# CloudView

User Guide

October 12, 2022

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-the-box AWS, Azure, GCP policies
- Continuously assess and report resource misconfigurations by checking against the controls from out-of-the-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.<br>Here are some examples:<br>- MFA should be enabled for console user - applies to AWS IAM Service and IAM User Resource<br>- Password policy should have upper case letter enforced - applies to AWS IAM Service<br>- 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. The connectors are created on the Connectors application. You can merge your existing CloudView connectors or create a new one on the app.

### 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 Permissions for Fargate Profile.

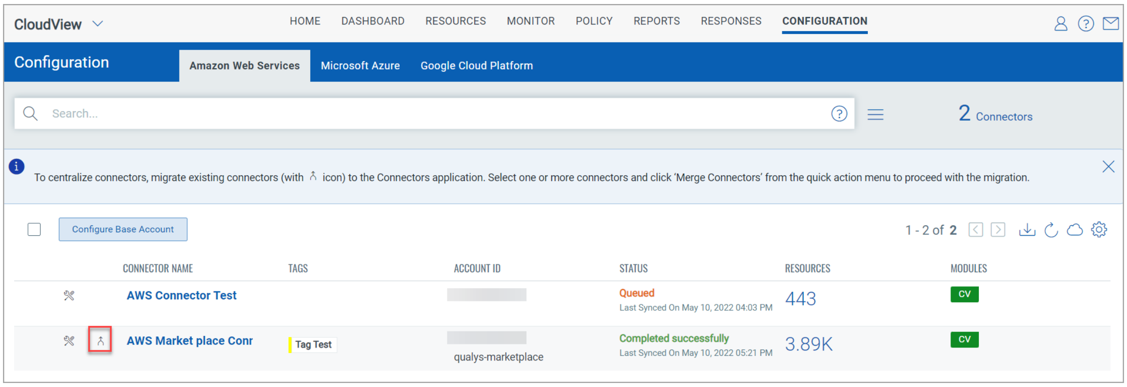
## Create a New Connector

New AWS connectors can only be created from the Connectors application. You can refer to the instructions mentioned in the Connectors Online help.

Merge Existing Connector

The changes to the CloudView connector configuration would not be allowed until you merge the CloudView connectors to Connectors application. You are requested to merge CloudView connectors to the Connectors application via the merge feature. After merging the connectors from CloudView, you can then update the connectors in the new Connectors application.

You can identify the connectors to be merged by looking for this icon. Show me.



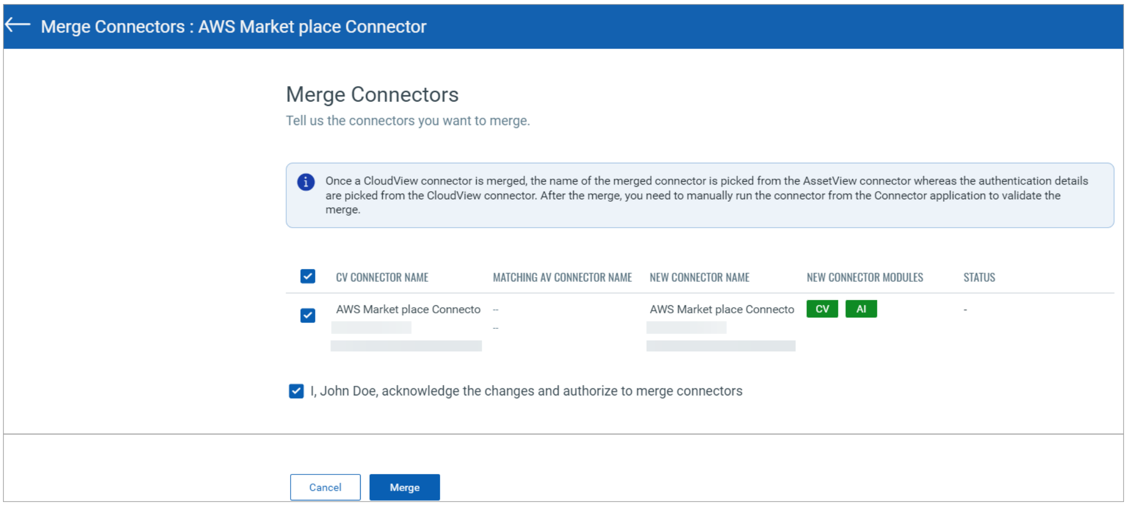
To centralize connectors, migrate existing connectors (with icon) to the Connectors application. Select one or more connectors and click 'Merge Connectors' from the quick action menu to proceed with the migration.

| CONNECTOR NAME | TAGS | ACCOUNT ID | STATUS | RESOURCES | MODULES |
|---|---|---|---|---|---|
| AWS Connector Test | | [redacted] | Queued<br>Last Synced On May 10, 2022 04:03 PM | 443 | CV |
| AWS Market place Conr | Tag Test | [redacted]<br>qualys-marketplace | Completed successfully<br>Last Synced On May 10, 2022 05:21 PM | 3.89K | CV |

1) Click on the connector to merge.

2) From the quick actions menu, click on Merge Connectors.

3) Select the connectors to merge. Show me.



Merge Connectors

Tell us the connectors you want to merge.

Once a CloudView connector is merged, the name of the merged connector is picked from the AssetView connector whereas the authentication details are picked from the CloudView connector. After the merge, you need to manually run the connector from the Connector application to validate the merge.

| ☑ | CV CONNECTOR NAME | MATCHING AV CONNECTOR NAME | NEW CONNECTOR NAME | NEW CONNECTOR MODULES | STATUS |
|---|---|---|---|---|---|
| ☑ | AWS Market place Connecto | -- | AWS Market place Connecto | CV AI | - |

☑ I, John Doe, acknowledge the changes and authorize to merge connectors

4) Authorize the merge and click on Merge.

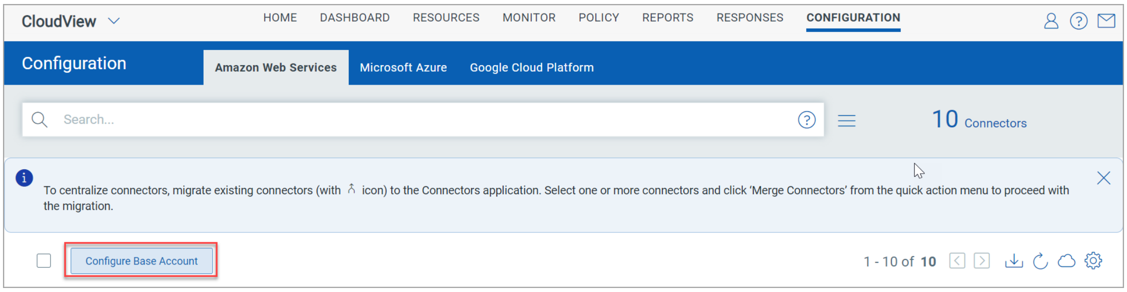
Once the merge is complete, the connectors are visible in the the AWS tab without the icon. The connector will continue to establish connection with AWS to start discovering resources from each region and evaluate them against policies.

Merge Base Account

If both CloudView and AssetView use different base accounts, you would be required to merge the base accounts to the one of your choice and then going further all the existing connectors of AssetView and CloudView, and the new connectors will take the merged base account in use.

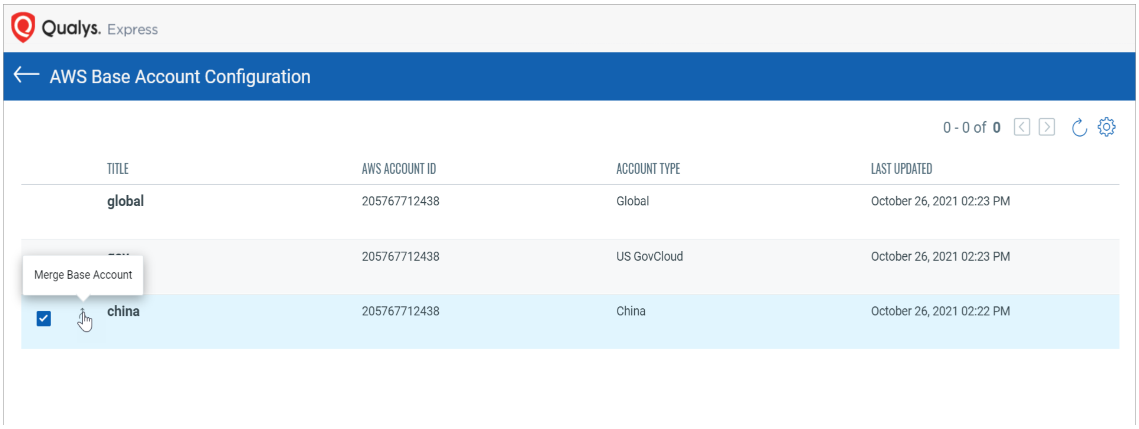
Navigate to Amazon Web Services from Configuration tab

1) Click 'Configure Base Account'. Show me.



To centralize connectors, migrate existing connectors (with icon) to the Connectors application. Select one or more connectors and click 'Merge Connectors' from the quick action menu to proceed with the migration.

2) Select the existing base account with the merge icon. Show me.



AWS Base Account Configuration

0 - 0 of 0

|  | TITLE | AWS ACCOUNT ID | ACCOUNT TYPE | LAST UPDATED |
|---|---|---|---|---|
|  | global | 205767712438 | Global | October 26, 2021 02:23 PM |
|  | gov | 205767712438 | US GovCloud | October 26, 2021 02:23 PM |
| ☑ | china | 205767712438 | China | October 26, 2021 02:22 PM |

3) Select the base account you want to merge the account with (CloudView/AssetView). Show me.

4) Authorize the merge and click on "Merge Base Account".

