14 or greater

CID 12: Ensure IAM password policy prevents password reuse

CID 13: Ensure IAM password policy expires passwords within 90 days or less

CID 14: Ensure no root account access key exists

CID 15: Ensure MFA is enabled for the root account

CId 16: Ensure hardware MFA is enabled for the root account

CID 17: Ensure IAM policies are attached only to groups or roles

CID 18: Avoid the use of the root account

CID 26: Ensure rotation for customer created CMKs is enabled

CID 49: Ensure a support role has been created to manage incidents with AWS Support

CID 50: Ensure IAM policies that allow full administrative privileges are not created

CloudTrail Controls

CID 19: Ensure CloudTrail is enabled in all regions

CID 20: Ensure CloudTrail log file validation is enabled

CID 21: Ensure the S3 bucket CloudTrail logs to is not publicly accessible

CID 22: Ensure CloudTrail trails are integrated with CloudWatch Logs

CID 24: Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket

CID 25: Ensure CloudTrail logs are encrypted at rest using KMS CMKs

CID 27: Ensure a log metric filter and alarm exist for unauthorized API calls

CID 28: Ensure a log metric filter and alarm exist for Management Console sign-in without MFA

CID 29: Ensure a log metric filter and alarm exist for usage of "root" account

CID 30: Ensure a log metric filter and alarm exist for IAM policy changes

CID 31: Ensure a log metric filter and alarm exist for CloudTrail configuration changes

CID 32: Ensure a log metric filter and alarm exist for AWS Management Console authentication failures

CID 33: Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer created CMKs

CID 34: Ensure a log metric filter and alarm exist for S3 bucket policy changes

CID 35: Ensure a log metric filter and alarm exist for AWS Config configuration changes

CID 36: Ensure a log metric filter and alarm exist for security group changes

CID 37: Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)

CID 38: Ensure a log metric filter and alarm exist for changes to network gateways

CID 39: Ensure a log metric filter and alarm exist for route table changes

CID 40: Ensure a log metric filter and alarm exist for VPC changes

VPC Controls

CID 41: Ensure no security groups allow ingress from 0.0.0.0/0 to port 22

CID 42: Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389

CID 43: Ensure VPC flow logging is enabled in all VPCs

CID 44: Ensure the default security group of every VPC restricts all traffic

Config Controls

CID 23: Ensure AWS Config is enabled in all regions

CIS Microsoft Azure Foundations Benchmark

We support controls for following Azure resources:

Security Centre Controls

CID 50015: Ensure that standard pricing tier is selected

CID 50004: Ensure that 'Automatic provisioning of monitoring agent' is set to 'On'

CID 50005: Ensure ASC Default policy setting Monitor System Updates is not Disabled

CID 50006: Ensure ASC Default policy setting Monitor OS Vulnerabilities is not Disabled

CID 50007: Ensure ASC Default policy setting Monitor Endpoint Protection is not Disabled

CID 50008: Ensure ASC Default policy setting Monitor Disk Encryption is not Disabled

CID 50009: Ensure ASC Default policy setting Monitor Network Security Groups is not Disabled

CID 50010: Ensure ASC Default policy setting Monitor Web Application Firewall is not Disabled

CID 50016: Ensure ASC Default policy setting Enable Next Generation Firewall(NGFW) Monitoring is not Disabled

CID 50017: Ensure ASC Default policy setting Monitor Vulnerability Assessment is not Disabled

CID 50018: Ensure ASC Default policy setting Monitor Storage Blob Encryption is not Disabled

CID 50019: Ensure ASC Default policy setting Monitor JIT Network Access is not Disabled

CID 50003: Ensure ASC Default policy setting Monitor Application Whitelisting is not Disabled

CID 50014: Ensure ASC Default policy setting Monitor SQL Auditing is not Disabled

CID 50025: Ensure ASC Default policy setting Monitor SQL Encryption is not Disabled

CID 50020: Ensure that 'Security contact emails' is set

CID 50021: Ensure that security contact 'Phone number' is set

CID 50022: Ensure that 'Send me emails about alerts' is set to 'On'

CID 50023: Ensure that 'Send email also to subscription owners' is set to 'On'

Storage Accounts Controls

CID 50011: Ensure that Secure transfer required for a Storage Account is set to Enabled

CID 50012: Ensure that 'Public access level' is set to Private for blob containers

SQL Servers Controls

CID 50013: Ensure that 'Auditing' is set to 'On'

CID 50013: Ensure that 'AuditActionGroups' in 'auditing' policy for a SQL server is set properly

(This will be part of next release of CIS benchmark)

CID 50028:Ensure that 'Threat Detection' is set to 'On'

CID 50028: Ensure that 'Threat Detection types' is set to 'All'

CID 50028: Ensure that 'Send alerts to' is set

CID 50028: Ensure that 'Email service and co-administrators' is 'Enabled'

CID 50013: Ensure that 'Auditing' Retention is 'greater than 90 days'

CID 50028: Ensure that 'Threat Detection' Retention is 'greater than 90 days'

CID 50035: Ensure that Azure Active Directory Admin is configured for a SQL Server

CID 50027: Ensure SQL server's TDE protector is encrypted with BYOK (Use your own key)

(This will be part of next release of CIS benchmark)

Logging and Monitoring Controls

CID 50024: Ensure that a Log Profile exists

CID 50024: Ensure that Activity Log Retention is set 365 days or greater

CID 50024: Ensure Audit Profile Captures all the activities

(This will be part of next release of CIS benchmark)

Networking Controls

CID 50029: Disable RDP access on Network Security Groups from Internet (ANY IP)

CID 50031: Disable SSH access on Network Security Groups from Internet (ANY IP)

CID 50002: Ensure that SQL server access is restricted from the internet

Virtual Machines Controls

CID 50032: Ensure that all the vm disks are encrypted

Controls for Other Security Considerations

CID 50030: Ensure that the expiry date is set on all Secrets

CID 50026: Ensure keyvault is recoverable

(This will be part of next release of CIS benchmark)

CloudView APIs

Many CloudView features are available through REST APIs. You can use Swagger tool to access the REST APIs we support.

