Qualys.

CloudView

User Guide

July 12, 2021

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

Table of Contents

About this Guide

Welcome to Qualys CloudView! We'll help you get acquainted with the Qualys solutions for securing your AWS, Azure, and GCP 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 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, Azure, GCP policies

- Continuously assess and report resource misconfigurations 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

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

- Administration

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.
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

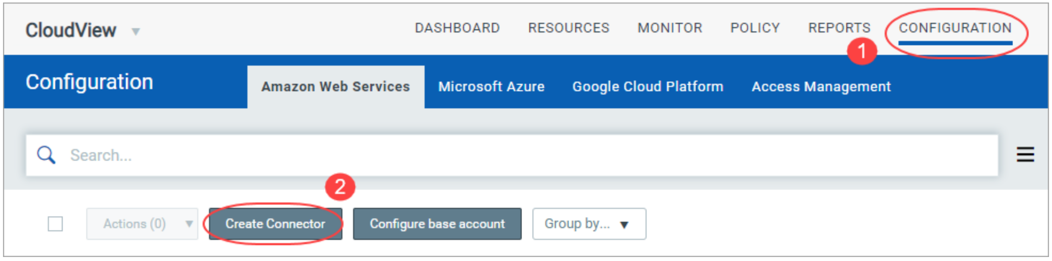
Configure AWS connectors for gathering resource information from your AWS account. It just takes a couple of minutes.

Base Account

The AWS connectors uses Qualys accounts to query the AWS APIs. If you do not wish to use the Qualys accounts, you can use the base account feature to use your own AWS account for AWS API queries from CloudView. You need to configure your AWS account ID and user credential for each base account type. For more information, refer to Base Account.

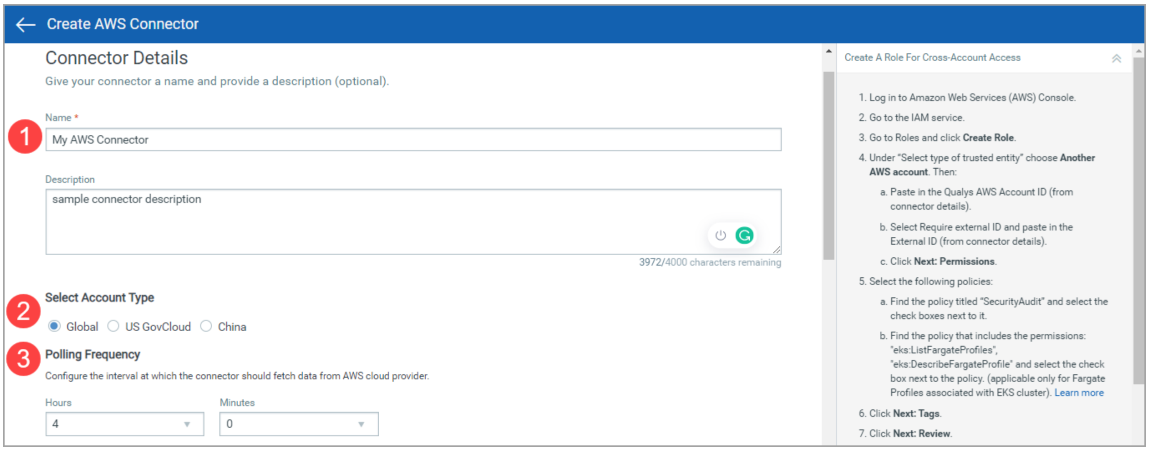
Steps to Create AWS Connector

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



Provide a name and description (optional) for your connector. Select an account type for your connector: Global, US GovCloud or China. You can choose only one account type per connector.

> Note: If you plan to use connector for China account type, ensure that you set up a base account. For more information, refer to Base Account.



Create AWS Connector

Connector Details

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

Name *: My AWS Connector

Description: sample connector description

3972/4000 characters remaining

Select Account Type

● Global ○ US GovCloud ○ China

Polling Frequency

Configure the interval at which the connector should fetch data from AWS cloud provider.

Hours: 4

Minutes: 0

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. Select the following policies:
   a. Find the policy titled "SecurityAudit" and select the check boxes next to it.
   b. Find the policy that includes the permissions: "eks:ListFargateProfiles", "eks:DescribeFargateProfile" and select the check box next to the policy. (applicable only for Fargate Profiles associated with EKS cluster). Learn more
6. Click **Next: Tags**.
7. Click **Next: Review**.

Select a frequency at which the connector should poll the cloud provider and fetch data. By default, the connector polling frequency is configured for every 4 hours. As a result, the connector will connect with the cloud provider every 4 hours to fetch the data.

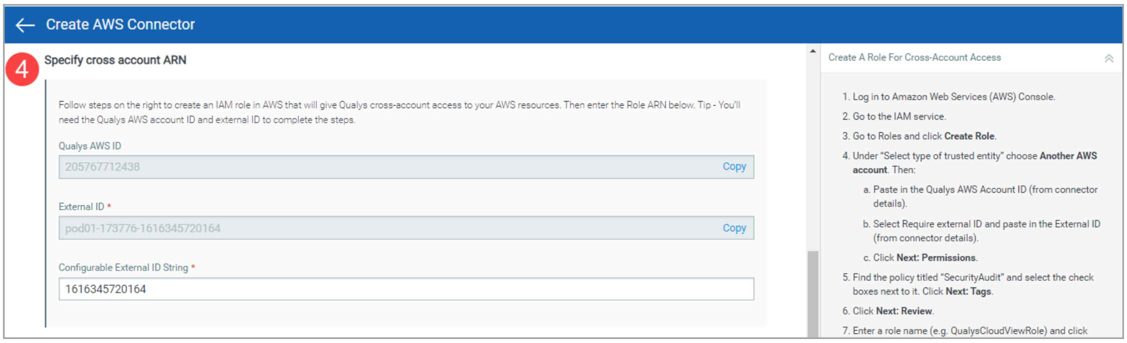
You can configure frequency from minimum one hour to maximum 24 hours. We recommend that you configure frequency of 4 hours or more for optimal use of your connector.

Configuring a low polling frequency (lesser than 4 hours) can affect the performance of the connector and may result in AWS API throttling error.

> **Note**:
> - If you trigger Run for the connector from the quick actions menu, the scheduled connector polling (as per the configured frequency) remains unaffected.
> - Configuration of connector polling frequency is enabled only for Cloud Security Assessment (CSA) users.

Now, 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.

To adhere to the AWS vendor requirement best practices, we have modified the format of the external ID. AWS requires that vendors provide a unique external ID value amongst all their customers when providing a vendor account for a trust relationship. To accommodate this requirement and provide flexibility to our customers we have implemented the below external ID format. The external ID consists of three parts. Two parts are pre-set by Qualys and the third part is editable by the customer.



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 ID: 205767712438 Copy

External ID *: pod01-173776-1616345720164 Copy

Configurable External ID String *: 1616345720164

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 boxes next to it. Click **Next: Tags**.
6. Click **Next: Review**.
7. Enter a role name (e.g. QualysCloudViewRole) and click

External ID format: <Qualys POD>-<Qualys Subscription ID>-<random alphanumeric number>

where,

Qualys POD (preset by Qualys) refers to the Qualys Platform associated with your Qualys subscription. View Qualys Platform Identifier to know more about Qualys platforms.

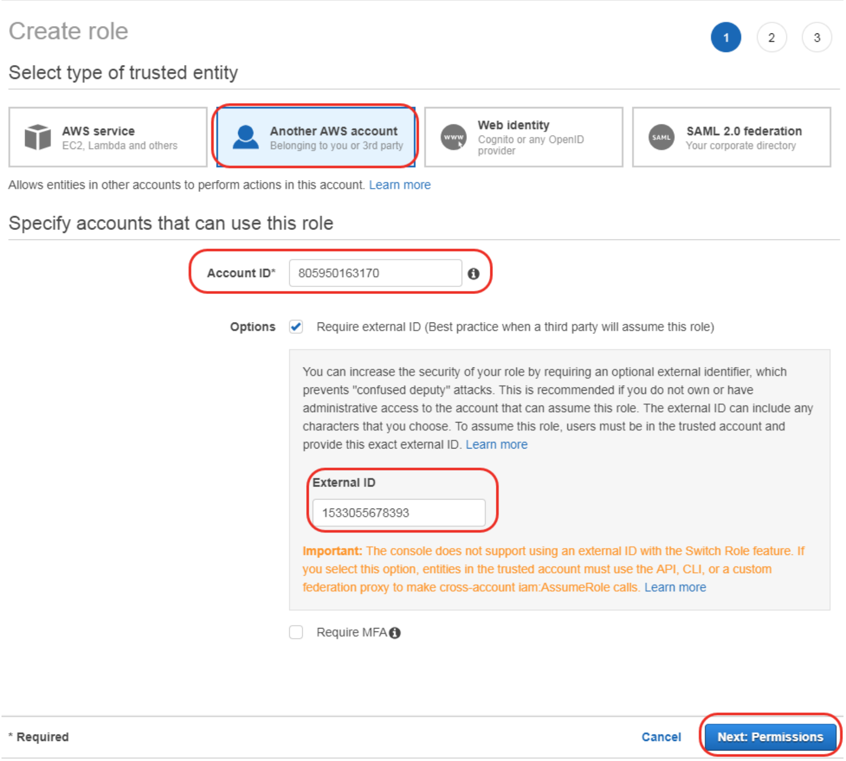
Qualys Subscription ID (preset by Qualys): Your unique Qualys Subscription ID.

random alphanumeric number: You can use a combination of alphabets (a-z, A-Z) and numbers without spaces to generate the unique number. You could use minimum 2 or maximum 1024 digits to complete the external ID combination in the new format. The special characters supported are: = , . @ : / .

Note: Special characters are not permitted in the random number.

IMPORTANT: All previously created connectors continue to work as configured. If the customer has to update a connector or create a new connector, they need to provide the external ID in the new format.

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.



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

□ Require MFA

* Required

Ensure that you do not opt for Require MFA option when you create a cross-account role for CloudView.

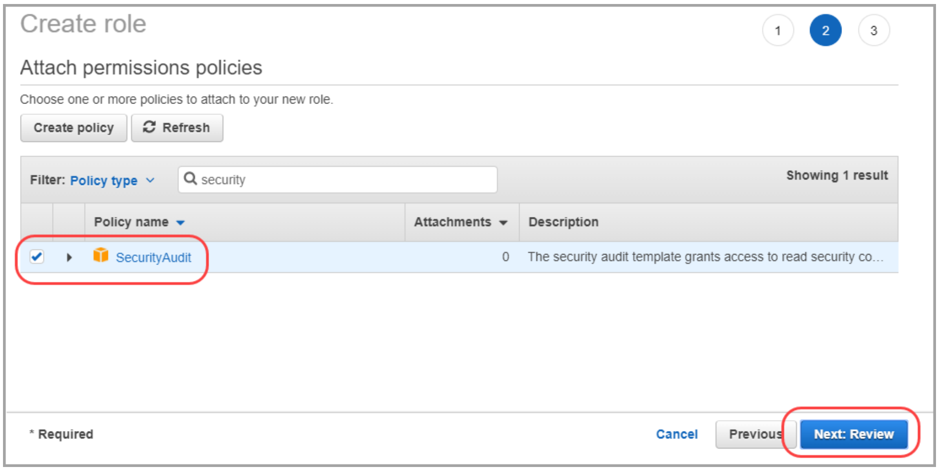
Select the following policies:

a) Find the policy titled “SecurityAudit” and select the check box next to it. Show me

b) Create a policy that includes the permissions: "eks:ListFargateProfiles", "eks:DescribeFargateProfile". Once you create the policy, find the policy and select the check box next to the policy. For detailed steps on the policy creation, see Permissions for Fargate Profile.

Note: You need the additional permissions only if you have FargateProfile resources in your cloud environment.

Click Next: tags and then Next: Review.



Create role

Attach permissions policies

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

Filter: Policy type

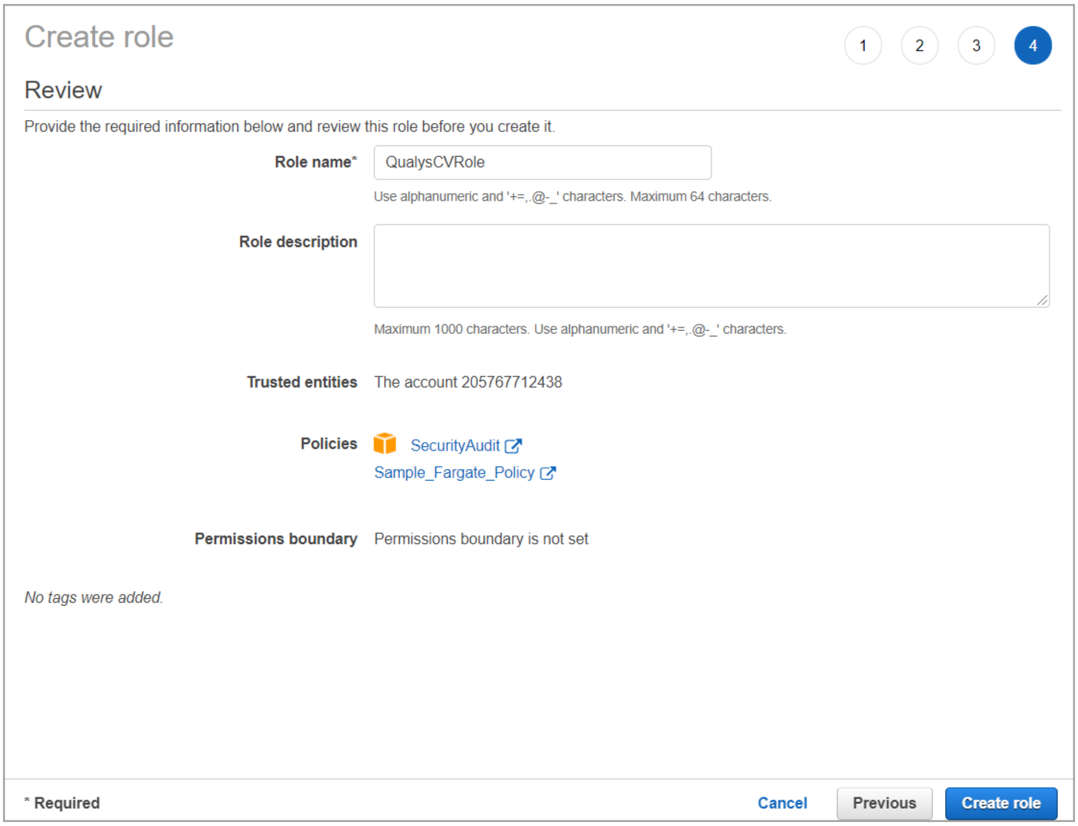
security

Showing 1 result

		Policy name	Attachments	Description
☑	▸	SecurityAudit	0	The security audit template grants access to read security co…

* 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.



Create role

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 205767712438

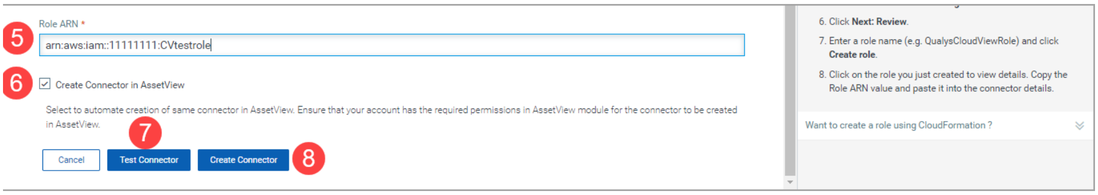
Policies SecurityAudit
Sample_Fargate_Policy

Permissions boundary Permissions boundary is not set

No tags were added.

* Required

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



Role ARN *

arn:aws:iam::11111111:CVtestrole

☑ Create Connector in AssetView

Select to automate creation of same connector in AssetView. Ensure that your account has the required permissions in AssetView module for the connector to be created in AssetView.

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 ?

Select Create Connector in AssetView check box (optional). Selecting this check box will ensure that a replica of the current connector is created and available in AssetView module. This will save the efforts of connector creation steps in AssetView module.

Pre-requisite Permission: User needs access to EC2 Connector page in AssetView module and 'Manage Asset Data Connectors' permission enabled in AssetView permissions.

Click Test Connector to verify if the connector can assume the provided role (created by user) and successfully authenticate in AWS cloud environment. If the test connection is successful, proceed with the connector creation process. If the test connection fails, you may need to check and update the credentials you provided for the connection to work.

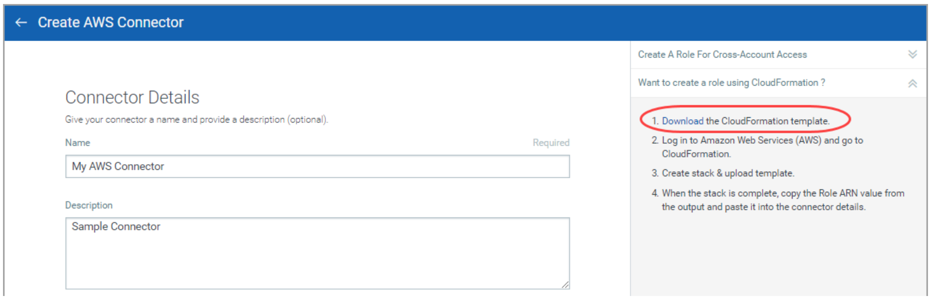
> Note: Ensure that you have all the pre-requisite permissions, correct cross-account role with necessary associated policies with the connector to successfully fetch resource details.

Then click Create Connector.

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

Want to create a role using CloudFormation?

Download the CloudFormation template from the Create AWS Connector window.



Connector Details

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

Name: My AWS Connector (Required)

Description: Sample Connector

Create A Role For Cross-Account Access

Want to create a role using CloudFormation ?

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 y downloading previously uploaded template file. When the stack is complete, copy the Role ARN from the output and paste it into the connector details.

Base Account

The AWS connectors uses Qualys accounts to query the AWS APIs. If you do not wish to use the Qualys accounts, you can use the base account feature to use your own AWS account for AWS API queries from CloudView. You need to configure your AWS account ID and user credential for each base account type.

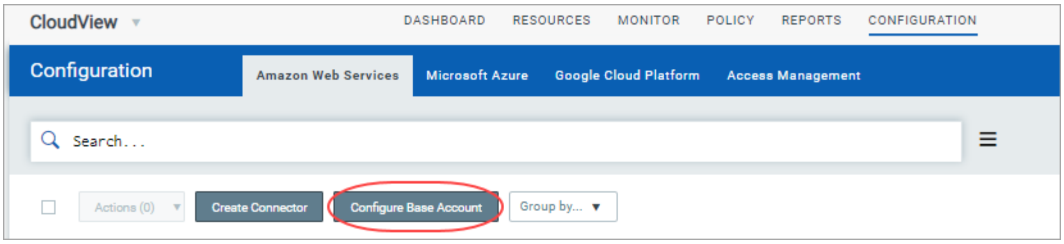
For example, you have 3 AWS accounts: Central Security Account, Production and Development. You can designate the Central Security Account as a base account to set up an AWS connector in CloudView to pull the resources from Production & Development account.

Create Base Account

Before you create a new connector, create a base account for the same account type (region). If you do not create a base account, you can still create a connector using Qualys account.

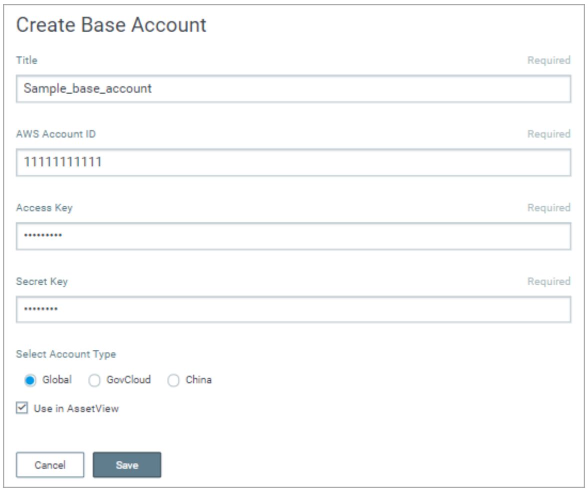
To create an AWS connector that uses your account to query the AWS APIs, you must first configure a base account of the same account type (Global, GovCloud, China). If you do not create a base account, you can still create a connector but it will use Qualys account to query the AWS APIs.

Go to Configuration > Amazon Web Services and then click Configure Base Account.



Click Create and provide title, AWS account ID, access and secret keys.

Select the account type. You can create only one base account per account type.


Create Base Account

Title Required
Sample_base_account

AWS Account ID Required
11111111111

Access Key Required
•••••••••

Secret Key Required
••••••••

Select Account Type
● Global ○ GovCloud ○ China

☑ Use in AssetView

Cancel Save

Ensure that user of the AWS account ID for which you configure that base account has policies associated in the AWS console. For more information on steps in AWS console, refer to Base Account Configuration in AWS Console.

(4) Select the Use in AssetView option to enable configured base account to be available in the AssetView App as well. This will save you from creating a separate base account in AssetView.

Edit Base Account

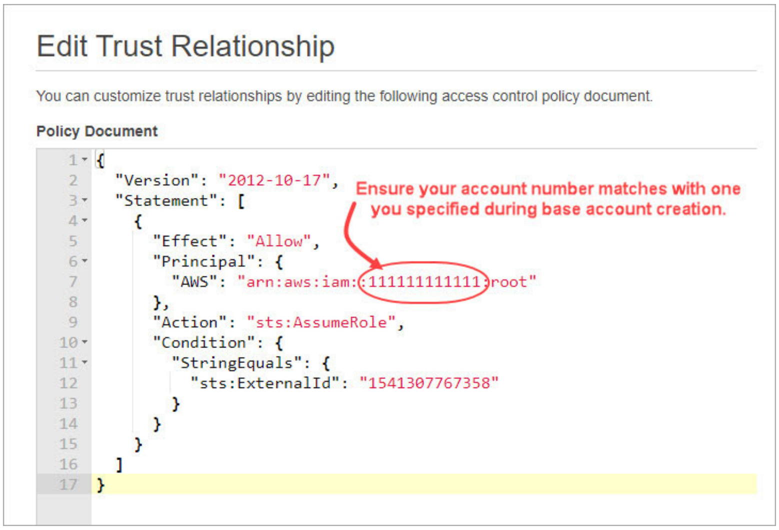
Select the base account you want to edit and click the quick action menu, then select Edit. You can edit name, AWS account ID, access keys and secret keys. You cannot edit the account type.

Updating Existing Connectors to Use Base Account

To update the existing AWS connectors using Qualys account to base account usage, you need to

-create a base account using AWS account ID

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



Edit Trust Relationship

You can customize trust relationships by editing the following access control policy document.

Policy Document

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111111111111:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "1541307767358"
        }
      }
    }
  ]
}
```

Ensure your account number matches with one you specified during base account creation.

Once you update the corresponding policy, all your existing connectors using the corresponding IAM role will be automatically upgraded to the configured base account.

What happens if I delete the base account?

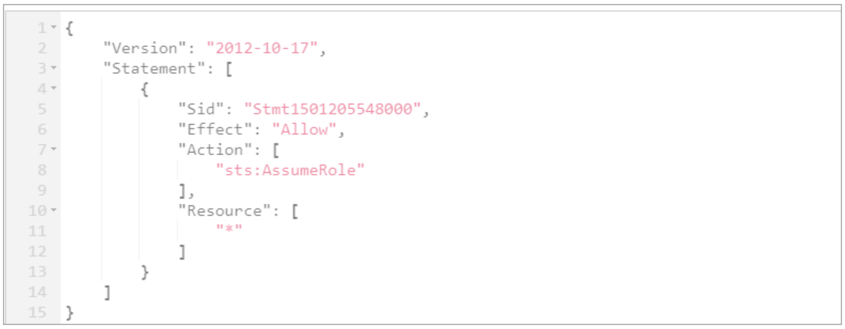
If you delete a base account, all the connectors that are associated with the base account will be automatically updated to Qualys account in Qualys Cloud Platform. However you need to go to your AWS account, update the account id in Trusted Entities of the IAM roles from base account ID to Qualys account ID.

Base Account Configuration in AWS Console

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

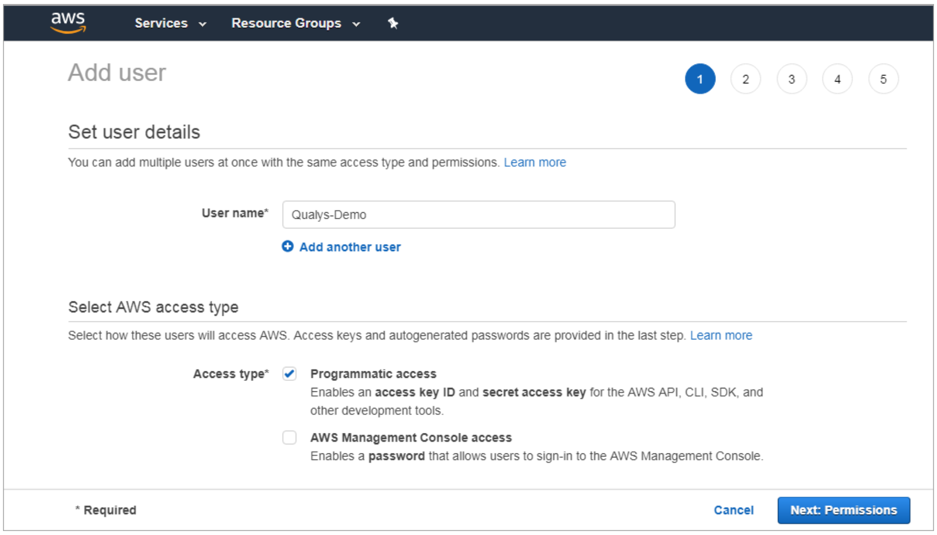
Create IAM User and associate policy in AWS

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



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

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



Add user

Set user details

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

User name* Qualys-Demo

Add another user

Select AWS access type

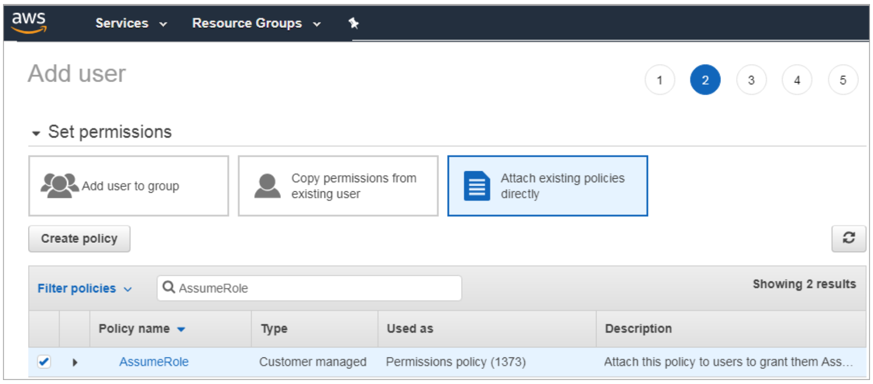
Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

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

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

* Required

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



		Policy name	Type	Used as	Description
☑	▸	AssumeRole	Customer managed	Permissions policy (1373)	Attach this policy to users to grant them Ass…

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

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

Permissions for Fargate Profile

To fetch information about Fargate profile resources, additional permissions are required. You need to assign additional permissions to the IAM role associated with the AWS connector to fetch information about the Fargate profile resources in your cloud environment.

You can create a new policy with the required permissions and attach the policy to the IAM role associated with the AWS connector.

Create the policy

1 - Log in to your Amazon Web Services (AWS) IAM console at https://console.aws.amazon.com/iam/ with user that has administrator permissions.

2 - In the navigation pane, choose Policies.

3 - In the content pane, choose Create policy.

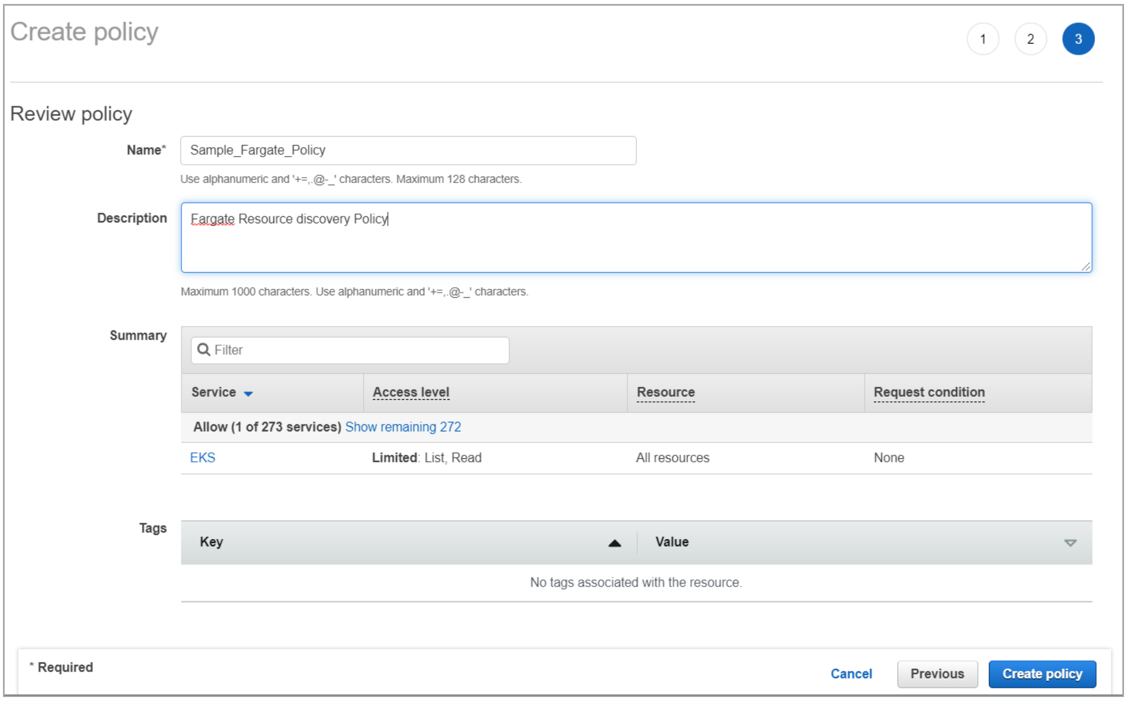
4 - Choose the JSON tab. Paste the following text into the JSON text box.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "InventoryPermissions",
            "Effect": "Allow",
            "Action": [
                "eks:ListFargateProfiles",
                "eks:DescribeFargateProfile"
```

```
                  ],
                  "Resource": "*"
              }
          ]
      }
```

5 - Click Next: Tags.

6 - Provide a name and description for the policy and then click Create policy. For example, let us create Sample_Fargate_Policy.



Create policy

Review policy

Name* Sample_Fargate_Policy

Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.

Description Fargate Resource discovery Policy

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

Summary

Service	Access level	Resource	Request condition
Allow (1 of 273 services) Show remaining 272			
EKS	**Limited**: List, Read	All resources	None

Tags

Key	Value
No tags associated with the resource.	

* Required

The policy is created with required permissions. The next steps is to associate the policy with the IAM role associated with the connector.

Attach Policy To The IAM Role

Once you create the policy, attach it with the role associated with the connector.

1 - Log in to your Amazon Web Services (AWS) IAM console at https://console.aws.amazon.com/iam/ with user that has administrator permissions.

2 - In the navigation pane, choose Roles.

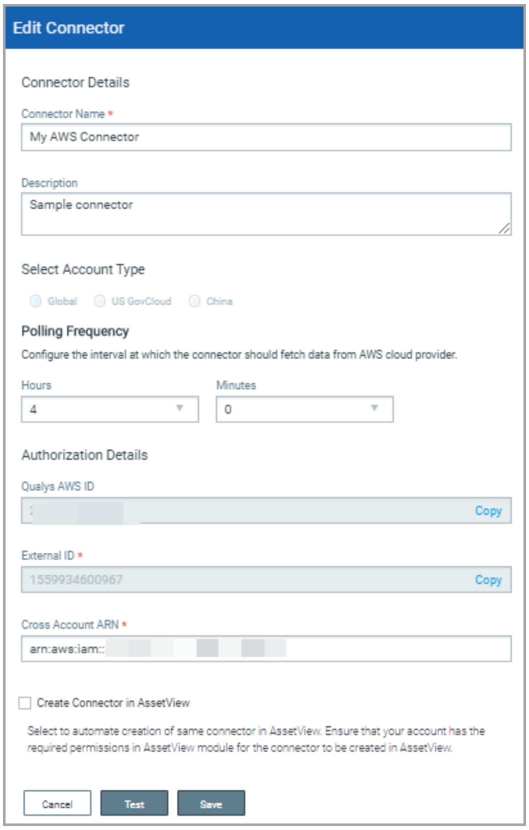
3 - Select the IAM Role being used by the connector.

4 - Choose the Permissions tab and click Attach Policies.

5 - Find the policy you created (example: Sample_Fargate_Policy) and click Attach Policy.

Editing AWS Connectors

Go to Configuration > Amazon Web Services and select the connector for which you would want to edit the details. From the quick actions menu, select View and go to Connector Information tab and click Edit.



Edit Connector

Connector Details

Connector Name *

My AWS Connector

Description

Sample connector

Select Account Type

● Global ○ US GovCloud ○ China

Polling Frequency

Configure the interval at which the connector should fetch data from AWS cloud provider.

Hours: 4

Minutes: 0

Authorization Details

Qualys AWS ID

[redacted] Copy

External ID *

1559934600967 Copy

Cross Account ARN *

arn:aws:iam::[redacted]

□ Create Connector in AssetView

Select to automate creation of same connector in AssetView. Ensure that your account has the required permissions in AssetView module for the connector to be created in AssetView.

You can now edit the required details.

Once you update the required details, you can click Test to verify if the connection to the AWS cloud provider is successful with the details you updated. If the test connection is successful, click Save and proceed.

If the test connection fails, you may need to check and update the credentials you provided for the connection to work.

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
- Lambda Function
- RDS
- EBS Volume
- EKS Cluster
- EKS Node Group
- EKS Fargate Profile

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

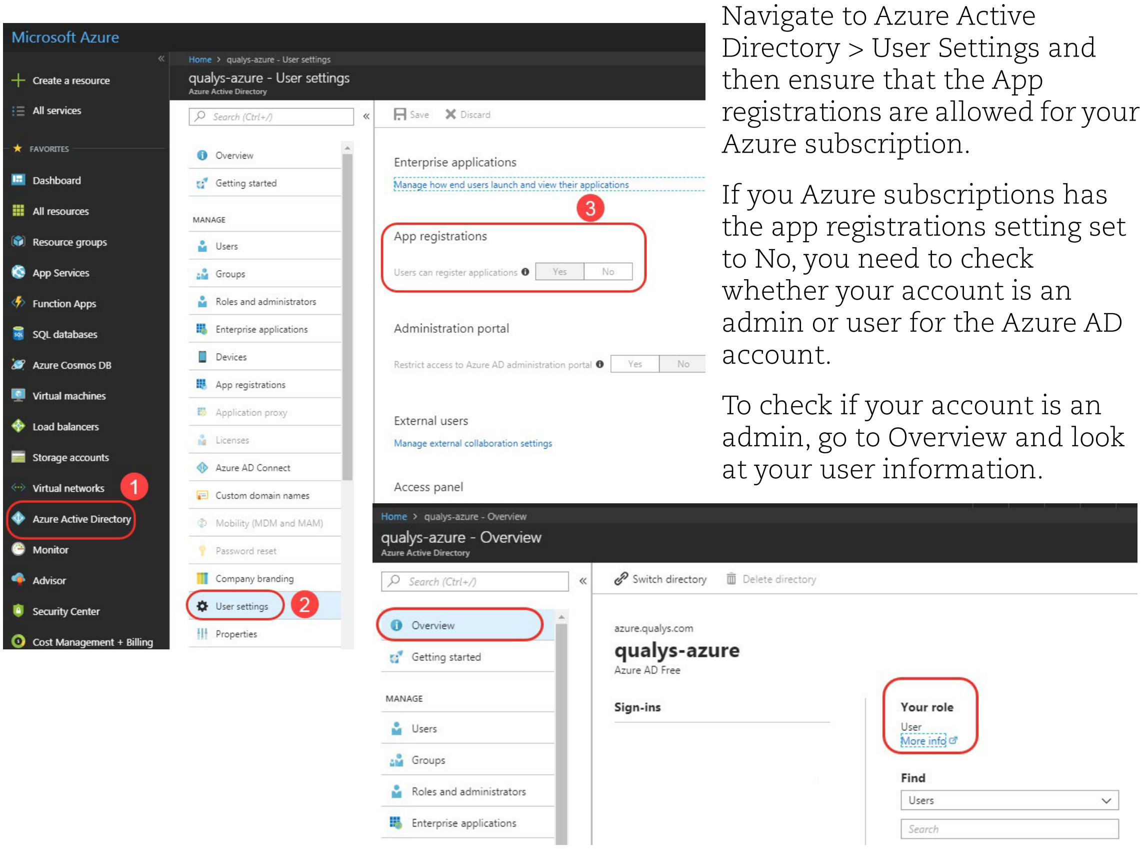
- Check Azure Subscription permissions to assign the application to a role in your Azure subscription

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.

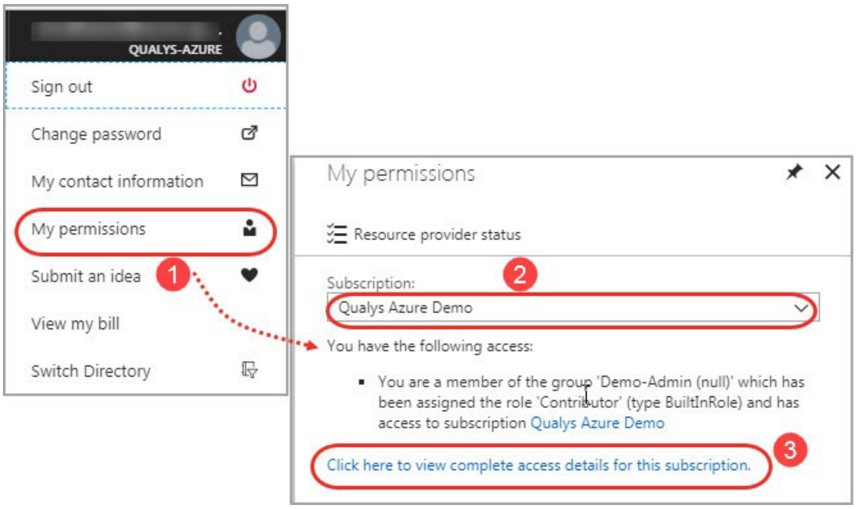


If your account is assigned to the User role, but the app registration setting is restricted to admin users, you will not be permitted to register new apps. In such case, ask your administrator to either assign you to the global administrator role, or to enable users to register apps.

Check Azure Subscription permissions

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

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.

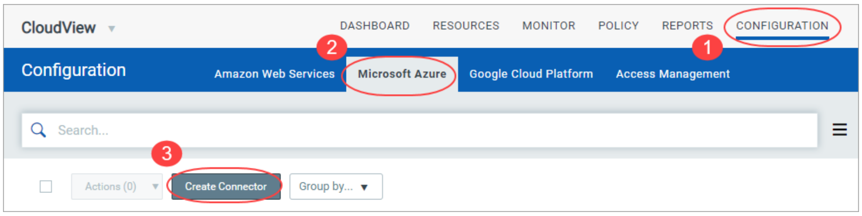


You have the following access:

- 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

Steps to Create Azure Connector

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



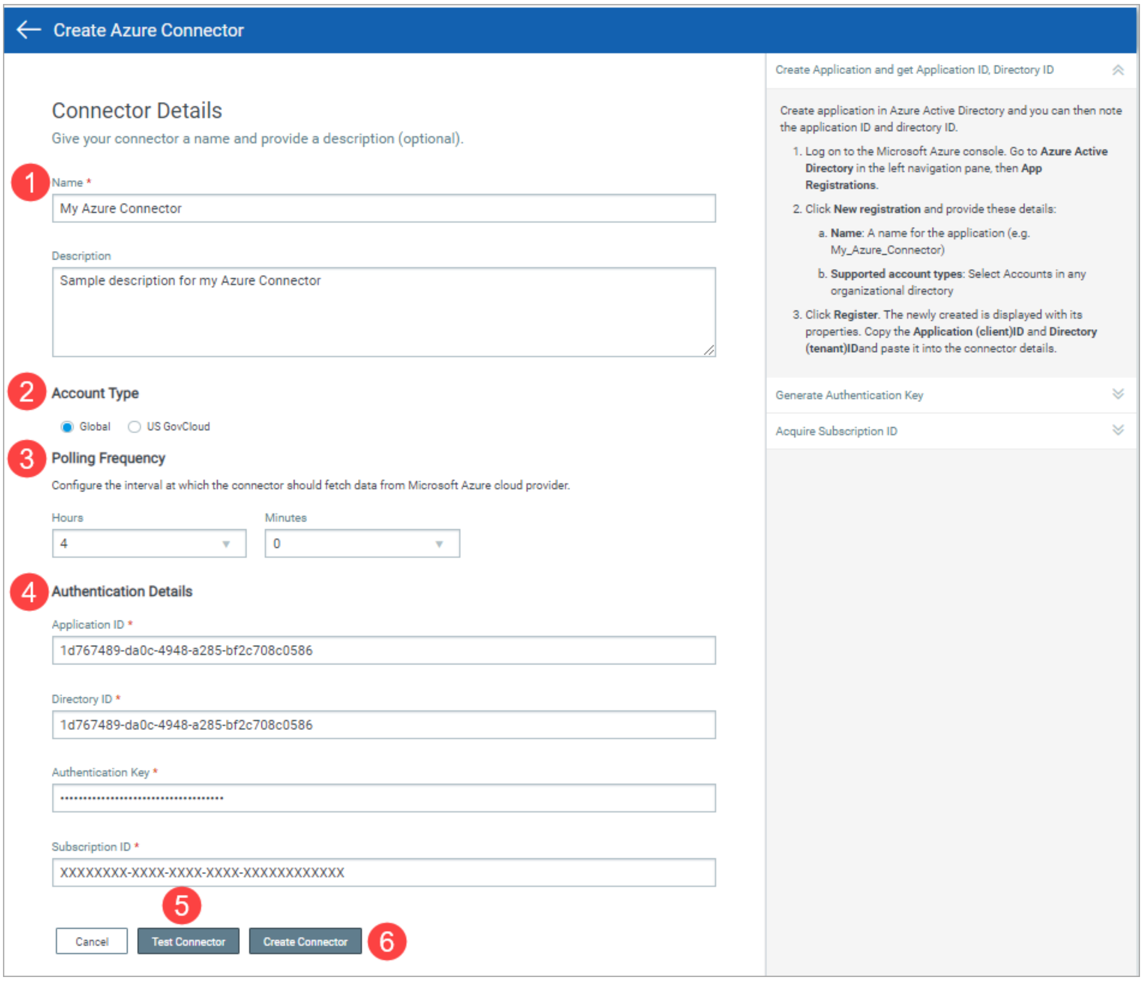
Provide a name and description (optional) for your connector. Select an account type for your connector: Global or US GovCloud. You can choose only one account type per connector

Configure a polling frequency. The polling frequency for a connector decides the rate at which the connector should poll the cloud provider and fetch the data.

Select a frequency at which the connector should poll the cloud provider and fetch data. By default, the connector polling frequency is configured for every 4 hours. As a result, the connector will connect with the cloud provider every 4 hours to fetch the data.

You can configure frequency from minimum one hour to maximum 24 hours. We recommend that you configure frequency of 4 hours or more for optimal use of your connector. Configuring a low polling frequency (lesser than 4 hours) can affect the performance of the connector and may result in Microsoft Azure API throttling error.

> Note:
> - If you trigger Run for the connector from the quick actions menu, the scheduled connector polling (as per the configured frequency) remains unaffected.
> - Configuration of connector polling frequency is enabled only for Cloud Security Assessment (CSA) users.



Connector Details

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

Name *: My Azure Connector

Description: Sample description for my Azure Connector

Account Type

● Global ○ US GovCloud

Polling Frequency

Configure the interval at which the connector should fetch data from Microsoft Azure cloud provider.

Hours: 4

Minutes: 0

Authentication Details

Application ID *: 1d767489-da0c-4948-a285-bf2c708c0586

Directory ID *: 1d767489-da0c-4948-a285-bf2c708c0586

Authentication Key *: ••••••••••••••••••••••••••••••••••••

Subscription ID *: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX

Create Application and get Application ID, Directory ID

Create application in Azure Active Directory and you can then note the application ID and directory 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 registration** and provide these details:
   a. **Name**: A name for the application (e.g. My_Azure_Connector)
   b. **Supported account types**: Select Accounts in any organizational directory
3. Click **Register**. The newly created is displayed with its properties. Copy the **Application (client)ID** and **Directory (tenant)ID**and paste it into the connector details.

Next, you need to configure the application ID, directory ID, authentication key and subscription ID from the Microsoft Azure console to paste into your connector details. To view the detailed configuration steps, refer to Configuration Steps on Microsoft Azure console section.

Click Test Connector to verify if the connector can successfully authenticate using the provided service principal credentials in Microsoft Azure cloud environment.

If the test connection is successful, proceed with the connector creation process. If the test connection fails, you may need to check and update the authentication details you provided for the connection to work.

> Note: Ensure that you have provide the correct authentication details that are set up as per the steps listed for the connector to successfully fetch resource details.

Click Create Connector.

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

Configuration Steps on Microsoft Azure console

Let us see the steps needed to be configured on Microsoft Azure Portal:

Create Application and get Application ID, Directory ID

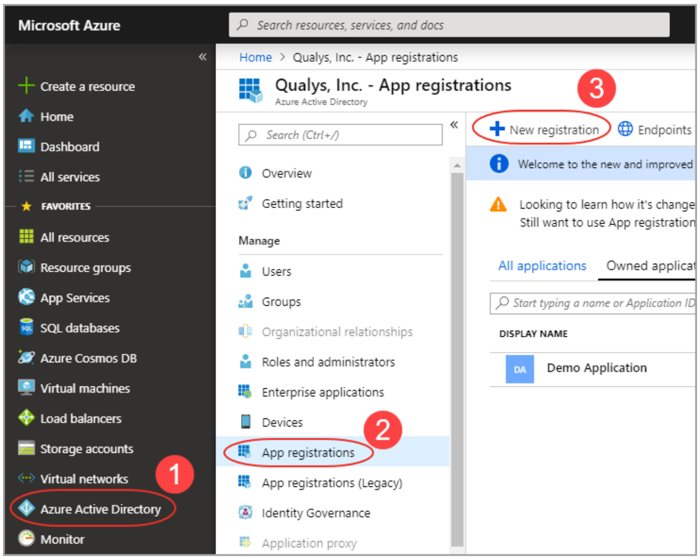
Configuring Authentication Key

Create Secret Key

Getting Subscription ID

Create Application and get Application ID, Directory ID

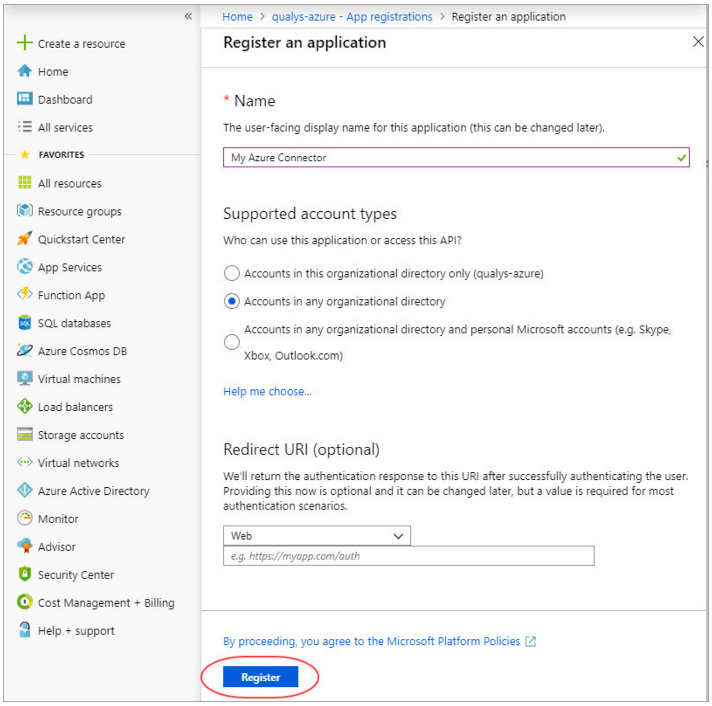
Create an application in Azure Active Directory. Log on to the Microsoft Azure console and go to Azure Active Directory in the left navigation pane, then App registrations. Click New registration.



Welcome to the new and improved

Looking to learn how it's change
Still want to use App registration

To register the application, you need to provide few details.



Register an application

* Name

The user-facing display name for this application (this can be changed later).

My Azure Connector ✓

Supported account types

Who can use this application or access this API?

○ Accounts in this organizational directory only (qualys-azure)

● Accounts in any organizational directory

○ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

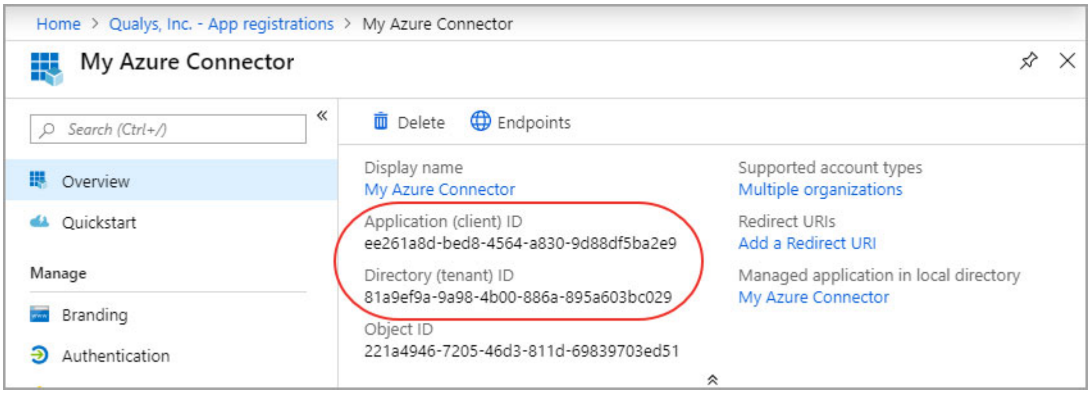
e.g. https://myapp.com/auth

By proceeding, you agree to the Microsoft Platform Policies

Provide these details:

- Name: A name for the application (e.g. My Azure Connector)
- Supported account types: Select Accounts in any organizational directory.

Click Register. The newly created application is displayed with its properties.



My Azure Connector

Display name
My Azure Connector

Application (client) ID
ee261a8d-bed8-4564-a830-9d88df5ba2e9

Directory (tenant) ID
81a9ef9a-9a98-4b00-886a-895a603bc029

Object ID
221a4946-7205-46d3-811d-69839703ed51

Supported account types
Multiple organizations

Redirect URIs
Add a Redirect URI

Managed application in local directory
My Azure Connector

Copy the Application (client) ID and Directory (tenant) ID and paste it into the connector details.

Configuring Authentication Key

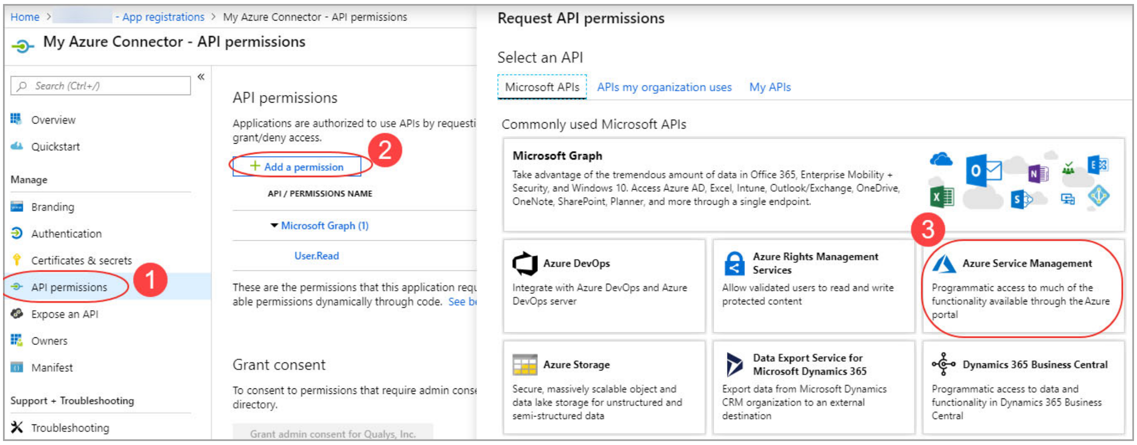
You must provide permission to the new application to access the Azure Service Management API and create a secret key.

