**Table of Contents**

**About this Guide** ........................................................................................................... 4
  - About Qualys ................................................................. 4
  - Qualys Support .......................................................... 4

**CloudView Overview** ............................................................................................... 5
  - Qualys Subscription and Modules required ......................................................... 5
  - Concepts and Terminologies ............................................................................... 6

**Get Started** ............................................................................................................... 7
  - AWS ...................................................................................................................... 7
    - Steps to Create AWS Connector ................................................................. 7
    - Base Account ............................................................................................ 12
    - Base Account Configuration in AWS Console ........................................ 14
    - Editing AWS Connectors ........................................................................ 16
    - AWS Resource Inventory ....................................................................... 17
  - Microsoft Azure .................................................................................................... 19
    - Pre-requisites ......................................................................................... 19
    - Steps to Create Azure Connector .......................................................... 20
    - Configuration Steps on Microsoft Azure console ................................... 22
    - Editing Microsoft Azure Connectors ...................................................... 29
    - Azure Resource Inventory ................................................................... 30
  - Google Cloud Platform .......................................................................................... 31
    - Steps to Create GCP Connector .............................................................. 31
    - Editing GCP Connectors ....................................................................... 36
    - GCP Resource Inventory ...................................................................... 36

**Managing Connector Access for Users** ................................................................. 37
  - User Permissions ............................................................................................ 37
  - New Users: Scope and Permissions ............................................................... 38
    - Create User ......................................................................................... 38
    - Assign Role to Users ........................................................................ 39
    - Manage Access for Users (Grouping Connectors) ................................... 40
    - Manage Access for Users .................................................................. 42
  - Defining Scope for Existing Users ................................................................. 44
    - Sub User (All Privileges) ..................................................................... 45
    - Sub User (Reader Privileges) ................................................................. 48

**Securing Cloud Resources** ..................................................................................... 50
  - Dashboard ................................................................................................. 50
  - Resources Details .................................................................................... 51
  - Instance Details ...................................................................................... 52
<table>
<thead>
<tr>
<th>AWS Policies</th>
<th>104</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIS Amazon Web Services Foundations Benchmark</td>
<td>104</td>
</tr>
<tr>
<td>AWS Best Practices Policy</td>
<td>106</td>
</tr>
<tr>
<td>AWS Lambda Best Practices Policy</td>
<td>109</td>
</tr>
<tr>
<td>AWS Database Service Best Practices Policy</td>
<td>111</td>
</tr>
<tr>
<td>Azure Policies</td>
<td>114</td>
</tr>
<tr>
<td>CIS Microsoft Azure Foundations Benchmark</td>
<td>114</td>
</tr>
<tr>
<td>Azure Best Practices Policy</td>
<td>118</td>
</tr>
<tr>
<td>Azure Function App Best Practices Policy</td>
<td>119</td>
</tr>
<tr>
<td>Azure Database Service Best Practices Policy</td>
<td>120</td>
</tr>
<tr>
<td>GCP Policies</td>
<td>122</td>
</tr>
<tr>
<td>CIS Google Cloud Platform Foundation Benchmark</td>
<td>122</td>
</tr>
<tr>
<td>GCP Best Practices Policy</td>
<td>126</td>
</tr>
<tr>
<td>GCP Cloud Functions Best Practices Policy</td>
<td>127</td>
</tr>
<tr>
<td>GCP Kubernetes Engine Best Practices Policy</td>
<td>127</td>
</tr>
<tr>
<td>GCP Cloud SQL Best Practices Policy</td>
<td>128</td>
</tr>
</tbody>
</table>
About this Guide

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

About Qualys

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

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

Qualys Support

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

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

With CloudView you’ll get these features:
- Discover assets and resources across all regions from multiple accounts and multiple cloud platforms
- Search resource metadata, view resource details and show associations across resources
- Out-of-box AWS, Azure, GCP policies
- Continuously assess and report resource misconfigurations by checking against the controls from out-of-box policies
- Build your own policies and customize controls to suit your need
- Ability to view, filter and export misconfigurations

Qualys Subscription and Modules required

Check that you have these modules available in your subscription:
- CloudView
- Vulnerability Management (only if you want to view host vulnerability information)
- AssetView
- Cloud Agents for VM
- Administration

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

Get familiar with common terms used in CloudView.

<table>
<thead>
<tr>
<th>Concept</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>A set of configuration checks that will assess different resources collected from your cloud account.</td>
</tr>
<tr>
<td>Control</td>
<td>A configuration check. Each check applies to a specific service/resource. Here are some examples:</td>
</tr>
<tr>
<td></td>
<td>- MFA should be enabled for console user - applies to AWS IAM Service and IAM User Resource</td>
</tr>
<tr>
<td></td>
<td>- Password policy should have upper case letter enforced - applies to AWS IAM Service</td>
</tr>
<tr>
<td></td>
<td>- Security group should not allow inbound access on port 22 from 0.0.0.0 - applies to EC2/VPC services and Security Group Resource</td>
</tr>
<tr>
<td>Service</td>
<td>A service is the high level grouping by functional area. Each service consists of different entities or resources.</td>
</tr>
<tr>
<td>Resource</td>
<td>A resource is an entity that you can work with. Examples include an Amazon EC2 instance, IAM User, Security Group.</td>
</tr>
<tr>
<td>Control Passed</td>
<td>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.</td>
</tr>
<tr>
<td>Control Failed</td>
<td>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.</td>
</tr>
<tr>
<td>Resource Passed</td>
<td>Resource is considered passed for a control if its attribute is configured as per the desired configuration in the control.</td>
</tr>
<tr>
<td>Resource Failed</td>
<td>Resource is considered failed for a control if its attribute is not configured as per the desired configuration in the control.</td>
</tr>
</tbody>
</table>
Get Started

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

AWS

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

Base Account

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

Steps to Create AWS Connector

Go to the Configuration > Amazon Web Services tab and click Create Connector.
Provide a name and description (optional) for your connector.

Select an account type for your connector: Global, US GovCloud or China. You can choose only one account type per connector.

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

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

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

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

Now, copy settings from the connector details: Qualys AWS Account ID and External ID. You’ll need these for creating your IAM role in AWS in the next step.

A unique external ID gets generated during connector creation. AWS recommends the External ID should be read-only field as one of its best practices. We generate a unique External ID, and auto-populate it. It is a read-only field and you cannot edit the External ID field, thereby enhancing the security of your AWS account.

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

![Create role](create_role.png)

Ensure that you do not opt for Require MFA option when you create a cross-account role for CloudView.
In Attach Permissions policies section, find the policy titled "SecurityAudit" and select the check box next to it. Click Next: tags and then Next: Review.

Save AWS role and get the ARN: Enter a role name (e.g. QualysCVRole), click Create role. Then click on the saved role to view role details and copy the ARN value.
Go back to your AWS connector in Qualys CloudView and paste the Role ARN value into the connector details.

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

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

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

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

Then click Create Connector.

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

Want to create a role using CloudFormation?
Download the CloudFormation template from the Create AWS Connector window.
Follow the steps on the screen to create a stack by downloading previously uploaded template file. When the stack is complete, copy the Role ARN from the output and paste it into the connector details.

**Base Account**

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

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

**Create Base Account**

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

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

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

Click Create and provide title, AWS account ID, access and secret keys.
Select the account type. You can create only one base account per account type.

