Table of Contents

About this Guide ........................................................................................................................................... 7
  About Qualys ................................................................................................................................................ 7
  Qualys Support ......................................................................................................................................... 7

CloudView Overview ................................................................................................................................. 8
  Qualys Subscription and Modules required .......................................................................................... 8
  Concepts and Terminologies .................................................................................................................. 9

Get Started ................................................................................................................................................ 10
  AWS ............................................................................................................................................................. 10
    Steps to Create AWS Connector ............................................................................................................ 10
    Base Account ...................................................................................................................................... 16
    Base Account Configuration in AWS Console ....................................................................................... 18
    Permissions for Fargate Profile ............................................................................................................. 19
    Create Custom Policy .......................................................................................................................... 21
    Editing AWS Connectors ...................................................................................................................... 23
    AWS Resource Inventory ..................................................................................................................... 23
  Microsoft Azure ....................................................................................................................................... 26
    Pre-requisites ..................................................................................................................................... 26
    Steps to Create Azure Connector .......................................................................................................... 27
    Configuration Steps on Microsoft Azure console .................................................................................. 29
    Editing Microsoft Azure Connectors ..................................................................................................... 37
    Azure Resource Inventory ..................................................................................................................... 37
  Google Cloud Platform ............................................................................................................................. 39
    Steps to Create GCP Connector ............................................................................................................ 39
    Assign Service Account to other projects ............................................................................................ 44
    Editing GCP Connectors ....................................................................................................................... 45
    GCP Resource Inventory ...................................................................................................................... 45
  Enable-Disable Connectors ..................................................................................................................... 46
    Disable Connector ............................................................................................................................... 46
    Enable Connector ............................................................................................................................... 46

Managing Connector Access for Users...................................................................................................... 48
  User Permissions ...................................................................................................................................... 48
  New Users: Scope and Permissions .......................................................................................................... 49
    Create User ......................................................................................................................................... 49
    Assign Role to Users ........................................................................................................................... 50
    Manage Access for Users (Grouping Connectors) ................................................................................ 51
  Manage Access for Users ....................................................................................................................... 53
  Defining Scope for Existing Users .......................................................................................................... 55
  Sub User (All Privileges) .......................................................................................................................... 56

Verity Confidential
Sub User (Reader Privileges) ................................................................. 59

Securing Cloud Resources ................................................................. 61
Unified Dashboard ............................................................................. 61
Resources Details ............................................................................. 61
  Instance Details ............................................................................. 63
  Vulnerability Details for Instances ............................................. 63
  Drill down to Vulnerability Details for Instances (only for AWS)  66
  View Security Group Information .............................................. 67
Resources Misconfigurations ......................................................... 69
  Search Using Resource Parameter Information .......................... 73
  Search Policy Controls ................................................................. 74
IaC Posture ...................................................................................... 77
  Search Policy Controls ................................................................. 77
Exceptions ...................................................................................... 80
  Create Exception ......................................................................... 80
  View Exceptions ......................................................................... 86
  Edit Exceptions? .......................................................................... 86
  Delete exceptions? ...................................................................... 87
  Exception History ........................................................................ 87
  Exception Status ......................................................................... 87

Policies and Controls .................................................................... 89
  Customize Controls ..................................................................... 89
  System Controls ......................................................................... 90
  User-Defined Controls ............................................................... 90
  Controls Category: Execution Type .......................................... 90
  Control Criticality ....................................................................... 91
  Copy Control and Customize .................................................... 92
Build Your Own Policy ................................................................. 93
  System Defined Policy ............................................................... 93
  Set Up Your Own Policy (Custom Policy) ................................ 93
  Policy Search ............................................................................. 95
  Associating Controls .................................................................. 95

Reports .......................................................................................... 96
  Assessment Reports ................................................................. 96
  On-Screen Reports .................................................................... 99
    Mandate Based Reporting .......................................................... 99
    Policy Based Report ................................................................ 103
    List of Mandates ..................................................................... 106

Responses ..................................................................................... 108
  Configure Rule-based Alerts ...................................................... 108
Create and Manage Actions ............................................................... 109
  Create a new Action ........................................................................ 109
  Manage Actions ........................................................................... 110
Create and Manage Rules ............................................................... 110
  Create New Rule ........................................................................... 110
  Manage Rules ............................................................................... 112
Manage Alerts .................................................................................. 112
  Sample Queries ........................................................................... 112
  Trigger Criteria ........................................................................... 113
Alerting Permissions ........................................................................ 114

**Remediating Cloud Resources** ......................................................... 116
Configuring Remediation ................................................................. 116
  Pre-requisites ............................................................................... 116
Configure Remediation for New Connectors: AWS ......................... 117
  Enable Remediation for New Connectors ..................................... 117
  Configuration on AWS Console ................................................. 118
  Enable Remediation for Existing AWS Connectors .................... 120
Configure Remediation: Microsoft Azure ........................................ 121
  Pre-requisites ............................................................................ 121
  Enable Remediation for New Azure Connectors ....................... 121
  Configuration on Microsoft Azure Console ............................... 122
  Enabling Remediation for Existing Azure Connectors ............... 123
Configure Remediation: GCP ............................................................ 123
  Enable Remediation for New GCP Connectors ........................... 123
  Configuration on GCP Console .................................................. 124
  Enabling Remediation for Existing GCP Connectors ................. 126
Viewing Remediation Activity .......................................................... 127
  Remediation Activity: AWS ...................................................... 127
  Remediation Activity: Microsoft Azure ..................................... 128
  Remediation Activity: GCP ....................................................... 128
Remediating Cloud Resources .......................................................... 129
  Remediable Evaluations .............................................................. 129
Actions for Cloud Resources (AWS) ................................................ 131
  Stop Instance ............................................................................ 131
  Remove IAM Profile ................................................................. 132
Permissions Required ........................................................................ 133

**CloudView APIs** ........................................................................... 136
Accessing APIs Using Swagger ......................................................... 136

**Securing Infrastructure as Code** ................................................... 138
Template Support ............................................................................. 138
Pre-requisites .................................................................................. 139
About this Guide

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

About Qualys

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

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

Qualys Support

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

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

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

Qualys Subscription and Modules required

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

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

Get familiar with common terms used in CloudView.