Accessing APIs Using Swagger

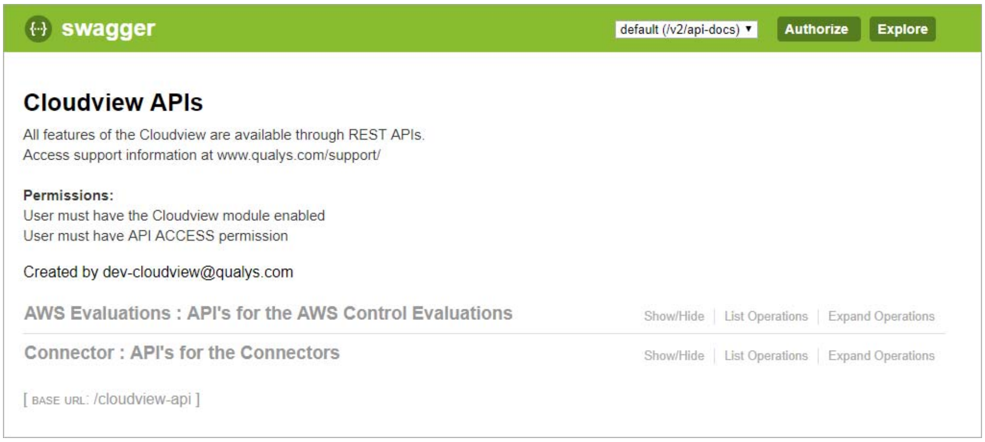
Swagger is a widely-adopted specification that allows for programmatically describing REST APIs. The Swagger UI provides all the details about the APIs and how to invoke them. This includes information like the HTTP verbs to use (GET, POST, PUT, etc.), the URL paths, allowable parameters and types, and so on.

You can directly access the Swagger UI from the following URL:

http://<QualysURL>/cloudview-api/swagger-ui.html

For example, if your account is on US Platform 2

https://qualysguard.qg2.apps.qualys.com/cloudview-api/swagger-ui.html


swagger
default (/v2/api-docs) ▾
Authorize
Explore

Cloudview APIs

All features of the Cloudview are available through REST APIs.
Access support information at www.qualys.com/support/

Permissions:
User must have the Cloudview module enabled
User must have API ACCESS permission

Created by dev-cloudview@qualys.com

AWS Evaluations : API's for the AWS Control Evaluations

Connector : API's for the Connectors

Show/Hide | List Operations | Expand Operations
Show/Hide | List Operations | Expand Operations

[BASE URL: /cloudview-api]

Qualys maintains multiple platforms. The Qualys URL that you should use for API requests depends on the platform where your account is located.

Qualys Platform URLs

Qualys US Platform 1	https://qualysguard.qualys.com
Qualys US Platform 2	https://qualysguard.qg2.apps.qualys.com
Qualys US Platform 3	https://qualysguard.qg3.apps.qualys.com
Qualys EU Platform 1	https://qualysguard.qualys.eu
Qualys EU Platform 2	https://qualysapi.qg2.apps.qualys.eu
Qualys India Platform 1	https://qualysguard.qg1.apps.qualys.in

Do I need to Authenticate?

Authentication to the Qualys Cloud Platform is necessary before you try out the APIs.

Simply, click Authorize and provide the user name and password. You can now use the APIs!

API List

Here is the list of the APIs we currently support and a short description of what you can achieve through the API.

API Objective	Operator	API Path	Description
AWS Evaluations			
Get the list of evaluations for an account	GET	https://<QualysURL>/cloudview-api/rest/1.5/aws/evaluations/{accountId}	Provide the AWS account ID (required parameter) and get the list of evaluations for AWS Controls associated with the specified AWS account. You also need to specify the page number and the number of records to be returned per page.
Get resource evaluations for an account and control	GET	https://<QualysURL>/cloudview-api/rest/1.5/aws/evaluations/{accountId}/resources/{controlId}	Get the resources evaluated for the specified AWS account ID (required parameter) and control ID (required parameter). You also need to specify the page number and the number of records to be returned per page.
Connector			
Get the list of connectors	GET	https://<QualysURL>/cloudview-api/rest/1.5/aws/connectors	Get the list of all the connectors in AWS account you specify. You also need to specify the page number and the number of records to be returned per page.
Get AWS account ID	GET	https://<QualysURL>/cloudview-api/rest/1.5/aws/connectors/qualysAwsAccountId	Get the AWS account ID of Qualys.
Get connector details	GET	https://<QualysURL>/cloudview-api/rest/1.5/aws/connectors/{connectorId}	Specify the connector ID and you can get the details of a connector.
Get error list	GET	https://<QualysURL>/cloudview-api/rest/1.5/aws/connectors/{connectorId}/errors	Get the list of errors encountered when executing a specific connector. You also need to specify the page number and the number of records to be returned per page.
Create new connector	POST	https://<QualysURL>/cloudview-api/rest/1.5/aws/connectors	Specify the connector details such as qualysAccountId, arn, externalId, and so on and create a new connector.