## 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.

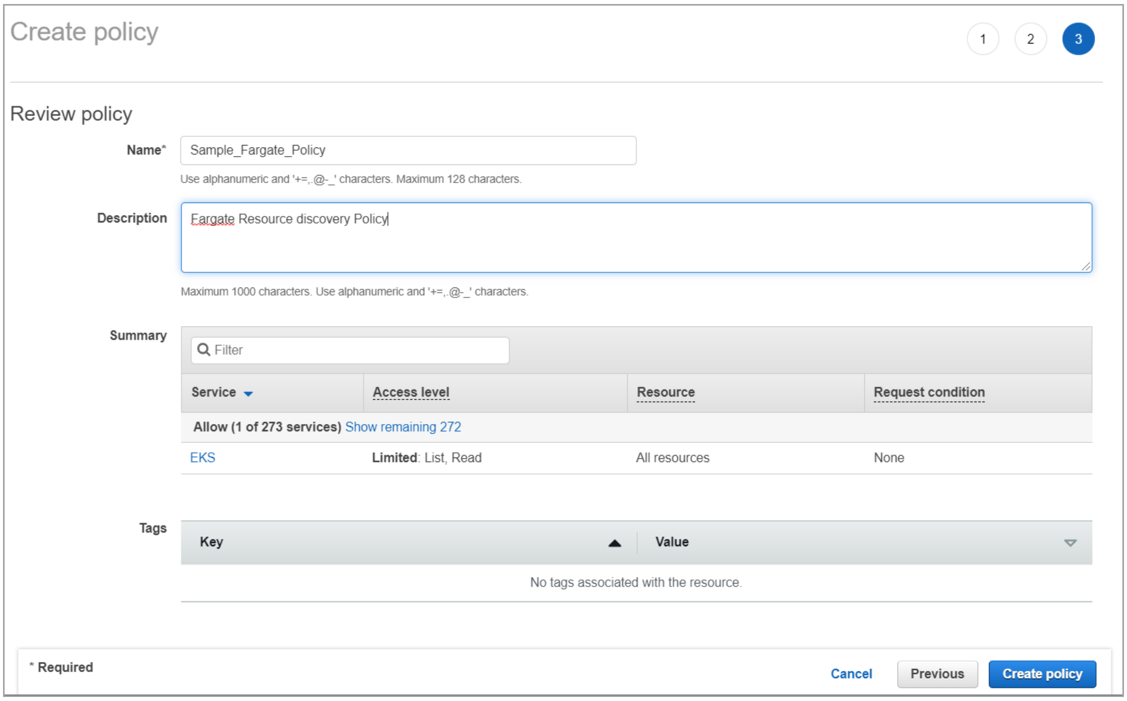
4 - Choose the JSON tab. Paste the following text into the JSON text box.

```
{
    "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.



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.

## Create Custom Policy

You need additional permissions to evaluate controls related to the following resources:

-Elastic File System (EFS)

- Step Functions
- Amazon Quantum Ledger Database (QLDB)
- Managed Streaming for Apache Kafka (MSK)
- API Gateway
- AWS Backup
- WAF
- Directory Service
- Lambda
- Elastic Block Storage (EBS)
- Elastic Map Reduce (EMR)
- Glue
- GuardDuty

Note: This additional permissions are not required for Cloud Inventory users.

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 Custom 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": "QualysCustomPolicyPermissions",
      "Effect": "Allow",
      "Action": [
        "states:DescribeStateMachine",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "kafka:ListClusters",
        "codebuild:BatchGetProjects",
        "wafv2:GetWebACLForResource",
        "backup:ListBackupVaults",
        "backup:DescribeBackupVault",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "guardduty:ListDetectors",
        "guardduty:GetDetector",
        "glue:GetDataCatalogEncryptionSettings",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "lambda:GetFunctionConcurrency"
      ],
      "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_Custom_Policy.

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_Custom_Policy) and click Attach Policy.

## 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 Azure connectors for gathering resource information from your Azure account. The connectors are created on the Connectors application. You can merge your existing CloudView connectors or create a new one on the app.

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.

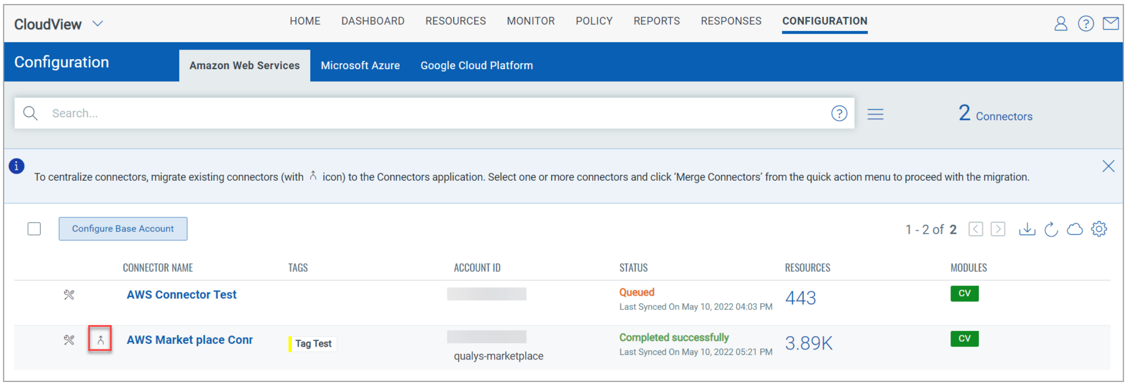
## Create a new Azure Connector

New Azure connectors can only be created from the Connectors application. You can refer to the instructions mentioned in the Connectors Online Help.

## Merge Existing Connector

The changes to the CloudView connector configuration would not be allowed until you merge the CloudView connectors to Connectors application. You are requested to merge CloudView connectors to the Connectors application via the merge feature. After merging the connectors from CloudView, you can then update the connectors in the new Connectors application.

You can identify the connectors to be merged by looking for this icon.



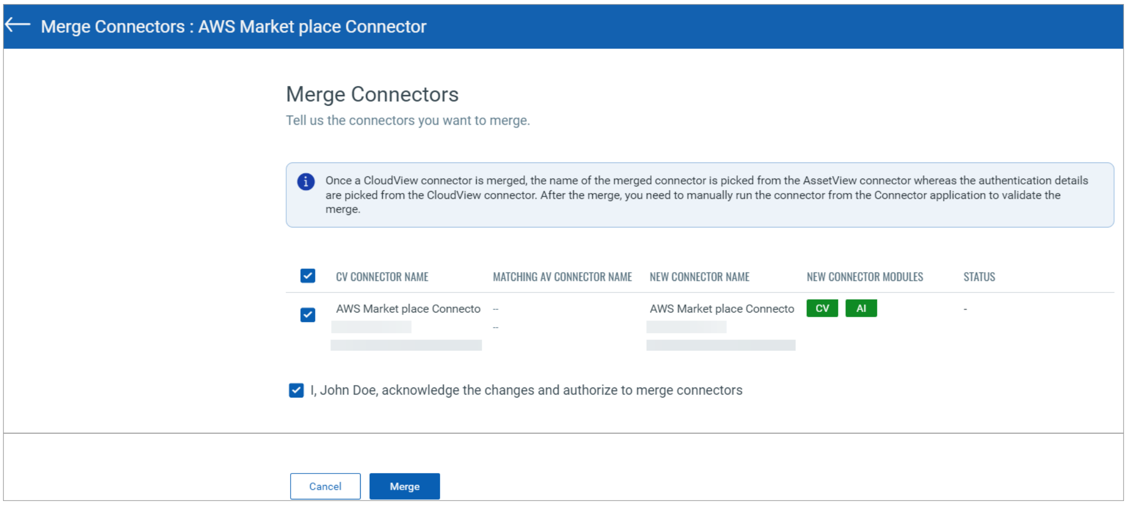
To centralize connectors, migrate existing connectors (with icon) to the Connectors application. Select one or more connectors and click 'Merge Connectors' from the quick action menu to proceed with the migration.

| CONNECTOR NAME | TAGS | ACCOUNT ID | STATUS | RESOURCES | MODULES |
|---|---|---|---|---|---|
| AWS Connector Test | | [redacted] | Queued<br>Last Synced On May 10, 2022 04:03 PM | 443 | CV |
| AWS Market place Conr | Tag Test | [redacted]<br>qualys-marketplace | Completed successfully<br>Last Synced On May 10, 2022 05:21 PM | 3.89K | CV |

1) Click on the connector to merge.

2) From the quick actions menu, click on Merge Connectors.

3) Select the connectors to merge.



Merge Connectors

Tell us the connectors you want to merge.

Once a CloudView connector is merged, the name of the merged connector is picked from the AssetView connector whereas the authentication details are picked from the CloudView connector. After the merge, you need to manually run the connector from the Connector application to validate the merge.

| ☑ | CV CONNECTOR NAME | MATCHING AV CONNECTOR NAME | NEW CONNECTOR NAME | NEW CONNECTOR MODULES | STATUS |
|---|---|---|---|---|---|
| ☑ | AWS Market place Connecto | -- | AWS Market place Connecto | CV AI | - |

☑ I, John Doe, acknowledge the changes and authorize to merge connectors

4) Authorize the merge and click on Merge.

Once the merge is complete, the connectors are visible in the the Azure tab without the icon. The connector will continue to establish connection with AWS to start discovering resources from each region and evaluate them against policies.

## 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

## 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 GCP connectors for gathering resource information from your GCP account. The connectors are created on the Connectors application. You can merge your existing CloudView connectors or create a new one on the app.

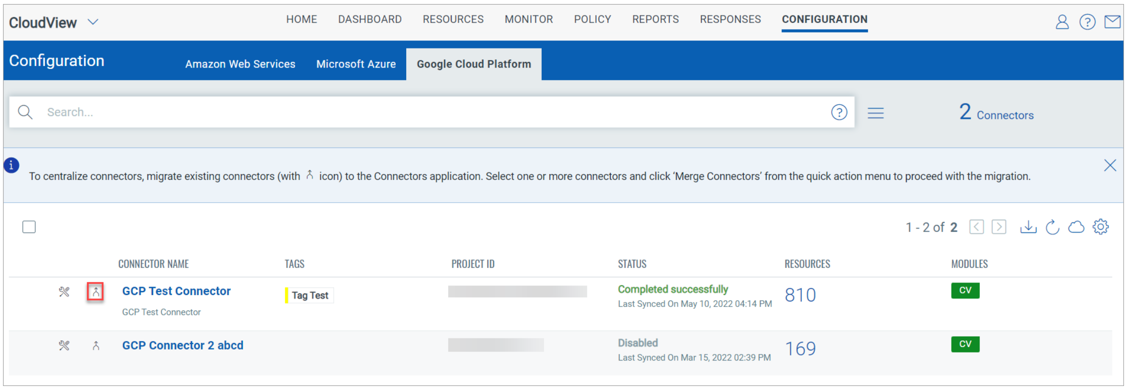
## Create a New Connector

New GCP connectors can only be created from the Connectors application. You can refer to the instructions mentioned in Connectors Online Help.

## Merge Existing Connector

The changes to the CloudView connector configuration would not be allowed until you merge the CloudView connectors to Connectors application. You are requested to merge CloudView connectors to the Connectors application via the merge feature. After merging the connectors from CloudView, you can then update the connectors in the new Connectors application.

You can identify the connectors to be merged by looking for this ⋏ icon.



To centralize connectors, migrate existing connectors (with ⋏ icon) to the Connectors application. Select one or more connectors and click 'Merge Connectors' from the quick action menu to proceed with the migration.

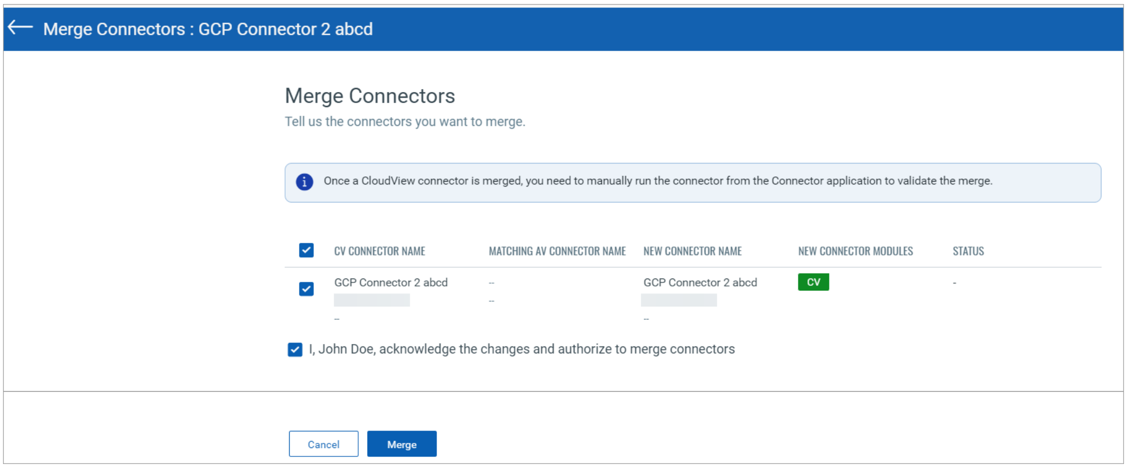
1 - 2 of 2

| CONNECTOR NAME | TAGS | PROJECT ID | STATUS | RESOURCES | MODULES |
|---|---|---|---|---|---|
| GCP Test Connector<br>GCP Test Connector | Tag Test | [redacted] | Completed successfully<br>Last Synced On May 10, 2022 04:14 PM | 810 | CV |
| GCP Connector 2 abcd | | [redacted] | Disabled<br>Last Synced On Mar 15, 2022 02:39 PM | 169 | CV |

1) Click on the connector to merge.

2) From the quick actions menu, click on Merge Connectors.

3) Select the connectors to merge. Show me.



Merge Connectors : GCP Connector 2 abcd

Merge Connectors

Tell us the connectors you want to merge.

Once a CloudView connector is merged, you need to manually run the connector from the Connector application to validate the merge.

| ☑ | CV CONNECTOR NAME | MATCHING AV CONNECTOR NAME | NEW CONNECTOR NAME | NEW CONNECTOR MODULES | STATUS |
|---|---|---|---|---|---|
| ☑ | GCP Connector 2 abcd<br>--<br>-- | --<br>-- | GCP Connector 2 abcd<br>--<br>-- | CV | - |

☑ I, John Doe, acknowledge the changes and authorize to merge connectors

4) Authorize the merge and click on Merge.

Once the merge is complete, the connectors are visible in the the GCP tab without the icon. The connector will continue to establish connection with AWS to start discovering resources from each region and evaluate them against policies.

## 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.

## 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

# 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 |
| 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

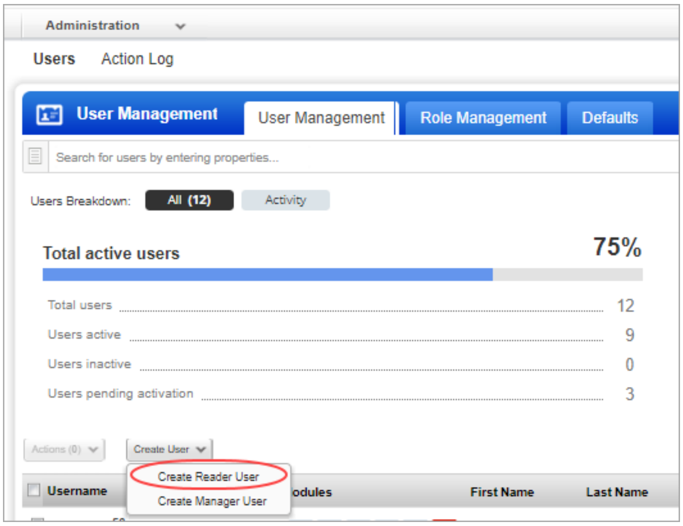
Configure Tag-based Access

## 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 Tags(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.

## Configure Tag-based Access

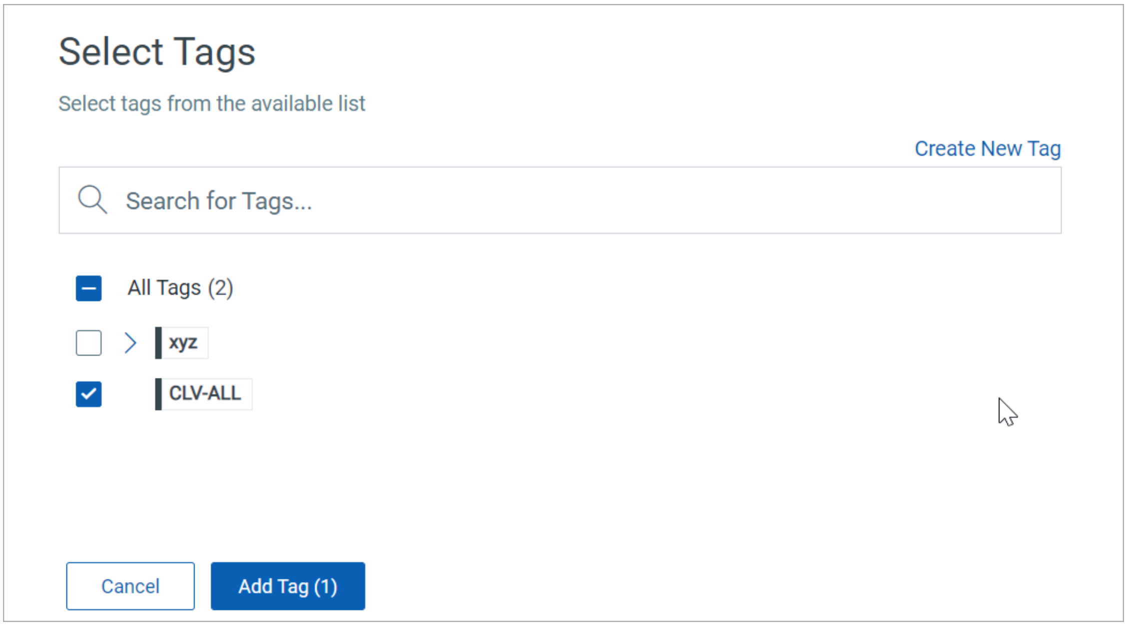
You can control access for connectors with the usage of tags. The tags help you to organize your connectors and to manage user access to them.

## What Happened to Groups?

With the introduction of the Connector app, all the CloudView groups that were assigned to CloudView connectors are migrated to Qualys tags with the prefix 'CLV-'. Connector groups that weren't assigned to any connectors are not migrated.

For example, if you group 'xk21-connector01' will now be available as tag 'CLV-xk21-connector01'

Users with groups assigned to them will now have the respective tags instead. Users without any groups or connector(s) assigned to them will instead have to be assigned 'CLV-ALL' so they can retain their access to connectors.



Select Tags

Select tags from the available list

## Tags

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

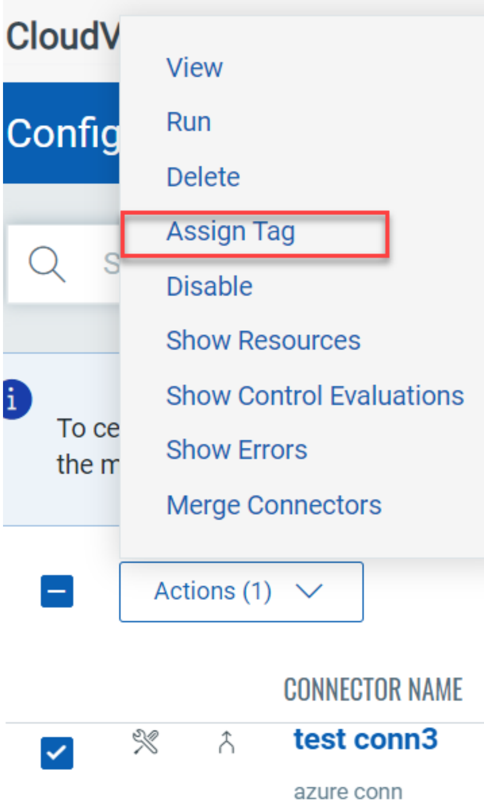
### Assign Tags to Connector

You can only assign tags from the CloudView application if the connector hasn't been merged with the Connector application.

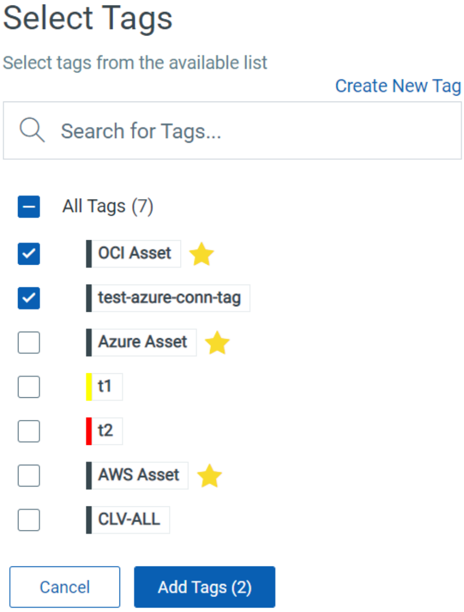
Note: For the connectors that are merged with the connector application, you can assign tags in the connector application. For more information on assigning tags to merged connectors, refer to the Connector online help.

To assign tags to a connector that is not merged, follow the steps below.

1) Select the connector and choose the 'Assign Tag' option from the quick action menu.



2) Select an existing tag and click on Add Tag.


Select Tags

Select tags from the available list

Create New Tag

Search for Tags...

- ☐ All Tags (7)
- ☑ OCI Asset ★
- ☑ test-azure-conn-tag
- ☐ Azure Asset ★
- ☐ t1
- ☐ t2
- ☐ AWS Asset ★
- ☐ CLV-ALL

Cancel | Add Tags (2)

Alternatively, you can create a new tag. For detailed steps on how to create a new tag, refer to Configure Tags.

The selected tags are assigned to the connector.

### Restrict User Access to all Connectors

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

# 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

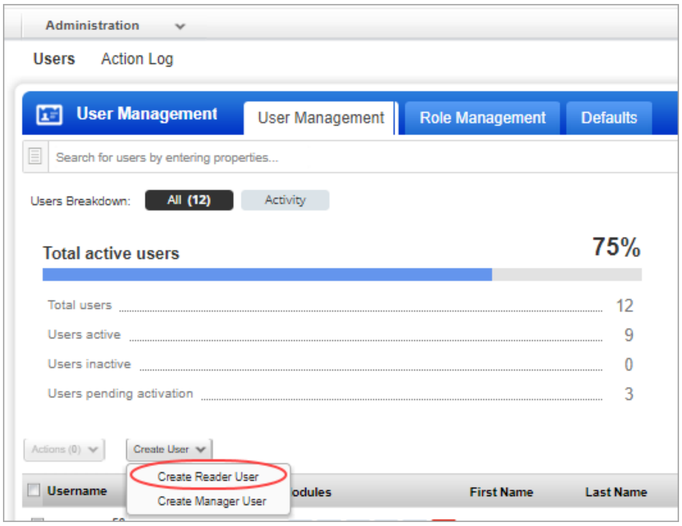
- Create and edit groups (connector tags)

- Create sub users and assign tags

- Access to CloudView reports (inherits Global Reporting permissions)

### Quick Steps

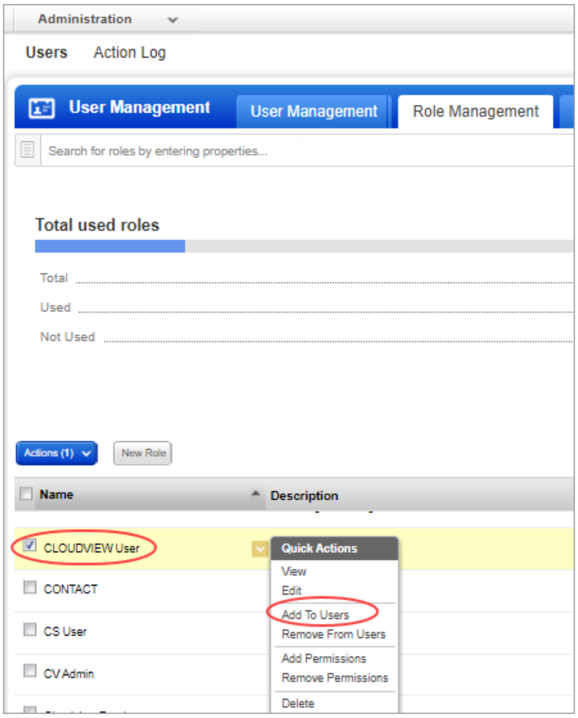
(1) Create a Reader User: Navigate to Administration module > User Management > Create User > Create Reader User.



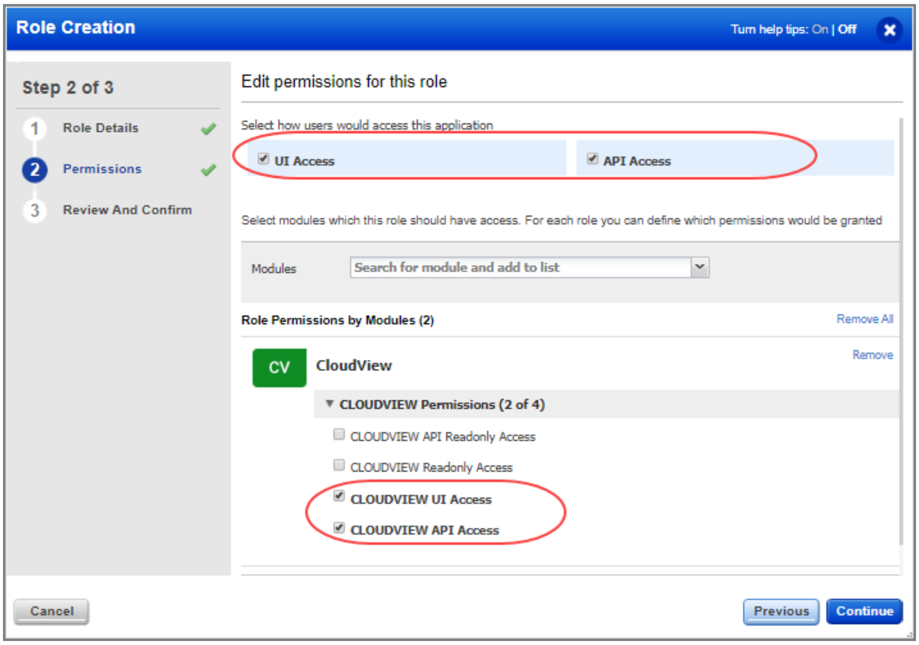
Total active users 75%

| | |
|---|---|
| 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.



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

▼ CLOUDVIEW Permissions (2 of 4)

□ CLOUDVIEW API Readonly Access

□ CLOUDVIEW Readonly Access

☑ CLOUDVIEW UI Access

☑ CLOUDVIEW API Access

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 Assign Global Reporting Permissions from the Reporting permissions to provide access to CloudView Reports. For more information, refer to Reporting Permission.

(4) 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

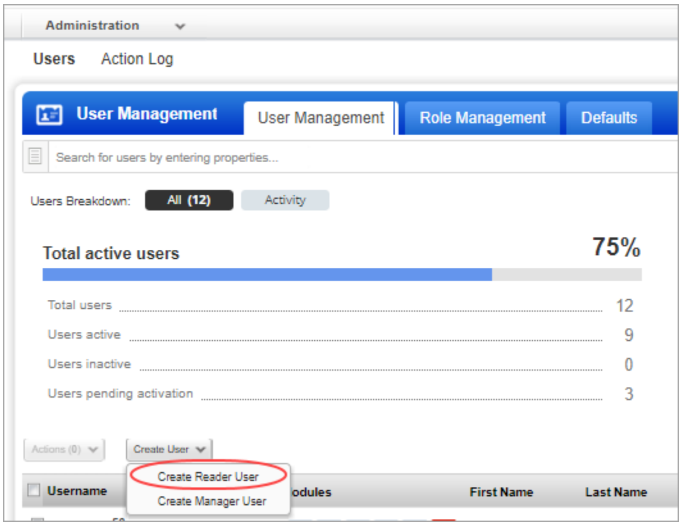
- Create and edit dashboards

- Access to CloudView reports (inherits permissions assigned by the Manager user)

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

## Quick Steps

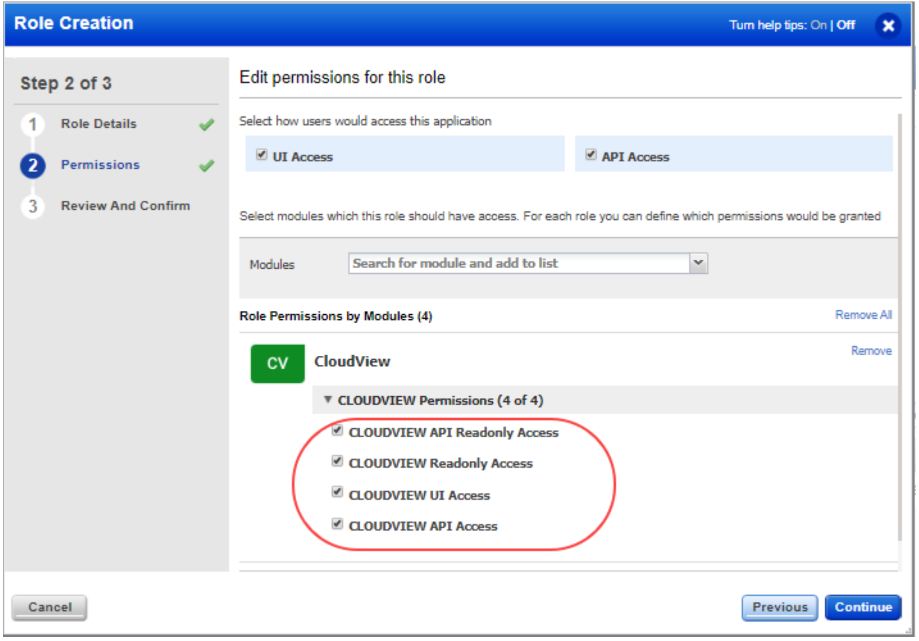
(1) Create a Reader User: Navigate to Administration module > User Management > Create User > Create Reader User.



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.



Role Creation

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)

CV CloudView

▼ CLOUDVIEW Permissions (4 of 4)

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

(3) Select Assign Global Reporting Permissions from the Reporting permissions to provide the Reader access to CloudView Reports. For more information, refer to Reporting Permission.

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

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

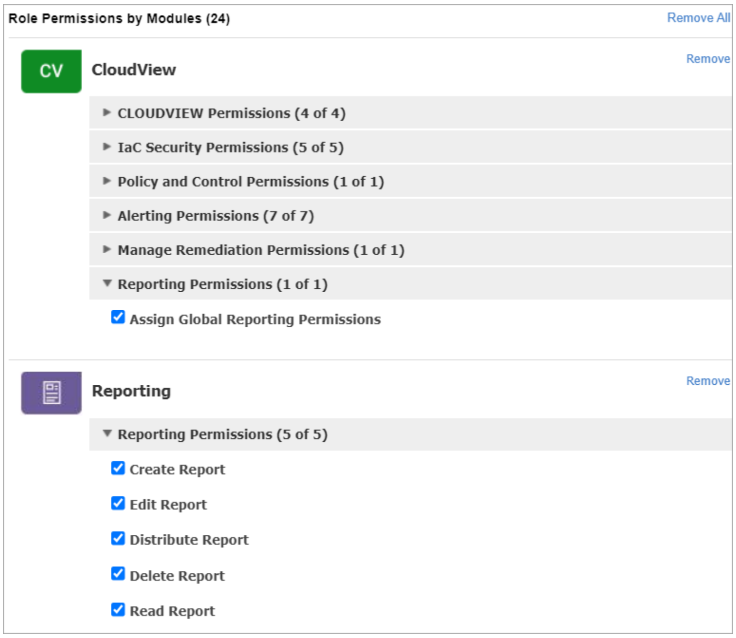
## Reporting Permission

We have added a new permission "Assign Global Reporting Permissions" under "Reporting Permissions" group of CloudView to provide users the permissions to create, read, edit, and delete reports in CloudView. By default, the Manager users have the global reporting permissions and CloudView reporting permissions.

All existing sub-users with the write permissions to CloudView will have the new reporting permissions enabled. All existing sub-users with read-only permissions will have the reporting permissions and that can be granted per need

We also provide a role 'CloudView - only Reports' which has the ‘Assign Global Reporting Permissions’ enabled. You can assign this role to any sub-user to provide access to CloudView reports.

The manager user can choose to enable or disable the reporting access to CloudView reports for sub-users to be able to perform reporting actions from the Administration utility. A sub-user can perform reporting actions when a user with the Manager role assigns the permission to the sub-user from the Administration utility.



Role Permissions by Modules (24)

CloudView

- ▶ CLOUDVIEW Permissions (4 of 4)
- ▶ IaC Security Permissions (5 of 5)
- ▶ Policy and Control Permissions (1 of 1)
- ▶ Alerting Permissions (7 of 7)
- ▶ Manage Remediation Permissions (1 of 1)
- ▼ Reporting Permissions (1 of 1)
  - ☑ Assign Global Reporting Permissions

Reporting

- ▼ Reporting Permissions (5 of 5)
  - ☑ Create Report
  - ☑ Edit Report
  - ☑ Distribute Report
  - ☑ Delete Report
  - ☑ Read Report

# 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.

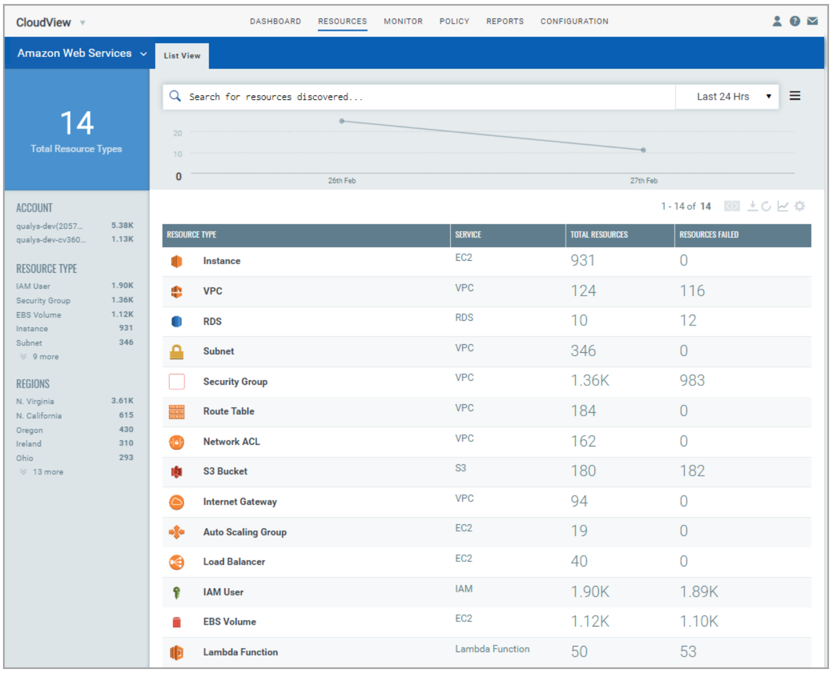
Refer to the Unified Dashboard online help for more details.

## 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.



| 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 |

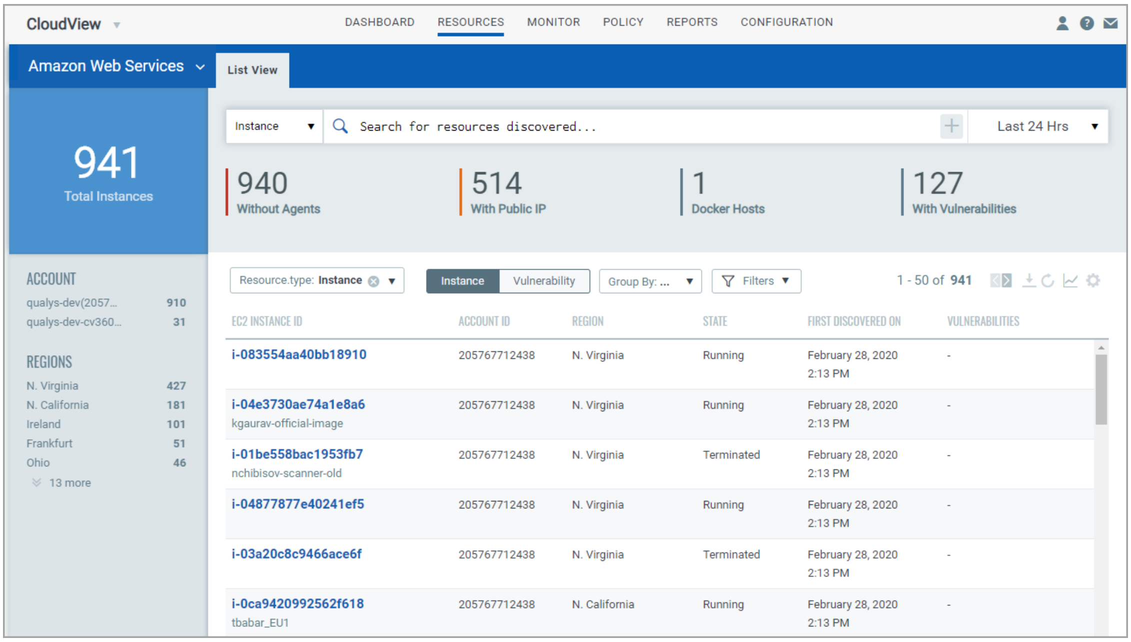
| REGIONS | |
|---|---|
| N. Virginia | 3.61K |
| N. California | 615 |
| Oregon | 430 |
| Ireland | 310 |
| Ohio | 293 |

| 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.



941 Total Instances

940 Without Agents

514 With Public IP

1 Docker Hosts

127 With Vulnerabilities

| 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<br>2:13 PM | - |
| i-04e3730ae74a1e8a6<br>kgaurav-official-image | 205767712438 | N. Virginia | Running | February 28, 2020<br>2:13 PM | - |
| i-01be558bac1953fb7<br>nchibisov-scanner-old | 205767712438 | N. Virginia | Terminated | February 28, 2020<br>2:13 PM | - |
| i-04877877e40241ef5 | 205767712438 | N. Virginia | Running | February 28, 2020<br>2:13 PM | - |
| i-03a20c8c9466ace6f | 205767712438 | N. Virginia | Terminated | February 28, 2020<br>2:13 PM | - |
| i-0ca9420992562f618<br>tbabar_EU1 | 205767712438 | N. California | Running | February 28, 2020<br>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:

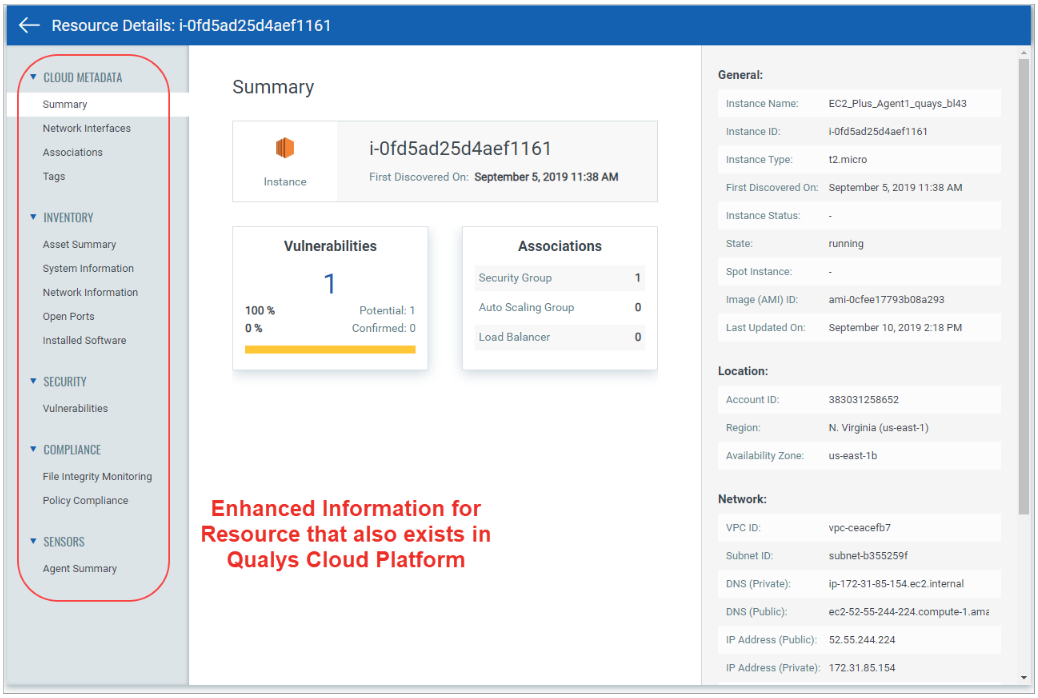
- The details are displayed for only Instance type of resources.

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 |

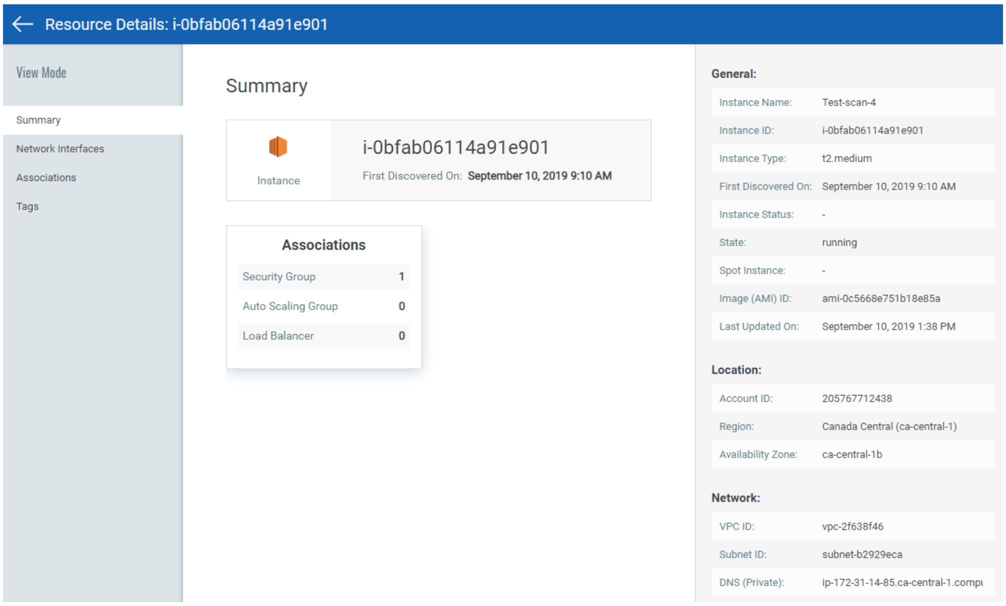
Location:

| | |
|---|---|
| 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 |

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:

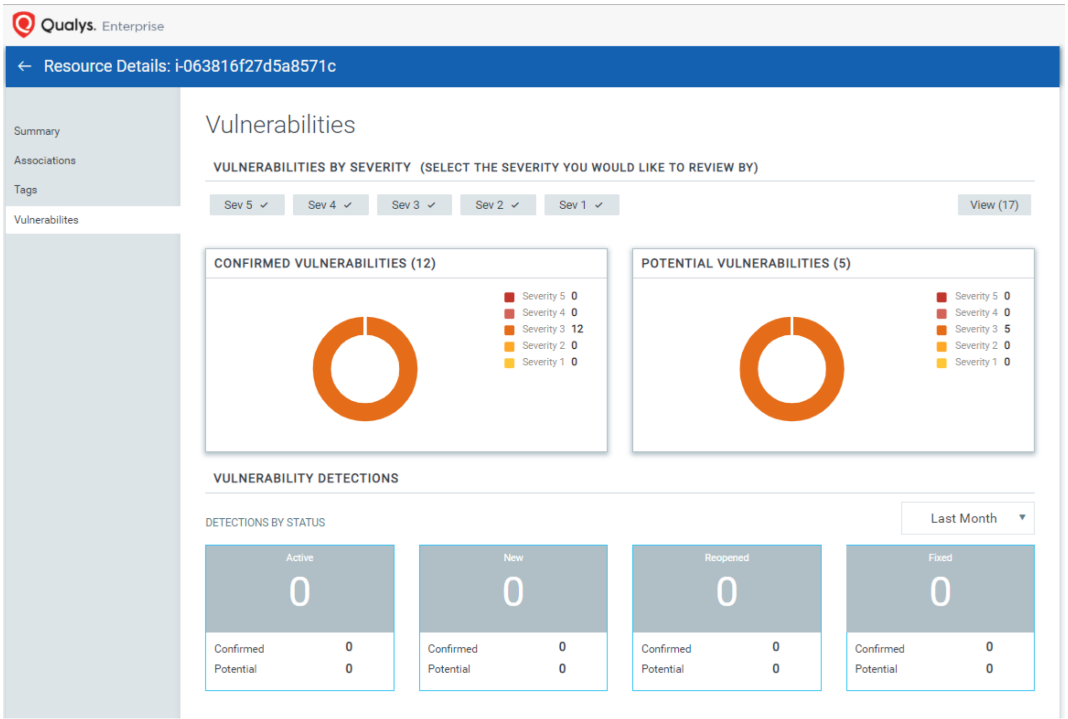
| | |
|---|---|
| Account ID: | 205767712438 |
| Region: | Canada Central (ca-central-1) |
| Availability Zone: | ca-central-1b |

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

Vulnerabilities

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

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)

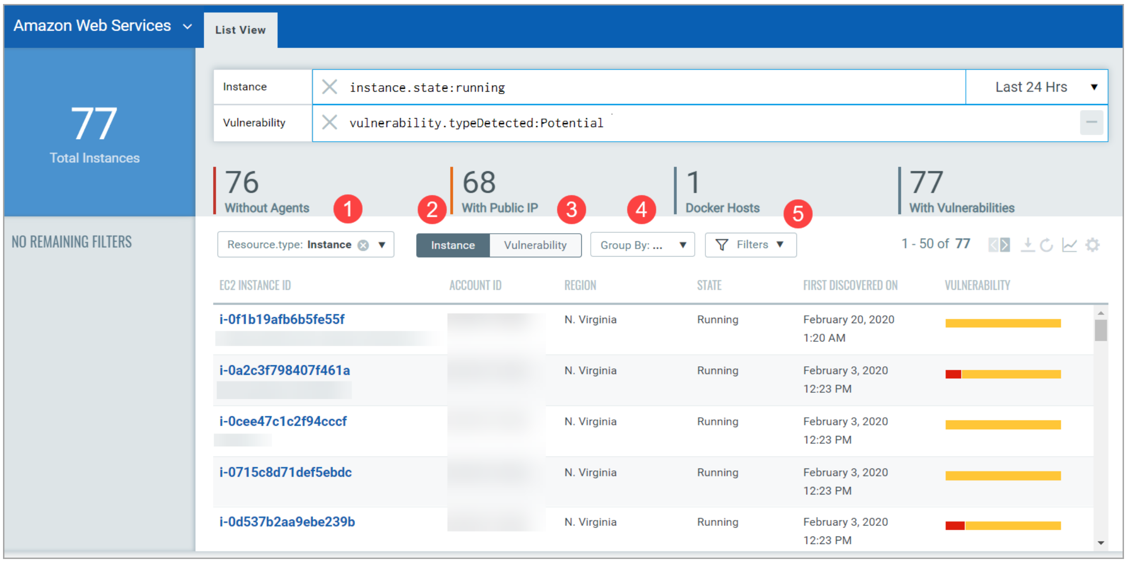
We provide you with multiple meta data filters to narrow down your search for vulnerability details. Using the new filters, you can get a complete view of vulnerability posture from an asset and vulnerability point of view.

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: instance.state:running — Last 24 Hrs

Vulnerability: vulnerability.typeDetected:Potential

Resource.type: Instance

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

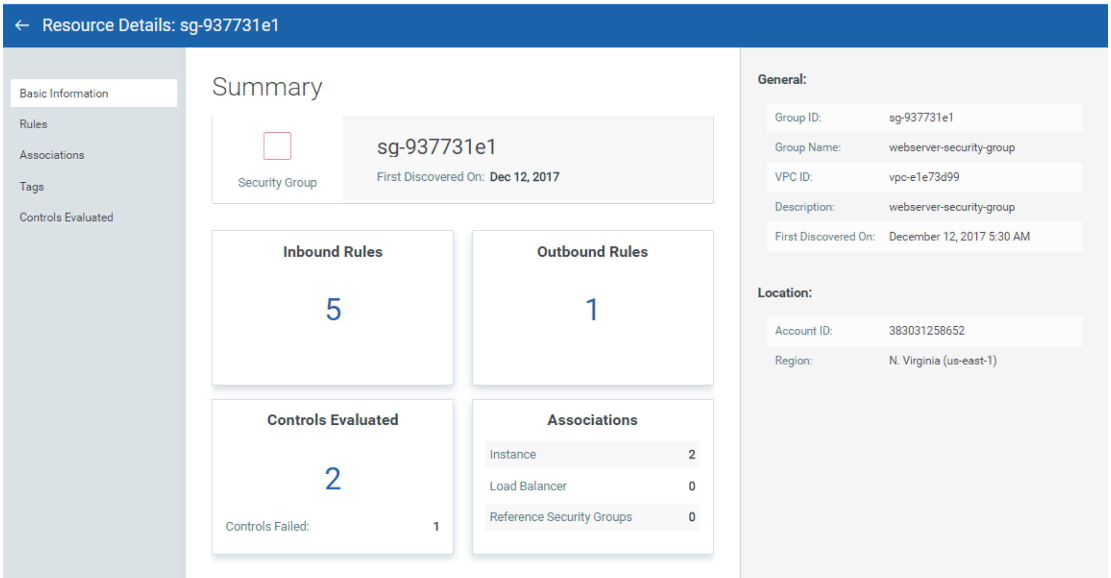
4 - Various group-by filters to narrow down your search

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: 5

Outbound Rules: 1

Controls Evaluated: 2
Controls Failed: 1

Associations

| | |
|---|---|
| Instance | 2 |
| Load Balancer | 0 |
| Reference Security Groups | 0 |

General:

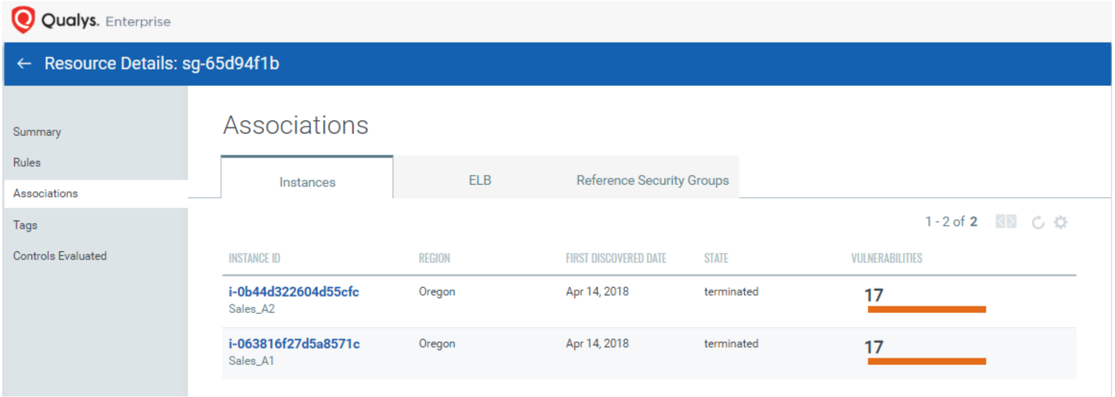
| | |
|---|---|
| Group ID: | sg-937731e1 |
| Group Name: | webserver-security-group |
| VPC ID: | vpc-e1e73d99 |
| Description: | webserver-security-group |
| First Discovered On: | December 12, 2017 5:30 AM |

Location:

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

### View Security Group Associations

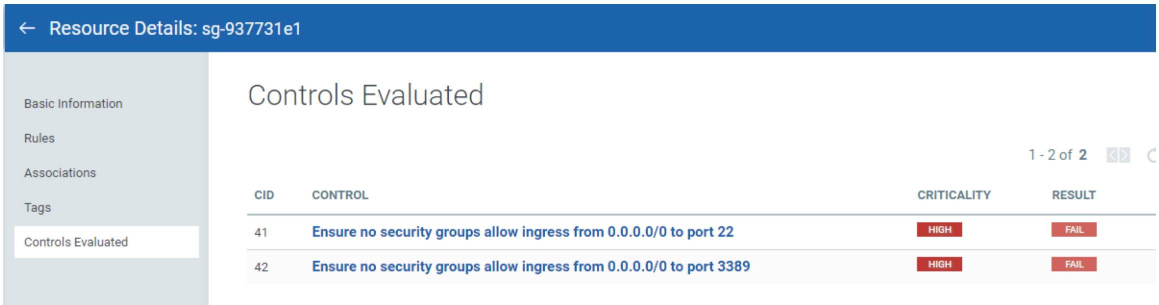
You can view various details about the associations such as the ID, region, state and so on.



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

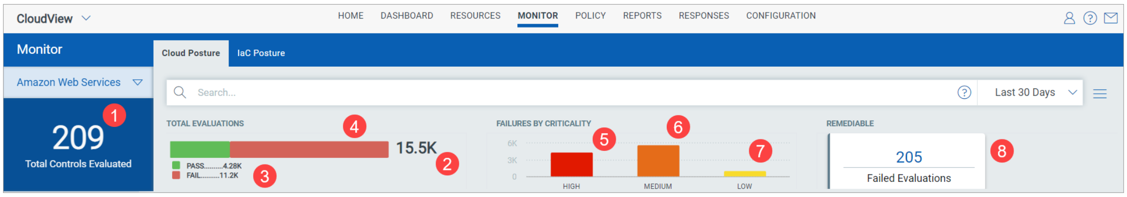
1 - 2 of 2

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

## Resources Misconfigurations

CloudView compares controls from the out-of-the-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



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.

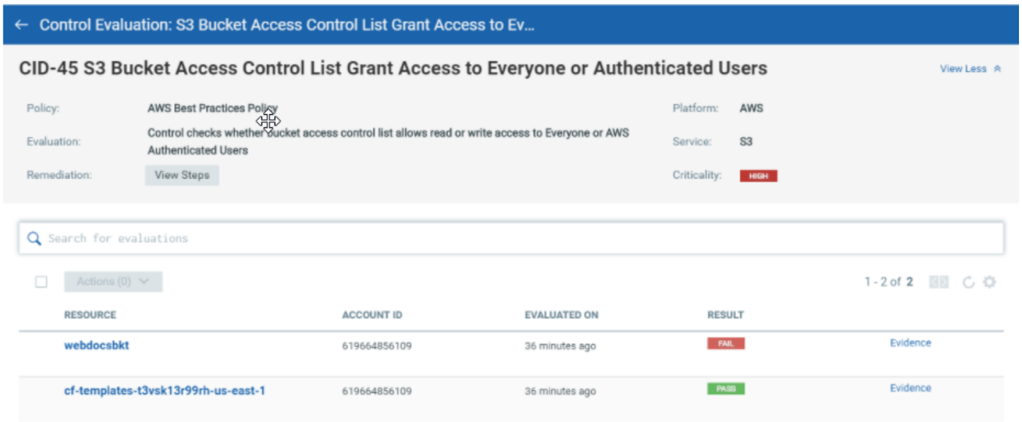
Note: When you change criticality of a control, the revised control criticality for existing evaluations is effective upon next connector run.

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

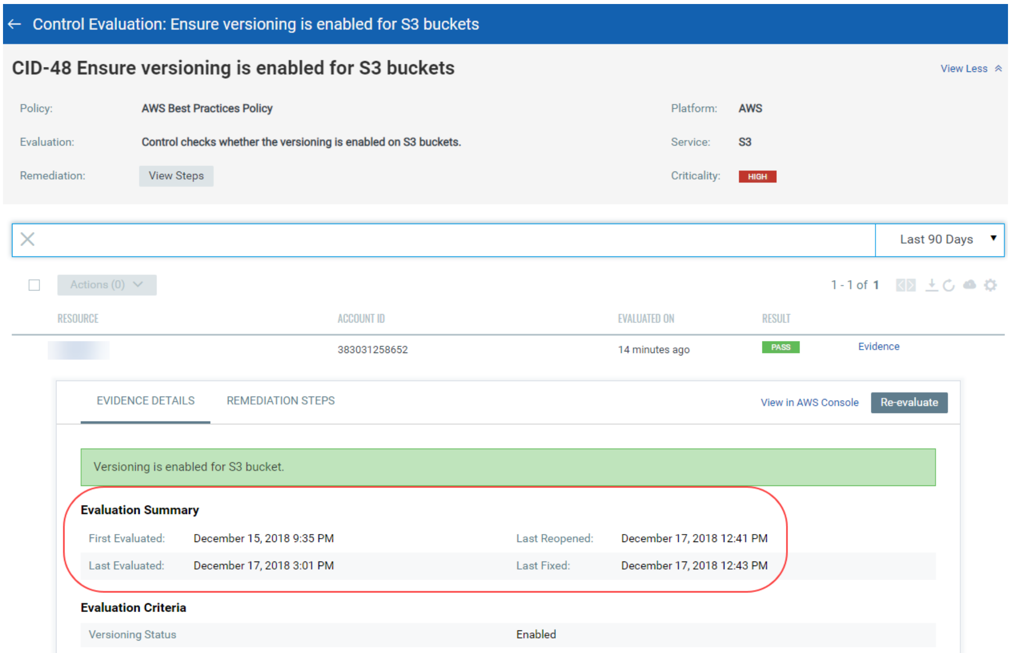
Search for evaluations

1 - 2 of 2

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

## Resource Evidence

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



← Control Evaluation: Ensure versioning is enabled for S3 buckets

CID-48 Ensure versioning is enabled for S3 buckets

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

Last 90 Days

1 - 1 of 1

| 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.

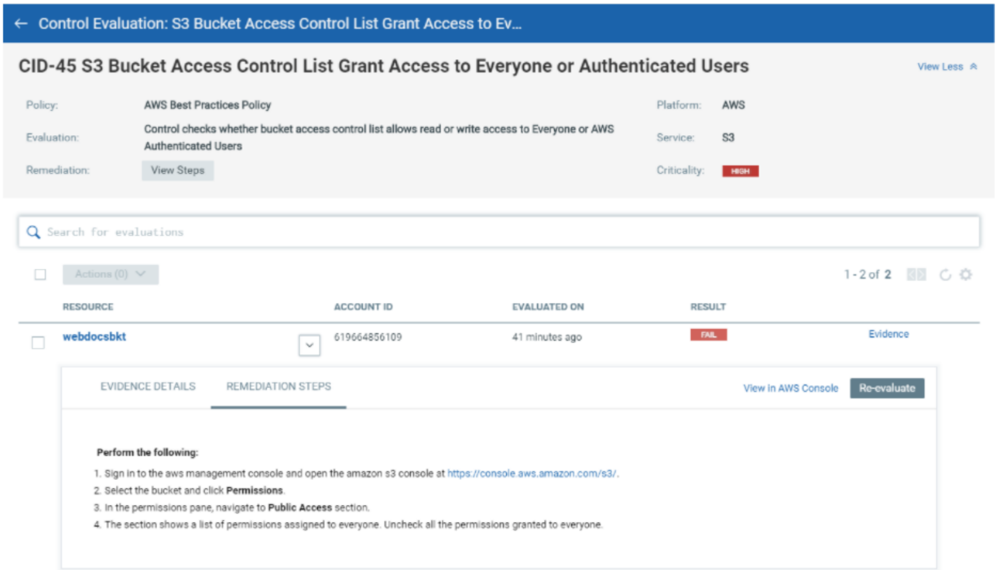
-Last Evaluated: The latest date when the control was evaluated.

-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.

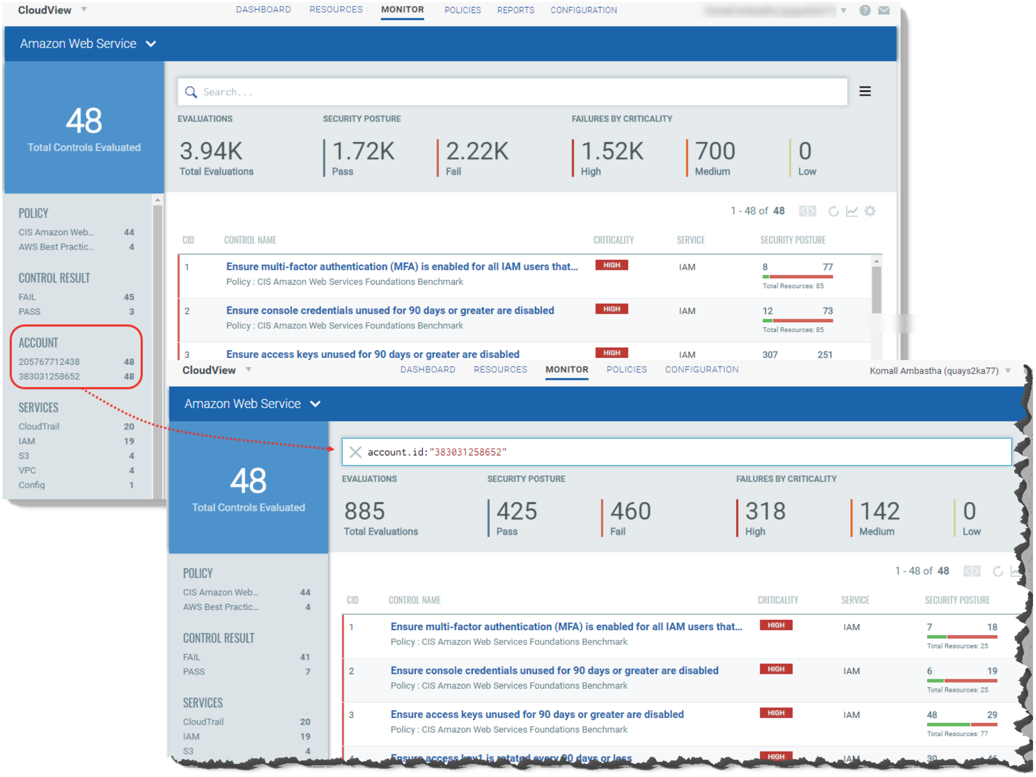

← Control Evaluation: S3 Bucket Access Control List Grant Access to Ev...
CID-45 S3 Bucket Access Control List Grant Access to Everyone or Authenticated Users
View Less
Policy: AWS Best Practices Policy
Platform: AWS
Evaluation: Control checks whether bucket access control list allows read or write access to Everyone or AWS Authenticated Users
Service: S3
Remediation: View Steps
Criticality: HIGH
Search for evaluations
Actions (0)
1 - 2 of 2
RESOURCE
ACCOUNT ID
EVALUATED ON
RESULT
webdocsbkt
619664856109
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<br>Total Evaluations | 1.72K<br>Pass | 2.22K<br>Fail | 1.52K<br>High | 700<br>Medium | 0<br>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...**<br>Policy : CIS Amazon Web Services Foundations Benchmark | HIGH | IAM | 8 77<br>Total Resources: 85 |
| 2 | **Ensure console credentials unused for 90 days or greater are disabled**<br>Policy : CIS Amazon Web Services Foundations Benchmark | HIGH | IAM | 12 73<br>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<br>Total Evaluations | 425<br>Pass | 460<br>Fail | 318<br>High | 142<br>Medium | 0<br>Low |

POLICY

| | |
|---|---|
| CIS Amazon Web... | 44 |
| AWS Best Practic... | 4 |

CONTROL RESULT

| | |
|---|---|
| FAIL | 41 |
| PASS | 7 |

SERVICES

| | |
|---|---|
| CloudTrail | 20 |
| IAM | 19 |
| S3 | 4 |

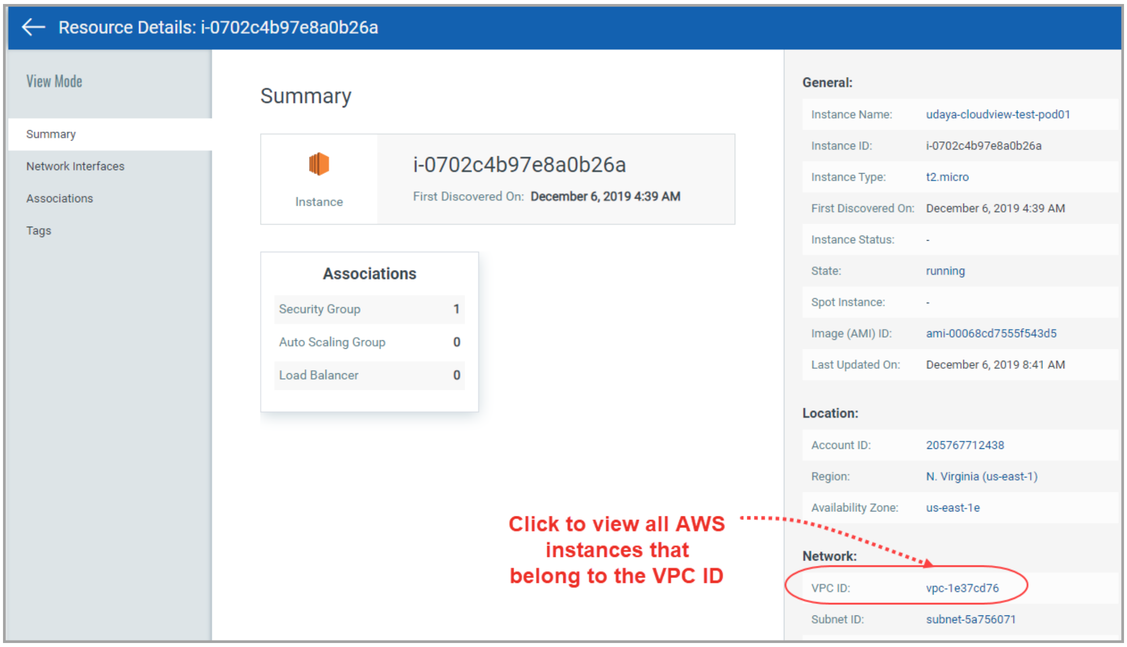
1 - 48 of **48**

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



Resource Details: i-0702c4b97e8a0b26a

Summary

Instance

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:**

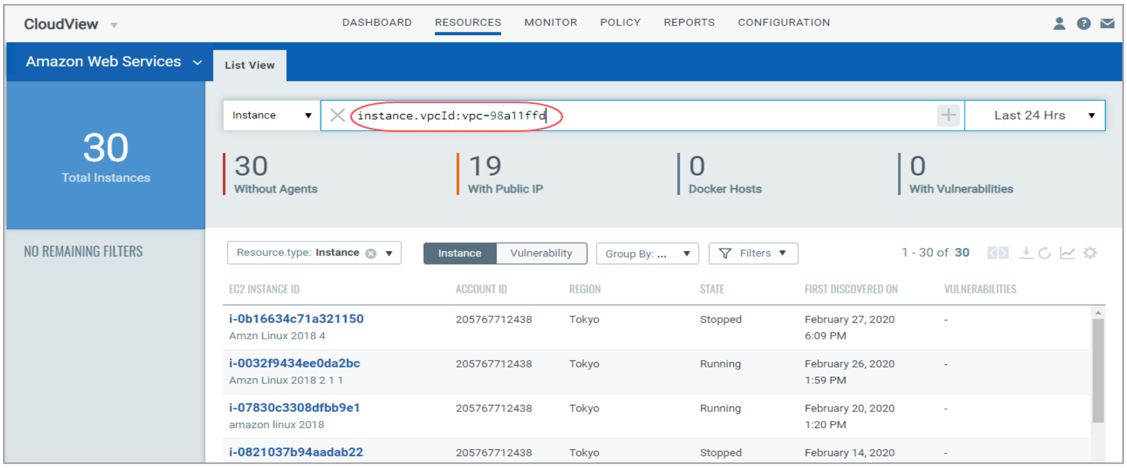
| | |
|---|---|
| Account ID: | 205767712438 |
| Region: | N. Virginia (us-east-1) |
| Availability Zone: | us-east-1e |

**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

instance.vpcId:vpc-98a11ffd

Last 24 Hrs

30 Total Instances

30 Without Agents

19 With Public IP

0 Docker Hosts

0 With Vulnerabilities

NO REMAINING FILTERS

Resource.type: Instance

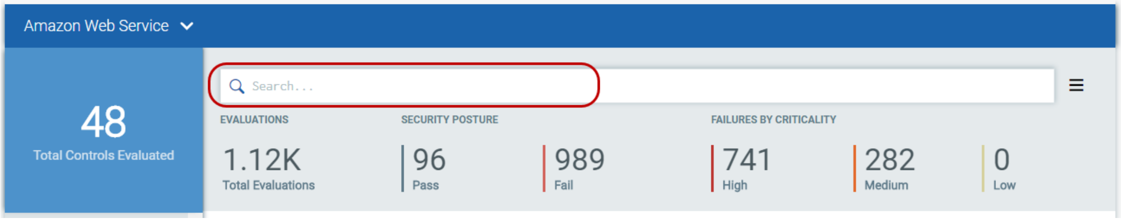
1 - 30 of 30

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

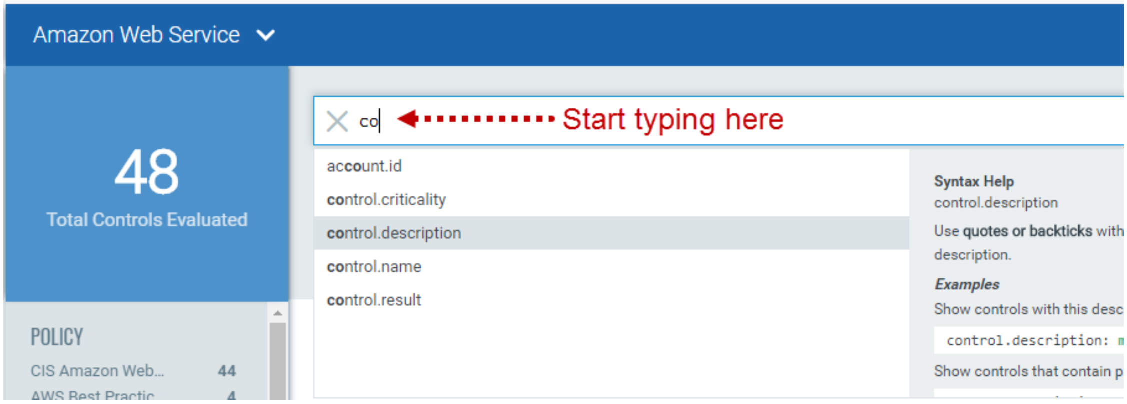
## Search Policy Controls

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

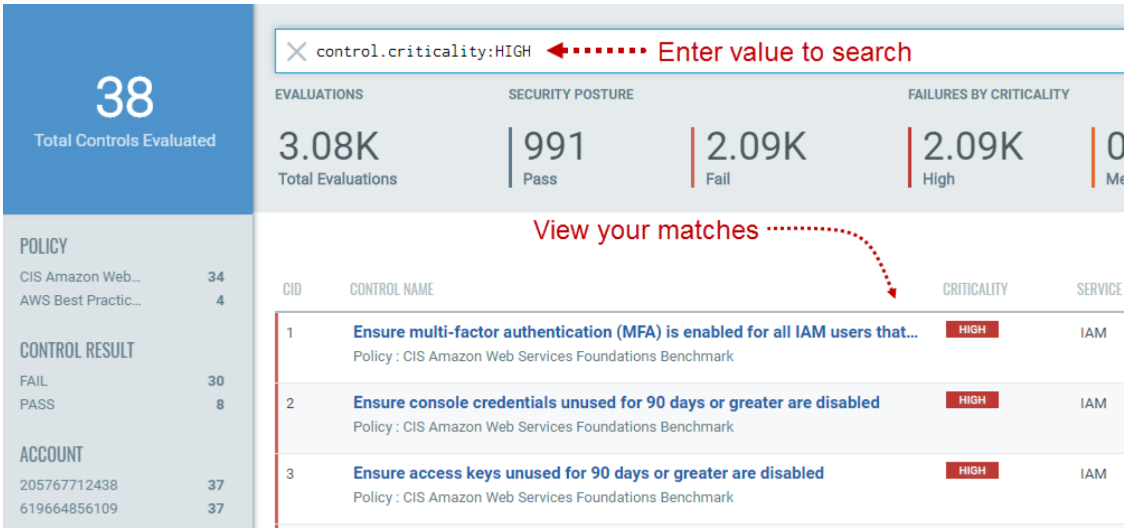
Go to Monitor tab. You'll notice a Search field above the controls list (you can also search on other tabs). This is where you'll enter your search query.



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

View your matches

38 Total Controls Evaluated

EVALUATIONS: 3.08K Total Evaluations

SECURITY POSTURE: 991 Pass | 2.09K Fail

FAILURES BY CRITICALITY: 2.09K High | 0 Me

POLICY

| | |
|---|---|
| CIS Amazon Web... | 34 |
| AWS Best Practic... | 4 |

CONTROL RESULT

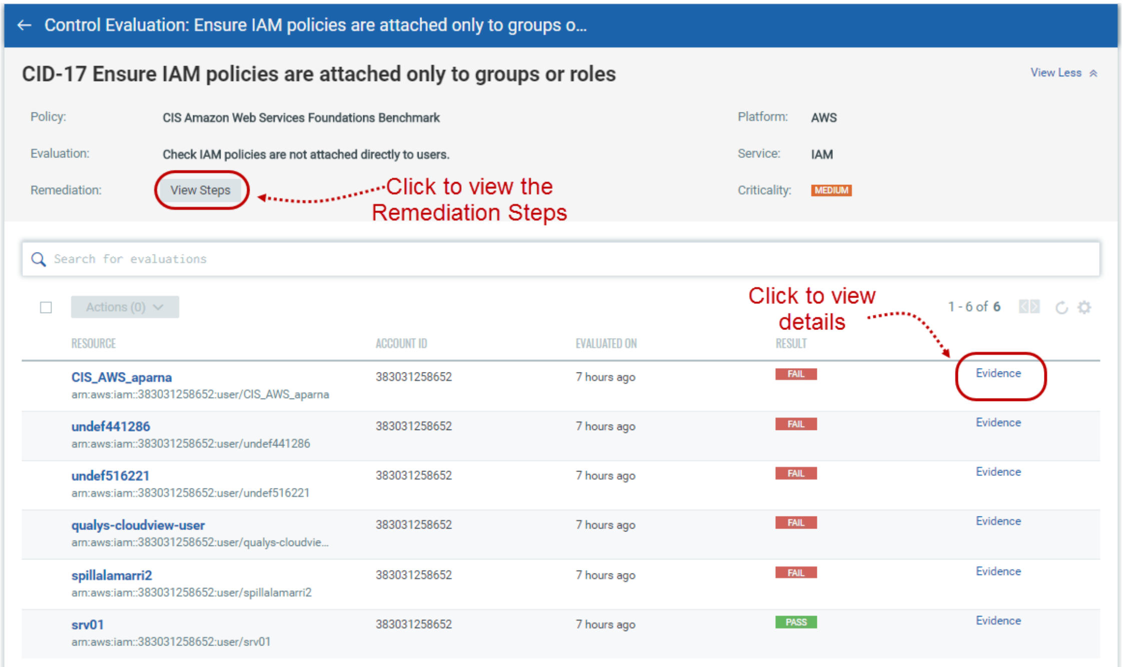
| | |
|---|---|
| FAIL | 30 |
| PASS | 8 |

ACCOUNT

| | |
|---|---|
| 205767712438 | 37 |
| 619664856109 | 37 |

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

Click to view the Remediation Steps

Platform: AWS

Service: IAM

Criticality: MEDIUM

Search for evaluations

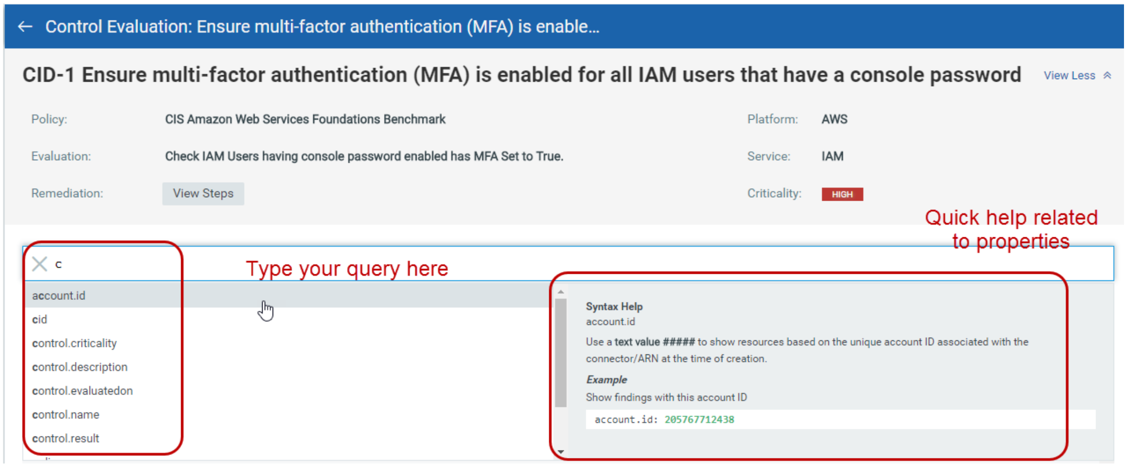
□ Actions (0)

Click to view details

1 - 6 of 6

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

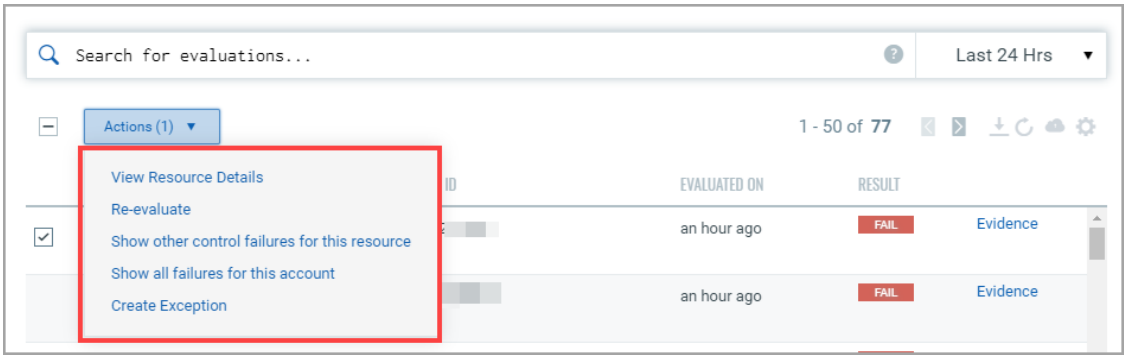
*Example*
Show findings with this account ID