Provide permission:

-Select the application that you created and go to API permissions > Add a permission.

-Select Azure Service Management API in Microsoft APIs for Request API permissions.

-Select user impersonation permission and click Add permission.



Applications are authorized to use APIs by requesti grant/deny access.

These are the permissions that this application requ able permissions dynamically through code. See b

To consent to permissions that require admin conse directory.

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Rights Management Services
Allow validated users to read and write protected content

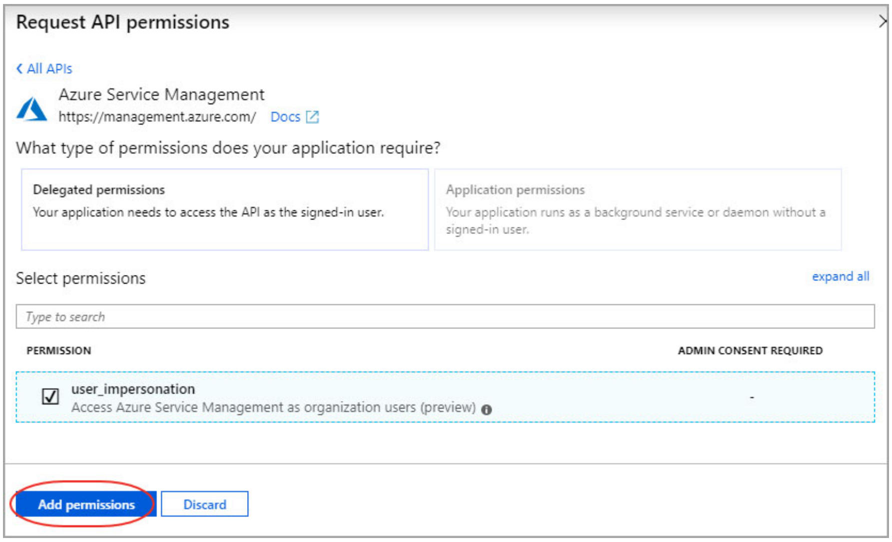
Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Azure Storage
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Data Export Service for Microsoft Dynamics 365
Export data from Microsoft Dynamics CRM organization to an external destination

Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

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



What type of permissions does your application require?

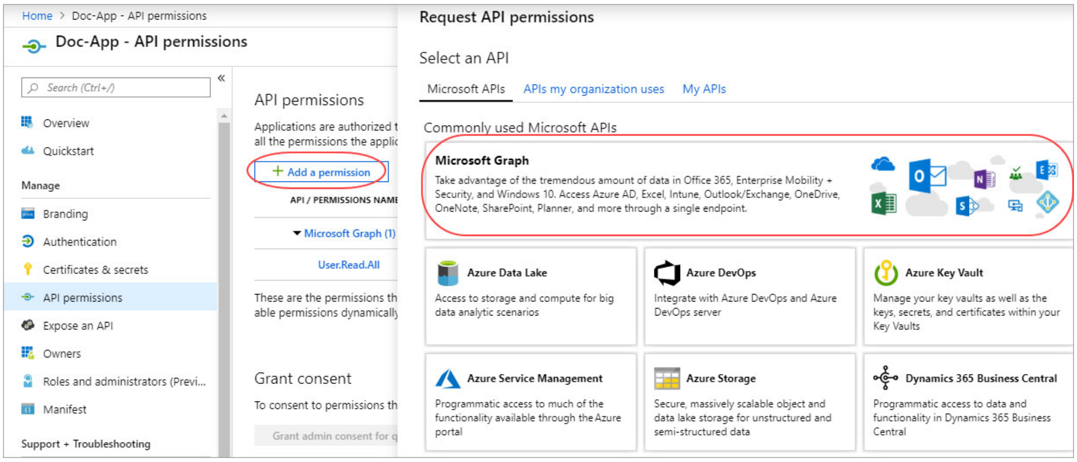
Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

PERMISSION	ADMIN CONSENT REQUIRED
☑ user_impersonation Access Azure Service Management as organization users (preview)	-

Click Add a permission.

Select Microsoft Graph in Microsoft APIs for Request API permissions.



Home > Doc-App - API permissions

Doc-App - API permissions

Search (Ctrl+/)

Overview

Quickstart

Manage

Branding

Authentication

Certificates & secrets

API permissions

Expose an API

Owners

Roles and administrators (Previ...

Manifest

Support + Troubleshooting

API permissions

Applications are authorized t
all the permissions the applic

+ Add a permission

API / PERMISSIONS NAME

Microsoft Graph (1)

User.Read.All

These are the permissions th
able permissions dynamically

Grant consent

To consent to permissions th

Grant admin consent for c

Request API permissions

Select an API

Microsoft APIs | APIs my organization uses | My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Data Lake
Access to storage and compute for big data analytic scenarios

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Key Vault
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Azure Storage
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

Select Application permissions and expand User permissions and select User.Read.All permission and click Add permissions.

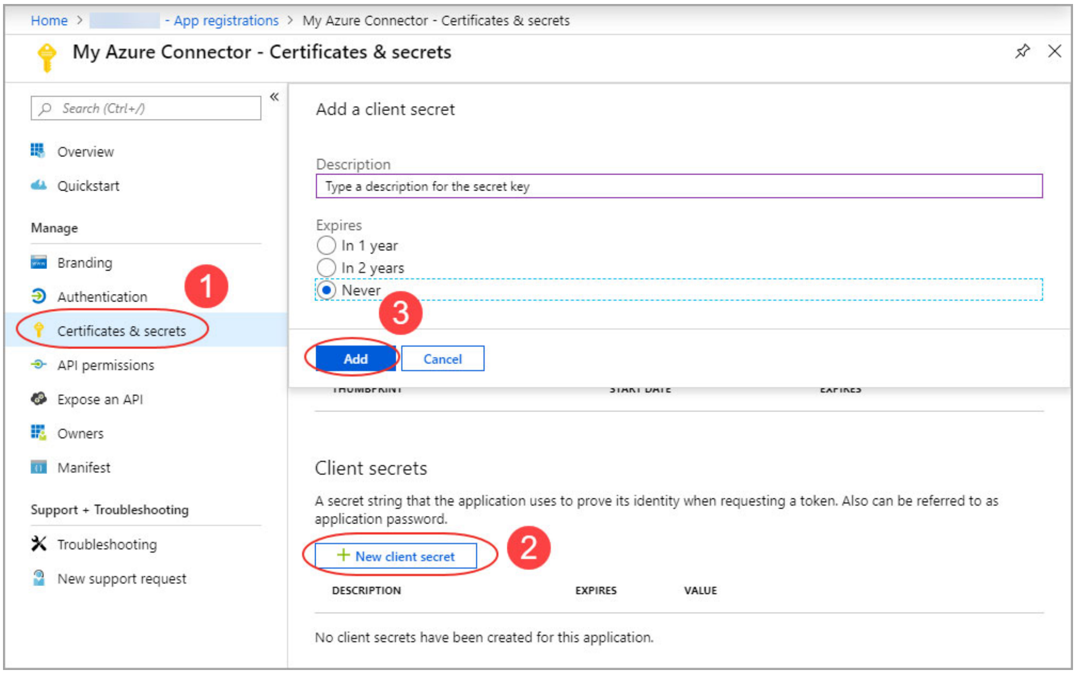
A confirmation notification “Permissions have changed. Users and/or admins will have to consent even if they have already done so previously.” is displayed on success.

Create Secret Key

-Select the application that you created and go to Certificates and Secrets > New client secret.

-Add a description and expiry duration for the secret key (recommended: Never) and click Add.

The value of the key appears in the Value field.



My Azure Connector - Certificates & secrets

Add a client secret

Description: Type a description for the secret key

Expires
○ In 1 year
○ In 2 years
● Never

Add Cancel

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

DESCRIPTION	EXPIRES	VALUE

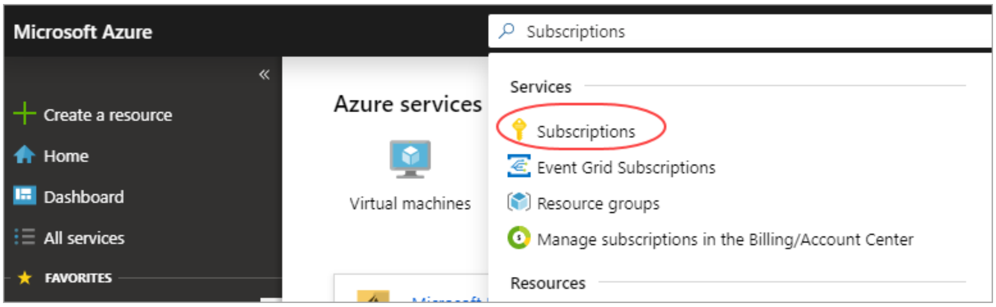
No client secrets have been created for this application.

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.

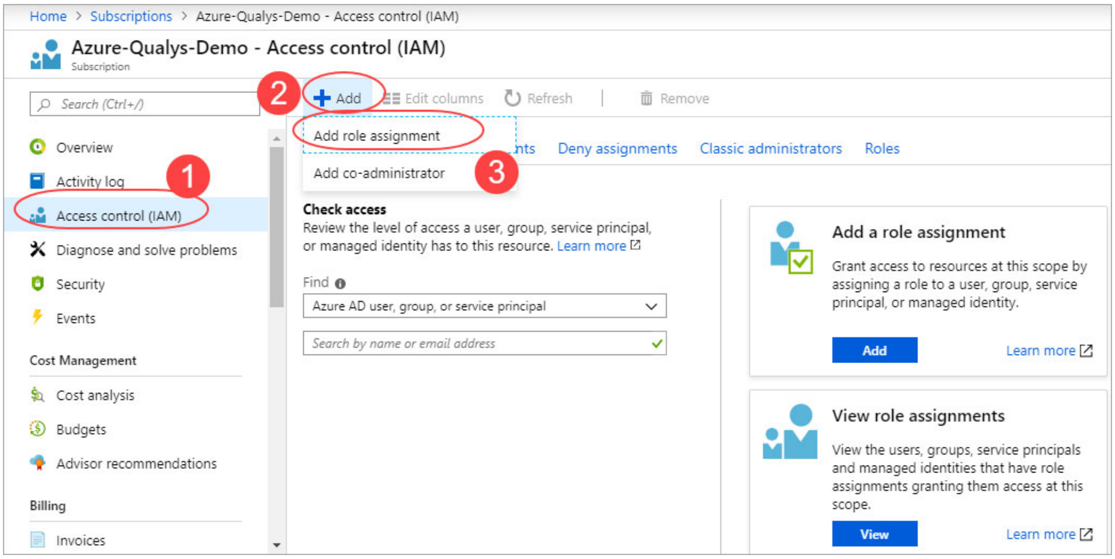
Getting Subscription ID

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 note the subscription ID. To grant permission to the application you created, choose Access Control (IAM).



Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Grant access to resources at this scope by assigning a role to a user, group, service principal, or managed identity.

View the users, groups, service principals and managed identities that have role assignments granting them access at this scope.

Assign two roles (Reader role and a custom role to the application).

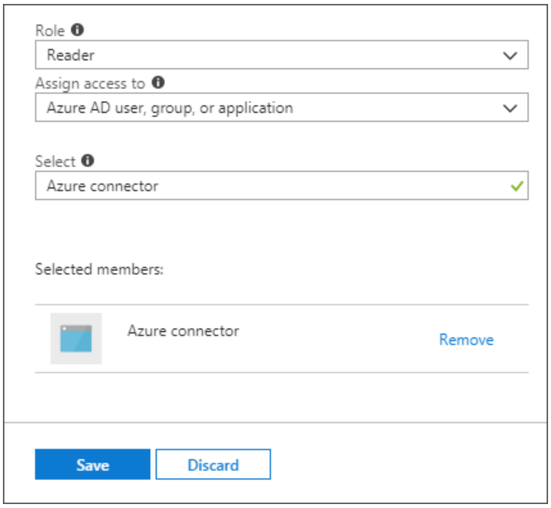
Assign Reader Role

a - To grant permission to the application you created, choose Access Control (IAM).

b - Go to Add > Add a role assignment. Pick the role as Reader. A Reader can view everything but cannot make any changes to the resources of a subscription.

c - Select Azure AD user, group, or service principal in Assign Access to dropdown.

d - Type the application name in Select drop-down and select the application you created.



Role: Reader

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

Select: Azure connector ✓

Selected members:

Azure connector — Remove

e - Click Save to finish assigning the role. You'll see your application in the list of users assigned to a role for that scope.

Assign Custom Role

Before you assign the custom role, create the custom role (QRole). Create Custom Role

a - Go to Add > Add a role assignment. Pick the custom role you created (QRole). The custom role can view but cannot make any changes to the resources of a subscription.

b - Select Azure AD user, group, or service principal in Assign Access to dropdown.

c - Type the application name in Select drop-down and select the application you created.

d - 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.

Create Custom Role

Perform the Azure CLI Shell commands. Create a JSON file with following content: Edit the content and add Subscription ID.

```
{
"Name": "QRole",
"IsCustom": true,
"Description": "Role for Qualys Connector",
"Actions":
[
   "Microsoft.Web/sites/config/list/action"
],
 "NotActions": [  ],
 "AssignableScopes":
[
   "/subscriptions/XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX"
]
}
```

Run command:

```
az role definition create --role-definition <Role-Definition-
Json_file>
```

Note: These additional permissions are required for control evaluation for CID 50047/50084, covered as a part of custom role.

References

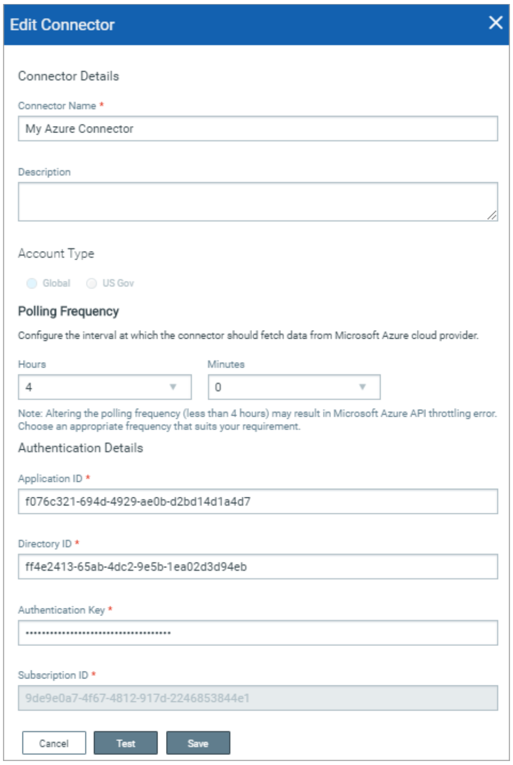
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-cli

https://docs.microsoft.com/en-us/azure/role-based-access-control/tutorial-custom-role-powershell

https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal

Editing Microsoft Azure Connectors

Go to Configuration > Microsoft Azure and select the connector for which you would want to edit the details. From the quick actions menu, select View and go to Connector Information tab and click Edit.



Edit Connector

Connector Details

Connector Name *
My Azure Connector

Description

Account Type
● Global ○ US Gov

Polling Frequency
Configure the interval at which the connector should fetch data from Microsoft Azure cloud provider.

Hours: 4
Minutes: 0

Note: Altering the polling frequency (less than 4 hours) may result in Microsoft Azure API throttling error. Choose an appropriate frequency that suits your requirement.

Authentication Details

Application ID *
f076c321-694d-4929-ae0b-d2bd14d1a4d7

Directory ID *
ff4e2413-65ab-4dc2-9e5b-1ea02d3d94eb

Authentication Key *
••••••••••••••••••••••••••••••••••••

Subscription ID *
9de9e0a7-4f67-4812-917d-2246853844e1

You can now edit the required details.

Once you update the required details, you can click Test to verify if the connection to the Microsoft Azure cloud provider is successful with the details you updated. If the test connection is successful, click Save and proceed.

If the test connection fails, you may need to check and update the authentication details you provided for the connection to work.

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.

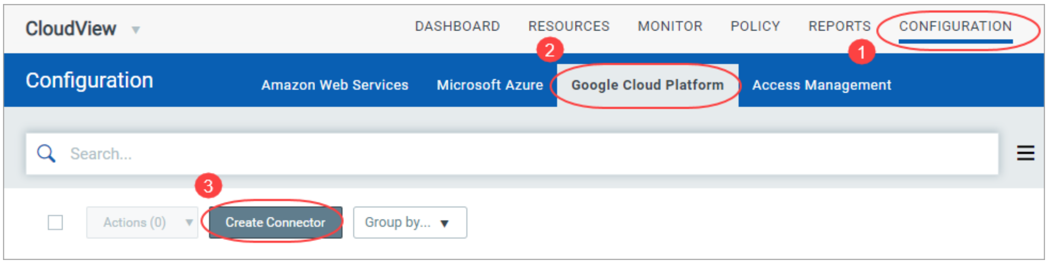
- SQL Server
- Function App
- SQL Server Database
- Resource Group
- Virtual Network
- Virtual Machine (virtual machines created using Resource Manager only)
- Network Security Group
- Web App (App Service)

Google Cloud Platform

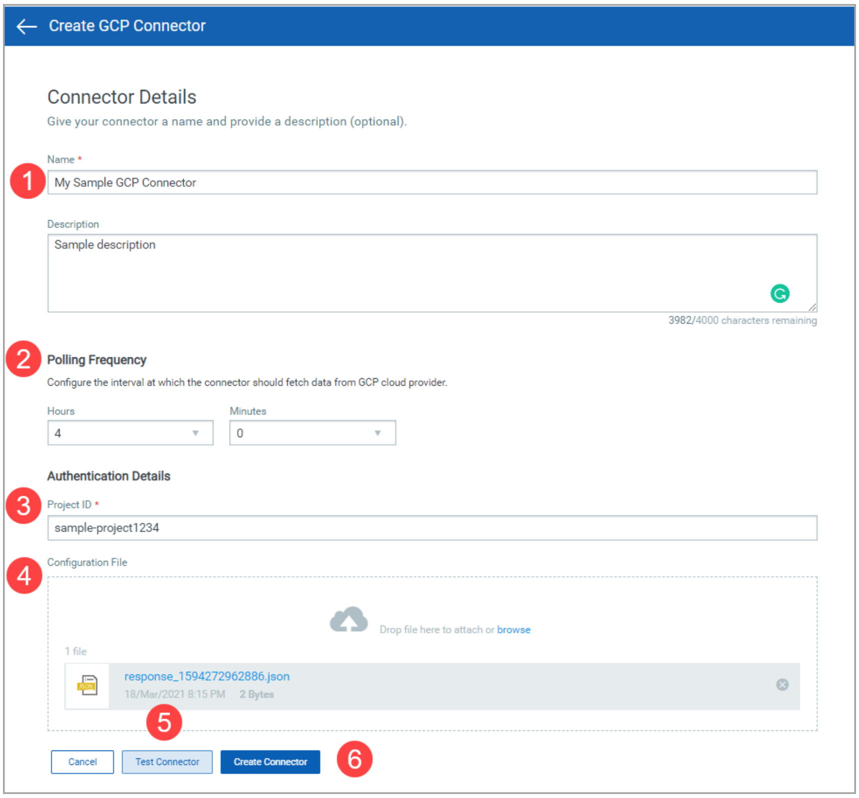
Configure a Google Cloud Platform (GCP) connector for gathering resource information from your Google Cloud Platform project. It just takes a couple of minutes.

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.



Connector Details

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

Name *: My Sample GCP Connector

Description: Sample description

3982/4000 characters remaining

Polling Frequency

Configure the interval at which the connector should fetch data from GCP cloud provider.

Hours: 4

Minutes: 0

Authentication Details

Project ID *: sample-project1234

Configuration File

Drop file here to attach or browse

1 file

response_1594272962886.json
18/Mar/2021 8:15 PM 2 Bytes

(2)Select a frequency at which the connector should poll the cloud provider and fetch data. By default, the connector polling frequency is configured for every 4 hours. As a result, the connector will connect with the cloud provider every 4 hours to fetch the data.

You can configure frequency from minimum one hour to maximum 24 hours. We recommend that you configure frequency of 4 hours or more for optimal use of your connector. Configuring a low polling frequency (lesser than 4 hours) can affect the performance of the connector and may result in GCP API throttling error.

> Note:
> - If you trigger Run for the connector from the quick actions menu, the scheduled connector polling (as per the configured frequency) remains unaffected.
> - Configuration of connector polling frequency is enabled only for Cloud Security Assessment (CSA) users.

(3) Provide a project Id for your GCP connector.

You can provide a distinct project ID for a GCP connector. You can use same service account for multiple projects. As a result, you can create multiple GCP connectors with same service account but distinct project IDs.

For detailed steps on using the same service account for multiple projects, see Assign Service Account to other projects.

(4) Create a service account and download the configuration file from the GCP console and then upload it to Qualys Cloud Platform to complete GCP connector creation.

(5) Click Test Connector to verify if the connector can successfully authenticate using the provided service account credentials in GCP cloud environment. If the test connection is successful, proceed with the connector creation process. If the test connection fails, you may need to check and update the authentication details (configuration file) you uploaded for the connection to work.

> Note: Ensure that you have uploaded the configuration file with correct project details for the connector to successfully fetch resource details.

(6) Click Create Connector.

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

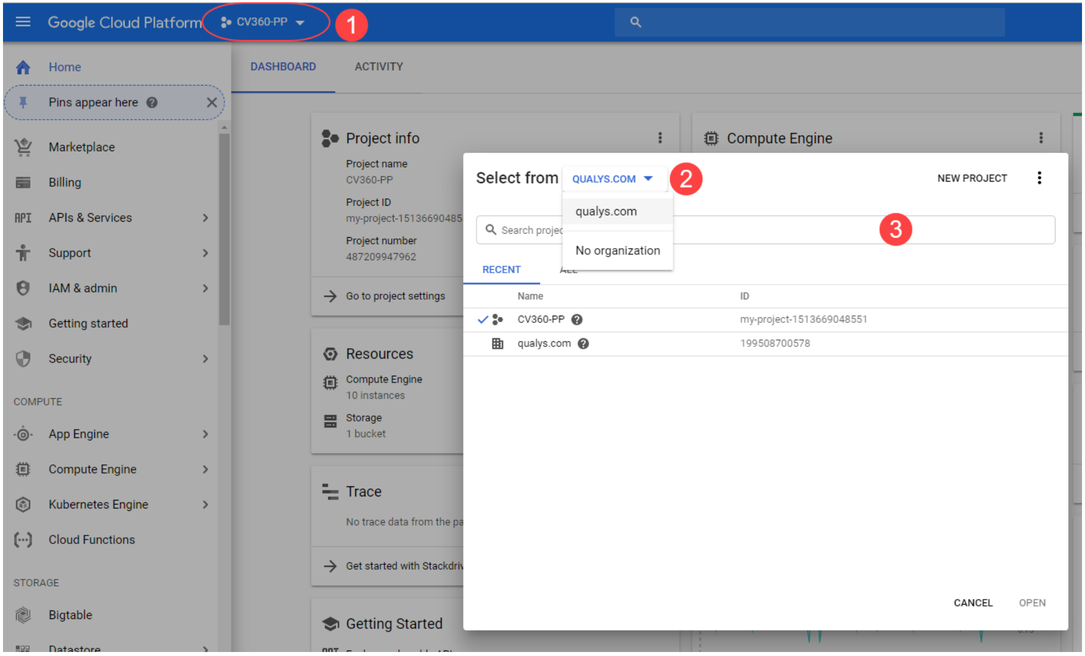
Let us see the steps to download the configuration (JSON) file from GCP console and set up the required authentication details. You need to enable access to the necessary APIs from the API library.

Enable Access to Compute Engine and Resource Manager API

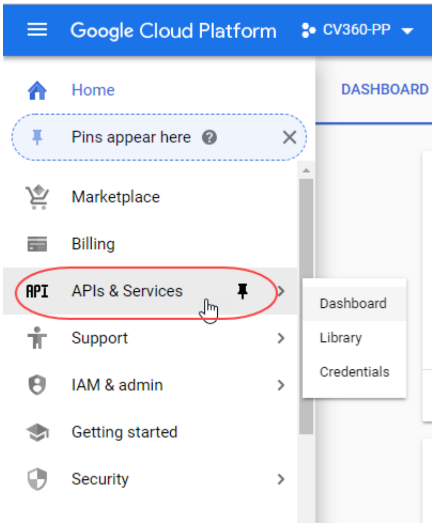
(1) Navigate to Google Cloud Platform (GCP) console.

(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 > Library.



(5) In API library, click the following APIs and enable them. If you need help finding the API, use the search field:

- Compute Engine API

- Cloud Resource Manager API

- Kubernetes Engine API

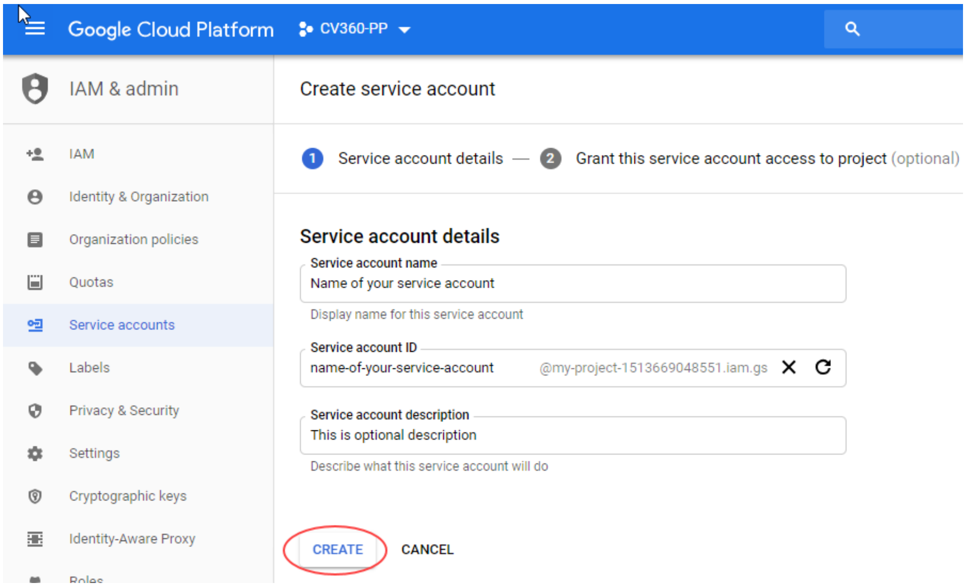
- Cloud SQL Admin API

- BigQuery API
- Cloud Functions API
- Cloud DNS API
- Cloud Key Management Service (KMS) API
- Cloud Logging API
- Stackdriver Monitoring API

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.



Create service account

1 Service account details — 2 Grant this service account access to project (optional)

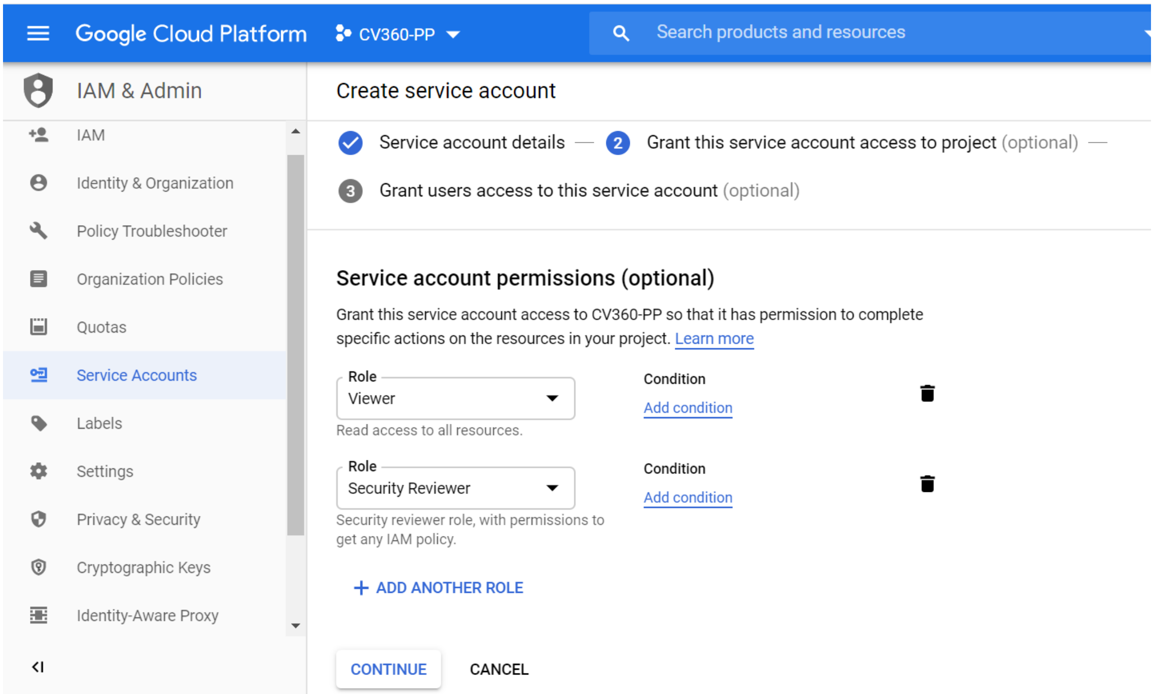
Service account details

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

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



Create service account

✓ Service account details — 2 Grant this service account access to project (optional) —

3 Grant users access to this service account (optional)

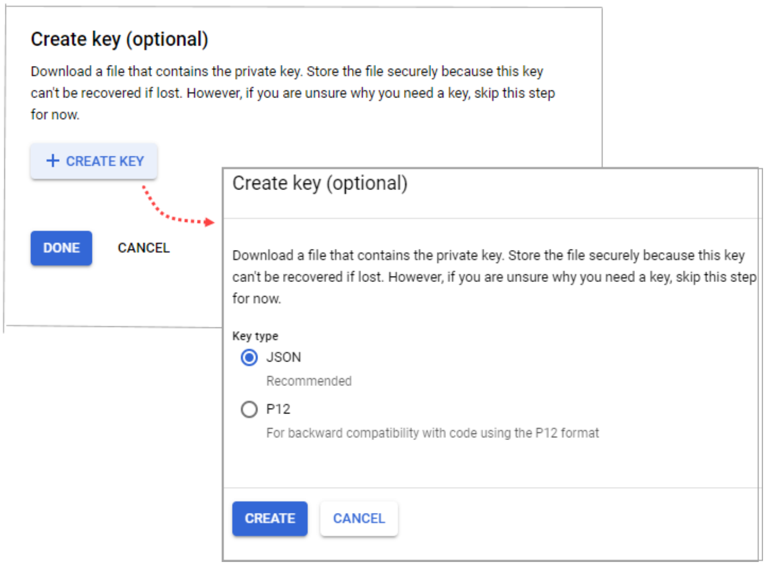
Service account permissions (optional)

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.
Condition: Add condition

Role: Security Reviewer
Security reviewer role, with permissions to get any IAM policy.
Condition: Add condition

(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.

Assign Service Account to other projects

You can use an existing service account for setting up connectors for additional projects. Simply, assign the service account as a member in IAM at the organization level or at the project level.

Let us view the steps for the same.

Assign Service Account in IAM at project level

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

(2) From the left navigation bar, select IAM & admin.

(3) Select the project from the drop-down menu in the top-left corner.

(4) In the IAM menu bar, click +ADD.

(5) In the New Members box, type the name of the service account and click the suggested value.

(6) In the Select a role drop-down box, select the appropriate role. Choose Viewer role and Security Reviewer role to assign at least reader permissions to the service account.

(7) Click Save.

(8) To add additional projects, repeat steps 3 through 7.

Assign Service Account in IAM at organization level

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

(2) In the left navigation bar, select IAM & admin.

(3) Select your organization from the drop-down menu in the top-left corner.

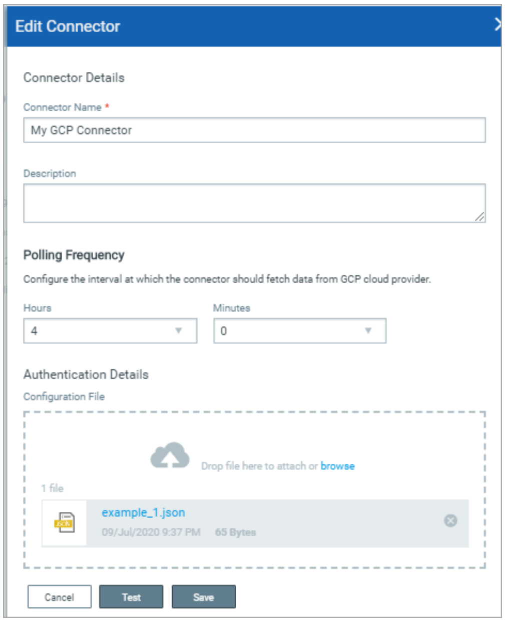
(4) In the IAM menu bar, click +ADD.

(5) In the New Members box, type the name of the service account and click the suggested value.

(6) In the Select a role drop-down box, select the appropriate role. Choose Viewer role and Security Reviewer role to assign at least reader permissions to the service account.

(7) Click Save.

Editing GCP Connectors



Edit Connector

Connector Details

Connector Name *: My GCP Connector

Description:

Polling Frequency

Configure the interval at which the connector should fetch data from GCP cloud provider.

Hours: 4

Minutes: 0

Authentication Details

Configuration File

Drop file here to attach or browse

1 file

example_1.json
09/Jul/2020 9:37 PM 65 Bytes

Go to Configuration > Google Cloud Platform and select the connector for which you would want to edit the details. From the quick actions menu, select View and go to Connector Information tab and click Edit.

You can now edit the required details.

Once you update the required details, you can click Test to verify if the connection to the GCP cloud provider is successful with the details you updated. If the test connection is successful, click Save and proceed.

If the test connection fails, you need to check and update the authentication details (configuration file) you uploaded for the connection to work.

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

- Cloud Functions

Enable-Disable Connectors

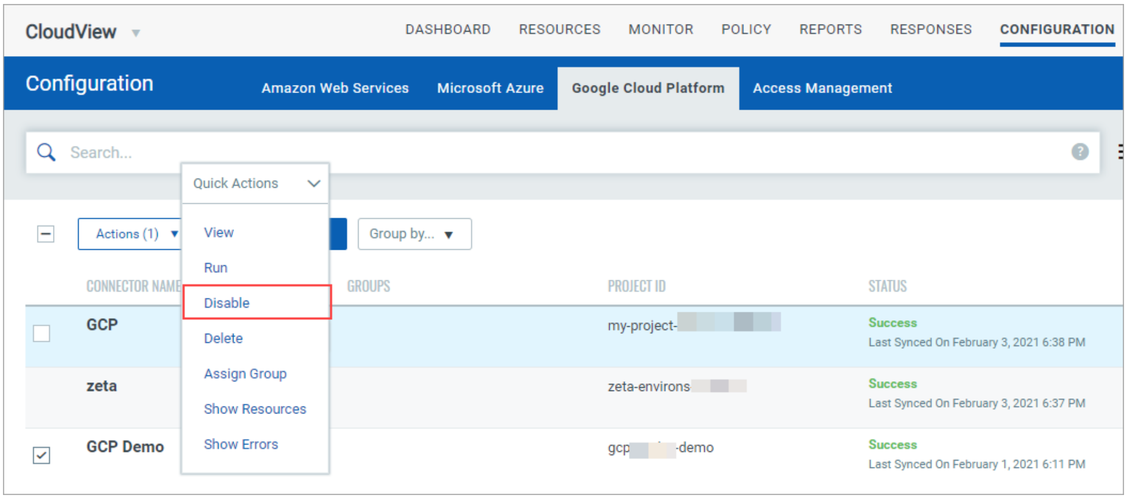
We give you the flexibility to enable or disable a connector with a single-click. When you disable a connector, it is not eligible for auto-run or manual run. You can view information, edit or delete a disabled connector.

Disable Connector

1) Go to Configuration tab and then the cloud provider tab, where the connector belongs.

2) Select the connector to be disabled and from the quick actions menu, select Disable from the quick actions menu.

3) Click on the confirmation message. The connector gets disabled.



	CONNECTOR NAME	GROUPS	PROJECT ID	STATUS
□	GCP		my-project-[redacted]	Success Last Synced On February 3, 2021 6:38 PM
	zeta		zeta-environs[redacted]	Success Last Synced On February 3, 2021 6:37 PM
☑	GCP Demo		gcp[redacted]-demo	Success Last Synced On February 1, 2021 6:11 PM

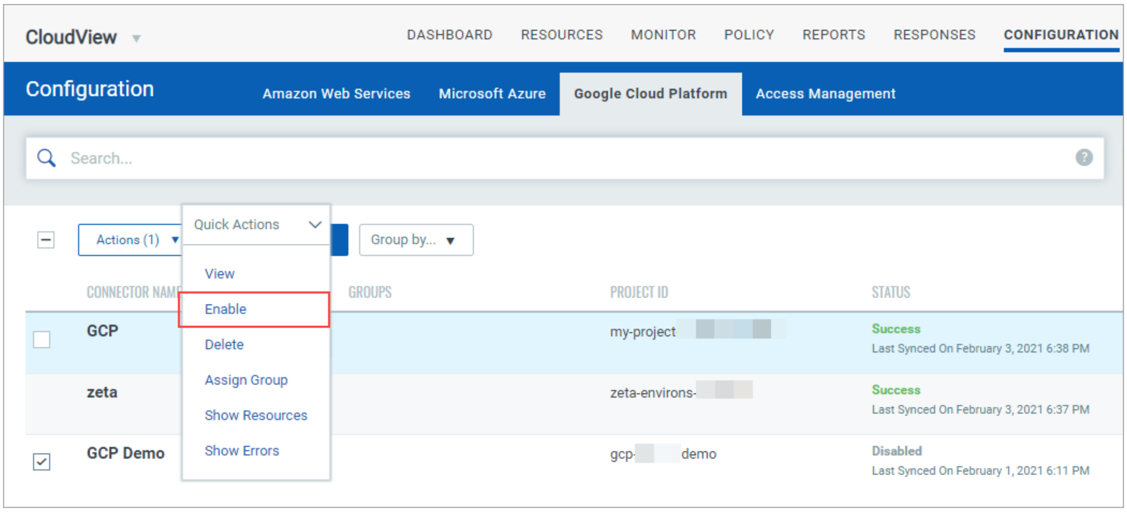
Note: Automatic or manual connector run skips the disabled connectors. Only connectors with enabled state are executed during connector run.

Enable Connector

1) Go to Configuration tab and then the cloud provider tab, where the connector belongs.

2) Select the connector to be disabled and from the quick actions menu, select Enable from the quick actions menu.

3) Click on the confirmation message. The connector gets enabled.



	CONNECTOR NAME	GROUPS	PROJECT ID	STATUS
□	GCP		my-project [redacted]	Success Last Synced On February 3, 2021 6:38 PM
	zeta		zeta-environs-[redacted]	Success Last Synced On February 3, 2021 6:37 PM
☑	GCP Demo		gcp-[redacted] demo	Disabled Last Synced On February 1, 2021 6:11 PM

Managing Connector Access for Users

You can create users and then assign a role to it to grant access as per the role you define. We support multiple user roles.

- User with Manager role: The most privileged users are users with Manager role as they have full privileges and access to all resources in the subscription. Only users with Manager role can create users and assign roles.

- Sub Users: There are two types of sub users that a user with Manager role can create. Depending on the permissions you assign to the role, you could categorize the sub users into all privileges or read only privileges.

All privilege: Sub User will have all the privileges in CloudView except creating and managing other users. For more information, refer to Sub User (All Privileges).

Reader privileges: Sub User with Reader role can only view the data displayed in CloudView module.

User Permissions

The following table provides a comparison of privileges granted to user roles.

Operations	**User (Manager role)**	**Sub User**	**Sub User (Reader role)**
Create New Users	Yes	No	No
Grant Access to Sub- Users	Yes	No	No
Update Access of Existing Users	Yes	No	No
Create and Assign Groups to Connectors	Yes	No	No
Manage Connectors	Yes	No	No
Manage Policies and Controls	Yes	Yes	No
Customize Controls	Yes	Yes	No
Reports	Yes	Yes	View only
Dashboards	Yes	Yes	Yes

New Users: Scope and Permissions

Only users with manager role have permissions to create new users and grant them permissions. Let us view the high level steps.

Create User

Assign Role to Users

Manage Access for Users (Grouping Connectors)

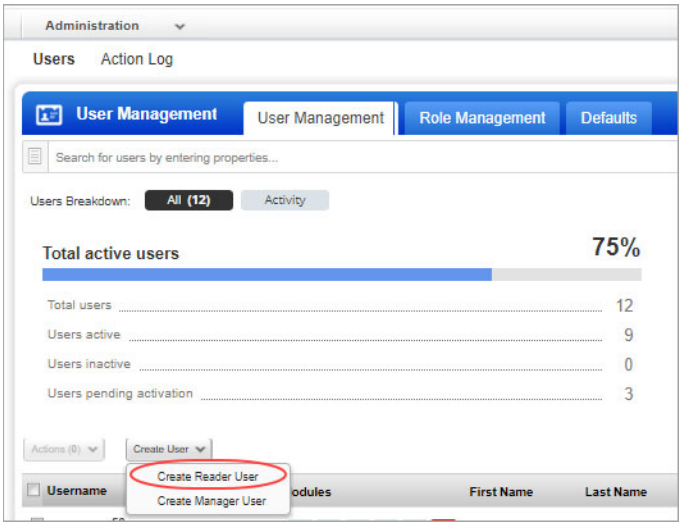
Manage Access for Users

Create User

Users with manager role can add users, up to the number allowed for the subscription service level.

Quick Steps

(1) Create a Reader User: Navigate to Administration module > User Management > Create User > Create Reader User.



Total active users 75%

Total users 12
Users active 9
Users inactive 0
Users pending activation 3

(2) Provide the necessary information for the user creation such as General Information, Locale, User Role, Asset Groups (optional), Permissions, Options, and Security.

Ensure that you select at least Reader role for User Role. For all other options you can retain the default settings.

(3) Click Save.

How do I grant a user permissions?

You can define a role and then assign the defined role to the user. The role you define decides the permissions assigned to the user. You do this by editing the user's account. For example, to create a user with full access, you need to enable all the permissions in a role and assign the role to user. You can assign the role to assign full access to multiple users at one go. Learn more

What happens after adding a new user?

When you create a new user, the user appears on the user accounts list with a status of "Pending Activation". The user will automatically receive a registration email with a secure one-time-only link to the credentials for their new account and login instructions. The registration email is sent to the email address defined in the user's account. The user's status changes to "Active" after logging in for the first time.

Assign Role to Users

Use the Administration utility (last option in the app picker) to view and manage users and grant access to CloudView application. On the User Management tab you'll see the apps each user has access to. Access is role based.

Refer to the online help available in the Administration utility for detailed information.

Tell me the steps

In the Administration utility, go to Users > Role Management. This is where you create new roles and make changes to the permissions for existing roles. You can also quickly assign roles to users from here.

Don't see this tab? You need to have 1) full permissions and scope, or 2) a role with the "Access Role Management Section" permission enabled in the Administration utility.

Tell me about various roles?

You can configure two sub user roles:

-Sub User with all privileges: We provide a predefined role named "CLOUDVIEW user". Assign the role to the required user and the user is granted full access in CloudView. Learn more

-Sub user with Reader privileges: The user with Reader role can only view the data displayed in CloudView module. Click New Role. Give the role a name and description, and then select the modules and permissions to privileges be granted to a user when the role is assigned. Learn more

How do I assign roles to users?

Select the role you want to assign and choose "Add To Users" from the Quick Actions menu. Then tell us which users should be assigned the role and click Save. You can remove roles from users in a similar way - just select the action Remove From Users.

How do I edit a role?

Select any role in the list and choose Edit from the Quick Actions menu.

You can change the role name and description and edit the assigned permissions. Any changes you make to a role will apply to all users assigned that role.

> Warning - Be careful when removing the UI access permission from a role. A user will not be able to log into the UI if they don't have at least one role with the UI access permission assigned.

Tell me about permissions

When you're editing the permissions for a role, you'll notice that you can define application access, modules to be accessible, and permissions within the module for the users with the current role.

Ensure that you have assigned CloudView module to be accessible for the users. Simply click the title of a group to expand its permissions. Then select the permissions you want to assign to the role.

- All privileges: Sub User will have all the privileges in CloudView except creating and managing other users. For more information, refer to Sub User (All Privileges).

- Reader privileges: Sub User with Reader role can only view the data displayed in CloudView module. For more information, refer to Sub User (Reader Privileges).

Can I delete a role?

Yes. Select the role and choose Delete from the Quick Actions menu. The role you delete will no longer be assigned to users. It is removed automatically from all users' accounts (that had it previously assigned) and those users will no longer have the permissions granted by the role.Warning - Be careful when removing the UI access permission from a role. A user will not be able to log into the UI if they don't have at least one role with the UI access permission assigned.

> Note: If you edit permissions for a pre-defined role or delete a pre-defined role, the user associated with the roles you edit can experience difference in access behavior.

Manage Access for Users (Grouping Connectors)

You can control access for sub users with the usage of groups. The groups help you to organize your connectors and to manage user access to them.

Groups

You can apply groups to connectors and form connector groups or segregate connectors using a specific group for a connector as well. Use groups to provide access or restrict access to users you create.

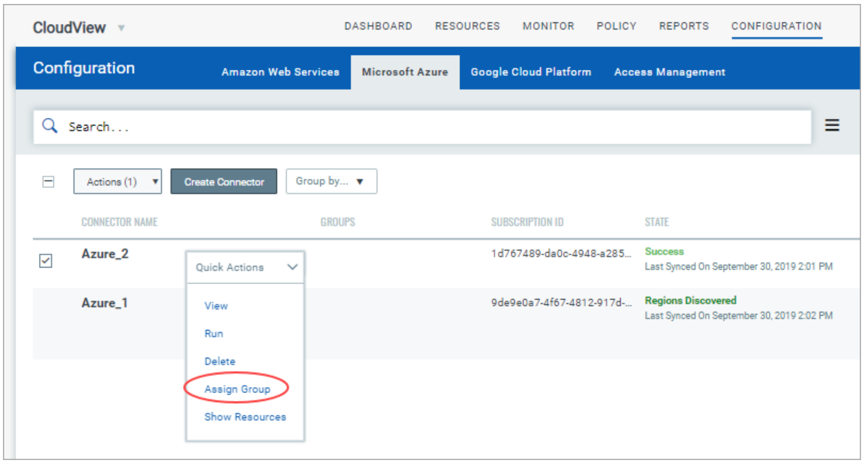
Assign Groups to Connector

Let us see how to create connector groups and provide access to a particular connector for a user.

(1) Navigate to Configuration tab and then the Cloud Provider (AWS, Azure, or GCP) for which you would want to create connector group.

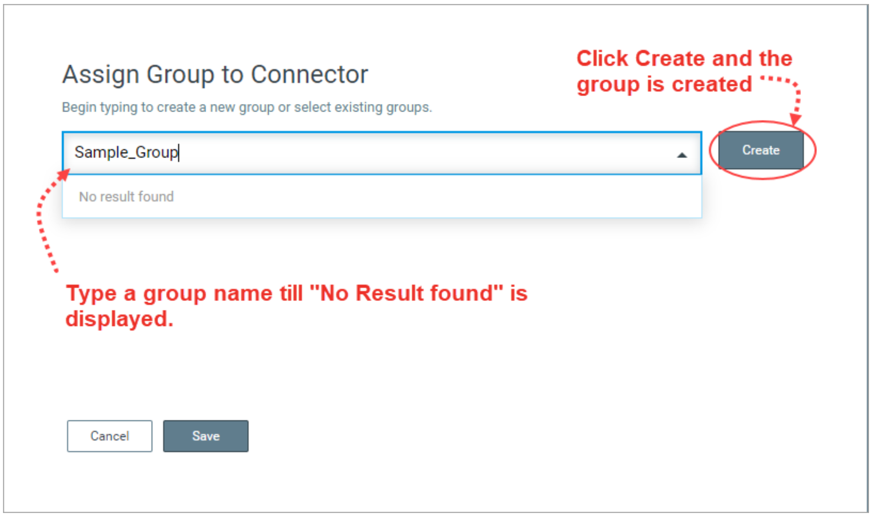
If you have multiple accounts or multiple connectors, you can restrict access to a particular account or connector using groups.

(2) Choose the connector for which you want to configure access and click Assign Group from the quick action menu.



	CONNECTOR NAME	GROUPS	SUBSCRIPTION ID	STATE
☑	Azure_2		1d767489-da0c-4948-a285...	Success Last Synced On September 30, 2019 2:01 PM
	Azure_1		9de9e0a7-4f67-4812-917d-...	Regions Discovered Last Synced On September 30, 2019 2:02 PM

(3) Type a name for the group and click Create and then click Save.


Assign Group to Connector

Begin typing to create a new group or select existing groups.

Sample_Group

No result found

Click Create and the group is created

Type a group name till "No Result found" is displayed.

To assign the groups to a sub user, you need to associate the group with the user. For more information, refer to Manage Access for Users.

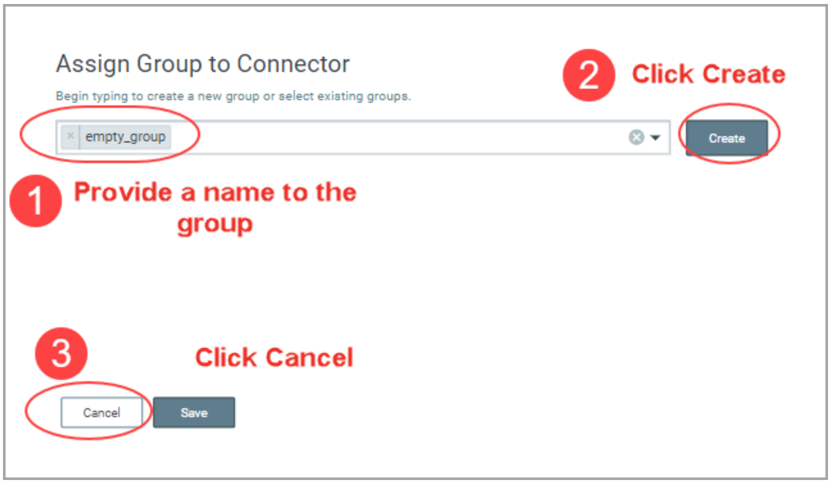
Restrict User Access to all Connectors

Note: By default, if no groups are assigned to a sub user, the sub user can access all connectors. To restrict access to all connectors, you need to create a group and not assign it to any connector but only to the user.

(1) Navigate to Configuration tab and then the Cloud Provider for which you would want to create connector groups.

(2) Choose any connector and click Assign Group from the quick action menu.

(3) Type a name for the group and click Create. **DO NOT** click Save but click Cancel.



Assign Group to Connector

Begin typing to create a new group or select existing groups.

empty_group

1 Provide a name to the group

2 Click Create

3 Click Cancel

A group is created without assigning it to any connector. Assign this group to the users through Access Management tab. The user is restricted from accessing any account.

To grant access to a connector in this case, you simply need to assign another group associated with a connector.

Manage Access for Users

The user with Manager role can assign access to sub users and decide which connectors are accessible to sub users. The Access Management tab lists all the sub users who can access the CloudView module.