Update existing connector	PUT	https://<QualysURL>/cloudview-api/rest/1.5/aws/connectors/{connectorId}	Specify the connector ID and the connector details such as qualysAccountId, arn, externalId, so on to update the specified connector.
Download AWS cloud formation template	GET	https://<QualysURL>/cloudview-api/rest/1.5/aws/connectors/aws/download	Specify the External Id to be used for generating the AWS cloud formation template and download the template.
Run provided connectors	POST	https://<QualysURL>/cloudview-api/rest/1.5/aws/connectors/run	Specify the IDs of the connectors that you want to run.
Delete connectors	DELETE	https://<QualysURL>/cloudview-api/rest/1.5/aws/connectors	Delete the specified connectors. Multiple connector IDs are comma separated.

Let us see few examples to understand how the REST APIs work.

API Examples

Example 1: Get the list of all the control evaluations (passed and failed) for a specified AWS account

Request URL: GET https://<QualysURL>/cloudview-api/rest/1.5/aws/evaluations/{accountId}

Sample URL:

```
GET https://qualysguard.qg2.apps.qualys.com/cloudview-
api/rest/1.5/aws/evaluations/11111111111?pageNo=1&pageSize=50
```

where:

-accountId (required): 11111111111 is sample AWS account ID associated with the connector

-pageNo (required):1 is the page to be returned

-pageSize:50 is the number of records to be returned per page

Sample Response:

```
{
  "content": [
    {
      "controlName": "Ensure IAM Password Policy is Enabled",
      "policyName": "CIS Amazon Web Services Foundations
Benchmark",
      "criticality": "HIGH",
      "service": "IAM",
      "result": "PASS",
      "controlId": "6",
      "passedResources": 1,
      "failedResources": 0
    },
    {
     "controlName": "Ensure IAM password policy requires at least
one uppercase letter",
      "policyName": "CIS Amazon Web Services Foundations
Benchmark",
      "criticality": "HIGH",
      "service": "IAM",
      "result": "FAIL",
      "controlId": "7",
      "passedResources": 0,
      "failedResources": 1
    },
...
,
  "last": true,
  "totalPages": 1,
  "totalElements": 39,
  "sort": null,
  "first": true,
  "numberOfElements": 39,
  "size": 50,
  "number": 0
}
```

Example 2: Get the list of all the failed control evaluations for a specific AWS account

In earlier example we provided both passed and failed control for a specified AWS account. Let us now filter failed controls using following request.

Request URL: GET https://<QualysURL>/cloudview-api/rest/1.5/aws/evaluations/{accountId}?filter=control.result:{FAIL}&pageNo=1&pageSize=50

Sample URL:

```
GET https://qualysguard.qg2.apps.qualys.com/cloudview-
api/rest/1.5/aws/evaluations/11111111111?filter=control.result:FAI
L&pageNo=1&pageSize=50
```

where:

-accountId (required): 11111111111 is sample AWS account ID associated with the connector

-filter=control.result:FAIL or PASS depending on the type of control evaluations you want to filter

-pageNo (required):1 is the page to be returned

-pageSize:50 is the number of records to be returned per page

Sample Response:

```
{
  "content": [
    {
      "controlName": "Ensure IAM password policy requires at least
one uppercase letter",
      "policyName": "CIS Amazon Web Services Foundations
Benchmark",
      "criticality": "HIGH",
      "service": "IAM",
      "result": "FAIL",
      "controlId": "7",
      "passedResources": 0,
      "failedResources": 1
    },
    {
      "controlName": "Ensure IAM password policy require at least
one symbol",
      "policyName": "CIS Amazon Web Services Foundations
Benchmark",
      "criticality": "HIGH",
      "service": "IAM",
      "result": "FAIL",
      "controlId": "9",
      "passedResources": 0,
      "failedResources": 1
...
],
  "last": true,
  "totalPages": 1,
  "totalElements": 33,
  "first": true,
  "sort": null,
  "numberOfElements": 33,
  "size": 50,
  "number": 0
}
```

Example 3: Get the resources evaluated by specifying AWS account Id and control Id

Request URL: GET https://<QualysURL>/cloudview-api/rest/1.5/aws/evaluations/{accountId}?resources/{conrolId}&pageNo=1&pageSize=50

Sample URL:

```
GET https://qualysguard.qg2.apps.qualys.com/cloudview-
api/rest/1.5/aws/evaluations/11111111111/resources/44?pageNo=1&pag
eSize=50
```

where:

-accountId (required): 11111111111 is sample AWS account ID associated with the connector

-44 is the control Id

-pageNo (required):1 is the page to be returned

-pageSize:50 is the number of records to be returned per page

Sample Response:

```
{
  "content": [
    {
      "resourceId": "sg-474f6a39",
      "region": "us-west-2",
      "accountId": "11111111111",
      "evaluatedOn": "2018-07-16T05:42:16+0000",
      "evidences": [
        {
          "settingName": "Number of Inbound Rules ",
          "actualValue": "1",
          "expectedValue": ""
        },
        {
          "settingName": "Number of Outbound Rules ",
          "actualValue": "1",
          "expectedValue": ""
        }
      ],
      "resourceType": "VPC_SECURITY_GROUP",
      "result": "FAIL"
    },
    {
      "resourceId": "sg-acd511c4",
      "region": "us-east-2",
      "accountId": "11111111111",
      "evaluatedOn": "2018-07-16T05:42:19+0000",
      "evidences": [
        {
          "settingName": "Number of Inbound Rules ",
          "actualValue": "1",
          "expectedValue": ""
        },
        {
          "settingName": "Number of Outbound Rules ",
          "actualValue": "1",
          "expectedValue": ""
        }
      ],
      "resourceType": "VPC_SECURITY_GROUP",
      "result": "FAIL"
    },
```

Example 4: Create AWS connector

Request URL: POST https://<QualysURL>/cloudview-api/rest/1.5/aws/connectors

Request Body

```
{
"arn": "<specify role arn>",
"description": "<give description for the connector",
"externalId": "<external ID of your connector>",
"name": "<name for the connector>",
"qualysAccountId": "805950163170"
}
```

where:

-arn: Specify the ARN of the cross-account role you created in your AWS account.