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

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

Edit Base Account

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

Updating Existing Connectors to Use Base Account

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

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

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

**What happens if I delete the base account?**

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

**Base Account Configuration in AWS Console**

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

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1581205545000",
      "Effect": "Allow",
      "Action": [ "sts:AssumeRole" ],
      "Resource": [ "*" ]
    }
  ]
}
```

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

Provide a user name and enable Programmatic access for the user. Click Next: Permissions.
Select Attach existing policies directly and then type the name of the policy that you created (AssumeRole) in Filter policies. Select the policy (AssumeRole) you configured and then click Next: Tags.

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

**Editing AWS Connectors**

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

You can now edit the required details.

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

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

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

**What do you achieve?**

- Get centralized visibility of services/resources across your multiple AWS accounts.
- Identify services/resources running your AWS account. For list of resources getting collected, refer Resources List.
- Identify the number of resources that are non-compliant.
- View resource details and their associations with other resources.
- Locate the resources by querying the resource attributed, account & region etc.
- Search tagged/untagged resources using AWS tags.
- Trend chart and time range will help you understand the how the resources are varied over the past 7, 30 days. You can also specify the custom range.
Resources List
CloudView will discover and fetch following AWS resources and their corresponding attributes.
- Subnet
- Network ACL
- Internet Gateway
- Load Balancer
- Instance
- Route Table
- S3 Bucket
- IAM User
- VPC
- Auto Scaling Group
- Security Group
- Lambda Function
- RDS
- EBS Volume
Microsoft Azure

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

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

Pre-requisites

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

- **Assign Azure Active Directory permissions** to register an application with your Azure Active Directory
- **Check Azure Subscription permissions** to assign the application to a role in your Azure subscription

**Assign Azure Active Directory permissions**

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

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

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

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

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

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

Steps to Create Azure Connector

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

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

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

Select a frequency at which the connector should poll the cloud provider and fetch data. By default, the connector polling frequency is configured for every 4 hours. As a result, the connector will connect with the cloud provider every 4 hours to fetch the data.
You can configure frequency from minimum one hour to maximum 24 hours. We recommend that you configure frequency of 4 hours or more for optimal use of your connector. Configuring a low polling frequency (lesser than 4 hours) can affect the performance of the connector and may result in Microsoft Azure API throttling error.

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

Next, you need to configure the application ID, directory ID, authentication key and subscription ID from the Microsoft Azure console to paste into your connector details. To view the detailed configuration steps, refer to Configuration Steps on Microsoft Azure console section.
Click Test Connector to verify if the connector can successfully authenticate using the provided service principal credentials in Microsoft Azure cloud environment.

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

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

Click Create Connector.

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

**Configuration Steps on Microsoft Azure console**

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

- Create Application and get Application ID, Directory ID
- Configuring Authentication Key
- Create Secret Key
- Getting Subscription ID

**Create Application and get Application ID, Directory ID**

Create an application in Azure Active Directory. Log on to the Microsoft Azure console and go to Azure Active Directory in the left navigation pane, then App registrations. Click New registration.
To register the application, you need to provide few details.

Provide these details:

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

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

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

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

Provide permission:

- Select the application that you created and go to API permissions > Add a permission.
- Select Azure Service Management API in Microsoft APIs for Request API permissions.
- Select user impersonation permission and click Add permission.

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

Click Add a permission.
Select Microsoft Graph in Microsoft APIs for Request API permissions.

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

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

Create Secret Key

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

- Add a description and expiry duration for the secret key (recommended: Never) and click Add.
The value of the key appears in the Value field.

Copy the key value at this time. You won’t be able to retrieve the key later. Note down the secret key and store it securely with you. You’ll need to provide the key value with the application ID to log on as the application.
Getting Subscription ID
Grant permission for the application to access subscriptions. Assign a role to the new application. The role defines the permissions for the new application to access subscriptions. Repeat these steps to add more subscriptions.

On the Microsoft Azure portal, navigate to Subscriptions.

Select the subscription for which you want to grant permission to the application and note the subscription ID. To grant permission to the application you created, choose Access Control (IAM).

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

**Assign Reader Role**

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

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

c - Select Azure AD user, group, or service principal in Assign Access to dropdown.
d - Type the application name in Select drop-down and select the application you created.

Assign Custom Role

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

a - Go to Add > Add a role assignment. Pick the custom role you created (QRole). The custom role can view but cannot make any changes to the resources of a subscription.
b - Select Azure AD user, group, or service principal in Assign Access to dropdown.
c - Type the application name in Select drop-down and select the application you created.
d - Click Save to finish assigning the role. You’ll see your application in the list of users assigned to a role for that scope.

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

Create Custom Role

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

```json
{
    "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:
```bash
az role definition create --role-definition <Role-Definition-Json_file>
```

References
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-cli
https://docs.microsoft.com/en-us/azure/role-based-access-control/tutorial-custom-role-powershell
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal

Editing Microsoft Azure Connectors

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

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

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

**Azure Resource Inventory**

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

**Resources List**

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

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

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

Steps to Create GCP Connector

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

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

(2) Select a frequency at which the connector should poll the cloud provider and fetch data. By default, the connector polling frequency is configured for every 4 hours. As a result, the connector will connect with the cloud provider every 4 hours to fetch the data.
You can configure frequency from minimum one hour to maximum 24 hours. We recommend that you configure frequency of 4 hours or more for optimal use of your connector. Configuring a low polling frequency (lesser than 4 hours) can affect the performance of the connector and may result in GCP API throttling error.

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

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

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

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

(5) Click Create Connector.

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

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

**Enable Access to Compute Engine and Resource Manager API**

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

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

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

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

- Compute Engine API
- Cloud Resource Manager API
- Kubernetes Engine API
- Cloud SQL Admin API
- BigQuery API
- Cloud Functions API
- Cloud DNS API
- Cloud Key Management Service (KMS) API
- Cloud Logging API
- Stackdriver Monitoring API

**Create Service Account and Download Configuration File**

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

(2) From the left sidebar, navigate to IAM & admin > Service accounts and click CREATE SERVICE ACCOUNT. Provide a name and description (optional) for the service account and click Create.
(3) Choose Viewer and Security Reviewer role to assign at least reader permissions to the service account and click Continue.

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

A message saying “Private key saved to your computer” is displayed and the JSON file is downloaded to your computer. Click Close and then click Done.
Upload the configuration (JSON) file and click Create Connector to complete GCP connector creation in Qualys Cloud Platform.

**Editing GCP Connectors**

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

You can now edit the required details.

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

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

**GCP Resource Inventory**

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

**Resources List**

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

- VM Instances
- Networks
- Firewall Rules
- Subnetworks
- Cloud Functions
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.

<table>
<thead>
<tr>
<th>Operations</th>
<th>User (Manager role)</th>
<th>Sub User</th>
<th>Sub User (Reader role)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New Users</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Grant Access to Sub-Users</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Update Access of Existing Users</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Create and Assign Groups to Connectors</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Manage Connectors</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Manage Policies and Controls</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Customize Controls</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Reports</td>
<td>Yes</td>
<td>Yes</td>
<td>View only</td>
</tr>
<tr>
<td>Dashboards</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
New Users: Scope and Permissions

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

Create User
Assign Role to Users
Manage Access for Users (Grouping Connectors)
Manage Access for Users

Create User

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

Quick Steps

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

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

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

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

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

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

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

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

Tell me about various roles?
You can configure two sub user roles:

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

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

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

How do I edit a role?
Select any role in the list and choose Edit from the Quick Actions menu.
You can change the role name and description and edit the assigned permissions. Any changes you make to a role will apply to all users assigned that role.

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

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

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

- All privileges: Sub User will have all the privileges in CloudView except creating and managing other users. For more information, refer to Sub User (All Privileges).
- Reader privileges: Sub User with Reader role can only view the data displayed in CloudView module. For more information, refer to Sub User (Reader Privileges).

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

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

Manage Access for Users (Grouping Connectors)
You can now control access for sub users with the usage of groups. The groups help you to organize your connectors and to manage user access to them.

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

Assign Groups to Connector
Let us see how to create connector groups and provide access to a particular connector for a user.
Managing Connector Access for Users
New Users: Scope and Permissions

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

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

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

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

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

New Users: Scope and Permissions

Restrict User Access to all Connectors

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

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

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

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

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

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

Manage Access for Users

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

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

Assign Scope to a User

(1) Navigate to Configuration > Access Management tab.

The Access Management tab is available only to user with Manager role. The user with Manager role can manage access for sub-users.
(2) Select the user, and click Manage Access from quick action menu.

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

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

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

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

- **Using connectors**
  
  When you define scope for a sub user, you could directly select the connectors for every Cloud Provider and associate it with the sub user. The sub user can then access all the connectors assigned to the sub user.
In the Connectors and Regions section, click the link for the specific Cloud Provider and then select the connector, and click Save.

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

**Defining Scope for Existing Users**

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

*Manage Access for Users (Grouping Connectors)*

*Manage Access for Users*

For more information refer to [Role-based Access Management](#).
**Sub User (All Privileges)**

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

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

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

**What can the Sub User with Full Access do?**

The user with full access role can

- Manage Connectors
- Manage controls and policies
- Create and edit dashboards
- Create and edit groups (connector groups)
- Create sub users and assign groups

**Quick Steps**

(1) Create a Reader User: Navigate to Administration module > User Management > Create User > Create Reader User.
(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.
(3) Select the required user from Users drop-down and click Save. You need to choose user whom you want to assign full access of CloudView.