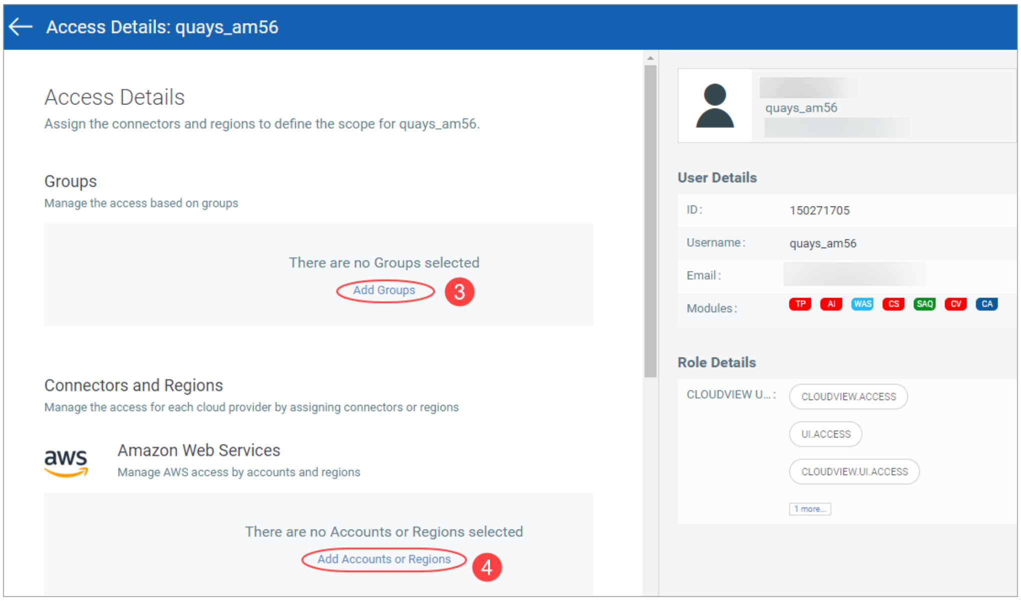
If you do not see any sub users, you can create sub users. To create new sub user, visit the Administration utility and create new users and assign role to each user.

Assign Scope to a User

(1) Navigate to Configuration > Access Management tab.

The Access Management tab is available only to user with Manager role. The user with Manager role can manage access for sub-users.

(2) Select the user, and click Manage Access from quick action menu.



Access Details: quays_am56

Access Details

Assign the connectors and regions to define the scope for quays_am56.

Groups

Manage the access based on groups

There are no Groups selected

Add Groups 3

Connectors and Regions

Manage the access for each cloud provider by assigning connectors or regions

Amazon Web Services

Manage AWS access by accounts and regions

There are no Accounts or Regions selected

Add Accounts or Regions 4

[redacted]
quays_am56
[redacted]

User Details

ID: 150271705

Username: quays_am56

Email: [redacted]

Modules: TP AI WAS CS SAQ CV CA

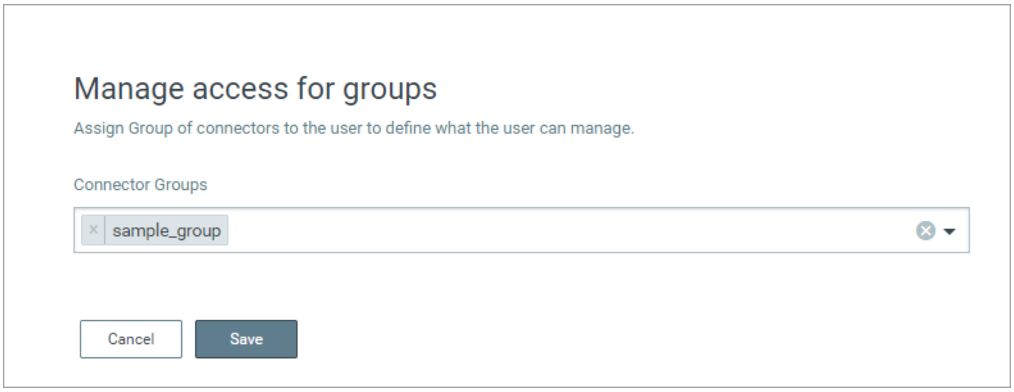
Role Details

CLOUDVIEW U...: CLOUDVIEW.ACCESS
UI.ACCESS
CLOUDVIEW.UI.ACCESS
1 more...

There are two options you could configure access for sub users:

- Using groups.

To assign the groups to a sub user, you need to associate the group with the user.



Manage access for groups

Assign Group of connectors to the user to define what the user can manage.

Connector Groups

sample_group

Click Add Groups and select the group, and click Save to associate the group with the user.

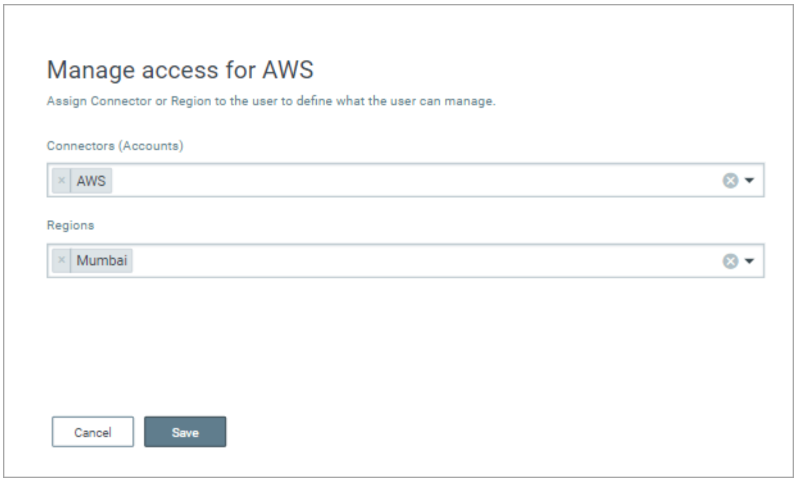
If a group is assigned to multiple connectors that belong to different Cloud Providers, the user can access all the connectors associated with the groups.

- Using connectors

When you define scope for a sub user, you could directly select the connectors for every Cloud Provider and associate it with the sub user. The sub user can then access all the connectors assigned to the sub user.

In the Connectors and Regions section, click the link for the specific Cloud Provider and then select the connector, and click Save.

You can select multiple connectors from multiple cloud providers as well. For AWS, you can select connector and region as well.



Manage access for AWS

Assign Connector or Region to the user to define what the user can manage.

Connectors (Accounts): AWS

Regions: Mumbai

Defining Scope for Existing Users

Only users with manager role have permissions to grant permissions to existing users and modify their permissions. Let us view the high level steps.

Manage Access for Users (Grouping Connectors)

Manage Access for Users

For more information refer to Role-based Access Management.

Sub User (All Privileges)

We provide a predefined role (CLOUDVIEW User) that fulfills the full-access permissions. You need to simply assign the predefined role (CLOUDVIEW User) to the user to grant them full access in CloudView.

The user with full access role can perform all the actions available to the user such as create connectors, manage policies, manage controls, and so on.

Permissions: Only users with manager role can access Administration module and create sub-users.

What can the Sub User with Full Access do?

The user with full access role can

- Manage Connectors

- Manage controls and policies

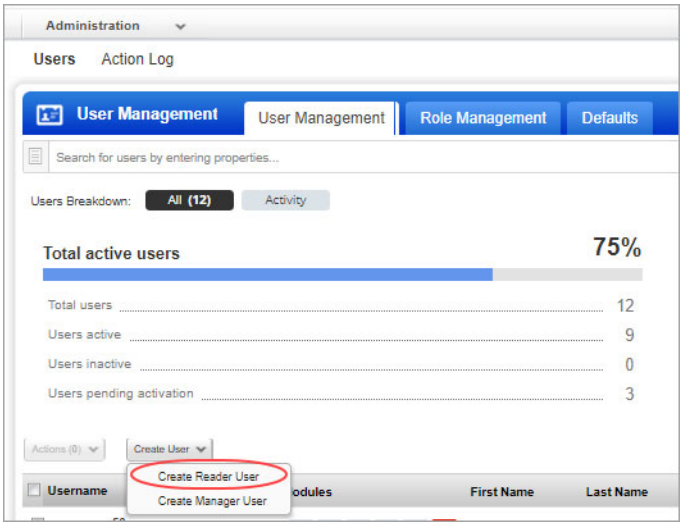
- Create and edit dashboards

- Create and edit groups (connector groups)

- Create sub users and assign groups

Quick Steps

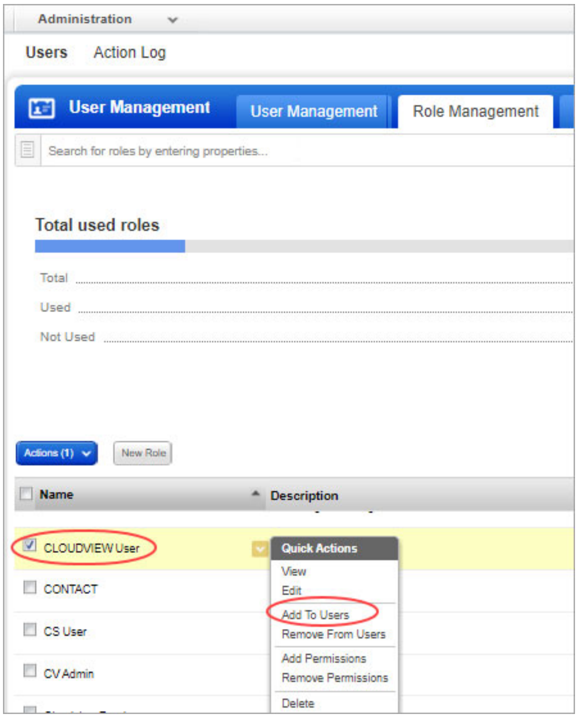
(1) Create a Reader User: Navigate to Administration module > User Management > Create User > Create Reader User.



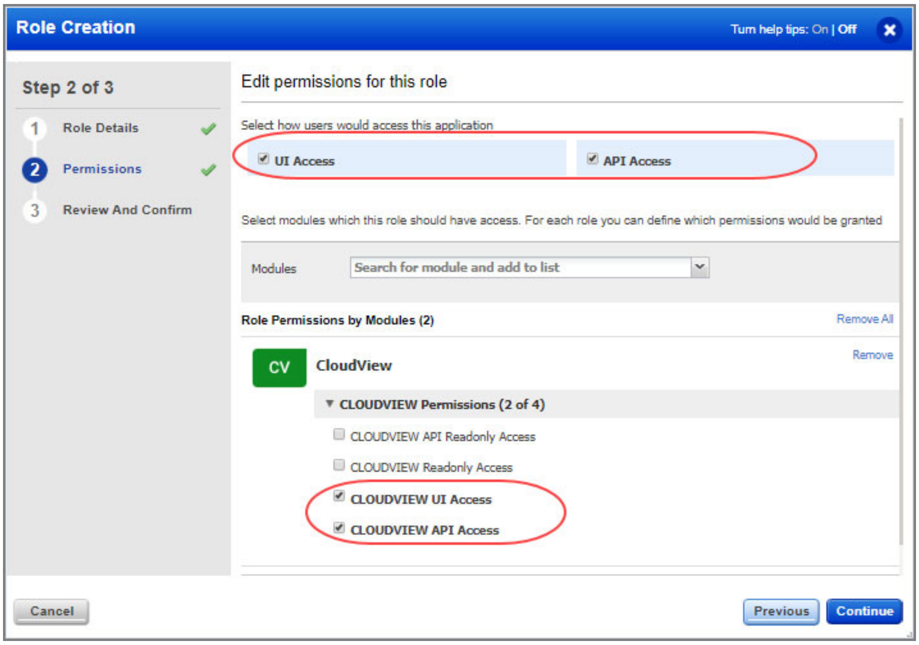
Total active users 75%

Total users	12
Users active	9
Users inactive	0
Users pending activation	3

(2) In Administration utility, go to Role Management tab, and select CLOUDVIEW user and select Add to Users from the quick action menu.



Alternatively, you could also create a new role and assign two permissions: CLOUDVIEW UI Access and CLOUDVIEW API Access permissions to the role and assign the role to the required user.


Role Creation
Turn help tips: On | Off
Step 2 of 3
1 Role Details ✓
2 Permissions ✓
3 Review And Confirm
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 (2)
Remove All
CV
CloudView
Remove
▼ CLOUDVIEW Permissions (2 of 4)
□ CLOUDVIEW API Readonly Access
□ CLOUDVIEW Readonly Access
☑ CLOUDVIEW UI Access
☑ CLOUDVIEW API Access
Cancel
Previous
Continue

Note: If all the four permissions are enabled, the read only permission overrides and sub user has only read privileges. For all privileges to be enabled, ensure that you enable only two permissions.

(3) Select the required user from Users drop-down and click Save. You need to choose user whom you want to assign full access of CloudView.

The new user is ready to use CloudView with full access capabilities!

Sub User (Reader Privileges)

You can create a new user role “Reader” (read-only-access permissions) and assign it to sub-users. The user with Reader role can only view the data displayed in CloudView module.

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

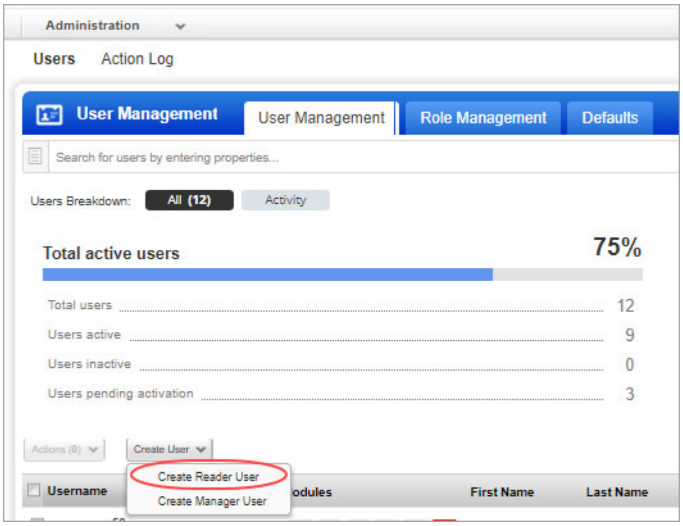
- Monitor controls, policies and resources

- Create and edit dashboards

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

Quick Steps

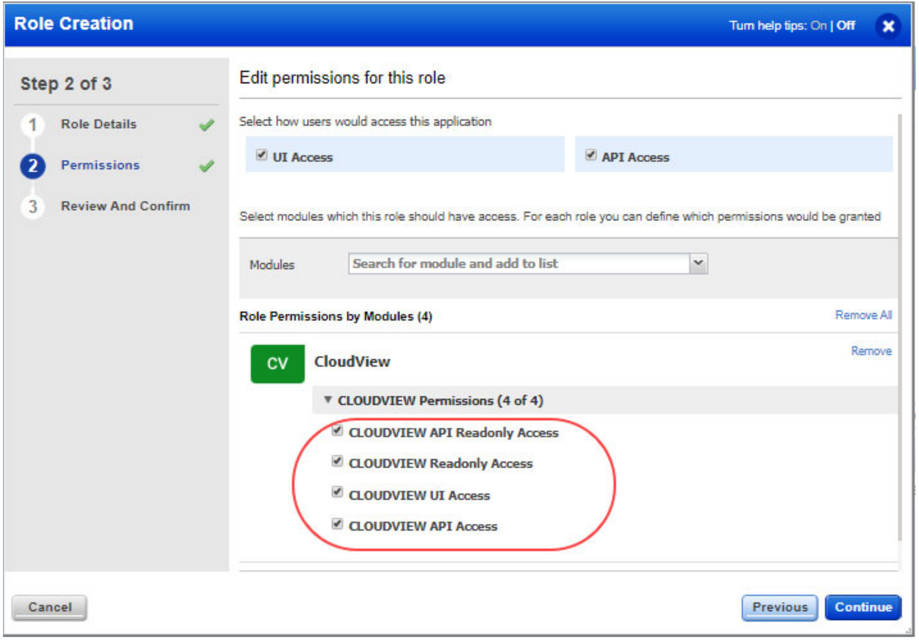
(1) Create a Reader User: Navigate to Administration module > User Management > Create User > Create Reader User.



Total active users 75%

Total users	12
Users active	9
Users inactive	0
Users pending activation	3

(2) Create a role in Administration utility and ensure that the role has UI access permission and CLOUDVIEW Readonly Access, CLOUDVIEW API Readonly Access enabled.



Step 2 of 3

1 Role Details ✓
2 Permissions ✓
3 Review And Confirm

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 (4) Remove All

CV CloudView Remove

▼ CLOUDVIEW Permissions (4 of 4)

☑ CLOUDVIEW API Readonly Access
☑ CLOUDVIEW Readonly Access
☑ CLOUDVIEW UI Access
☑ CLOUDVIEW API Access

(3) Assign the role to the newly created user.

The new reader user is ready to use CloudView with monitoring capabilities!

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.

Unified Dashboard

Dashboards help you visualize your cloud resources, evaluation of your cloud resources, see your threat exposure, leverage saved searches, and fix resource misconfigurations quickly.

We have integrated Unified Dashboard (UD) with CloudView. UD brings information from all Qualys applications into a single place for visualization. UD provides a powerful new dashboarding framework along with platform service that will be consumed and used by all other products to enhance the existing dashboard capabilities.

You can use the default CloudView dashboard provided by Qualys or easily configure widgets to pull information from other modules/applications and add them to your dashboard. You can also add as many dashboards as you like to customize your CloudView view.

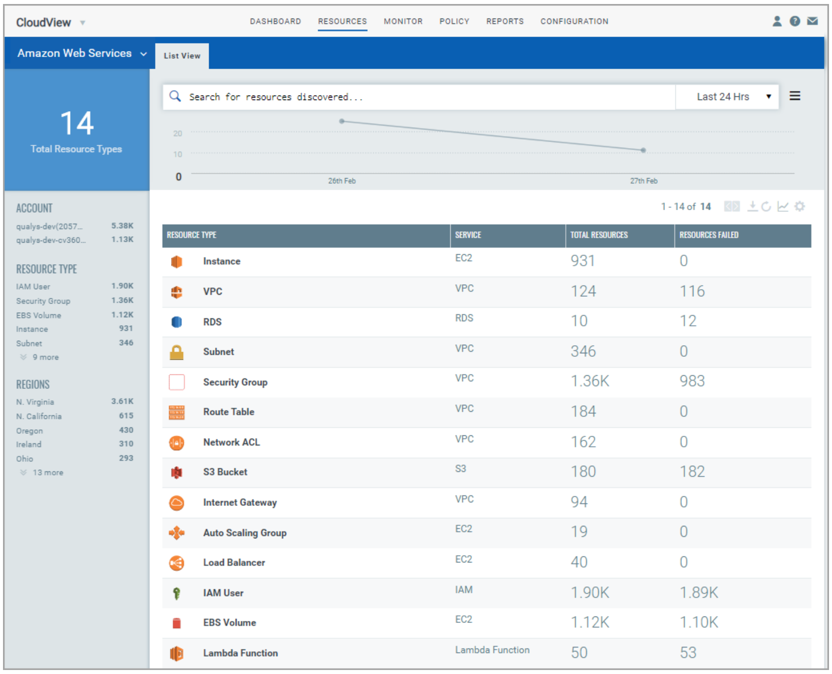
Refer to the Unified Dashboard online help for more details.

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.



14
Total Resource Types

ACCOUNT	
qualys-dev(2057...	5.38K
qualys-dev-cv360...	1.13K

RESOURCE TYPE	
IAM User	1.90K
Security Group	1.36K
EBS Volume	1.12K
Instance	931
Subnet	346
9 more	

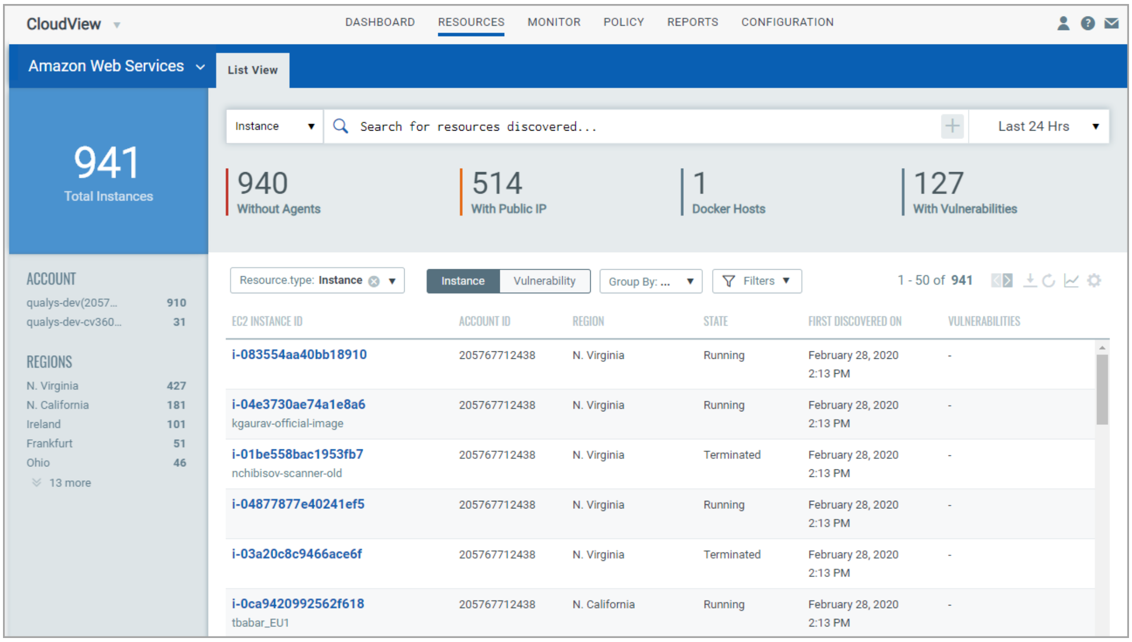
REGIONS	
N. Virginia	3.61K
N. California	615
Oregon	430
Ireland	310
Ohio	293
13 more	

RESOURCE TYPE	SERVICE	TOTAL RESOURCES	RESOURCES FAILED
Instance	EC2	931	0
VPC	VPC	124	116
RDS	RDS	10	12
Subnet	VPC	346	0
Security Group	VPC	1.36K	983
Route Table	VPC	184	0
Network ACL	VPC	162	0
S3 Bucket	S3	180	182
Internet Gateway	VPC	94	0
Auto Scaling Group	EC2	19	0
Load Balancer	EC2	40	0
IAM User	IAM	1.90K	1.89K
EBS Volume	EC2	1.12K	1.10K
Lambda Function	Lambda Function	50	53

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.



ACCOUNT	
qualys-dev(2057...	910
qualys-dev-cv360...	31

REGIONS	
N. Virginia	427
N. California	181
Ireland	101
Frankfurt	51
Ohio	46
13 more	

EC2 INSTANCE ID	ACCOUNT ID	REGION	STATE	FIRST DISCOVERED ON	VULNERABILITIES
i-083554aa40bb18910	205767712438	N. Virginia	Running	February 28, 2020 2:13 PM	-
i-04e3730ae74a1e8a6 kgaurav-official-image	205767712438	N. Virginia	Running	February 28, 2020 2:13 PM	-
i-01be558bac1953fb7 nchibisov-scanner-old	205767712438	N. Virginia	Terminated	February 28, 2020 2:13 PM	-
i-04877877e40241ef5	205767712438	N. Virginia	Running	February 28, 2020 2:13 PM	-
i-03a20c8c9466ace6f	205767712438	N. Virginia	Terminated	February 28, 2020 2:13 PM	-
i-0ca9420992562f618 tbabar_EU1	205767712438	N. California	Running	February 28, 2020 2:13 PM	-

Then click on any EC2 Instance ID to see the number of detected vulnerabilities, resource associations, location and network information. You can also perform actions on instances such as stop instance or remove IAM profile. These actions are supported only if you have enabled remediation for the connector associated with the instances. For more information, refer to Actions for Cloud Resources (AWS).

Vulnerability Details for Instances

We show vulnerability details for instance type of resources in CloudView. The details include resource inventory, security details, compliance details, and sensor details.

Few points to note for the resource details to be visible:

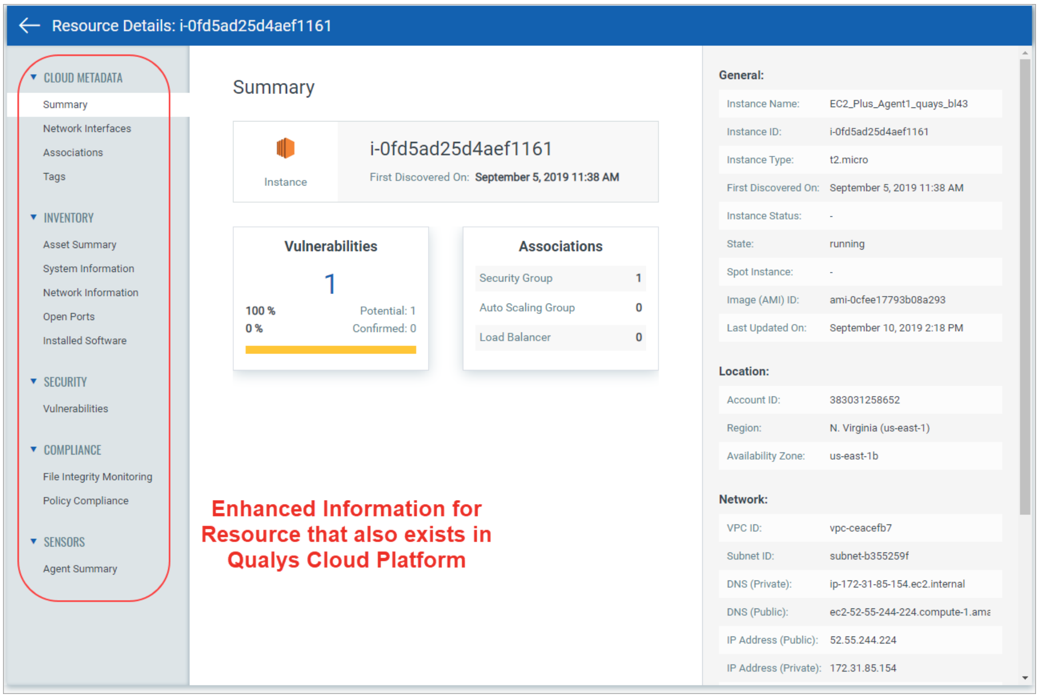
- The details are displayed for only Instance type of resources.

AWS: Instance, Azure: Virtual Machine, GCP: VM Instances

- The resource (asset) must also be detected during Qualys scan or must have Qualys Cloud Agent installed on it. The resource (asset) must be available in Qualys Cloud Platform (AssetView).

- If the resource has Qualys Cloud Agent installed, the Agent Summary section displays corresponding details.

Go to Resources and then select the Cloud Provider (AWS, Azure, or Google Cloud Platform). Now, select the resource of instance type and click the resource. The Resource Details page displays the enhanced details.



i-0fd5ad25d4aef1161
First Discovered On: **September 5, 2019 11:38 AM**

Vulnerabilities: 1
100 % Potential: 1
0 % Confirmed: 0

Associations	
Security Group	1
Auto Scaling Group	0
Load Balancer	0

General:

Instance Name:	EC2_Plus_Agent1_quays_bl43
Instance ID:	i-0fd5ad25d4aef1161
Instance Type:	t2.micro
First Discovered On:	September 5, 2019 11:38 AM
Instance Status:	-
State:	running
Spot Instance:	-
Image (AMI) ID:	ami-0cfee17793b08a293
Last Updated On:	September 10, 2019 2:18 PM

Location:

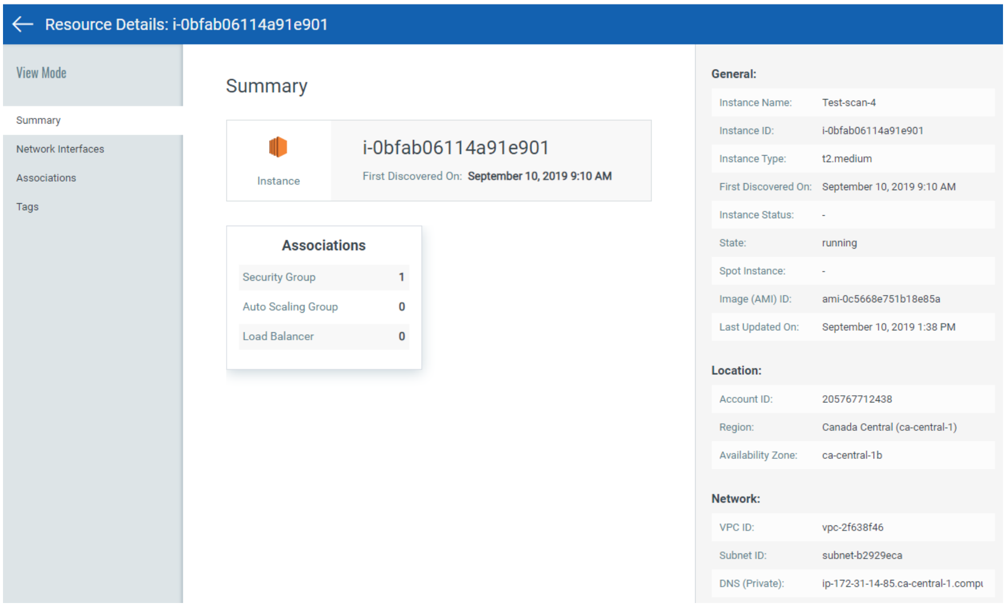
Account ID:	383031258652
Region:	N. Virginia (us-east-1)
Availability Zone:	us-east-1b

Network:

VPC ID:	vpc-ceacefb7
Subnet ID:	subnet-b355259f
DNS (Private):	ip-172-31-85-154.ec2.internal
DNS (Public):	ec2-52-55-244-224.compute-1.ama
IP Address (Public):	52.55.244.224
IP Address (Private):	172.31.85.154

Enhanced Information for Resource that also exists in Qualys Cloud Platform

Note: If the resource does not exist in Qualys Cloud Platform, the View Mode is displayed for the resource.



i-0bfab06114a91e901
First Discovered On: **September 10, 2019 9:10 AM**

Associations	
Security Group	1
Auto Scaling Group	0
Load Balancer	0

General:

Instance Name:	Test-scan-4
Instance ID:	i-0bfab06114a91e901
Instance Type:	t2.medium
First Discovered On:	September 10, 2019 9:10 AM
Instance Status:	-
State:	running
Spot Instance:	-
Image (AMI) ID:	ami-0c5668e751b18e85a
Last Updated On:	September 10, 2019 1:38 PM

Location:

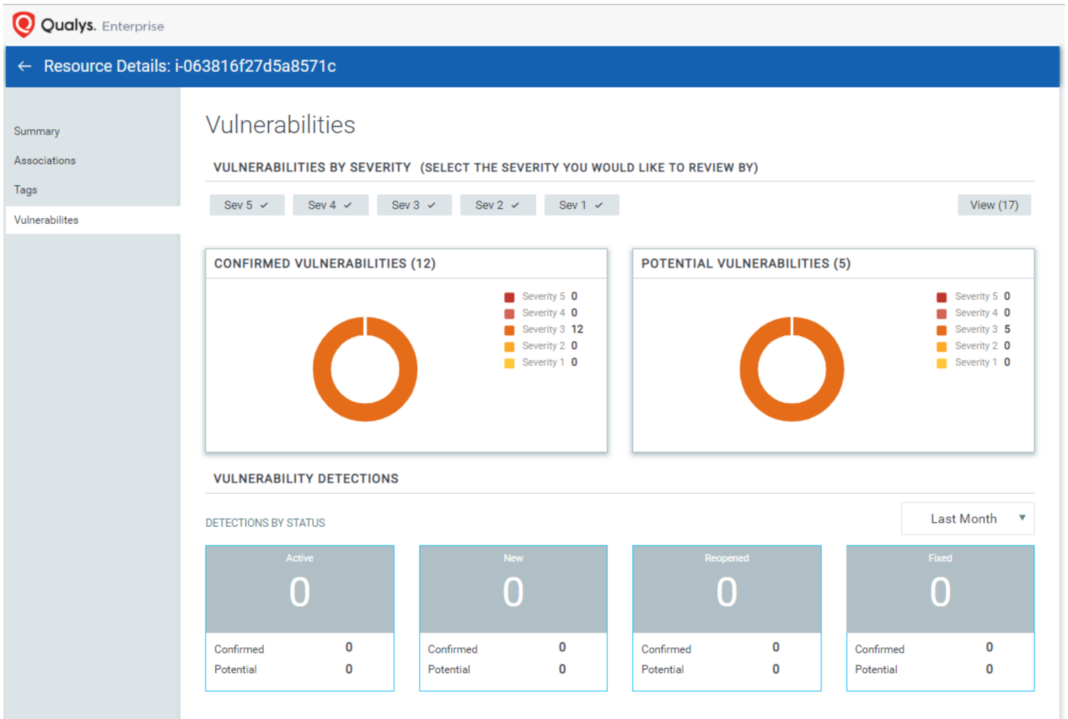
Account ID:	205767712438
Region:	Canada Central (ca-central-1)
Availability Zone:	ca-central-1b

Network:

VPC ID:	vpc-2f638f46
Subnet ID:	subnet-b2929eca
DNS (Private):	ip-172-31-14-85.ca-central-1.compu

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

- Summary
- Associations
- Tags
- Vulnerabilites

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	Confirmed 0	Confirmed 0	Confirmed 0
Potential 0	Potential 0	Potential 0	Potential 0

Drill down to Vulnerability Details for Instances (only for AWS)

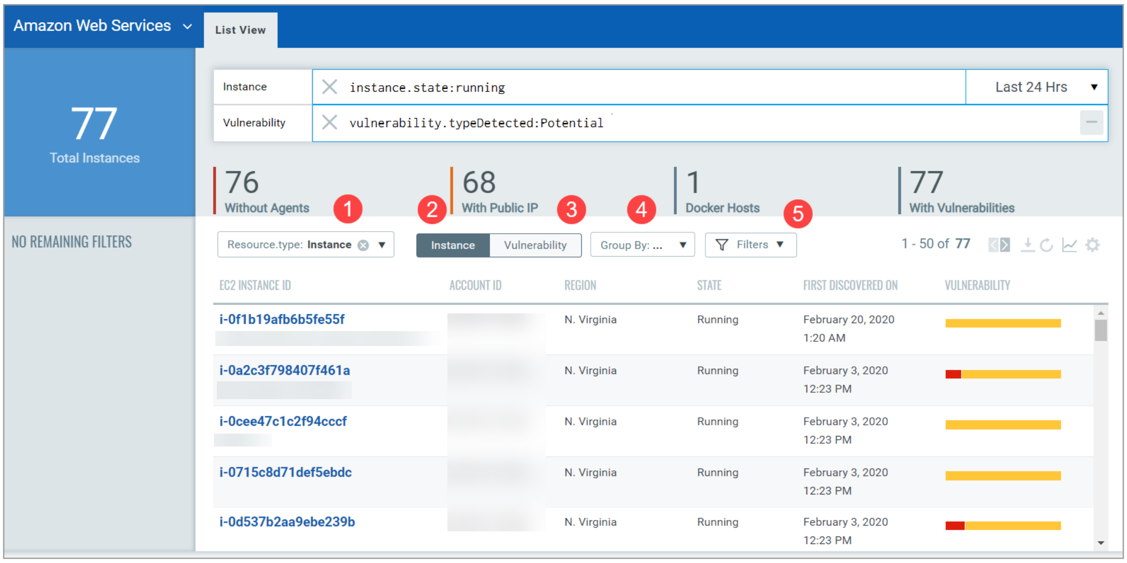
We provide you with multiple meta data filters to narrow down your search for vulnerability details. Using the new filters, you can get a complete view of vulnerability posture from an asset and vulnerability point of view.

Under Resources tab, select the Instance type of resource (AWS). Choose Instance resource type from the Resource drop-down.

The Resource Type drop-down is available to quickly view resource inventory of different types of resources. You can use the various metadata filters, group by options and custom query capabilities to find what you are interested in.

> Note: The vulnerability data is available only for Instance type of resource (AWS cloud provider) and only after the Instances have been scanned.

.



```
instance.state:running
vulnerability.typeDetected:Potential
```

EC2 INSTANCE ID	ACCOUNT ID	REGION	STATE	FIRST DISCOVERED ON	VULNERABILITY
i-0f1b19afb6b5fe55f	[redacted]	N. Virginia	Running	February 20, 2020 1:20 AM	
i-0a2c3f798407f461a	[redacted]	N. Virginia	Running	February 3, 2020 12:23 PM	
i-0cee47c1c2f94cccf	[redacted]	N. Virginia	Running	February 3, 2020 12:23 PM	
i-0715c8d71def5ebdc	[redacted]	N. Virginia	Running	February 3, 2020 12:23 PM	
i-0d537b2aa9ebe239b	[redacted]	N. Virginia	Running	February 3, 2020 12:23 PM	

1 - Indicates the type of resource

2 - Click to view instances in your inventory

3 - Click to view vulnerabilities that affect the instances in your cloud environment

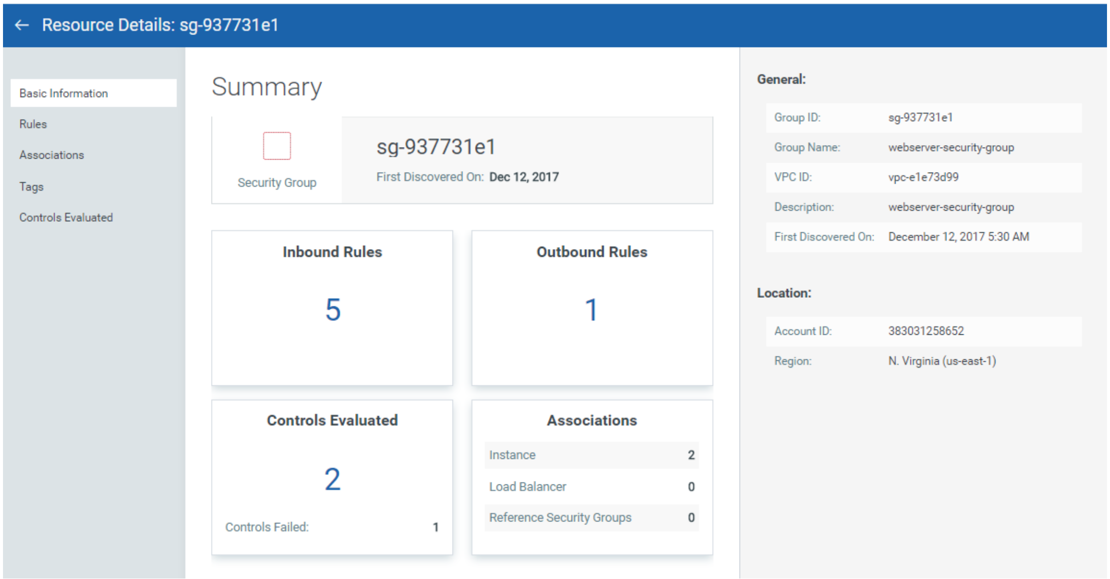
4 - Various group-by filters to narrow down your search

5 - Filters for Type of vulnerabilities

Using the various filters, you can drill down to view vulnerabilities that exists on instances. The search tokens give you further flexibility to narrow down your search results.

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	Outbound Rules
5	1

Controls Evaluated: 2
Controls Failed: 1

Associations	
Instance	2
Load Balancer	0
Reference Security Groups	0

General:

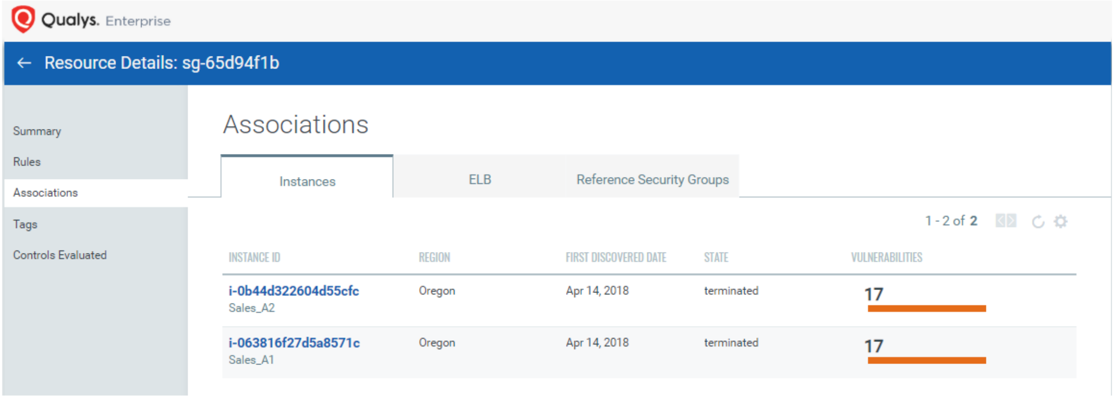
Group ID:	sg-937731e1
Group Name:	webserver-security-group
VPC ID:	vpc-e1e73d99
Description:	webserver-security-group
First Discovered On:	December 12, 2017 5:30 AM

Location:

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

View Security Group Associations

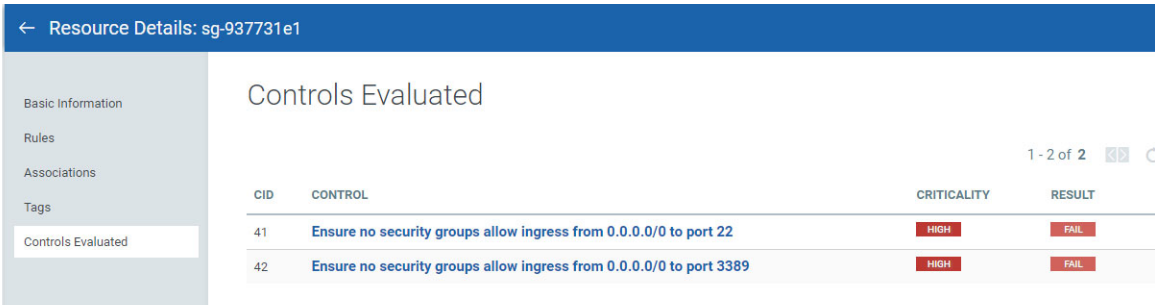
You can view various details about the associations such as the ID, region, state and so on.



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.



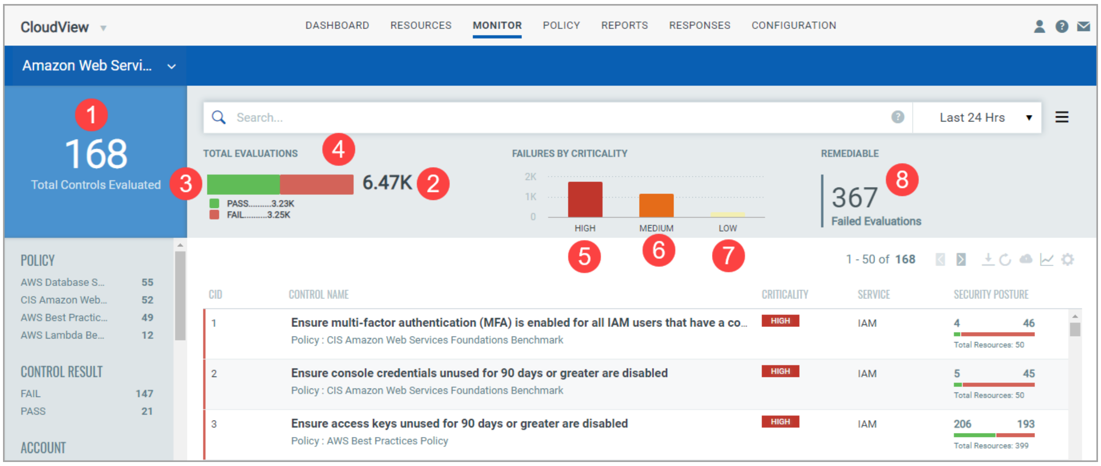
Controls Evaluated

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



POLICY	
AWS Database S...	55
CIS Amazon Web...	52
AWS Best Practic...	49
AWS Lambda Be...	12

CONTROL RESULT	
FAIL	147
PASS	21

ACCOUNT

CID	CONTROL NAME	CRITICALITY	SERVICE	SECURITY POSTURE
1	Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a co... Policy : CIS Amazon Web Services Foundations Benchmark	HIGH	IAM	4 46 Total Resources: 50
2	Ensure console credentials unused for 90 days or greater are disabled Policy : CIS Amazon Web Services Foundations Benchmark	HIGH	IAM	5 45 Total Resources: 50
3	Ensure access keys unused for 90 days or greater are disabled Policy : AWS Best Practices Policy	HIGH	IAM	206 193 Total Resources: 399

Let us see what each number signifies

1 - Total number of controls that are evaluated.

2 - Total number of evaluations. A unique combination of resource and control is treated as one evaluation.

3 - Number of evaluations that Passed. The Pass count includes control evaluations that are passed as well as passed with exception.

4 - Number of evaluations that Failed

5 - Number of failed evaluations with high criticality

6 - Number of failed evaluations with medium criticality

7 - Number of failed evaluations with low criticality

8 - Number of failed evaluations that can be remediated. Click to view the controls with failed evaluations that are remediable. For more information on remediating cloud misconfigurations, see Remediating Cloud Resources.

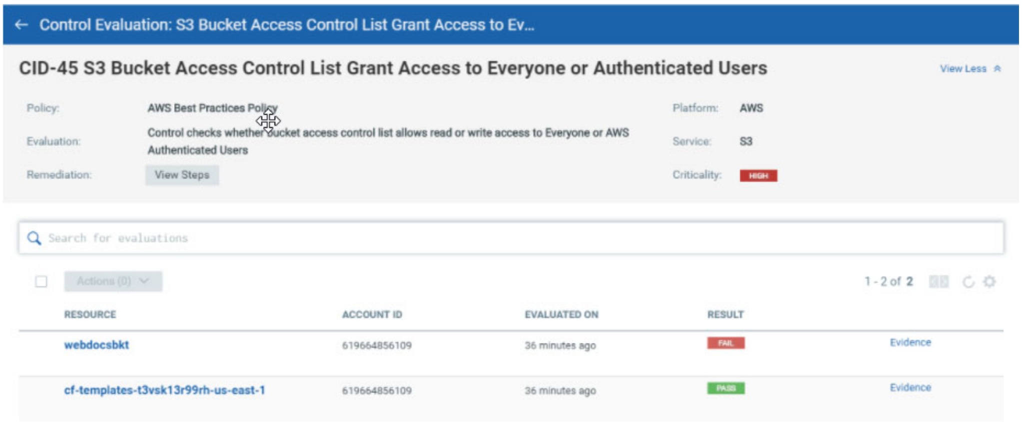
Note: When you change criticality of a control, the revised control criticality for existing evaluations is effective upon next connector run.

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 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

Policy: AWS Best Practices Policy

Evaluation: Control checks whether bucket access control list allows read or write access to Everyone or AWS Authenticated Users

Remediation: View Steps

Platform: AWS

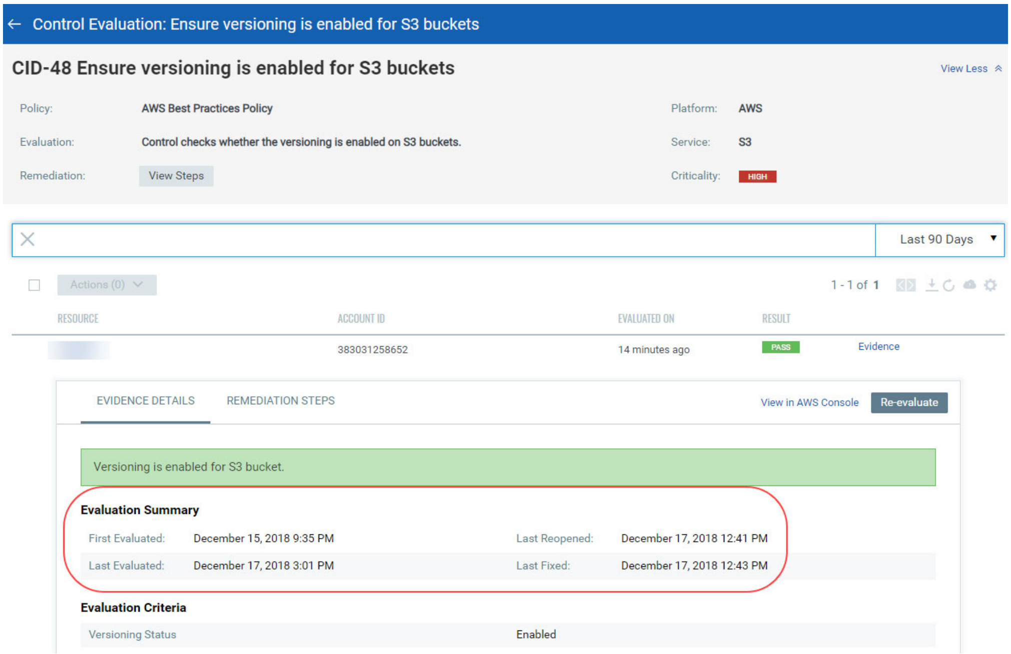
Service: S3

Criticality: HIGH

□	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.



CID-48 Ensure versioning is enabled for S3 buckets

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

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

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.

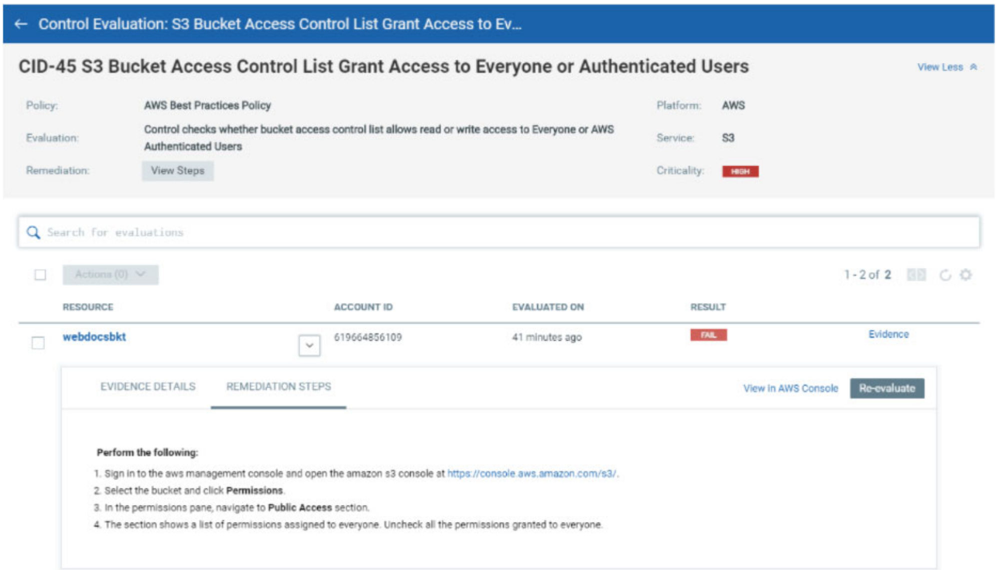
-Last Evaluated: The latest date when the control was evaluated.

-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.