<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 - 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 it’s 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 it’s 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.

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

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

where,

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

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

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

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

IMPORTANT: All previously created connectors continue to work as configured. If the customer has to update a connector or create a new connector, they need to provide the external ID in the new format.
Launch your AWS console, and go to IAM > Roles and click Create Role. In the Create role window, choose “Another AWS account”. Paste in the Qualys account ID and the External ID that you copied in the previous step. Click Next: Permissions.

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

Select the following policies:

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

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

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

c) Create a custom policy that includes additional permissions (applicable only for Elastic File System (EFS), Step Functions, Amazon Quantum Ledger Database (QLDB), Managed Streaming for Apache Kafka (MSK), API Gateway, AWS Backup, WAF, and CodeBuild resources). Find the custom policy you create and select the check box next to the policy. For detailed steps on the creation of custom policy and the required permissions, see Create Custom Policy.
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": "Stmt1581205548000",
    "Effect": "Allow",
    "Action": [
      "sts:AssumeRole"
    ],
    "Resource": [
      "*"
    ]
  }
]
```

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

![Create IAM User Image]
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.

Permissions for Fargate Profile

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

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

Create the policy

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

2 - In the navigation pane, choose Policies.

3 - In the content pane, choose Create policy.

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

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "InventoryPermissions",
            "Effect": "Allow",
            "Action": [
                "eks:ListFargateProfiles",
                "eks:DescribeFargateProfile"
            ]
        }
    ]
}
```
5 - Click Next: Tags.

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

![Create policy](image)

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

### Attach Policy To The IAM Role

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

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

2 - In the navigation pane, choose Roles.

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

4 - Choose the Permissions tab and click Attach Policies.

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

You need additional permissions to evaluate controls related to the following resources:
- Elastic File System (EFS)
- Step Functions
- Amazon Quantum Ledger Database (QLDB)
- Managed Streaming for Apache Kafka (MSK)
- API Gateway
- AWS Backup
- WAF
- CodeBuild

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

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

Create the Custom Policy

1 - Log in to your Amazon Web Services (AWS) IAM console at https://console.aws.amazon.com/iam/ with user that has administrator permissions.
2 - In the navigation pane, choose Policies.
3 - In the content pane, choose Create policy.
4 - Choose the JSON tab. Paste the following text into the JSON text box.

```json
{
   "Version":"2012-10-17",
   "Statement":[
   {
      "Sid":"QualysCustomPolicyPermissions",
      "Effect":"Allow",
      "Action":[
         "states:DescribeStateMachine",
         "elasticfilesystem:DescribeFileSystemPolicy",
         "qldb:ListLedgers",
         "qldb:DescribeLedger",
         "kafka:ListClusters",
         "codebuild:BatchGetProjects",
         "wafv2:GetWebACLForResource",
         "backup:ListBackupVaults",
         "backup:DescribeBackupVault"
      ],
      "Resource":"*"
   }
}"
```

5 - Click Next: Tags.

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

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

**Attach Policy To The IAM Role**

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

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

2 - In the navigation pane, choose Roles.

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

4 - Choose the Permissions tab and click Attach Policies.

5 - Find the policy you created (example: Sample_Custom_Policy) and click Attach Policy.
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
- EKS Cluster
- EKS Node Group
- EKS Fargate Profile
Microsoft Azure

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

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

Pre-requisites

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

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

**Assign Azure Active Directory permissions**

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

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

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

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

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

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

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](image)

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

**Assign Custom Role**

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

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

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

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

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

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

**Create Custom Role**

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

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

Run command:

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

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

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

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

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) Provide a project Id for your GCP connector.

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

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

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

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

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

(6) Click Create Connector.

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

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

Enable Access to Compute Engine and Resource Manager API

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

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

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

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

**Assign Service Account to other projects**

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

Let us view the steps for the same.

**Assign Service Account in IAM at project level**

1. Login to Google Cloud Platform (GCP) console.
2. From the left navigation bar, select IAM & admin.
3. Select the project from the drop-down menu in the top-left corner.
4. In the IAM menu bar, click +ADD.
5. In the New Members box, type the name of the service account and click the suggested value.
6. In the Select a role drop-down box, select the appropriate role. Choose Viewer role and Security Reviewer role to assign at least reader permissions to the service account.
7. Click Save.
8. To add additional projects, repeat steps 3 through 7.

**Assign Service Account in IAM at organization level**

1. Login to Google Cloud Platform (GCP) console.
2. In the left navigation bar, select IAM & admin.
3. Select your organization from the drop-down menu in the top-left corner.
4. In the IAM menu bar, click +ADD.
5. In the New Members box, type the name of the service account and click the suggested value.
6. In the Select a role drop-down box, select the appropriate role. Choose Viewer role and Security Reviewer role to assign at least reader permissions to the service account.
7. Click Save.
**Editing GCP Connectors**

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

You can now edit the required details.

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

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

**GCP Resource Inventory**

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

**Resources List**

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

- VM Instances
- Networks
- Firewall Rules
- Subnetworks
- Cloud Functions
Enable-Disable Connectors

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

Disable Connector

1) Go to Configuration tab and then the cloud provider tab, where the connector belongs.
2) Select the connector to be disabled and from the quick actions menu, select Disable from the quick actions menu.
3) Click on the confirmation message. The connector gets disabled.

Enable Connector

1) Go to Configuration tab and then the cloud provider tab, where the connector belongs.
2) Select the connector to be disabled and from the quick actions menu, select Enable from the quick actions menu.

Note: Automatic or manual connector run skips the disabled connectors. Only connectors with enabled state are executed during connector run.
3) Click on the confirmation message. The connector gets enabled.
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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Assign Groups to Connector**
Let us see how to create connector groups and provide access to a particular connector for a user.
(1) Navigate to Configuration tab and then the Cloud Provider (AWS, Azure, or GCP) for which you would want to create connector group.