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

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.
Sub User (Reader Privileges)

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

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

What can the Reader User do?
The user with reader role can
- View connectors
- Monitor controls, policies and resources
- Create and edit dashboards

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

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

(3) Assign the role to the newly created user.
The new reader user is ready to use CloudView with monitoring capabilities!
Securing Cloud Resources

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

Dashboard

The Qualys CloudView application provides out-of-the box default AWS Dashboard providing a summary of inventory and security posture across resources. We also support Microsoft Azure dashboard.

The default dashboard provides:
- Resource inventory - Route Tables, EC2 Instances, VPC, Subnets, IAM Users, etc
- Total evaluation failures i.e. the resources misconfigurations by control criticality
- Security posture at each region level showing resources and failures
- Top 5 Accounts with maximum control failures
- Top 5 Failed controls

Check out this sample dashboard
Resources Details

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

Resources Summary

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

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.

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

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.

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

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.

View Security Group Associations

You can view various details about the associations such as the ID, region, state and so on.
View Controls Evaluated
You can view the controls that are evaluated for the resource and if the controls have passed or failed.

<table>
<thead>
<tr>
<th>#</th>
<th>CONTROL</th>
<th>CRITICALITY</th>
<th>RESULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>41</td>
<td>Ensure no security groups allow ingress from 0.0.0.0/0 to port 22</td>
<td></td>
<td>FAIL</td>
</tr>
<tr>
<td>42</td>
<td>Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389</td>
<td></td>
<td>FAIL</td>
</tr>
</tbody>
</table>
Resources Misconfigurations

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

Controls Evaluation View

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

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.

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

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.
View Control Evaluation Results per Account

Quickly view how many controls are passed/failed by clicking the account filter.
Search Using Resource Parameter Information

You can now 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 now 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.

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

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.

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.

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 the 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.

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

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

- Resource Information: The resource information provides details of the resources associated with the exception you are creating.

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.

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.

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.
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.

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.
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.
Policies and Controls

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

Customize Controls

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

Control Criticality

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

### Change Criticality

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

- **High** (System Default)
  - Controls with severe impact.
- **Medium**
  - Controls with medium impact.
- **Low**
  - Controls with minimal impact.

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

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

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

- for System Defined Controls. Such controls cannot be customized. You cannot alter the parameter values for such system-defined controls.
- used to indicate that the control can be customized to suit your need. You can change the parameters values for such controls and customize them as per your organization’s requirements.

User-Defined Controls

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

Copy Control and Customize

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

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

For example, let us modify the minimum password length to 10 for AWS CID 11.
(1) Select the control and click Create Copy from quick action menu.

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

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

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

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

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

**Can I delete controls?**
Yes. Choose the user-defined control to be deleted and choose Edit from the quick action menu. You can delete only user-defined controls. You cannot delete system-defined control.
Build Your Own Policy
A policy is a collection of controls used to measure and report compliance for a set of resources. Your compliance reports will show you resource compliance status (pass or fail) with the policy controls. You could use the policies we provide or build your own policy.

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

Set Up Your Own Policy (Custom Policy)
You can create your own custom policy and associate the required controls to be evaluated for the custom policy.

(1) Navigate to Policy > Policy > New.

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

(3) Associating Controls:
- System Defined
- User defined

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

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.

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 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 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.

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

4) Select the required compliance policy from the Select Policy drop-down for which you want to evaluate your cloud resources. You can select multiple policies as well.

5) Select the group, connector, or a combination of groups and connector you want to evaluate for compliance.
6) Type a search query to define the criteria for your report. You can use Qualys Query Language (QQL) that populates the supported search tokens as you type in the search bar. Click Next.

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

**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 CSV format.
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.

3) Select the cloud provider for which you want to generate the mandate report.
4) Select the Mandate in the report type and then click Next.
   - Select the Policy from the drop-down. You can select multiple policies.
   - Select the Mandate from the drop-down. You can select only one mandate.
5) Select the groups, connector, or a combination of groups and connector you want to evaluate for compliance.

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

![Sample Mandate Based Report](image)

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.

![Policy Based Report](image)
2) Provide a title and description (optional) to the report template.

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

4) Select the Policy in the report type, select the Policy from the drop-down and then click Next. You can select multiple policies.
4) Select the group, connector, or a combination of groups and connector you want to evaluate for compliance.

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

List of Mandates
We support the following mandates for report generation.
1. CIS Critical Security Controls (Top 5)
2. Payment Card Industry Data Security Standard (PCI-DSS)
3. CIS Critical Security Controls (Top 20)
4. NIST Cyber Security Framework (CSF)
5. Cloud Controls Matrix (CCM)
6. Criminal Justice Information Services (CJIS) Security Policy
7. IRS Publication 1075
8. Minimum Acceptable Risk Standards for Exchanges (MARS-E)
10. Health Insurance Portability and Accountability (HIPAA) Security Rule
11. The Australian Signals Directorate - The Essential 8 Strategies (ASD 8)
12. NERC Critical Infrastructure Protection (CIP)
13. ANSSI 40 Essential Measures for a Healthy Network
15. Reserve Bank of India (RBI) - Baseline Cyber Security and Resilience Requirements (Annex 1)
16. NCSC Basic Cyber Security Controls (BCSC)
17. ISO/IEC 27001:2013
18. NESA UAE Information Assurance Standards (IAS)
19. NIST 800-171 (Special Publication)
20. Sarbanes-Oxley Act: IT Security
22. General Data Protection Regulation (GDPR)
23. IRDAI Guidelines On Information and Cyber Security for Insurers
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


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

<table>
<thead>
<tr>
<th>Platform Type</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qualys US Platform 1</td>
<td><a href="https://qualysguard.qualys.com">https://qualysguard.qualys.com</a></td>
</tr>
<tr>
<td>Qualys US Platform 2</td>
<td><a href="https://qualysguard.qg2.apps.qualys.com">https://qualysguard.qg2.apps.qualys.com</a></td>
</tr>
<tr>
<td>Qualys US Platform 3</td>
<td><a href="https://qualysguard.qg3.apps.qualys.com">https://qualysguard.qg3.apps.qualys.com</a></td>
</tr>
<tr>
<td>Qualys EU Platform 1</td>
<td><a href="https://qualysguard.qualys.eu">https://qualysguard.qualys.eu</a></td>
</tr>
<tr>
<td>Qualys EU Platform 2</td>
<td><a href="https://qualysapi.qg2.apps.qualys.eu">https://qualysapi.qg2.apps.qualys.eu</a></td>
</tr>
<tr>
<td>Qualys India Platform 1</td>
<td><a href="https://qualysguard.qg1.apps.qualys.in">https://qualysguard.qg1.apps.qualys.in</a></td>
</tr>
<tr>
<td>Qualys Canada Platform</td>
<td><a href="https://qualysapi.qg1.apps.qualys.ca">https://qualysapi.qg1.apps.qualys.ca</a></td>
</tr>
</tbody>
</table>

### Do I need to Authenticate?

Authentication to the Qualys Cloud Platform is necessary before you try out the APIs. Simply, click Authorize and provide the user name and password. You can now use the APIs!
What’s more in CloudView

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

Automatic Connector Creation

We have built few scripts that could ease tasks for you in CloudView.
- Connector Creation: There are various scripts you could use to automate connector creation task.
- Export to Splunk: Use CloudView_Splunk_Scripted_Inputs to integrate CloudView via python scripted inputs into Splunk Enterprise.
- Alerting data: You could use slack_cloudview_alerts to integrate CloudView Assessment data into Slack for alerting.

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

Role-based Access Management

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

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

You can:
- Block or provide UI access to CloudView module
- Provide UI access to CloudView module with restricted permissions (read-only user)
- Provide full UI access to CloudView module with all permissions

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

Tell me the difference between sub user roles

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

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

Reader privileges: Sub User with Reader role can only view the data displayed in CloudView module.
**How do I manage access for sub users?**

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

- **Direct scope definition for sub user**

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

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

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

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

- **Using groups**

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

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

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

  Choose the connector for which you want to configure access and click Assign Group from the quick action menu.
Type a name for the group and click Create and then click Save.

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

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

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

**Tell me about GroupBy option**

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

Alternatively, you could use search token.

group.name: <groupname>

and the search result lists all the connectors for a cloud provider associated with the group.
Tell me Scope and Access Conflicts
Consider a sub user whose direct scope definition conflicts with the access assigned through groups. In such cases, the scope overrides and the sub user is able to access the connectors defined directly through the scope of the user.

Let us consider two different examples to understand the conflicts better.

Case 1: A sub user is assigned a group named AWS_important that includes access to two AWS connectors. Also, the sub user has been directly assigned access to five other AWS connectors. In such case, the sub user is able to access all the seven connectors.