← 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

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

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

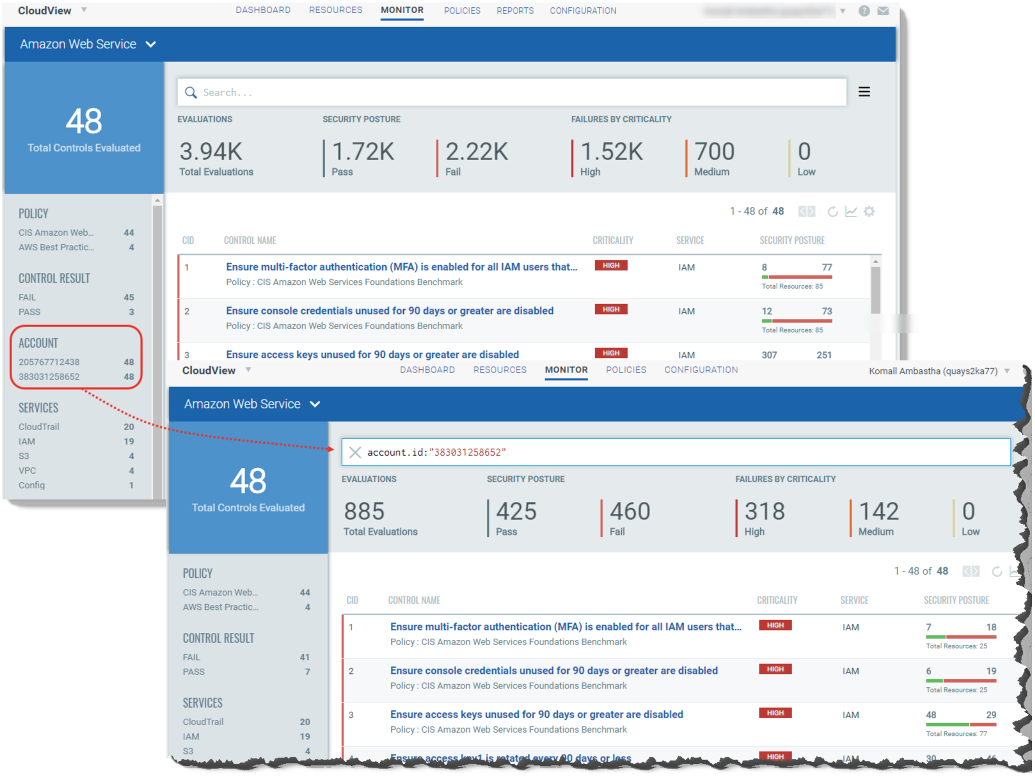
EVIDENCE DETAILS | REMEDIATION STEPS | View in AWS Console | Re-evaluate

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.



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

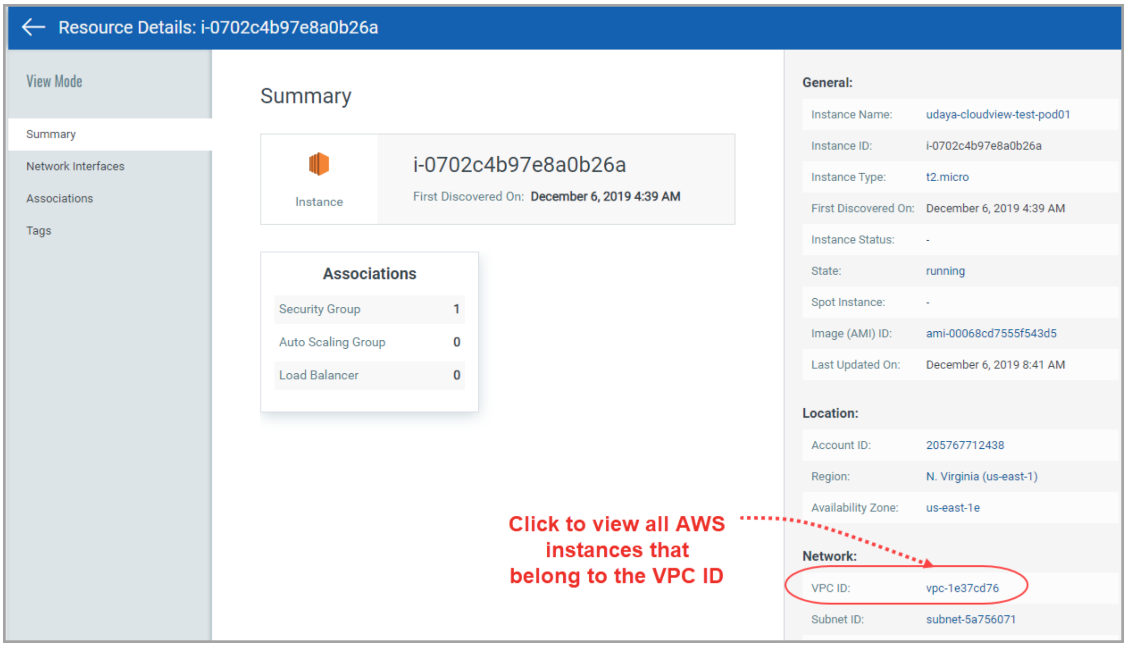
1 - 48 of 48

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
4	Ensure access key1 is rotated every 90 days or less	HIGH	IAM	30 46

Search Using Resource Parameter Information

You can search for all resources that match with the parameter information of a resource.For example, if you have a resource with certain specific parameter such as an AWS instance with specific VPC. You could search for all resources that belong to the same VPC ID and resource type.

Go to Resources, select Instance resource type and click on the EC2 Instance ID to view the details of the resource. All the searchable parameter information for that resource type is displayed with links on the right side.



i-0702c4b97e8a0b26a

First Discovered On: December 6, 2019 4:39 AM

Associations

Security Group	1
Auto Scaling Group	0
Load Balancer	0

General:

Instance Name:	udaya-cloudview-test-pod01
Instance ID:	i-0702c4b97e8a0b26a
Instance Type:	t2.micro
First Discovered On:	December 6, 2019 4:39 AM
Instance Status:	-
State:	running
Spot Instance:	-
Image (AMI) ID:	ami-00068cd7555f543d5
Last Updated On:	December 6, 2019 8:41 AM

Location:

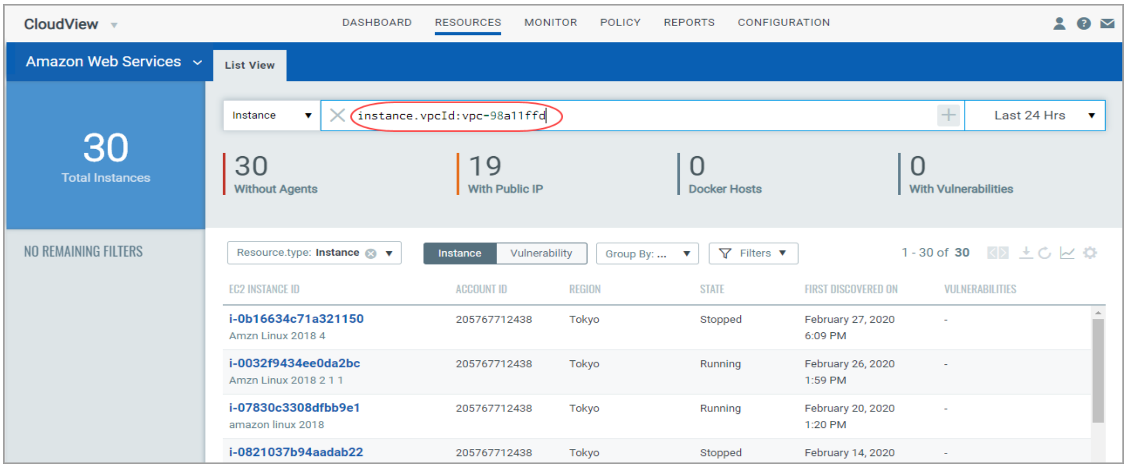
Account ID:	205767712438
Region:	N. Virginia (us-east-1)
Availability Zone:	us-east-1e

Network:

VPC ID:	vpc-1e37cd76
Subnet ID:	subnet-5a756071

Click to view all AWS instances that belong to the VPC ID

Click the link to automatically form the search query based on the VPC ID and view the search results.



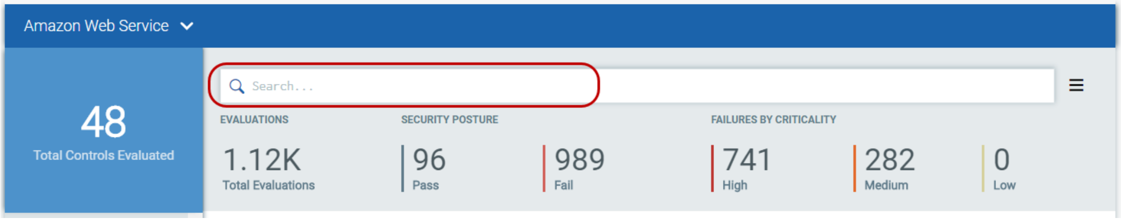
```
instance.vpcId:vpc-98a11ffd
```

EC2 INSTANCE ID	ACCOUNT ID	REGION	STATE	FIRST DISCOVERED ON	VULNERABILITIES
i-0b16634c71a321150 Amzn Linux 2018 4	205767712438	Tokyo	Stopped	February 27, 2020 6:09 PM	-
i-0032f9434ee0da2bc Amzn Linux 2018 2 1 1	205767712438	Tokyo	Running	February 26, 2020 1:59 PM	-
i-07830c3308dfbb9e1 amazon linux 2018	205767712438	Tokyo	Running	February 20, 2020 1:20 PM	-
i-0821037b94aadab22	205767712438	Tokyo	Stopped	February 14, 2020	-

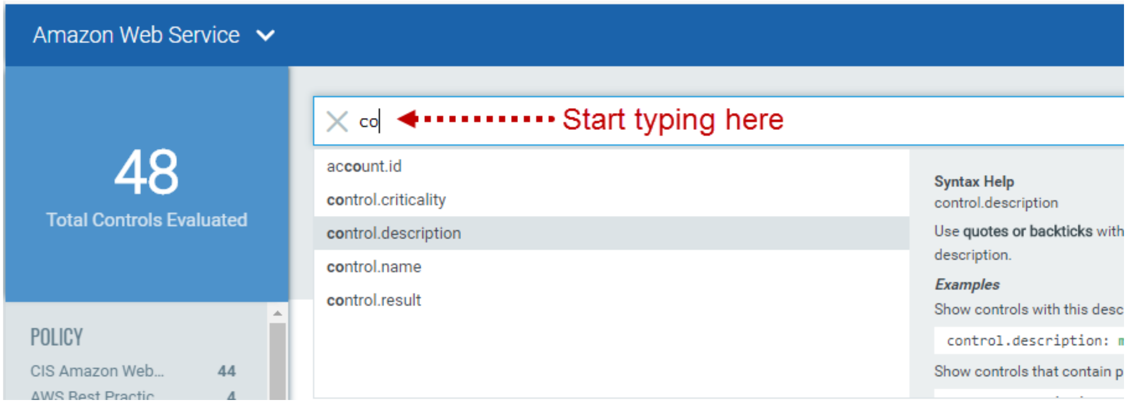
Search Policy Controls

Find all about your policies and control evaluations and get up to date information quickly using Qualys Advanced Search.

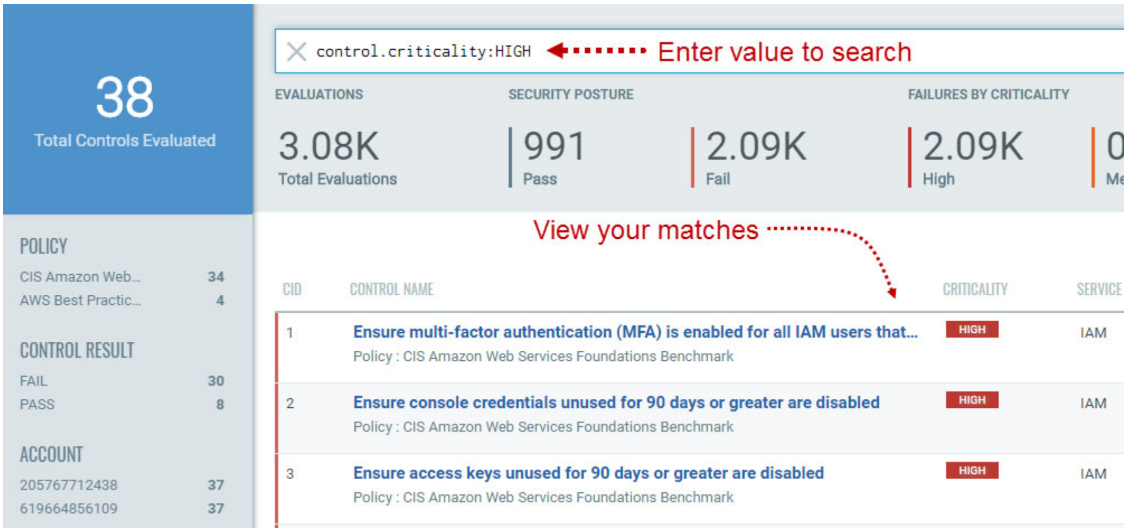
Go to Monitor tab. You'll notice a Search field above the controls list (you can also search on other tabs). This is where you'll enter your search query.



Start typing and we'll show you the properties you can search such as account ID, control criticality, control result, etc. Select the one you're interested in.



Now enter the value you want to match, and press Enter. You can also choose a date range. That's it! Your matches will appear in the list.



control.criticality:HIGH

Enter value to search

38
Total Controls Evaluated

POLICY	
CIS Amazon Web...	34
AWS Best Practic...	4

CONTROL RESULT	
FAIL	30
PASS	8

ACCOUNT	
205767712438	37
619664856109	37

EVALUATIONS: 3.08K Total Evaluations

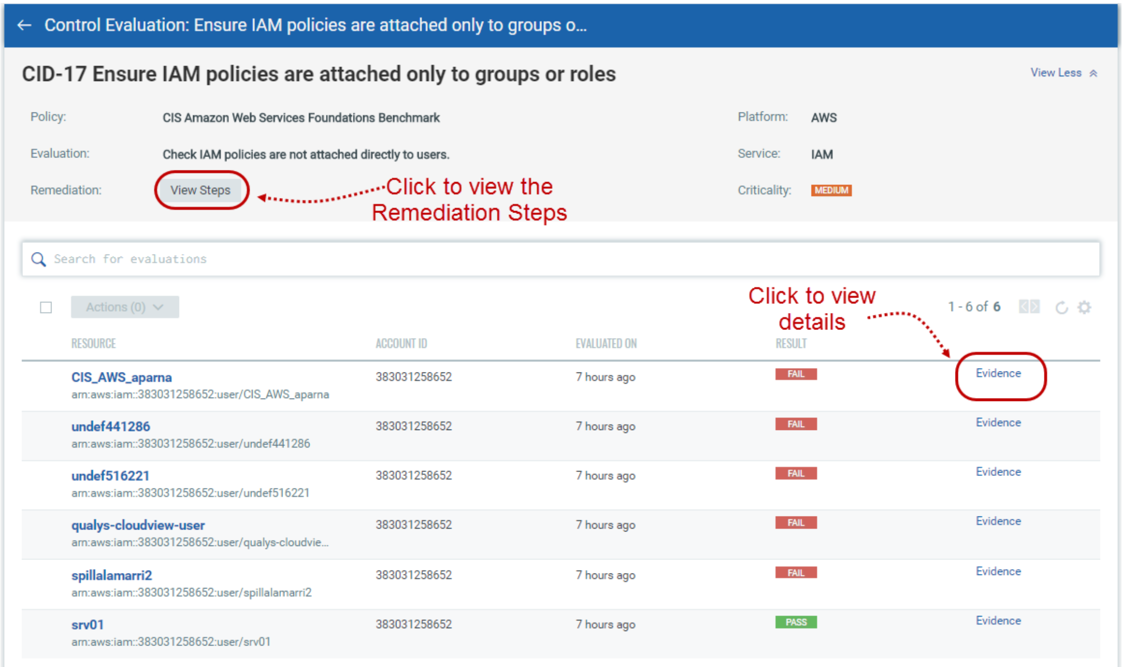
SECURITY POSTURE: 991 Pass | 2.09K Fail

FAILURES BY CRITICALITY: 2.09K High | 0 Me

View your matches

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

You'll notice a Search field and this is where you'll enter your search query.



Control Evaluation: Ensure IAM policies are attached only to groups o...

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

View Less

Policy: CIS Amazon Web Services Foundations Benchmark

Evaluation: Check IAM policies are not attached directly to users.

Remediation: View Steps

Platform: AWS

Service: IAM

Criticality: MEDIUM

Click to view the Remediation Steps

Search for evaluations

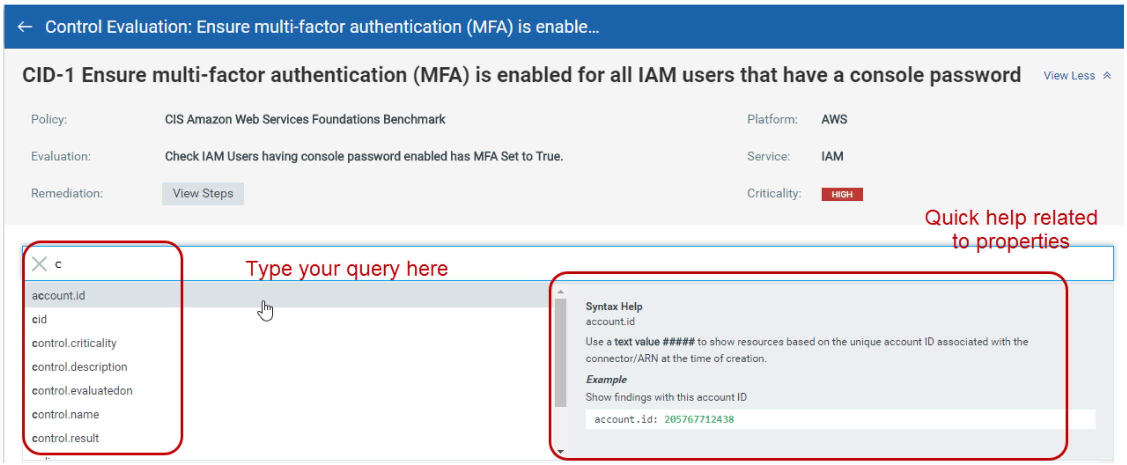
□ Actions (0)

Click to view details

1 - 6 of 6

RESOURCE	ACCOUNT ID	EVALUATED ON	RESULT	
CIS_AWS_aparna arn:aws:iam::383031258652:user/CIS_AWS_aparna	383031258652	7 hours ago	FAIL	Evidence
undef441286 arn:aws:iam::383031258652:user/undef441286	383031258652	7 hours ago	FAIL	Evidence
undef516221 arn:aws:iam::383031258652:user/undef516221	383031258652	7 hours ago	FAIL	Evidence
qualys-cloudview-user arn:aws:iam::383031258652:user/qualys-cloudvie...	383031258652	7 hours ago	FAIL	Evidence
spillalamarri2 arn:aws:iam::383031258652:user/spillalamarri2	383031258652	7 hours ago	FAIL	Evidence
srv01 arn:aws:iam::383031258652:user/srv01	383031258652	7 hours ago	PASS	Evidence

Start typing and we'll show you the properties you can search such as cid, control.name, and so on. Select the one you're interested in.



← Control Evaluation: Ensure multi-factor authentication (MFA) is enable...

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

Policy: CIS Amazon Web Services Foundations Benchmark

Evaluation: Check IAM Users having console password enabled has MFA Set to True.

Remediation: View Steps

Platform: AWS

Service: IAM

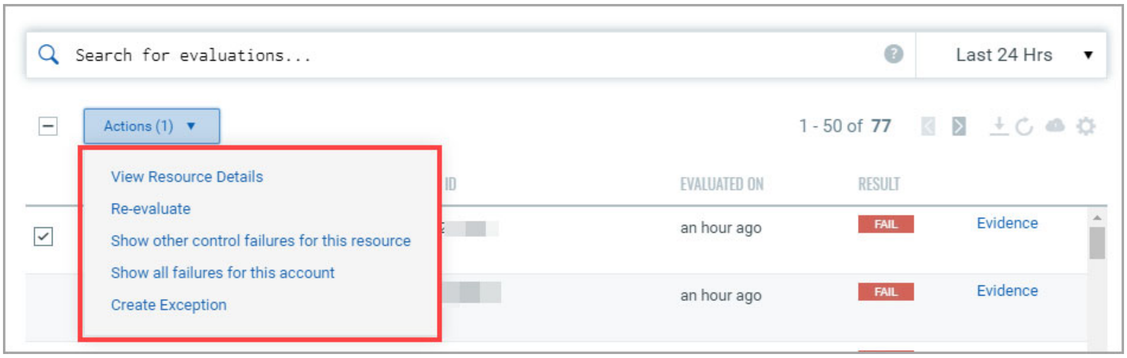
Criticality: HIGH

Syntax Help
account.id
Use a **text value #####** to show resources based on the unique account ID associated with the connector/ARN at the time of creation.

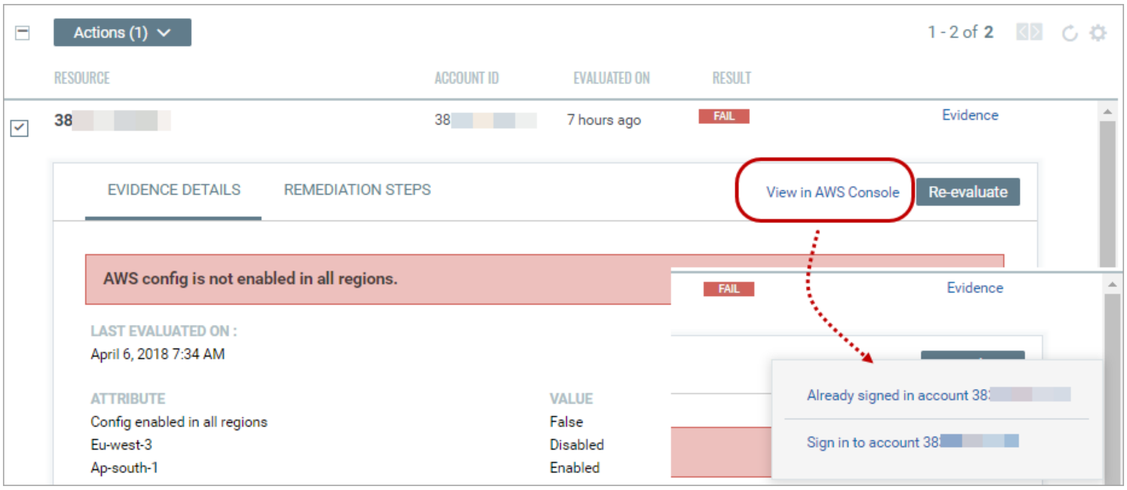
Example
Show findings with this account ID

```
account.id: 205767712438
```

You could perform various actions on the controls such as re-evaluate the control, create exception for a failed resource, and so on. Select the control and click Actions or the quick actions menu. See Exceptions to know more about exception.



To know what led the control to pass or fail, click Evidence. The Evidence details will tell you the reason that led the control to pass or fail.



AWS config is not enabled in all regions.

LAST EVALUATED ON :
April 6, 2018 7:34 AM

ATTRIBUTE	VALUE
Config enabled in all regions	False
Eu-west-3	Disabled
Ap-south-1	Enabled

Exceptions

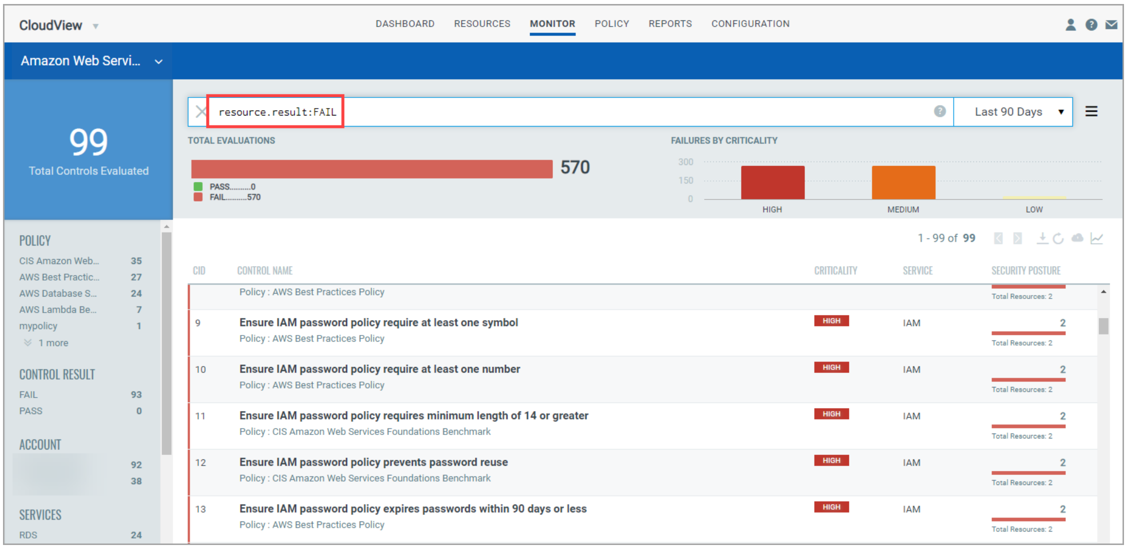
You may want to create exceptions to exempt certain cloud resources from a particular control or temporarily change the status of a resource for a particular control from Failed to PassE (Pass with Exception).

For example, it may be the policy in an organization that a particular cloud resource is not allowed on any server or port. However, there could be a business need for the organization to provide an exception for one or more resources on a temporary basis. This may be required to support a custom application or other business need. You could use exceptions in such scenarios.

Create Exception

Here are quick steps to create an exception.

1. Go to Monitor tab. You'll notice a Search field above the controls list. Enter your search query for failed evaluations and click the required control in the search results to view the control evaluations.



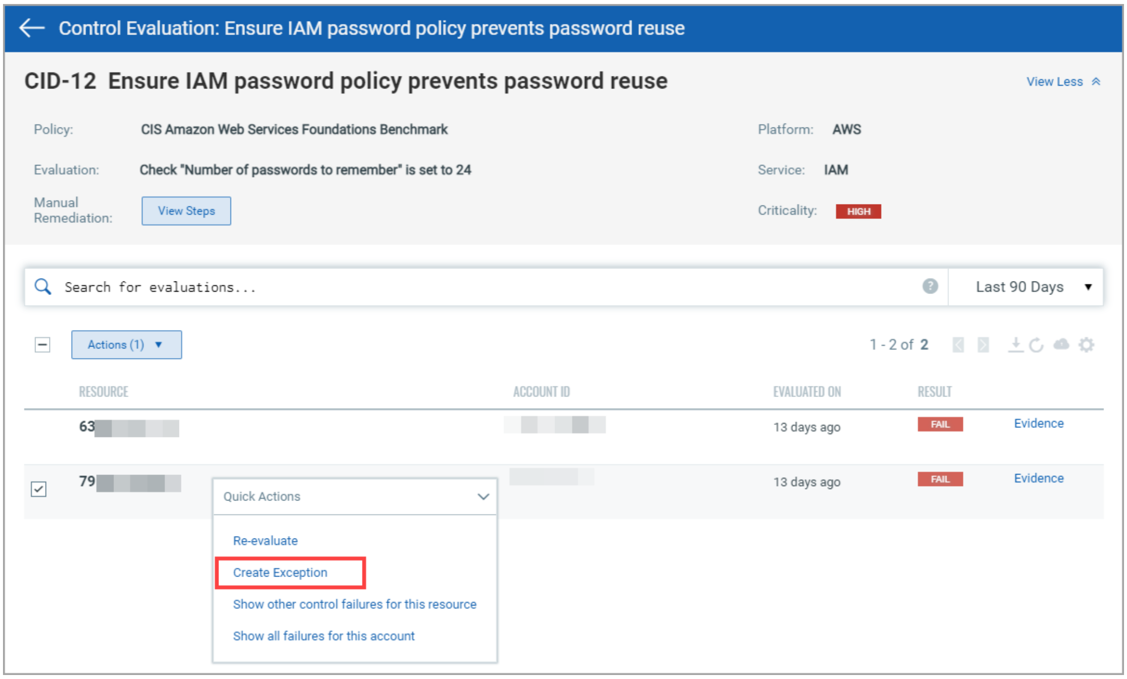
resource.result:FAIL

Last 90 Days

POLICY	
CIS Amazon Web...	35
AWS Best Practic...	27
AWS Database S...	24
AWS Lambda Be...	7
mypolicy	1
1 more	
CONTROL RESULT	
FAIL	93
PASS	0
ACCOUNT	
[redacted]	92
[redacted]	38
SERVICES	
RDS	24

CID	CONTROL NAME	CRITICALITY	SERVICE	SECURITY POSTURE
	Policy : AWS Best Practices Policy			Total Resources: 2
9	Ensure IAM password policy require at least one symbol Policy : AWS Best Practices Policy	HIGH	IAM	2 Total Resources: 2
10	Ensure IAM password policy require at least one number Policy : AWS Best Practices Policy	HIGH	IAM	2 Total Resources: 2
11	Ensure IAM password policy requires minimum length of 14 or greater Policy : CIS Amazon Web Services Foundations Benchmark	HIGH	IAM	2 Total Resources: 2
12	Ensure IAM password policy prevents password reuse Policy : CIS Amazon Web Services Foundations Benchmark	HIGH	IAM	2 Total Resources: 2
13	Ensure IAM password policy expires passwords within 90 days or less Policy : AWS Best Practices Policy	HIGH	IAM	2 Total Resources: 2

2. Select the failed resource for which you want to create an exception and click Create Exception from the quick actions menu.



Control Evaluation: Ensure IAM password policy prevents password reuse

CID-12 Ensure IAM password policy prevents password reuse

Policy: CIS Amazon Web Services Foundations Benchmark

Platform: AWS

Evaluation: Check "Number of passwords to remember" is set to 24

Service: IAM

Manual Remediation: View Steps

Criticality: HIGH

Search for evaluations...

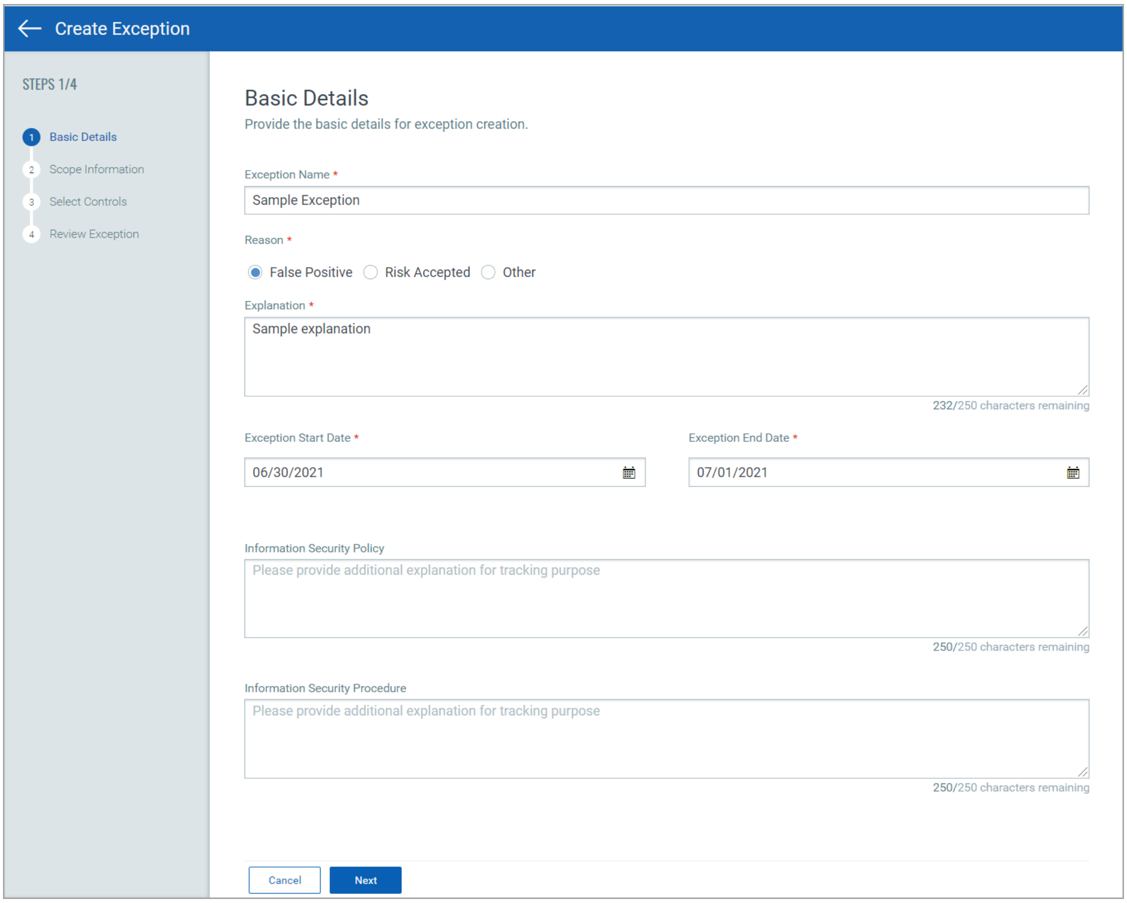
Last 90 Days

	RESOURCE	ACCOUNT ID	EVALUATED ON	RESULT	
	63[redacted]	[redacted]	13 days ago	FAIL	Evidence
☑	79[redacted]	[redacted]	13 days ago	FAIL	Evidence

Note: The Create Exception option is available in the quick action menu only for resources with failed control evaluations (FAIL).

3. The Exception wizard is displayed. Provide the following details for the exception:

- Basis details such as name for the exception, reason to create the exception, an explanation, start and end date for the exception. Optionally, you could also provide the information regarding the security policy and procedure for which the exception is being created.



Basic Details

Provide the basic details for exception creation.

Exception Name *: Sample Exception

Reason *: ● False Positive ○ Risk Accepted ○ Other

Explanation *: Sample explanation

232/250 characters remaining

Exception Start Date *: 06/30/2021

Exception End Date *: 07/01/2021

Information Security Policy: Please provide additional explanation for tracking purpose

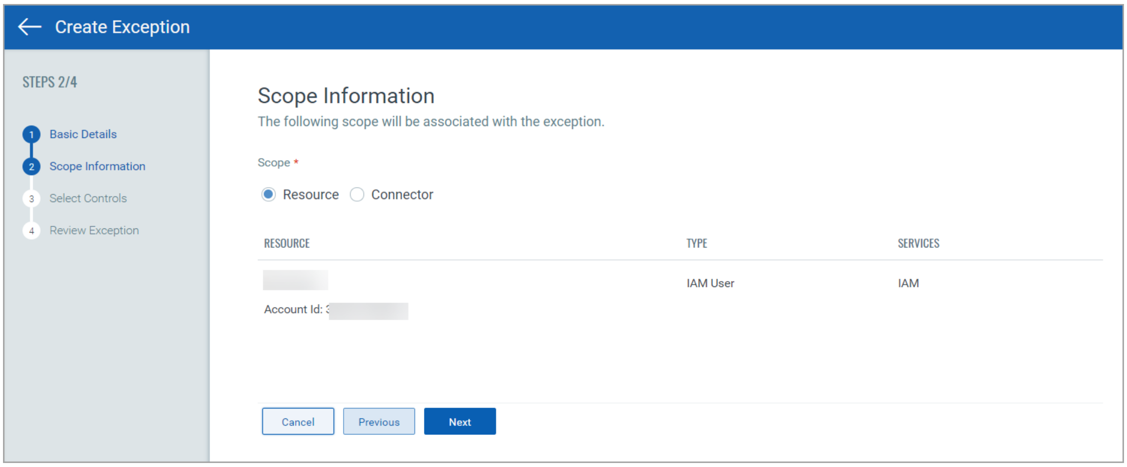
250/250 characters remaining

Information Security Procedure: Please provide additional explanation for tracking purpose

250/250 characters remaining

- Scope Information: Decides the scope of the exception you are creating. By default, Resource option is selected. You could expand the scope of the exception to all resources in a specific account.

- Resource: Choose to create exception at resource level and the exception is applicable only for the selected resource.



Scope Information

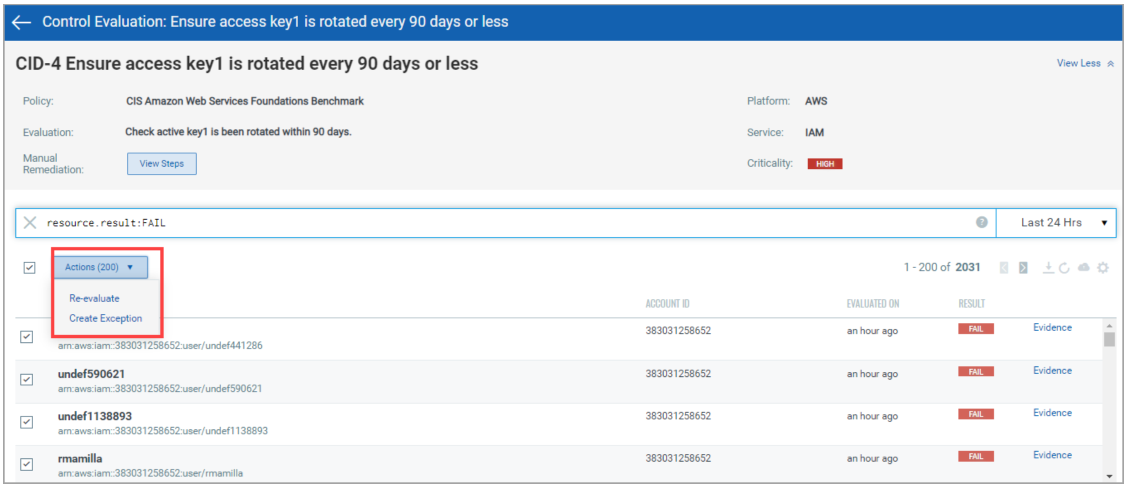
The following scope will be associated with the exception.

Scope *

● Resource ○ Connector

RESOURCE	TYPE	SERVICES
[redacted] Account Id: 3[redacted]	IAM User	IAM

You can associate maximum 200 resources with an exception during creation. For example, if you configure number of rows shown to be 200, and then select all resources on the page and click Create Exception from Actions menu.



Control Evaluation: Ensure access key1 is rotated every 90 days or less
View Less

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

Policy: CIS Amazon Web Services Foundations Benchmark

Evaluation: Check active key1 is been rotated within 90 days.

Manual Remediation: View Steps

Platform: AWS

Service: IAM

Criticality: HIGH

```
resource.result:FAIL
```

Last 24 Hrs

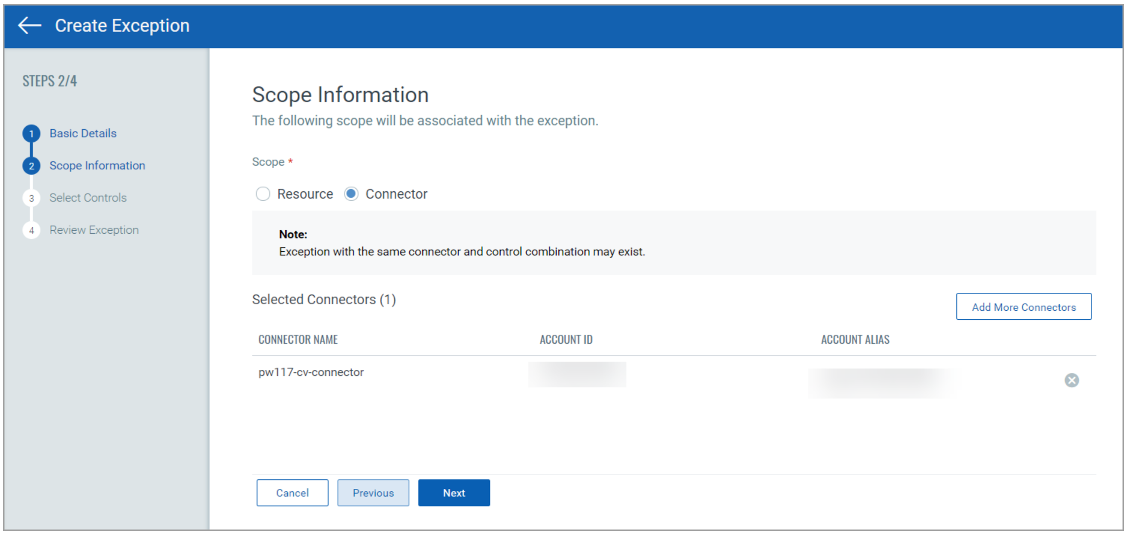
☑ Actions (200) ▾
Re-evaluate
Create Exception

1 - 200 of 2031

		ACCOUNT ID	EVALUATED ON	RESULT	
☑	arn:aws:iam::383031258652:user/undef441286	383031258652	an hour ago	FAIL	Evidence
☑	**undef590621** arn:aws:iam::383031258652:user/undef590621	383031258652	an hour ago	FAIL	Evidence
☑	**undef1138893** arn:aws:iam::383031258652:user/undef1138893	383031258652	an hour ago	FAIL	Evidence
☑	**rmamilla** arn:aws:iam::383031258652:user/rmamilla	383031258652	an hour ago	FAIL	Evidence

As a result, all the selected 200 resources get associated with the exception you create. As we have a limitation of displaying 200 rows on a page, we cannot associate more than 200 resources with a single exception.

- Connector: Choose to create exception for all resources in the account associated with the connector. By default, the connector associated with the resource is selected. You could click Add More Connectors to add multiple connectors for the exception.



Scope Information

The following scope will be associated with the exception.

Scope *

○ Resource ● Connector

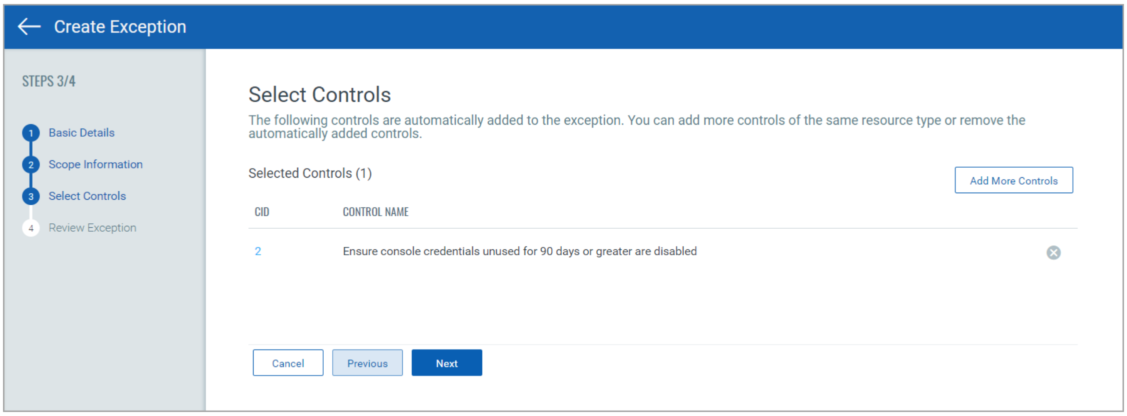
Note:
Exception with the same connector and control combination may exist.

Selected Connectors (1)

CONNECTOR NAME	ACCOUNT ID	ACCOUNT ALIAS
pw117-cv-connector	[redacted]	[redacted]

Note: The exception created at connector level is implemented on the resource evaluation result in the next connector run.

- Controls: The control for which the evaluation failed is auto-populated. Click Add More Controls to include more controls of the same resource type.



Select Controls

The following controls are automatically added to the exception. You can add more controls of the same resource type or remove the automatically added controls.

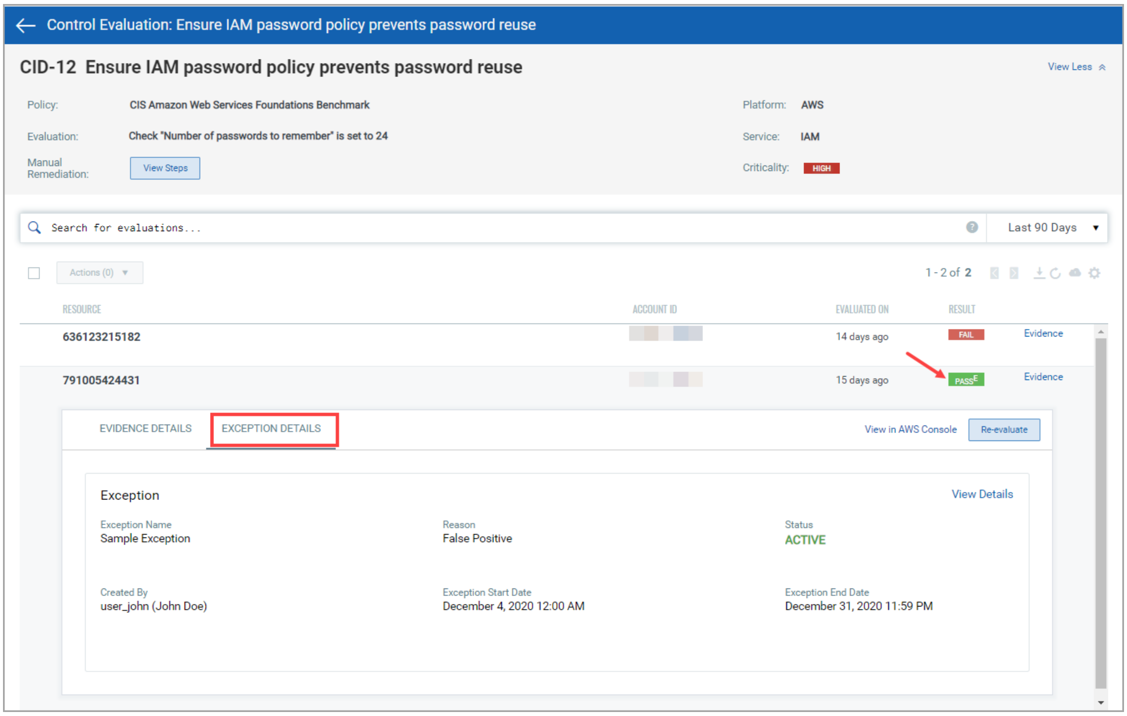
Selected Controls (1)

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

4. Review the information you provide for the exception and click Create Exception.

That’s it! The exception is created. The exceptions you create are listed in Exceptions tab. Go to Policy > Exceptions to view the list of all exceptions.

Once the exception is in ACTIVE status, the resource result immediately changes from Fail to PassE (Pass with Exception). The Exception Details section in Evidence displays all the exception details. The exception details are updated only when the exception status changes or on every connector run.



Control Evaluation: Ensure IAM password policy prevents password reuse

CID-12 Ensure IAM password policy prevents password reuse

Policy: CIS Amazon Web Services Foundations Benchmark

Evaluation: Check "Number of passwords to remember" is set to 24

Manual Remediation:

Platform: AWS

Service: IAM

Criticality: HIGH

RESOURCE	ACCOUNT ID	EVALUATED ON	RESULT	
636123215182	[redacted]	14 days ago	FAIL	Evidence
791005424431	[redacted]	15 days ago	PASSE	Evidence

Exception

Exception Name
Sample Exception

Reason
False Positive

Status
ACTIVE

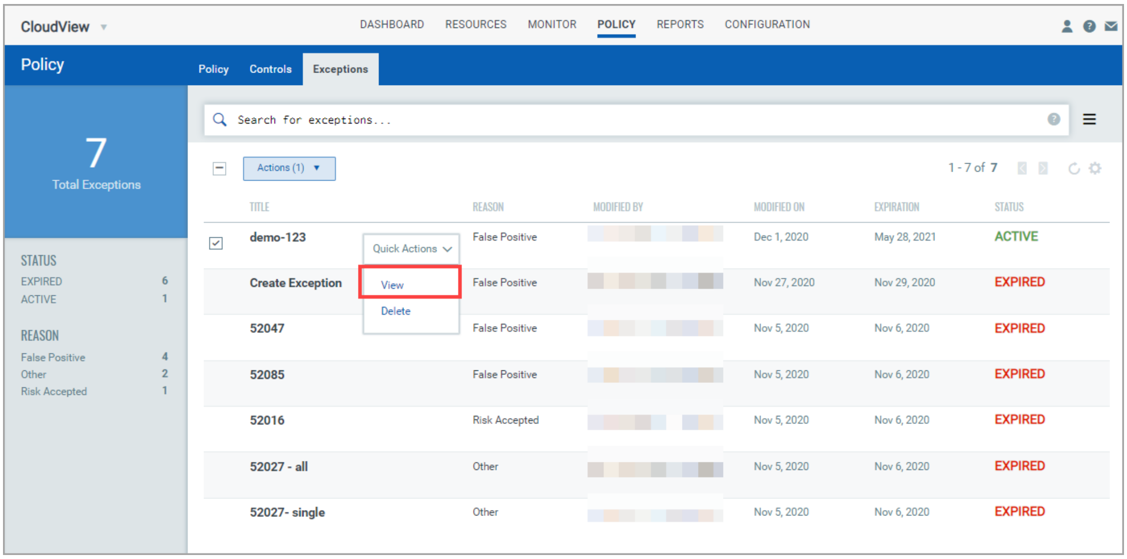
Created By
user_john (John Doe)

Exception Start Date
December 4, 2020 12:00 AM

Exception End Date
December 31, 2020 11:59 PM

View Exceptions

Go to Policy > Exceptions to see exceptions. Select View from the quick actions menu for any exception to view complete details about the exception. You can also view a history log for the exception.



7
Total Exceptions

STATUS

EXPIRED	6
ACTIVE	1

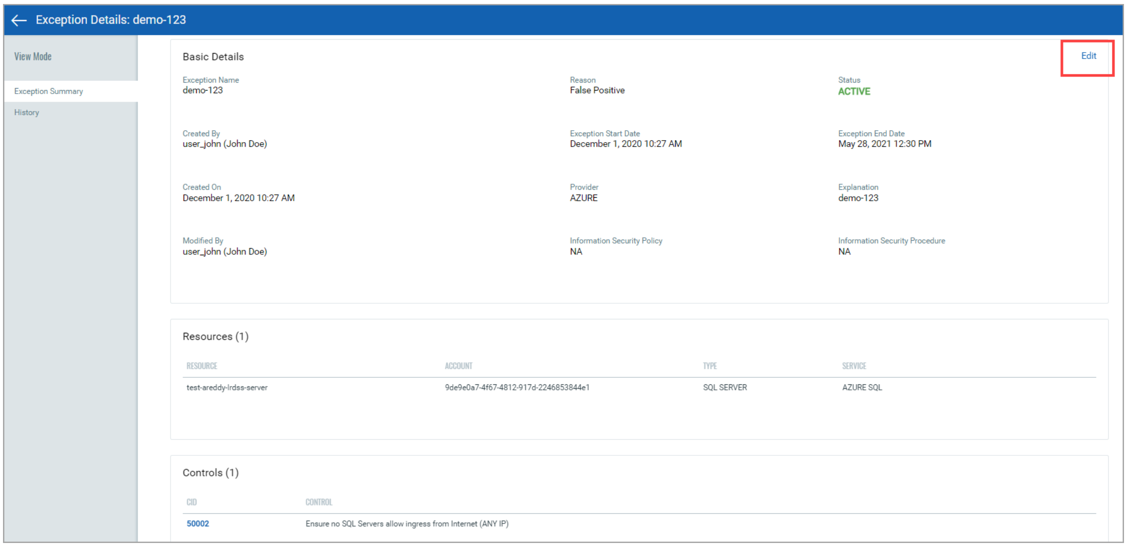
REASON

False Positive	4
Other	2
Risk Accepted	1

TITLE	REASON	MODIFIED BY	MODIFIED ON	EXPIRATION	STATUS
☑ demo-123	False Positive	[redacted]	Dec 1, 2020	May 28, 2021	ACTIVE
Create Exception	False Positive	[redacted]	Nov 27, 2020	Nov 29, 2020	EXPIRED
52047	False Positive	[redacted]	Nov 5, 2020	Nov 6, 2020	EXPIRED
52085	False Positive	[redacted]	Nov 5, 2020	Nov 6, 2020	EXPIRED
52016	Risk Accepted	[redacted]	Nov 5, 2020	Nov 6, 2020	EXPIRED
52027 - all	Other	[redacted]	Nov 5, 2020	Nov 6, 2020	EXPIRED
52027- single	Other	[redacted]	Nov 5, 2020	Nov 6, 2020	EXPIRED

Edit Exceptions?

You can edit exceptions when they are in active status. You can change the start date, end date, explanation, controls associated with the exception, information security policy, and information security procedure. Go to Policy > Exceptions to see exceptions. Select View from the quick actions menu. Click Edit in the Exception Summary tab to edit the required exception details.



Basic Details

Exception Name
demo-123

Reason
False Positive

Status
ACTIVE

Created By
user_john (John Doe)

Exception Start Date
December 1, 2020 10:27 AM

Exception End Date
May 28, 2021 12:30 PM

Created On
December 1, 2020 10:27 AM

Provider
AZURE

Explanation
demo-123

Modified By
user_john (John Doe)

Information Security Policy
NA

Information Security Procedure
NA

Resources (1)

RESOURCE	ACCOUNT	TYPE	SERVICE
test-areddy-lrdss-server	9de9e0a7-4f67-4812-917d-2246853844e1	SQL SERVER	AZURE SQL

Controls (1)

CID	CONTROL
50002	Ensure no SQL Servers allow ingress from Internet (ANY IP)

Note: You cannot edit exceptions that are expired.