-description is optional and you can give a short description stating the purpose of the connector you want to create.

-externalId: Specify the external ID that you have provided in AWS while creating the cross-account role.

-name is the name for the connector you want to create.

Sample Response:

```
201 Created
```

The response code 201 is returned when the connector is successfully created.

What’s more in CloudView

We also provide you with many more quick features such as downloading data in CSV format, saving your search queries, using date filters.

Role-based Access Management

Qualys CloudView is subject to Role-Based Access Control. Users are granted access to features and functions based on Roles. These Roles are a consolidate of fine grained Permissions.

A set of Permissions are grouped together as a Role. A User is assigned one, or more, Roles. The sum of the Permissions that are granted a User represent all the rights to access features and functions that a User has.

You can:

-Block or provide UI access to CloudView module

-Provide UI access to CloudView module with restricted permissions (read-only user)

-Provide full UI access to CloudView module with all permissions

Permissions: Only users with access to Administration module can create sub-users with reader role.

What can the Reader User do?

The user with reader role can

-View connectors

-Monitor controls, policies and resources

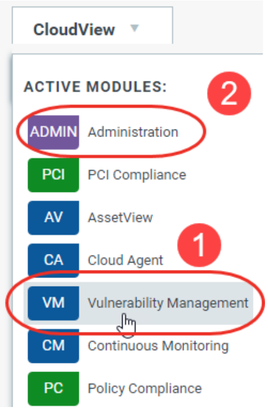
-Create and edit dashboards

However, the user with reader role cannot create connector or evaluate controls, policies.

Quick Steps

1) Create a User in Vulnerability Management (Navigate to Vulnerability Management module from module picker and then go to Users tab to create a new user).

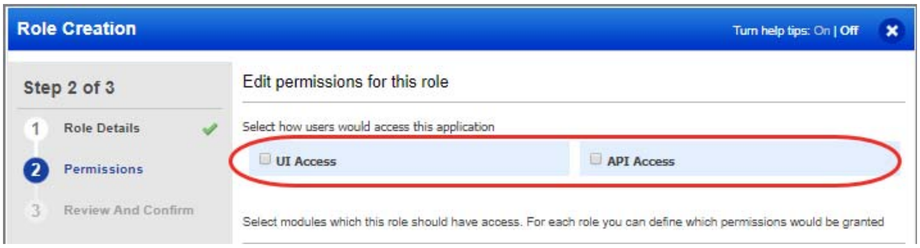
2) Create a role in Administration utility (Navigate to Administration utility from module picker and then go to Role Management tab).



Let us consider scenarios to configure different level of access for users. You could create different roles or modify permissions for an existing role.

Access

These permissions do not refer to a specific feature or function but determine if access to the interface as a whole is allowed for a user.



Edit permissions for this role

Select how users would access this application

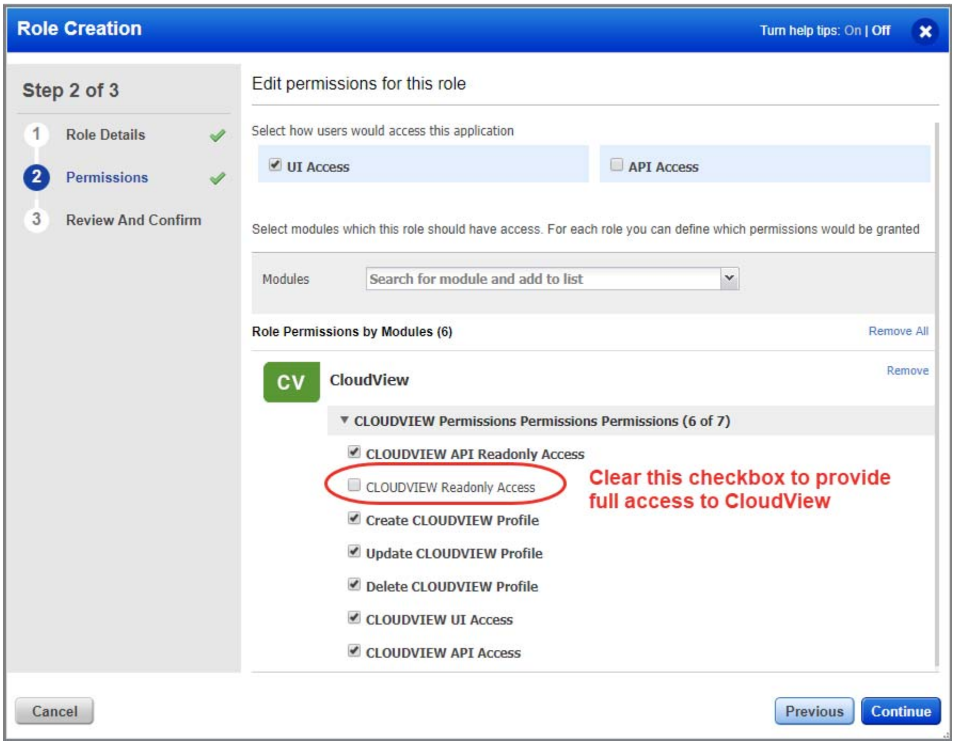
□ UI Access
□ API Access

Select modules which this role should have access. For each role you can define which permissions would be granted

UI Access: Allow or deny a given user account access to the graphical user interface. This permission must be in at least one Role for a user to be able to log into Qualys' web site and use the Qualys CloudView module.