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

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

(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.
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 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.
Managing Connector Access for Users
New Users: Scope and Permissions

(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.

![Manage access for AWS](image)

**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.
Managing Connector Access for Users
Sub User (All Privileges)

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

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

The new user is ready to use CloudView with full access capabilities!
Sub User (Reader Privileges)

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

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

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

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

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

Unified Dashboard

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

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

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

Refer to the Unified Dashboard online help for more details.

Resources Details

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

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

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. You can also perform actions on instances such as stop instance or remove IAM profile. These actions are supported only if you have enabled remediation for the connector associated with the instances. For more information, refer to Actions for Cloud Resources (AWS).

Vulnerability Details for Instances

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

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

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

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

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

- If the resource has Qualys Cloud Agent installed, the Agent Summary section displays corresponding details.
Go to Resources and then select the Cloud Provider (AWS, Azure, or Google Cloud Platform). Now, select the resource of instance type and click the resource. The Resource Details page displays the enhanced details.

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.
Securing Cloud Resources
Resources Misconfigurations

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

Controls Evaluation View

Let us see what each number signifies

1 - Total number of controls that are evaluated.
2 - Total number of evaluations. A unique combination of resource and control is treated as one evaluation.
3 - Number of evaluations that Passed. The Pass count includes control evaluations that are passed as well as passed with exception.
4 - Number of evaluations that Failed
5 - Number of failed evaluations with high criticality
6 - Number of failed evaluations with medium criticality
7 - Number of failed evaluations with low criticality
8 - Number of evaluations that can be remediated. Click to view the controls with failed evaluations that are remediable. For more information on remediating cloud misconfigurations, see Remediating Cloud Resources.

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

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

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

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

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

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

Resources Misconfigurations

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.

IaC Posture

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

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

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

Search Policy Controls

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

Go to Monitor > IaC Posture tab. You’ll notice a Search bar above the controls list (you can also search on other tabs). This is where you can enter your search query.
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 also view other failed control for the same resource. Select the control and click Actions or the quick actions menu.

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

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

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

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

Exceptions

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

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

Create Exception

Here are quick steps to create an exception.
1. Go to Monitor tab. You’ll notice a Search field above the controls list. Enter your search query for failed evaluations and click the required control in the search results to view the control evaluations.

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.

- Scope Information: Decides the scope of the exception you are creating. By default, Resource option is selected. You could expand the scope of the exception to all resources in a specific account.
• Resource: Choose to create exception at resource level and the exception is applicable only for the selected resource.

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

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

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

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.

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

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

Customize Controls

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

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

- 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.

Controls Category: Execution Type

The column "Execution Type" on the Controls tab tells you the type of control. The categorization is done depending on the execution type of the control.
- Run Time Controls are controls for evaluations on deployed cloud resources.
- Build Time Controls are controls for cloud resources that reside within the IaC templates.
- Run & Build Time Controls are controls for evaluations on cloud resources in your environment and those which reside within the IaC templates.
Control Criticality

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

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

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.

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

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

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-the-box. To view the complete list of policies and associated controls that Qualys provides, refer to Appendix: List of Policies and Controls.

Set Up Your Own Policy (Custom Policy)

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

(1) Navigate to Policy > Policy > New.

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

You could choose the controls depending on their execution type:

- **Run Time**: controls for evaluations on deployed cloud resources.
- **Build Time**: controls for evaluations on cloud resources within the IaC templates.
Click Next.

(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 or PDF format using our quick actions menu. For detailed information and steps on Assessment report, see Assessment Reports.

**On-Screen Reports**

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

**Assessment Reports**

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

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

**Tell me the Steps**

It’s easy to create a custom report template.

1) Just go to Reports > Reports tab and then click Create New Report.
2) Provide a title and description (optional) to the report template.

3) Choose the report format: CSV or PDF.

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

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

Note:
- For CSV report format, you can select multiple policies.
- For PDF report format, you can select only one policy.

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

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

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

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

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

10) Review the configured report settings in the Summary pane and then click Create and Run Report.
Re-run Assessment Report
To re-run a report, select the report from the Reports page and click Run Again from the quick actions menu.

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

Click Run Report to initiate the report generation.

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

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

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

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

The Report Summary displays the report settings.

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

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

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

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

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

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

We support report generation of policies and mandates for all the cloud providers we support: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). To view the complete list of mandates that we support, see the List of Mandates section.
Launch the Mandate Based Report to view the compliance posture of the organization in terms of the underlying Security baseline against selected Mandates. This allows you to choose any one mandates you have to comply with and get a view of compliance posture in terms of their selected policies.

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

Tell me the Steps

It's easy to create a custom report template.

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

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

**Summary**

Review the report configuration options.

**Basic Information**

- **Title:** My Custom Report
- **Description:** Sample report
- **Cloud Provider:** GCP
- **Policy:** GCP Best Practices Policy
- **Mandate:** CIS Critical Security Controls (Top 5)
- **Format:** On-Screen Report

**Connectors**

<table>
<thead>
<tr>
<th>Selected Groups (1):</th>
</tr>
</thead>
<tbody>
<tr>
<td>GroupTest</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Selected Connectors (1):</th>
</tr>
</thead>
<tbody>
<tr>
<td>GCP-demo</td>
</tr>
</tbody>
</table>
Sample Mandate Based Report

Policy Based Report

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

It’s easy to create a custom report template.

1) Just go to Reports > On-Screen Reports > Create New Template.
2) Provide a title and description (optional) to the report template.