Delete exceptions?

Yes. Users with required permissions can delete any exception. Users with reader permissions can only view exceptions.

Important - When exceptions are deleted, the exception history is permanently removed and cannot be recovered.

Exception History

All actions are logged in the exception history with the name of the user who performed the action and a time stamp for when the action took place. Select View from the quick actions menu for any exception and then go to the History section. The original exception request and each action taken on the exception since the request are listed.

Exception Status

Exception status levels include:

Inactive: An exception is in inactive status if the current date is lesser than the start date of the Exception. Once the current date and start date match, the exception automatically changes to active status.

Active: An exception is in active status when the current date falls between the start date and end date of the Exception.

Expired: An exception is in expired status if the current date exceeds the end date of the Exception. When an exception is expired, a status of Fail appears again for the resource in control evaluation.

Use Existing Exception to Create New Exception

Go to Policy > Exceptions to see exceptions. Select an existing exception from the list and click Copy from the quick actions menu. The exception creation wizard is displayed with settings pre-configured from the existing exception. Thus, you can alter the required settings and create a new exception using the pre-populated configuration.

Policies and Controls

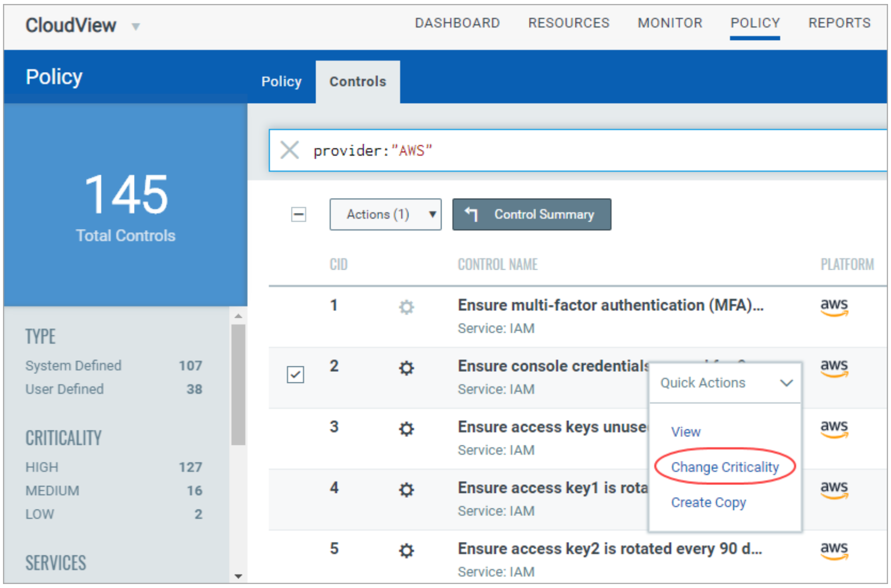
CloudView continuously discovers resources and ensures resources are compliant in relation to respective Benchmark & Best Practices policy provided out-of-the-box.

Customize Controls

Controls are the building blocks of the policies used to measure and report compliance for a set of hosts. We provide many controls for you to choose from and you can customize them too. Controls play the key part in the compliance posture of resource.

Control Criticality

You can modify the criticality of any control to suit your need. If the control criticality needs to be changed to match your environment, you can select the control, select Change Criticality from quick action menu.

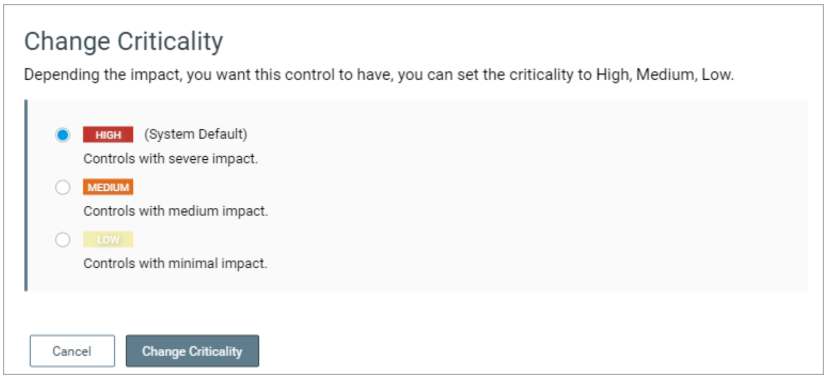


provider:"AWS"

TYPE	
System Defined	107
User Defined	38
CRITICALITY	
HIGH	127
MEDIUM	16
LOW	2
SERVICES	

	CID	CONTROL NAME	PLATFORM
□	1	Ensure multi-factor authentication (MFA)... Service: IAM	aws
☑	2	Ensure console credentials Service: IAM	aws
□	3	Ensure access keys unuse Service: IAM	aws
□	4	Ensure access key1 is rota Service: IAM	aws
□	5	Ensure access key2 is rotated every 90 d... Service: IAM	aws

Select the criticality you want to assign to the control and click Change Criticality.



Change Criticality

Depending the impact, you want this control to have, you can set the criticality to High, Medium, Low.

● HIGH (System Default)
Controls with severe impact.

○ MEDIUM
Controls with medium impact.

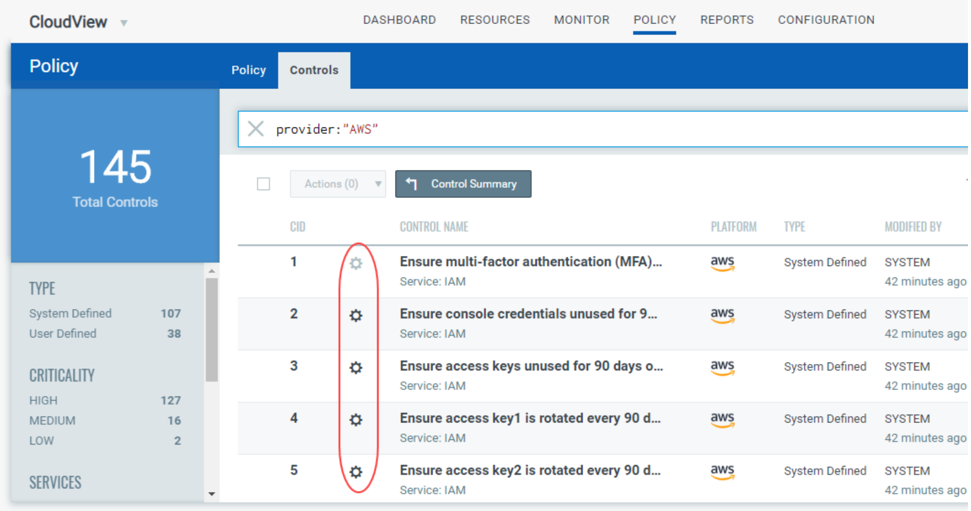
○ LOW
Controls with minimal impact.

Note: When you change criticality, the revised control criticality for existing evaluations is effective on Monitor View upon next connector run.

Let us consider a scenario where a control with HIGH criticality evaluated three resources. Now, if you change the criticality of the control to LOW, the change in evaluation results reflects only after connector run. During the connector run, assume that only two resources get detected. The control evaluation results for resources that get detected post connector run will reflect LOW criticality. However, control evaluation result for the resource that did not get detected post connector run will be counted as HIGH criticality.

System Controls

System-defined Control is a predefined control provided by Qualys. Few system-defined controls are customizable while others are not. The control indicator icon tells us if the control is customizable or not.



provider:"AWS"

145
Total Controls

TYPE

System Defined	107
User Defined	38

CRITICALITY

HIGH	127
MEDIUM	16
LOW	2

CID		CONTROL NAME	PLATFORM	TYPE	MODIFIED BY
1	⚙	Ensure multi-factor authentication (MFA)... Service: IAM	aws	System Defined	SYSTEM 42 minutes ago
2	⚙	Ensure console credentials unused for 9... Service: IAM	aws	System Defined	SYSTEM 42 minutes ago
3	⚙	Ensure access keys unused for 90 days o... Service: IAM	aws	System Defined	SYSTEM 42 minutes ago
4	⚙	Ensure access key1 is rotated every 90 d... Service: IAM	aws	System Defined	SYSTEM 42 minutes ago
5	⚙	Ensure access key2 is rotated every 90 d... Service: IAM	aws	System Defined	SYSTEM 42 minutes ago

⚙ - for System Defined Controls. Such controls cannot be customized. You cannot alter the parameter values for such system-defined controls.

⚙ - used to indicate that the control can be customized to suit your need. You can change the parameters values for such controls and customize them as per your organization’s requirements.

User-Defined Controls

⚙ used to indicate that the control can be customized. You can copy any system-defined control to make your own user-defined controls that you can customize to meet your needs.

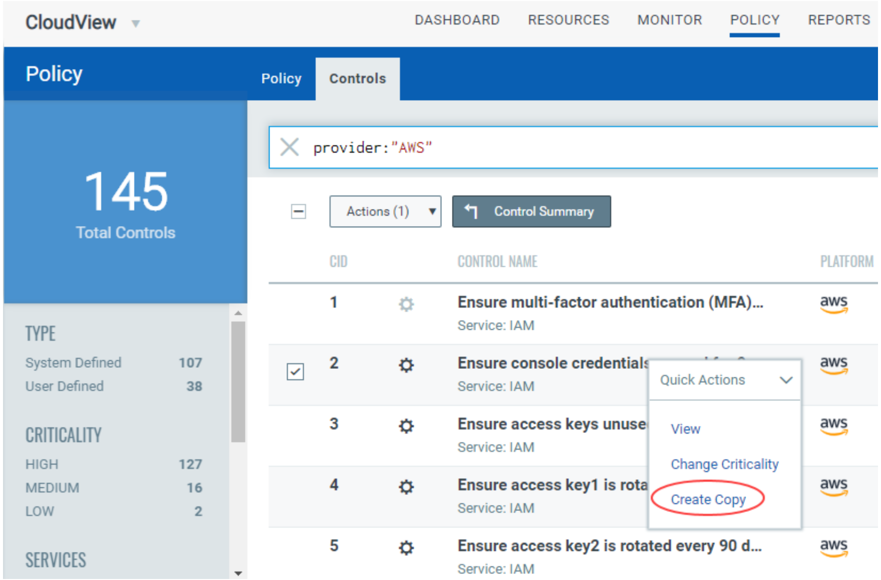
Copy Control and Customize

Go to Policy > Controls and select the control to be customized, select Create Copy from the quick action menu. The ⚙ icon is used to indicate that the control can be customized. Currently, 12 AWS and 2 Azure controls are customizable.

You can then modify the parameters of the control as per your requirement and save the customized control. The customized control is available to associate with policy and evaluate the resources.

For example, let us modify the minimum password length to 10 for AWS CID 11.

(1) Select the control and click Create Copy from quick action menu.



provider:"AWS"

145
Total Controls

TYPE	
System Defined	107
User Defined	38
CRITICALITY	
HIGH	127
MEDIUM	16
LOW	2
SERVICES	

	CID	CONTROL NAME	PLATFORM
	1	Ensure multi-factor authentication (MFA)... Service: IAM	aws
☑	2	Ensure console credentials Service: IAM	aws
	3	Ensure access keys unuse Service: IAM	aws
	4	Ensure access key1 is rota Service: IAM	aws
	5	Ensure access key2 is rotated every 90 d... Service: IAM	aws

(2) Change the name of control and criticality if needed. Click Next

(3) Set the expected value in Evaluation Parameter to 10. Change other aspects such as Evaluation Description, Evaluation Message as per your need. Click Next.

(4) Update the Additional Details if needed. Click Create.

That's it! Your new custom control is ready to use.

Can I edit controls?

Yes. Choose the user-defined control to be edited and choose Edit from the quick action menu. You can edit only user-defined controls. You cannot edit system-defined control.

Can I delete controls?

Yes. Choose the user-defined control to be deleted and choose Edit from the quick action menu. You can delete only user-defined controls. You cannot delete system-defined control.

Build Your Own Policy

A policy is a collection of controls used to measure and report compliance for a set of resources. Your compliance reports will show you resource compliance status (pass or fail) with the policy controls. You could use the policies we provide of build your own policy.

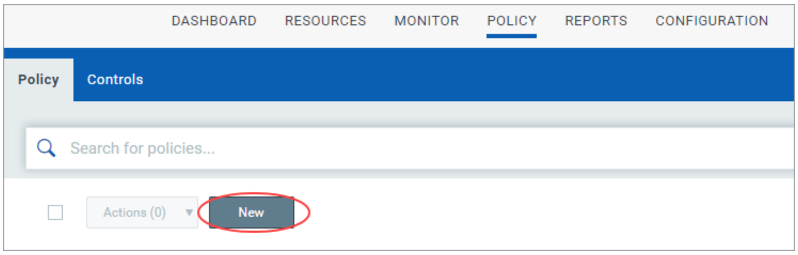
System Defined Policy

CloudView continuously discovers resources and ensures resources are compliant in relation to respective Benchmark & Best Practices policy provided out-of box. To view the complete list of policies and associated controls that Qualys provides, refer to Appendix: List of Policies and Controls.

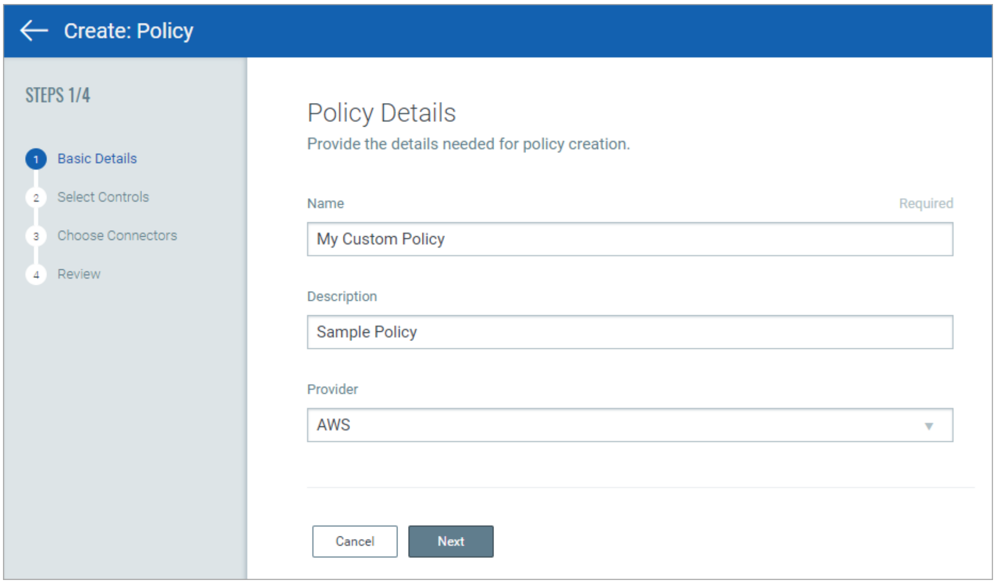
Set Up Your Own Policy (Custom Policy)

You can create your own custom policy and associate the required the controls to be evaluated for the custom policy.

(1) Navigate to Policy > Policy > New.



(2) Provide the basic details for the custom policy such as name, description and select the cloud provider. Click Next.



Policy Details

Provide the details needed for policy creation.

Name (Required): My Custom Policy

Description: Sample Policy

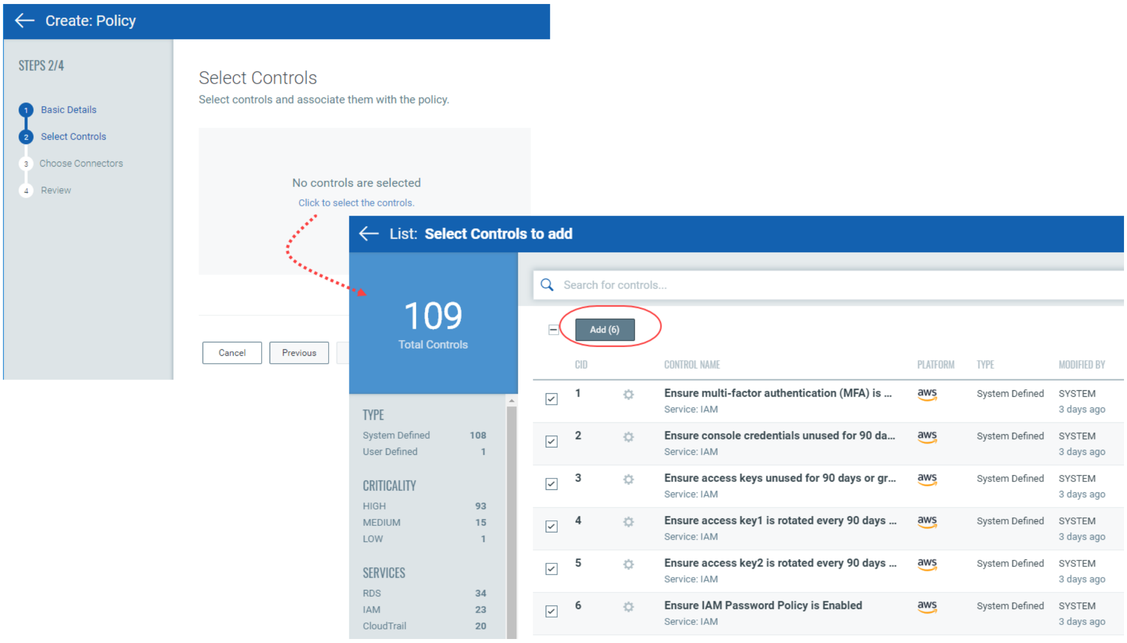
Provider: AWS

(3) Associating Controls:

- System Defined

-User defined

Select the controls to be associated with the policy and click Add. Click Next.



Create: Policy

STEPS 2/4

1 Basic Details
2 Select Controls
3 Choose Connectors
4 Review

Select Controls

Select controls and associate them with the policy.

No controls are selected

Click to select the controls.

Cancel | Previous

List: **Select Controls to add**

109 Total Controls

TYPE

System Defined	108
User Defined	1

CRITICALITY

HIGH	93
MEDIUM	15
LOW	1

SERVICES

RDS	34
IAM	23
CloudTrail	20

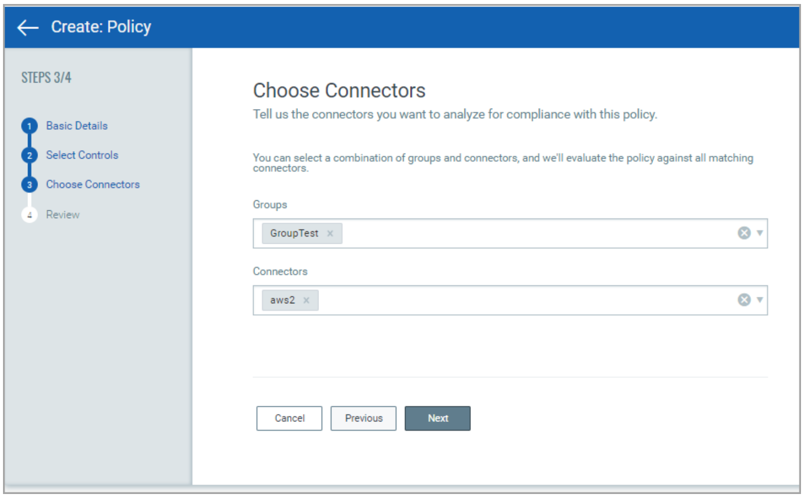
Search for controls...

Add (6)

	CID		CONTROL NAME	PLATFORM	TYPE	MODIFIED BY
☑	1		Ensure multi-factor authentication (MFA) is ... Service: IAM	aws	System Defined	SYSTEM 3 days ago
☑	2		Ensure console credentials unused for 90 da... Service: IAM	aws	System Defined	SYSTEM 3 days ago
☑	3		Ensure access keys unused for 90 days or gr... Service: IAM	aws	System Defined	SYSTEM 3 days ago
☑	4		Ensure access key1 is rotated every 90 days ... Service: IAM	aws	System Defined	SYSTEM 3 days ago
☑	5		Ensure access key2 is rotated every 90 days ... Service: IAM	aws	System Defined	SYSTEM 3 days ago
☑	6		Ensure IAM Password Policy is Enabled Service: IAM	aws	System Defined	SYSTEM 3 days ago

You can associate system-defined controls or create your own custom control using existing control to suit your need. For more information, refer to Customize Controls.

(4) Select the connector groups or connectors that should be analyzed for policy compliance. Click Next.



Create: Policy

STEPS 3/4

1 Basic Details
2 Select Controls
3 Choose Connectors
4 Review

Choose Connectors

Tell us the connectors you want to analyze for compliance with this policy.

You can select a combination of groups and connectors, and we'll evaluate the policy against all matching connectors.

Groups: GroupTest ×

Connectors: aws2 ×

Cancel | Previous | Next

That’s it. Your custom policy is ready to use.

Policy Search

Find all about your policies and get up to date information quickly using Qualys Advanced Search. Start typing in the Search field and we'll show you the properties you can search such as policy.name, provider, etc. Select the one you're interested in.

Search for policies based on the properties.

Now enter the value you want to match, and press Enter. That's it! Your matches will appear in the list. For detailed steps on how to form search queries, click here.

Associating Controls

You could build your policy by associating relevant controls to it.

Reports

You can generate reports to view the compliance posture of your cloud resources. Run reports to learn whether your resources are compliant with mandates and compliance policies.

The reports you could generate are:

Assessment Reports

You can generate a report to view the compliance evaluation of your resources for multiple policies in your cloud environment. You can use our Qualys Query Language (QQL) query driven report wizard to generate on-demand assessment report. When the report is successfully created, you can also download it in CSV or PDF format using our quick actions menu. For detailed information and steps on Assessment report, see Assessment Reports.

On-Screen Reports

Create a custom template for the reports by telling us the settings. The report templates are saved and available to you. Every time you want to view the report, just select Run Report from the quick actions menu. You can edit the report template to reconfigure or change the report settings. Depending on the criteria you define in the report template, you could generate two types of reports: Mandate Based Reporting and Policy Based Report.

Assessment Reports

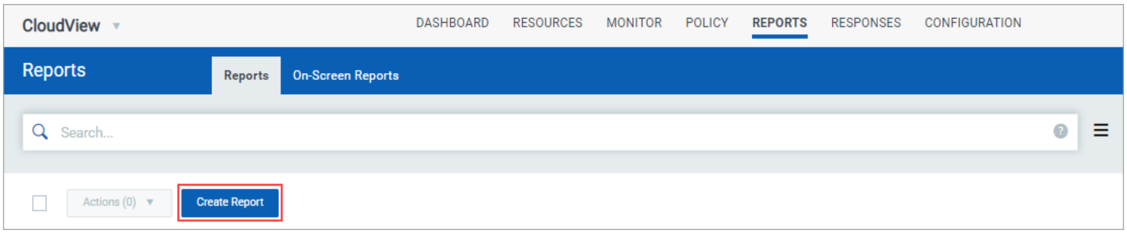
Use assessment reports to view the compliance of your resources for the defined policies in CloudView. You can use Qualys Query Language (QQL) to generate the on-demand assessment reports.

Create an assessment report by telling us the settings. The report settings are saved and available to you. Once you generate an assessment report, you can view the report summary, reconfigure the report settings, and download the report in CSV or PDF format.

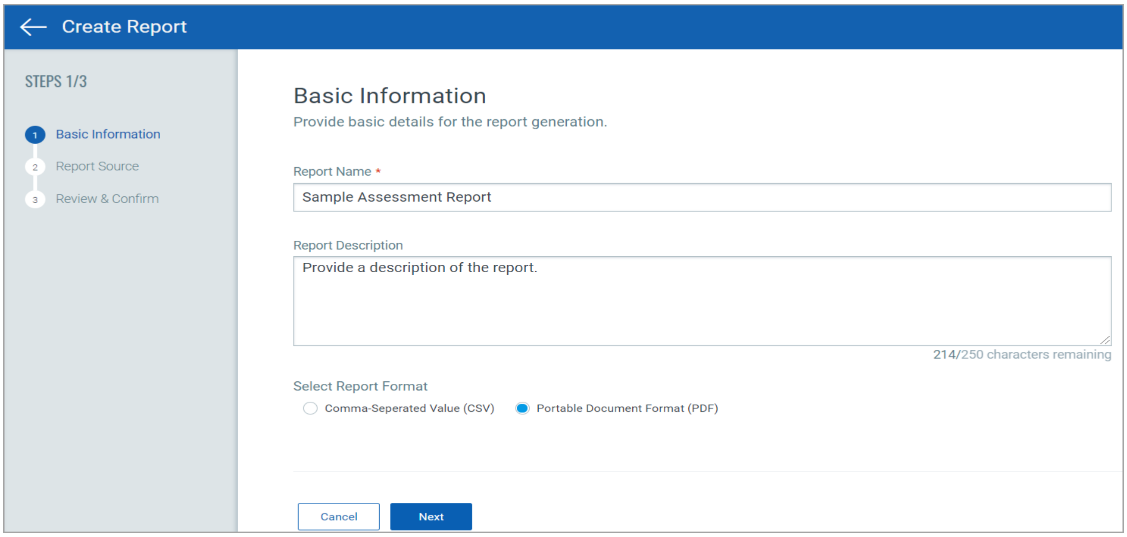
Tell me the Steps

It's easy to create a custom report template.

1) Just go to Reports > Reports tab and then click Create New Report.



2) Provide a title and description (optional) to the report template.



Basic Information

Provide basic details for the report generation.

Report Name *
Sample Assessment Report

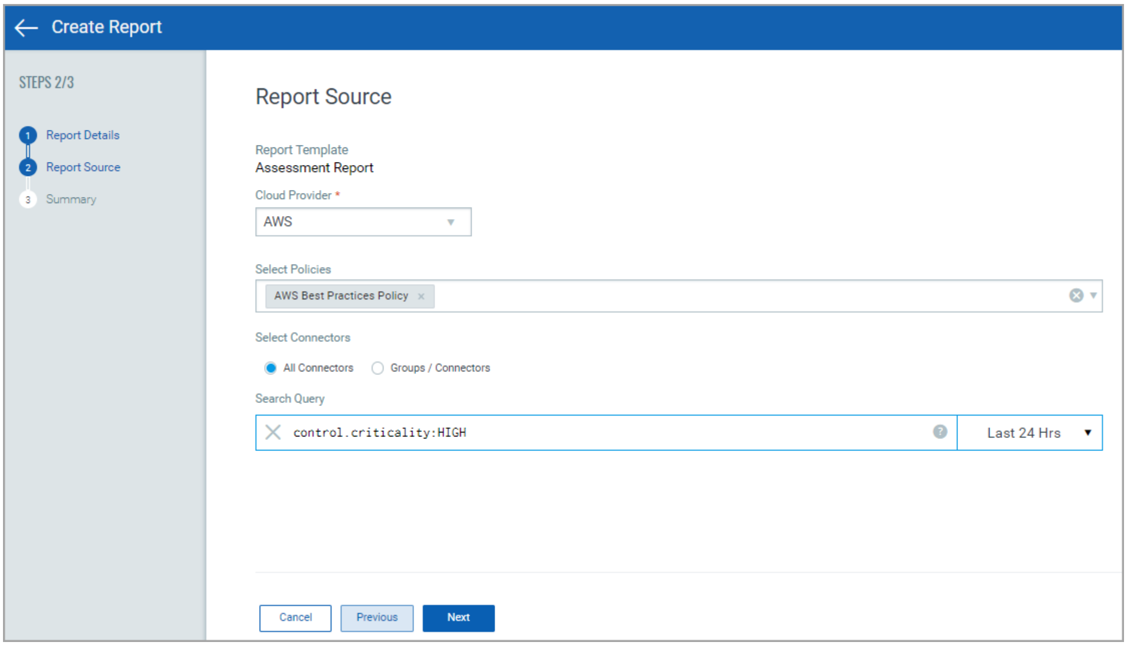
Report Description
Provide a description of the report.

214/250 characters remaining

Select Report Format
○ Comma-Seperated Value (CSV) ● Portable Document Format (PDF)

3) Choose the report format: CSV or PDF.

4) Select the cloud provider for which you want to generate the assessment report.



Report Source

Report Template
Assessment Report

Cloud Provider *
AWS

Select Policies
AWS Best Practices Policy ×

Select Connectors
● All Connectors ○ Groups / Connectors

Search Query
control.criticality:HIGH
Last 24 Hrs

5) Select the required compliance policy from the Select Policy drop-down for which you want to evaluate your cloud resources.

Note:

- For CSV report format, you can select multiple policies.

- For PDF report format, you can select only one policy.

6) Select the group, connector, or a combination of groups and connector you want to evaluate for compliance.

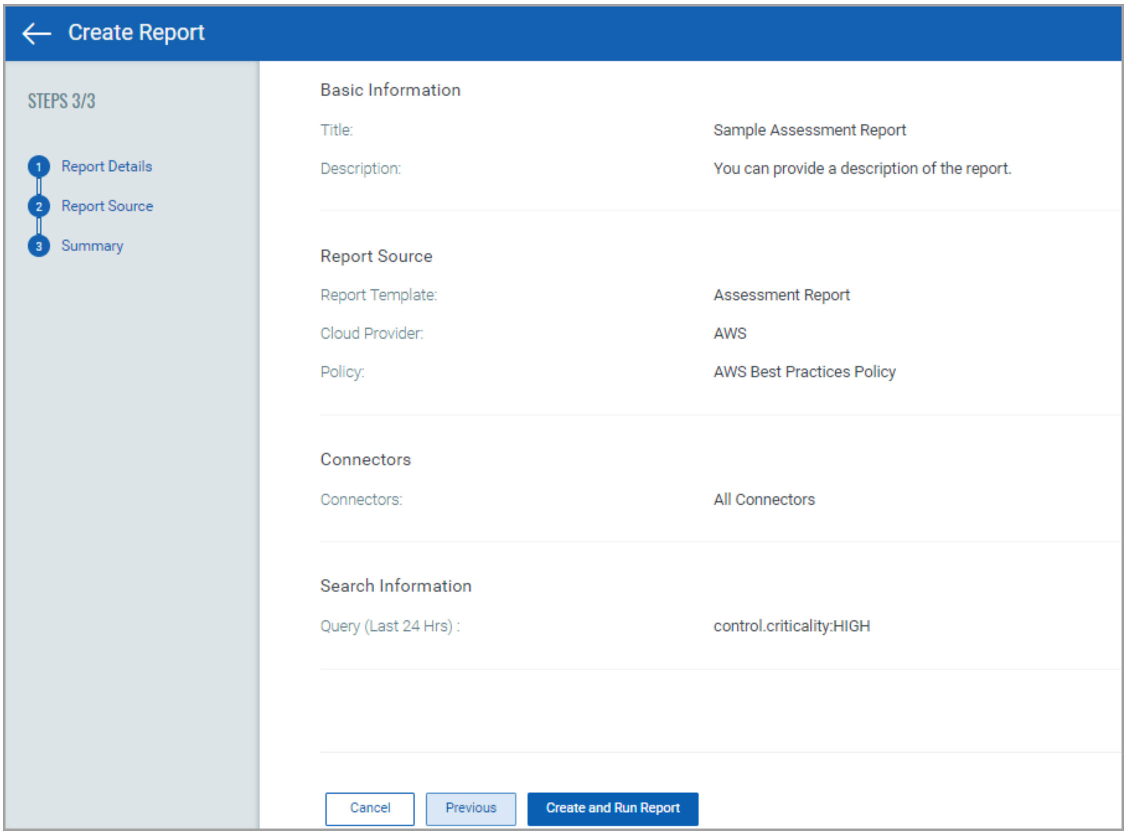
7) Use `evaluatedOn` search query token to specify the date criteria for report you want to generate.

8) Select Resource Summary check box to include details resource ID, connector, control ID, resource type, evaluation date, and resource result in the report (applicable only for PDF report format).

Note: Assessment reports containing up to 8k records with Resource Summary get successfully downloaded. Download of assessment report exceeding 8k records and Resource Summary is currently not supported for PDF reports.

9) Resource Evaluation Result: Select the evaluation results to be included in the reports for resources evaluated against the controls that meet criteria defined in Search Query. You could choose from Pass, PassE (pass with exceptions), and Fail options. You can choose multiple options.

10) Review the configured report settings in the Summary pane and then click Create and Run Report.



Basic Information

Title: Sample Assessment Report

Description: You can provide a description of the report.

Report Source

Report Template: Assessment Report

Cloud Provider: AWS

Policy: AWS Best Practices Policy

Connectors

Connectors: All Connectors

Search Information

Query (Last 24 Hrs) : control.criticality:HIGH

Re-run Assessment Report

To re-run a report, select the report from the Reports page and click Run Again from the quick actions menu.

The Create report wizard with pre-populated settings is displayed. You can retain the current report settings or edit as per your need.

Click Run Report to initiate the report generation.

The report is then listed on the Reports page. You can download the report once the status is Completed.

Download Assessment Report

To download a report, select the report from the Reports page and click Download from the quick actions menu.

The report is downloaded in format you specified during report creation.

View Assessment Report Settings

To view a report settings, select the report from the Reports page and click Info from the quick actions menu.

The Report Summary displays the report settings.

Delete Assessment Report

To delete a report, select the report from the Reports page and click Delete from the quick actions menu.

A confirmation dialog box is displayed. Click Yes to proceed with the deletion of the report.

The reports are automatically deleted after 7 days (from the date of creation).

On-Screen Reports

Create a custom template for the reports by telling us the settings. The report templates are saved and available to you. Every time you want to view the report, just select Run Report from the quick actions menu.

You can edit the report template to reconfigure or change the report settings. Depending on the criteria you define in the report template, you could generate two types of reports: Mandate Report and Policy Report.

Mandate Based Reporting

Mandates are regulatory requirements, best practice standards or compliance frameworks designed by Security/business driven certification communities and/or government bodies.

We support report generation of policies and mandates for all the cloud providers we support: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). To view the complete list of mandates that we support, see the List of Mandates section.

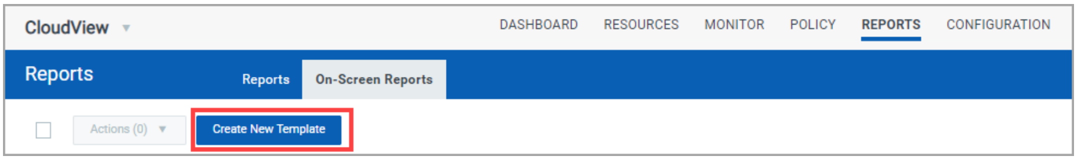
Launch the Mandate Based Report to view the compliance posture of the organization in terms of the underlying Security baseline against selected Mandates. This allows you to choose any one mandates you have to comply with and get a view of compliance posture in terms of their selected policies.

The reports are meant only for viewing and currently, we do not support saving, downloading or publishing the reports.

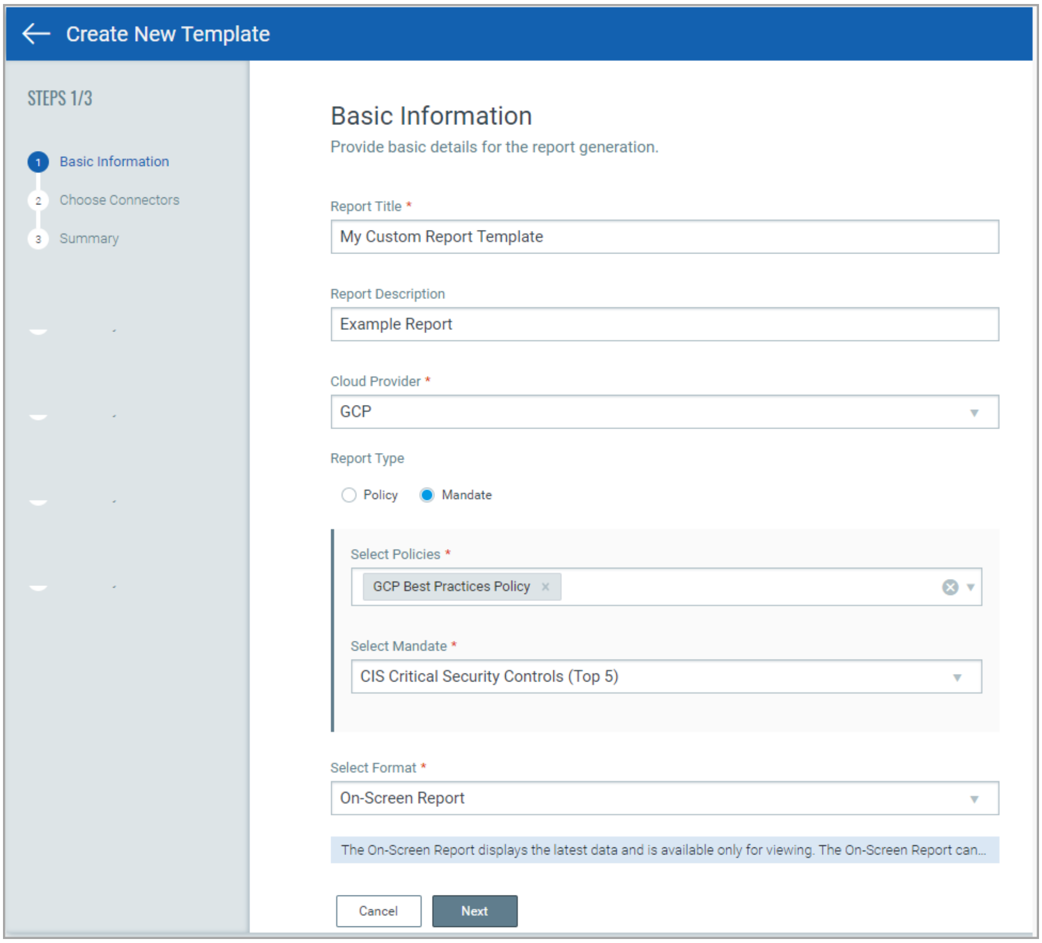
Tell me the Steps

It's easy to create a custom report template.

1) Just go to Reports > On-Screen Reports > Create New Template.



2) Provide a title and description (optional) to the report template.



Basic Information

Provide basic details for the report generation.

Report Title * My Custom Report Template

Report Description Example Report

Cloud Provider * GCP

Report Type ○ Policy ● Mandate

Select Policies * GCP Best Practices Policy

Select Mandate * CIS Critical Security Controls (Top 5)

Select Format * On-Screen Report

The On-Screen Report displays the latest data and is available only for viewing. The On-Screen Report can...

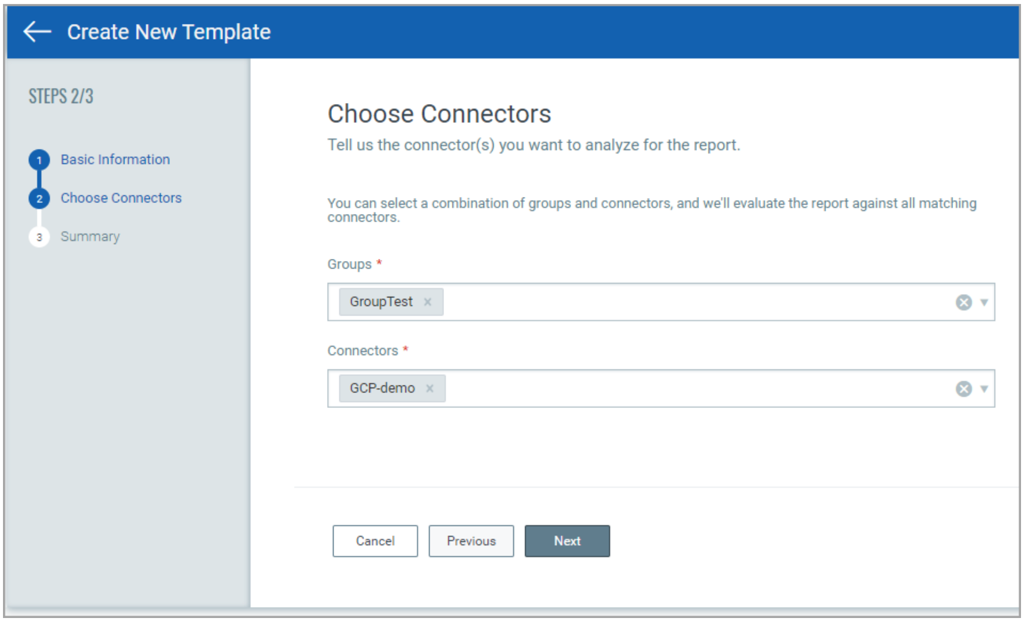
3) Select the cloud provider for which you want to generate the mandate report.

4) Select the Mandate in the report type and then click Next.

-Select the Policy from the drop-down. You can select multiple policies.

-Select the Mandate from the drop-down. You can select only one mandate.

5) Select the groups, connector, or a combination of groups and connector you want to evaluate for compliance.



Create New Template

STEPS 2/3

1 Basic Information
2 Choose Connectors
3 Summary

Choose Connectors

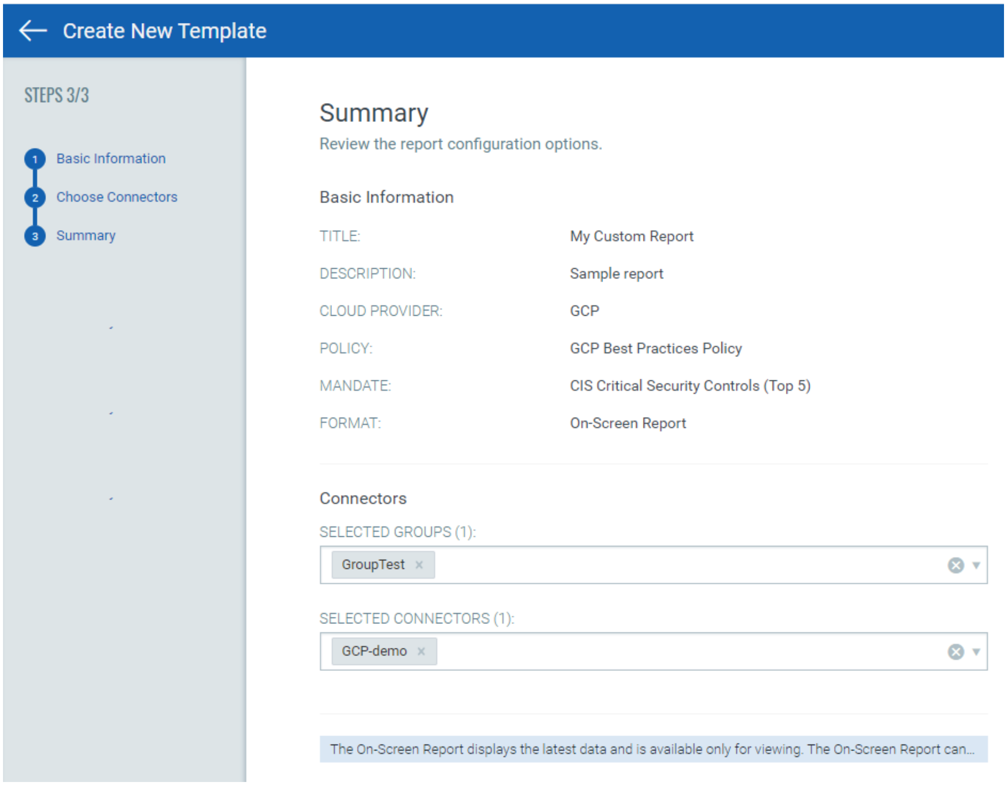
Tell us the connector(s) you want to analyze for the report.

You can select a combination of groups and connectors, and we'll evaluate the report against all matching connectors.

Groups *: GroupTest

Connectors *: GCP-demo

6) Review the configured report template settings in the Summary and then click Create Template and Run Report.



Summary

Review the report configuration options.

Basic Information

TITLE:	My Custom Report
DESCRIPTION:	Sample report
CLOUD PROVIDER:	GCP
POLICY:	GCP Best Practices Policy
MANDATE:	CIS Critical Security Controls (Top 5)
FORMAT:	On-Screen Report

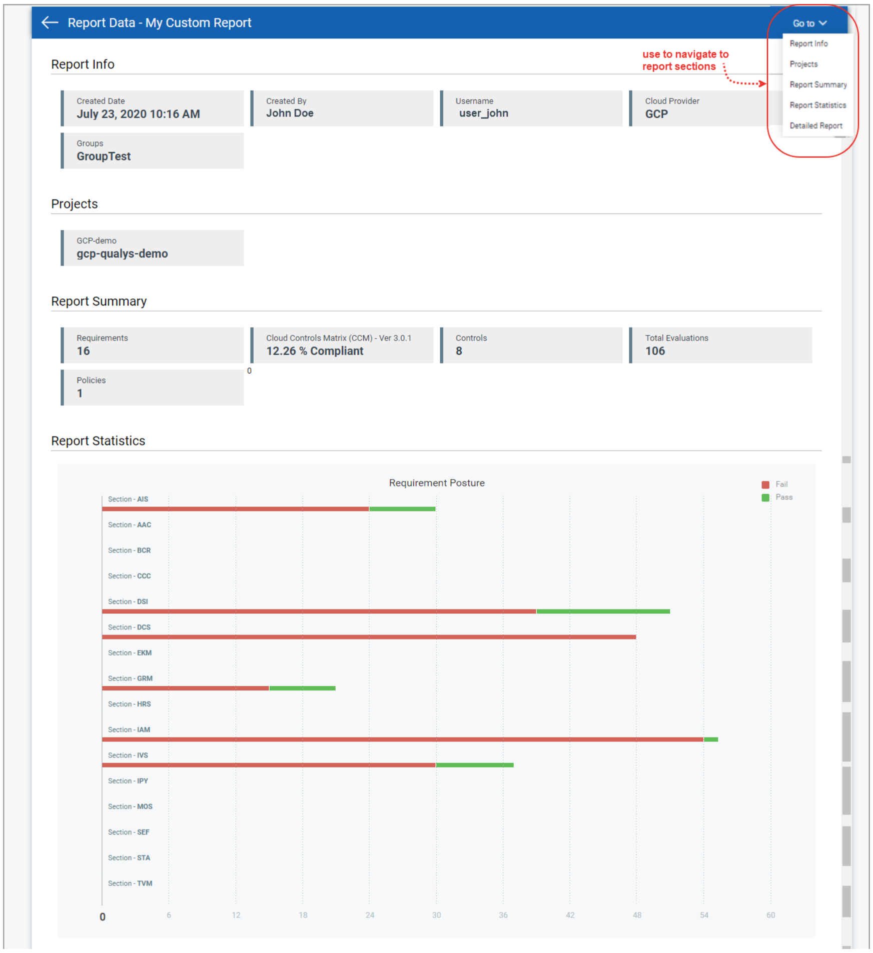
Connectors

SELECTED GROUPS (1):
GroupTest ×

SELECTED CONNECTORS (1):
GCP-demo ×

The On-Screen Report displays the latest data and is available only for viewing. The On-Screen Report can...

Sample Mandate Based Report



Report Data - My Custom Report

use to navigate to report sections

Report Info

Created Date
July 23, 2020 10:16 AM

Created By
John Doe

Username
user_john

Cloud Provider
GCP

Groups
GroupTest

Projects

GCP-demo
gcp-qualys-demo

Report Summary

Requirements
16

Cloud Controls Matrix (CCM) - Ver 3.0.1
12.26 % Compliant

Controls
8

Total Evaluations
106

Policies
1

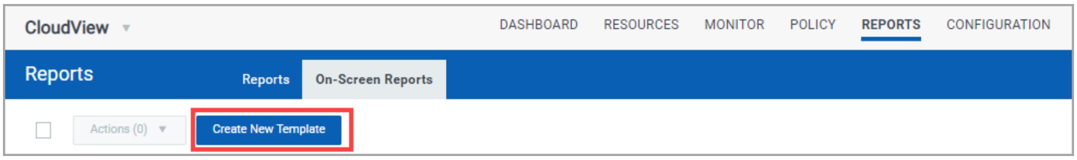
Report Statistics

Policy Based Report

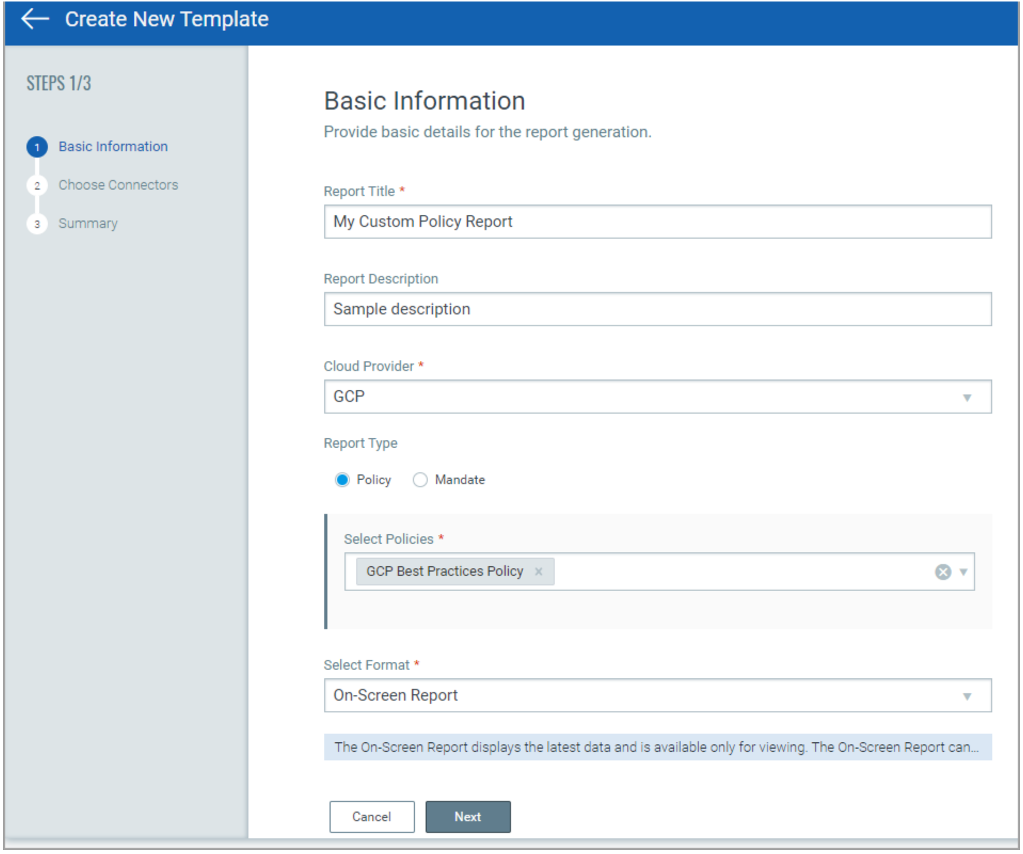
Policies are set of controls. We provide ability to generate policy specific compliance report. We support report generation of policies for all the cloud providers we support: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

It's easy to create a custom report template.

1) Just go to Reports > On-Screen Reports > Create New Template.



2) Provide a title and description (optional) to the report template.



Basic Information

Provide basic details for the report generation.

Report Title *: My Custom Policy Report

Report Description: Sample description

Cloud Provider *: GCP

Report Type: ● Policy ○ Mandate

Select Policies *: GCP Best Practices Policy

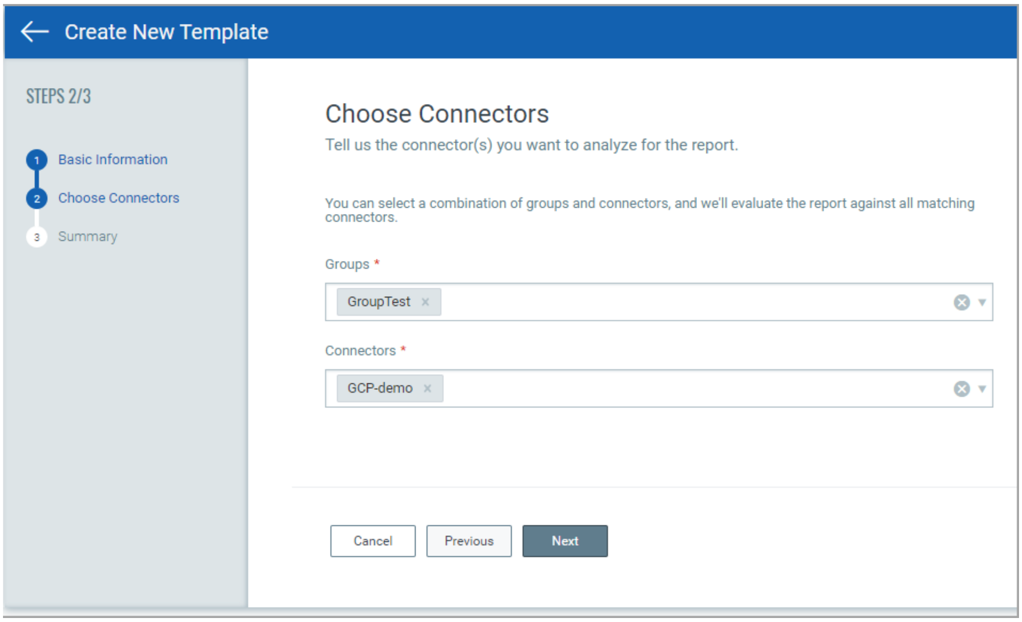
Select Format *: On-Screen Report

The On-Screen Report displays the latest data and is available only for viewing. The On-Screen Report can...