Case 2: A sub user is assigned a group that includes none of the connectors. In such case, the sub user cannot access any connector.

However, if the same sub user is directly assigned connectors through scope definition, the sub user can access the connectors that are directly assigned.

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

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

The download is limited to 10,000 records.
1) Use our search to narrow down your results.
2) Select Download from the Tools menu.
3) Click Download. That’s it!
What’s more in CloudView
Choosing Data Range

Choose 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.

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.

Give your search a title.

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

Delete any saved search you’re no longer interested in.
**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.
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.

a - Choose widget type: Count, Table, Column, Pie  
b - Choose data source from the dropdown. For example: Azure Resources.  
c - Provide a name for your widget.  
d - Choose the resource type  
e - Type your search query using pre-defined tokens.

The Preview pane displays the preview of your widget.

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

From the Actions menu on the dashboard, you can also import and export widget configurations to a file in a json format, allowing you to share the widgets between accounts or within the Qualys community.
**Resizing and layout.**
Resize any widget horizontally, drag & drop widgets to change the layout. Refresh your view.

1) Click the Tools icon on your dashboard.
2) Select Edit Dashboard Layout
3) Adjust the width for any widget or drag the widget to a new location.
4) Click OK to save your changes.

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

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

**Configure number of Resources, Controls**
You might also want to choose the number of resources or controls displayed in your Live Feed widget. You can choose to display: Top 10, Top 5, or Top 3 failed controls or resources.
Appendix: List of Policies and Controls

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

The Policies tab lists the policies we currently support.

**AWS**
- CIS Amazon Web Services Foundations Benchmark
- AWS Best Practices Policy
- AWS Lambda Best Practices Policy
- AWS Database Service Best Practices Policy

**Azure**
- CIS Microsoft Azure Foundations Benchmark
- Azure Best Practices Policy
- Azure Function App Best Practices Policy
- Azure Database Service Best Practices Policy

**GCP**
- CIS Google Cloud Platform Foundation Benchmark
- GCP Best Practices Policy
- GCP Cloud Functions Best Practices Policy
- GCP Cloud SQL Best Practices Policy
- GCP Kubernetes Engine Best Practices Policy
**AWS Policies**

Let us view all the policies and associated controls for AWS.

**CIS Amazon Web Services Foundations Benchmark**

We support controls for following AWS resources:

- **Identity and Access Management (IAM)**
- CloudTrail
- VPC
- Config
- Network ACLs
- S3 Bucket

**Identity and Access Management (IAM)**

- CID 1: Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password
- CID 2: Ensure console credentials unused for 90 days or greater are disabled
- CID 4: Ensure access key1 is rotated every 90 days or less
- CID 5: Ensure access key2 is rotated every 90 days or less
- CID 11: Ensure IAM password policy requires minimum length of 14 or greater
- CID 12: Ensure IAM password policy prevents password reuse
- CID 14: Ensure no root account access key exists
- CID 15: Ensure MFA is enabled for the root account
- CID 16: Ensure hardware MFA is enabled for the root account
- CID 18: Avoid the use of the root account
- CID 26: Ensure rotation for customer created CMKs is enabled
- CID 49: Ensure a support role has been created to manage incidents with AWS Support
- CID 50: Ensure IAM policies that allow full administrative privileges are not created
- CID 68: Ensure that all the expired SSL/TLS certificates stored in AWS IAM are removed:
  This control needs current date to evaluate. Not supported in current framework.
- CID 160: Ensure that IAM Access analyzer is enabled
- CID 171: Ensure there is only one active access key available for any single IAM user
- CID 175: Ensure no Inline Policies are attached to IAM Users directly
- CID 176: Ensure no Managed Policies are attached to IAM Users directly
CloudTrail
CID 19: Ensure CloudTrail is enabled in all regions
CID 20: Ensure CloudTrail log file validation is enabled
CID 21: Ensure the S3 bucket CloudTrail logs to is not publicly accessible
CID 22: Ensure CloudTrail trails are integrated with CloudWatch Logs
CID 24: Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket
CID 25: Ensure CloudTrail logs are encrypted at rest using KMS CMKs
CID 27: Ensure a log metric filter and alarm exist for unauthorized API calls
CID 28: Ensure a log metric filter and alarm exist for Management Console sign-in without MFA
CID 29: Ensure a log metric filter and alarm exist for usage of "root" account
CID 30: Ensure a log metric filter and alarm exist for IAM policy changes
CID 31: Ensure a log metric filter and alarm exist for CloudTrail configuration changes
CID 32: Ensure a log metric filter and alarm exist for AWS Management Console authentication failures
CID 33: Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer created CMKs
CID 34: Ensure a log metric filter and alarm exist for S3 bucket policy changes
CID 35: Ensure a log metric filter and alarm exist for AWS Config configuration changes
CID 36: Ensure a log metric filter and alarm exist for security group changes
CID 37: Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)
CID 38: Ensure a log metric filter and alarm exist for changes to network gateways
CID 39: Ensure a log metric filter and alarm exist for route table changes
CID 40: Ensure a log metric filter and alarm exist for VPC changes
CID 172: Ensure a log metric filter and alarm exists for AWS Organizations changes

VPC
CID 41: Ensure no security groups allow ingress from 0.0.0.0/0 to port 22
CID 42: Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389
CID 43: Ensure VPC flow logging is enabled in all VPCs
CID 44: Ensure the default security group of every VPC restricts all traffic

Config
CID 23: Ensure AWS Config is enabled in all regions
Appendix: List of Policies and Controls

AWS Policies

Network ACLs
CID 161: Ensure no Network ACLs allow ingress from 0.0.0.0/0 to port 22
CID 170: Ensure no Network ACLs allow ingress from 0.0.0.0/0 to port 3389

S3 Bucket
CID 59: Ensure "Block new public bucket policies" for a bucket is set to true.
CID 60: Ensure that "Block public and cross-account access" if bucket has public policies for bucket is set to true.
CID 61: Ensure that "Block new public ACLs and uploading public objects" for a bucket is set to true.
CID 62: Ensure that "Remove public access granted through public ACLs" for a bucket is set to true

AWS Best Practices Policy
We support controls for following AWS resources:

IAM
S3 Controls
EC2 Images
EBS Volumes
KMS Key
KMS Key Store
Load Balancers
EFS
Redis
Memcached
ES Domain
Route S3
FireHose
KMS

IAM
CID 3: Ensure access keys unused for 90 days or greater are disabled
CID 6: Ensure IAM Password Policy is Enabled
CID 7: Ensure IAM password policy requires at least one uppercase letter
CID 8: Ensure IAM password policy require at least one lowercase letter
CID 9: Ensure IAM password policy require at least one symbol
CID 10: Ensure IAM password policy require at least one number
CID 13: Ensure IAM password policy expires passwords within 90 days or less
CID 17: Ensure IAM policies are attached only to groups or roles

**S3 Controls**
CID 45: S3 Bucket Access Control List Grant Access to Everyone or Authenticated Users
CID 46: Ensure S3 Bucket Policy does not allow anonymous (public) access to S3 bucket
CID 47: Ensure access logging is enabled for S3 buckets
CID 48: Ensure versioning is enabled for S3 buckets
CID 57: Ensure that bucket policy enforces encryption in transit
CID 63: Ensure 'Block new public bucket policies' for an AWS Account is set to true.
CID 64: Ensure 'Block public and cross-account access to buckets that have public policies' for an AWS Account is set to true.
CID 65: Ensure 'Block new public ACLs and uploading public objects' for an account is set to true.
CID 66: Ensure 'Remove public access granted through public ACLs' for an account is set to true.
CID 67: Ensure Server Side Encryption (SSE) is enabled for S3 bucket.