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. ISO/IEC 27001:2013
2. Cloud Controls Matrix (CCM)
3. NERC Critical Infrastructure Protection (CIP)
<table>
<thead>
<tr>
<th>No.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>ANSSI 40 Essential Measures for a Healthy Network</td>
</tr>
<tr>
<td>6</td>
<td>The Australian Signals Directorate - The Essential 8 Strategies (ASD 8)</td>
</tr>
<tr>
<td>7</td>
<td>Reserve Bank of India (RBI) - Baseline Cyber Security and Resilience Requirements (Annex 1)</td>
</tr>
<tr>
<td>8</td>
<td>NESA UAE Information Assurance Standards (IAS)</td>
</tr>
<tr>
<td>9</td>
<td>APRA Prudential Practice Guide (PPG): CPG 234 - Management of Security Risk in Information and Information Technology</td>
</tr>
<tr>
<td>10</td>
<td>IRDAI Guidelines On Information and Cyber Security for Insurers</td>
</tr>
<tr>
<td>11</td>
<td>General Data Protection Regulation (GDPR)</td>
</tr>
<tr>
<td>12</td>
<td>Minimum Acceptable Risk Standards for Exchanges (MARS-E)</td>
</tr>
<tr>
<td>13</td>
<td>NCSC Basic Cyber Security Controls (BCSC)</td>
</tr>
<tr>
<td>14</td>
<td>IRS Publication 1075</td>
</tr>
<tr>
<td>15</td>
<td>NIST Cyber Security Framework (CSF)</td>
</tr>
<tr>
<td>16</td>
<td>Sarbanes-Oxley Act: IT Security</td>
</tr>
<tr>
<td>17</td>
<td>Monetary Authority of Singapore (MAS) - Notice 834: Cyber Hygiene Practices</td>
</tr>
<tr>
<td>18</td>
<td>NIST Special Publication 800-171</td>
</tr>
<tr>
<td>19</td>
<td>CIS Controls Version 8</td>
</tr>
<tr>
<td>20</td>
<td>Criminal Justice Information Services (CJIS) Security Policy</td>
</tr>
<tr>
<td>21</td>
<td>Cybersecurity Maturity Model Certification (CMMC) Level 1</td>
</tr>
<tr>
<td>22</td>
<td>Cybersecurity Maturity Model Certification (CMMC) Level 2</td>
</tr>
<tr>
<td>23</td>
<td>Cybersecurity Maturity Model Certification (CMMC) Level 4</td>
</tr>
<tr>
<td>24</td>
<td>Cybersecurity Maturity Model Certification (CMMC) Level 5</td>
</tr>
<tr>
<td>25</td>
<td>Cybersecurity Maturity Model Certification (CMMC) Level 3</td>
</tr>
<tr>
<td>26</td>
<td>Payment Card Industry Data Security Standard (PCI-DSS) v3.2.1</td>
</tr>
<tr>
<td>28</td>
<td>Federal Risk and Authorization Management Program (FedRAMP H) - High Security Baseline</td>
</tr>
<tr>
<td>29</td>
<td>Federal Risk and Authorization Management Program (FedRAMP M) - Moderate Security Baseline</td>
</tr>
<tr>
<td>30</td>
<td>NIST 800-53 (Special Publication)</td>
</tr>
</tbody>
</table>
Responses

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

For example, you can set up alerts for:
- Resources failing for particular control
- Evaluation result of highly critical controls
- Evaluation result of controls of specific policy
- Resources failing in the latest connector run

Configure Rule-based Alerts

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

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

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

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

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

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

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

Create a new Action

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

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

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

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

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

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

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

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

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

Create and Manage Rules

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

Create New Rule

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

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

(3) In the Rule Query section, specify a query for the rule. The system uses this query to search for events. Use the Test Query button to test your query. Click Sample Queries link to select from the predefined queries.
(4) In the Trigger Criteria section, choose from three trigger criteria that work in conjunction with the rule query. The trigger criteria are: Single Match, Time-Window Count Match and Time-Window Scheduled Match. For more information on trigger criteria, see Trigger Criteria.

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

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

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

Manage Alerts

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

- Search for alerts using our search tokens.
- Select a period to view the rules triggered during that time frame.
- Click any bar to jump to the alerts triggered in a certain time-frame.
- Use these filters to group the alerts by rule name, action name, email recipients and status.

Sample Queries

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

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

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

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

Scenario 3: Rules with specific action triggered to specific recipient.
**Trigger Criteria**

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

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

- Select Time-Window Scheduled Match when you want to generate alerts for matching events that occurred during a scheduled time. The rule will be triggered only when an event matching your search criteria is found during the time specified in the schedule. Choose a date and time range for creating a schedule and specify how often you want to run the schedule for example, daily, weekly and monthly. For example, send daily alerts with all matches in a scheduled window between 4 pm and 5 pm.
For the Weekly option, select the days of the week on which schedule will run. For example, send weekly alerts with all matches generated between 2.19 pm and 3.19 pm on every Monday and Wednesday.

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

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

### Alerting Permissions

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

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

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

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

- Remediate resource misconfigurations
- Perform actions on cloud resources

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

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

Configuring Remediation

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

Pre-requisites

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

- Cloud Security Assessment (CSA) Subscription
- Administration

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

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

Quick Steps

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

Step 1. Configure Connectors For Remediation

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

The detailed steps for each cloud provider:

Configure Remediation for New Connectors: AWS
Configure Remediation: Microsoft Azure
Configure Remediation: GCP
Step 2. Remediating Cloud Resources
The Monitor tab lists the controls that are available for remediation and the count of failed evaluations that could be remediated.

Step 3. Actions for Cloud Resources (AWS)
The Resources tab provides you with actions that you can execute on instances to quickly fix unknown behavior of an instance or vulnerability on an instance.

Configure Remediation for New Connectors: AWS
You can enable remediation when you create AWS connectors or edit existing connectors. It just takes a couple of minutes.

Enable Remediation for New Connectors
Go to the Configuration > Amazon Web Services tab and click Create Connector.

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

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

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

All the resources detected by this connector will be evaluated. You can then initiate remediation for the failed resources.
Then click Create Connector.
That's it! The connector will establish a connection with AWS to start discovering resources from each region and evaluate them against policies.

**Configuration on AWS Console**
You could either use cloud formation template or manually configure the roles and permissions needed for remediation.