3) Select the cloud provider for which you want to generate the policy report.

4) Select the Policy in the report type, select the Policy from the drop-down and then click Next. You can select multiple policies.

4) Select the group, connector, or a combination of groups and connector you want to evaluate for compliance.



Create New Template

STEPS 2/3

1 Basic Information
2 Choose Connectors
3 Summary

Choose Connectors

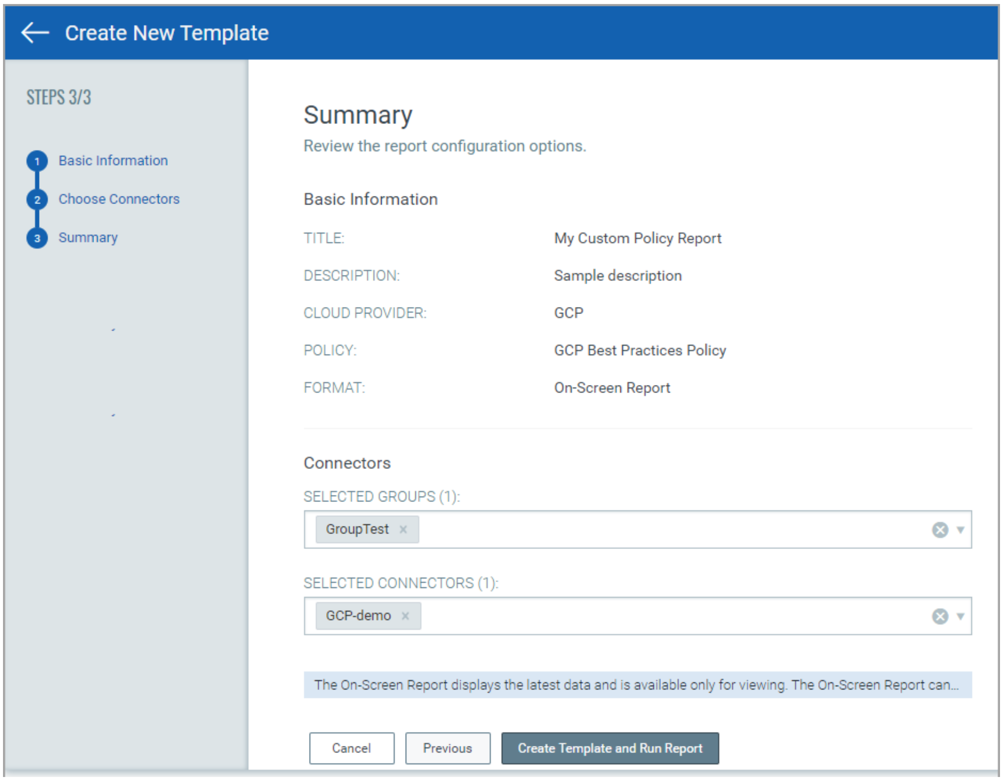
Tell us the connector(s) you want to analyze for the report.

You can select a combination of groups and connectors, and we'll evaluate the report against all matching connectors.

Groups *: GroupTest

Connectors *: GCP-demo

5) Review the configured report template settings in the Summary and then click Create Template and Run Report.



Create New Template

STEPS 3/3

1 Basic Information
2 Choose Connectors
3 Summary

Summary

Review the report configuration options.

Basic Information

TITLE: My Custom Policy Report
DESCRIPTION: Sample description
CLOUD PROVIDER: GCP
POLICY: GCP Best Practices Policy
FORMAT: On-Screen Report

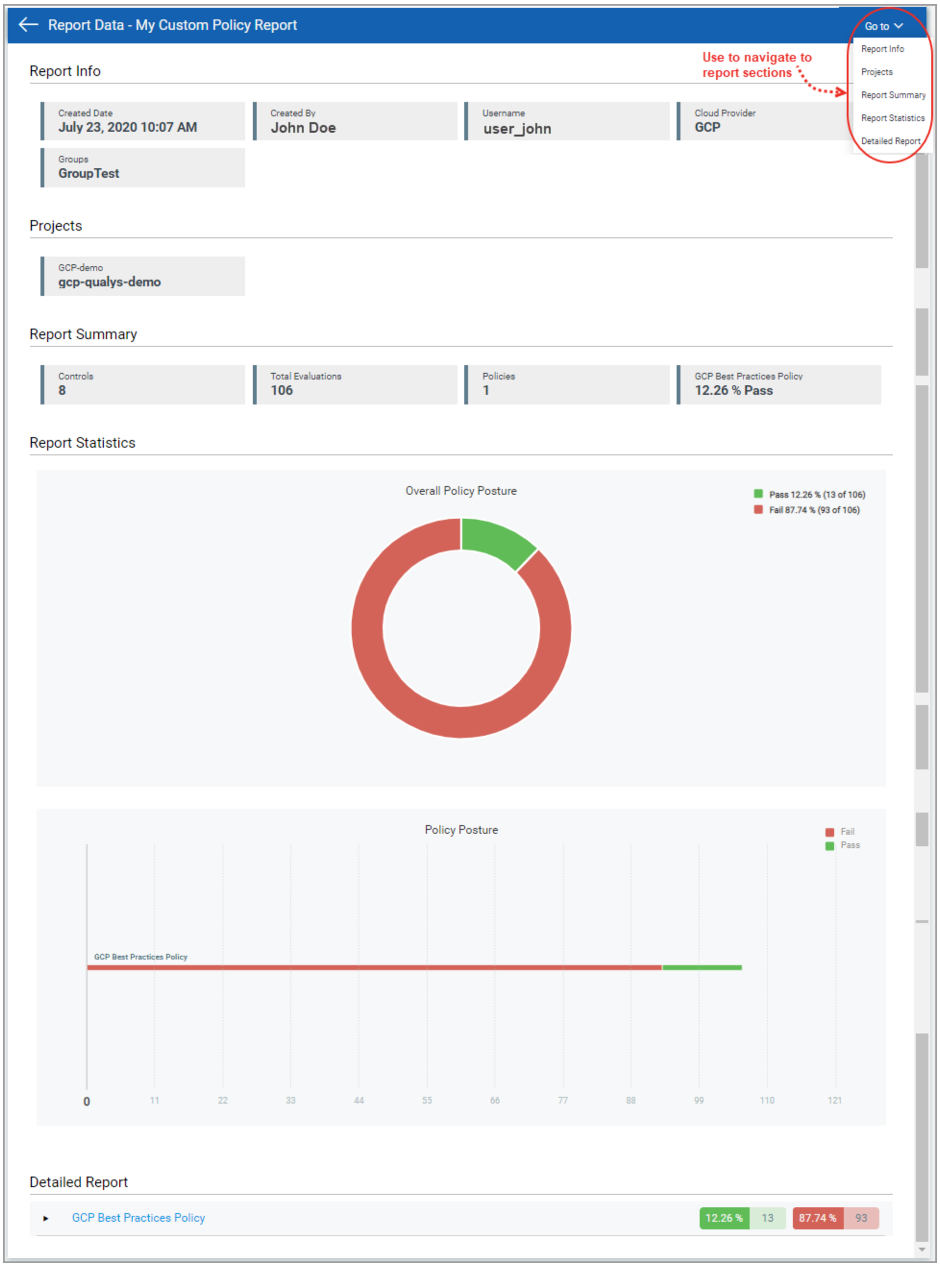
Connectors

SELECTED GROUPS (1): GroupTest

SELECTED CONNECTORS (1): GCP-demo

The On-Screen Report displays the latest data and is available only for viewing. The On-Screen Report can...

Sample Policy Based Report



Report Data - My Custom Policy Report

Report Info

Created Date: July 23, 2020 10:07 AM

Created By: John Doe

Username: user_john

Cloud Provider: GCP

Groups: GroupTest

Projects

GCP-demo: gcp-qualys-demo

Report Summary

Controls: 8

Total Evaluations: 106

Policies: 1

GCP Best Practices Policy: 12.26 % Pass

Report Statistics

Overall Policy Posture
🟩 Pass 12.26 % (13 of 106)
🟥 Fail 87.74 % (93 of 106)
Policy Posture
🟥 Fail
🟩 Pass
GCP Best Practices Policy
0
11
22
33
44
55
66
77
88
99
110
121

Detailed Report

▸	GCP Best Practices Policy	12.26 %	13	87.74 %	93

List of Mandates

We support the following mandates for report generation.

1.CIS Critical Security Controls (Top 5)

2.Payment Card Industry Data Security Standard (PCI-DSS)

3.CIS Critical Security Controls (Top 20)

4.NIST Cyber Security Framework (CSF)

5.Cloud Controls Matrix (CCM)

6.Criminal Justice Information Services (CJIS) Security Policy

7.IRS Publication 1075

8.Minimum Acceptable Risk Standards for Exchanges (MARS-E)

9.APRA Prudential Practice Guide (PPG): CPG 234 - Management of Security Risk in Information and Information Technology

10.Health Insurance Portability and Accountability (HIPAA) Security Rule

11.The Australian Signals Directorate - The Essential 8 Strategies (ASD 8)

12.NERC Critical Infrastructure Protection (CIP)

13.ANSSI 40 Essential Measures for a Healthy Network

14.SWIFT Customer Security Controls Framework - Customer Security Programme

15.Reserve Bank of India (RBI) - Baseline Cyber Security and Resilience Requirements (Annex 1)

16.NCSC Basic Cyber Security Controls (BCSC)

17.ISO/IEC 27001:2013

18.NESA UAE Information Assurance Standards (IAS)

19.NIST 800-171 (Special Publication)

20.Sarbanes-Oxley Act: IT Security

21.Federal Risk and Authorization Management Program (FedRAMP M) - Moderate Security Baseline

22.General Data Protection Regulation (GDPR)

23.IRDAI Guidelines On Information and Cyber Security for Insurers

24.Federal Risk and Authorization Management Program (FedRAMP H) - High Security Baseline

Responses

You can set up rules to alert you and keep you aware of resources that fail certain critical control evaluations and allow for fixing resource misconfigurations. Instead of having to actively monitor the system, these alerts ask for attention and intervention only when necessary, and make you aware of changes or significant findings as soon as the rules are met.

For example, you can set up alerts for:

- Resources failing for particular control

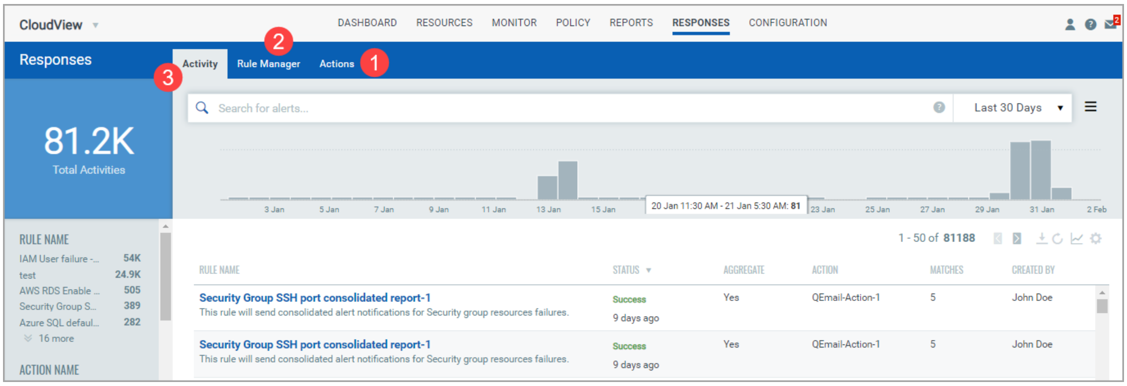
- Evaluation result of highly critical controls

- Evaluation result of controls of specific policy

- Resources failing in the latest connector run

Configure Rule-based Alerts

Just tell us what you consider to be a significant finding or event and the mechanism in which you want to be alerted.



RULE NAME	
IAM User failure -...	54K
test	24.9K
AWS RDS Enable ...	505
Security Group S...	389
Azure SQL defaul...	282

RULE NAME	STATUS	AGGREGATE	ACTION	MATCHES	CREATED BY
Security Group SSH port consolidated report-1 This rule will send consolidated alert notifications for Security group resources failures.	Success 9 days ago	Yes	QEmail-Action-1	5	John Doe
Security Group SSH port consolidated report-1 This rule will send consolidated alert notifications for Security group resources failures.	Success 9 days ago	Yes	QEmail-Action-1	5	John Doe

(1) Define actions that the rule must take in response to the alert. For detailed steps, see Create and Manage Actions.

(2) Set up your rules in the Rule Manager tab. For detailed steps, see Create and Manage Rules.

(3) Monitor all the alerts that were sent after the rules were triggered. For detailed steps, see, Manage Alerts.

That's it! You are all set to start being alerted about your cloud-resources.

Create and Manage Actions

Define the method in which you want to be alerted once any rule created by you is triggered. Alerts are initiated when events matching a condition is detected and the action you configure for the condition match is triggered.

Actions that you can choose are send the alert messages by Email, PagerDuty or Post to Slack.

Create a new Action

(1) Go to Responses > Actions > New Action.

(2) Provide required details in the respective sections to create a new action:

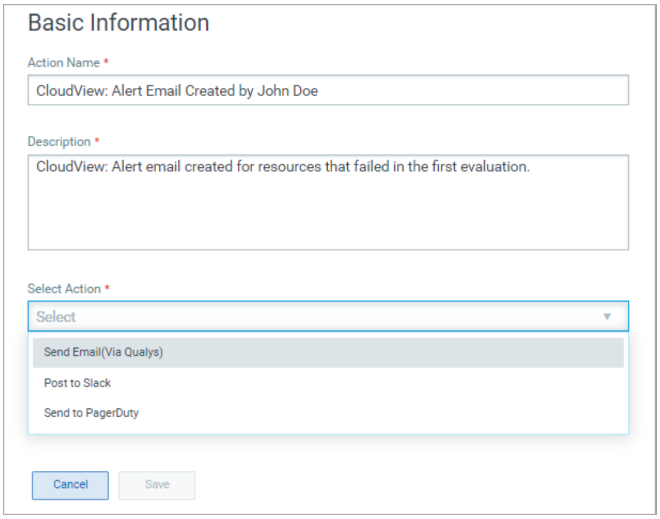
In the Basic Information section, provide a name and description for the action. Select an action to specify the mode of sending alert messages by either Email (Via Qualys)/Send Email (Your SMTP), Post to Slack or Send to Pager Duty.

(3) For the selected action, provide the required message settings.

- Send Email (Via Qualys)/Send Email (Your SMTP) to receive email alerts. Specify the recipients' email ID who will receive the alerts, subject of the alert message and the customized alert message.

- Send to PagerDuty to send alerts to your PagerDuty account. Provide the service key to connect to your PagerDuty account. In Default Message Settings, specify the subject and the customized alert message.

- Post to Slack to post alert messages to your Slack account. Provide the Webhook URI to connect to your slack account to post alert messages. In Default Message Settings, specify the subject of the alert message and the customized alert message.



Basic Information

Action Name *
CloudView: Alert Email Created by John Doe

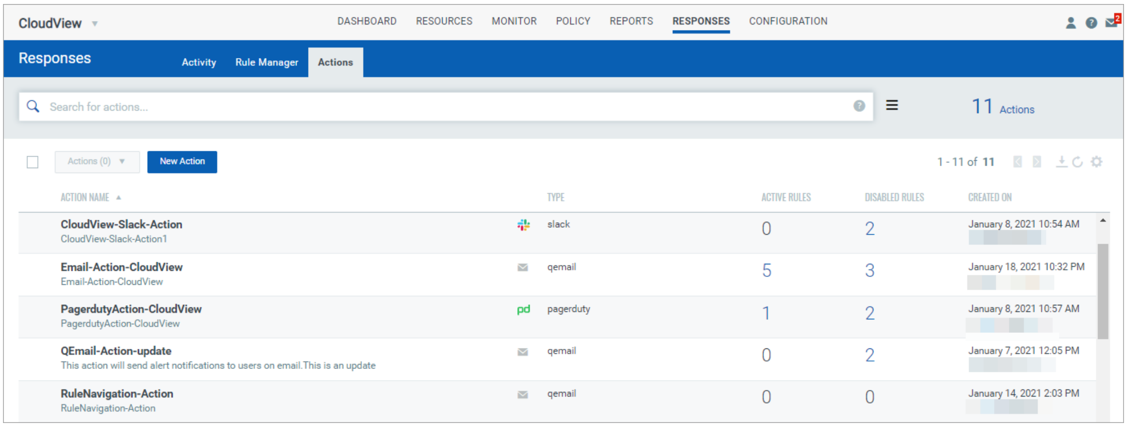
Description *
CloudView: Alert email created for resources that failed in the first evaluation.

Select Action *
Select

Manage Actions

View the newly created actions in the Actions tab with the details such as name of the action, type of the action, the number of rules for which this action is chosen are active or inactive and the user who created the rule.

You can use the Actions menu (for bulk selections) or Quick Actions menu to edit action, delete actions and save an existing action along with its configuration to create a new action with a new name. Use the search bar to search for actions using the search tokens.



ACTION NAME	TYPE	ACTIVE RULES	DISABLED RULES	CREATED ON
CloudView-Slack-Action CloudView-Slack-Action1	slack	0	2	January 8, 2021 10:54 AM [redacted]
Email-Action-CloudView Email-Action-CloudView	qemail	5	3	January 18, 2021 10:32 PM [redacted]
PagerdutyAction-CloudView PagerdutyAction-CloudView	pd pagerduty	1	2	January 8, 2021 10:57 AM [redacted]
QEmail-Action-update This action will send alert notifications to users on email.This is an update	qemail	0	2	January 7, 2021 12:05 PM [redacted]
RuleNavigation-Action RuleNavigation-Action	qemail	0	0	January 14, 2021 2:03 PM [redacted]

Create and Manage Rules

Rules can be used to define the criteria to trigger the alert notifications. You can use our pre-defined search tokens and form the queries for the criteria. You can then associate an action to be executed when the criteria defined in the rule is met.

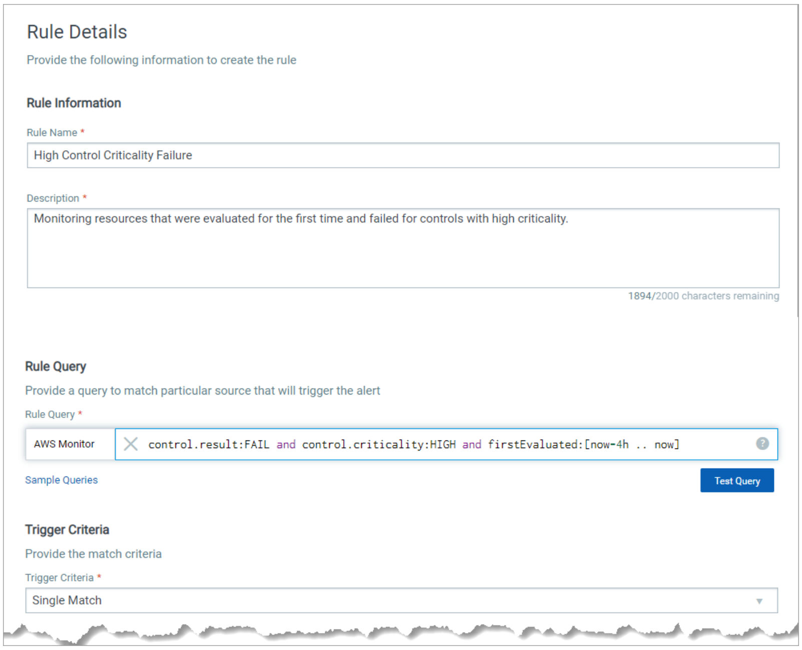
Create New Rule

(1) Go to Responses > Rule Manager > New Rule.

(2) Provide a name and description of the new rule in the Rule Name and Description.

(3) In the Rule Query section, specify a query for the rule. The system uses this query to search for events. Use the Test Query button to test your query. Click Sample Queries link to select from the predefined queries.

(4) In the Trigger Criteria section, choose from three trigger criteria that work in conjunction with the rule query. The trigger criteria are: Single Match, Time-Window Count Match and Time-Window Scheduled Match. For more information on trigger criteria, see Trigger Criteria.



Rule Details

Provide the following information to create the rule

Rule Information

Rule Name *
High Control Criticality Failure

Description *
Monitoring resources that were evaluated for the first time and failed for controls with high criticality.
1894/2000 characters remaining

Rule Query

Provide a query to match particular source that will trigger the alert

Rule Query *
AWS Monitor

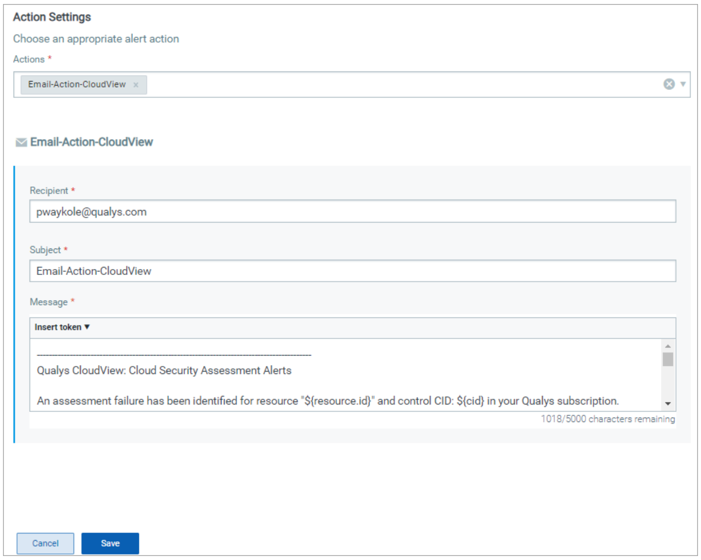
```
control.result:FAIL and control.criticality:HIGH and firstEvaluated:[now-4h .. now]
```

Trigger Criteria

Provide the match criteria

Trigger Criteria *
Single Match

(5) In the Action Settings section, choose the actions that you want the system to perform when an alert is triggered.



Action Settings

Choose an appropriate alert action

Actions *
Email-Action-CloudView

Email-Action-CloudView

Recipient *
pwaykole@qualys.com

Subject *
Email-Action-CloudView

Message *

Qualys CloudView: Cloud Security Assessment Alerts

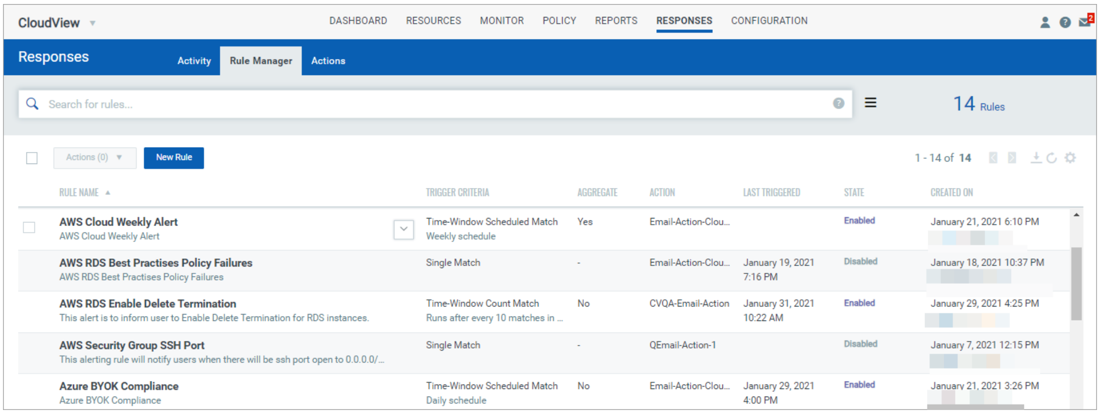
An assessment failure has been identified for resource "${resource.id}" and control CID: ${cid} in your Qualys subscription.

1018/5000 characters remaining

Manage Rules

The Rule Manager tab lists all the rules that you have created with rule name, trigger criteria selected for the rule, alert message aggregating enabled or disabled for the rule, action chosen for the rule, date and time when the rule is last triggered and state of the rule, whether the rule is enabled or disabled and created date and time of the rule.

You can use the Actions menu or Quick Actions menu to edit, enable, disable, delete rules and save an existing rule along with its configuration to create a new rule with a new name. Use the search bar to search for rules using the search tokens.



RULE NAME	TRIGGER CRITERIA	AGGREGATE	ACTION	LAST TRIGGERED	STATE	CREATED ON
AWS Cloud Weekly Alert AWS Cloud Weekly Alert	Time-Window Scheduled Match Weekly schedule	Yes	Email-Action-Clou...		Enabled	January 21, 2021 6:10 PM [redacted]
AWS RDS Best Practises Policy Failures AWS RDS Best Practises Policy Failures	Single Match	-	Email-Action-Clou...	January 19, 2021 7:16 PM	Disabled	January 18, 2021 10:37 PM [redacted]
AWS RDS Enable Delete Termination This alert is to inform user to Enable Delete Termination for RDS instances.	Time-Window Count Match Runs after every 10 matches in ...	No	CVQA-Email-Action	January 31, 2021 10:22 AM	Enabled	January 29, 2021 4:25 PM [redacted]
AWS Security Group SSH Port This alerting rule will notify users when there will be ssh port open to 0.0.0.0/...	Single Match	-	QEmail-Action-1		Disabled	January 7, 2021 12:15 PM [redacted]
Azure BYOK Compliance Azure BYOK Compliance	Time-Window Scheduled Match Daily schedule	No	Email-Action-Clou...	January 29, 2021 4:00 PM	Enabled	January 21, 2021 3:26 PM [redacted]

Manage Alerts

The Activity tab lists all the alerts. Here you will see for each alert, rule name, success or failure in sending the alert message, aggregate enabled (Yes) or disabled (No) for the rule, action chosen for the rule, matches found for the rule and the user who created the rule.

-Search for alerts using our search tokens.

-Select a period to view the rules triggered during that time frame.

-Click any bar to jump to the alerts triggered in a certain time-frame.

-Use these filters to group the alerts by rule name, action name, email recipients and status.

Sample Queries

Scenario 1: Rules with specific name and are successfully executed with PagerDuty action.

```
ruleName:"api test sub name rule" and status:SUCCESS and
action.type:PAGERDUTY
```

Scenario 2: Rules that were triggered during a certain date range

```
statusDate:[2021-01-02 ... 2021-06-02] and status:SUCCESS
```

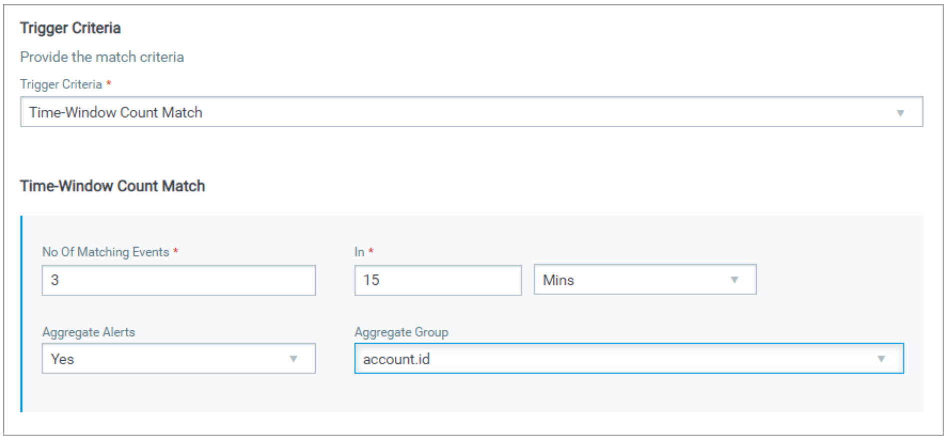
Scenario 3: Rules with specific action triggered to specific recipient.

```
action.type:EMAIL and action.emailRecipient:abc@example.com
```

Trigger Criteria

- Select Single Match if you want the system to generate an alert each time the system detects an event matching your search query

- Select Time-Window Count Match when you want to generate alerts based on the number of events returned by the search query in a fixed time interval. For example, an alert will be sent when three matching events are found within 15 minutes window..



Trigger Criteria

Provide the match criteria

Trigger Criteria *: Time-Window Count Match

Time-Window Count Match

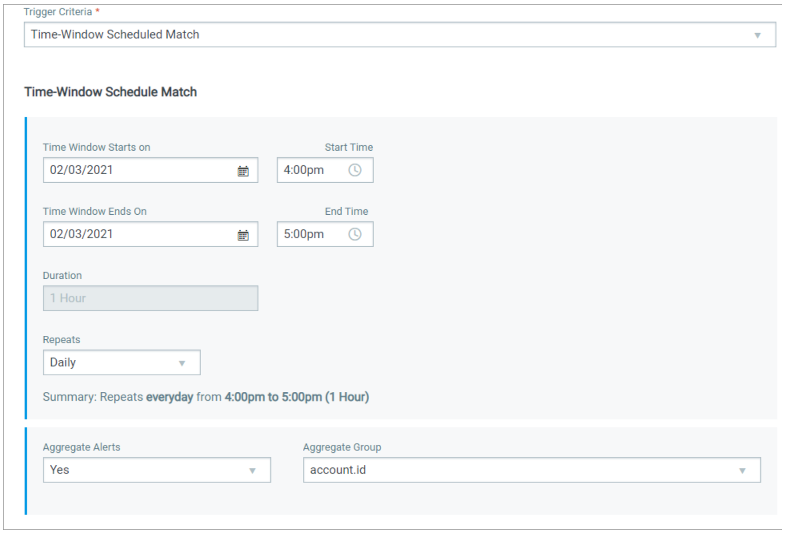
No Of Matching Events *: 3

In *: 15 Mins

Aggregate Alerts: Yes

Aggregate Group: account.id

- Select Time-Window Scheduled Match when you want to generate alerts for matching events that occurred during a scheduled time. The rule will be triggered only when an event matching your search criteria is found during the time specified in the schedule. Choose a date and time range for creating a schedule and specify how often you want to run the schedule for example, daily, weekly and monthly. For example, send daily alerts with all matches in a scheduled window between 4 pm and 5 pm.



Trigger Criteria *: Time-Window Scheduled Match

Time-Window Schedule Match

Time Window Starts on: 02/03/2021

Start Time: 4:00pm

Time Window Ends On: 02/03/2021

End Time: 5:00pm

Duration: 1 Hour

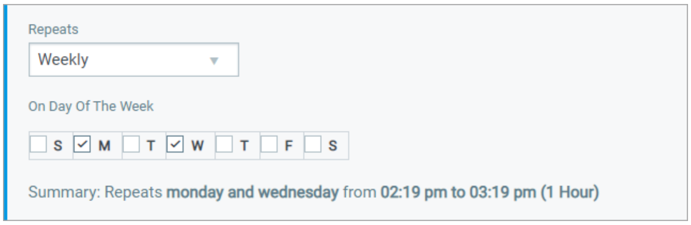
Repeats: Daily

Summary: Repeats **everyday** from **4:00pm to 5:00pm (1 Hour)**

Aggregate Alerts: Yes

Aggregate Group: account.id

For the Weekly option, select the days of the week on which schedule will run. For example, send weekly alerts with all matches generated between 2.19 pm and 3.19 pm on every Monday and Wednesday.



Repeats

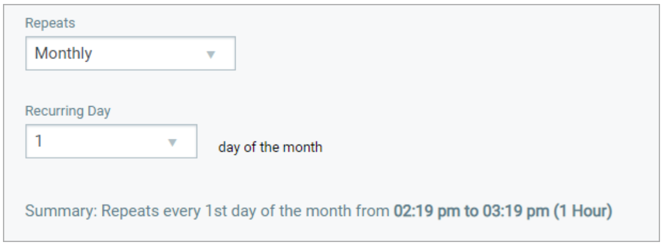
Weekly

On Day Of The Week

□ S ☑ M □ T ☑ W □ T □ F □ S

Summary: Repeats **monday and wednesday** from **02:19 pm to 03:19 pm (1 Hour)**

For the Monthly option, specify the day of the month on which the schedule will run. For example, send monthly alerts on the first day of every month.



Repeats

Monthly

Recurring Day

1 day of the month

Summary: Repeats every 1st day of the month from **02:19 pm to 03:19 pm (1 Hour)**

For Select Time-Window Count Match and Select Time-Window Scheduled Match, you have the option to aggregate the alerts by aggregate groups such as based on account Id, subscription Id, and so on.

Alerting Permissions

Assign permissions related to alerting to your user. Depending on the permissions assigned, the user can perform actions like creating, editing, or deleting rules and actions.

Using the Administration module, the Manager user for that subscription can assign these permissions to other users.

Only the user having the Alerting Access permission can view the Responses tab on the CloudView UI.

Remediating Cloud Resources

CloudView provides you information on resource misconfigurations. With the remediation feature, you can:

- Remediate resource misconfigurations

- Perform actions on cloud resources

You can remediate your AWS, Azure, and GCP resource misconfigurations.

By default the remediation feature is enabled only for Cloud Security Assessment (CSA) users.

Configuring Remediation

You can not only detect and evaluate cloud resources but also remediate resources in your cloud environment. You can quickly fix resource misconfigurations and remediate your cloud resources.

Pre-requisites

Ensure that you have the following modules available in your subscription:

- Cloud Security Assessment (CSA) Subscription

- Administration

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

A user with Manager role or sub-user with Manage Remediation permission can use the remediation feature. For more information on the configuring access for remediation, see Managing Remediation Permission.

Quick Steps

With the remediation enabled for the connectors, while resources are discovered and evaluated by CloudView, you are provided with one-click remediation option. We will walk you through the steps.

Step 1. Configure Connectors For Remediation

Configuration connectors for remediation involves two steps: enable remediation for the connector and then assign write access for the connector

The detailed steps for each cloud provider:
Configure Remediation for New Connectors: AWS

Configure Remediation: Microsoft Azure

Configure Remediation: GCP

Step 2. Remediating Cloud Resources

The Monitor tab lists the controls that are available for remediation and the count of failed evaluations that could be remediated.

Step 3. Actions for Cloud Resources (AWS)

The Resources tab provides you with actions that you can execute on instances to quickly fix unknown behavior of an instance or vulnerability on an instance.

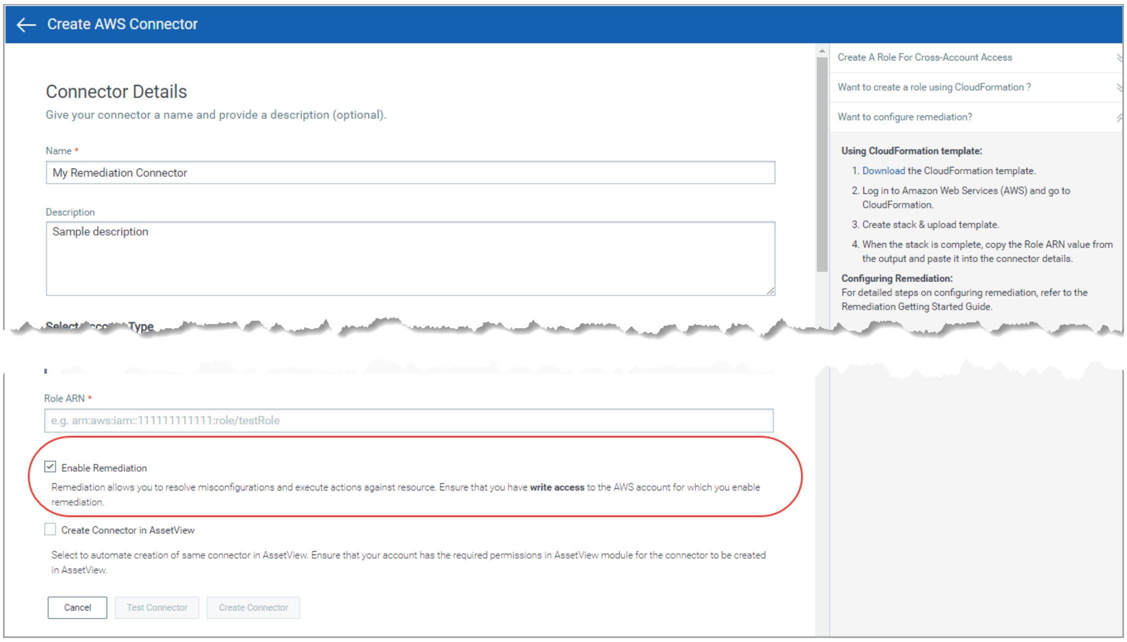
Configure Remediation for New Connectors: AWS

You can enable remediation when you create AWS connectors or edit existing connectors. It just takes a couple of minutes.

Enable Remediation for New Connectors

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

Provide a name and description (optional) for your connector. Configure the required settings for the AWS connector. For detailed information on connector creations steps, refer to Steps to Create AWS Connector.


Create AWS Connector
Create A Role For Cross-Account Access
Want to create a role using CloudFormation ?
Want to configure remediation?
Cancel
Test Connector
Create Connector

Connector Details

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

Name *
My Remediation Connector

Description
Sample description

Select Account Type

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

☑ Enable Remediation

Remediation allows you to resolve misconfigurations and execute actions against resource. Ensure that you have **write access** to the AWS account for which you enable remediation.

□ Create Connector in AssetView

Select to automate creation of same connector in AssetView. Ensure that your account has the required permissions in AssetView module for the connector to be created in AssetView.

Using CloudFormation template:

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.

Configuring Remediation:
For detailed steps on configuring remediation, refer to the Remediation Getting Started Guide.

Select **Enable Remediation** check box to enable remediation for the connector.

Ensure that the connector has write access to the AWS account for which you enable remediation. For more information on assigning write access, refer to Configuration on AWS Console section.

All the resources detected by this connector will be evaluated. You can then initiate remediation for the failed resources.

Then click Create Connector.

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

Configuration on AWS Console

You could either use cloud formation template or manually configure the roles and permissions needed for remediation.

Configuration Using CloudFormation Template:

1. Download the CloudFormation template from the Create AWS Connector window.

2. Log on to Amazon Web Services (AWS) and go to CloudFormation.

3. Create stack & upload the template.

When the stack creation is complete, copy the Role ARN value from the output and paste it into the connector details.

Manual Configuration

The manual configuration for remediation includes two parts: creating custom policy and adding the custom policy to the IAM role.

Creating Custom Policy

1. Go to IAM console at https://console.aws.amazon.com/iam/.

2. In the left navigation pane, choose Policies.

3. Click Create policy.

4. Click JSON tab.

5. Paste the following policy document into the JSON tab.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RemediationPermission",
            "Effect": "Allow",
            "Action": [
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:StopInstances",
                "ec2:ModifySnapshotAttribute",
                "ec2:ModifyImageAttribute",
                "s3:PutBucketPublicAccessBlock",
                "s3:PutAccountPublicAccessBlock",
                "s3:PutBucketVersioning",
                "rds:ModifyDBInstance",
                "rds:ModifyDBClusterSnapshotAttribute",
                "rds:ModifyCluster",
                "redshift:ModifyCluster"
            ],
            "Resource": "*"
        }
    ]
}
```

6. Click Review policy.

7. On the Review policy page, type a Name and a Description (optional).

8. Click Create policy.

Adding Policy to IAM Role

1.Go to IAM console at https://console.aws.amazon.com/iam/.

2. In the left navigation pane, choose Roles.

3. From the IAM Roles displayed, choose the IAM Role provided during the connector creation step in CloudView.

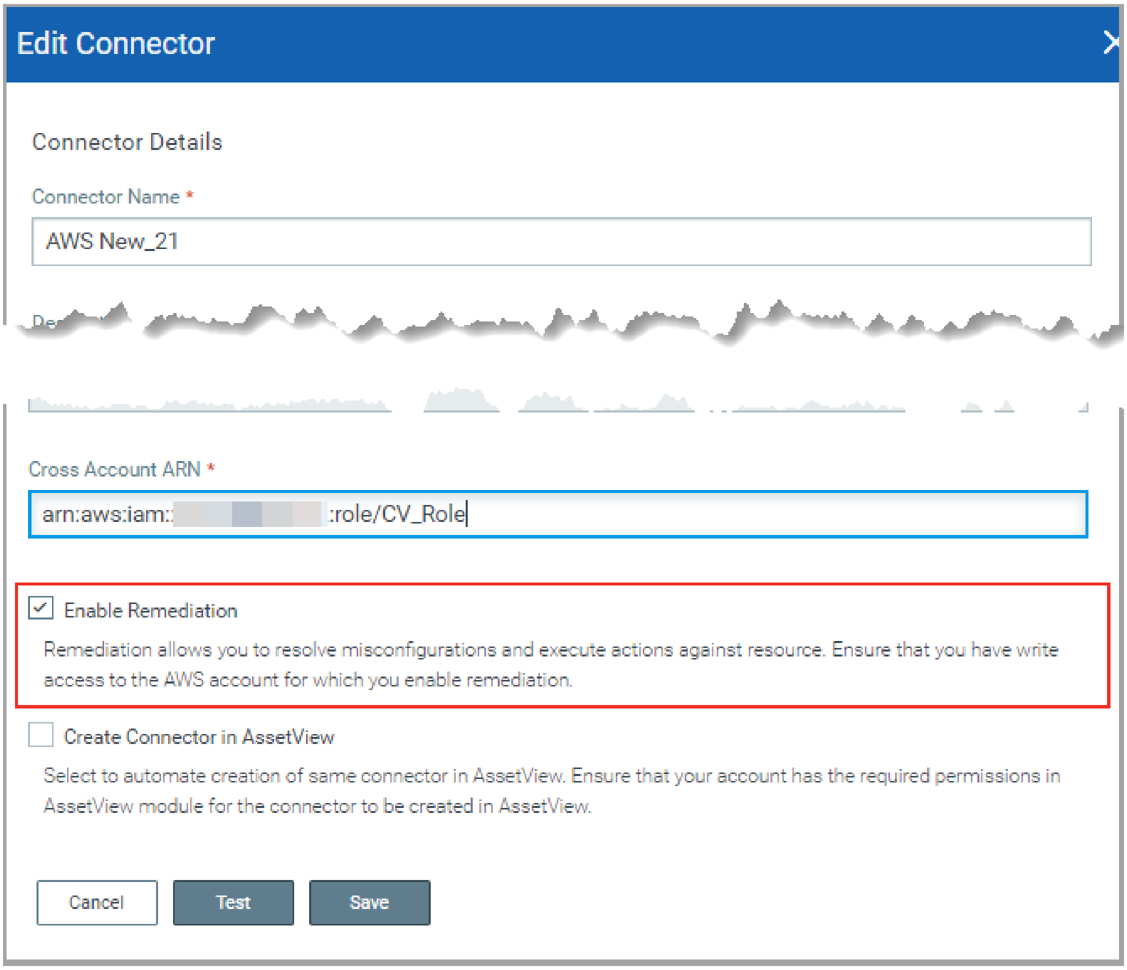
4. Go to Permissions tab and choose Attach policies.

5. Select the check box on the left for the Custom policy you created above.

6. Click Attach policy.

Enable Remediation for Existing AWS Connectors

Go to Configuration > Amazon Web Services and select the connector for which you would want to edit the details. From the quick actions menu, select View and go to Connector Information tab and click Edit.



Edit Connector

Connector Details

Connector Name *

AWS New_21

Cross Account ARN *

arn:aws:iam::[redacted]:role/CV_Role

☑ Enable Remediation

Remediation allows you to resolve misconfigurations and execute actions against resource. Ensure that you have write access to the AWS account for which you enable remediation.

□ Create Connector in AssetView

Select to automate creation of same connector in AssetView. Ensure that your account has the required permissions in AssetView module for the connector to be created in AssetView.

You can edit the required details. Select the Enable Remediation check box and click Save. Once you edit the connector settings, ensure that you also configure the roles and permissions needed for remediation on the AWS console. For more information on configuration of roles and permissions on AWS console, refer to Configuration on AWS Console section.

To fetch the updated resources, you need to select Run from the quick actions menu for the AWS connector.

Configure Remediation: Microsoft Azure

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

Pre-requisites

Before you create an Azure connector, ensure that you meet the following requirements:

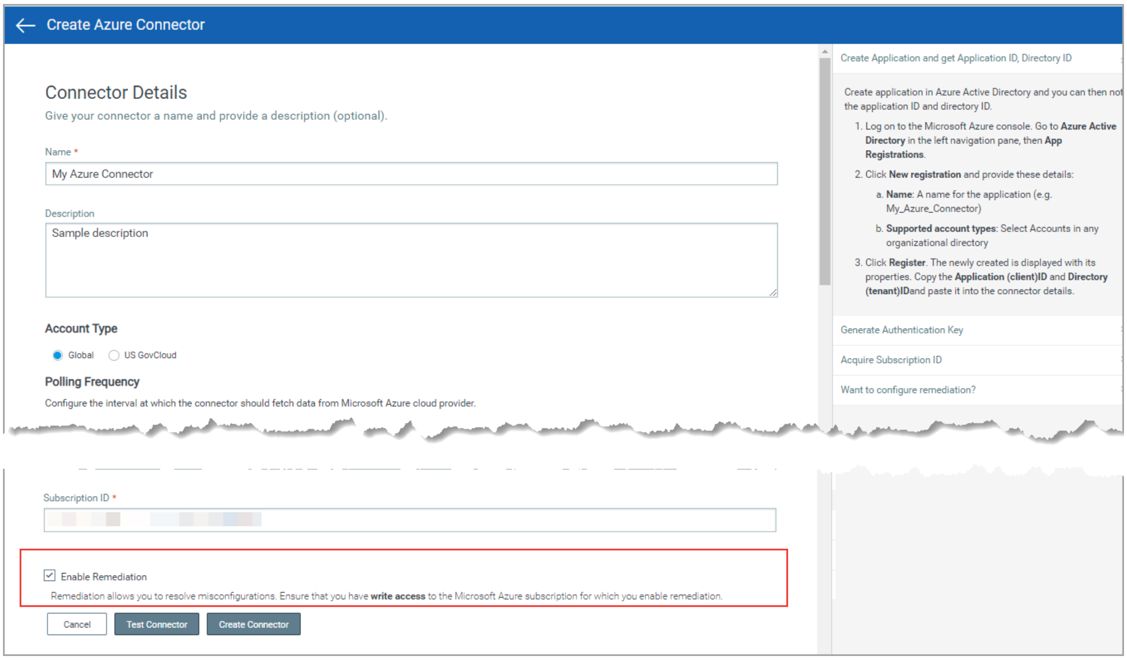
- Enable Remediation for Azure Connector to register an application with your Azure Active Directory.

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

Enable Remediation for New Azure Connectors

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

Provide a name and description (optional) for your connector. Configure the required settings for the Azure connector. For detailed information on connector creations steps, refer to Steps to Create Azure Connector.



Create Azure Connector

Connector Details

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

Name *

My Azure Connector

Description

Sample description

Account Type

● Global ○ US GovCloud

Polling Frequency

Configure the interval at which the connector should fetch data from Microsoft Azure cloud provider.

Subscription ID *

[redacted]

☑ Enable Remediation

Remediation allows you to resolve misconfigurations. Ensure that you have **write access** to the Microsoft Azure subscription for which you enable remediation.

Create Application and get Application ID, Directory ID

Create application in Azure Active Directory and you can then not
the application ID and directory 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 registration** and provide these details:
   a. **Name**: A name for the application (e.g. My_Azure_Connector)
   b. **Supported account types**: Select Accounts in any organizational directory
3. Click **Register**. The newly created is displayed with its properties. Copy the **Application (client)ID** and **Directory (tenant)ID**and paste it into the connector details.

Generate Authentication Key

Acquire Subscription ID

Want to configure remediation?

Select Enable Remediation check box to enable remediation for the connector.

Click Create Connector.

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

Configuration on Microsoft Azure Console

You can configure the roles and permissions needed for remediation on the Microsoft Azure portal.

Manual Configuration

The manual configuration for remediation includes two parts: creating custom role and adding the custom role to the application.

Creating Custom Role

1. Go to IAM console on the Microsoft Azure Portal.

2. In the search bar, search for Subscriptions and click Subscriptions, under the Services category.

3. In the Subscriptions page, choose your subscription.

4. Click Access control (IAM) navigation pane.

5. Scroll to Create a custom role card and click Add.

6. Provide a name for the Custom role, select Start from scratch option for Baseline permissions and click Next.

7. On the Permissions tab, click Add permissions and add the permissions listed below:

```
- Microsoft.Sql/servers/firewallRules/delete
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/write
- Microsoft.Network/networkSecurityGroups/write
- Microsoft.Web/sites/config/write
- Microsoft.Web/sites/write
```

8. Click Review + create.

9. Click Create.

Adding Custom Role to the application

1. Go to the Microsoft Azure Portal.

2. In the search bar, search for Subscriptions and click Subscriptions under the Services category.

3. On the Subscriptions page, choose your subscription.

4. Click Access control (IAM) navigation pane.

5. Find Add a role assignment card and click Add.

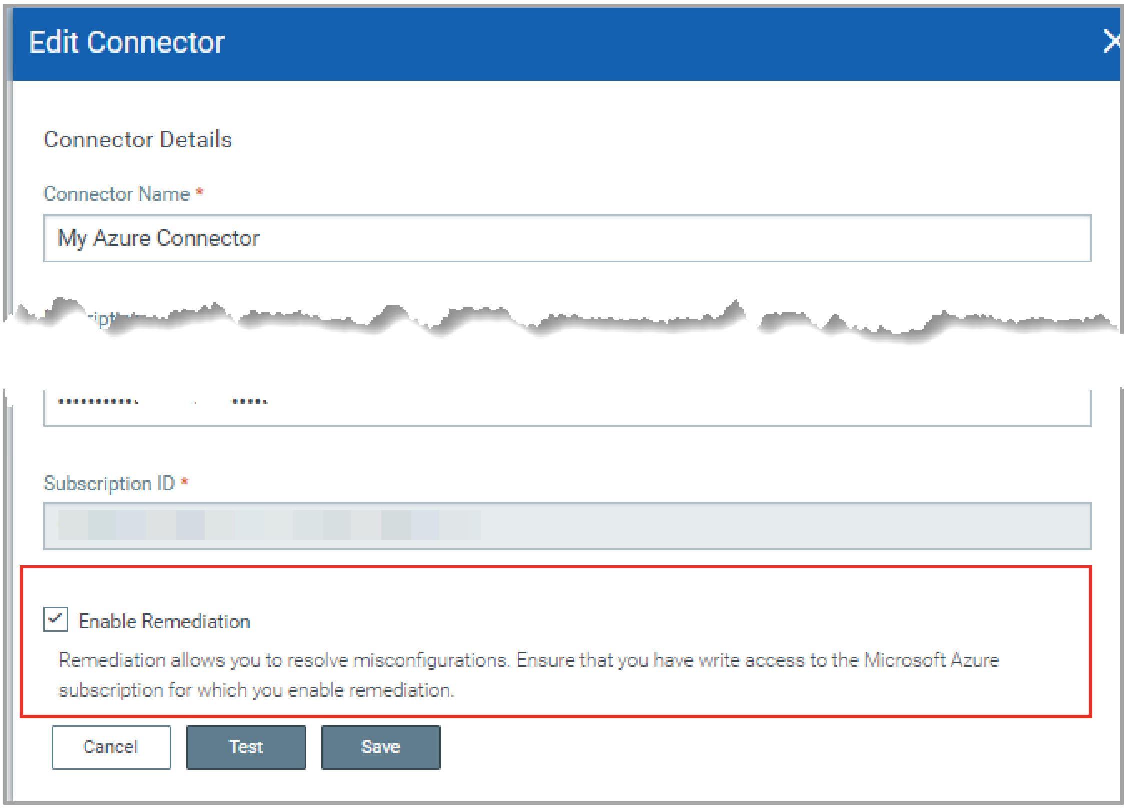
6. In the Role field, choose the custom role you created (If the custom role does not appear in the drop-down, refresh the page).

7. Select drop-down choose the App provide during the connector creation.

8. Click Save.

Enabling Remediation for Existing Azure Connectors

Go to Configuration > Microsoft Azure and select the connector for which you would want to edit the details. From the quick actions menu, select View and go to Connector Information tab and click Edit.



Edit Connector

Connector Details

Connector Name *

My Azure Connector

Subscription ID *

☑ Enable Remediation

Remediation allows you to resolve misconfigurations. Ensure that you have write access to the Microsoft Azure subscription for which you enable remediation.

You can edit the required details. Select the Enable Remediation check box and click Save. Once you edit the connector settings, ensure that you also configure the roles and permissions needed for remediation on the Azure console.

For more information on configuration of roles and permissions on Microsoft Azure console, refer to Configuration on Microsoft Azure Console.

To fetch the updated resources, you need to select Run from the quick actions menu for the Azure connector.

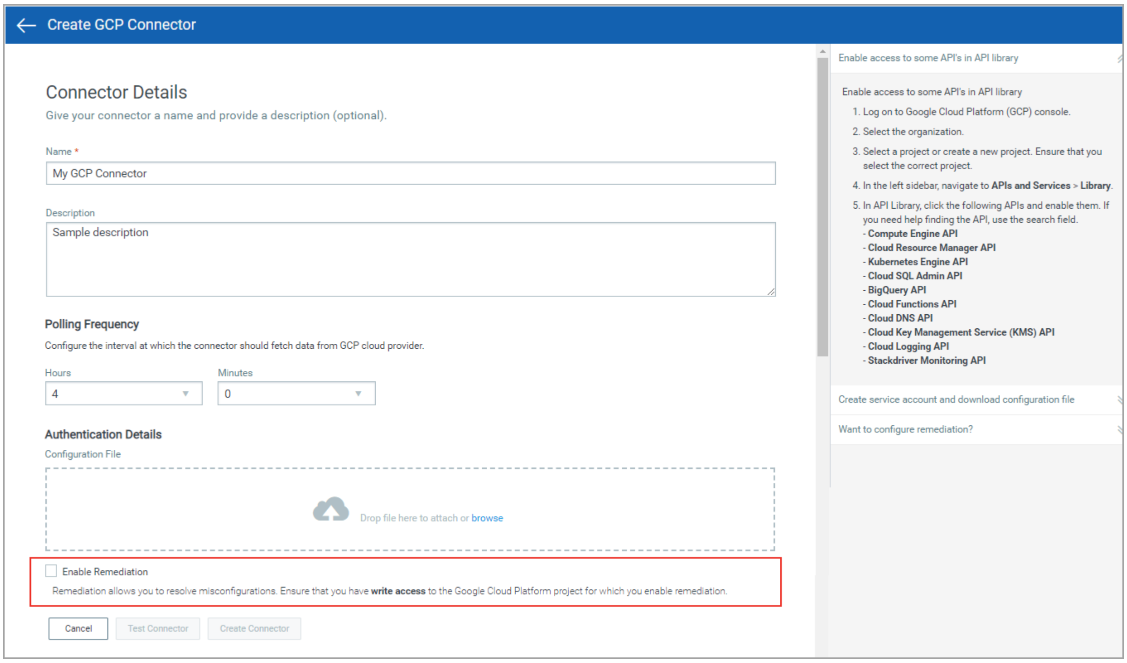
Configure Remediation: GCP

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

Enable Remediation for New GCP Connectors

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

Provide a name and description (optional) for your connector. Configure the required settings for the GCP connector. For detailed information on connector creations steps, refer to Steps to Create GCP Connector.



Create GCP Connector

Connector Details

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

Name *

My GCP Connector

Description

Sample description

Polling Frequency

Configure the interval at which the connector should fetch data from GCP cloud provider.

Hours: 4

Minutes: 0

Authentication Details

Configuration File

Drop file here to attach or browse

□ Enable Remediation

Remediation allows you to resolve misconfigurations. Ensure that you have **write access** to the Google Cloud Platform project for which you enable remediation.

Enable access to some API's in API library

Enable access to some API's in API library

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** > **Library**.
5. In API Library, click the following APIs and enable them. If you need help finding the API, use the search field.
   - **Compute Engine API**
   - **Cloud Resource Manager API**
   - **Kubernetes Engine API**
   - **Cloud SQL Admin API**
   - **BigQuery API**
   - **Cloud Functions API**
   - **Cloud DNS API**
   - **Cloud Key Management Service (KMS) API**
   - **Cloud Logging API**
   - **Stackdriver Monitoring API**

Create service account and download configuration file

Want to configure remediation?

Select Enable Remediation check box to enable remediation for the connector. All the resources detected by this connector will be evaluated. You can then initiate remediation for the failed resources.

Then click Create Connector.

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

Configuration on GCP Console

You could manually configure the roles and permissions needed for remediation on the Google Cloud Platform portal. The configuration for remediation includes two parts:

Creating Custom Role

1. Go to IAM console on the Google Cloud Platform Portal.

2. From the drop-down list at the top, select the project for which you want to create a role.

3. Click CREATE ROLE and provide the required details.

4. Click Add Permissions.

5. In the Add Permissions window, add the following permissions:

```
- compute.firewalls.update
```

```
    - compute.instances.setMetadata
    - storage.buckets.setIamPolicy
    - cloudfunctions.functions.setIamPolicy
    - bigquery.datasets.update
    - cloudsql.instances.update
    - cloudkms.cryptoKeys.setIamPolicy
```

6. Click CREATE.

The custom role is created. You need to add the custom role to the IAM member.

Adding Custom Role to the IAM Member

1.Go to IAM-Admin page on the Google Cloud Platform Portal - IAM Admin.

2. In the IAM members list, choose the member used for creating the connector.

3. Click the edit icon on the right side of the Selected IAM member row.

4. In the Edit permissions window, click ADD ANOTHER ROLE and then choose the Custom role created in the above step.

5. Click Save.

The custom role is added to the IAM member.

Add Compute Engine default service account access to CloudView service account

1. Go to Service accounts page by visiting Google Cloud Platform Portal - Service Accounts.

2. From the service accounts list select Compute Engine default service accounts, which is of pattern PROJECT_NUMBER-compute@developer.gserviceaccount.com and check the box on the left.

3. On the right pane, click ADD MEMBER.

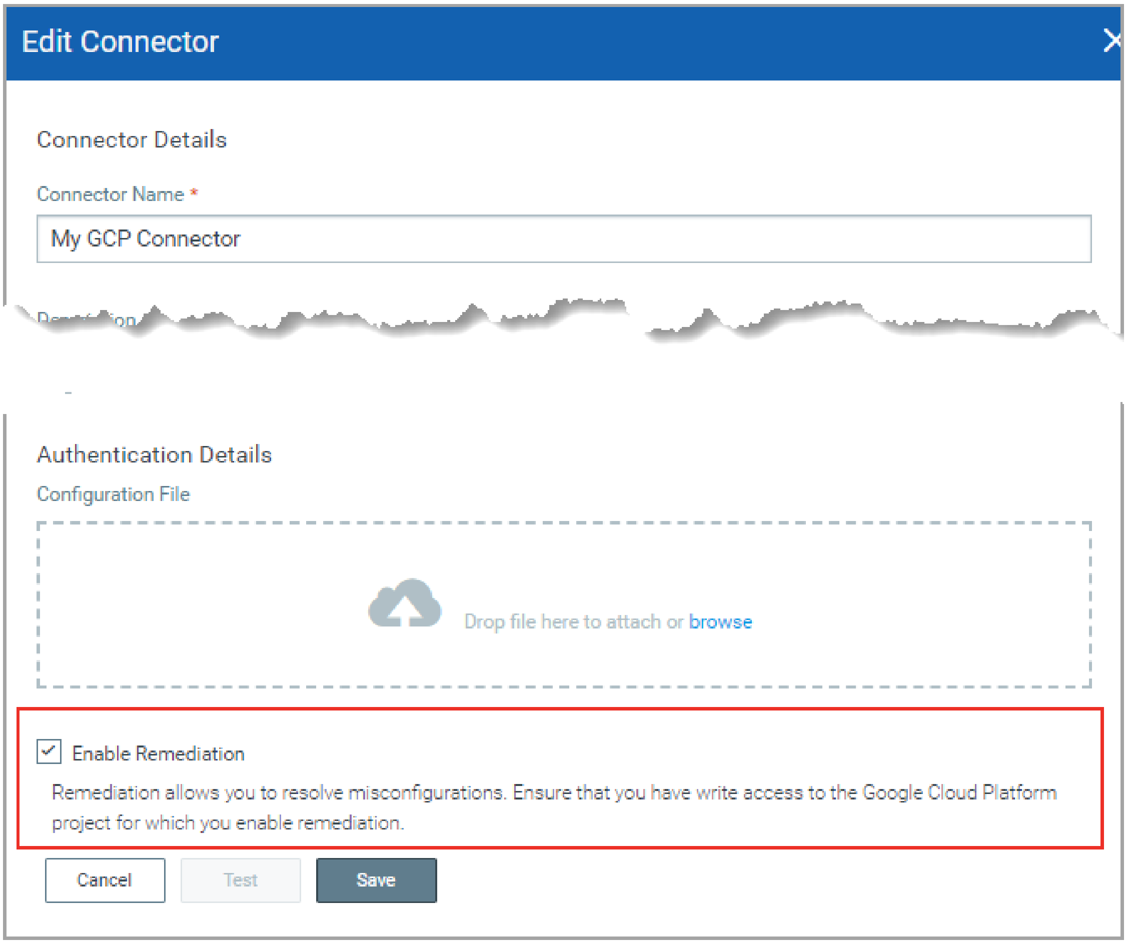
4. In the New members field, choose the service account provided during connector creation.

5. In Select a role field, choose Service Account User role.

6. Click SAVE.

Enabling Remediation for Existing GCP Connectors

Go to Configuration > Google Cloud Platform and select the connector for which you would want to edit the details. From the quick actions menu, select View and go to Connector Information tab and click Edit.



Edit Connector

Connector Details

Connector Name *

My GCP Connector

Authentication Details

Configuration File

Drop file here to attach or browse

☑ Enable Remediation

Remediation allows you to resolve misconfigurations. Ensure that you have write access to the Google Cloud Platform project for which you enable remediation.

You can edit the required details. Select the Enable Remediation check box and click Save. Remediation is enabled for the connector. Once you edit the connector settings, ensure that you also configure the roles and permissions needed for remediation on the GCP console.

For more information on configuration of roles and permissions on GCP console, refer to Configuration on GCP Console.

To fetch the updated resources, you need to select Run from the quick actions menu for the GCP connector.

Viewing Remediation Activity

You can view the all the remediation activities that are triggered in your Qualys account for all the 3 cloud providers.

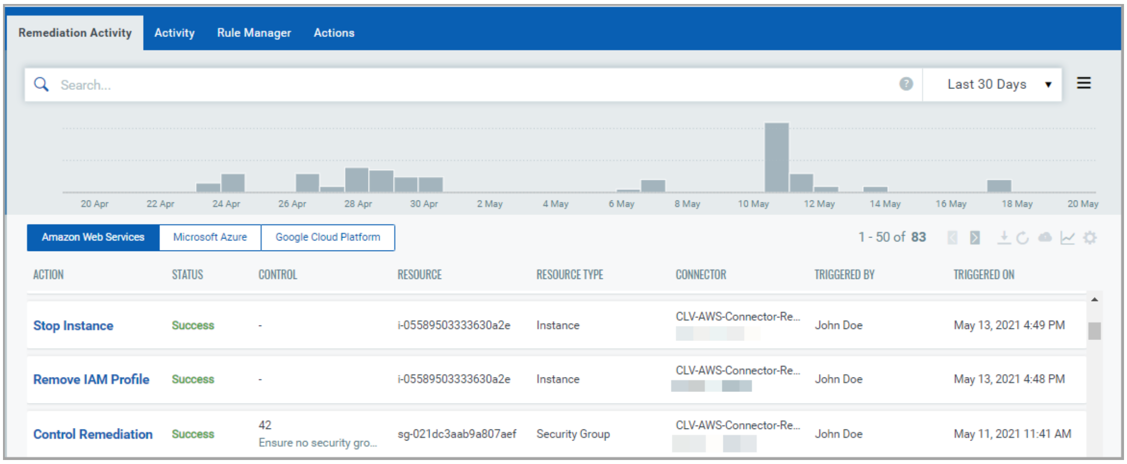
Go to Responses > Remediation Activity. Activities for every cloud are listed under the respective sub tabs.

You could use filters listed in the left pane or form search queries using the search tokens supported by Qualys Query Language (QQL) to filter the activities.

By default, the remediation activity logs are retained for 30 days. The logs older than 30 days are automatically deleted.

Remediation Activity: AWS

All the activities that are triggered for AWS resources are listed under Responses > Remediation Activity> AWS sub-tab. The Action column indicates the type of remediation activity initiated for a resource.



ACTION	STATUS	CONTROL	RESOURCE	RESOURCE TYPE	CONNECTOR	TRIGGERED BY	TRIGGERED ON
Stop Instance	Success	-	i-05589503333630a2e	Instance	CLV-AWS-Connector-Re... [redacted]	John Doe	May 13, 2021 4:49 PM
Remove IAM Profile	Success	-	i-05589503333630a2e	Instance	CLV-AWS-Connector-Re... [redacted]	John Doe	May 13, 2021 4:48 PM
Control Remediation	Success	42 Ensure no security gro...	sg-021dc3aab9a807aef	Security Group	CLV-AWS-Connector-Re... [redacted]	John Doe	May 11, 2021 11:41 AM

Actions for AWS resources:

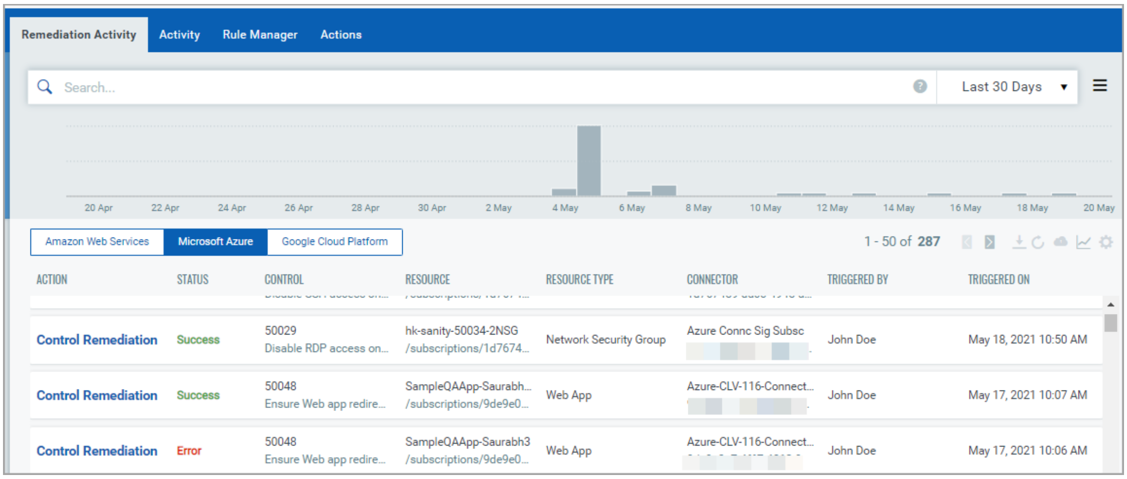
- Stop Instance: indicates stop instance action was initiated for the AWS resource.

- Remove IAM Profile: indicates remove IAM profile action was initiated for the AWS resource.

- Control Remediation: indicates Remediate Now button was used to trigger remediation of the AWS resource for the specified CID.

Remediation Activity: Microsoft Azure

All the activities that are triggered for Azure resources are listed under Responses > Remediation Activity> Microsoft Azure sub-tab. The Action column indicates the type of remediation activity initiated for a resource.



1 - 50 of 287

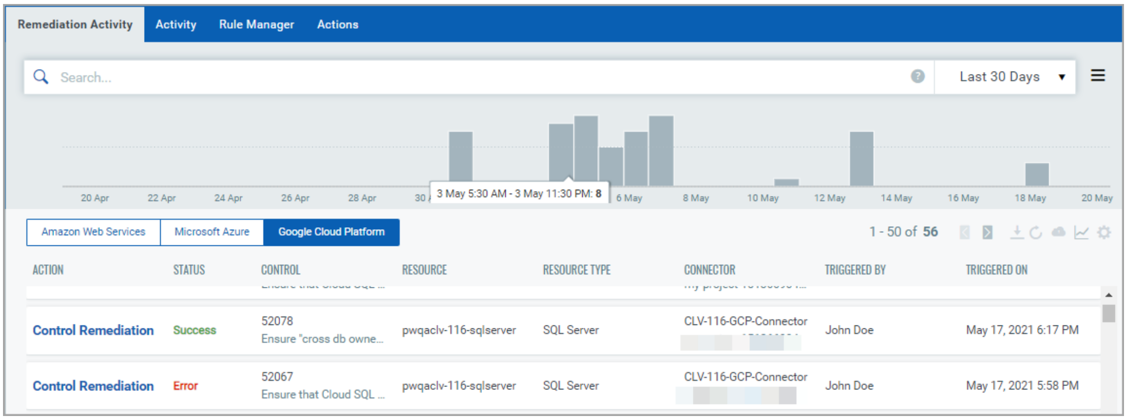
ACTION	STATUS	CONTROL	RESOURCE	RESOURCE TYPE	CONNECTOR	TRIGGERED BY	TRIGGERED ON
Control Remediation	Success	50029 Disable RDP access on...	hk-sanity-50034-2NSG /subscriptions/1d7674...	Network Security Group	Azure Connc Sig Subsc [redacted]	John Doe	May 18, 2021 10:50 AM
Control Remediation	Success	50048 Ensure Web app redire...	SampleQAApp-Saurabh... /subscriptions/9de9e0...	Web App	Azure-CLV-116-Connect... [redacted]	John Doe	May 17, 2021 10:07 AM
Control Remediation	Error	50048 Ensure Web app redire...	SampleQAApp-Saurabh3 /subscriptions/9de9e0...	Web App	Azure-CLV-116-Connect... [redacted]	John Doe	May 17, 2021 10:06 AM

Action for Azure resources:

Control Remediation: indicates Remediate Now button was used to trigger remediation of the Azure resource for the specified CID.

Remediation Activity: GCP

All the activities that are triggered for Azure resources are listed under Responses > Remediation Activity> Google Cloud Platform sub-tab. The Action column indicates the type of remediation activity initiated for a resource.



1 - 50 of 56

ACTION	STATUS	CONTROL	RESOURCE	RESOURCE TYPE	CONNECTOR	TRIGGERED BY	TRIGGERED ON
Control Remediation	Success	52078 Ensure "cross db owne...	pwqaclv-116-sqlserver	SQL Server	CLV-116-GCP-Connector [redacted]	John Doe	May 17, 2021 6:17 PM
Control Remediation	Error	52067 Ensure that Cloud SQL ...	pwqaclv-116-sqlserver	SQL Server	CLV-116-GCP-Connector [redacted]	John Doe	May 17, 2021 5:58 PM

Action for GCP resources:

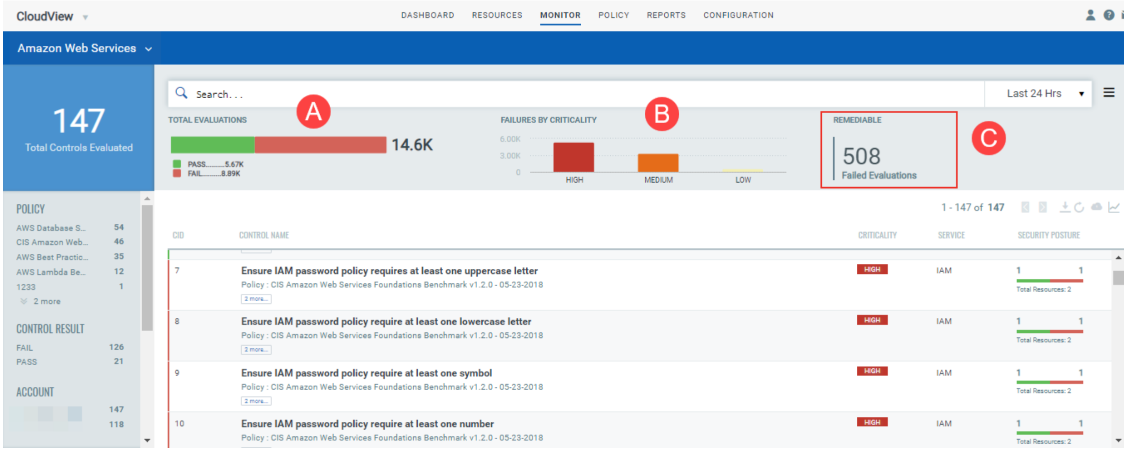
Control Remediation: indicates Remediate Now button was used to trigger remediation of the GCP resource for the specified CID.

Remediating Cloud Resources

We provide you widget cards on Monitor tab which provides total evaluations, failures by criticality, and the count of failed evaluations that can be fixed through remediation.

Remediable Evaluations

With remediation enabled, you can filter out controls with failed evaluations that can be remediated.



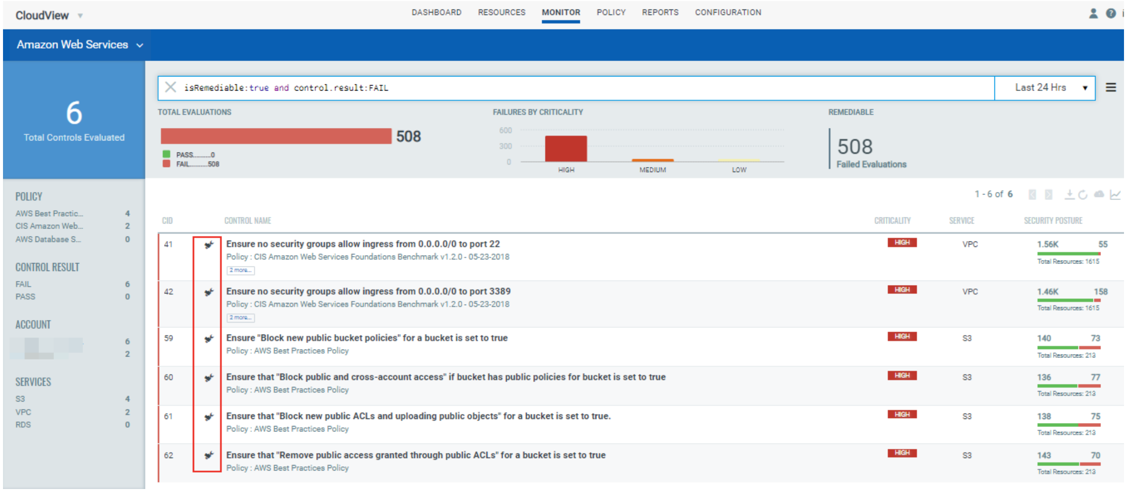
CID	CONTROL NAME	CRITICALITY	SERVICE	SECURITY POSTURE
7	Ensure IAM password policy requires at least one uppercase letter Policy : CIS Amazon Web Services Foundations Benchmark v1.2.0 - 05-23-2018 2 more...	HIGH	IAM	1 1 Total Resources: 2
8	Ensure IAM password policy require at least one lowercase letter Policy : CIS Amazon Web Services Foundations Benchmark v1.2.0 - 05-23-2018 2 more...	HIGH	IAM	1 1 Total Resources: 2
9	Ensure IAM password policy require at least one symbol Policy : CIS Amazon Web Services Foundations Benchmark v1.2.0 - 05-23-2018 2 more...	HIGH	IAM	1 1 Total Resources: 2
10	Ensure IAM password policy require at least one number Policy : CIS Amazon Web Services Foundations Benchmark v1.2.0 - 05-23-2018	HIGH	IAM	1 1 Total Resources: 2

Total Evaluations: Count of passed and failed control evaluations.

Failure by Criticality: Failed Evaluations that are categorized as per failure criticality: High, Medium, and Low.

Remediable: Count of failed evaluations that can be remediated. Click to view the controls with failed evaluations that are remediable.

The “ ✈ ” icon indicates that these controls are available for remediation. Click on one of the controls to proceed with Remediation.

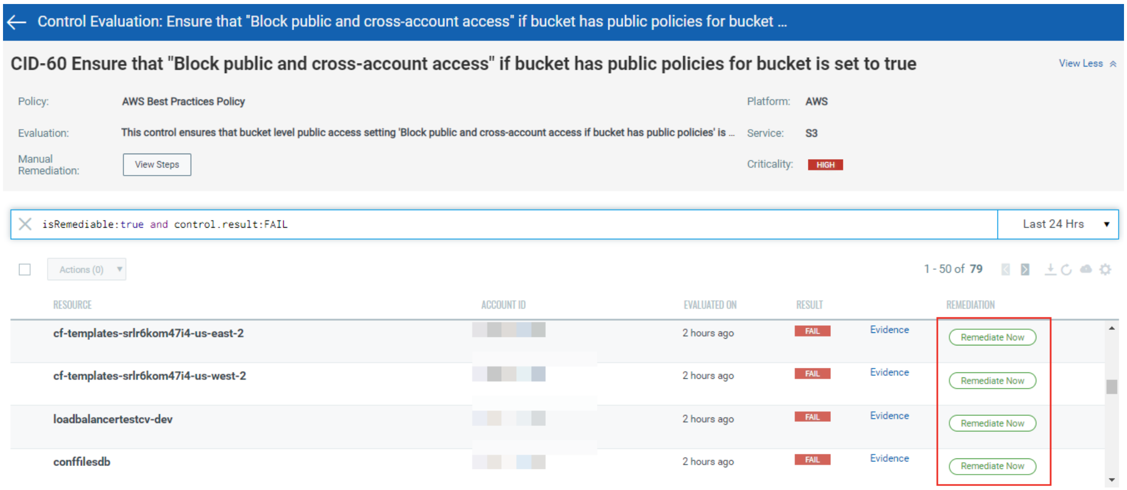


`isRemediable:true and control.result:FAIL`

POLICY	
AWS Best Practic...	4
CIS Amazon Web...	2
AWS Database S...	0
CONTROL RESULT	
FAIL	6
PASS	0
ACCOUNT	
[redacted]	6
[redacted]	2
SERVICES	
S3	4
VPC	2
RDS	0

CID		CONTROL NAME	CRITICALITY	SERVICE	SECURITY POSTURE
41	✈	Ensure no security groups allow ingress from 0.0.0.0/0 to port 22 Policy : CIS Amazon Web Services Foundations Benchmark v1.2.0 - 05-23-2018 2 more...	HIGH	VPC	1.56K 55 Total Resources: 1615
42	✈	Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389 Policy : CIS Amazon Web Services Foundations Benchmark v1.2.0 - 05-23-2018 2 more...	HIGH	VPC	1.46K 158 Total Resources: 1615
59	✈	Ensure "Block new public bucket policies" for a bucket is set to true Policy : AWS Best Practices Policy	HIGH	S3	140 73 Total Resources: 213
60	✈	Ensure that "Block public and cross-account access" if bucket has public policies for bucket is set to true Policy : AWS Best Practices Policy	HIGH	S3	136 77 Total Resources: 213
61	✈	Ensure that "Block new public ACLs and uploading public objects" for a bucket is set to true. Policy : AWS Best Practices Policy	HIGH	S3	138 75 Total Resources: 213
62	✈	Ensure that "Remove public access granted through public ACLs" for a bucket is set to true Policy : AWS Best Practices Policy	HIGH	S3	143 70 Total Resources: 213

Let us consider an example of CID 60.



Control Evaluation: Ensure that "Block public and cross-account access" if bucket has public policies for bucket ...
View Less
View Steps
Last 24 Hrs
Actions (0)
1 - 50 of 79

CID-60 Ensure that "Block public and cross-account access" if bucket has public policies for bucket is set to true

Policy: AWS Best Practices Policy

Evaluation: This control ensures that bucket level public access setting 'Block public and cross-account access if bucket has public policies' is ...

Manual Remediation: View Steps

Platform: AWS

Service: S3

Criticality: HIGH

`isRemediable:true and control.result:FAIL`

RESOURCE	ACCOUNT ID	EVALUATED ON	RESULT		REMEDIATION
cf-templates-srlr6kom47i4-us-east-2	[redacted]	2 hours ago	FAIL	Evidence	Remediate Now
cf-templates-srlr6kom47i4-us-west-2	[redacted]	2 hours ago	FAIL	Evidence	Remediate Now
loadbalancertestcv-dev	[redacted]	2 hours ago	FAIL	Evidence	Remediate Now
conffilesdb	[redacted]	2 hours ago	FAIL	Evidence	Remediate Now

Click Remediate Now.

The Remediation Resource pop-up is displayed. It displays the resources on which action is executed as a part of remediation. The action to be executed and the impact of the action is also listed.

For example, if we initiate remediation for resources that have failed for CID 60. The “Block public and cross-account access to buckets and objects through any public bucket or access point policies" property is enabled for the resource as remediation action.

As a result, the S3 bucket resource ignores public and cross-account access for buckets or access points with policies that grant public access to buckets and objects. Provide a comment for remediation.and select the I, <user name>, authorize to execute remediation actions on the selected resources check box.

Click Remediate.

The Remediation status is now changed to Queued state. Once the remediation is successfully completed, the status of the evaluations changes from FAIL to PASS.

Note: The Evidence details are updated only after the connector run. The Last Remediation Activity tab in Evidence lists the remediation details.

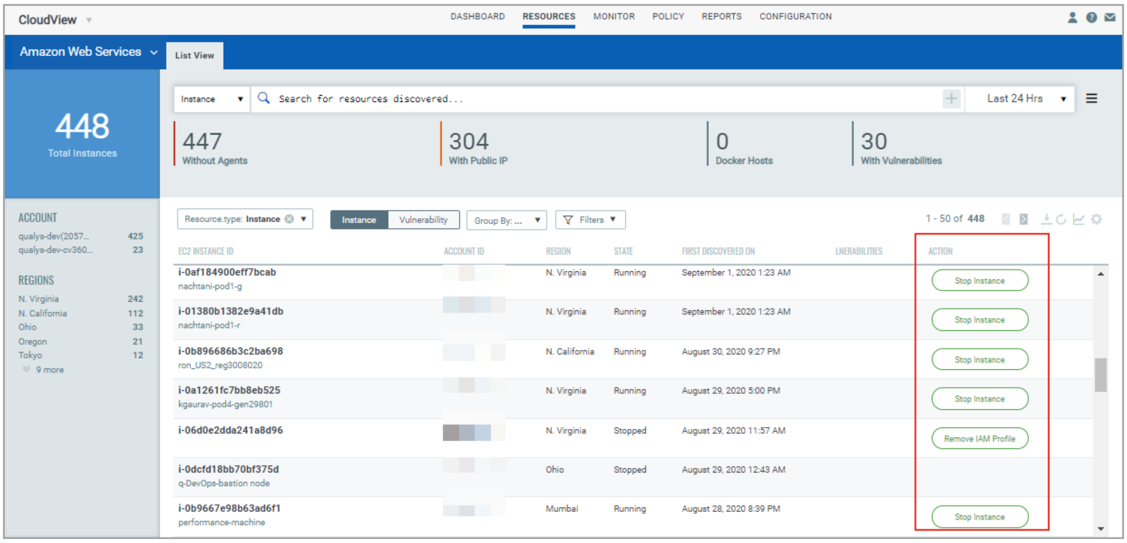
Actions for Cloud Resources (AWS)

We provide you with actions that you can execute on instances to quickly fix unknown behavior of an instance or vulnerability on an instance.

Use Case: Search EC2 instance with critical vulnerability having IAM profile associated.

Action: Stop Instance, Remove IAM Profile

Benefit: Block instance having critical vulnerability from accessing AWS services or stop instance to quarantine it.



448 Total Instances

447 Without Agents

304 With Public IP

0 Docker Hosts

30 With Vulnerabilities

ACCOUNT	
qualys-dev(2057...	425
qualys-dev-cv360...	23

REGIONS	
N. Virginia	242
N. California	112
Ohio	33
Oregon	21
Tokyo	12
9 more	

Resource.type: Instance

1 - 50 of 448

EC2 INSTANCE ID	ACCOUNT ID	REGION	STATE	FIRST DISCOVERED ON	LNERABILITIES	ACTION
i-0af184900eff7bcab nachtani-pod1-g	[redacted]	N. Virginia	Running	September 1, 2020 1:23 AM		Stop Instance
i-01380b1382e9a41db nachtani-pod1-r	[redacted]	N. Virginia	Running	September 1, 2020 1:23 AM		Stop Instance
i-0b896686b3c2ba698 ron_US2_reg3008020	[redacted]	N. California	Running	August 30, 2020 9:27 PM		Stop Instance
i-0a1261fc7bb8eb525 kgaurav-pod4-gen29801	[redacted]	N. Virginia	Running	August 29, 2020 5:00 PM		Stop Instance
i-06d0e2dda241a8d96	[redacted]	N. Virginia	Stopped	August 29, 2020 11:57 AM		Remove IAM Profile
i-0dcfd18bb70bf375d q-DevOps-bastion node	[redacted]	Ohio	Stopped	August 29, 2020 12:43 AM		
i-0b9667e98b63ad6f1 performance-machine	[redacted]	Mumbai	Running	August 28, 2020 8:39 PM		Stop Instance

You can directly control remediable actions from Qualys for Instance resources.

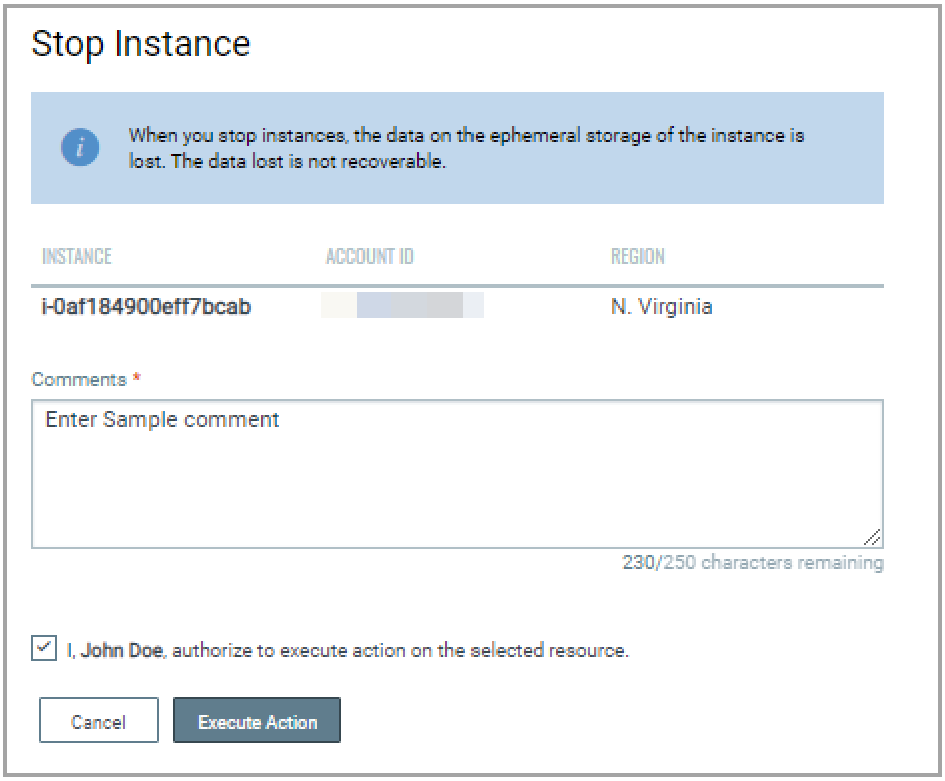
We support the following actions for AWS Instance resources:

Stop Instance

The Stop Instance action allows you stop an already running instance on AWS cloud. You can use the action as an immediate response on a newly detected unknown instance. For example, if you operate only in Mumbai region, but instances are detected in North Carolina region (where you do not operate). In such cases, the first response action towards such unknown instance would be to stop the instance and then troubleshoot it.

You can now execute actions on such instances from Qualys console.

1. Go to Resources > Amazon Web Services > Instance resource type. All the instances in your account are listed. The Actions column displays the possible actions.



Stop Instance

When you stop instances, the data on the ephemeral storage of the instance is lost. The data lost is not recoverable.

INSTANCE	ACCOUNT ID	REGION
i-0af184900eff7bcab	[redacted]	N. Virginia

Comments *

Enter Sample comment

230/250 characters remaining

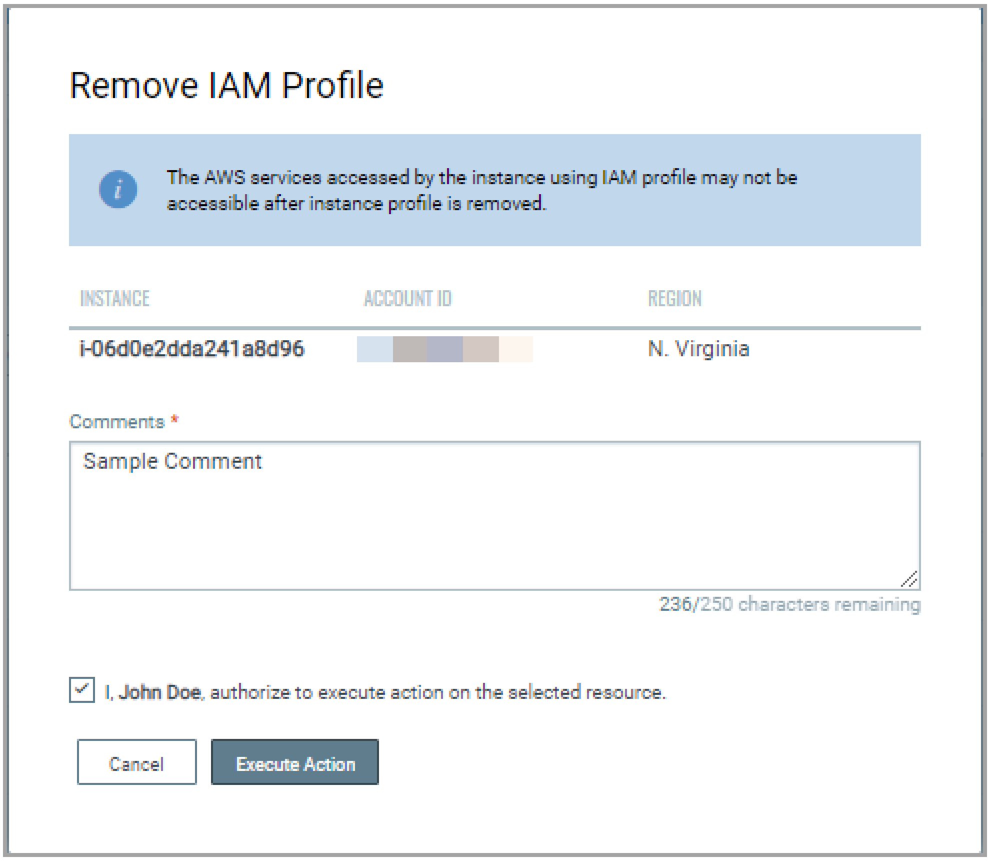
☑ I, John Doe, authorize to execute action on the selected resource.

Click the Stop Instance action.

Remove IAM Profile

The Remove IAM profile action allows you disassociate an IAM profile from the instance. Removing IAM profile stops access to other AWS resources that may be available through the associated IAM role. You can execute the action in following scenarios:

Go to Resources > Amazon Web Services > Instance resource type. All the instances in your account are listed. The Actions column displays the possible actions.



Remove IAM Profile

The AWS services accessed by the instance using IAM profile may not be accessible after instance profile is removed.

INSTANCE	ACCOUNT ID	REGION
i-06d0e2dda241a8d96	[redacted]	N. Virginia

Comments *

Sample Comment

236/250 characters remaining

☑ I, John Doe, authorize to execute action on the selected resource.

Click Remove IAM Profile action.

The Remove IAM profile pop-up is displayed.

Specify a comment and select the authorization check box.

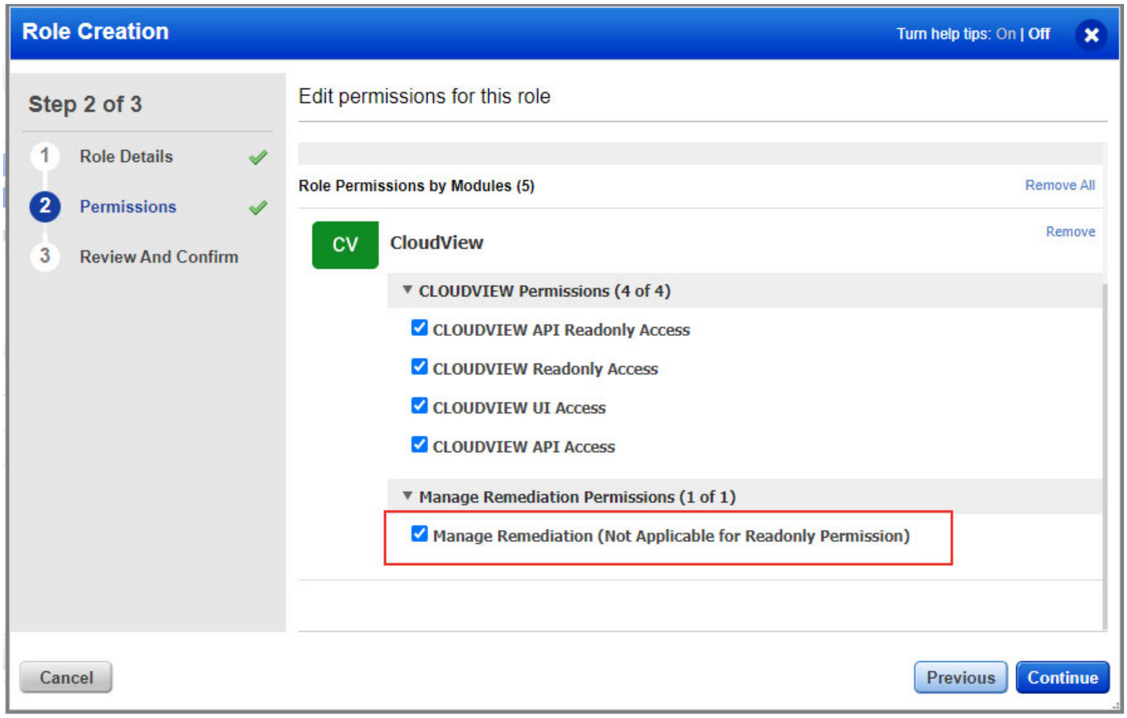
Click Execute Action.

You can view the history of actions executed on instances. Simply, select the instance, and select Show Action Log from the quick action menu. The Action Log displays the list of actions executed on the instance.

Permissions Required

We have provided permission for remediation. You can choose to enable to disable remediation for sub-users.

By default, remediation is accessible to all the Manager users. You can assign access to sub-users based on their Roles. For a sub user to be able to perform remediation actions, a user with Manager role needs to assign the permission to the sub users from the Administration utility.


Role Creation

Step 2 of 3

1 Role Details ✓
2 Permissions ✓
3 Review And Confirm

Edit permissions for this role

Role Permissions by Modules (5)

CV CloudView

▼ CLOUDVIEW Permissions (4 of 4)
☑ CLOUDVIEW API Readonly Access
☑ CLOUDVIEW Readonly Access
☑ CLOUDVIEW UI Access
☑ CLOUDVIEW API Access

▼ Manage Remediation Permissions (1 of 1)
☑ Manage Remediation (Not Applicable for Readonly Permission)

There are two types of sub users that a user with Manager role can create. Depending on the permissions you assign to the role, you could categorize the sub users as follows:

All privilege: You need to assigns Manage Remediation permission to a sub user with all privileges so that the sub user can perform all actions related to remediation.

Reader privileges: Sub user with Reader role can view remediable controls and connectors for which remediation is enabled. The sub user can neither create or edit connectors with remediation enable, nor can they execute any remediation actions on any of the resources.

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

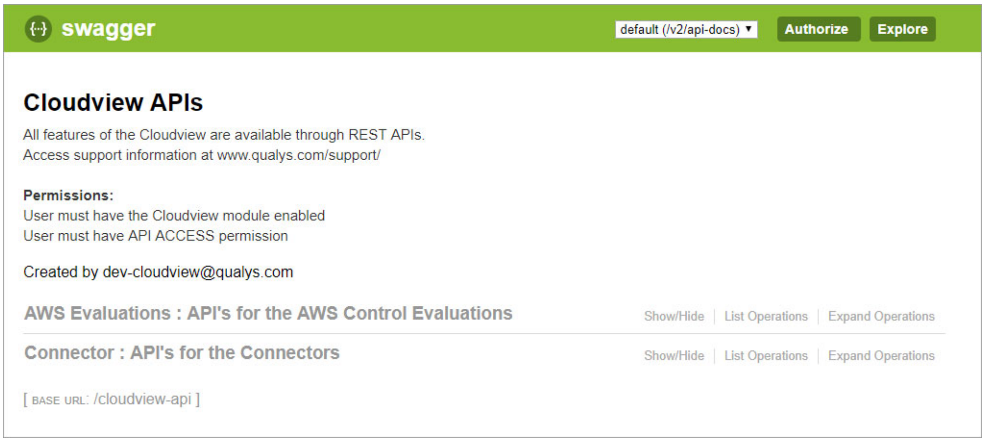
Swagger is a widely-adopted specification that allows for programmatically describing REST APIs. The Swagger UI provides all the details about the APIs and how to invoke them. This includes information like the HTTP verbs to use (GET, POST, PUT, etc.), the URL paths, allowable parameters and types, and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

API Examples

You can view examples and details on API usage in our CloudView API User Guide.

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
Qualys Canada Platform	https://qualysapi.qg1.apps.qualys.ca

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!

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.

Automatic Connector Creation

We have built few scripts that could ease tasks for you in CloudView.

-Connector Creation: There are various scripts you could use to automate connector creation task.

-Export to Splunk: Use CloudView_Splunk_Scripted_Inputs to integrate CloudView via python scripted inputs into Splunk Enterprise.

-Alerting data: You could use slack_cloudview_alerts to integrate CloudView Assessment data into Slack for alerting.

You could automate few steps using the scripts we provide. For complete details and list of scripts, click here.

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.

Tell me the difference between sub user roles

There are two types of sub users that a user with Manager role can create. Depending on the permissions you assign to the role, you could categorize the sub users as follows:

All privilege: Sub User will have all the privileges in CloudView except creating and managing other users.

Reader privileges: Sub User with Reader role can only view the data displayed in CloudView module.

How do I manage access for sub users?

There are two options you could configure access for sub users

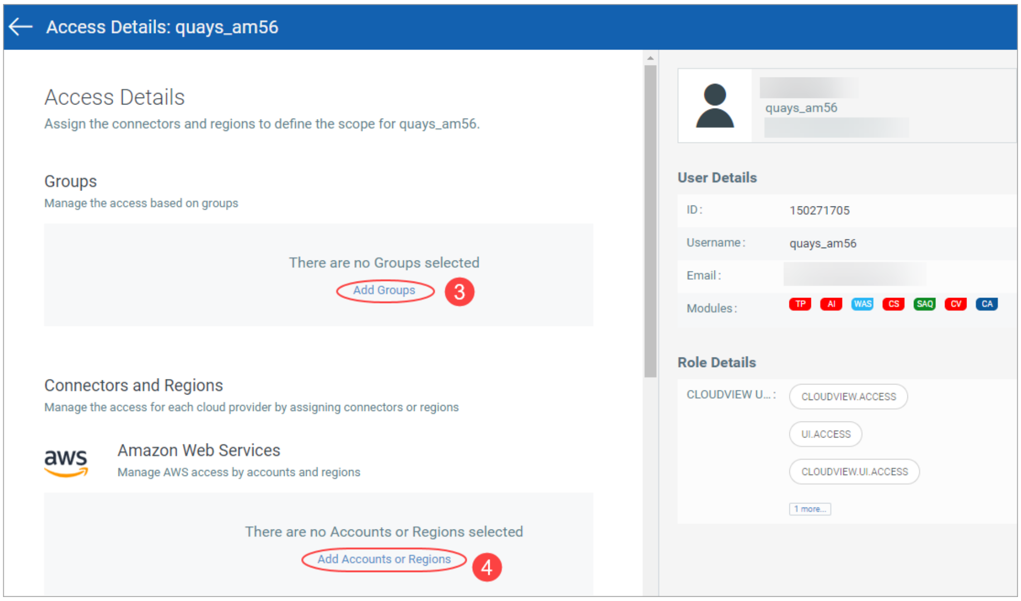
- Direct scope definition for sub user

When you define scope for a sub user, you could directly select the connectors for every Cloud Provider and associate it with the sub user. The sub user can then access all the connectors defined in the scope for the sub user.

In the Access Management tab, select the user and select Manage Access from the quick action menu. Click Add Accounts link for the specific Cloud Provider and then select the connector, and click Save.

You can select multiple connectors from multiple cloud providers as well.

For AWS, you can select connector and region as well.



Access Details: quays_am56

Access Details

Assign the connectors and regions to define the scope for quays_am56.

Groups

Manage the access based on groups

There are no Groups selected

Connectors and Regions

Manage the access for each cloud provider by assigning connectors or regions

Amazon Web Services

Manage AWS access by accounts and regions

There are no Accounts or Regions selected

[redacted]
quays_am56
[redacted]

User Details

ID: 150271705
Username: quays_am56
Email: [redacted]
Modules: TP AI WAS CS SAQ CV CA

Role Details

CLOUDVIEW U...: CLOUDVIEW.ACCESS UI.ACCESS CLOUDVIEW.UI.ACCESS 1 more...

- Using groups

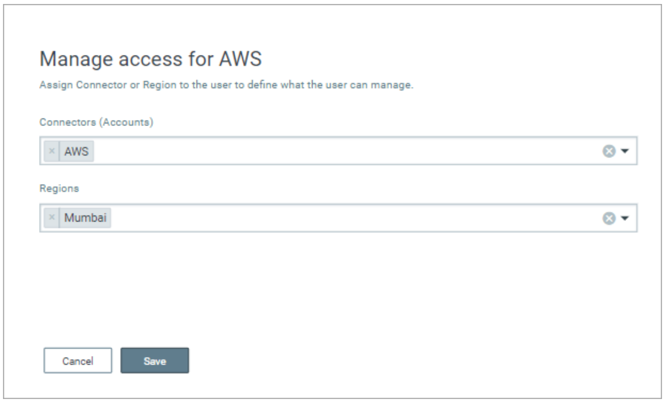
Use connector groups to configure connector access for a sub user.

By default, the sub user can access all connectors as no group is assigned to any user. Assign group to user to provide access or restrict access to connectors associated with the group.

Navigate to Configuration tab and then the Cloud Provider (AWS, Azure, or GCP) for which you would want to create connector groups.

Choose the connector for which you want to configure access and click Assign Group from the quick action menu.

Type a name for the group and click Create and then click Save.



Manage access for AWS

Assign Connector or Region to the user to define what the user can manage.

Connectors (Accounts): AWS

Regions: Mumbai

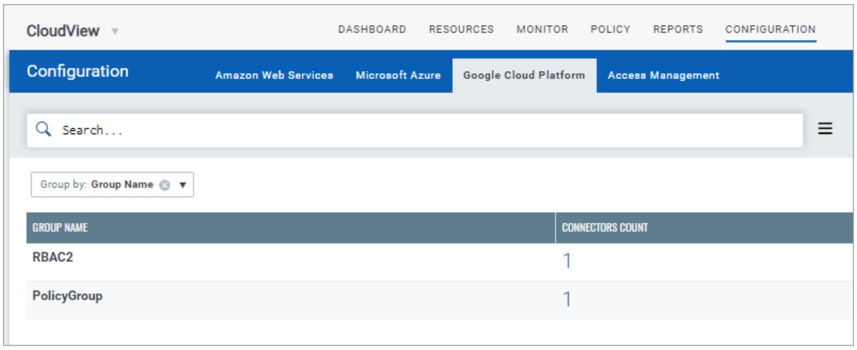
How to change default behavior for sub users with all privileges?

A sub user with all privileges is able to perform all functions and access all connectors by default. If you want to restrict the access to single connector, simply create connector group and assign it to the sub user. The sub user can then access only the single connector associated with the assigned group.

To configure access to multiple connectors, assign a common group to all such connectors and associate it with the required users.

Tell me about GroupBy option

To view the list of connectors grouped together for a single cloud provider, simply click the Group by option.



Group by: Group Name

GROUP NAME	CONNECTORS COUNT
RBAC2	1
PolicyGroup	1

Alternatively, you could use search token.