```
account.id: 205767712438
```

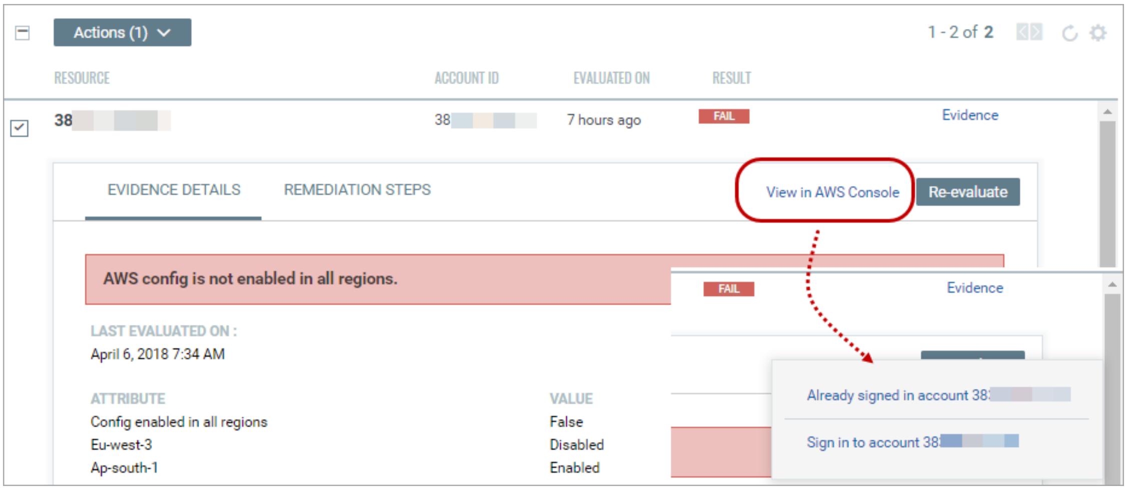
Type your query here

Quick help related to properties

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.



| RESOURCE | ACCOUNT ID | EVALUATED ON | RESULT | |
|---|---|---|---|---|
| 38[redacted] | 38[redacted] | 7 hours ago | FAIL | Evidence |

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 |

Already signed in account 38[redacted]

Sign in to account 38[redacted]

## IaC Posture

The IaC posture sub-tab under Monitor tab provides your compliance posture of resources residing in your Infrastructure as Code (IaC) templates.

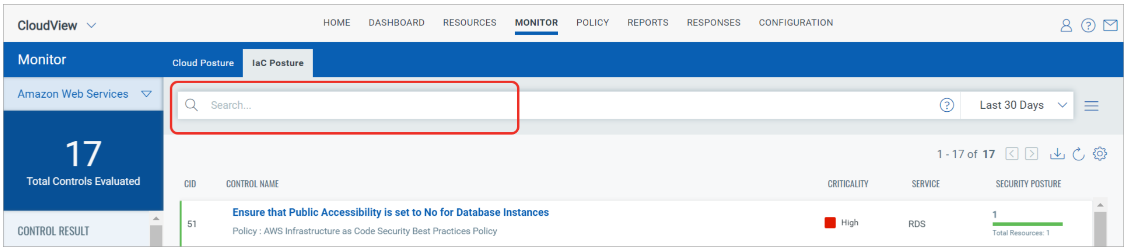
Note: The IaC evaluations are displayed for scans initiated from Git integrations. For more information on Git integrations, refer to the Secure IaC section in CloudView User Guide.

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

### Search Policy Controls

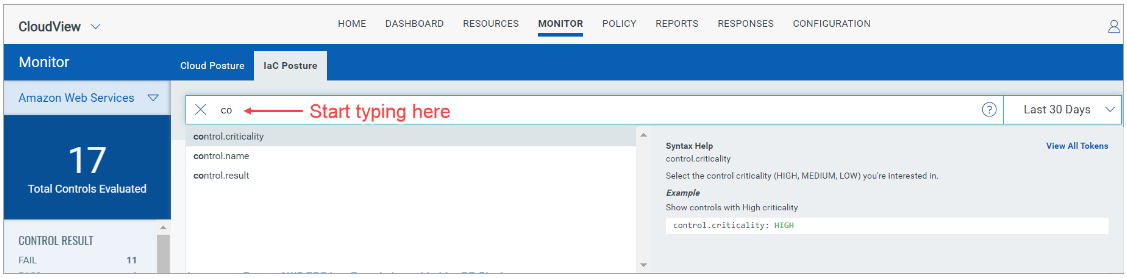
Find all about your policies and control evaluations and quickly get up-to-date information using Qualys Advanced Search.

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



| CID | CONTROL NAME | CRITICALITY | SERVICE | SECURITY POSTURE |
|---|---|---|---|---|
| 51 | Ensure that Public Accessibility is set to No for Database Instances<br>Policy : AWS Infrastructure as Code Security Best Practices Policy | High | RDS | 1<br>Total Resources: 1 |

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.



Start typing here

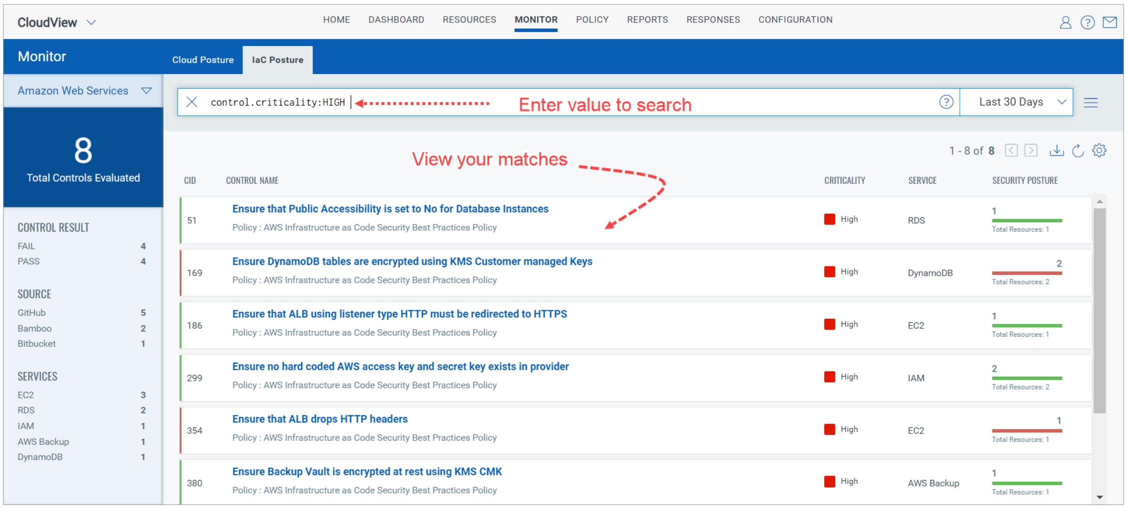
17
Total Controls Evaluated

CONTROL RESULT
FAIL 11

**Syntax Help**
control.criticality
Select the control criticality (HIGH, MEDIUM, LOW) you're interested in.
*Example*
Show controls with High criticality