**Configuration Using CloudFormation Template:**
1. Download the CloudFormation template from the Create AWS Connector window.
2. Log on to Amazon Web Services (AWS) and go to CloudFormation.
3. Create stack & upload the template.
When the stack creation is complete, copy the Role ARN value from the output and paste it into the connector details.

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

**Creating Custom Policy**
2. In the left navigation pane, choose Policies.
3. Click Create policy.
4. Click JSON tab.
5. Paste the following policy document into the JSON tab.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RemediationPermission",
            "Effect": "Allow",
            "Action": [
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:StopInstances",
                "ec2:ModifySnapshotAttribute",
                "ec2:ModifyImageAttribute",
                "s3:PutBucketPublicAccessBlock",
                "s3:PutAccountPublicAccessBlock",
                "s3:PutBucketVersioning",
```
Remediating Cloud Resources
Configure Remediation for New Connectors: AWS

```
"rds:ModifyDBInstance",
"rds:ModifyDBClusterSnapshotAttribute",
"rds:ModifyDBCluster",
"redshift:ModifyCluster"
],
"Resource": "*
```

6. Click Review policy.

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

8. Click Create policy.

Adding Policy to IAM Role

2. In the left navigation pane, choose Roles.

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

4. Go to Permissions tab and choose Attach policies.

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

6. Click Attach policy.
Enable Remediation for Existing AWS Connectors

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

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

To fetch the updated resources, you need to select Run from the quick actions menu for the AWS connector.
Configure Remediation: Microsoft Azure

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

Pre-requisites

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

- Enable Remediation for Azure Connector to register an application with your Azure Active Directory.
- Check Azure Subscription permissions to assign the application to a role in your Azure subscription.

Enable Remediation for New Azure Connectors

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

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

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

Click Create Connector.

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

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

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

Creating Custom Role
1. Go to IAM console on the Microsoft Azure Portal.
2. In the search bar, search for Subscriptions and click Subscriptions, under the Services category.
3. In the Subscriptions page, choose your subscription.
4. Click Access control (IAM) navigation pane.
5. Scroll to Create a custom role card and click Add.
6. Provide a name for the Custom role, select Start from scratch option for Baseline permissions and click Next.
7. On the Permissions tab, click Add permissions and add the permissions listed below:
   - Microsoft.Sql/servers/firewallRules/delete
   - Microsoft.Storage/storageAccounts/write
   - Microsoft.Storage/storageAccounts/blobServices/containers/write
   - Microsoft.Network/networkSecurityGroups/write
   - Microsoft.Web/sites/config/write
   - Microsoft.Web/sites/write
8. Click Review + create.
9. Click Create.

Adding Custom Role to the application
1. Go to the Microsoft Azure Portal.
2. In the search bar, search for Subscriptions and click Subscriptions under the Services category.
3. On the Subscriptions page, choose your subscription.
4. Click Access control (IAM) navigation pane.
5. Find Add a role assignment card and click Add.
6. In the Role field, choose the custom role you created (If the custom role does not appear in the drop-down, refresh the page).
7. Select drop-down choose the App provide during the connector creation.
8. Click Save.
Enabling Remediation for Existing Azure Connectors

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

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

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

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

Configure Remediation: GCP

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

Enable Remediation for New GCP Connectors

Go to the Configuration > Google Cloud Platform and then click Create Connector.
Provide a name and description (optional) for your connector. Configure the required settings for the GCP connector. For detailed information on connector creations steps, refer to Steps to Create GCP Connector.

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

Then click Create Connector.

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

Configuration on GCP Console

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

Creating Custom Role
2. From the drop-down list at the top, select the project for which you want to create a role.
3. Click CREATE ROLE and provide the required details.
4. Click Add Permissions.
5. In the Add Permissions window, add the following permissions:
   - compute.firewalls.update
- compute.instances.setMetadata
- storage.buckets.setIamPolicy
- cloudfunctions.functions.setIamPolicy
- bigquery.datasets.update
- cloudsql.instances.update
- cloudkms.cryptoKeys.setIamPolicy

6. Click CREATE.

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

**Adding Custom Role to the IAM Member**

2. In the IAM members list, choose the member used for creating the connector.
3. Click the edit icon on the right side of the Selected IAM member row.
4. In the Edit permissions window, click ADD ANOTHER ROLE and then choose the Custom role created in the above step.
5. Click Save.

The custom role is added to the IAM member.

**Add Compute Engine default service account access to CloudView service account**

2. From the service accounts list select Compute Engine default service accounts, which is of pattern PROJECT_NUMBER-compute@developer.gserviceaccount.com and check the box on the left.
3. On the right pane, click ADD MEMBER.
4. In the New members field, choose the service account provided during connector creation.
5. In Select a role field, choose Service Account User role.
6. Click SAVE.
Enabling Remediation for Existing GCP Connectors

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

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

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

To fetch the updated resources, you need to select Run from the quick actions menu for the GCP connector.
Remediating Cloud Resources
Viewing Remediation Activity

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

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

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

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

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

Actions for AWS resources:
- Stop Instance: indicates stop instance action was initiated for the AWS resource.
- Remove IAM Profile: indicates remove IAM profile action was initiated for the AWS resource.
- Control Remediation: indicates Remediate Now button was used to trigger remediation of the AWS resource for the specified CID.
Remediation Activity: Microsoft Azure

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

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

Remediation Activity: GCP

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

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