**EC2 Images**
CID 114: Ensure Images (AMIs) owned by an AWS account are not public
CID 126: Ensure AMIs owned by an AWS account are encrypted

**EBS Volumes**
CID 115: Ensure that EBS Volumes attached to EC2 instances are encrypted
CID 116: Ensure that Unattached EBS Volumes are encrypted
CID 127: Ensure AWS EBS Volume snapshots are encrypted
CID 145: Ensure CMK is used to encrypt data at rest for EFS
CID 146: Ensure that AWS Elastic Block Store (EBS) volume snapshots are not public

**KMS Key**
CID 58: Ensure that the key expiry is set for CMKs with external key material.
CID 119: Ensure no AWS Managed CMKs is present
CID 120: Ensure no CMK is marked for deletion
CID 121: Ensure only Root user of the AWS Account should be allowed full access on the CMK
CID 122: Permissions to delete key is not granted to any Principal other than the Root user of AWS Account
CID 123: Ensure CMK administrators are not the user of the key

**KMS Key Store**
CID 124: Ensure all Custom key stores are connected to their CloudHSM clusters

**Load Balancers**
CID 128: Ensure access log is enabled for Elastic load balancer
CID 129: Ensure access log is enabled for Classic Elastic load balancer
CID 130: Ensure Classic Elastic load balancer is not using unencrypted protocol
CID 131: Ensure Elastic load balancer listener is not using unencrypted protocol

**EFS**
CID 144: Ensure EFS Encryption is enabled for data at rest

**Redis**
CID 148: Ensure that AWS ElastiCache Redis clusters are not associated with default VPC
CID 149: Ensure that AWS ElastiCache redis clusters are not using their default endpoint ports
CID 151: Ensure AWS ElastiCache Redis cluster with MultiAZ Automatic Failover feature is set to enabled
CID 152: Ensure AWS ElastiCache Redis cluster with Redis AUTH feature is enabled
CID 153: Ensure that AWS ElastiCache Redis clusters are In-Transit encrypted
CID 154: Ensure that AWS ElastiCache Redis clusters are Data At-Rest encrypted
CID 155: Ensure that AWS ElastiCache Redis clusters are Data At-Rest encrypted with CMK

**Memcached**
CID 147: Ensure that AWS ElastiCache Memcached clusters are not associated with default VPC
CID 150: Ensure that AWS ElastiCache memcached clusters are not using their default endpoint ports

**ES Domain**
CID 156: Ensure node-to-node encryption feature is enabled for AWS Elasticsearch Service domains
CID 157: Ensure AWS Elasticsearch Service domains have enabled the support for publishing slow logs to AWS CloudWatch Logs
CID 158: Ensure AWS Elasticsearch Service domains are not publicly accessible
CID 159: Ensure AWS Elasticsearch Service domains are using the latest version of Elasticsearch engine
Appendix: List of Policies and Controls

AWS Policies

Route 53
CID 162: Ensure AWS Route 53 Registered domain has Transfer lock enabled
CID 163: Ensure AWS Route 53 Registered domain has Auto renew Enabled
CID 164: Ensure AWS Route 53 Registered domain is not expired

FireHose
CID 165: Ensure AWS Kinesis Data Firehose delivery stream with Direct PUT and other sources as source has Server-side encryption configured
CID 166: Ensure AWS Kinesis Data Firehose delivery stream with Kinesis Data stream as source has Server-side encryption configured
CID 167: Ensure AWS Kinesis Data Firehose delivery stream with Direct PUT and other sources as source has Server-side encryption configured with KMS Customer Managed Keys

KMS
CID 174: Ensure that Customer managed KMS keys use external key material

AWS Lambda Best Practices Policy
We support AWS Lambda Best Practices Policy specifically for Lambda resources. The pre-defined system policy is loaded with following system-defined controls.
CID 97: Ensure that Lambda function has tracing enabled
CID 98: Ensure that Lambda Function is not using An IAM role for more than one Lambda Function
CID 99: Ensure that Multiple Triggers are not configured in Lambda Function
CID 100: Ensure that Lambda Runtime Version is latest and not custom
CID 101: Ensure that Lambda function does not have Admin Privileges
CID 102: Ensure that Lambda function does not have Cross Account Access
CID 103: Ensure that Lambda Environment Variables at-rest are encrypted with CMK
CID 104: Ensure that Lambda Environment Variables are encrypted using AWS encryption helpers for encryption in transit
CID 105: Ensure that Lambda function is not Exposed (Ensure that Lambda function does not allows anonymous invocation)
CID 106: Ensure that VPC access for Lambda Function is not set to default(Null)
CID 107: Ensure that AWS Lambda excess Permissions are removed
Note: This control is not applicable for GovCloud region.
CID 125: Ensure that multiple triggers are not configured for Lambda Function Aliases
Appendix: List of Policies and Controls
AWS Policies

**AWS Database Service Best Practices Policy**

We have AWS Database Service Best Practices Policy. This policy covers best practices for Paas database configuration exposed by AWS.

**RDS**

**RedShift Clusters**

**DocumentDB Instance**

**Document DB Clusters**

**Neptune DB Clusters**

**RDS**

CID 51: Ensure that Public Accessibility is set to No for Database Instances
CID 52: Ensure DB snapshot is not publicly visible
CID 53: Ensure Encryption is enabled for the database Instance
CID 54: Ensure database Instance snapshot is encrypted
CID 55: Ensure auto minor version upgrade is enabled for a Database Instance
CID 56: Ensure database Instance is not listening on to a standard/default port
CID 69: Ensure automated backups are enabled for RDS database instances
CID 70: Ensure that Deletion Protection is enabled for RDS DB Cluster
CID 71: Ensure that Deletion Protection is enabled for RDS Database instances
CID 72: Ensure that IAM Database Authentication is Enabled for the DB Cluster
CID 73: Ensure that IAM Database Authentication is Enabled for the DB Instances
CID 74: Ensure that AWS RDS Log Exports is enabled for DB Cluster
CID 75: Ensure that AWS RDS Log Exports is enabled for DB Instances
CID 76: Ensure that RDS Database Master username is not set to well-known/default
CID 77: Ensure VPC security group attached to RDS Database Instance does not allows Inbound traffic from ANY source IP
CID 78: Ensure RDS DB instances are not present in public subnets
CID 79: Ensure RDS DB Cluster are not present in public subnets
CID 80: Ensure Event Subscriptions for Instance Level Events is Enabled for DB Instances
CID 81: Ensure RDS Microsoft SQL instance enforces encrypted connections only
CID 82: Ensure RDS PostgreSQL instance enforces encrypted connections only
CID 83: Ensure RDS PostgreSQL Cluster enforces encrypted connections only
CID 84: Ensure that Encryption is enabled for the RDS DB Cluster
CID 85: Ensure RDS DB Cluster snapshots are encrypted
CID 86: Ensure CMK is used to protect RDS DB Cluster encryption key
CID 87: Ensure CMK is used to protect RDS Db Instance encryption key
CID 88: Ensure DB instance replication is set to the another Zone for High Availability
CID 89: Ensure that DB Cluster replication is set to the another Zone for High Availability
CID 90: Ensure RDS database Cluster snapshots are not public
CID 91: Ensure that Enhance monitoring is enabled for RDS Database Instance
CID 92: Ensure that AWS RDS DB Cluster with copy tags to snapshots option is enabled
CID 93: Ensure AWS RDS instances with copy tags to snapshots option is enabled
CID 94: Ensure Event Subscriptions for cluster Level Events is Enabled for DB Clusters
CID 95: Ensure MYSQL DB Instance backup Binary logs configuration is not enabled
CID 96: Ensure backup configuration is enabled for MSSQL DB Instances
CID 117: Ensure that RDS Instances certificates are rotated

**RedShift Clusters**
CID 108: Ensure Version Upgrade is enabled for AWS Redshift clusters to automatically receive upgrades
CID 109: Ensure that AWS Redshift database clusters are not using default endpoint port
CID 110: Ensure that Redshift clusters are not publicly accessible
CID 111: Ensure that AWS Redshift clusters master username is not set to well-known/default
CID 112: Ensure that AWS Redshift clusters encryption is set for data at rest
CID 113: Ensure audit logging is enabled for AWS Redshift clusters for security and troubleshooting purposes

**DocumentDB Instance**
CID 118: Ensure that DocumentDB Instances certificates are rotated

**Document DB Clusters**
CID 132: Ensure DocumentDB database cluster master username is not set to well-known/default
CID 133: Ensure backup retention is set to minimum of 7 days for DocumentDB clusters
CID 134: Ensure audit logs is enabled for Log export to CloudWatch for DocumentDB clusters
CID 135: Ensure deletion protection is enabled for DocumentDB clusters
CID 136: Ensure DocumentDB Cluster is not listening on default port
Neptune DB Clusters
CID 137: Ensure multi-AZ high availability is enabled for neptune database cluster
CID 138: Ensure neptune database cluster is not listening on default port
CID 139: Ensure IAM db authentication is enabled for neptune database cluster
CID 140: Ensure backup retention is set to minimum of 7 days for neptune database cluster
CID 141: Ensure Audit logs is enabled for log exports to cloudwatch for neptune database cluster
CID 142: Ensure Auto minor version upgrade is enabled for neptune database instances
CID 143: Ensure deletion protection is enabled for neptune database cluster

DynamoDB
CID 169: Ensure DynamoDB tables are encrypted using KMS Customer managed Keys
CID 173: Ensure DynamoDB tables are not configured using DEFAULT encryption
Appendix: List of Policies and Controls
Azure Policies

Let us view all the policies and associated controls for Azure.