```
control.criticality: HIGH
```

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

View your matches

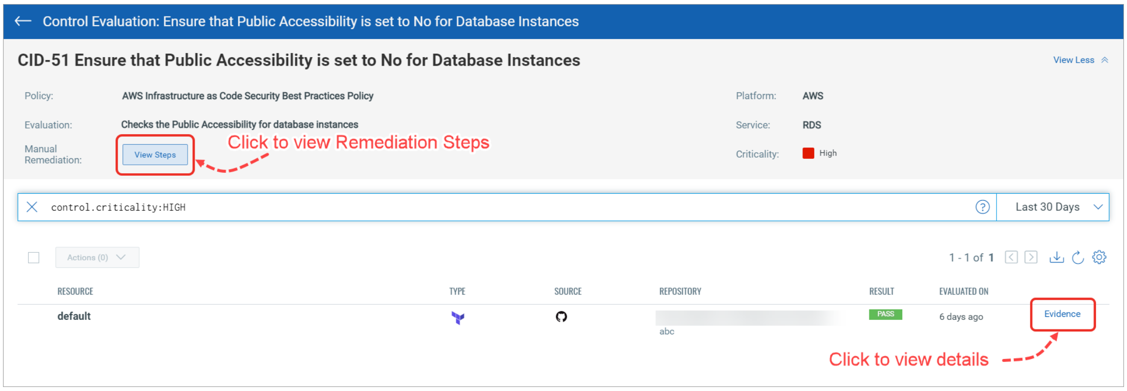
8
Total Controls Evaluated

CONTROL RESULT
FAIL 4
PASS 4

SOURCE
GitHub 5
Bamboo 2
Bitbucket 1

SERVICES
EC2 3
RDS 2
IAM 1
AWS Backup 1
DynamoDB 1

| CID | CONTROL NAME | CRITICALITY | SERVICE | SECURITY POSTURE |
|---|---|---|---|---|
| 51 | **Ensure that Public Accessibility is set to No for Database Instances**<br>Policy : AWS Infrastructure as Code Security Best Practices Policy | 🟥 High | RDS | 1<br>Total Resources: 1 |
| 169 | **Ensure DynamoDB tables are encrypted using KMS Customer managed Keys**<br>Policy : AWS Infrastructure as Code Security Best Practices Policy | 🟥 High | DynamoDB | 2<br>Total Resources: 2 |
| 186 | **Ensure that ALB using listener type HTTP must be redirected to HTTPS**<br>Policy : AWS Infrastructure as Code Security Best Practices Policy | 🟥 High | EC2 | 1<br>Total Resources: 1 |
| 299 | **Ensure no hard coded AWS access key and secret key exists in provider**<br>Policy : AWS Infrastructure as Code Security Best Practices Policy | 🟥 High | IAM | 2<br>Total Resources: 2 |
| 354 | **Ensure that ALB drops HTTP headers**<br>Policy : AWS Infrastructure as Code Security Best Practices Policy | 🟥 High | EC2 | 1<br>Total Resources: 1 |
| 380 | **Ensure Backup Vault is encrypted at rest using KMS CMK**<br>Policy : AWS Infrastructure as Code Security Best Practices Policy | 🟥 High | AWS Backup | 1<br>Total Resources: 1 |



Control Evaluation: Ensure that Public Accessibility is set to No for Database Instances

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

Policy: AWS Infrastructure as Code Security Best Practices Policy
Evaluation: Checks the Public Accessibility for database instances
Manual Remediation:
Platform: AWS
Service: RDS
Criticality: 🟥 High

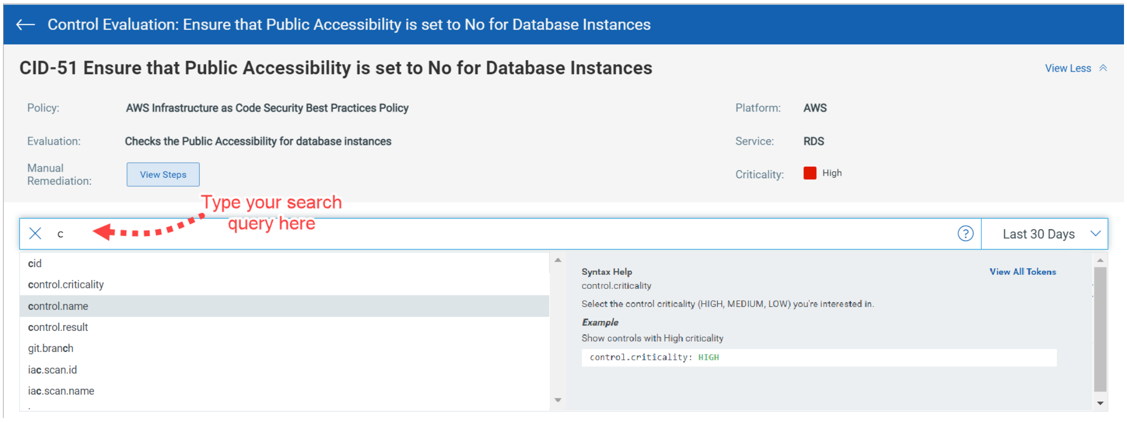
Click to view Remediation Steps

```
control.criticality:HIGH
```

| RESOURCE | TYPE | SOURCE | REPOSITORY | RESULT | EVALUATED ON |
|---|---|---|---|---|---|
| default | | | abc | PASS | 6 days ago |

Click to view details

You'll notice a Search field and this is where you'll enter your search query. 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 that Public Accessibility is set to No for Database Instances

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

Policy: AWS Infrastructure as Code Security Best Practices Policy

Evaluation: Checks the Public Accessibility for database instances

Manual Remediation: View Steps

Platform: AWS

Service: RDS

Criticality: 🟥 High

Type your search query here

c

cid
control.criticality
control.name
control.result
git.branch
iac.scan.id
iac.scan.name

Syntax Help

control.criticality

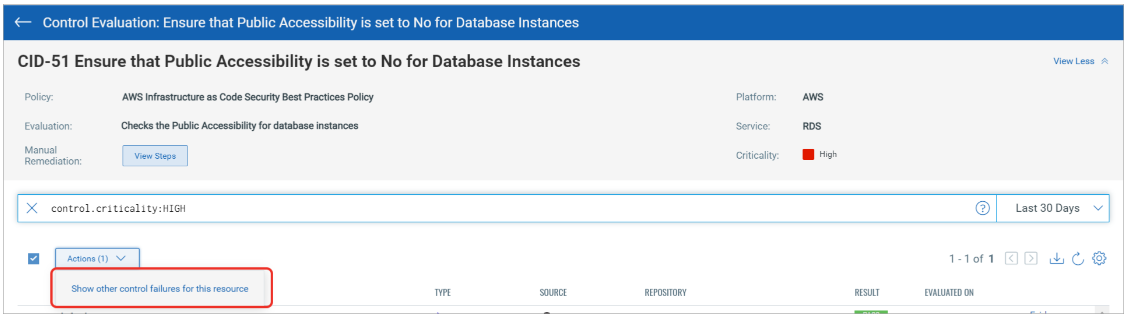
Select the control criticality (HIGH, MEDIUM, LOW) you're interested in.

*Example*

Show controls with High criticality

```
control.criticality: HIGH
```

You could also view other failed control for the same resource. Select the control and click Actions or the quick actions menu.



Control Evaluation: Ensure that Public Accessibility is set to No for Database Instances

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

Policy: AWS Infrastructure as Code Security Best Practices Policy

Evaluation: Checks the Public Accessibility for database instances

Manual Remediation: View Steps

Platform: AWS

Service: RDS

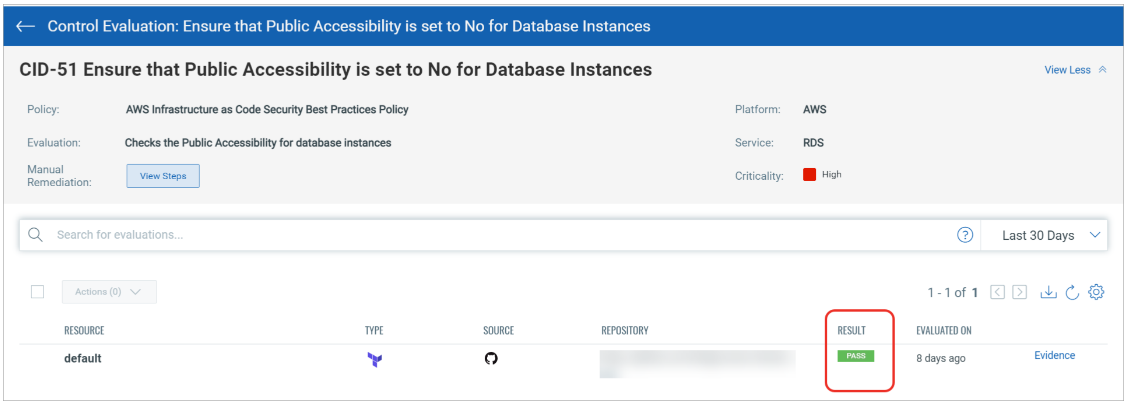
Criticality: 🟥 High

```
control.criticality:HIGH
```

☑ Actions (1)

Show other control failures for this resource

The Result column indicates the evaluation result of the resource against the control.



Control Evaluation: Ensure that Public Accessibility is set to No for Database Instances

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

Policy: AWS Infrastructure as Code Security Best Practices Policy

Evaluation: Checks the Public Accessibility for database instances

Manual Remediation: View Steps

Platform: AWS

Service: RDS

Criticality: 🟥 High

Search for evaluations...

□ Actions (0)

| RESOURCE | TYPE | SOURCE | REPOSITORY | RESULT | EVALUATED ON | |
|---|---|---|---|---|---|---|
| default | | | | PASS | 8 days ago | Evidence |

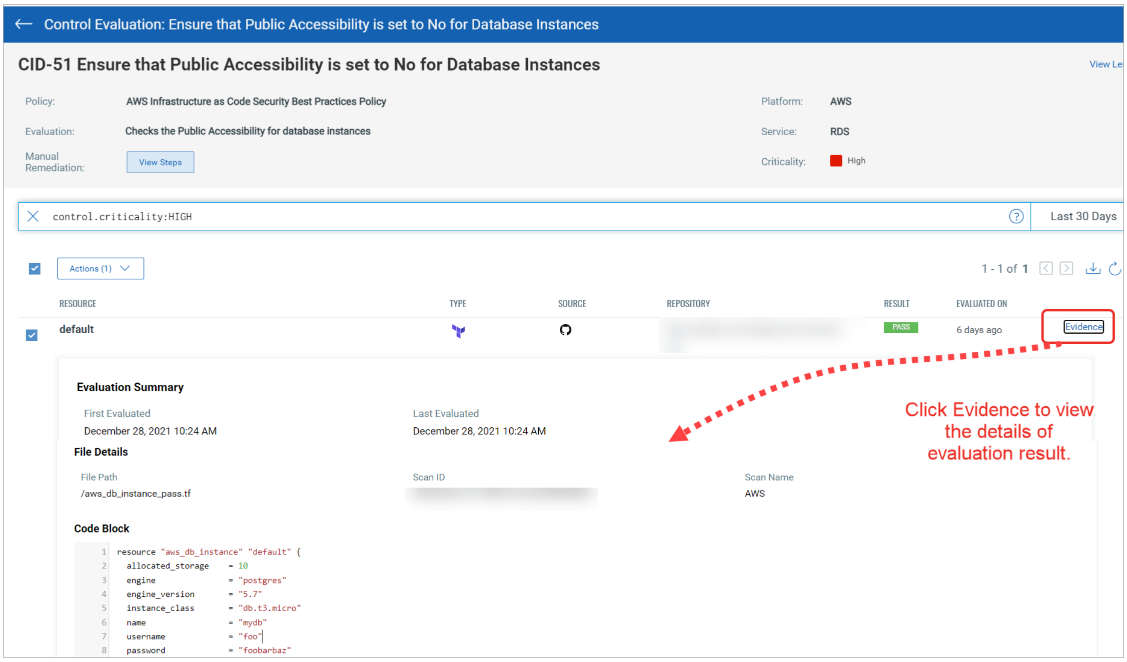
Depending on the evaluation result, the Result column displays one of the following values:

- Fail: Indicates the resource failed the control evaluation.

- Pass: Indicates the resource has passed the control evaluation.

- Skip: Indicates the resource skipped the control evaluation. To know more about how to skip control evaluation for resources, see Exceptions.

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 or skip.



← Control Evaluation: Ensure that Public Accessibility is set to No for Database Instances

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

Policy: AWS Infrastructure as Code Security Best Practices Policy

Evaluation: Checks the Public Accessibility for database instances

Manual Remediation: View Steps

Platform: AWS

Service: RDS

Criticality: 🟥 High

control.criticality:HIGH

| ☑ | RESOURCE | TYPE | SOURCE | REPOSITORY | RESULT | EVALUATED ON | |
|---|---|---|---|---|---|---|---|
| ☑ | default | | | [redacted] | PASS | 6 days ago | Evidence |

Evaluation Summary

First Evaluated
December 28, 2021 10:24 AM

Last Evaluated
December 28, 2021 10:24 AM

File Details

File Path
/aws_db_instance_pass.tf

Scan ID
[redacted]

Scan Name
AWS

Code Block