API Access: Allow or deny a given user account access to the Application Programming Interface. This permission may impact custom integration projects that were built around a customer's Qualys service by a 3rd party.

Scenario 1: Provide full UI access to CloudView module with all permissions



Edit permissions for this role

Select how users would access this application

☑ UI Access ☐ API Access

Select modules which this role should have access. For each role you can define which permissions would be granted

Modules: Search for module and add to list

Role Permissions by Modules (6) — Remove All

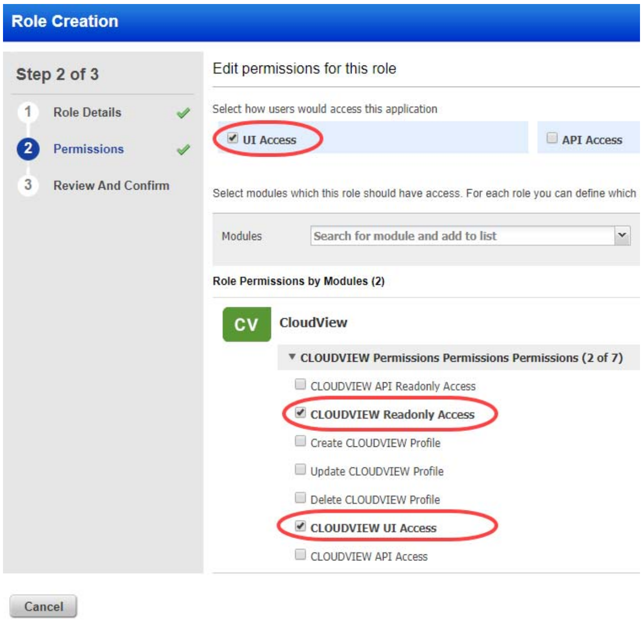
CV CloudView — Remove

▼ CLOUDVIEW Permissions Permissions Permissions (6 of 7)

- ☑ CLOUDVIEW API Readonly Access
- ☐ CLOUDVIEW Readonly Access
- ☑ Create CLOUDVIEW Profile
- ☑ Update CLOUDVIEW Profile
- ☑ Delete CLOUDVIEW Profile
- ☑ CLOUDVIEW UI Access
- ☑ CLOUDVIEW API Access

Clear this checkbox to provide full access to CloudView

Scenario 2:Provide UI access to CloudView module with restricted permissions (read-only user)



Edit permissions for this role

Select how users would access this application

☑ UI Access ☐ API Access

Select modules which this role should have access. For each role you can define which

Modules: Search for module and add to list

Role Permissions by Modules (2)

CV CloudView

▼ CLOUDVIEW Permissions Permissions Permissions (2 of 7)

- ☐ CLOUDVIEW API Readonly Access
- ☑ CLOUDVIEW Readonly Access
- ☐ Create CLOUDVIEW Profile
- ☐ Update CLOUDVIEW Profile
- ☐ Delete CLOUDVIEW Profile
- ☑ CLOUDVIEW UI Access
- ☐ CLOUDVIEW API Access

Ensure that the role has UI access permission and CLOUDVIEW Readonly Access, CLOUDVIEW UI Access enabled

Once you configure the permissions for a role, assign the role to the required users, and the users will gain access as per the configured permissions.

Download Datalist

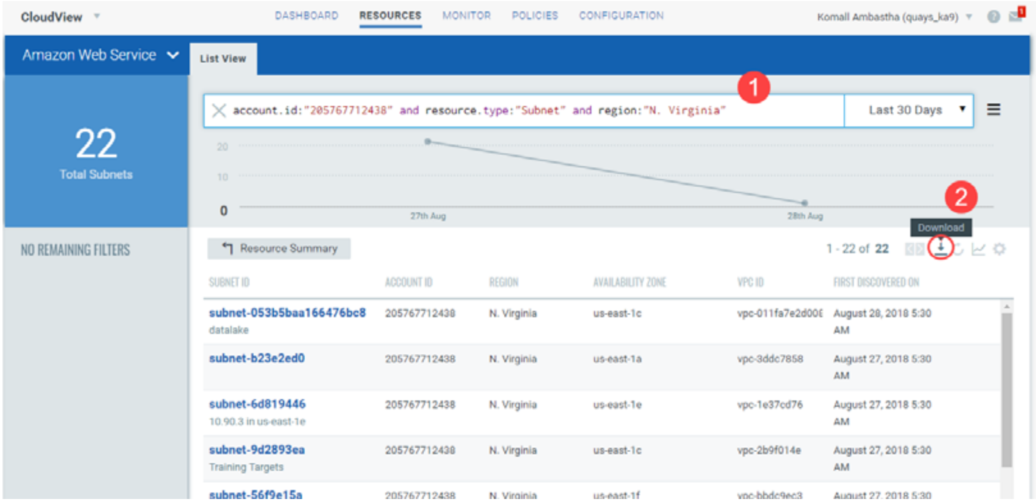
By downloading datalist to your local system you can easily manage the list outside of the Qualys platform and share them with other users. You can download results in CSV format.

The datalist that is available for download includes resources (grouped view and resource view), controls, control evaluations, and connectors list.

The download is limited to 5,000 records.

1) Use our search to narrow down your results.

2) Select Download from the Tools menu.