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

Remediable Evaluations

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

Total Evaluations: Count of passed and failed control evaluations.

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

Remediable: Count of failed evaluations that can be remediated. Click to view the controls with failed evaluations that are remediable.
The "[Remediation Icon]" icon indicates that these controls are available for remediation. Click on one of the controls to proceed with Remediation.

Let us consider an example of CID 60.

Click Remediate Now.

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

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

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

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

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

**Actions for Cloud Resources (AWS)**

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

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

Action: Stop Instance, Remove IAM Profile

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

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

We support the following actions for AWS Instance resources:

**Stop Instance**

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

You can now execute actions on such instances from Qualys console.
1. Go to Resources > Amazon Web Services > Instance resource type. All the instances in your account are listed. The Actions column displays the possible actions.

Click the Stop Instance action.

Remove IAM Profile

The Remove IAM profile action allows you to disassociate an IAM profile from the instance. Removing IAM profile stops access to other AWS resources that may be available through the associated IAM role. You can execute the action in following scenarios:
Go to Resources > Amazon Web Services > Instance resource type. All the instances in your account are listed. The Actions column displays the possible actions.

![Remove IAM Profile](image)

Click Remove IAM Profile action.

The Remove IAM profile pop-up is displayed.

Specify a comment and select the authorization check box.

Click Execute Action.

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

**Permissions Required**

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

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

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

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

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

Accessing APIs Using Swagger

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

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

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

For example, if your account is on US Platform 2


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</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!
Securing Infrastructure as Code

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

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

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

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

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

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

- Scanning Template Files Using CLI
- Scanning Template Files Using API

Template Support

This Qualys IaC Security version supports following template files:

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

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

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

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

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

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

Scanning Template Files Using CLI

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

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

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

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

[Click here](#) for more information and detailed steps.

Install Qualys IaC Security CLI

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

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

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

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

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

<table>
<thead>
<tr>
<th>Common Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c, --config_file</td>
<td>(Optional) Path of the credentials config file set using &quot;config&quot; command</td>
</tr>
<tr>
<td>-a, --platform_url</td>
<td>Qualys Platform URL</td>
</tr>
<tr>
<td>-u, --user</td>
<td>Qualys username</td>
</tr>
<tr>
<td>-p, --password</td>
<td>Qualys password</td>
</tr>
<tr>
<td>-m, --format</td>
<td>Provides the output in JSON format. [json]</td>
</tr>
<tr>
<td>-x, --proxy</td>
<td>Provide proxy in JSON format For example, {&quot;http&quot;:&quot;http://&lt;user&gt;:&lt;password&gt;@&lt;host&gt;:&lt;port&gt;&quot;,&quot;https&quot;:&quot;https://&lt;host&gt;:&lt;port&gt;&quot;}</td>
</tr>
<tr>
<td>-h, --help</td>
<td>Show this message and exit</td>
</tr>
</tbody>
</table>

scan

| -n, --scan name | (required) Name of the scan |
| -d, --path | (required) Single template file or a directory path |
| -f, --filter | Use regular expression to filter to and include the input files. Example: ".*[.]tf$" Note: This option must used only when directory path is specified in the path option |
| -as, --async | Launches/Triggers the IaC scan asynchronously |
| -q, --quiet | Show only failed checks |
| -g, --tag | Add the tag (in JSON format) to the scan For example, ["env":"linux"],["test_key":"tags"]] |
| -s, --save_output | (optional) Save the output in the current directory |

getresult

| -s, --save_output | (optional) Save the output in the current directory |

listscans

| -i, --scan_id | Scan ID |

config

| -a, --platform_url | (required) Qualys Platform URL |
| -u, --user | (required) Qualys username |
| -p, --password | (required) Qualys password |
| -c, --config_file | (optional) File path to store the configuration |
Below are some of common scenarios for command usage. Usage of parameters vary based on use cases.

**Configure IaC CLI (optional command)**

1. **Trigger Scan** *(add -d)*
2. **Get the scan results**
3. Get the whole scan list
4. Get the scan list of single Scan ID

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

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

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

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

- **config_file**: name or path of the config file

where,

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

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

A user can use the config file using below ways:

- Use Config file from home directory:
  ```bash
  qiac <commands|params>
  ```
- User Config file from custom directory:
  
  qiac <commands|params> -c <location of config file>

where,

the commands could be scan, getresults, listscans.

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

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

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

- With password (add -p)

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

- Without password (remove -p)

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

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

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

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

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