```
resource "aws_db_instance" "default" {
  allocated_storage    = 10
  engine               = "postgres"
  engine_version       = "5.7"
  instance_class       = "db.t3.micro"
  name                 = "mydb"
  username             = "foo"
  password             = "foobarbaz"
```

Click Evidence to view the details of evaluation result.

## Exceptions

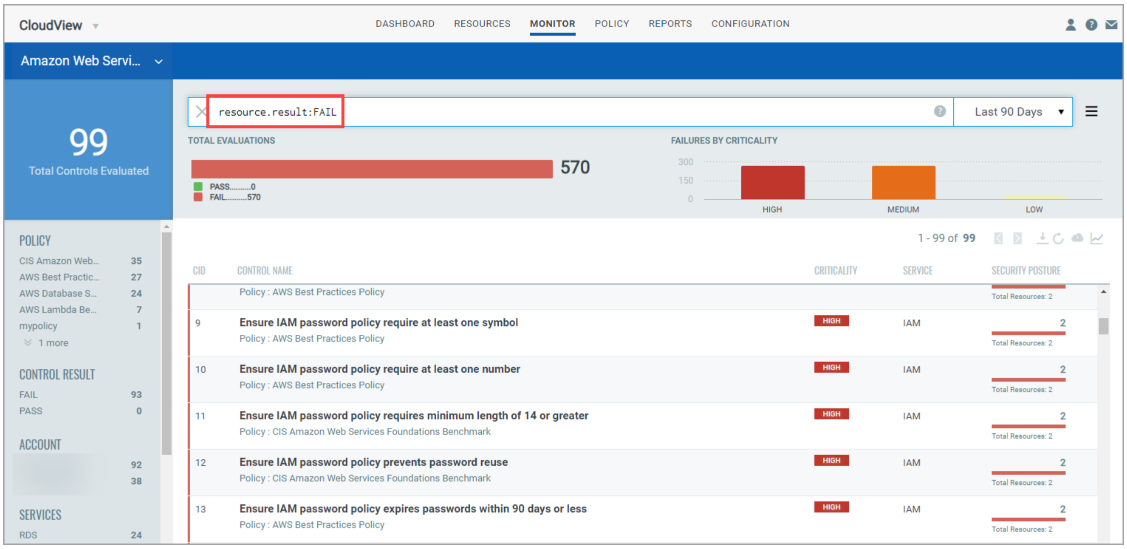
You may want to create exceptions to exempt certain cloud resources from a particular control or temporarily change the status of a resource for a particular control from Failed to PassE (Pass with Exception).

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

99
Total Controls Evaluated

570
🟩 PASS.........0
🟥 FAIL.........570

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

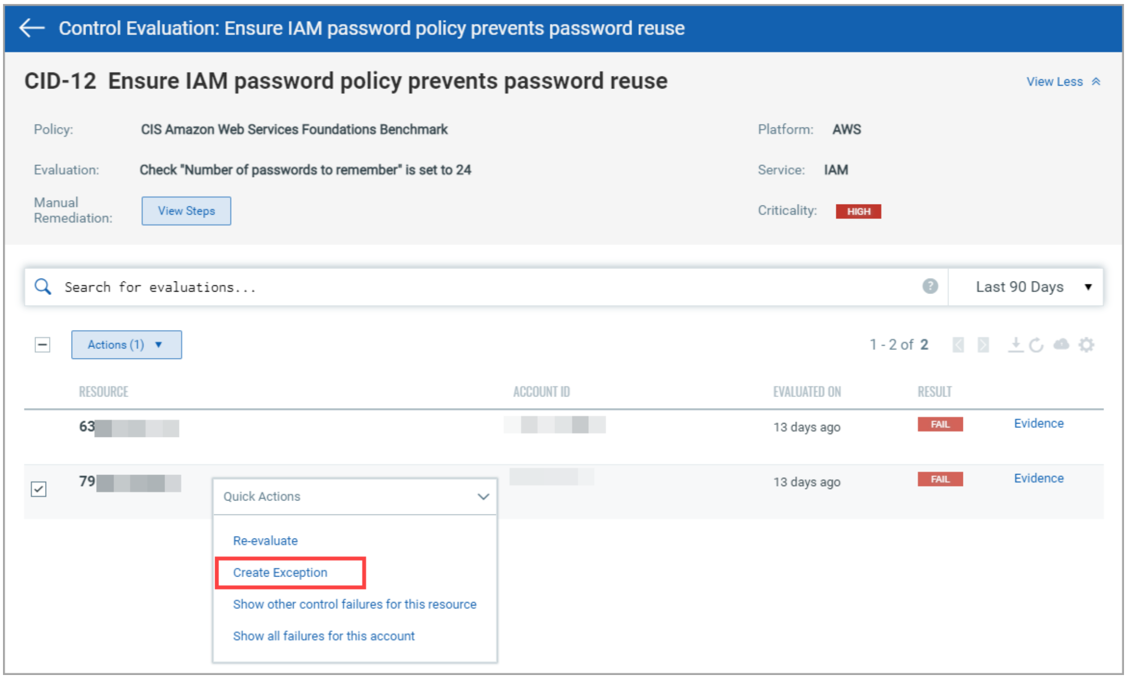
ACCOUNT
92
38

SERVICES
RDS 24

1 - 99 of 99

| 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<br>Policy : AWS Best Practices Policy | HIGH | IAM | 2<br>Total Resources: 2 |
| 10 | Ensure IAM password policy require at least one number<br>Policy : AWS Best Practices Policy | HIGH | IAM | 2<br>Total Resources: 2 |
| 11 | Ensure IAM password policy requires minimum length of 14 or greater<br>Policy : CIS Amazon Web Services Foundations Benchmark | HIGH | IAM | 2<br>Total Resources: 2 |
| 12 | Ensure IAM password policy prevents password reuse<br>Policy : CIS Amazon Web Services Foundations Benchmark | HIGH | IAM | 2<br>Total Resources: 2 |
| 13 | Ensure IAM password policy expires passwords within 90 days or less<br>Policy : AWS Best Practices Policy | HIGH | IAM | 2<br>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...

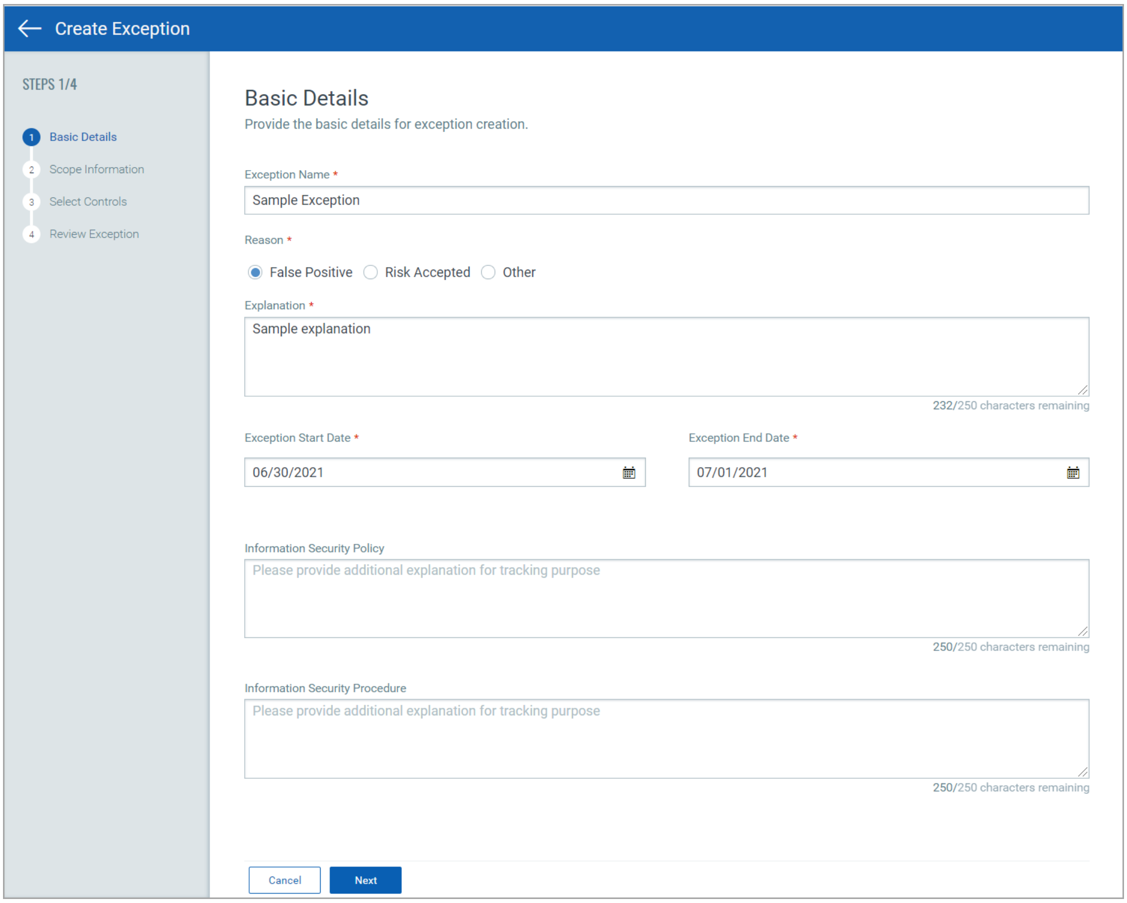
1 - 2 of 2

| | 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.



Create Exception

STEPS 1/4

1 Basic Details
2 Scope Information
3 Select Controls
4 Review Exception

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

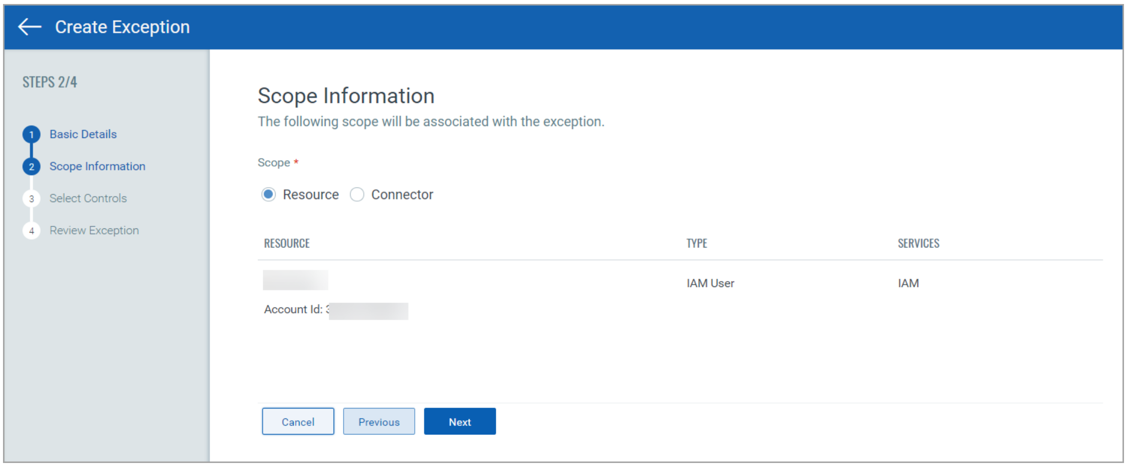
250/250 characters remaining

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

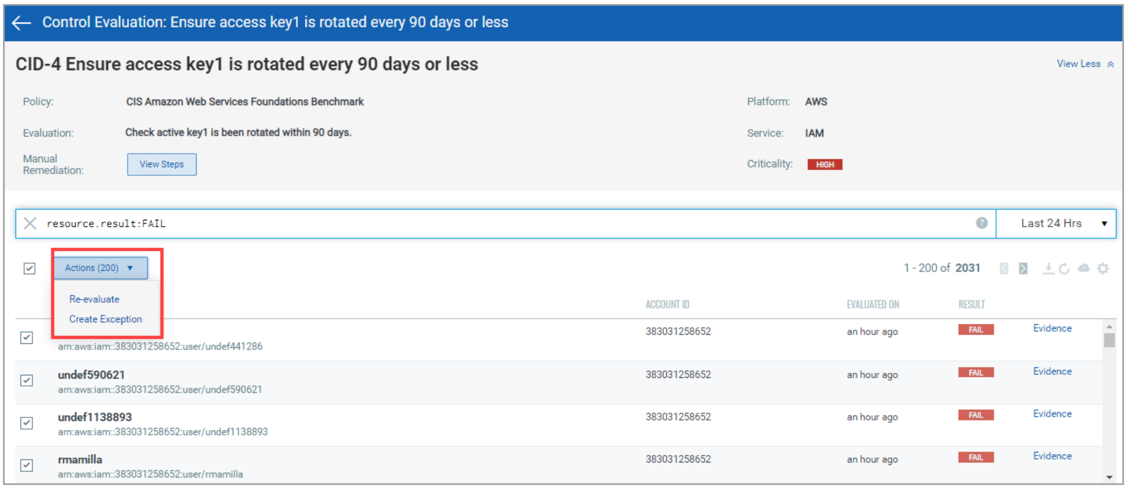
The following scope will be associated with the exception.

Scope *

● Resource ○ Connector

| RESOURCE | TYPE | SERVICES |
|---|---|---|
| [redacted]<br>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.



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:

Platform: AWS

Service: IAM

Criticality: HIGH

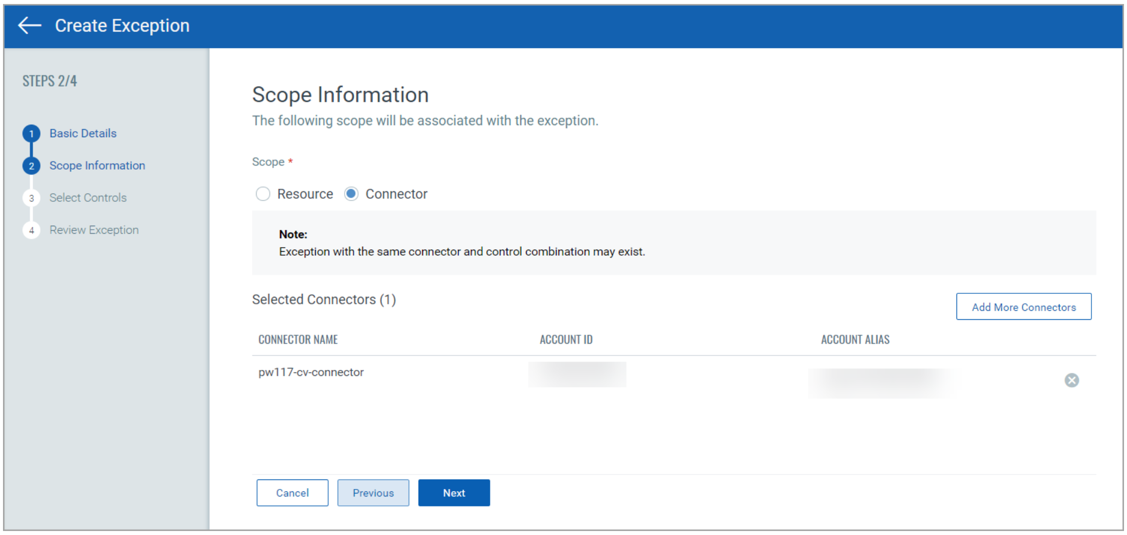
```
resource.result:FAIL
```

1 - 200 of 2031

| ☑ | | ACCOUNT ID | EVALUATED ON | RESULT | |
|---|---|---|---|---|---|
| ☑ | arn:aws:iam::383031258652:user/undef441286 | 383031258652 | an hour ago | FAIL | Evidence |
| ☑ | **undef590621**<br>arn:aws:iam::383031258652:user/undef590621 | 383031258652 | an hour ago | FAIL | Evidence |
| ☑ | **undef1138893**<br>arn:aws:iam::383031258652:user/undef1138893 | 383031258652 | an hour ago | FAIL | Evidence |
| ☑ | **rmamilla**<br>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.



Create Exception

STEPS 2/4

1 Basic Details
2 Scope Information
3 Select Controls
4 Review 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)

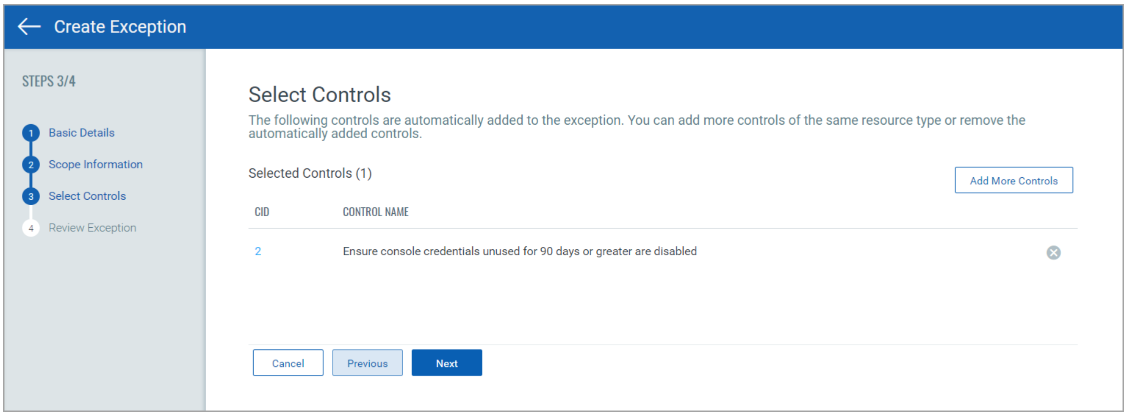
Add More Connectors

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

Cancel Previous Next

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.



Create Exception

STEPS 3/4

1 Basic Details
2 Scope Information
3 Select Controls
4 Review Exception

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)

Add More Controls

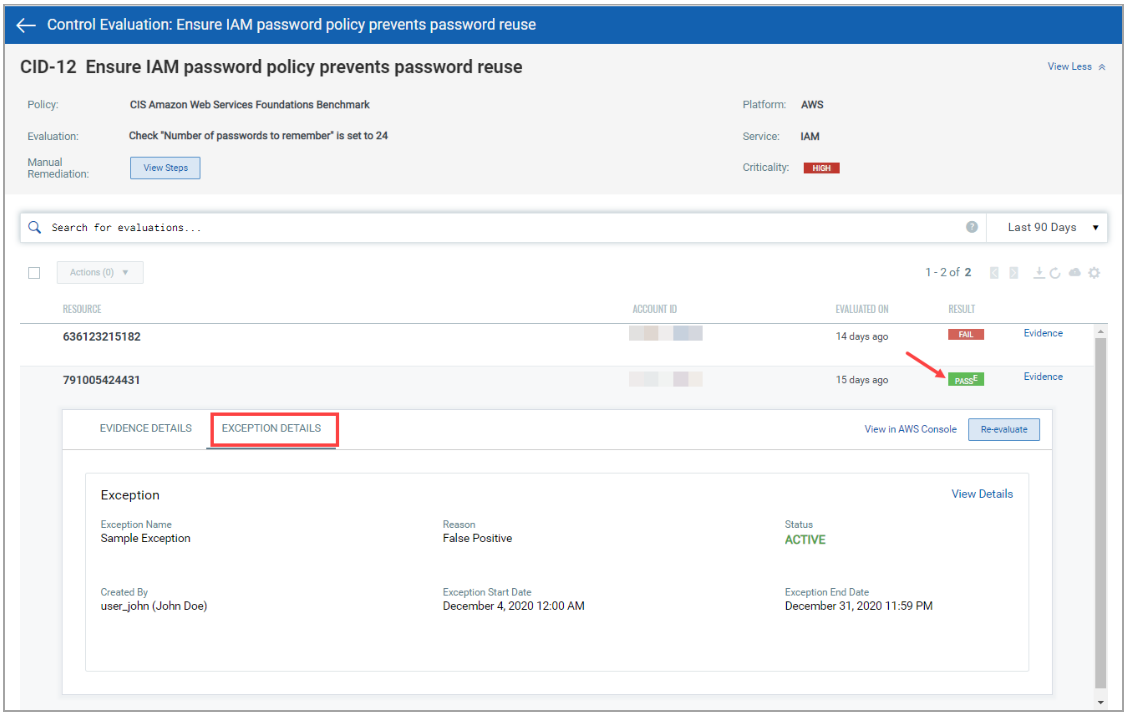
| CID | CONTROL NAME |
|---|---|
| 2 | Ensure console credentials unused for 90 days or greater are disabled |

Cancel Previous Next

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: View Steps

Platform: AWS

Service: IAM

Criticality: HIGH

| RESOURCE | ACCOUNT ID | EVALUATED ON | RESULT | |
|---|---|---|---|---|
| 636123215182 | [redacted] | 14 days ago | FAIL | Evidence |
| 791005424431 | [redacted] | 15 days ago | PASS^E | Evidence |

Exception

Exception Name: Sample Exception

Reason: False Positive

Status: ACTIVE

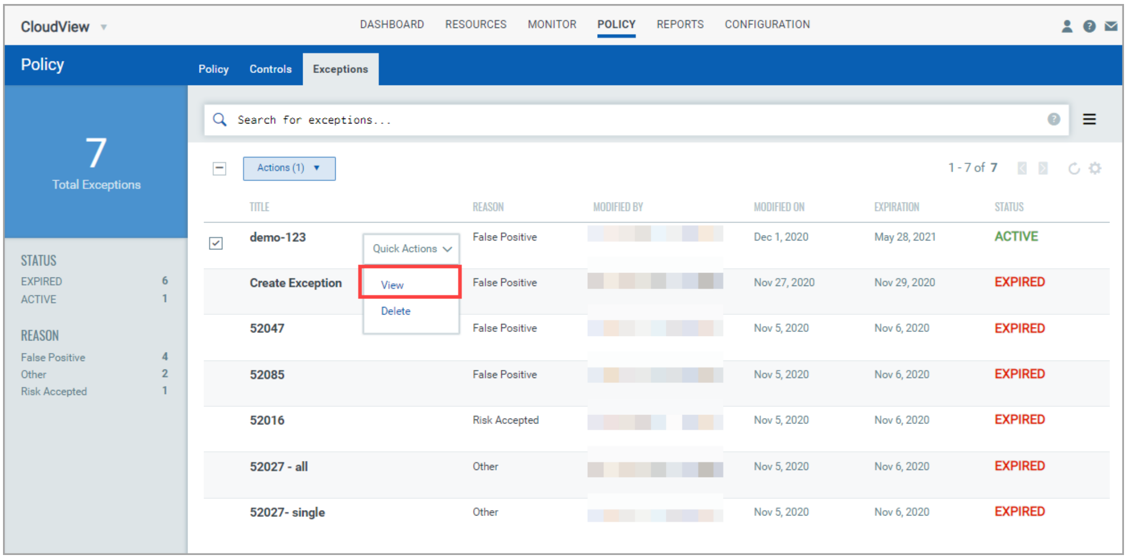
Created By: user_john (John Doe)

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 |

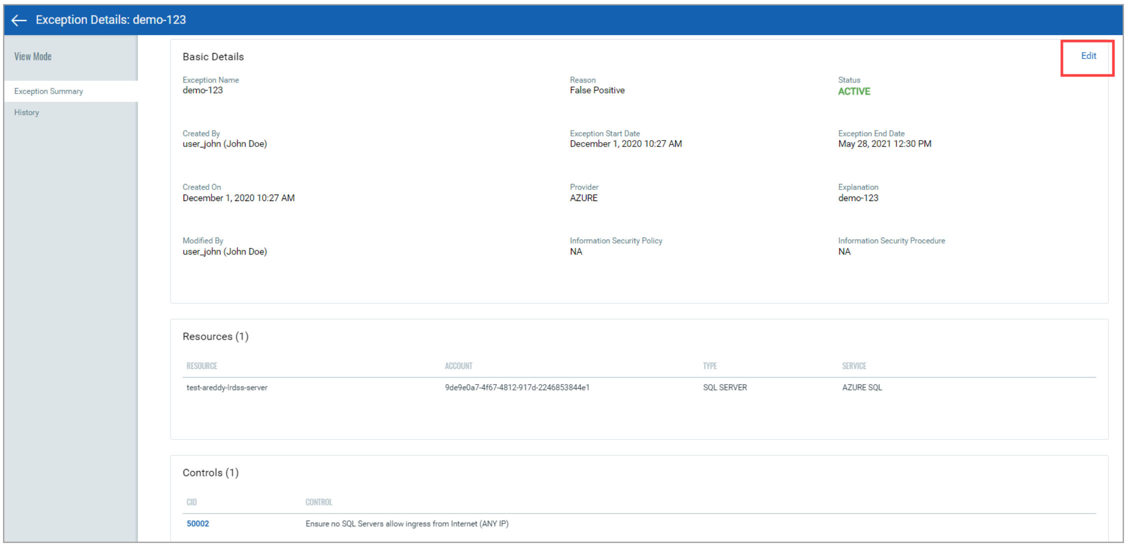
| REASON | |
|---|---|
| False Positive | 4 |
| Other | 2 |
| Risk Accepted | 1 |

1 - 7 of 7

| | 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

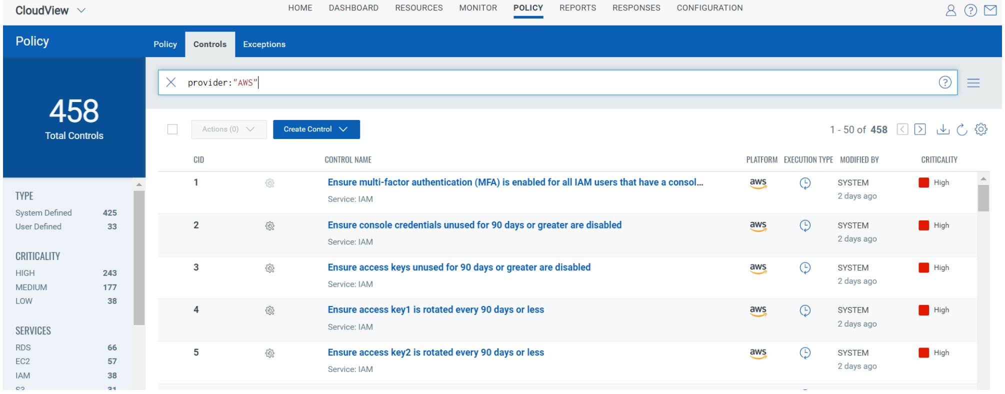
CloudView continuously discovers resources and ensures resources are compliant in relation to respective Benchmark & Best Practices policy provided out-of-the-box.

## 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.

## 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"

458
Total Controls

1 - 50 of 458

| TYPE | |
|---|---|
| System Defined | 425 |
| User Defined | 33 |
| **CRITICALITY** | |
| HIGH | 243 |
| MEDIUM | 177 |
| LOW | 38 |
| **SERVICES** | |
| RDS | 66 |
| EC2 | 57 |
| IAM | 38 |

| CID | | CONTROL NAME | PLATFORM | EXECUTION TYPE | MODIFIED BY | CRITICALITY |
|---|---|---|---|---|---|---|
| 1 | ⚙ | Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a consol...<br>Service: IAM | aws | | SYSTEM<br>2 days ago | 🟥 High |
| 2 | ⚙ | Ensure console credentials unused for 90 days or greater are disabled<br>Service: IAM | aws | | SYSTEM<br>2 days ago | 🟥 High |
| 3 | ⚙ | Ensure access keys unused for 90 days or greater are disabled<br>Service: IAM | aws | | SYSTEM<br>2 days ago | 🟥 High |
| 4 | ⚙ | Ensure access key1 is rotated every 90 days or less<br>Service: IAM | aws | | SYSTEM<br>2 days ago | 🟥 High |
| 5 | ⚙ | Ensure access key2 is rotated every 90 days or less<br>Service: IAM | aws | | SYSTEM<br>2 days ago | 🟥 High |

⚙ - 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

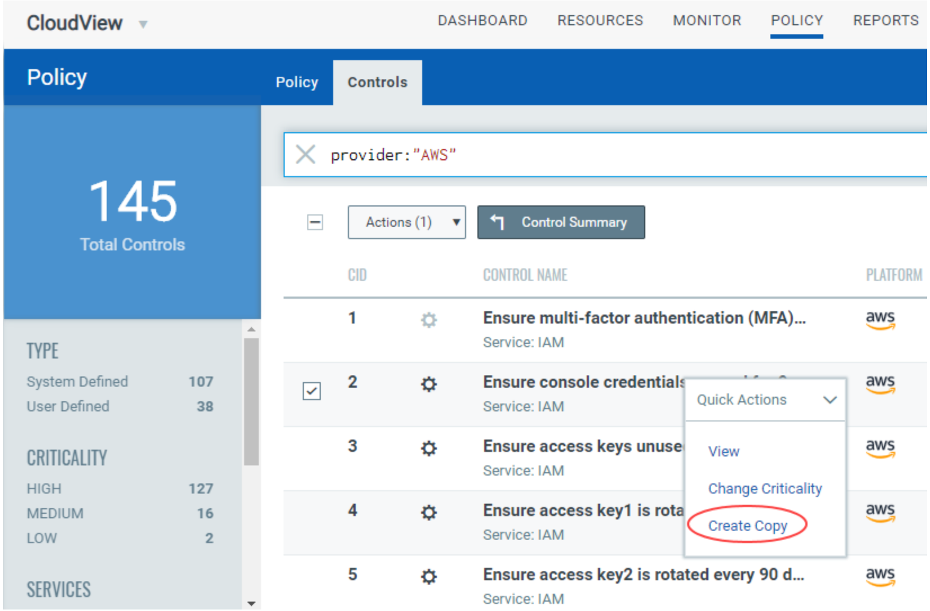
Go to Policy > Controls and select the control to be customized, select Create Copy from the quick action menu. The ⚙ icon is used to indicate that the control can be customized. Currently, 12 AWS and 3 Azure controls are customizable.

> Note: This is available only when Manage Custom Control permissions is enabled in CloudView permissions.

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)...<br>Service: IAM | aws |
| ☑ | 2 | ⚙ | Ensure console credentials<br>Service: IAM | aws |
| | 3 | ⚙ | Ensure access keys unuse<br>Service: IAM | aws |
| | 4 | ⚙ | Ensure access key1 is rota<br>Service: IAM | aws |
| | 5 | ⚙ | Ensure access key2 is rotated every 90 d...<br>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. For more information, see Manage Custom Control Permissions.

### 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. For more information, see Manage Custom Control Permissions.

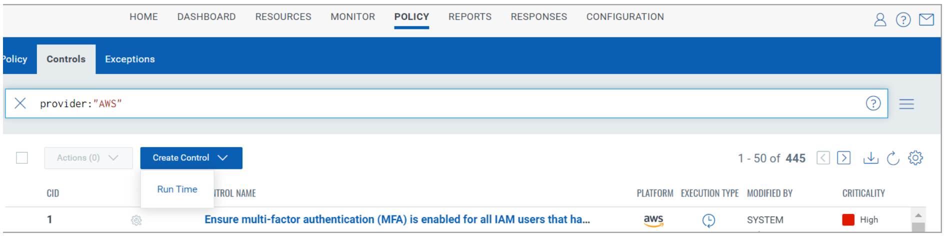
## Create a Customized Control

You can create your own custom control and associate it to the custom policy to be evaluated for the custom policy.

> Note: Currently, you can create customized controls for Amazon Web Services (AWS).

(1) Navigate to Policy > Control > Amazon Web Services.

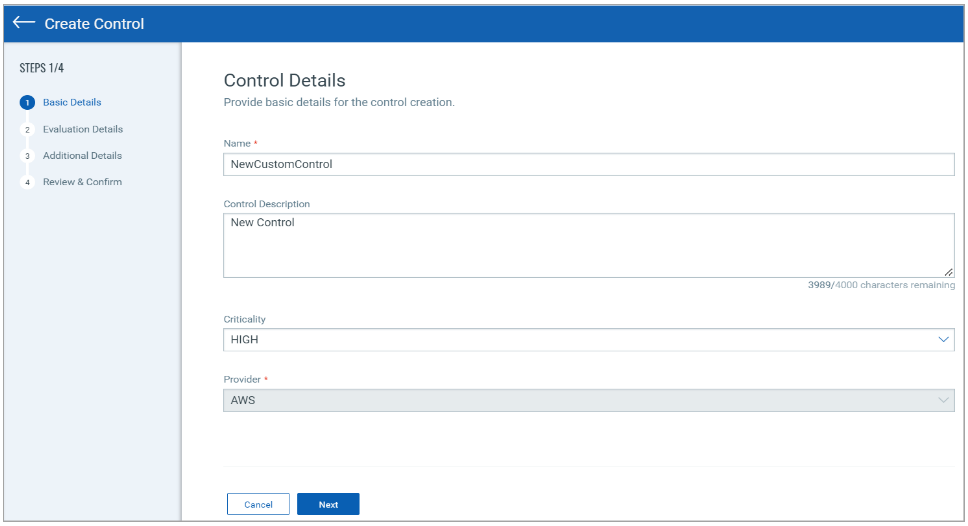
(2) Click Create Control > Run Time.



provider:"AWS"

| CID | CONTROL NAME | PLATFORM | EXECUTION TYPE | MODIFIED BY | CRITICALITY |
|---|---|---|---|---|---|
| 1 | Ensure multi-factor authentication (MFA) is enabled for all IAM users that ha... | aws | | SYSTEM | 🟥 High |

(3)Provide the basic details for the control such as Name, Description, select the Criticality and cloud Provider, and click Next.



Control Details

Provide basic details for the control creation.

Name *: NewCustomControl

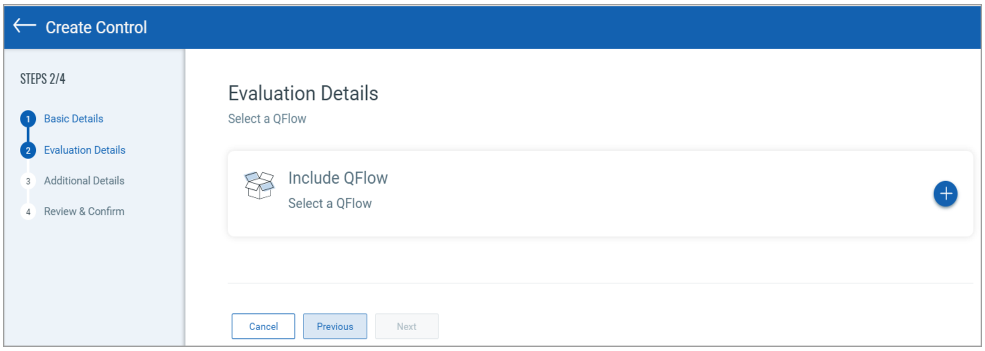
Control Description: New Control

3989/4000 characters remaining

Criticality: HIGH

Provider *: AWS

(4) Click ⊕ icon to include QFlow that is created in Qualys Flow app.



Evaluation Details

Select a QFlow

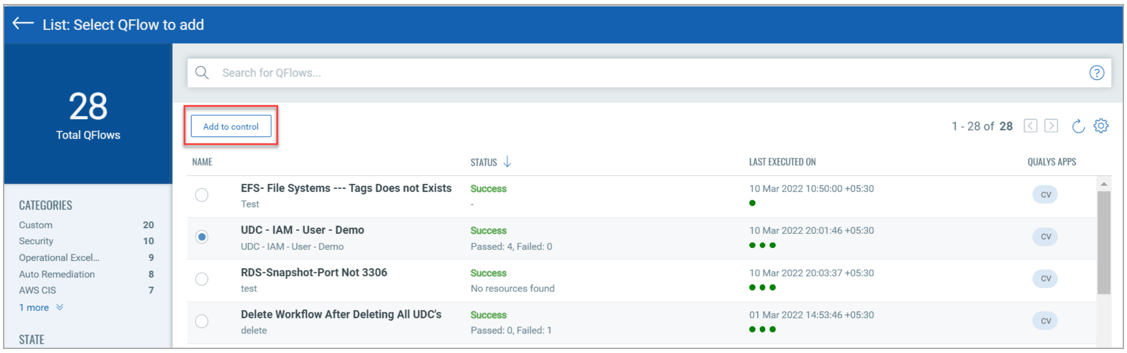
Include QFlow

Select a QFlow

If you do not have Read Permissions to Qualys Flow module, the ⊕ icon is not available. For details on permissions, refer to Manage Custom Control Permissions.

For more information on the Qualys Flow application, refer to Qualys Flow Getting Started Guide.

(5) Select the QFlow from the list and click Add to control.



CATEGORIES

| | |
|---|---|
| Custom | 20 |
| Security | 10 |
| Operational Excel... | 9 |
| Auto Remediation | 8 |
| AWS CIS | 7 |
| 1 more | |

| | NAME | STATUS | LAST EXECUTED ON | QUALYS APPS |
|---|---|---|---|---|
| ○ | EFS- File Systems --- Tags Does not Exists<br>Test | Success<br>- | 10 Mar 2022 10:50:00 +05:30<br>● | CV |
| ● | UDC - IAM - User - Demo<br>UDC - IAM - User - Demo | Success<br>Passed: 4, Failed: 0 | 10 Mar 2022 20:01:46 +05:30<br>● ● ● | CV |
| ○ | RDS-Snapshot-Port Not 3306<br>test | Success<br>No resources found | 10 Mar 2022 20:03:37 +05:30<br>● ● ● | CV |
| ○ | Delete Workflow After Deleting All UDC's<br>delete | Success<br>Passed: 0, Failed: 1 | 01 Mar 2022 14:53:46 +05:30<br>● ● ● | CV |

For the QFlow to be displayed in the list, in the Qualys Flow application, the CloudView node should be added while creating the QFlow and the QFlow should be deployed (enabled).

(6) The QFlow is added in the control, click Next.

(7) Fill in the additional details for your reference, like the objective of adding this control in Rationale, remediation steps if you want to suggest in Remediation, References and click Next.

(8) Review the details of your control and click Create Control.

Associate the control to a user-defined policy to be evaluated for the custom policy. For details on creating a custom policy, refer to Build Your Own Policy

## Controls Category: Execution Type

The column "Execution Type" on the Controls tab tells you the type of control. The categorization is done depending on the execution type of the control.

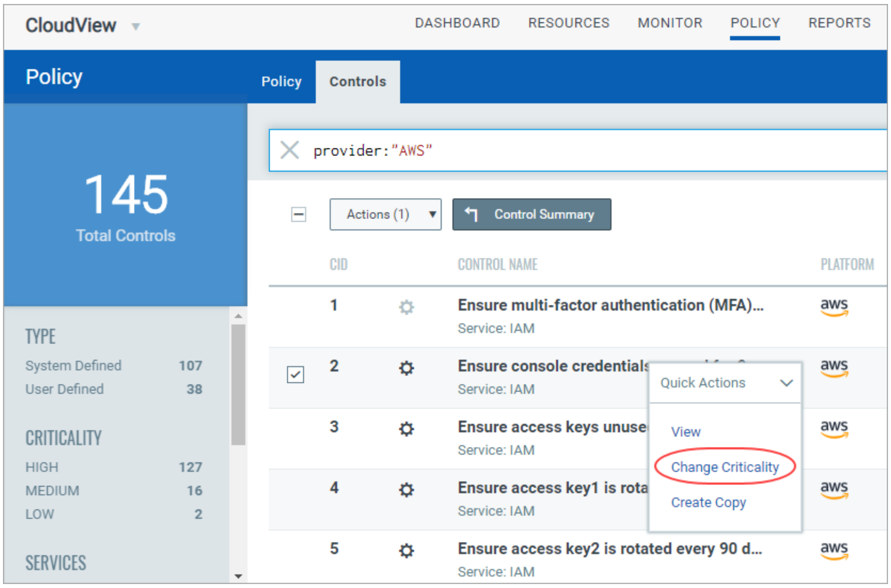
- Run Time Controls are controls for evaluations on deployed cloud resources.

- Build Time Controls are controls for cloud resources that reside within the IaC templates.

- Run & Build Time Controls are controls for evaluations on cloud resources in your environment and those which reside within the IaC templates.

## 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 |

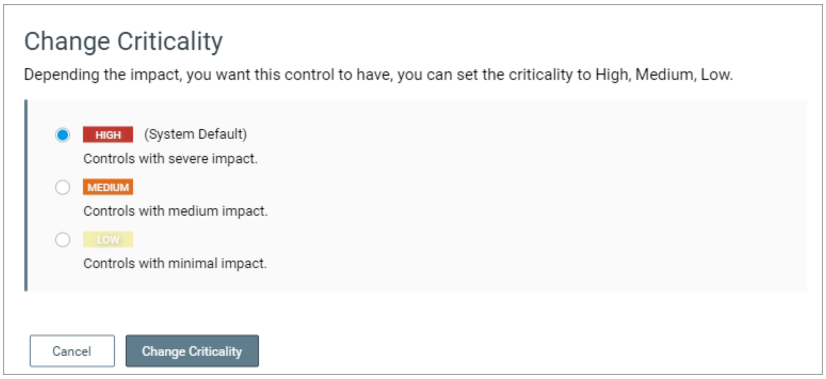
CRITICALITY

| | |
|---|---|
| HIGH | 127 |
| MEDIUM | 16 |
| LOW | 2 |

SERVICES

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

## Manage Custom Control Permissions

We have provided specific permissions for the user-defined controls.

By default, permission to create/edit user-defined controls 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 create or edit user-defined controls, a user with Manager role needs to assign permission to the sub users from the Administration utility.

### Permissions for user-defined controls

For creating copy of existing controls, editing, or deleting user-defined controls, you must enable the Manage Custom Control permission for the CloudView application.

With this permission, the user can perform the following actions:

- Create copy of run-time control for all Cloud providers.

- Delete user-defined controls for all Cloud providers. The controls can be QFlow-based controls or controls created as a copy of other run-time controls.

### Permissions for QFlow-based controls

For creating and editing QFlow-based controls, you must enable the Read Permissions for the Qualys Flow module in addition to the Manage Custom Controls permissions in the CloudView application.

With these permissions, the user can perform the following actions:

- Create QFlow-based controls for AWS cloud provider.

- Refresh QFlow while editing the control created for AWS cloud provider.

# 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.

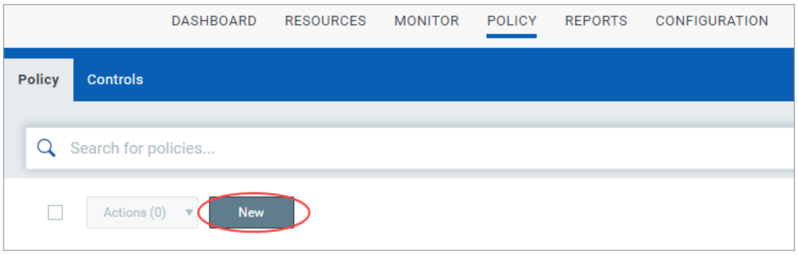
## System Defined Policy

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



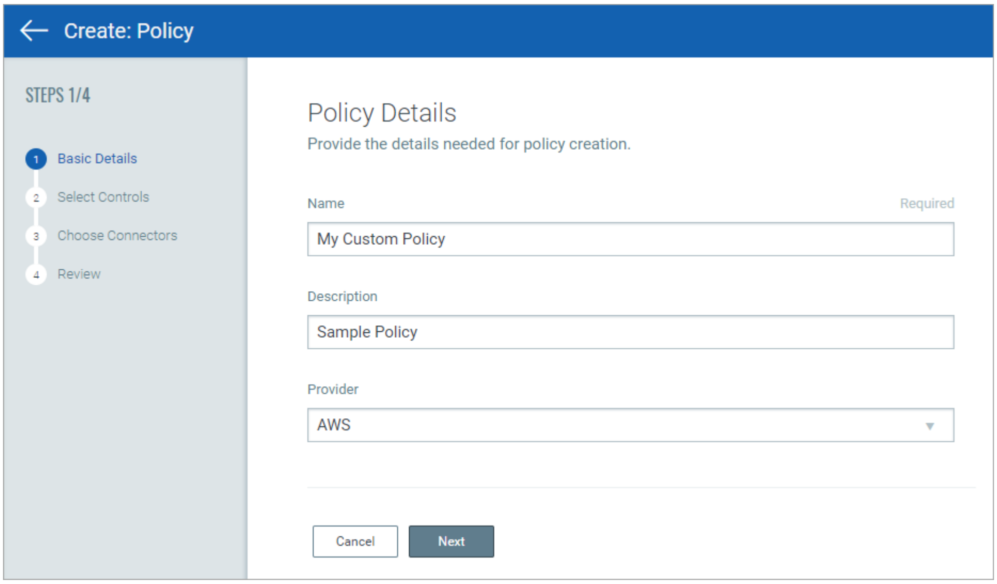
(2) Provide the basic details for the custom policy such as name, description, select the cloud provider, and select the type of execution controls to be included in the policy.

You could choose the controls depending on their execution type:

- Run Time: controls for evaluations on deployed cloud resources.

- Build Time: controls for evaluations on cloud resources within the IaC templates.

Click Next.



Policy Details

Provide the details needed for policy creation.

Name: My Custom Policy (Required)

Description: Sample Policy

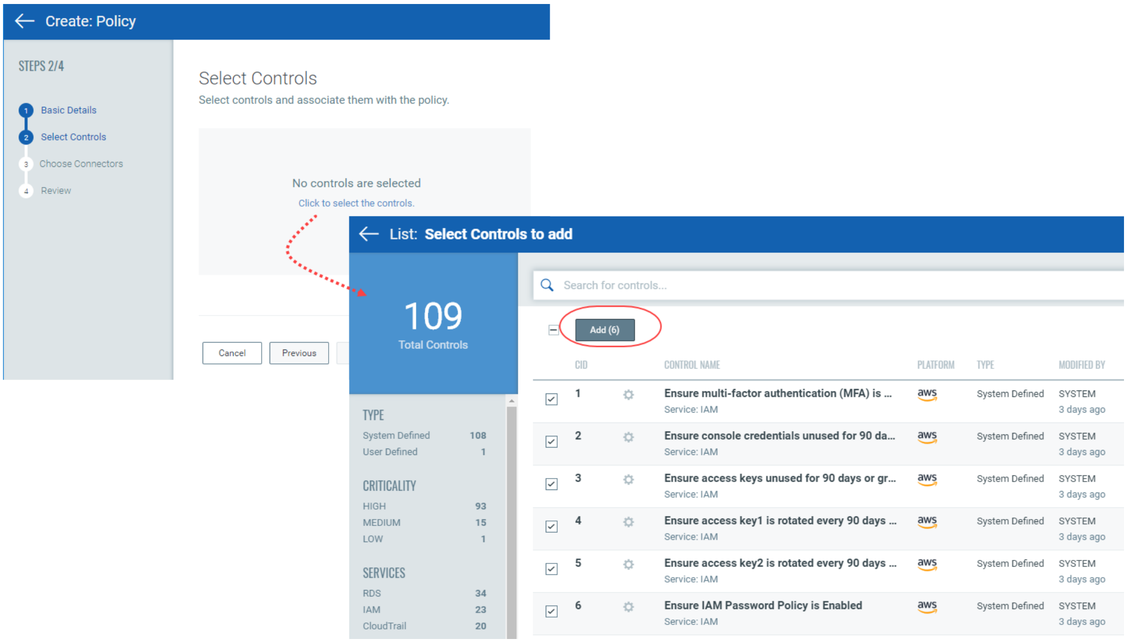
Provider: AWS

(3) Associating Controls:

- System Defined

-User defined

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



Select Controls

Select controls and associate them with the policy.

No controls are selected

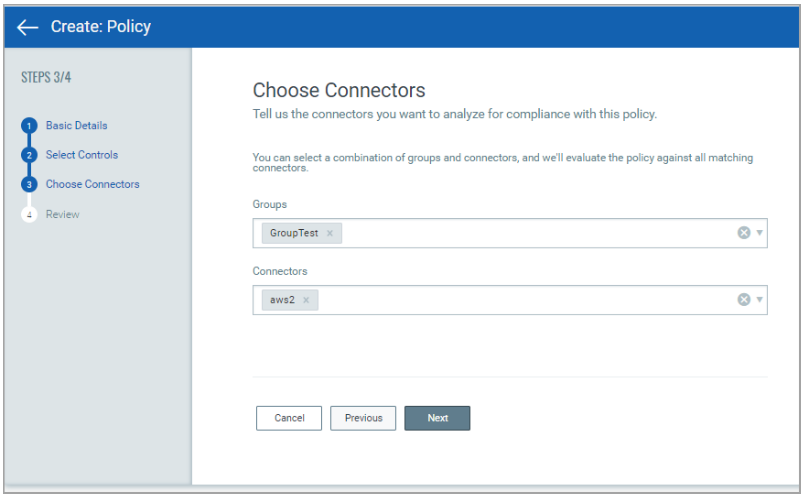
Click to select the controls.

| TYPE | |
|---|---|
| System Defined | 108 |
| User Defined | 1 |
| **CRITICALITY** | |
| HIGH | 93 |
| MEDIUM | 15 |
| LOW | 1 |
| **SERVICES** | |
| RDS | 34 |
| IAM | 23 |
| CloudTrail | 20 |

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



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 ×

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

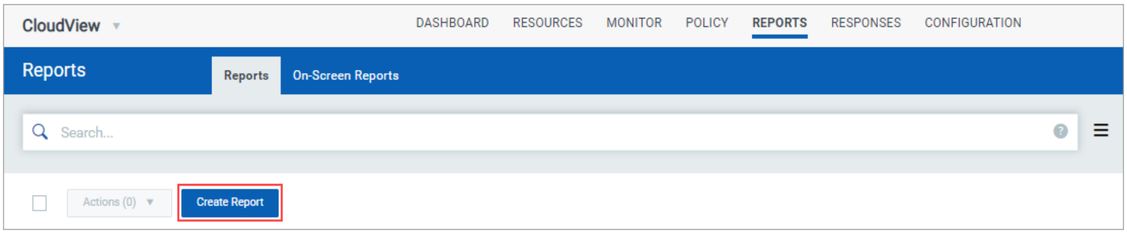
Use assessment reports to view the compliance of your resources for the defined policies in CloudView. You can use Qualys Query Language (QQL) to generate the on-demand assessment reports.

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.

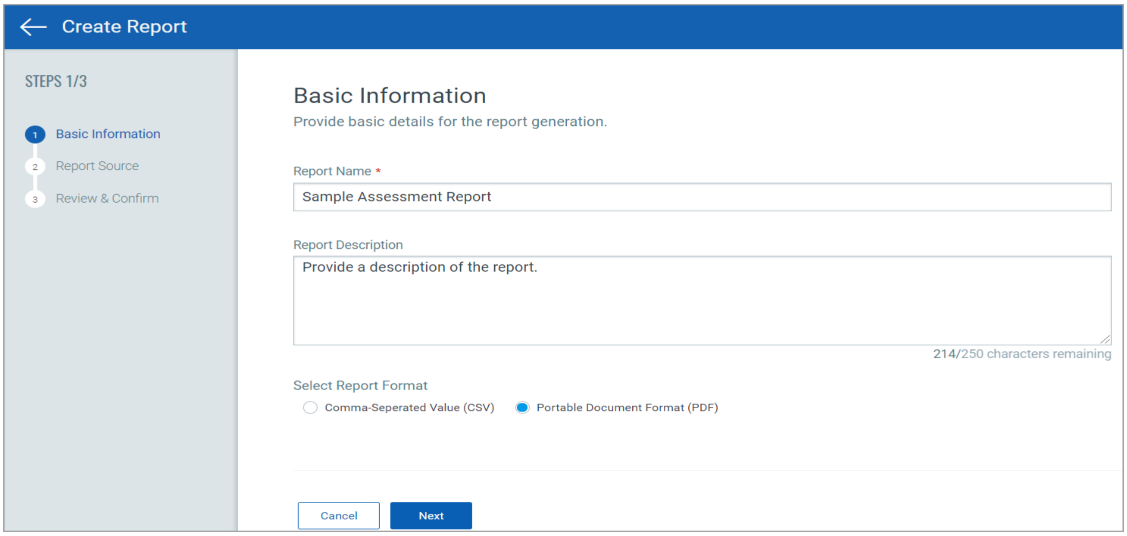
### Tell me the Steps

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.

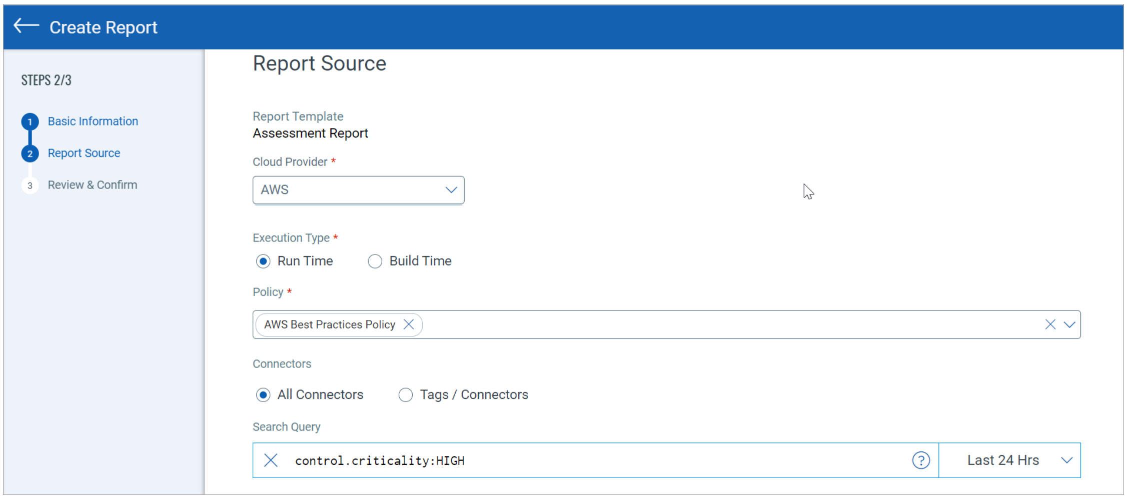
214/250 characters remaining

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

Execution Type *: ● Run Time ○ Build Time

Policy *: AWS Best Practices Policy

Connectors: ● All Connectors ○ Tags / Connectors

Search Query: `control.criticality:HIGH` Last 24 Hrs

5) Select the execution type of the controls

6) 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.

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

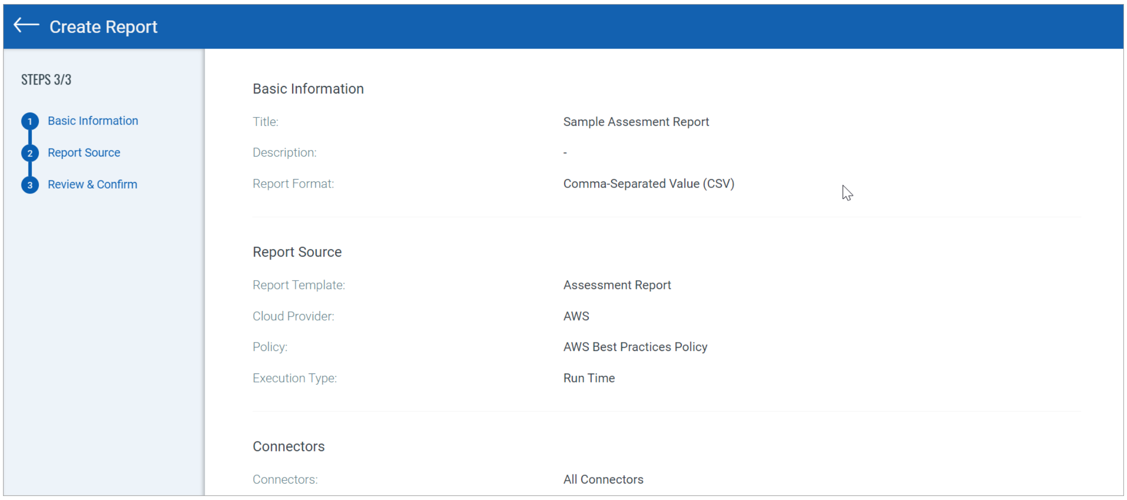
8) Use `evaluatedOn` search query token to specify the date criteria for report you want to generate.

9) 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.

10) 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.

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



Basic Information

| | |
|---|---|
| Title: | Sample Assesment Report |
| Description: | - |
| Report Format: | Comma-Separated Value (CSV) |

Report Source

| | |
|---|---|
| Report Template: | Assessment Report |
| Cloud Provider: | AWS |
| Policy: | AWS Best Practices Policy |
| Execution Type: | Run Time |

Connectors

| | |
|---|---|
| Connectors: | All Connectors |

## 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.

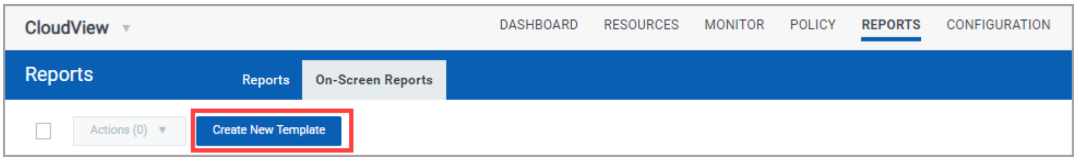
Launch the Mandate Based Report to view the compliance posture of the organization in terms of the underlying Security baseline against selected Mandates. This allows you to choose any one mandates you have to comply with and get a view of compliance posture in terms of their selected policies.

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

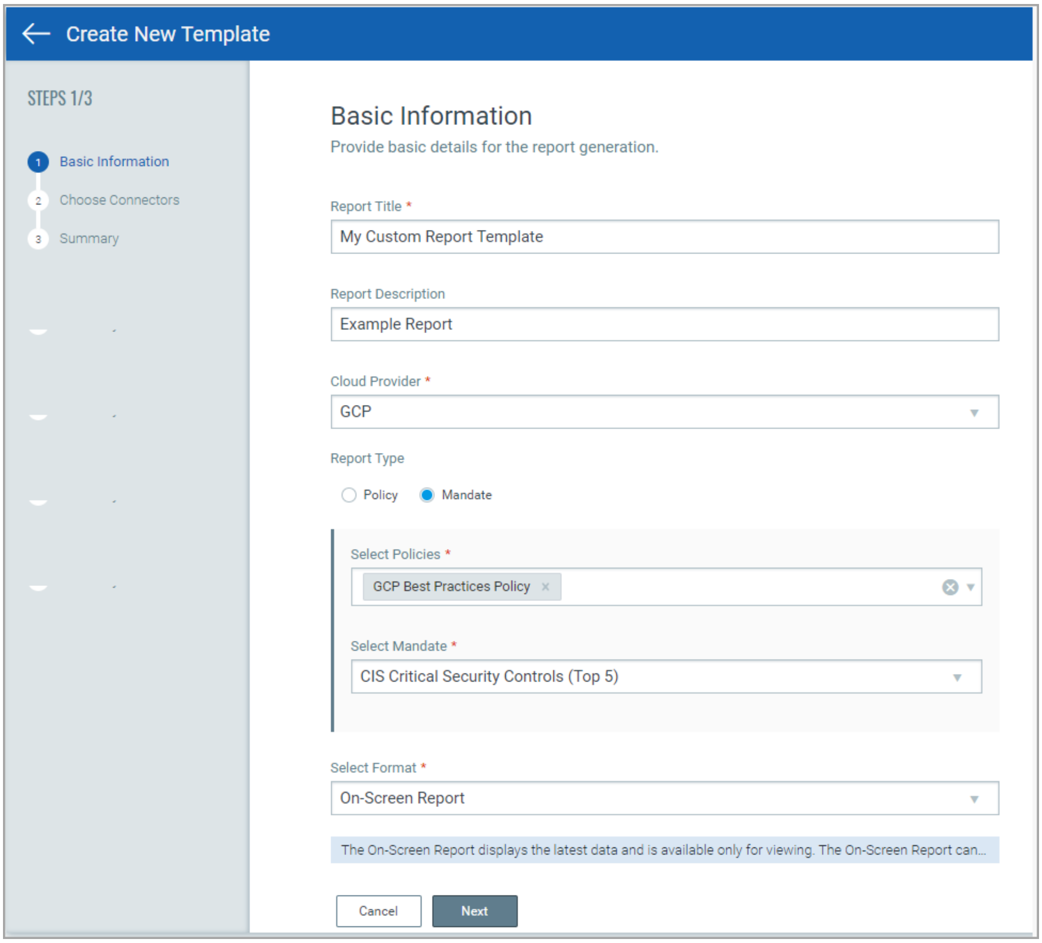
### Tell me the Steps

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.



Create New Template

STEPS 1/3

1 Basic Information
2 Choose Connectors
3 Summary

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...

Cancel Next

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

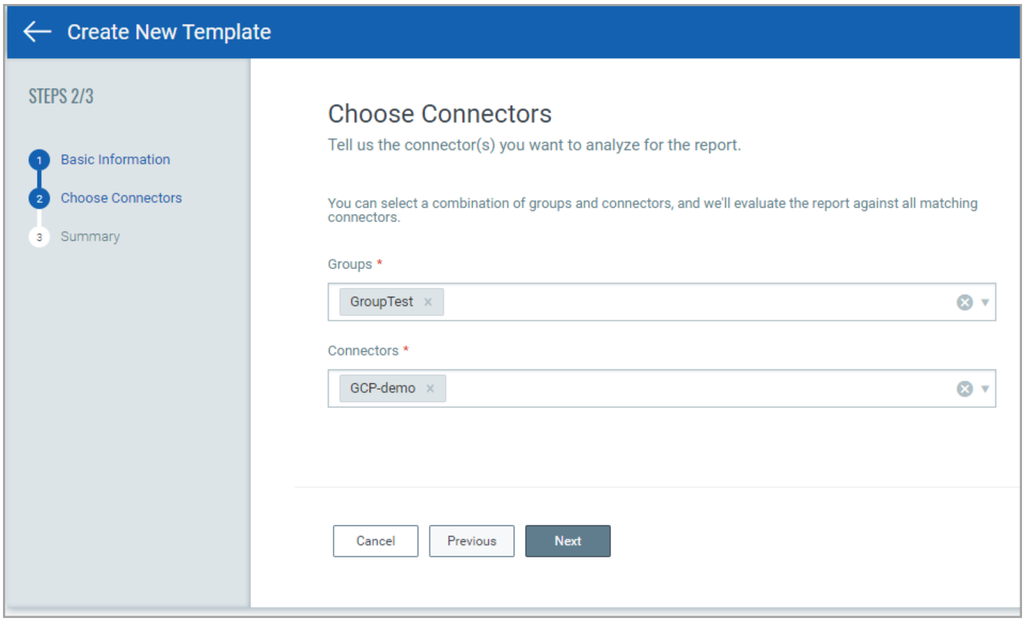
4) Select the Mandate in the report type and then click Next.

-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 execution type

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



Choose Connectors

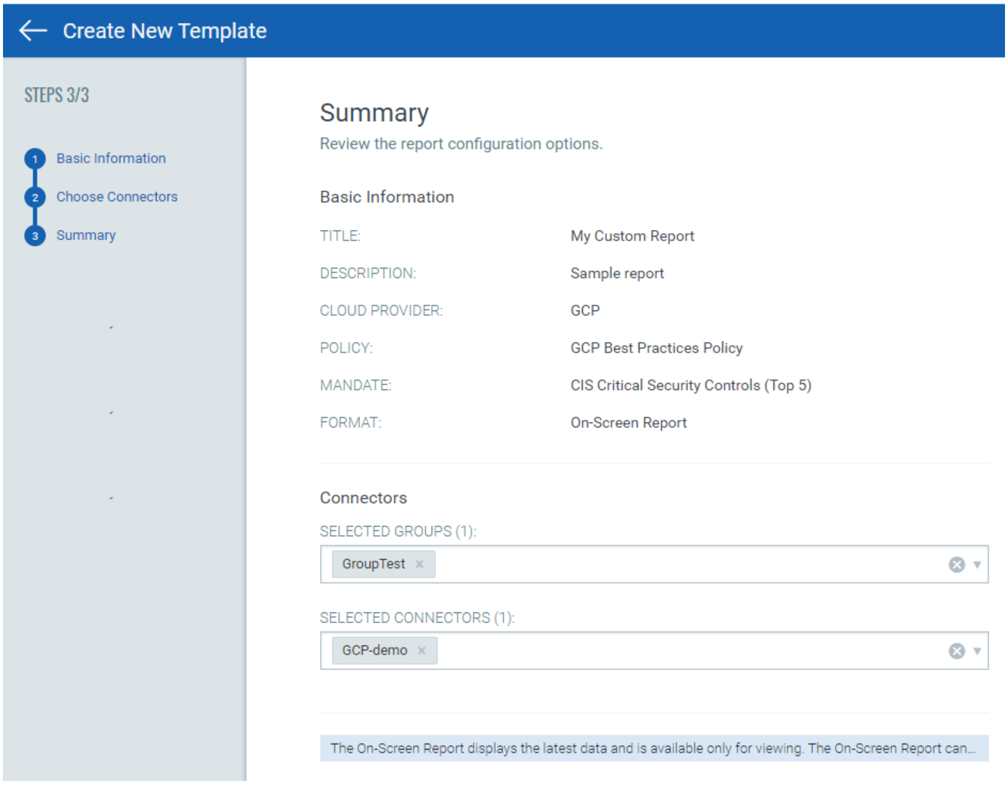
Tell us the connector(s) you want to analyze for the report.

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

Groups *: GroupTest ×

Connectors *: GCP-demo ×

7) 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 |

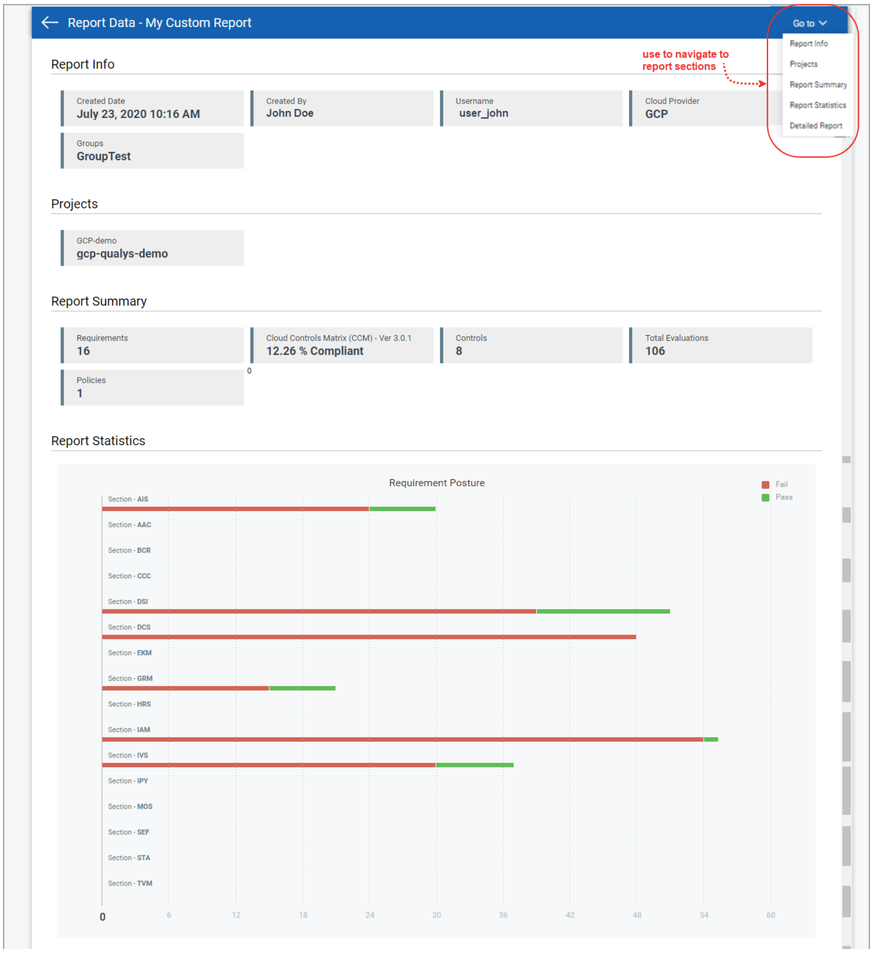
Connectors

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

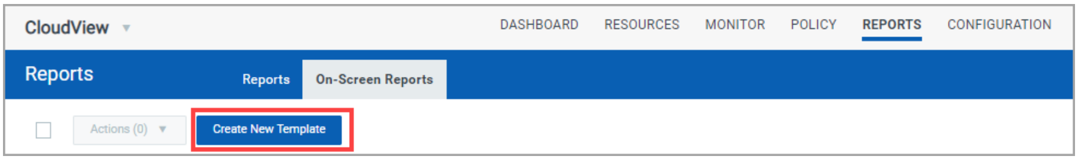
Report Statistics

## Policy Based Report

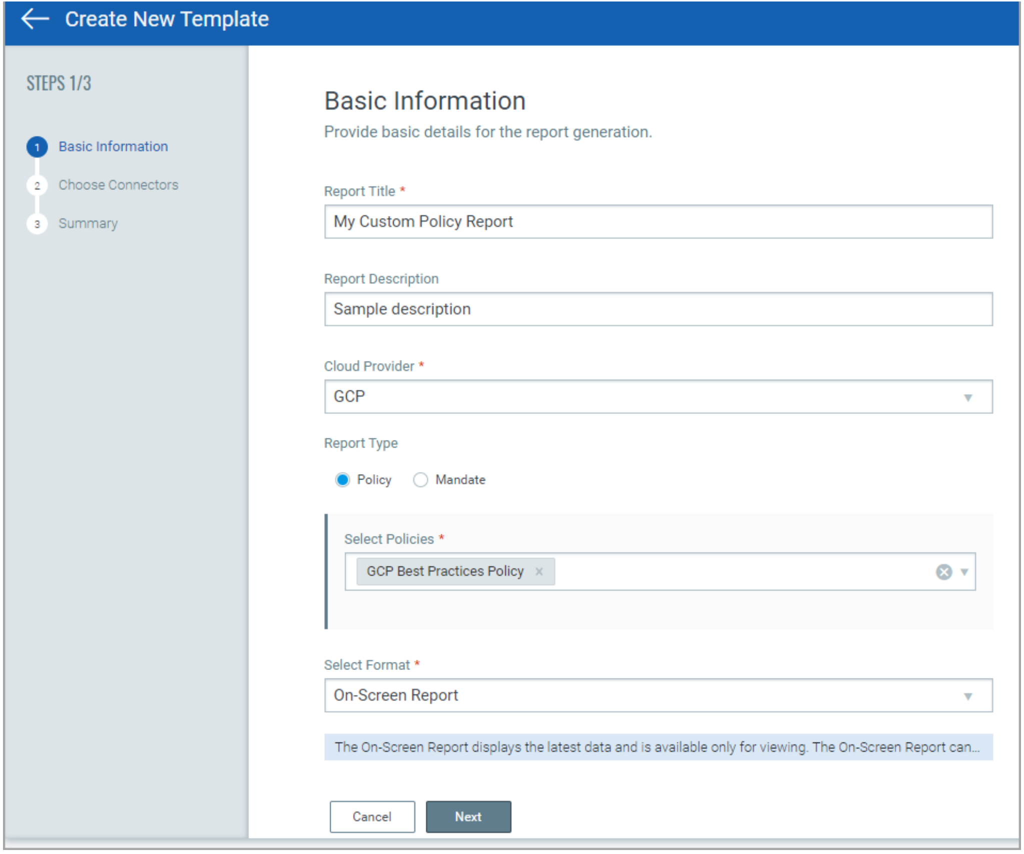
Policies are set of controls. We provide ability to generate policy specific compliance report. We support report generation of policies for all the cloud providers we support: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

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.



Create New Template

STEPS 1/3

1 Basic Information
2 Choose Connectors
3 Summary

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

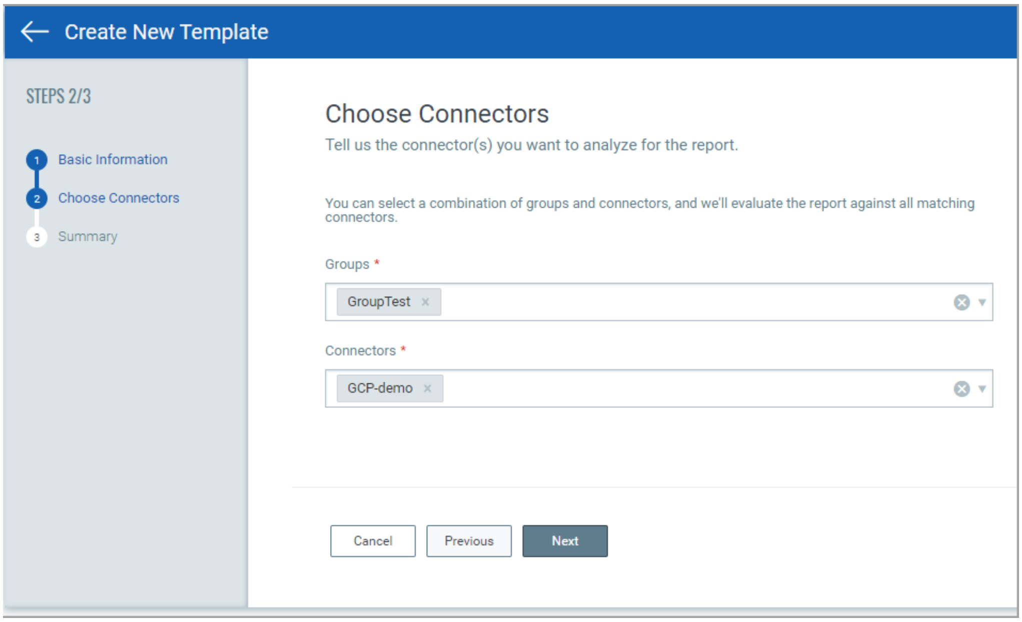
The On-Screen Report displays the latest data and is available only for viewing. The On-Screen Report can...

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.

5) Select runtime or buildtime in execution type.

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



Create New Template

Choose Connectors

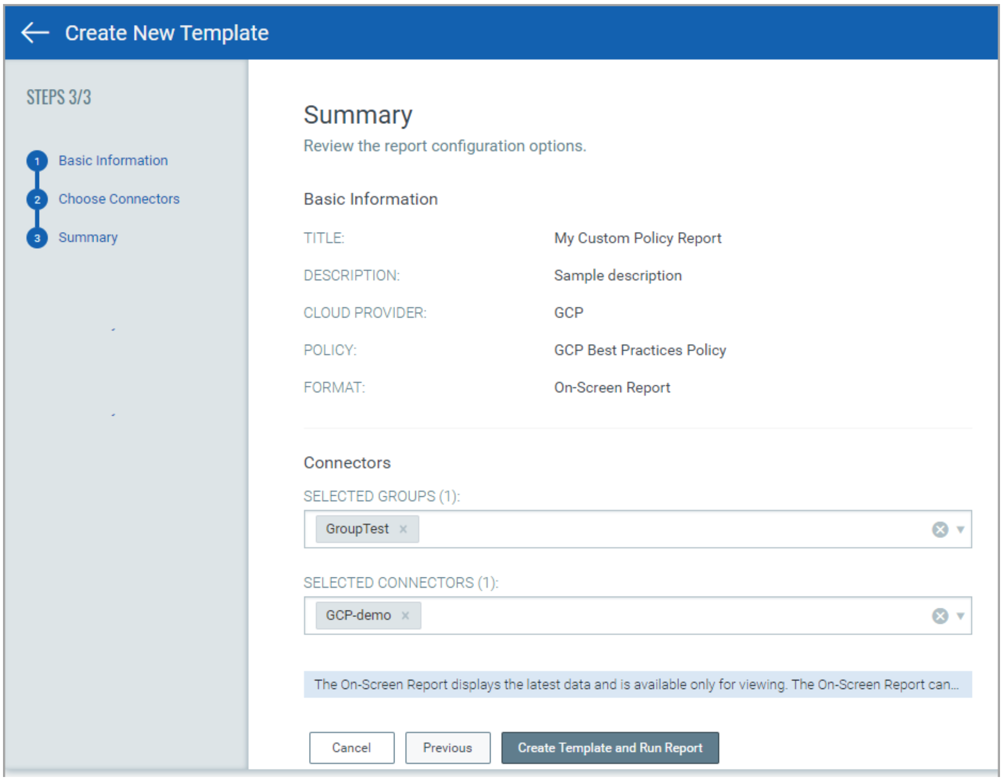
Tell us the connector(s) you want to analyze for the report.

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

Groups *: GroupTest

Connectors *: GCP-demo

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



Create New Template

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 |

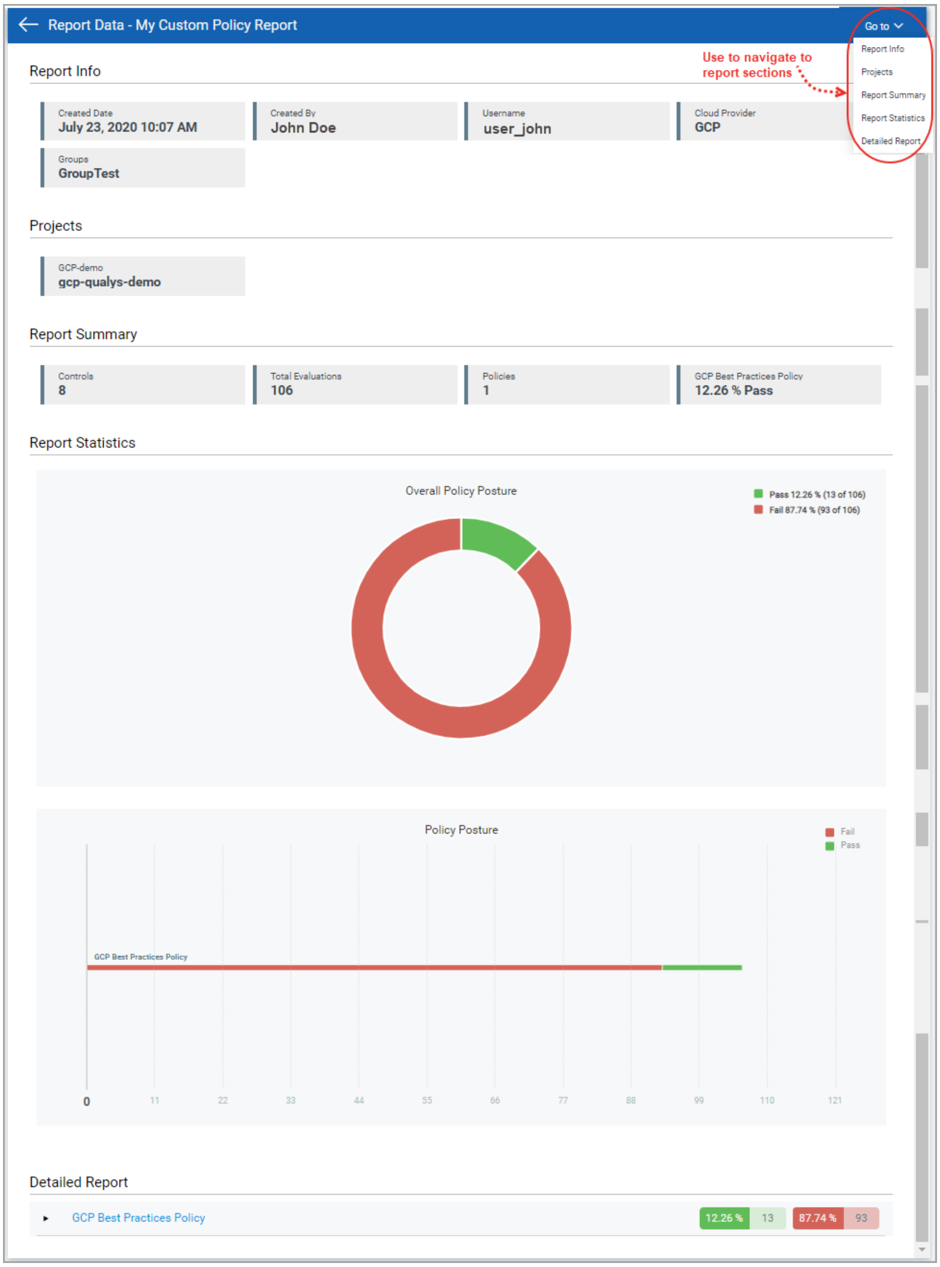
Connectors

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



Use to navigate to report sections

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

Detailed Report

▸ GCP Best Practices Policy 12.26 % 13 87.74 % 93

## List of Mandates

We support the following mandates for report generation.

1. ISO/IEC 27001:2013
2. Cloud Controls Matrix (CCM)
3. NERC Critical Infrastructure Protection (CIP)

**4** Health Insurance Portability and Accountability (HIPAA) Security Rule 45 CFR Parts 160/164, Subparts A/C:1996

**5** ANSSI 40 Essential Measures for a Healthy Network

**6** The Australian Signals Directorate - The Essential 8 Strategies (ASD 8)

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

**8** NESA UAE Information Assurance Standards (IAS)

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

**10** IRDAI Guidelines On Information and Cyber Security for Insurers

**11** General Data Protection Regulation (GDPR)

**12** Minimum Acceptable Risk Standards for Exchanges (MARS-E)

**13** NCSC Basic Cyber Security Controls (BCSC)

**14** IRS Publication 1075

**15** NIST Cyber Security Framework (CSF)

**16** Sarbanes-Oxley Act: IT Security

**17** Monetary Authority of Singapore (MAS) - Notice 834: Cyber Hygiene Practices

**18** NIST Special Publication 800-171

**19** CIS Controls Version 8

**20** Criminal Justice Information Services (CJIS) Security Policy

**21** Cybersecurity Maturity Model Certification (CMMC) Level 1

**22** Cybersecurity Maturity Model Certification (CMMC) Level 2

**23** Cybersecurity Maturity Model Certification (CMMC) Level 4

**24** Cybersecurity Maturity Model Certification (CMMC) Level 5

**25** Cybersecurity Maturity Model Certification (CMMC) Level 3

**26** Payment Card Industry Data Security Standard (PCI-DSS) v3.2.1

**27** SWIFT Customer Security Controls Framework - Customer Security Programme v2019

**28** Federal Risk and Authorization Management Program (FedRAMP H) - High Security Baseline

**29** Federal Risk and Authorization Management Program (FedRAMP M) - Moderate Security Baseline

**30** NIST 800-53 (Special Publication)

# 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

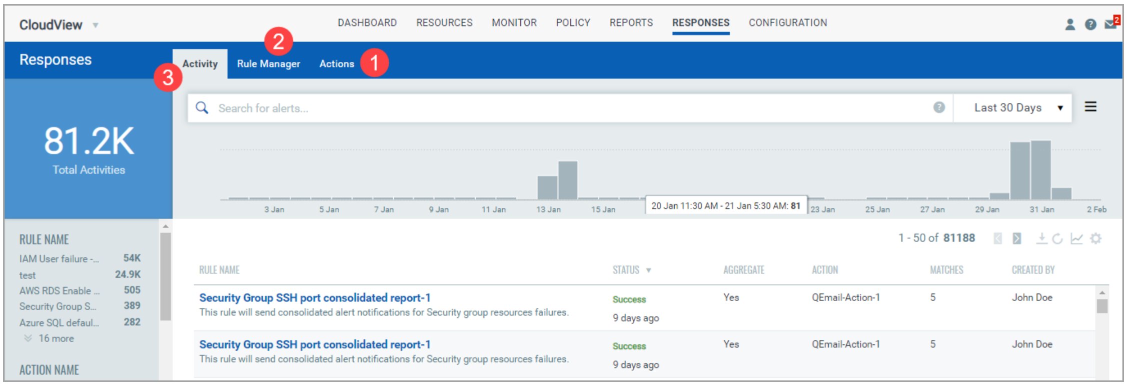
- Evaluation result of highly critical controls

- 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<br>This rule will send consolidated alert notifications for Security group resources failures. | Success<br>9 days ago | Yes | QEmail-Action-1 | 5 | John Doe |
| Security Group SSH port consolidated report-1<br>This rule will send consolidated alert notifications for Security group resources failures. | Success<br>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:

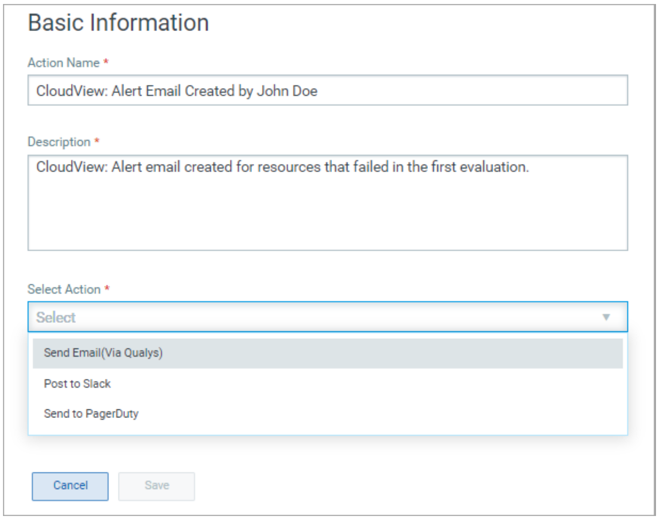
In the Basic Information section, provide a name and description for the action. Select an action to specify the mode of sending alert messages by either Email (Via Qualys)/Send Email (Your SMTP), Post to Slack or Send to Pager Duty.

(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

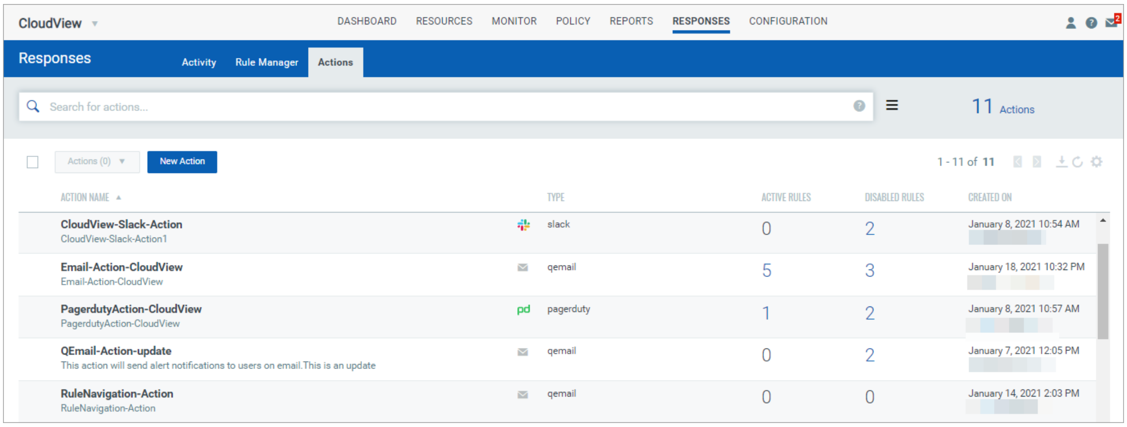
Description *
CloudView: Alert email created for resources that failed in the first evaluation.

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

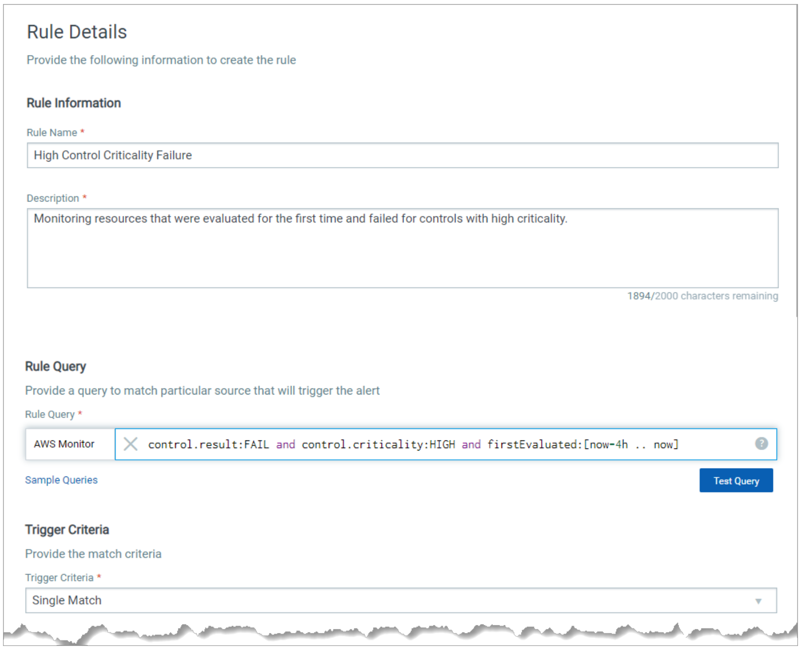
## Create New Rule

(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

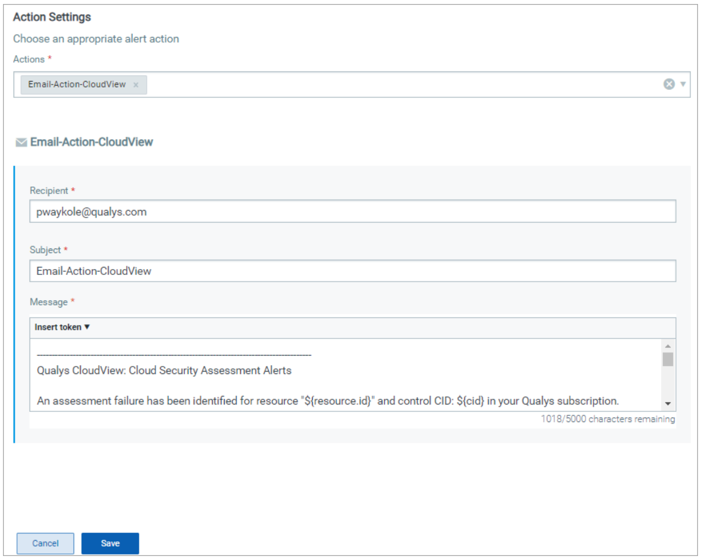
```
control.result:FAIL and control.criticality:HIGH and firstEvaluated:[now-4h .. now]
```

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 *
Insert token ▾

----------------------------------------------------------------------------------------

Qualys CloudView: Cloud Security Assessment Alerts

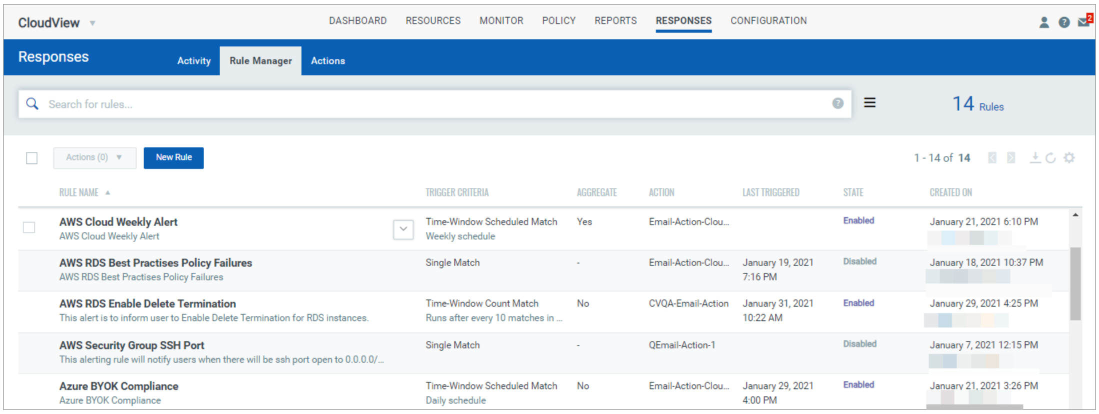
An assessment failure has been identified for resource "${resource.id}" and control CID: ${cid} in your Qualys subscription.

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<br>AWS Cloud Weekly Alert | Time-Window Scheduled Match<br>Weekly schedule | Yes | Email-Action-Clou... | | Enabled | January 21, 2021 6:10 PM<br>[redacted] |
| | AWS RDS Best Practises Policy Failures<br>AWS RDS Best Practises Policy Failures | Single Match | - | Email-Action-Clou... | January 19, 2021<br>7:16 PM | Disabled | January 18, 2021 10:37 PM<br>[redacted] |
| | AWS RDS Enable Delete Termination<br>This alert is to inform user to Enable Delete Termination for RDS instances. | Time-Window Count Match<br>Runs after every 10 matches in ... | No | CVQA-Email-Action | January 31, 2021<br>10:22 AM | Enabled | January 29, 2021 4:25 PM<br>[redacted] |
| | AWS Security Group SSH Port<br>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<br>[redacted] |
| | Azure BYOK Compliance<br>Azure BYOK Compliance | Time-Window Scheduled Match<br>Daily schedule | No | Email-Action-Clou... | January 29, 2021<br>4:00 PM | Enabled | January 21, 2021 3:26 PM<br>[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
```