CIS Microsoft Azure Foundations Benchmark
We support controls for following Azure resources:

Security Centre
Storage Accounts
SQL Server Database
SQL Servers
MySQL Server
PostgreSQL Server
Logging and Monitoring
Networking
Virtual Machines
Web App
Key Vault
Kubernetes
Azure Active Directory

Security Centre
CID 50003: Ensure ASC Default policy setting Monitor Application Whitelisting is not Disabled
CID 50004: Ensure that 'Automatic provisioning of monitoring agent' is set to 'On'
CID 50005: Ensure ASC Default policy setting Monitor System Updates is not Disabled
CID 50006: Ensure ASC Default policy setting Monitor OS Vulnerabilities is not Disabled
CID 50007: Ensure ASC Default policy setting Monitor OS Endpoint Protection is not Disabled
CID 50008: Ensure ASC Default policy setting Monitor Disk Encryption is not Disabled
CID 50009: Ensure ASC Default policy setting Monitor Network Security Groups is not Disabled
CID 50010: Ensure ASC Default policy setting Monitor Web Application Firewall is not Disabled
CID 50014: Ensure ASC Default policy setting Monitor SQL Auditing is not Disabled
CID 50015: Ensure that standard pricing tier is selected
CID 50016: Ensure ASC Default policy setting Enable Next Generation Firewall (NGFW) Monitoring is not Disabled
CID 50017: Ensure ASC Default policy setting Monitor Vulnerability Assessment is not Disabled
CID 50018: Ensure ASC Default policy setting Monitor Storage Blob Encryption is not Disabled
CID 50019: Ensure ASC Default policy setting Monitor JIT Network Access is not Disabled
CID 50020: Ensure that 'Security contact emails' is set
CID 50021: Ensure that security contact 'Phone number' is set
CID 50022: Ensure that 'Send me emails about alerts' is set to 'On'
CID 50023: Ensure that 'Send email also to subscription owners' is set to 'On'
CID 50025: Ensure ASC Default policy setting Monitor SQL Encryption is not Disabled
CID 50078: Ensure that Settings - Threat Detection for Windows Defender ATP (WDATP) is selected
CID 50079: Ensure that Standard pricing tier is enabled for PaaS SQL servers
CID 50080: Ensure that Standard pricing tier is enabled for App Service
CID 50081: Ensure that Standard pricing tier is enabled for Storage Accounts
CID 50082: Ensure any of the ASC Default policy setting is not set to “Disabled”

Storage Accounts
CID 50011: Ensure that Secure transfer required for a Storage Account is set to Enabled
CID 50012: Ensure that 'Public access level' is set to Private for blob containers
CID 50052: Ensure default network access rule for Storage Accounts is set to deny
CID 50053: Ensure 'Trusted Microsoft Services' is enabled for Storage Account access

SQL Server Database
CID 50001: Ensure that Data encryption is set to ON for a SQL database

SQL Servers
CID 50002: Ensure no SQL Servers allow ingress from Internet (ANY IP)
CID 50013: Ensure that default Auditing policy for a SQL Server is configured to capture and retain the activity logs
CID 50027: Ensure SQL servers TDE protector is encrypted with BYOK (Use your own key)
CID 50028: Ensure that Advanced Data Security is enabled and Advanced Threat Protection settings is configured properly for a SQL Server
CID 50035: Ensure that Azure Active Directory Admin is configured for a SQL Server
CID 50083: Ensure that ADS - Vulnerability Assessment (VA) is enabled and configured properly

**MySQL Server**
CID 50039: Ensure 'Enforce SSL connection' is set to 'ENABLED' for MySQL Database Server

**PostgreSQL Server**
CID 50040: Ensure "Enforce SSL connection" is set to "ENABLED" for PostgreSQL Database Server
CID 50041: Ensure server parameter log_checkpoints" is set to "ON" for PostgreSQL Database Server
CID 50042: Ensure server parameter log_connections" is set to "ON" for PostgreSQL Database Server
CID 50043: Ensure server parameter log_disconnections" is set to "ON" for PostgreSQL Database Server
CID 50044: Ensure server parameter log_duration" is set to "ON" for PostgreSQL Database Server
CID 50045: Ensure server parameter log_retention_days" is greater than 3 days for PostgreSQL Database Server
CID 50074: Ensure server parameter connection_throttling" is set to "ON" for PostgreSQL Database Server

**Logging and Monitoring**
CID 50024: Ensure that LogProfile for a subscription is configured properly
CID 50063: Ensure Activity Log Alert exists for Create Policy Assignment
CID 50064: Ensure Activity Log Alert exists for Create or Update Network Security Group
CID 50065: Ensure Activity Log Alert exists for Delete Network Security Group
CID 50066: Ensure Activity Log Alert exists for Create or Update Network Security Group Rule
CID 50067: Ensure Activity Log Alert exists for Delete Network Security Group Rule
CID 50068: Ensure Activity Log Alert exists for Create or Update Security Solution
CID 50069: Ensure Activity Log Alert exists for Delete Security Solution
CID 50070: Ensure Activity Log Alert exists for Create or Update SQL Server Firewall Rule
CID 50071: Ensure Activity Log Alert exists for Update Security Policy
CID 50056: Ensure Storage account containing container with activity logs is encrypted with BYOK
CID 50076: Ensure storage container storing activity logs is not publicly accessible
Appendix: List of Policies and Controls

Azure Policies

Networking
CID 50029: Disable RDP access on Network Security Groups from Internet (ANY IP)
CID 50031: Disable SSH access on Network Security Groups from Internet (ANY IP)
CID 50055: Ensure Network Security Group Flow Log retention is greater than 90 days
CID 50062: Ensure Network Watcher is Enabled for your Subscription

Virtual Machines
CID 50032: Ensure that all unattached VM disks are encrypted
CID 50033: Ensure that all attached VM disks are encrypted
CID 50034: Ensure disks are encrypted for Windows VMs with ADE version 1.1

Web App
CID 50047: Ensure App Service Authentication is set on Azure App Service
CID 50048: Ensure web app redirects all HTTP traffic to HTTPS in Azure App Service
CID 50049: Ensure web app has 'Client Certificates (Incoming client certificates)' set to 'On'
CID 50050: Ensure that 'Register with Azure Active Directory' is enabled on App Service
CID 50051: Ensure web app is using the latest version of TLS encryption version
CID 50061: Ensure that 'HTTP Version' is latest, if used to run the web app

Key Vault
CID 50026: Ensure keyvault is recoverable
CID 50030: Ensure that the expiry date is set on all Secrets
CID 50054: Ensure that logging for Azure KeyVault is 'Enabled'
CID 50075: Ensure that diagnostic settings for Azure KeyVault is set to ON

Kubernetes
CID 50046: Enable RBAC within Azure Kubernetes Services
Note: This control is not applicable for GovCloud

Azure Active Directory
CID 50072: Ensure that there are no guest users
Note: This control is not applicable for GovCloud
CID 50073: Ensure no custom subscription owner roles are created
Azure Best Practices Policy

We support Azure Best Practices Policy to evaluate the following controls.

Virtual Machines

Snapshot

Security Center

SQL Servers

Kubernetes

Application Gateway

Container Registries

Monitor

Virtual Network Subnet

Resource Group

Virtual Machines
CID 50034: Ensure disks are encrypted for Windows VMs with ADE version 1.1
CID 50130: Ensure that the endpoint protection for all Virtual Machines is installed

Snapshot
CID 50038: Ensure disk snapshots are encrypted.