```
group.name: <groupname>
```

and the search result lists all the connectors for a cloud provider associated with the group.

Tell me Scope and Access Conflicts

Consider a sub user whose direct scope definition conflicts with the access assigned through groups. In such cases, the scope overrides and the sub user is able to access the connectors defined directly through the scope of the user.

Let us consider two different examples to understand the conflicts better.

Case 1: A sub user is assigned a group named AWS_important that includes access to two AWS connectors. Also, the sub user has been directly assigned access to five other AWS connectors. In such case, the sub user is able to access all the seven connectors.

Case 2: A sub user is assigned a group that includes none of the connectors. In such case, the sub user cannot access any connector.

However, if the same sub user is directly assigned connectors through scope definition, the sub user can access the connectors that are directly assigned.

Download Datalist

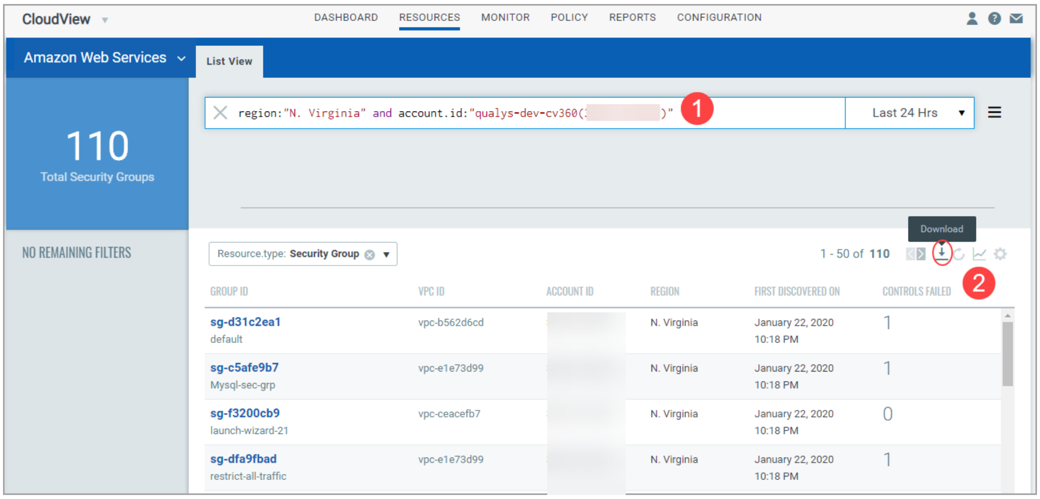
By downloading datalist to your local system you can easily manage the list outside of the Qualys platform and share them with other users. You can download results in CSV format.

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 10,000 records.

1) Use our search to narrow down your results.

2) Select Download from the Tools menu.



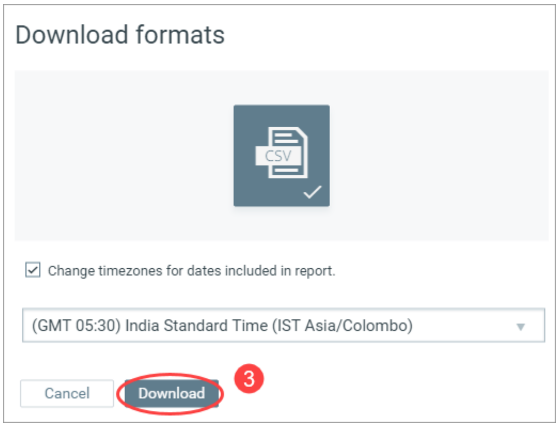
region:"N. Virginia" and account.id:"qualys-dev-cv360([redacted])"

Resource.type: Security Group

1 - 50 of 110

GROUP ID	VPC ID	ACCOUNT ID	REGION	FIRST DISCOVERED ON	CONTROLS FAILED
sg-d31c2ea1 default	vpc-b562d6cd	[redacted]	N. Virginia	January 22, 2020 10:18 PM	1
sg-c5afe9b7 Mysql-sec-grp	vpc-e1e73d99	[redacted]	N. Virginia	January 22, 2020 10:18 PM	1
sg-f3200cb9 launch-wizard-21	vpc-ceacefb7	[redacted]	N. Virginia	January 22, 2020 10:18 PM	0
sg-dfa9fbad restrict-all-traffic	vpc-e1e73d99	[redacted]	N. Virginia	January 22, 2020 10:18 PM	1

3) Click Download. That's it!



Download formats

☑ Change timezones for dates included in report.

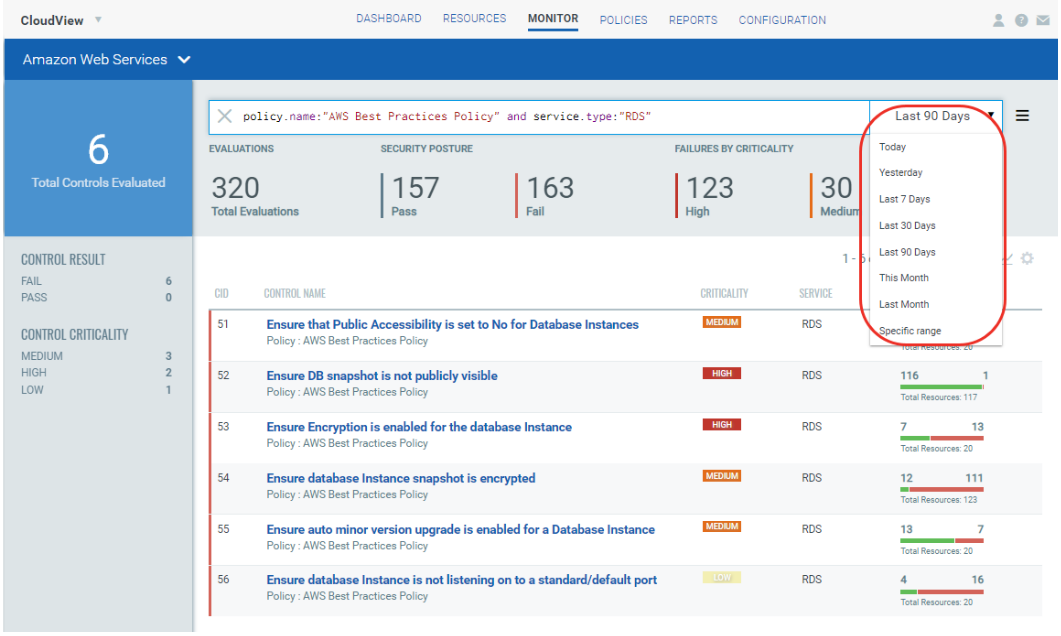
(GMT 05:30) India Standard Time (IST Asia/Colombo)

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"
```

Last 90 Days

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

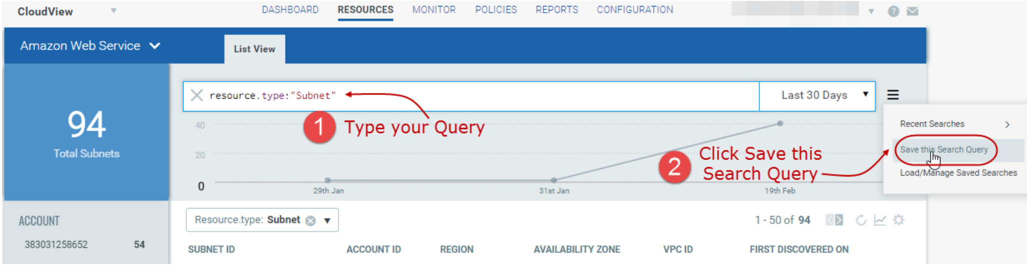
1 - 6

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"
```

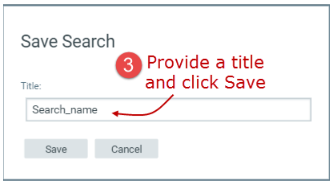
Last 30 Days

Resource.type: **Subnet**

1 Type your Query

2 Click Save this Search Query

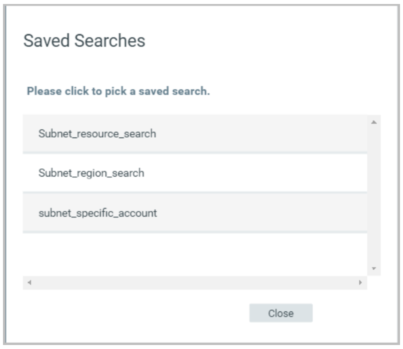
Give your search a title.



Title: Search_name

3 Provide a title and click Save

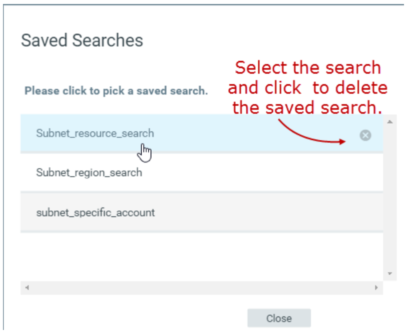
Choose Load/manage Saved Searches to use one of the searches you previously saved.



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.



Please click to pick a saved search.

- Subnet_resource_search
- Subnet_region_search
- subnet_specific_account

Select the search and click to delete the saved search.

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.

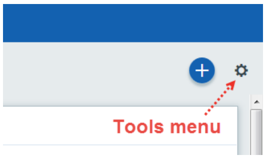
Each dashboard is a collection of widgets showing resource data of interest. You can create multiple dashboards and switch between them.

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

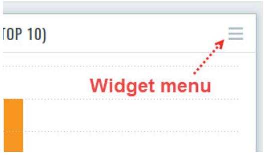
How to Take Action

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.



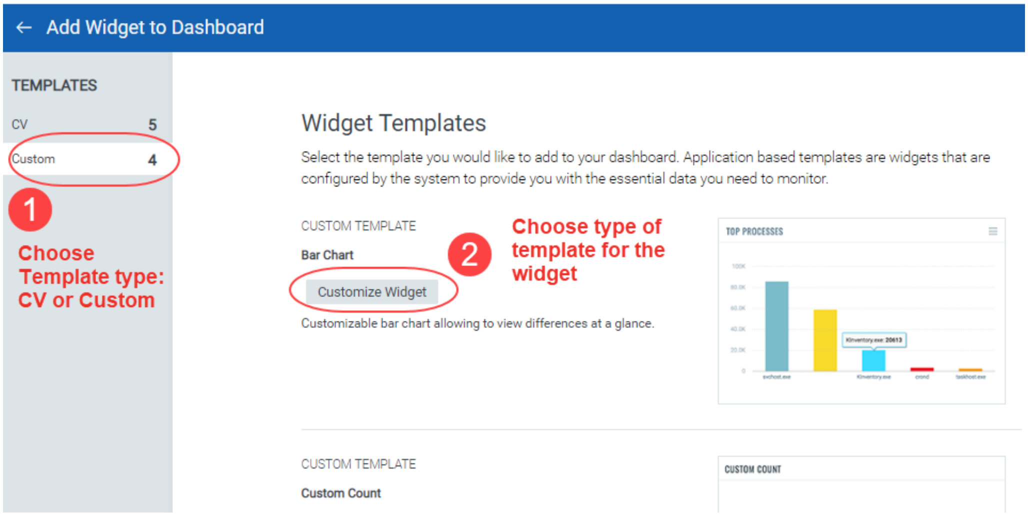
Take actions on a single widget: edit widget, delete widget, refresh widget data, create template from widget, export widget.



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.

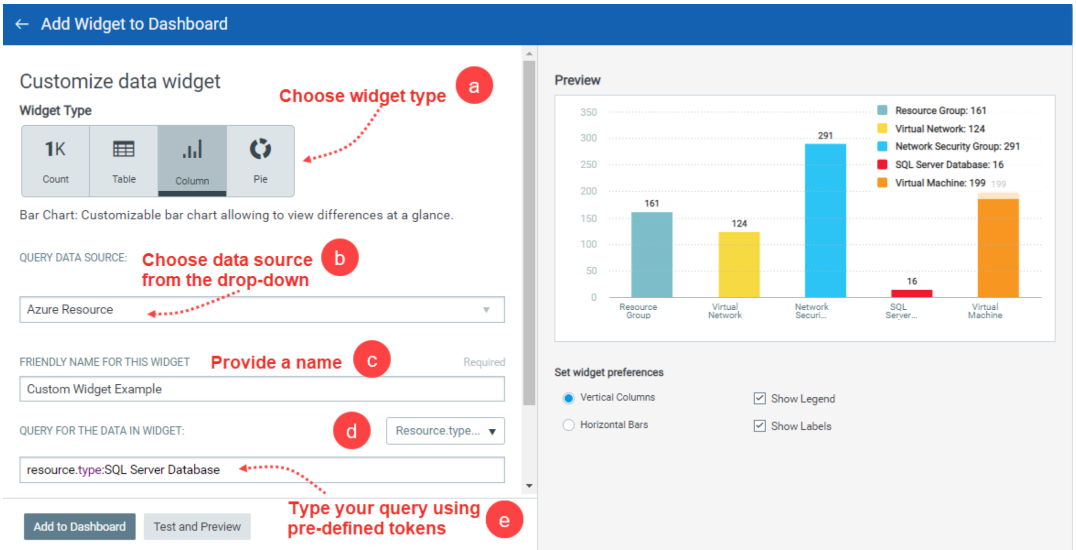


Widget Templates

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.

Customizable bar chart allowing to view differences at a glance.

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

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

QUERY DATA SOURCE: Azure Resource

FRIENDLY NAME FOR THIS WIDGET (Required): Custom Widget Example

QUERY FOR THE DATA IN WIDGET: Resource.type...

resource.type:SQL Server Database

Preview

Set widget preferences

● Vertical Columns

○ Horizontal Bars

☑ Show Legend

☑ 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 - Choose the resource type

e - 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.

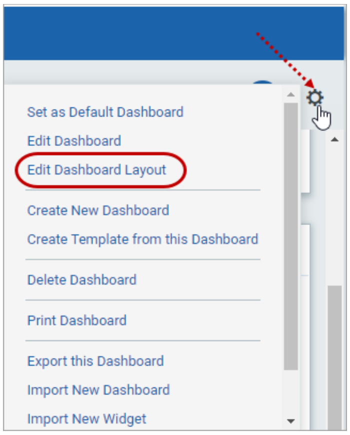
Resize any widget horizontally, drag & drop widgets to change the layout. Refresh your view.

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.

Appendix: List of 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

CIS Amazon Web Services Foundations Benchmark

AWS Best Practices Policy

AWS Lambda Best Practices Policy

AWS Database Service Best Practices Policy

Azure

CIS Microsoft Azure Foundations Benchmark

Azure Best Practices Policy

Azure Function App Best Practices Policy

Azure Database Service Best Practices Policy

GCP

CIS Google Cloud Platform Foundation Benchmark

GCP Best Practices Policy

GCP Cloud Functions Best Practices Policy

GCP Cloud SQL Best Practices Policy

GCP Kubernetes Engine Best Practices Policy

AWS Policies

Let us view all the policies and associated controls for AWS.

CIS Amazon Web Services Foundations Benchmark

We support controls for following AWS resources:

Identity and Access Management (IAM)

CloudTrail

VPC

Config

Network ACLs

S3 Bucket

Identity and Access Management (IAM)

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

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

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

CID 12: Ensure IAM password policy prevents password reuse

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 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

CID 68: Ensure that all the expired SSL/TLS certificates stored in AWS IAM are removed: This control needs current date to evaluate. Not supported in current framework.

CID 160: Ensure that IAM Access analyzer is enabled

CID 171: Ensure there is only one active access key available for any single IAM user

CID 175: Ensure no Inline Policies are attached to IAM Users directly

CID 176: Ensure no Managed Policies are attached to IAM Users directly

CloudTrail

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

CID 172: Ensure a log metric filter and alarm exists for AWS Organizations changes

VPC

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

CID 23: Ensure AWS Config is enabled in all regions

Network ACLs

CID 161: Ensure no Network ACLs allow ingress from 0.0.0.0/0 to port 22

CID 170: Ensure no Network ACLs allow ingress from 0.0.0.0/0 to port 3389

S3 Bucket

CID 59: Ensure "Block new public bucket policies" for a bucket is set to true.

CID 60: Ensure that "Block public and cross-account access" if bucket has public policies for bucket is set to true.

CID 61: Ensure that "Block new public ACLs and uploading public objects" for a bucket is set to true.

CID 62: Ensure that "Remove public access granted through public ACLs" for a bucket is set to true

CID 177: Ensure that Object-level logging for write events is enabled for S3 bucket

CID 178: Ensure that Object-level logging for read events is enabled for S3 bucket

AWS Best Practices Policy

We support controls for following AWS resources:

IAM

S3 Controls

EC2 Images

EBS Volumes

KMS Key

KMS Key Store

Load Balancers

EFS

Redis

Memcached

ES Domain

Route S3

FireHose

KMS

Directory

IAM

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

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

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

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

CID 63: Ensure 'Block new public bucket policies' for an AWS Account is set to true.

CID 64: Ensure 'Block public and cross-account access to buckets that have public policies' for an AWS Account is set to true.

CID 65: Ensure 'Block new public ACLs and uploading public objects' for an account is set to true.

CID 66: Ensure 'Remove public access granted through public ACLs' for an account is set to true.

CID 67: Ensure Server Side Encryption (SSE) is enabled for S3 bucket.

EC2 Images

CID 114: Ensure Images (AMIs) owned by an AWS account are not public

CID 126: Ensure AMIs owned by an AWS account are encrypted

EBS Volumes

CID 115: Ensure that EBS Volumes attached to EC2 instances are encrypted

CID 116: Ensure that Unattached EBS Volumes are encrypted

CID 127: Ensure AWS EBS Volume snapshots are encrypted

CID 145: Ensure CMK is used to encrypt data at rest for EFS

CID 146: Ensure that AWS Elastic Block Store (EBS) volume snapshots are not public

CID 203: Ensure EBS volumes are encrypted with customer managed master keys

CID 204: Ensure AWS EBS Volume snapshots are encrypted with customer managed master keys

KMS Key

CID 58: Ensure that the key expiry is set for CMKs with external key material.

CID 119: Ensure no AWS Managed CMKs is present

CID 120: Ensure no CMK is marked for deletion

CID 121: Ensure only Root user of the AWS Account should be allowed full access on the CMK

CID 122: Permissions to delete key is not granted to any Principal other than the Root user of AWS Account

CID 123: Ensure CMK administrators are not the user of the key

KMS Key Store

CID 124: Ensure all Custom key stores are connected to their CloudHSM clusters

Load Balancers

CID 128: Ensure access log is enabled for Elastic load balancer

CID 129: Ensure access log is enabled for Classic Elastic load balancer

CID 130: Ensure Classic Elastic load balancer is not using unencrypted protocol

CID 131: Ensure Elastic load balancer listener is not using unencrypted protocol

CID 184: Ensure there are no Internet facing Application load balancers

CID 185: Ensure ALB using listener type HTTPS must have SSL Security Policy

CID 186: Ensure that ALB using listener type HTTP must be redirected to HTTPS

CID 187: Ensure that ALB listeners have HTTPS enabled Target Groups

EFS

CID 144: Ensure EFS Encryption is enabled for data at rest

Redis

CID 148: Ensure that AWS ElastiCache Redis clusters are not associated with default VPC

CID 149: Ensure that AWS ElastiCache redis clusters are not using their default endpoint ports

CID 151: Ensure AWS ElastiCache Redis cluster with MultiAZ Automatic Failover feature is set to enabled

CID 152: Ensure AWS ElastiCache Redis cluster with Redis AUTH feature is enabled

CID 153: Ensure that AWS ElastiCache Redis clusters are In-Transit encrypted

CID 154: Ensure that AWS ElastiCache Redis clusters are Data At-Rest encrypted

CID 155: Ensure that AWS ElastiCache Redis clusters are Data At-Rest encrypted with CMK

Memcached

CID 147: Ensure that AWS ElastiCache Memcached clusters are not associated with default VPC

CID 150: Ensure that AWS ElastiCache memcached clusters are not using their default endpoint ports

ES Domain

CID 156: Ensure node-to-node encryption feature is enabled for AWS Elasticsearch Service domains
CID 157: Ensure AWS Elasticsearch Service domains have enabled the support for publishing slow logs to AWS CloudWatch Logs
CID 158: Ensure AWS Elasticsearch Service domains are not publicly accessible
CID 159: Ensure AWS Elasticsearch Service domains are using the latest version of Elasticsearch engine

Route S3

CID 162: Ensure AWS Route 53 Registered domain has Transfer lock enabled

CID 163: Ensure AWS Route 53 Registered domain has Auto renew Enabled

CID 164: Ensure AWS Route 53 Registered domain is not expired

FireHose

CID 165: Ensure AWS Kinesis Data Firehose delivery stream with Direct PUT and other sources as source has Server-side encryption configured

CID 166: Ensure AWS Kinesis Data Firehose delivery stream with Kinesis Data stream as source has Server-side encryption configured

CID 167: Ensure AWS Kinesis Data Firehose delivery stream with Direct PUT and other sources as source has Server-side encryption configured with KMS Customer Managed Keys

KMS

CID 174: Ensure that Customer managed KMS keys use external key material

Directory

CID 188: Ensure IncreaseVolumeSize is Disabled for Workspace directories in all regions

CID 205: Ensure "RestartWorkspace" is Enabled in all the regions

CID 208: Ensure WorkDocs is not enabled in Workspace Directories

CID 209: Ensure Access to Internet Access is not enabled in Workspace Directories

CID 210: Ensure Local Administrator setting is not enabled in Workspace Directories

CID 211: Ensure Maintenance Mode is not enabled in Workspace Directories

CID 212: Ensure Device Type Windows Access Control is not enabled in Workspace Directories

CID 213: Ensure Device Type MacOS Access Control is not enabled in Workspace Directories

CID 214: Ensure Device Type Web Access Control is not enabled in Workspace Directories

CID 215: Ensure Device Type iOS Access Control is not enabled in Workspace Directories

CID 216: Ensure Device Type Android Access Control is not enabled in Workspace Directories

CID 217: Ensure Device Type ChromeOS Access Control is not enabled in Workspace Directories

CID 218: Ensure Device Type ZeroClient Access Control is not enabled in Workspace Directories

AWS Lambda Best Practices Policy

We support AWS Lambda Best Practices Policy specifically for Lambda resources. The pre-defined system policy is loaded with following system-defined controls.

CID 97: Ensure that Lambda function has tracing enabled

CID 98: Ensure that Lambda Function is not using An IAM role for more than one Lambda Function

CID 99: Ensure that Multiple Triggers are not configured in Lambda Function

CID 100: Ensure that Lambda Runtime Version is latest and not custom

CID 101: Ensure that Lambda function does not have Admin Privileges

CID 102: Ensure that Lambda function does not have Cross Account Access

CID 103: Ensure that Lambda Environment Variables at-rest are encrypted with CMK

CID 104: Ensure that Lambda Environment Variables are encrypted using AWS encryption helpers for encryption in transit

CID 105: Ensure that Lambda function is not Exposed (Ensure that Lambda function does not allows anonymous invocation)

CID 106: Ensure that VPC access for Lambda Function is not set to default(Null)

CID 107: Ensure that AWS Lambda excess Permissions are removed

Note: This control is not applicable for GovCloud region.

CID 125: Ensure that multiple triggers are not configured for Lambda Function Aliases

AWS Database Service Best Practices Policy

We have AWS Database Service Best Practices Policy. This policy covers best practices for PaaS database configuration exposed by AWS.

RDS

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

CID 69: Ensure automated backups are enabled for RDS database instances

CID 70: Ensure that Deletion Protection is enabled for RDS DB Cluster

CID 71: Ensure that Deletion Protection is enabled for RDS Database instances

CID 72: Ensure that IAM Database Authentication is Enabled for the DB Cluster

CID 73: Ensure that IAM Database Authentication is Enabled for the DB Instances

CID 74: Ensure that AWS RDS Log Exports is enabled for DB Cluster

CID 75: Ensure that AWS RDS Log Exports is enabled for DB Instances

CID 76: Ensure that RDS Database Master username is not set to well-known/default

CID 77: Ensure VPC security group attached to RDS Database Instance does not allows Inbound traffic from ANY source IP

CID 78: Ensure RDS DB instances are not present in public subnets

CID 79: Ensure RDS DB Cluster are not present in public subnets

CID 80: Ensure Event Subscriptions for Instance Level Events is Enabled for DB Instances

CID 81: Ensure RDS Microsoft SQL instance enforces encrypted connections only

CID 82: Ensure RDS PostgreSQL instance enforces encrypted connections only

CID 83: Ensure RDS PostgreSQL Cluster enforces encrypted connections only

CID 84: Ensure that Encryption is enabled for the RDS DB Cluster

CID 85: Ensure RDS DB Cluster snapshots are encrypted

CID 86: Ensure CMK is used to protect RDS DB Cluster encryption key

CID 87: Ensure CMK is used to protect RDS Db Instance encryption key

CID 88: Ensure DB instance replication is set to the another Zone for High Availability

CID 89: Ensure that DB Cluster replication is set to the another Zone for High Availability

CID 90: Ensure RDS database Cluster snapshots are not public

CID 91: Ensure that Enhance monitoring is enabled for RDS Database Instance

CID 92: Ensure that AWS RDS DB Cluster with copy tags to snapshots option is enabled

CID 93: Ensure AWS RDS instances with copy tags to snapshots option is enabled

CID 94: Ensure Event Subscriptions for cluster Level Events is Enabled for DB Clusters

CID 95: Ensure MYSQL DB Instance backup Binary logs configuration is not enabled

CID 96: Ensure backup configuration is enabled for MSSQL DB Instances

CID 117: Ensure that RDS Instances certificates are rotated

RedShift Clusters

CID 108: Ensure Version Upgrade is enabled for AWS Redshift clusters to automatically receive upgrades

CID 109: Ensure that AWS Redshift database clusters are not using default endpoint port

CID 110: Ensure that Redshift clusters are not publicly accessible

CID 111: Ensure that AWS Redshift clusters master username is not set to well-known/default

CID 112: Ensure that AWS Redshift clusters encryption is set for data at rest

CID 113: Ensure audit logging is enabled for AWS Redshift clusters for security and troubleshooting purposes

CID 189: Ensure Automated backup retention is set for Redshift Cluster

DocumentDB Instance

CID 118: Ensure that DocumentDB Instances certificates are rotated

Document DB Clusters

CID 132: Ensure DocumentDB database cluster master username is not set to well-known/default

CID 133: Ensure backup retention is set to minimum of 7 days for DocumentDB clusters

CID 134: Ensure audit logs is enabled for Log export to CloudWatch for DocumentDB clusters

CID 135: Ensure deletion protection is enabled for DocumentDB clusters

CID 136: Ensure DocumentDB Cluster is not listening on default port

CID 206: Ensure Document DB Cluster snapshots are encrypted

CID 207: Ensure Document database Cluster snapshots are not public

Neptune DB Clusters

CID 137: Ensure multi-AZ high availability is enabled for neptune database cluster

CID 138: Ensure neptune database cluster is not listening on default port

CID 139: Ensure IAM db authentication is enabled for neptune database cluster

CID 140: Ensure backup retention is set to minimum of 7 days for neptune database cluster

CID 141: Ensure Audit logs is enabled for log exports to cloudwatch for neptune database cluster

CID 142: Ensure Auto minor version upgrade is enabled for neptune database instances

CID 143: Ensure deletion protection is enabled for neptune database cluster

CID 219: Ensure Neptune DB Cluster snapshots are encrypted

CID 220: Ensure Neptune database Cluster snapshots are not public

DynamoDB

CID 169: Ensure DynamoDB tables are encrypted using KMS Customer managed Keys

CID 173: Ensure DynamoDB tables are not configured using DEFAULT encryption

Azure Policies

Let us view all the policies and associated controls for Azure.

CIS Microsoft Azure Foundations Benchmark

We support controls for following Azure resources:

Security Centre

Storage Accounts

SQL Server Database

SQL Servers

MySQL Server

PostgreSQL Server

Logging and Monitoring

Networking

Virtual Machines

Web App

Key Vault

Kubernetes

Azure Active Directory

Security Centre

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

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'

CID 50078: Ensure that Settings - Threat Detection for Windows Defender ATP (WDATP) is selected

CID 50079: Ensure that Standard pricing tier is enabled for PaaS SQL servers

CID 50080: Ensure that Standard pricing tier is enabled for App Service

CID 50081: Ensure that Standard pricing tier is enabled for Storage Accounts

CID 50082: Ensure any of the ASC Default policy setting is not set to “Disabled"

CID 50139: Ensure that Azure Defender is set to On for Kubernetes

CID 50140: Ensure that Azure Defender is set to On for Container Registries

CID 50141: Ensure that Azure Defender is set to On for Key Vault

Storage Accounts

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

CID 50052: Ensure default network access rule for Storage Accounts is set to deny

CID 50053: Ensure 'Trusted Microsoft Services' is enabled for Storage Account access

CID 50133: Ensure soft delete is enabled for Azure Storage.

CID 50134: Ensure Storage Service Encryption is enabled for Storage Accounts.

SQL Server Database

CID 50001: Ensure that Data encryption is set to ON for a SQL database

SQL Servers

CID 50002: Ensure no SQL Servers allow ingress from Internet (ANY IP)

CID 50013: Ensure that default Auditing policy for a SQL Server is configured to capture and retain the activity logs

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

CID 50028: Ensure that Advanced Data Security is enabled and Advanced Threat Protection settings is configured properly for a SQL Server

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

CID 50083: Ensure that ADS - Vulnerability Assessment (VA) is enabled and configured properly

MySQL Server

CID 50039: Ensure 'Enforce SSL connection' is set to 'ENABLED' for MySQL Database Server

PostgreSQL Server

CID 50040: Ensure Enforce SSL connection" is set to "ENABLED" for PostgreSQL Database Server"

CID 50041: Ensure server parameter log_checkpoints" is set to "ON" for PostgreSQL Database Server"

CID 50042: Ensure server parameter log_connections" is set to "ON" for PostgreSQL Database Server"

CID 50043: Ensure server parameter log_disconnections" is set to "ON" for PostgreSQL Database Server"

CID 50045: Ensure server parameter log_retention_days" is greater than 3 days for PostgreSQL Database Server"

CID 50074: Ensure server parameter connection_throttling" is set to "ON" for PostgreSQL Database Server"

CID 50117: Ensure no PostgreSQL Server allow ingress from Internet (ANY IP)

Logging and Monitoring

CID 50063: Ensure Activity Log Alert exists for Create Policy Assignment

CID 50064: Ensure Activity Log Alert exists for Create or Update Network Security Group

CID 50065: Ensure Activity Log Alert exists for Delete Network Security Group

CID 50066: Ensure Activity Log Alert exists for Create or Update Network Security Group Rule

CID 50067: Ensure Activity Log Alert exists for Delete Network Security Group Rule

CID 50068: Ensure Activity Log Alert exists for Create or Update Security Solution

CID 50069: Ensure Activity Log Alert exists for Delete Security Solution

CID 50070: Ensure Activity Log Alert exists for Create or Update SQL Server Firewall Rule

CID 50071: Ensure Activity Log Alert exists for Update Security Policy

CID 50056: Ensure Storage account containing container with activity logs is encrypted with BYOK

CID 50076: Ensure storage container storing activity logs is not publicly accessible

CID 50135: Ensure that Activity Log Alert exists for Delete Policy Assignment

CID 50142: Ensure Diagnostic Setting captures appropriate categories

Networking

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 50055: Ensure Network Security Group Flow Log retention is greater than 90 days

CID 50062: Ensure Network Watcher is Enabled for your Subscription

Virtual Machines

CID 50032: Ensure that all unattached VM disks are encrypted

CID 50033: Ensure that all attached VM disks are encrypted

CID 50034: Ensure disks are encrypted for Windows VMs with ADE version 1.1

CID 50130: Ensure that the endpoint protection for all Virtual Machines is installed

Web App

CID 50047: Ensure App Service Authentication is set on Azure App Service

CID 50048: Ensure web app redirects all HTTP traffic to HTTPS in Azure App Service

CID 50049: Ensure web app has 'Client Certificates (Incoming client certificates)' set to 'On'

CID 50050: Ensure that 'Register with Azure Active Directory' is enabled on App Service

CID 50051: Ensure web app is using the latest version of TLS encryption version

CID 50061: Ensure that 'HTTP Version' is latest, if used to run the web app

CID 50136: Ensure FTP deployments are disabled for web apps.

Key Vault

CID 50026: Ensure keyvault is recoverable

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

CID 50054: Ensure that logging for Azure KeyVault is 'Enabled'

CID 50075: Ensure that diagnostic settings for Azure KeyVault is set to ON

Kubernetes

CID 50046: Enable RBAC within Azure Kubernetes Services

Note: This control is not applicable for GovCloud

Azure Active Directory

CID 50072: Ensure that there are no guest users

Note: This control is not applicable for GovCloud

CID 50073: Ensure no custom subscription owner roles are created

Disks

CID 50137: Ensure that 'OS and Data' disks are encrypted with CMK

Network Security Group

CID 50138: Ensure that UDP services are restricted from the Internet

Azure Best Practices Policy

We support Azure Best Practices Policy to evaluate the following controls.

Virtual Machines

CID 50034: Ensure disks are encrypted for Windows VMs with ADE version 1.1

Snapshot

CID 50038: Ensure disk snapshots are encrypted.

Security Center

CID 50077: Ensure that Settings - Threat Detection for Microsoft Cloud App Security (MCAS) is selected

CID 50078: Ensure that Settings - Threat Detection for Windows Defender ATP (WDATP) is selected

CID 50082: Ensure any of the ASC Default policy setting is not set to 'Disabled'

PostgreSQL Servers

CID 50044: Ensure server parameter log_duration" is set to "ON" for PostgreSQL Database Server"

SQL Servers

CID 50083: Ensure that ADS - Vulnerability Assessment (VA) is enabled and configured properly

Kubernetes

CID 50090: Ensure that Azure AKS cluster monitoring is enabled

CID 50091: Ensure that Azure AKS cluster HTTP application routing is disabled

CID 50092: Ensure that Azure AKS cluster Azure CNI networking is enabled

Application Gateway

CID 50093: Ensure that Azure Application Gateway have Web application firewall (WAF) enabled

CID 50094: Ensure that Azure Application Gateway allows TLSv1.2 or above

Container Registries

CID 50057: Ensure that Azure Container Registry using the deprecated classic registry

Monitor

CID 50059: Ensure Activity Log Alert for Delete SQL server firewall rule

CID 50125: Ensure Activity Log Alert exists for Create/Update Storage Account

CID 50126: Ensure Activity Log Alert exists for Delete Storage Account

CID 50127: Ensure Activity Log Alert exists for Create or Update Virtual Machine

CID 50128: Ensure Activity Log Alert exists for Deallocate Virtual Machine

CID 50129: Ensure Activity Log Alert exists for Delete Virtual Machine

Virtual Network Subnet

CID 50060: Ensure that Azure Virtual Network subnet is configured with a Network Security Group

Resource Group

CID 50036: Ensure that Azure Resource Group have a resource lock

Security Centre

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

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

CID 50006: Ensure that Vulnerabilities in security configuration on your machines should be remediated is set to On

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

CID 50015: Ensure that standard pricing tier is selected

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

CID 50017: Ensure that Vulnerabilities should be remediated by a Vulnerability Assessment solution

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

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

CID 50071: Ensure that Activity Log Alert exists for Update Security Policy

Logging and Monitoring

CID 50024: Ensure that LogProfile for a subscription is configured properly

Azure Function App Best Practices Policy

We support Azure Function App Best Practices Policy to help you in automated auditing and reporting on the Azure Function app misconfigurations, unwarranted access, and non-standard deployments, and provide remediation steps to manage risks.

Function App

CID 50084: Ensure App Service Authentication is set on Function Apps

CID 50085: Ensure Function app redirects all HTTP traffic to HTTPS

CID 50086: Ensure function app has 'Client Certificates (Incoming client certificates)' set to 'On'

CID 50087: Ensure that 'Register with Azure Active Directory' is enabled on Function app

CID 50088: Ensure function app is using the latest version of TLS encryption version

CID 50089: Ensure that 'HTTP Version' is latest, if used to run the function app

Azure Database Service Best Practices Policy

We have a policy that helps in automated auditing and reporting on the Azure Database service resources misconfigurations, unwarranted access and non-standard deployments, and provides remediation steps to manage risks. To help secure your Azure resources, follow the recommendations for the Database services of Azure.

SQL Server Database

SQL Servers

MySQL Server

MaridDB Server

PostgreSQL Server

CosmosDB

SQL Server Database

CID 50095: Ensure that default Auditing policy for a SQL Database is configured to capture and retain the activity logs

CID 50096: Ensure that Advanced Data Security is enabled and Advanced Threat Protection settings is configured properly for a SQL Database

SQL Servers

CID 50098: Ensure that 'ssl_minimal_tls_version_enforced' is set to '1.2' for SQL server

MySQL Server

CID 50102: Ensure that Advanced Threat Protection settings is configured properly for Azure Database for MySQL Server

CID 50103: Ensure that TLS is enforced and the minimum version be set to 1.2 for Azure Database for MYSQL server

CID 50104: Ensure no MySQL Server allow ingress from Internet (ANY IP)

CID 50105: Ensure that 'geo_redundant_backup_enabled' is set to Enabled for Azure Database for MySQL server

CID 50106: Ensure that Public Network Access is Disabled for Azure Database for MySQL server

CID 50107: Ensure that Azure Database for MySQL server diagnostic setting is configured properly

CID 50131: Ensure that Azure Active Directory authentication is configured for MySql server

MaridDB Server

CID 50108: Ensure that Advanced Threat Protection settings is configured properly for Azure Database for MariaDB Server

CID 50109: Ensure 'Enforce SSL connection' is set to 'ENABLED' for Azure Database for MariaDB server

CID 50110: Ensure that TLS is enforced and the minimum version be set to 1.2 for Azure Database for MariaDB server

CID 50111: Ensure no MariaDB Server allow ingress from Internet (ANY IP)

CID 50112: Ensure that 'geo_redundant_backup_enabled' is set to Enabled for Azure Database for MariaDB server

CID 50113: Ensure that Public Network Access is Disabled for Azure Database for MariaDB server

PostgreSQL Server

CID 50115: Ensure that Advanced Threat Protection settings is configured properly for Azure Database for PostgreSQL Server

CID 50116: Ensure that TLS is enforced and the minimum version be set to 1.2 for Azure Database for PostgreSQL server

CID 50118: Ensure that 'geo_redundant_backup_enabled' is set to Enabled for Azure Database for PostgreSQL server

CID 50119: Ensure that Public Network Access is Disabled for Azure Database for PostgreSQL server

CID 50120: Ensure that Azure Database for PostgreSQL server diagnostic setting is configured properly

CID 50132: Ensure that Azure Active Directory authentication is configured for PostgreSql server

CosmosDB

CID 50121: Ensure that automatic-failover is set for Azure CosmosDB

CID 50122: Ensure that Diagnostic settings are set for CosmosDB

CID 50123: Ensure that lock is set on Azure CosmosDB

CID 50124: Ensure that CosmosDB does not allow access from all networks

GCP Policies

Let us view all the policies and associated controls for GCP.

CIS Google Cloud Platform Foundation Benchmark

We support controls for following Google Cloud Platform (GCP) resources:

IAM & Admin

Logs Router

Logs-based metrics

Storage

Network

Firewall rules

Subnetwork

Cloud SQL- Mysql

Cloud SQL- SQL Server

Cloud SQL- PostgreSQL

Cloud Functions

VM Instances

Dataset

Table

Cloud DNS

IAM & Admin

CID 52000: Ensure that corporate login credentials are used instead of Gmail accounts

CID 52001: Ensure that there are only GCP-managed service account keys for each service account

CID 52002: Ensure that ServiceAccount has no Admin privileges

CID 52003: Ensure that IAM users are not assigned Service Account User role at project level

CID 52004: Ensure user-managed/external keys for service accounts are rotated every 90 days or less

CID 52005: Ensure Encryption keys are rotated within a period of 365 days

CID 52006: Ensure that Separation of duties is enforced while assigning KMS related roles

CID 52007: Ensure that IAM users are not assigned Service Account Token Creator role at project level

CID 52008: Ensure that Cloud Audit Logging is configured properly across all services and all users from a project

CID 52090: Ensure that Cloud KMS cryptokeys are not anonymously or publicly accessible

Logs Router

CID 52009: Ensure that sinks are configured for all Log entries

Logs-based metrics

CID 52011: Ensure log metric filter and alerts exists for Project Ownership assignments/changes

CID 52012: Ensure log metric filter and alerts exists for Audit Configuration Changes

CID 52013: Ensure log metric filter and alerts exists for Custom Role changes

CID 52014: Ensure log metric filter and alerts exists for VPC Network Firewall rule changes

CID 52015: Ensure log metric filter and alerts exists for VPC network route changes

CID 52016: Ensure log metric filter and alerts exists for VPC network changes

CID 52017: Ensure log metric filter and alerts exists for Cloud Storage IAM permission changes

CID 52018: Ensure log metric filter and alerts exists for SQL instance configuration changes

Storage

CID 52030: Ensure that Cloud Storage bucket is not anonymously or publicly accessible

CID 52036: Ensure that Cloud Storage buckets have uniform bucket-level access enabled

CID 52057: Ensure that there are no harmful object life cycle rules are created on Storage Buckets

CID 52058: Ensure that object retention policy is set on storage buckets

CID 52099: Ensure that retention policies on log buckets are configured using Bucket Lock

Network

CID 52019: Ensure the default network does not exist in a project

CID 52034: Ensure legacy networks do not exist for a project

Firewall rules

CID 52021: Ensure that SSH access is restricted from the internet

CID 52022: Ensure that RDP access is restricted from the internet

Subnetwork

CID 52024: Ensure VPC Flow logs is enabled for every subnet in VPC Network

Cloud SQL- Mysql

CID 52032: Ensure that Cloud SQL - Mysql database Instance requires all incoming connections to use SSL

CID 52033: Ensure that Cloud SQL - Mysql database Instances are not open to the world

CID 52075: Ensure 'skip_show_database' database flag for Cloud SQL - Mysql instance is set to 'on'

CID 52076: Ensure 'local_infile' database flag for Cloud SQL - Mysql instance is set to 'off'

CID 52084: Ensure Cloud SQL - MySql Instance do not have public IP addresses

CID 52087: Ensure Cloud SQL- MySql instance is configured with automated backups

Cloud SQL- SQL Server

CID 52035: Ensure that MySQL Database Instance does not allows root login from any Host

CID 52067: Ensure that Cloud SQL - SQL Server database instance requires all incoming connections to use SSL

CID 52068: Ensure that Cloud SQL - SQL Server database Instances are not open to the world

CID 52077: Ensure 'external scripts enabled' database flag for Cloud SQL - SQL Server instance is set to 'off'

CID 52078: Ensure 'cross db ownership chaining' database flag for Cloud SQL - SQL Server instance is set to 'off'

CID 52081: Ensure 'remote access' database flag for Cloud SQL - SQL Server instance is set to 'off'

CID 52082: Ensure '3625 (trace flag)' database flag for Cloud SQL - SQL Server instance is set to 'off'

CID 52083: Ensure 'contained database authentication' database flag for Cloud SQL SQL Server instance is set to 'off'

CID 52085: Ensure Cloud SQL - SQL server Instance do not have public IP addresses

CID 52088: Ensure Cloud SQL- SQL server is configured with automated backups

CID 52080: Ensure 'user options' database flag for Cloud SQL - SQL Server instance is not configured

Cloud SQL- PostgreSQL

CID 52059: Ensure 'log_connections' database flag for Cloud SQL - PostgreSQL instance is set to 'on'

CID 52060: Ensure 'log_disconnections' database flag for Cloud SQL - PostgreSQL instance is set to 'on'

CID 52061: Ensure 'log_duration' database flag for Cloud SQL PostgreSQL instance is set to 'on'

CID 52062: Ensure 'log_error_verbosity' database flag for Cloud SQL - PostgreSQL instance is set to 'DEFAULT' or stricter

CID 52063: Ensure log_statement" database flag for Cloud SQL - PostgreSQL instance is set to "ddl" or stricter"

CID 52064: Ensure 'log_hostname' database flag for Cloud SQL - PostgreSQL instance is set to 'off'

CID 52065: Ensure that Cloud SQL - PostgreSQL database instance requires all incoming connections to use SSL

CID 52066: Ensure that Cloud SQL - PostgreSQL database Instances are not open to the world

CID 52069: Ensure 'log_lock_waits' database flag for Cloud SQL - PostgreSQL instance is set to 'on'

CID 52070: Ensure 'log_temp_files' database flag for Cloud SQL - PostgreSQL instance is set to '0' (on)

CID 52071: Ensure 'log_min_error_statement' database flag for Cloud SQL - PostgreSQL instance is set to 'Error' or stricter

CID 52072: Ensure 'log_min_messages' database flag for Cloud SQL - PostgreSQL instance is set to 'Error' or stricter

CID 52073: Ensure 'log_min_duration_statement' database flag for Cloud SQL - PostgreSQL instance is set to '-1'

(disabled)

CID 52074: Ensure 'log_checkpoints' database flag for Cloud SQL - PostgreSQL instance is set to 'on'

CID 52086: Ensure Cloud SQL - PostgreSQL Instance do not have public IP addresses

CID 52089: Ensure Cloud SQL - PostgreSQL instance is configured with automated backups

CID 52112: Ensure log_parser_stats database flag for Cloud SQL PostgreSQL instance is set to off

CID 52113: Ensure log_planner_stats database flag for Cloud SQL PostgreSQL instance is set to off

CID 52114: Ensure log_executor_stats database flag for Cloud SQL PostgreSQL instance is set to off

CID 52115: Ensure 'log_statement_stats' database flag for Cloud SQL PostgreSQL instance is set to off

Cloud Functions

CID 52054: Ensure that Default service account is not used for the cloud function

CID 52055: Ensure that Runtime used in cloud function is not deprecated

CID 52056: Ensure that Cloud function is not anonymously or publicly accessible

VM Instances

CID 52020: Ensure that IP forwarding is not enabled on Instances

CID 52025: Ensure that instances are not configured to use the default service account with full access to all Cloud APIs

CID 52026: Ensure Block Project-wide SSH keys "enabled for VM instances"

CID 52027: Ensure oslogin is enabled for a Project

CID 52028: Ensure Enable connecting to serial ports "is not enabled for VM Instance"

CID 52029: Ensure VM disks for critical VMs are encrypted with Customer-Supplied Encryption Keys (CSEK)

CID 52091: Ensure Compute instances are launched with Shielded VM enabled

CID 52093: Ensure that instances are not configured to use default service account

CID 52094: Ensure that Compute instances do not have public IP addresses

CID 52111: Ensure that Compute instances have Confidential Computing enabled

Dataset

CID 52095: Ensure that BigQuery Dateset is encrypted with Customer-managed key

CID 52098: Ensure that BigQuery datasets are not anonymously or publicly accessible

Table

CID 52096: Ensure that BigQuery Table is encrypted with Customer-managed key

Cloud DNS

CID 52100: Ensure that DNSSEC is enabled for Cloud DNS

CID 52109: Ensure that GCP Cloud DNS zones is using RSASHA1 algorithm for DNSSEC key-signing

CID 52110” Ensure that GCP Cloud DNS zones is using RSASHA1 algorithm for DNSSEC zone-signing

GCP Best Practices Policy

We support GCP Best Practices Policy to evaluate the following controls.

Storage

VM Instance

Subnetwork

Storage

CID 52010: Ensure that object versioning is enabled on buckets

CID 52031: Ensure that logging is enabled for Cloud storage buckets

CID 52057: Ensure that there are no harmful object life cycle rules are created on Storage Buckets

CID 52058: Ensure that object retention policy is set on buckets

CID 52108: Ensure that GCP Storage bucket is encrypted using customer-managed key

VM Instance

CID 52092: Ensure oslogin is enabled for VM instance

Subnetwork

CID 52023: Ensure Private Google Access is enabled for all subnetwork in VPC Network

GCP Cloud Functions Best Practices Policy

We have GCP Cloud Functions Best Practices Policy that covers Cloud Functions Services of Google Cloud Platform. The controls in this policy are targeted only for Cloud Functions service.

Function App

CID 52054: Ensure that Default service account is not used for the Cloud Function

CID 52055: Ensure that Runtime used in Cloud Function is not deprecated

CID 52056: Ensure that Cloud Function is not anonymously or publicly accessible

GCP Kubernetes Engine Best Practices Policy

We have GCP Kubernetes Engine Best Practices Policy. It covers Google Kubernetes Engine Service of Google Cloud Platform. The controls in this policy are targeted only towards Google Kubernetes Engine service. The pre-defined GCP Kubernetes Engine Best Practices is loaded with the 22 system-defined controls.

CID 52037: Ensure that GCP Kubernetes cluster intra-node visibility is enabled

CID 52038: Ensure Legacy Authorization is set to Disabled on Kubernetes Engine Clusters

CID 52039: Ensure Kubernetes web UI / Dashboard is disabled

CID 52040: Ensure Automatic node repair is enabled for Kubernetes Clusters

CID 52041: Ensure Automatic node upgrades is enabled on Kubernetes Engine Clusters nodes

CID 52042: Ensure that GCP Kubernetes Engine Clusters have HTTP load balancing enabled

CID 52043: Ensure Network policy is enabled on Kubernetes Engine Clusters

CID 52044: Ensure that GCP Kubernetes Engine Clusters have Alpha cluster feature disabled

CID 52045: Ensure Kubernetes Cluster is created with Alias IP ranges enabled

CID 52046: Ensure PodSecurityPolicy controller is enabled on the Kubernetes Engine Clusters

CID 52047: Ensure Kubernetes Cluster is created with Private cluster enabled

CID 52048: Ensure Private Google Access is set on Kubernetes Engine Cluster Subnets

CID 52049: Ensure default Service account is not used for Project access in Kubernetes Clusters

CID 52050: Ensure Kubernetes Clusters created with limited service account Access scopes for Project access

CID 52051: Ensure Stackdriver Kubernetes Engine Monitoring is set to Enabled on Kubernetes Engine Clusters

CID 52052: Ensure that Application-Layer secret encryption is enabled for Kubernetes cluster

CID 52053: Ensure that Master authorized network is enabled for Kubernetes cluster

CID 52101: Ensure Binary Authorization is set to Enabled on Kubernetes Engine Clusters

CID 52102: Ensure Container-Optimized OS (cos) is used for Kubernetes Engine Clusters Node image

CID 52103: Ensure GCP Kubernetes Engine Clusters are not using the default network

CID 52104: Ensure that network traffic egress metering is enabled on Kubernetes Engine Clusters

CID 52105: Ensure that legacy compute engine metadata endpoint for GCP Kubernetes Engine Cluster Node is disabled

GCP Cloud SQL Best Practices Policy

We have GCP Cloud SQL Best Practices Policy that covers Cloud SQL Service of Google Cloud Platform. The controls in this policy are targeted only towards Cloud SQL service.

Cloud SQL- PostgreSQL

Cloud SQL- Mysql

Cloud SQL - SQL Server

Cloud SQL- PostgreSQL

CID 52107: Ensure that Cloud SQL - PostgreSQL database instance Point-in-time recovery is enabled

Cloud SQL- Mysql

CID 52106: Ensure that Cloud SQL Mysql database instance Binary logs configuration is enabled

Cloud SQL - SQL Server

CID 52097: Ensure 'default trace enabled' database flag for Cloud SQL - SQL Server instance is set to 'on'