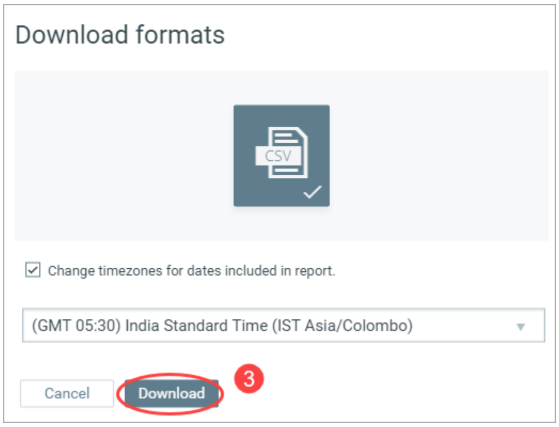


```
account.id:"205767712438" and resource.type:"Subnet" and region:"N. Virginia"
```

Last 30 Days

SUBNET ID	ACCOUNT ID	REGION	AVAILABILITY ZONE	VPC ID	FIRST DISCOVERED ON
subnet-053b5baa166476bc8 datalake	205767712438	N. Virginia	us-east-1c	vpc-011fa7e2d00	August 28, 2018 5:30 AM
subnet-b23e2ed0	205767712438	N. Virginia	us-east-1a	vpc-3ddc7858	August 27, 2018 5:30 AM
subnet-6d819446 10.90.3 in us-east-1e	205767712438	N. Virginia	us-east-1e	vpc-1e37cd76	August 27, 2018 5:30 AM
subnet-9d2893ea Training Targets	205767712438	N. Virginia	us-east-1c	vpc-2b9f014e	August 27, 2018 5:30 AM
subnet-56f9e15a	205767712438	N. Virginia	us-east-1f	vpc-bbdc9ec3	August 27, 2018 5:30

3) Click Download. That's it!



Download formats

☑ Change timezones for dates included in report.

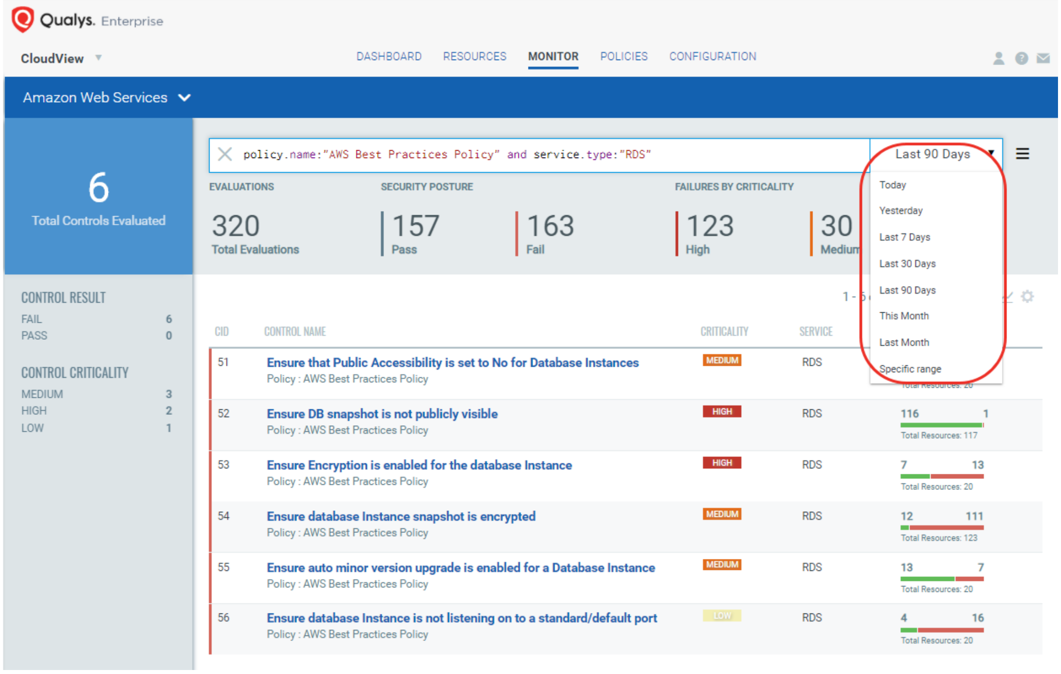
(GMT 05:30) India Standard Time (IST Asia/Colombo)

Select the Change timezones for dates included in a report checkbox and select the required timezone to convert the dates in the CSV report to the desired timezone.

Choosing Data Range

Narrow down your search results for controls using our new date filter. The new date filter provides 8 options: Today, Yesterday, Last 7 days, Last 30 days, Last 90 days, This Month, Last Month, and Specific range. Depending on the date option you choose, the search results displays controls that are evaluated within the chosen date range.

Go to Monitor tab, type your search query in the search pane and then choose the date filter to further filter your search results.



```
policy.name:"AWS Best Practices Policy" and service.type:"RDS"
```