Security Center
CID 50077: Ensure that Settings - Threat Detection for Microsoft Cloud App Security (MCAS) is selected
CID 50078: Ensure that Settings - Threat Detection for Windows Defender ATP (WDATP) is selected
CID 50082: Ensure any of the ASC Default policy setting is not set to 'Disabled'

SQL Servers
CID 50083: Ensure that ADS - Vulnerability Assessment (VA) is enabled and configured properly

Kubernetes
CID 50090: Ensure that Azure AKS cluster monitoring is enabled
CID 50091: Ensure that Azure AKS cluster HTTP application routing is disabled
CID 50092: Ensure that Azure AKS cluster Azure CNI networking is enabled

Application Gateway
CID 50093: Ensure that Azure Application Gateway have Web application firewall (WAF) enabled
CID 50094: Ensure that Azure Application Gateway allows TLSv1.2 or above

**Container Registries**
CID 50057: Ensure that Azure Container Registry using the deprecated classic registry

**Monitor**
CID 50059: Ensure Activity Log Alert for Delete SQL server firewall rule
CID 50125: Ensure Activity Log Alert exists for Create/Update Storage Account
CID 50126: Ensure Activity Log Alert exists for Delete Storage Account
CID 50127: Ensure Activity Log Alert exists for Create or Update Virtual Machine
CID 50128: Ensure Activity Log Alert exists for Deallocate Virtual Machine
CID 50129: Ensure Activity Log Alert exists for Delete Virtual Machine

**Virtual Network Subnet**
CID 50060: Ensure that Azure Virtual Network subnet is configured with a Network Security Group

**Resource Group**
CID 50036: Ensure that Azure Resource Group have a resource lock

**Azure Function App Best Practices Policy**

We support Azure Function App Best Practices Policy to help you in automated auditing and reporting on the Azure Function app misconfigurations, unwarranted access, and non-standard deployments, and provide remediation steps to manage risks.

**Function App**
CID 50084: Ensure App Service Authentication is set on Function Apps
CID 50085: Ensure Function app redirects all HTTP traffic to HTTPS
CID 50086: Ensure function app has 'Client Certificates (Incoming client certificates)' set to 'On'
CID 50087: Ensure that 'Register with Azure Active Directory' is enabled on Function app
CID 50088: Ensure function app is using the latest version of TLS encryption version
CID 50089: Ensure that 'HTTP Version' is latest, if used to run the function app
Appendix: List of Policies and Controls

Azure Policies

Azure Database Service Best Practices Policy

We have a policy that helps in automated auditing and reporting on the Azure Database service resources misconfigurations, unwarranted access and non-standard deployments, and provides remediation steps to manage risks. To help secure your Azure resources, follow the recommendations for the Database services of Azure.

**SQL Server Database**

**SQL Servers**

**MySQL Server**

**MariaDB Server**

**PostgreSQL Server**

**CosmosDB**

**SQL Server Database**

CID 50095: Ensure that default Auditing policy for a SQL Database is configured to capture and retain the activity logs

CID 50096: Ensure that Advanced Data Security is enabled and Advanced Threat Protection settings is configured properly for a SQL Database

**SQL Servers**

CID 50098: Ensure that ‘ssl_minimal_tls_version_enforced’ is set to ‘1.2’ for SQL server

**MySQL Server**

CID 50102: Ensure that Advanced Threat Protection settings is configured properly for Azure Database for MySQL Server

CID 50103: Ensure that TLS is enforced and the minimum version be set to 1.2 for Azure Database for MYSQL server

CID 50104: Ensure no MySQL Server allow ingress from Internet (ANY IP)

CID 50105: Ensure that ‘geo_redundant_backup_enabled’ is set to Enabled for Azure Database for MySQL server

CID 50106: Ensure that Public Network Access is Disabled for Azure Database for MySQL server

CID 50107: Ensure that Azure Database for MySQL server diagnostic setting is configured properly

CID 50131: Ensure that Azure Active Directory authentication is configured for MySql server

**MariaDB Server**

CID 50108: Ensure that Advanced Threat Protection settings is configured properly for Azure Database for MariaDB Server
CID 50109: Ensure 'Enforce SSL connection' is set to 'ENABLED' for Azure Database for MariaDB server

CID 50110: Ensure that TLS is enforced and the minimum version be set to 1.2 for Azure Database for MariaDB server

CID 50111: Ensure no MariaDB Server allow ingress from Internet (ANY IP)

CID 50112: Ensure that 'geo_redundant_backup_enabled' is set to Enabled for Azure Database for MariaDB server

CID 50113: Ensure that Public Network Access is Disabled for Azure Database for MariaDB server

**PostgreSQL Server**

CID 50115: Ensure that Advanced Threat Protection settings is configured properly for Azure Database for PostgreSQL Server

CID 50116: Ensure that TLS is enforced and the minimum version be set to 1.2 for Azure Database for PostgreSQL server

CID 50117: Ensure no PostgreSQL Server allow ingress from Internet (ANY IP)

CID 50118: Ensure that 'geo_redundant_backup_enabled' is set to Enabled for Azure Database for PostgreSQL server

CID 50119: Ensure that Public Network Access is Disabled for Azure Database for PostgreSQL server

CID 50120: Ensure that Azure Database for PostgreSQL server diagnostic setting is configured properly

CID 50132: Ensure that Azure Active Directory authentication is configured for PostgreSQL server

**CosmosDB**

CID 50121: Ensure that automatic-failover is set for Azure CosmosDB

CID 50122: Ensure that Diagnostic settings are set for CosmosDB

CID 50123: Ensure that lock is set on Azure CosmosDB

CID 50124: Ensure that CosmosDB does not allow access from all networks
GCP Policies

Let us view all the policies and associated controls for GCP.

CIS Google Cloud Platform Foundation Benchmark

We support controls for following Google Cloud Platform (GCP) resources:

IAM & Admin
Logs Router
Logs-based metrics
Storage
Network
Firewall rules
Subnetwork
Cloud SQL- Mysql
Cloud SQL- SQL Server
Cloud SQL- PostgreSQL
Cloud Functions
VM Instances
Dataset
Cloud DNS

IAM & Admin
CID 52000: Ensure that corporate login credentials are used instead of Gmail accounts
CID 52001: Ensure that there are only GCP-managed service account keys for each service account
CID 52002: Ensure that ServiceAccount has no Admin privileges
CID 52003: Ensure that IAM users are not assigned Service Account User role at project level
CID 52004: Ensure user-managed/external keys for service accounts are rotated every 90 days or less
CID 52005: Ensure Encryption keys are rotated within a period of 365 days
CID 52006: Ensure that Separation of duties is enforced while assigning KMS related roles
CID 52007: Ensure that IAM users are not assigned Service Account Token Creator role at project level
CID 52008: Ensure that Cloud Audit Logging is configured properly across all services and all users from a project
CID 52090: Ensure that Cloud KMS cryptokeys are not anonymously or publicly accessible

Logs Router
CID 52009: Ensure that sinks are configured for all Log entries

Logs-based metrics
CID 52011: Ensure log metric filter and alerts exists for Project Ownership assignments/changes
CID 52012: Ensure log metric filter and alerts exists for Audit Configuration Changes
CID 52013: Ensure log metric filter and alerts exists for Custom Role changes
CID 52014: Ensure log metric filter and alerts exists for VPC Network Firewall rule changes
CID 52015: Ensure log metric filter and alerts exists for VPC network route changes
CID 52016: Ensure log metric filter and alerts exists for VPC network changes
CID 52017: Ensure log metric filter and alerts exists for Cloud Storage IAM permission changes
CID 52018: Ensure log metric filter and alerts exists for SQL instance configuration changes

Storage
CID 52030: Ensure that Cloud Storage bucket is not anonymously or publicly accessible
CID 52036: Ensure that Cloud Storage buckets have uniform bucket-level access enabled
CID 52057: Ensure that there are no harmful object life cycle rules are created on Storage Buckets
CID 52058: Ensure that object retention policy is set on storage buckets
CID 52099: Ensure that retention policies on log buckets are configured using Bucket Lock

Network
CID 52019: Ensure the default network does not exist in a project
CID 52034: Ensure legacy networks do not exist for a project

Firewall rules
CID 52021: Ensure that SSH access is restricted from the internet
CID 52022: Ensure that RDP access is restricted from the internet

Subnetwork
CID 52024: Ensure VPC Flow logs is enabled for every subnet in VPC Network

Cloud SQL - Mysql
CID 52032: Ensure that Cloud SQL - Mysql database Instance requires all incoming connections to use SSL
CID 52033: Ensure that Cloud SQL - Mysql database Instances are not open to the world
CID 52076: Ensure 'local_infile' database flag for Cloud SQL - Mysql instance is set to 'off'
CID 52084: Ensure Cloud SQL - MySQL Instance do not have public IP addresses
CID 52087: Ensure Cloud SQL- MySQL instance is configured with automated backups

Cloud SQL- SQL Server
CID 52067: Ensure that Cloud SQL - SQL Server database instance requires all incoming connections to use SSL
CID 52068: Ensure that Cloud SQL - SQL Server database Instances are not open to the world
CID 52078: Ensure 'cross db ownership chaining' database flag for Cloud SQL - SQL Server instance is set to 'off'
CID 52083: Ensure 'contained database authentication' database flag for Cloud SQL SQL Server instance is set to 'off'
CID 52085: Ensure Cloud SQL - SQL server Instance do not have public IP addresses
CID 52088: Ensure Cloud SQL- SQL server is configured with automated backups