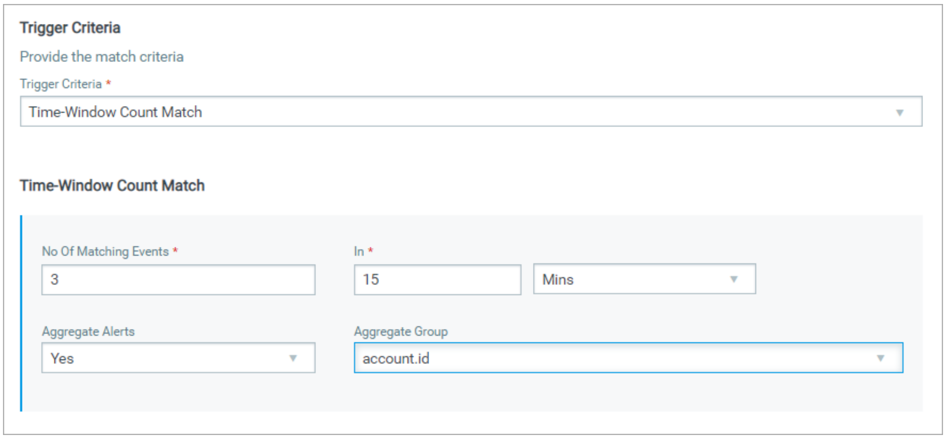
Scenario 3: Rules with specific action triggered to specific recipient.

```
    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

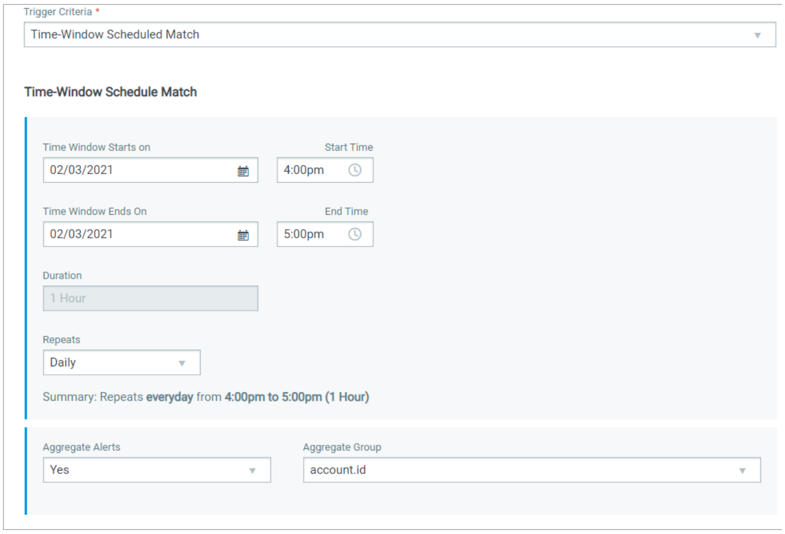
No Of Matching Events *: 3

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

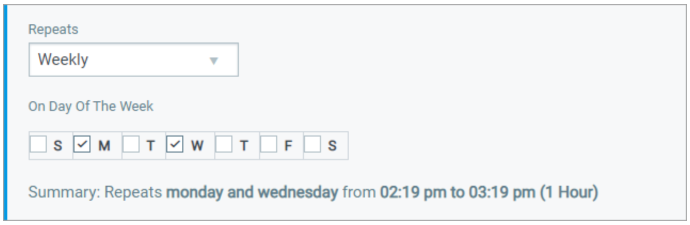
Repeats: Daily

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

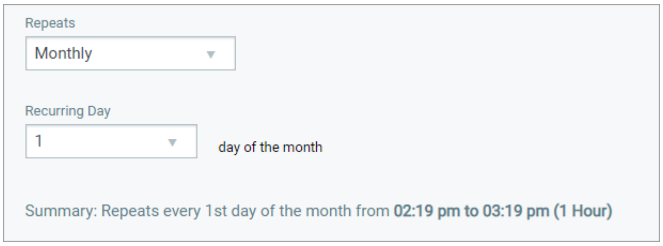
Weekly ▾

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.

# 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

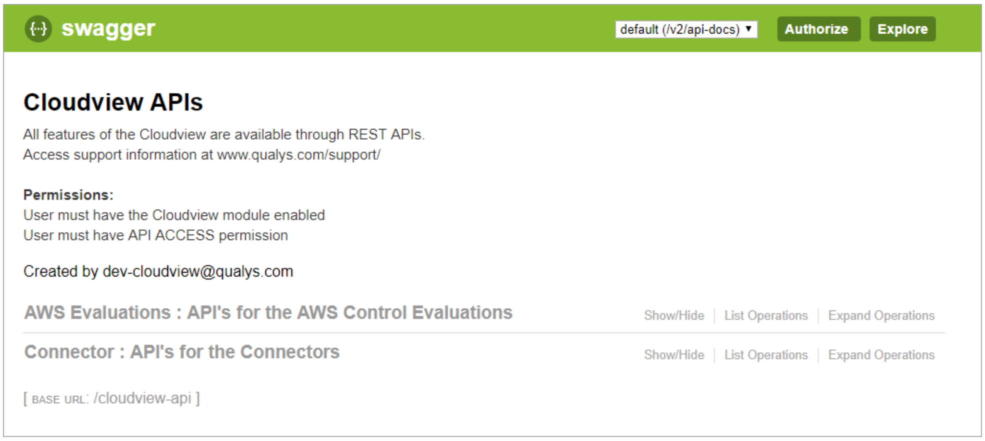
Swagger is a widely-adopted specification that allows for programmatically describing REST APIs. The Swagger UI provides all the details about the APIs and how to invoke them. This includes information like the HTTP verbs to use (GET, POST, PUT, etc.), the URL paths, allowable parameters and types, and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

# 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: 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: AWS

You can enable remediation when you create AWS connectors or edit existing connectors. Refer to the Connector online help for more information on enabling remediation for new connectors.

## Configure Remediation: Microsoft Azure

Configure Microsoft Azure connectors for gathering resource information from your Microsoft Azure account. Refer to the Connector online help for more information on enabling remediation for new connectors.

### 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.

## Configure Remediation: GCP

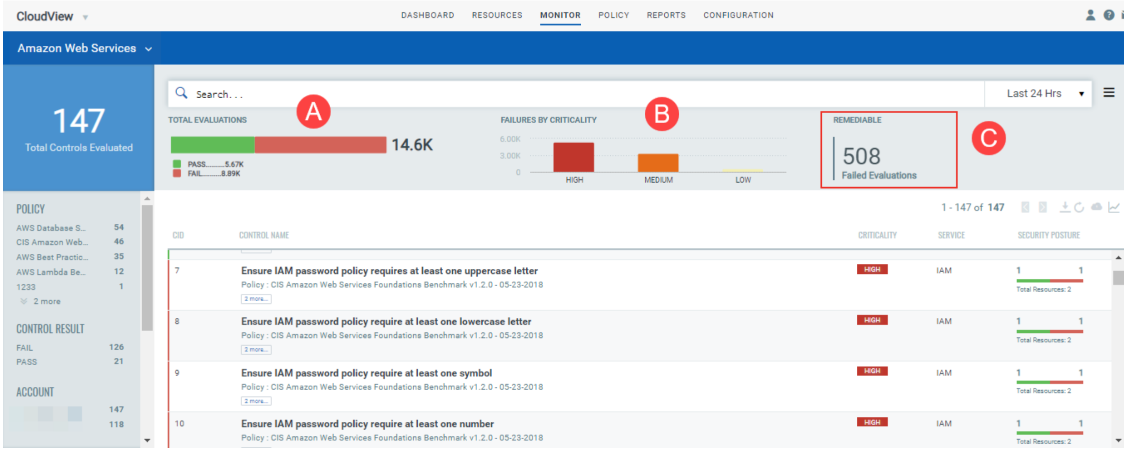
Configure a Google Cloud Platform (GCP) connector for gathering resource information from your Google Cloud Platform project. Refer to the Connector online help for more information on enabling remediation for new connectors.

## 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.



POLICY

| | |
|---|---|
| AWS Database S... | 54 |
| CIS Amazon Web... | 46 |
| AWS Best Practic... | 35 |
| AWS Lambda Be... | 12 |
| 1233 | 1 |

2 more

CONTROL RESULT

| | |
|---|---|
| FAIL | 126 |
| PASS | 21 |

ACCOUNT

| | |
|---|---|
| [redacted] | 147 |
| [redacted] | 118 |

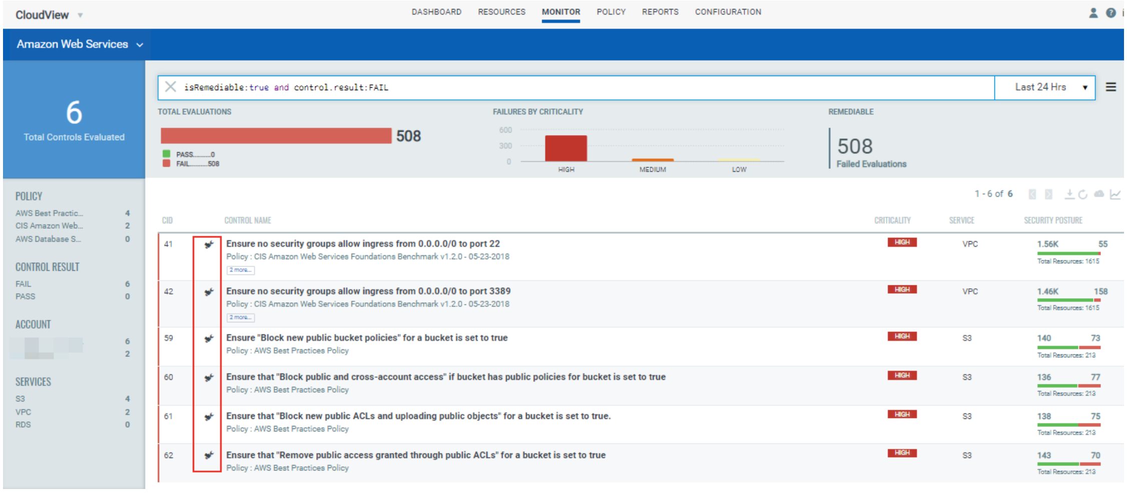
| CID | CONTROL NAME | CRITICALITY | SERVICE | SECURITY POSTURE |
|---|---|---|---|---|
| 7 | Ensure IAM password policy requires at least one uppercase letter<br>Policy : CIS Amazon Web Services Foundations Benchmark v1.2.0 - 05-23-2018<br>2 more... | HIGH | IAM | 1 1<br>Total Resources: 2 |
| 8 | Ensure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

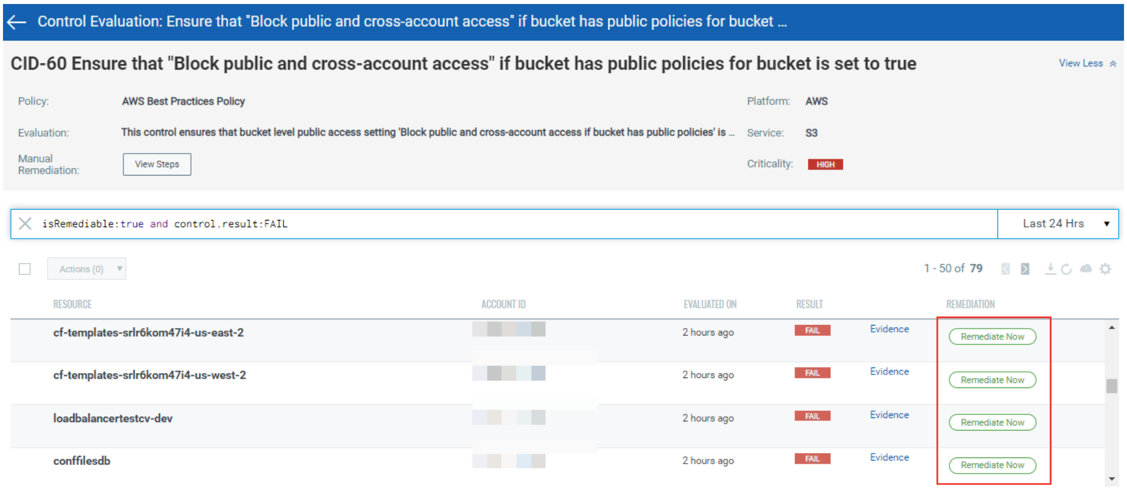
| | |
|---|---|
| [redacted] | 6 |
| [redacted] | 2 |

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

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 | Platform: | AWS |
| Evaluation: | This control ensures that bucket level public access setting 'Block public and cross-account access if bucket has public policies' is ... | Service: | S3 |
| Manual Remediation: | View Steps | Criticality: | HIGH |