- With save output option (-s)

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

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

  scan_response_<scanId>.json

**2: Get the scan results**

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

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

with config file option
Securing Infrastructure as Code

Scanning Template Files Using API

qiact getresult -c <Path of the config file> -c <Path of the config file>

3: Get the whole scan list
The command returns list of all the IaC scans.

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

with config file option

qiact listscans -c <Path of the config file>

4: Get the scan list of single Scan ID
The command returns single IaC scan as per the scan Id you provide.

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

with config file option

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

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

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

Scanning Template Files Using API
Qualys has introduced new API to launch the IaC scan and fetch the scan results and scan lists.

1) Trigger IaC Scan (POST)
2) Get Scan Results (GET)
3) Get List of Scans (GET)
For complete details, refer to Secure IaC section in CloudView API User Guide.
**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 consolidation 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!
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-the-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
RDS
IAM User

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
CID 199: Ensure not to setup access keys during initial user setup for all IAM users that have a console password except for the master account

**CloudTrail**
CID 19: Ensure CloudTrail is enabled in all regions
CID 20: Ensure CloudTrail log file validation is enabled
CID 21: Ensure the S3 bucket CloudTrail logs to is not publicly accessible
CID 22: Ensure CloudTrail trails are integrated with CloudWatch Logs
CID 24: Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket
CID 25: Ensure CloudTrail logs are encrypted at rest using KMS CMKs
CID 27: Ensure a log metric filter and alarm exist for unauthorized API calls
CID 28: Ensure a log metric filter and alarm exist for Management Console sign-in without MFA
CID 29: Ensure a log metric filter and alarm exist for usage of "root" account
CID 30: Ensure a log metric filter and alarm exist for IAM policy changes
CID 31: Ensure a log metric filter and alarm exist for CloudTrail configuration changes
CID 32: Ensure a log metric filter and alarm exist for AWS Management Console authentication failures
CID 33: Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer created CMKs
CID 34: Ensure a log metric filter and alarm exist for S3 bucket policy changes
CID 35: Ensure a log metric filter and alarm exist for AWS Config configuration changes
CID 36: Ensure a log metric filter and alarm exist for security group changes
CID 37: Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)
CID 38: Ensure a log metric filter and alarm exist for changes to network gateways
CID 39: Ensure a log metric filter and alarm exist for route table changes
CID 40: Ensure a log metric filter and alarm exist for VPC changes
CID 172: Ensure a log metric filter and alarm exists for AWS Organizations changes

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

**Config**
CID 23: Ensure AWS Config is enabled in all regions

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

**S3 Bucket**
CID 59: Ensure “Block new public bucket policies” for a bucket is set to true.
CID 60: Ensure that “Block public and cross-account access” if bucket has public policies for bucket is set to true.
CID 61: Ensure that “Block new public ACLs and uploading public objects” for a bucket is set to true.
CID 62: Ensure that “Remove public access granted through public ACLs” for a bucket is set to true.
CID 177: Ensure that Object-level logging for write events is enabled for S3 bucket
CID 178: Ensure that Object-level logging for read events is enabled for S3 bucket
CID 255: Ensure MFA Delete is enabled on S3 buckets

**RDS**
CID 53: Ensure Encryption is enabled for the database Instance

**IAM User**
CID 199: Ensure not to setup access keys during initial user setup for all IAM users that have a console password except for the master account

**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
Appendix: List of Policies and Controls

AWS Policies

EFS
Redis
Memcached
ES Domain
Route S3
FireHose
KMS
Directory
Workspace
Transit gateway
Rest API Gateway
EMR
ACM
Config
Step Function
CloudWatch Log Group
SNS Topic
SQS Queue
System Manager
Security Group
SageMaker Notebook
ECR Images
ECR Repository
ECS Cluster
MSK_CLUSTER
Network Load Balancer
CloudFront
MQ Broker
Global Accelerator
CodeBuild
Athena Workgroup
DMS Replication
VPC Endpoints
Cloud Formation Stack
Secrets
Auto Scaling Group
Backup Vaults
Glacier Vault
SQS Queue
Network ACL
DynamoDB Table
Route 53 Record
EC2 Instance
EC2
Transfer Server

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

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

CID 66: Ensure 'Remove public access granted through public ACLs' for an account is set to true.

CID 67: Ensure Server Side Encryption (SSE) is enabled for S3 bucket.

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

**EBS Volumes**
CID 115: Ensure that EBS Volumes attached to EC2 instances are encrypted
CID 116: Ensure that Unattached EBS Volumes are encrypted
CID 127: Ensure AWS EBS Volume snapshots are encrypted
CID 145: Ensure CMK is used to encrypt data at rest for EFS
CID 146: Ensure that AWS Elastic Block Store (EBS) volume snapshots are not public
CID 203: Ensure EBS volumes are encrypted with customer managed master keys
CID 204: Ensure AWS EBS Volume snapshots are encrypted with customer managed master keys

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

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

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

AWS Policies

CID 184: Ensure there are no Internet facing Application load balancers
CID 185: Ensure ALB using listener type HTTPS must have SSL Security Policy
CID 186: Ensure that ALB using listener type HTTP must be redirected to HTTPS
CID 187: Ensure that ALB listeners have HTTPS enabled Target Groups
CID 193: Ensure that NLB balancer listener is not using unencrypted protocol
CID 194: Ensure that Classic Elastic load balancer is not internet facing
CID 195: Ensure Classic Elastic Load balancer must have SSL Security Policy
CID 245: Ensure there are no Internet facing Network load balancers
CID 246: Ensure NLB using listener type TLS must have SSL Security Policy
CID 247: Ensure that NLB listeners using TLS have TLS enabled Target Groups configured
CID 248: Ensure that NLB listeners using default insecure ports are not configured for passthrough
CID 249: Ensure AWS NLB logging is enabled
CID 338: Ensure that load balancer is using TLS 1.2
CID 351: Ensure that Elastic Load Balancer(s) uses SSL certificates provided by AWS Certificate Manager
CID 354: Ensure that ALB drops HTTP headers
CID 360: Ensure that ELB is cross-zone-load-balancing enabled
CID 367: Ensure that Load Balancer has deletion protection enabled
CID 369: Ensure that Load Balancer (Network/Gateway) has cross-zone load balancing enabled
CID 395: Ensure that auto Scaling groups that are associated with a load balancer, are using Elastic Load Balancing health checks
CID 403: Ensure public-facing ALB are protected by WAF

EFS