Cloud SQL- PostgreSQL
CID 52059: Ensure 'log_connections' database flag for Cloud SQL - PostgreSQL instance is set to 'on'
CID 52060: Ensure 'log_disconnections' database flag for Cloud SQL - PostgreSQL instance is set to 'on'
CID 52065: Ensure that Cloud SQL - PostgreSQL database instance requires all incoming connections to use SSL
CID 52066: Ensure that Cloud SQL - PostgreSQL database Instances are not open to the world
CID 52069: Ensure 'log_lock_waits' database flag for Cloud SQL - PostgreSQL instance is set to 'on'
CID 52070: Ensure 'log_temp_files' database flag for Cloud SQL - PostgreSQL instance is set to '0' (on)
CID 52072: Ensure 'log_min_messages' database flag for Cloud SQL - PostgreSQL instance is set to 'Error' or stricter
CID 52073: Ensure 'log_min_duration_statement' database flag for Cloud SQL - PostgreSQL instance is set to '-1' (disabled)
CID 52074: Ensure 'log_checkpoints' database flag for Cloud SQL - PostgreSQL instance is set to 'on'
CID 52086: Ensure Cloud SQL - PostgreSQL Instance do not have public IP addresses
CID 52089: Ensure Cloud SQL - PostgreSQL is configured with automated backups

**Cloud Functions**
CID 52054: Ensure that Default service account is not used for the cloud function
CID 52055: Ensure that Runtime used in cloud function is not deprecated
CID 52056: Ensure that Cloud function is not anonymously or publicly accessible

**VM Instances**
CID 52020: Ensure that IP forwarding is not enabled on Instances
CID 52025: Ensure that instances are not configured to use the default service account with full access to all Cloud APIs
CID 52026: Ensure Block Project-wide SSH keys "enabled for VM instances"
CID 52027: Ensure oslogin is enabled for a Project
CID 52028: Ensure Enable connecting to serial ports "is not enabled for VM Instance"
CID 52029: Ensure VM disks for critical VMs are encrypted with Customer-Supplied Encryption Keys (CSEK)
CID 52091: Ensure Compute instances are launched with Shielded VM enabled
CID 52093: Ensure that instances are not configured to use default service account
CID 52094: Ensure that Compute instances do not have public IP addresses

**Datasets**
CID 52098: Ensure that BigQuery datasets are not anonymously or publicly accessible

**Cloud DNS**
CID 52100: Ensure that DNSSEC is enabled for Cloud DNS
GCP Best Practices Policy

We support GCP Best Practices Policy to evaluate the following controls.

Storage

CID 52010: Ensure that object versioning is enabled on buckets
CID 52031: Ensure that logging is enabled for Cloud storage buckets
CID 52057: Ensure that there are no harmful object life cycle rules are created on Storage Buckets
CID 52058: Ensure that object retention policy is set on buckets
CID 52108: Ensure that GCP Storage bucket is encrypted using customer-managed key

VM Instance

CID 52092: Ensure oslogin is enabled for VM instance

Dataset

CID 52095: Ensure that BigQuery Dataset is encrypted with Customer-managed key

Table

CID 52096: Ensure that BigQuery Table is encrypted with Customer-managed key

Subnetwork

CID 52023: Ensure Private Google Access is enabled for all subnetwork in VPC Network

Cloud DNS

CID 52109: Ensure that GCP Cloud DNS zones is using RSASHA1 algorithm for DNSSEC key-signing
CID 52110: Ensure that GCP Cloud DNS zones is using RSASHA1 algorithm for DNSSEC zone-signing
Appendix: List of Policies and Controls

GCP Policies

**GCP Cloud Functions Best Practices Policy**

We have GCP Cloud Functions Best Practices Policy that covers Cloud Functions Services of Google Cloud Platform. The controls in this policy are targeted only for Cloud Functions service.

**Function App**

CID 52054: Ensure that Default service account is not used for the Cloud Function

CID 52055: Ensure that Runtime used in Cloud Function is not deprecated

CID 52056: Ensure that Cloud Function is not anonymously or publicly accessible

**GCP Kubernetes Engine Best Practices Policy**

We have GCP Kubernetes Engine Best Practices Policy. It covers Google Kubernetes Engine Service of Google Cloud Platform. The controls in this policy are targeted only towards Google Kubernetes Engine service. The pre-defined GCP Kubernetes Engine Best Practices is loaded with the 22 system-defined controls.

CID 52037: Ensure that GCP Kubernetes cluster intra-node visibility is enabled

CID 52038: Ensure Legacy Authorization is set to Disabled on Kubernetes Engine Clusters

CID 52039: Ensure Kubernetes web UI / Dashboard is disabled

CID 52040: Ensure Automatic node repair is enabled for Kubernetes Clusters

CID 52041: Ensure Automatic node upgrades is enabled on Kubernetes Engine Clusters nodes

CID 52042: Ensure that GCP Kubernetes Engine Clusters have HTTP load balancing enabled

CID 52043: Ensure Network policy is enabled on Kubernetes Engine Clusters

CID 52044: Ensure that GCP Kubernetes Engine Clusters have Alpha cluster feature disabled

CID 52045: Ensure Kubernetes Cluster is created with Alias IP ranges enabled

CID 52046: Ensure PodSecurityPolicy controller is enabled on the Kubernetes Engine Clusters

CID 52047: Ensure Kubernetes Cluster is created with Private cluster enabled

CID 52048: Ensure Private Google Access is set on Kubernetes Engine Cluster Subnets

CID 52049: Ensure default Service account is not used for Project access in Kubernetes Clusters

CID 52050: Ensure Kubernetes Clusters created with limited service account Access scopes for Project access

CID 52051: Ensure Stackdriver Kubernetes Engine Monitoring is set to Enabled on Kubernetes Engine Clusters
CID 52052: Ensure that Application-Layer secret encryption is enabled for Kubernetes cluster
CID 52053: Ensure that Master authorized network is enabled for Kubernetes cluster
CID 52101: Ensure Binary Authorization is set to Enabled on Kubernetes Engine Clusters
CID 52102: Ensure Container-Optimized OS (cos) is used for Kubernetes Engine Clusters Node image
CID 52103: Ensure GCP Kubernetes Engine Clusters are not using the default network
CID 52104: Ensure that network traffic egress metering is enabled on Kubernetes Engine Clusters
CID 52105: Ensure that legacy compute engine metadata endpoint for GCP Kubernetes Engine Cluster Node is disabled

**GCP Cloud SQL Best Practices Policy**

We have GCP Cloud SQL Best Practices Policy that covers Cloud SQL Service of Google Cloud Platform. The controls in this policy are targeted only towards Cloud SQL service.

**Cloud SQL- PostgreSQL**

CID 52061: Ensure 'log_duration' database flag for Cloud SQL PostgreSQL instance is set to 'on'
CID 52062: Ensure 'log_error_verbosity' database flag for Cloud SQL - PostgreSQL instance is set to 'DEFAULT' or stricter
CID 52063: Ensure log_statement" database flag for Cloud SQL - PostgreSQL instance is set to "ddl" or stricter"
CID 52064: Ensure 'log_hostname' database flag for Cloud SQL - PostgreSQL instance is set to 'off'
CID 52071: Ensure 'log_min_error_statement' database flag for Cloud SQL - PostgreSQL instance is set to 'Error' or stricter
CID 52107: Ensure that Cloud SQL - PostgreSQL database instance Binary logs configuration is enabled

**Cloud SQL- Mysql**

CID 52035: Ensure that MySQL Database Instance does not allows root login from any Host
CID 52075: Ensure 'skip_show_database' database flag for Cloud SQL - Mysql instance is set to 'on'
CID 52106: Ensure that Cloud SQL Mysql database instance Binary logs configuration is enabled
Cloud SQL - SQL Server
CID 52077: Ensure 'external scripts enabled' database flag for Cloud SQL - SQL Server instance is set to 'off'
CID 52080: Ensure 'user options' database flag for Cloud SQL - SQL Server instance is not configured
CID 52081: Ensure 'remote access' database flag for Cloud SQL - SQL Server instance is set to 'off'
CID 52082: Ensure '3625 (trace flag)' database flag for Cloud SQL - SQL Server instance is set to 'off'
CID 52097: Ensure 'default trace enabled' database flag for Cloud SQL - SQL Server instance is set to 'on'