6 Total Controls Evaluated

EVALUATIONS: 320 Total Evaluations

SECURITY POSTURE: 157 Pass | 163 Fail

FAILURES BY CRITICALITY: 123 High | 30 Medium

CONTROL RESULT

FAIL	6
PASS	0

CONTROL CRITICALITY

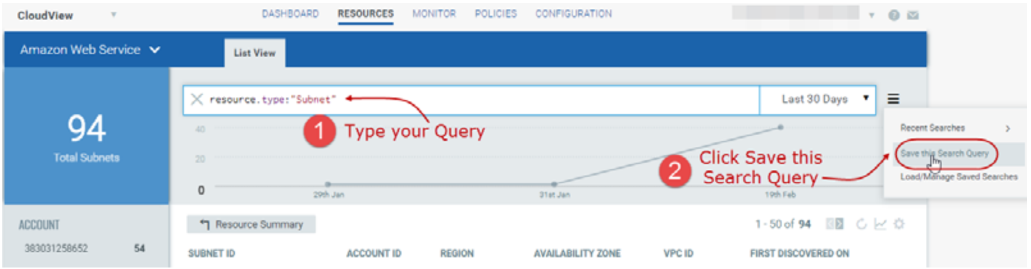
MEDIUM	3
HIGH	2
LOW	1

CID	CONTROL NAME	CRITICALITY	SERVICE	
51	Ensure that Public Accessibility is set to No for Database Instances Policy : AWS Best Practices Policy	MEDIUM	RDS	Total Resources: 20
52	Ensure DB snapshot is not publicly visible Policy : AWS Best Practices Policy	HIGH	RDS	116 1 Total Resources: 117
53	Ensure Encryption is enabled for the database Instance Policy : AWS Best Practices Policy	HIGH	RDS	7 13 Total Resources: 20
54	Ensure database Instance snapshot is encrypted Policy : AWS Best Practices Policy	MEDIUM	RDS	12 111 Total Resources: 123
55	Ensure auto minor version upgrade is enabled for a Database Instance Policy : AWS Best Practices Policy	MEDIUM	RDS	13 7 Total Resources: 20
56	Ensure database Instance is not listening on to a standard/default port Policy : AWS Best Practices Policy	LOW	RDS	4 16 Total Resources: 20

Saved Search

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

Enter your search query and then click Save this Search Query.



```
resource.type:"Subnet"
```

1 Type your Query

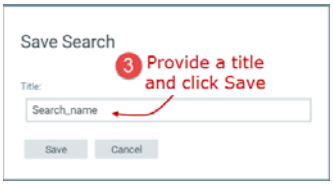
2 Click Save this Search Query

94 Total Subnets

ACCOUNT	
383031258652	54

SUBNET ID	ACCOUNT ID	REGION	AVAILABILITY ZONE	VPC ID	FIRST DISCOVERED ON

Give your search a title.

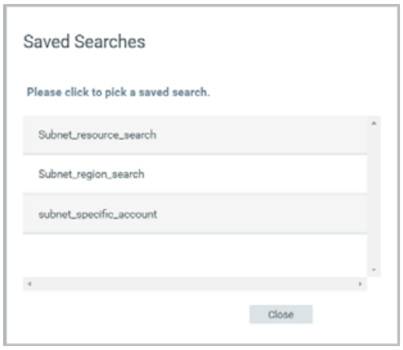


Save Search

3 Provide a title and click Save

Title: Search_name

Choose Load/manage Saved Searches to use one of the searches you previously saved.



Saved Searches

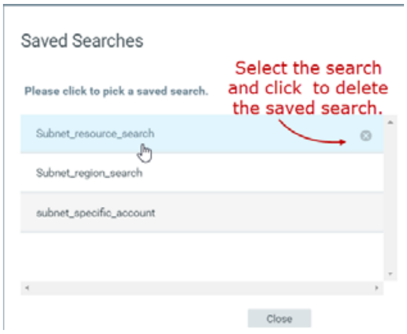
Please click to pick a saved search.

Subnet_resource_search

Subnet_region_search

subnet_specific_account

Delete any saved search you're no longer interested in.



Saved Searches

Select the search and click to delete the saved search.

Please click to pick a saved search.

Subnet_resource_search

Subnet_region_search

subnet_specific_account

Customize Dashboards

Dashboards help you visualize your assets. You can add widgets with search queries to see exactly what you're interested in. You can also export and import Dashboard and Widget configurations, from the Tools menu, to a file in a json format allowing you to share them between accounts or within the Qualys community.

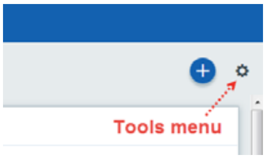
Each dashboard is a collection of widgets showing resource data of interest. You can create multiple dashboards and switch between them.

You can personalize the default dashboard - add widgets, resize them, move them around to change the layout. Use the menu to manage your dashboards.

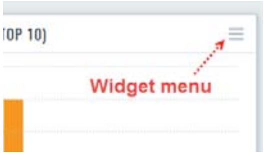
How to Take Action

Here's a quick look at your dashboard options. :

Take actions on the entire dashboard set the default, create dashboard, change layout, delete, print, export dashboard, import dashboard and import widget.



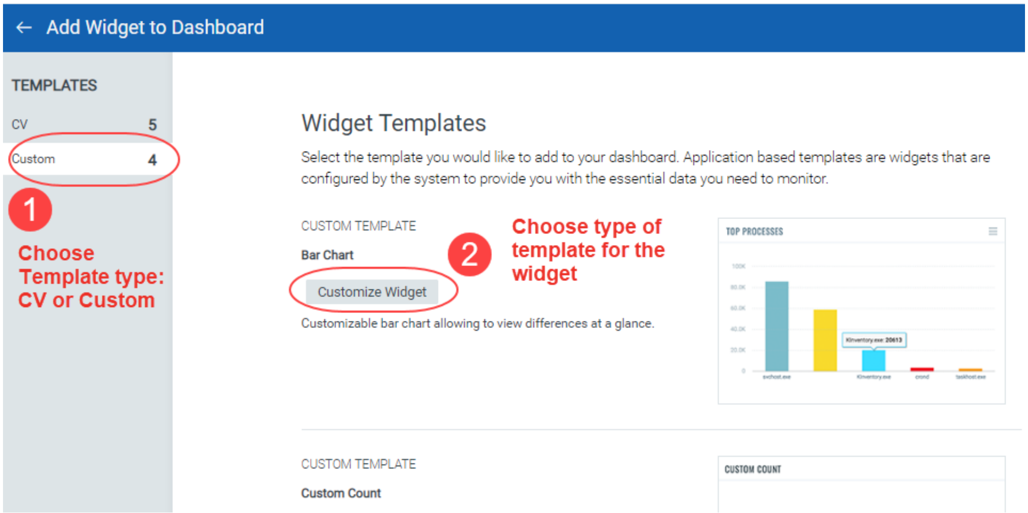
Take actions on a single widget: edit widget, delete widget, refresh widget data, create template from widget, export widget.