```
isRemediable:true and control.result:FAIL
```

Last 24 Hrs

1 - 50 of 79

| 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.

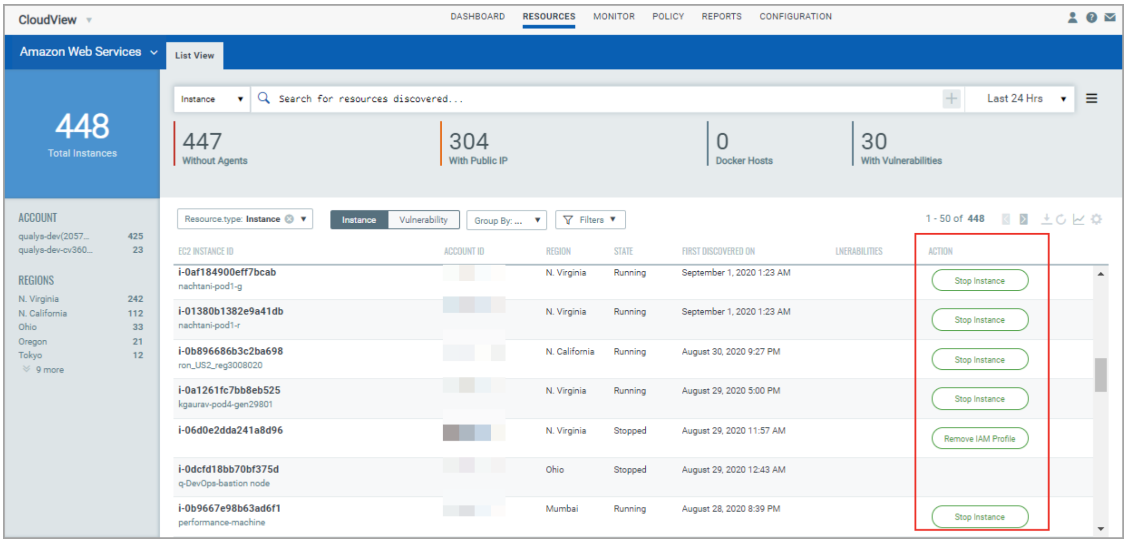
## Actions for Cloud Resources (AWS)

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<br>nachtani-pod1-g | [redacted] | N. Virginia | Running | September 1, 2020 1:23 AM | | Stop Instance |
| i-01380b1382e9a41db<br>nachtani-pod1-r | [redacted] | N. Virginia | Running | September 1, 2020 1:23 AM | | Stop Instance |
| i-0b896686b3c2ba698<br>ron_US2_reg3008020 | [redacted] | N. California | Running | August 30, 2020 9:27 PM | | Stop Instance |
| i-0a1261fc7bb8eb525<br>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<br>q-DevOps-bastion node | [redacted] | Ohio | Stopped | August 29, 2020 12:43 AM | | |
| i-0b9667e98b63ad6f1<br>performance-machine | [redacted] | Mumbai | Running | August 28, 2020 8:39 PM | | Stop Instance |

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

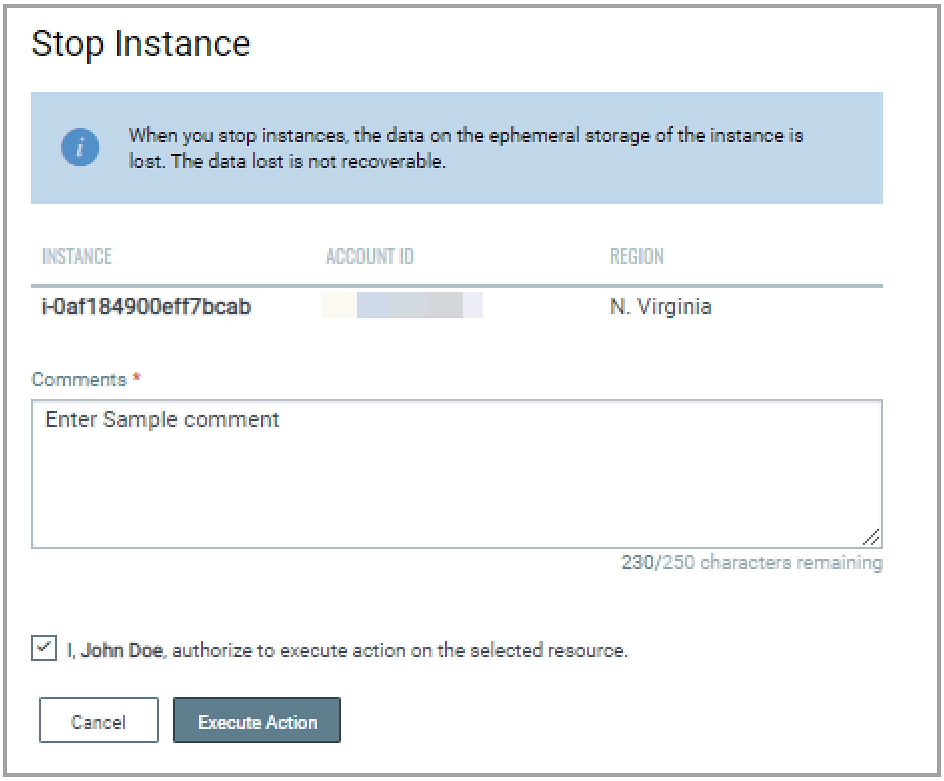
We support the following actions for AWS Instance resources:

## 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

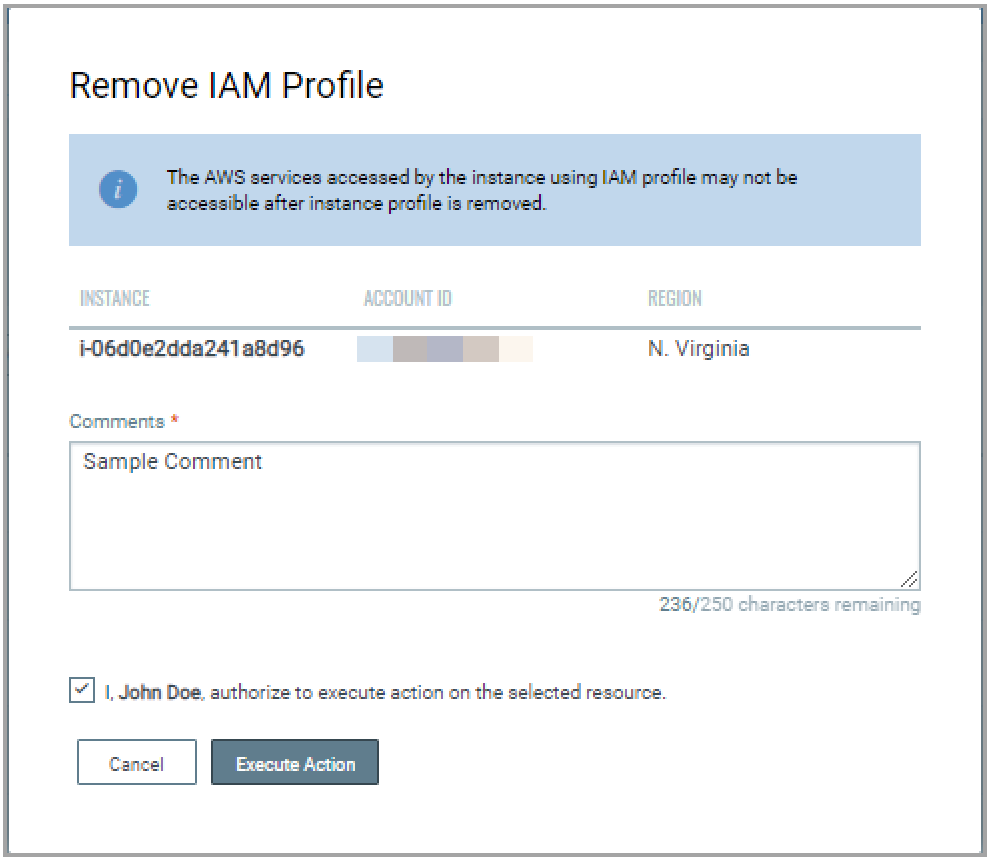
☑ I, **John Doe**, authorize to execute action on the selected resource.

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.

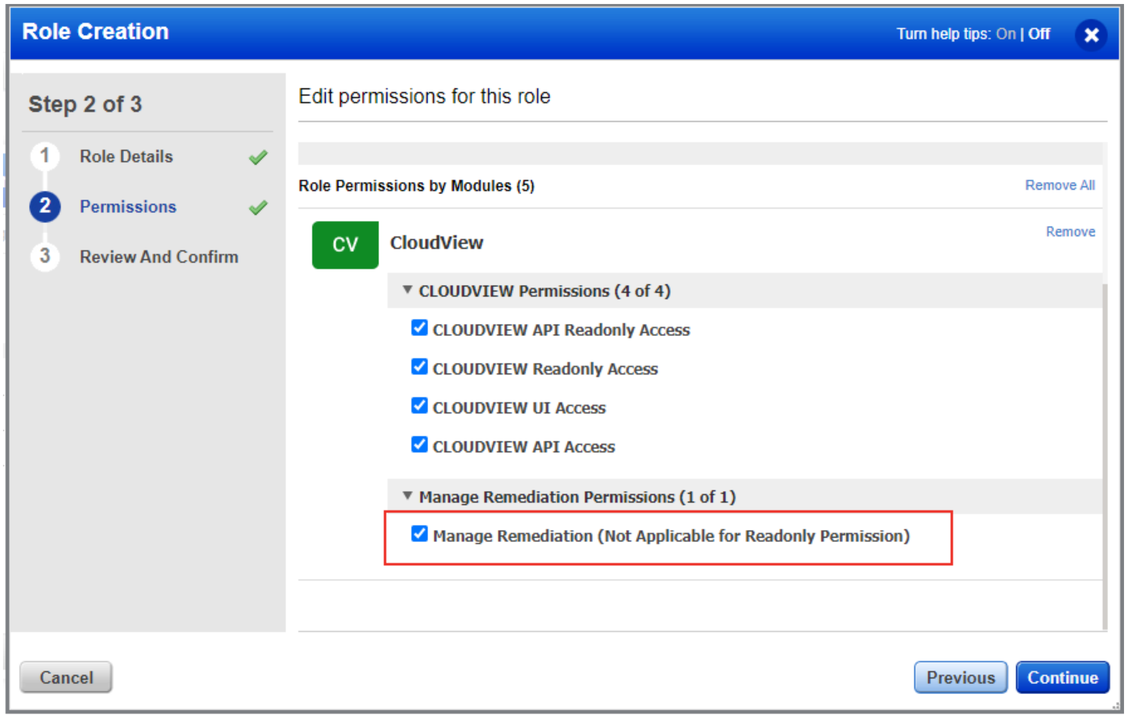
Click Execute Action.

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.



Edit permissions for this role

Role Permissions by Modules (5)

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.

# 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.

## Download Datalist

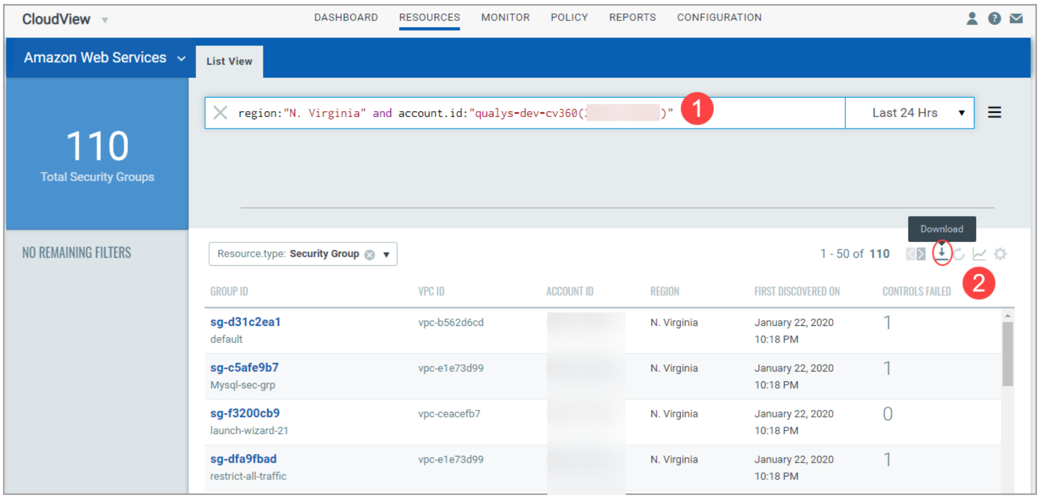
By downloading datalist to your local system you can easily manage the list outside of the Qualys platform and share them with other users. You can download results in CSV format.

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.



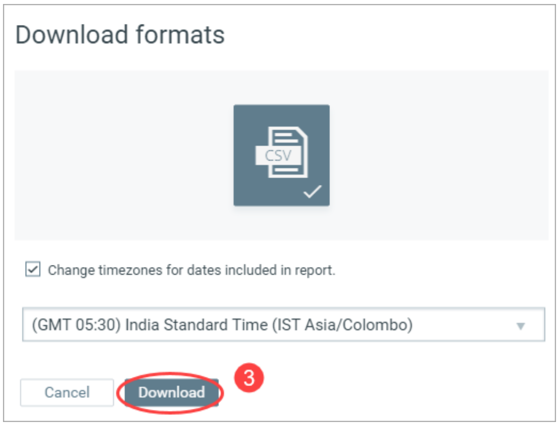
region:"N. Virginia" and account.id:"qualys-dev-cv360([redacted])"

Resource.type: Security Group

1 - 50 of 110

| GROUP ID | VPC ID | ACCOUNT ID | REGION | FIRST DISCOVERED ON | CONTROLS FAILED |
|---|---|---|---|---|---|
| sg-d31c2ea1<br>default | vpc-b562d6cd | [redacted] | N. Virginia | January 22, 2020<br>10:18 PM | 1 |
| sg-c5afe9b7<br>Mysql-sec-grp | vpc-e1e73d99 | [redacted] | N. Virginia | January 22, 2020<br>10:18 PM | 1 |
| sg-f3200cb9<br>launch-wizard-21 | vpc-ceacefb7 | [redacted] | N. Virginia | January 22, 2020<br>10:18 PM | 0 |
| sg-dfa9fbad<br>restrict-all-traffic | vpc-e1e73d99 | [redacted] | N. Virginia | January 22, 2020<br>10:18 PM | 1 |

3) Click Download. That's it!



Download formats

☑ Change timezones for dates included in report.

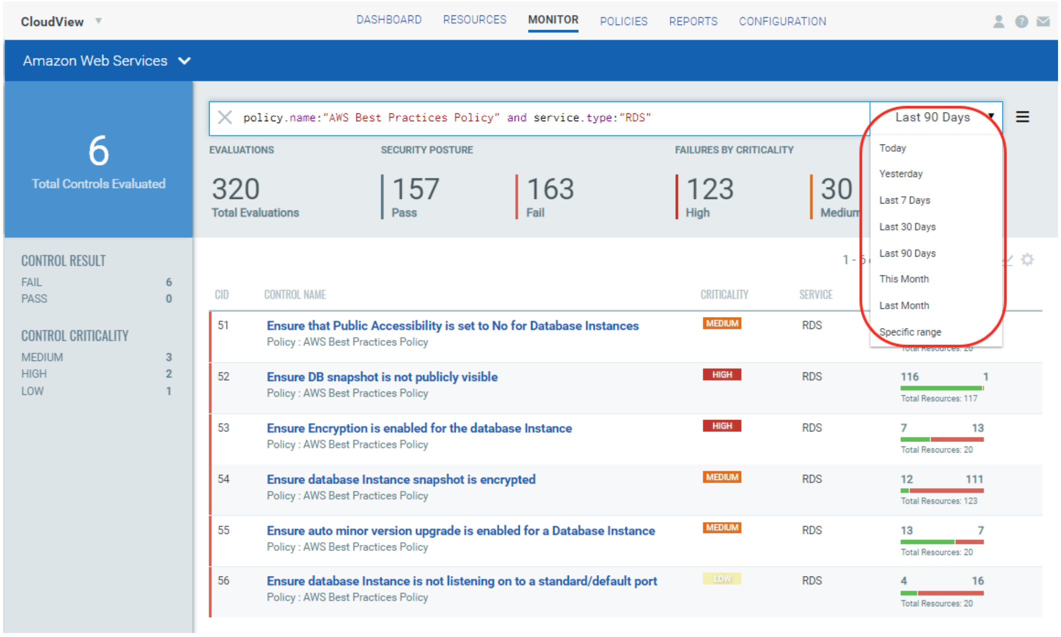
(GMT 05:30) India Standard Time (IST Asia/Colombo) ▾

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"
```

6 Total Controls Evaluated

EVALUATIONS: 320 Total Evaluations

SECURITY POSTURE: 157 Pass, 163 Fail

FAILURES BY CRITICALITY: 123 High, 30 Medium

CONTROL RESULT

| | |
|---|---|
| FAIL | 6 |
| PASS | 0 |

CONTROL CRITICALITY

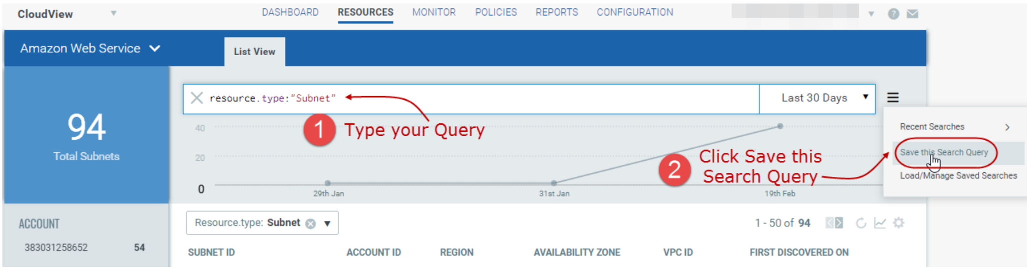
| | |
|---|---|
| MEDIUM | 3 |
| HIGH | 2 |
| LOW | 1 |

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



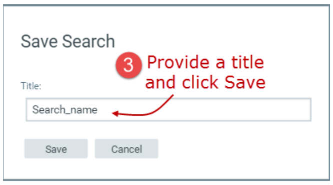
`resource.type:"Subnet"`

Resource.type: **Subnet**

1 Type your Query

2 Click Save this Search Query

Give your search a title.

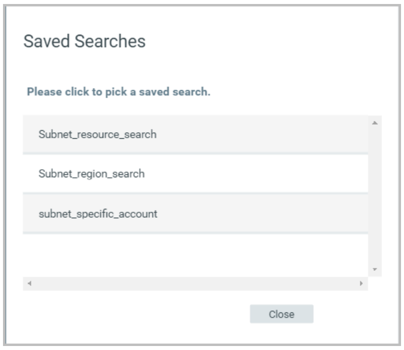


Save Search

Title: Search_name

3 Provide a title and click Save

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



Saved Searches

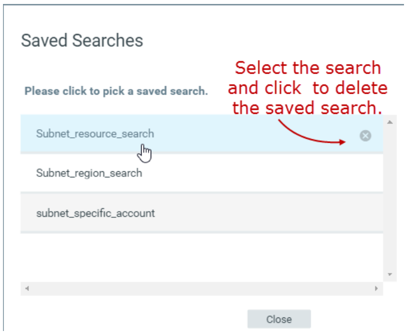
Please click to pick a saved search.

Subnet_resource_search

Subnet_region_search

subnet_specific_account

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



Saved Searches

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.

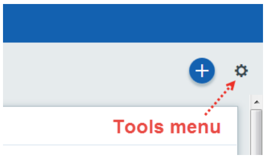
Each dashboard is a collection of widgets showing resource data of interest. You can create multiple dashboards and switch between them.

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

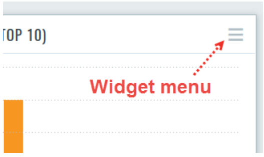
## How to Take Action

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.



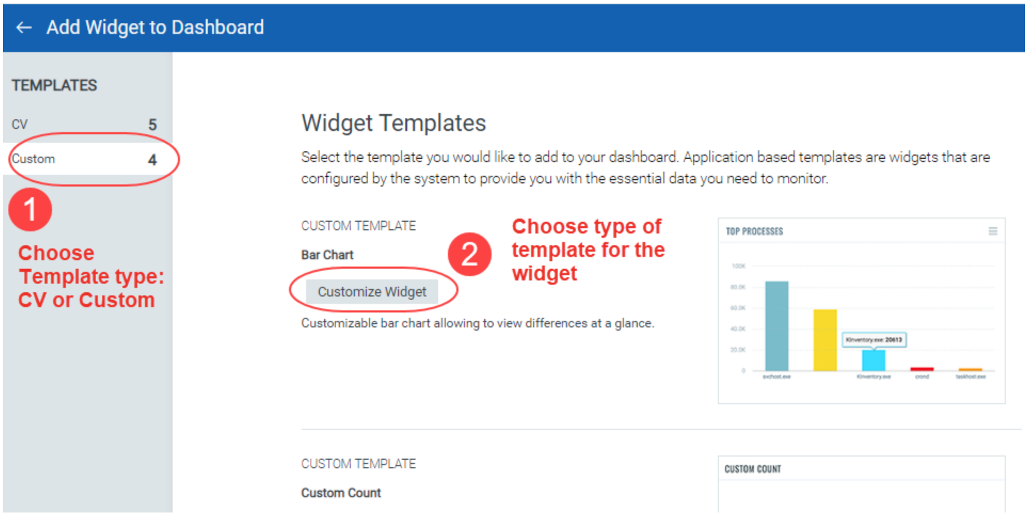
Take actions on a single widget: edit widget, delete widget, refresh widget data, create template from widget, export widget.



## 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.

CUSTOM TEMPLATE

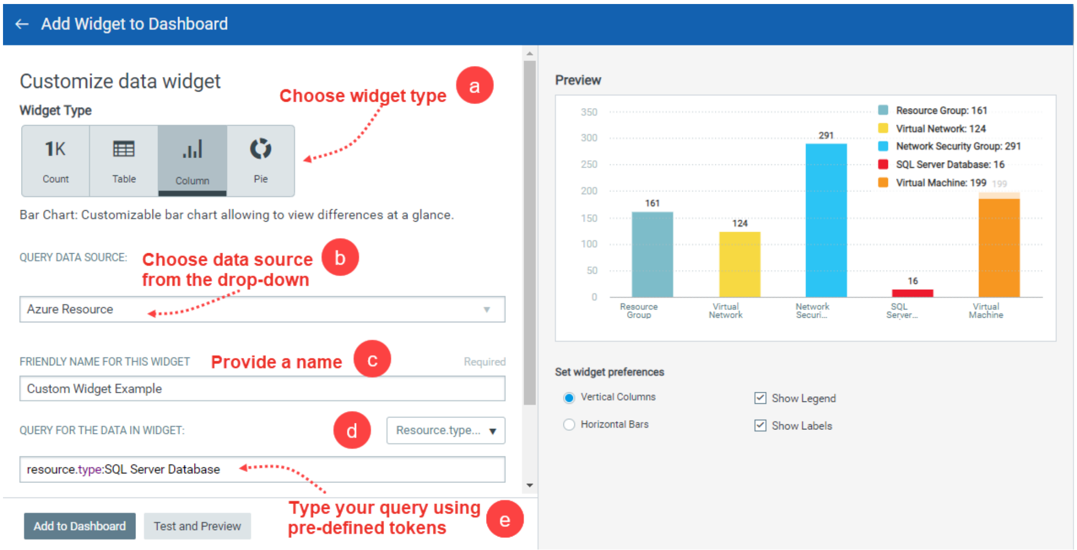
Bar Chart

Customizable bar chart allowing to view differences at a glance.

CUSTOM TEMPLATE

Custom Count

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



← Add Widget to Dashboard

Customize data widget

Widget Type: Column

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

Set widget preferences

● Vertical Columns

○ Horizontal Bars

☑ Show Legend

☑ Show Labels

Choose widget type a

Choose data source from the drop-down b

Provide a name c

d

Type your query using pre-defined tokens e

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.

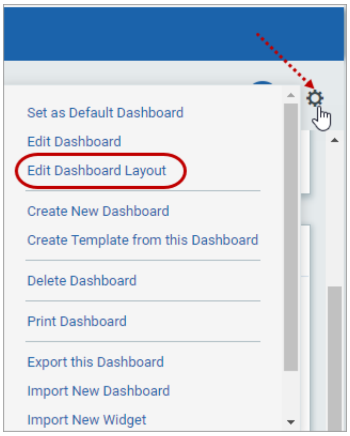
Resize any widget horizontally, drag & drop widgets to change the layout. Refresh your view.

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.

# Securing Infrastructure as Code

In the current continuous integration and continuous deployment (CICD) environment, the scans are conducted on cloud resources after deployment. As a result, you secure the cloud resources post deployment. We execute Infrastructure as Code (IaC) Security scan for AWS Terraform. With arrival of IaC scan, you can now secure your code (IaC) before it gets deployed in the cloud environment.

The Qualys IaC Security feature will help shifting security and compliance posture of cloud security to left, allowing evaluation of cloud resource misconfigurations even before actual deployment. Using this feature, cloud infrastructure teams can prevent misconfigurations before it really happens.

The first step towards IaC security is triggering an IaC scan. In the current scenario, the scans are executed after the cloud resources are deployed in the cloud environment. As a result, fixing of misconfigurations happens post deployment. However, using this feature, you can trigger the scan on IaC (configuration file) before the cloud resources are deployed in the environment.

Once you trigger the scan, we will evaluate the configuration file (IaC) against pre-defined controls.

IaC scanning works by uploading the template file or zip containing multiple files to CloudView, either via our CLI or API. The template is processed, and the response returns a scan ID. The returned scan id then can be used to fetch the scan report which provides the evaluation results giving you a clear picture of the misconfigurations (if any) that need to be fixed to secure your code before the actual deployment.

You can scan the templates either through CLI commands or using APIs:

Scanning Template Files Using CLI

Scanning Template Files Using API

## Template Support

This Qualys IaC Security version supports following template files:

- **AWS, Azure, and GCP Terraform Templates:** The .tf template files - IaC Security scan supports over 100 terraform resource types.

- **AWS, Azure, and GCP Terraform Plan**: The .json plan files - To scan the plan files, you need to make those files available in JSON format. Refer https://www.terraform.io/docs/internals/json-format.html

- **AWS Cloudformation Template**: We support the file types:.json, .yaml, .yml, .template

- **Compressed Template File Formats:** We are supporting following compressed template file format: .zip, .7z, .tar, .tar.gz, .gz

## Pre-requisites

Users with a non-expired paid/trial version of Cloud Security Assessment (CSA) subscription that has API access enabled. The following users with required permissions can access IaC:

- A user with Manager access
- A sub-user with the CLOUDVIEW API Access

## Scanning Template Files Using CLI

Qualys provides a IaC scanning CLI which can be installed on any machines having python3. Qualys IaC Security CLI is based on Python PIP Platform.

**Recommendation**: Before you proceed with installation, we are recommend you to create a python virtual environment so that other python projects are not hampered.

We can create a python3 virtual environment using the below commands:

- MAC/Unix: `python3 -m pip install --user virtualenv`
- Windows: `py -m pip install --user virtualenv`

Click here for more information and detailed steps.

### Install Qualys IaC Security CLI

Use the following command to install the Qualys IaC through command line interface (CLI).

```
pip install Qualys-IaC-Security
```

Once Qualys IaC Security is installed, you may verify the installation by running the following commands.

```
$ qiac -v  / --version
Version: <installed version>

$ qiac -h  / --help
Usage: Show this message and exit.
```

## List of Commands

| Common Options | Description |
|---|---|
| -c, --config_file | (Optional) Path of the credentials config file set using "config" command |
| -a, --platform_url | Qualys Platform URL |
| -u, --user | Qualys username |
| -p, --password | Qualys password |
| -m, --format | Provides the output in JSON format. [json] |
| -x, --proxy | Provide proxy in JSON format<br>For example,. {\"http\":\"http://<user>:<password>@<host>:<port>\",\"https\":\"https://<host>:<port>\"} |
| -h, --help | Show this message and exit |
| **scan** | |
| -n, --scan name | (required) Name of the scan |
| -pn, --policy_name | Cloud security assessment (CSA) policy name [Execution type: Build time] |
| -d, --path | (required) Single template file or a directory path |
| -f, --filter | Use regular expression to filter to and include the input files.<br>Example: ".*[.]tf$"<br>Note: This option must used only when directory path is specified in the path option |
| -as, --async | Launches/Triggers the IaC scan asynchronously |
| -q, --quiet | Show only failed checks |
| -g, --tag | Add the tag (in JSON format) to the scan<br>For example, [{"env":"linux"},{"test_key":"tags"}] |
| -s, --save_output | (optional) Save the output in the current directory |
| **getresult** | |
| -i, --scan_id | Scan ID |
| -s, --save_output | (optional) Save the output in the current directory |
| **listscans** | |
| -i, --scan_id | Scan ID |
| **config** | |
| -a, --platform_url | (required) Qualys Platform URL |
| -u, --user | (required) Qualys username |
| -p, --password | (required) Qualys password |
| -c, --config_file | (optional) File path to store the configuration |

Below are some of common scenarios for command usage. Usage of parameters vary based on use cases.

Configure IaC CLI (optional command)

1: Trigger Scan (add -d)

2: Get the scan results

3: Get the whole scan list

4: Get the scan list of single Scan ID

### Configure IaC CLI (optional command)

The command configures user's credentials. This command is optional and should be used only when a user wants to store Qualys credentials in flat file for subsequent uses. Once this file is correctly configured, the user need not provide the Qualys platform URL, username, and password details for every CLI command. The authentication details are picked from the configuration file.

The following command collects Qualys credentials and stores it at the home directory (.qiac.yaml).

```
qiac config  -a <Qualys Platform URL> -u <username> -p <password>
```

**Note**: The parameters: **Qualys Platform URL**, **username**, and **password** are mandatory for this command.

```
config_file : name or path of the config file
```

where,

**name**: if the name is provided, then a config file with the specified name is created.

**path**: if the path is provided, then the config file is created at the specified path with the default name. The default name is .qiac.yaml.

This command saves the config file on the user's home directory with the name .qiac.yaml. If a user doesn't want to save the config file in the home directory, the user can use the config_file option to provide the config file path. The config_file option saves the file at the specified path.

A user can use the config file using below ways:

- Use Config file from home directory:

```
qiac <commands|params>
```

- User Config file from custom directory:

```
qiac <commands|params> -c <location of config file>
```

where,

the commands could be scan, getresults, listscans.

**Note**: If the user does not provide credentials in command options, then CLI checks for the config file in the current directory. If the config file is not present in the current directory, then CLI checks the user's home directory.

### 1: Trigger Scan (add -d)

The command uploads scan artifacts (-d) to Qualys platform, generate scan Id and return as an output. You may/may not want to add password parameter in CLI.

- With password (add -p)

```
qiac scan -a <Qualys Platform URL> -u <username> -p <password> -n
<scan name> -d <path or single file>
```

- Without password (remove -p)

```
qiac scan -a <Qualys Platform URL> -u <username> -n <scan name> -d
<path or single file>
```

- With config file option (add -d: single file option)

```
qiac scan -n <scan name> -c <Path of the config file> -d <path or
single file>
```

- With config file option (add -d: multiple file option)

```
qiac scan -n <name of the scan> -c < Path of the config file >  -d
<path1 to a file or directory> -d <path2 to a file or directory> -
d <path3 to a file or directory>
```

- With save output option (-s)

```
qiac scan -n <scan name> -c <Path of the config file> -d <path or
single file> -m <file format:JSON> -s
```

**Note**: Ensure that you always use file format option (-m JSON) along with -s option. The option -s saves the scan output in the current directory in JSON format. The file name is as follows:

scan_response_<scanId>.json

- With policy name option (-pn)

```
qiac scan -a <Qualys Platform URL> -u <username> -p <password> -n
<scan name> -d <path or single file> -pn <policy name>
```

**Note**: The policy name should be entered in single quotes for Linux users and in double quotes for Windows users. The policy name must match with existing policies in CloudView.

### 2: Get the scan results

The command returns IaC scan result for the provided scan id (-i) in a default tabular format.

```
qiac getresult -a <Qualys Platform URL> -u <username> -p
<password> -i <scan id>
```

with config file option

```
qiac getresult -c <Path of the config file> -c <Path of the config
file>
```

### 3: Get the whole scan list

The command returns list of all the IaC scans.

```
qiac listscans -a <Qualys Platform URL> -u <username> -p
<password>
```

with config file option

```
qiac listscans -c <Path of the config file>
```

### 4: Get the scan list of single Scan ID

The command returns single IaC scan as per the scan Id you provide.

```
qiac listscans -a <Qualys Platform URL> -u <username> -p
<password> -i <scan id>
```

with config file option

```
qiac listscans -c <Path of the config file> -i <scan id>
```

## Understanding Scan Output

In command line interface (CLI), the output is defaulted to tabular display. CLI can output JSON response with additional input parameter for format.

For details on elements in JSON output format, refer to Secure IaC section in CloudView API User Guide.

# Scanning Template Files Using API

Qualys has introduced new API to launch the IaC scan and fetch the scan results and scan lists.

1) Trigger IaC Scan (POST)

2) Get Scan Results (GET)

3) Get List of Scans (GET)

For complete details, refer to Secure IaC section in CloudView API User Guide.

# 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-the-box.

The Policies tab lists the policies we currently support. To view the complete list of policies and associated controls that Qualys provides, refer to Qualys CloudView Policy Document.