Adding custom widgets

1) Start by clicking the Add Widget button on your dashboard.

2) Pick one of our templates: CV pane has five default templates to choose from - or choose Custom pane to create your own widget. Let us consider an example of creating customized bar widget for Azure resources.



Widget Templates

Select the template you would like to add to your dashboard. Application based templates are widgets that are configured by the system to provide you with the essential data you need to monitor.

CUSTOM TEMPLATE

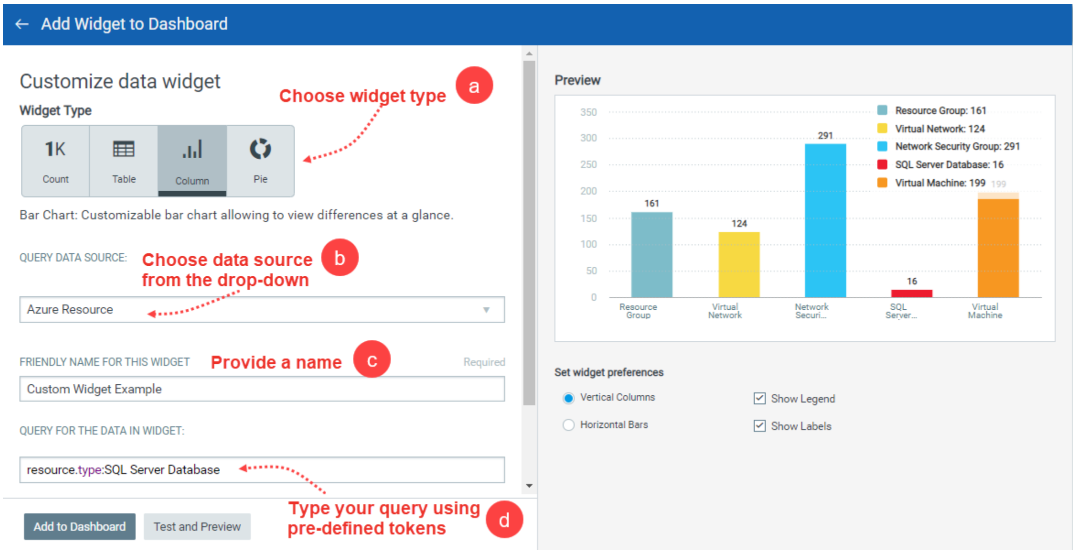
Bar Chart

Customizable bar chart allowing to view differences at a glance.

CUSTOM TEMPLATE

Custom Count

3) Each widget is unique. Define your custom settings. For some you'll select query data source, a query, group by option, limit and layout - count, table, bar graph, pie chart.



← Add Widget to Dashboard

Customize data widget

Widget Type

Choose widget type a

Bar Chart: Customizable bar chart allowing to view differences at a glance.

QUERY DATA SOURCE: Choose data source from the drop-down b

Azure Resource

FRIENDLY NAME FOR THIS WIDGET Provide a name c Required

Custom Widget Example

QUERY FOR THE DATA IN WIDGET:

resource.type:SQL Server Database

Type your query using pre-defined tokens d

Add to Dashboard | Test and Preview

Preview

Set widget preferences

● Vertical Columns ☑ Show Legend

○ Horizontal Bars ☑ Show Labels

a - Choose widget type: Count, Table, Column, Pie

b - Choose data source from the dropdown. For example: Azure Resources.

c - Provide a name for your widget.

d - Type your search query using pre-defined tokens.

The Preview pane displays the preview of your widget.

4) Click Add to Dashboard to view the widget in the dashboard. You could view the preview of the widget using the Test and Preview button.

From the Actions menu on the dashboard, you can also import and export widget configurations to a file in a json format, allowing you to share the widgets between accounts or within the Qualys community.

Resizing and layout.

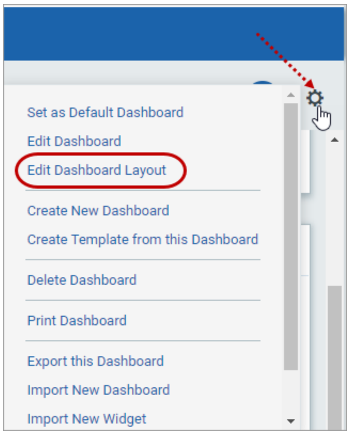
Resize any widget horizontally, drag & drop widgets to change the layout. Refresh your view.

1) Click the Tools icon on your dashboard.

2) Select Edit Dashboard Layout

3) Adjust the width for any widget or drag the widget to a new location.

4) Click OK to save your changes.



Refresh your view

You might want to see the latest data for a particular widget. Select the widget menu and choose Refresh.

To refresh all widgets in one go, choose the Refresh Dashboard option from the Tools menu and all the widgets on the dashboard will be refreshed.

Configure number of Resources, Controls

You might also want to choose the number of resources or controls displayed in your Live Feed widget. You can choose to display: Top 10, Top 5, or Top 3 failed controls or resources.