CID 144: Ensure EFS Encryption is enabled for data at rest
CID 252: Ensure to encrypt the data in transit when using NFS between the client and EFS service

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
CID 285: Ensure all data stored in the Elasticsearch is securely encrypted at rest
CID 326: Ensure Elasticsearch Domain enforces HTTPS
CID 359: Ensure that Elasticsearch is configured inside a VPC

Route S3
CID 162: Ensure AWS Route 53 Registered domain has Transfer lock enabled
CID 163: Ensure AWS Route 53 Registered domain has Auto renew Enabled
CID 164: Ensure AWS Route 53 Registered domain is not expired

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

KMS
CID 174: Ensure that Customer managed KMS keys use external key material
Appendix: List of Policies and Controls
AWS Policies

Directory
CID 188: Ensure IncreaseVolumeSize is Disabled for Workspace directories in all regions
CID 205: Ensure "RestartWorkspace" is Enabled in all the regions
CID 208: Ensure WorkDocs is not enabled in Workspace Directories
CID 209: Ensure Access to Internet Access is not enabled in Workspace Directories
CID 210: Ensure Local Administrator setting is not enabled in Workspace Directories
CID 211: Ensure Maintenance Mode is not enabled in Workspace Directories
CID 212: Ensure Device Type Windows Access Control is not enabled in Workspace Directories
CID 213: Ensure Device Type MacOS Access Control is not enabled in Workspace Directories
CID 214: Ensure Device Type Web Access Control is not enabled in Workspace Directories
CID 215: Ensure Device Type iOS Access Control is not enabled in Workspace Directories
CID 216: Ensure Device Type Android Access Control is not enabled in Workspace Directories
CID 217: Ensure Device Type ChromeOS Access Control is not enabled in Workspace Directories
CID 218: Ensure Device Type ZeroClient Access Control is not enabled in Workspace Directories
CID 221: Ensure ChangeComputeType is Disabled in all regions for Workspace Directories
CID 222: Ensure SwitchRunningMode is Disabled in all regions for Workspace Directories
CID 223: Ensure RebuildWorkspace is Disabled in all regions for Workspace Directories
CID 224: Ensure only AD Connector directory type is allowed for AWS Directories

Workspace
CID 179: Ensure MFA is enabled in AWS Directory
CID 181: Ensure proper protocol is configured for Radius server in AWS Directory
CID 197: Ensure to encrypt the Volumes (Root and User) with the customer managed master keys in the same account and the region
CID 225: Ensure to enable the encryption of the Root volumes for Workspaces in all regions
CID 226: Ensure to enable the encryption of the User volumes for Workspaces in all regions

Transit gateway
CID 228: Ensure to disable default route table association for Transit Gateways in all regions
CID 229: Ensure to disable default route table propagation for Transit Gateways in all regions

**Rest API Gateway**
CID 227: Ensure Amazon API Gateway APIs are only accessible through private API endpoints in all regions
CID 242: Ensure logging is not set to OFF for Rest APIs Stage in all regions
CID 244: Ensure accessLogSettings exists with the destinationArn and in the json format for Rest API Stage in all regions
CID 243: Ensure to enable encryption if caching is enabled for Rest API Stage in all regions
CID 318: Ensure API Gateway has X-Ray Tracing enabled
CID 388: Ensure API Gateway stage have logging level defined as appropriate and have metrics enabled

**EMR**
CID 234: Ensure to configure certificate provider type to custom in EMR security configuration
CID 235: Ensure to enable data in transit encryption for EMR security configurations
CID 237: Ensure termination protection is enabled for EMR Clusters
CID 385: Ensure that EMR Cluster security configuration encryption is using SSE-KMS
CID 342: Ensure that EMR clusters with Kerberos have Kerberos Realm set

**ACM**
CID 238: Ensure ACM uses imported certificates only and does not create/issue certificates
CID 239: Ensure expired certificates are removed from AWS ACM
CID 240: Ensure ACM certificates should not have domain with wildcard(*)
CID 241: Ensure that the certificate use appropriate algorithms and Key size

**Config**
CID 230: Ensure to enable config for the all resources for Config Service
CID 231: Ensure to enable config for the global resources like IAM for Config Service
CID 233: Ensure to configure s3 buckets which contains details for the resources that Config records
CID 232: Ensure to configure data retention period for the configuration items for Config Service

**Step Function**
CID 200: Ensure to log state machine’s execution history to CloudWatch Logs
CloudWatch Log Group
CID 373: Ensure to encrypt cloudwatch log groups
CID 313: Ensure CloudWatch Log Group has a retention period set to 7 days or greater

SNS Topic
CID 290: Ensure SNS Topics have encryption at rest enabled
CID 182: Ensure SNS Topics do not Allow 'Everyone' to Publish
CID 183: Ensure SNS Topics do not Allow 'Everyone' to Subscribe
CID 383: Ensure SNS topic policy is not public by only allowing specific services or principals to access it

SQS Queue
CID 291: Ensure SNS Queue have encryption at rest enabled

System Manager
CID 236: Ensure that all AWS Systems Manager (SSM) parameters are encrypted

Security Group
CID 196: Ensure AWS VPC subnets have automatic public IP assignment disabled

SageMaker Notebook
CID 288: Ensure SageMaker Notebook is encrypted at rest using KMS CMK
CID 347: Ensure that direct internet access is disabled for an Amazon SageMaker Notebook Instance
CID 334: Ensure all data stored in the Sagemaker Endpoint is securely encrypted at rest

ECR Images
CID 377: Ensure ECR image scanning on push is enabled

ECR Repository
CID 358: Ensure that ECR repositories are encrypted using KMS
CID 305: Ensure ECR Image Tags are immutable
CID 293: Ensure ECR repository policy is not set to public

ECS Cluster
CID 312: Ensure container insights are enabled on ECS cluster

MSK_CLUSTER
CID 324: Ensure MSK Cluster encryption at rest and in transit is enabled

Network Load Balancer
CID 202: Ensure to update the Security Policy of the Network Load Balance
**CloudFront**
CID 295: Ensure cloudfront distribution ViewerProtocolPolicy is set to HTTPS
CID 314: Ensure that CloudFront Distribution has WAF enabled
CID 327: Ensure Cloudfront distribution has Access Logging enabled

**MQ Broker**
CID 303: Ensure MQ Broker logging is enabled
CID 315: Ensure MQ Broker is not publicly exposed

**Global Accelerator**
CID 319: Ensure Global Accelerator accelerator has flow logs enabled

**CodeBuild**
CID 321: Ensure that CodeBuild Project encryption is not disabled

**Athena Workgroup**
CID 325: Ensure Athena Workgroup should enforce configuration to prevent client disabling encryption
CID 374: Ensure that Athena Workgroup is encrypted

**DMS Replication**
CID 329: Ensure that DMS replication instance is not publicly accessible

**VPC Endpoints**
CID 348: Ensure that VPC Endpoint Service is configured for Manual Acceptance

**Cloud Formation Stack**
CID 349: Ensure that CloudFormation stacks are sending event notifications to an SNS topic

**Secrets**
CID 366: Ensure that Secrets Manager secret is encrypted using KMS

**Auto Scaling Group**
CID 370: Ensure that Autoscaling groups supply tags to launch configurations
CID 286: Ensure all data stored in the Launch configuration EBS is securely encrypted

**Backup Vaults**
CID 380: Ensure Backup Vault is encrypted at rest using KMS CMK

**Glacier Vault**
CID 381: Ensure Glacier Vault access policy is not public by only allowing specific services or principals to access it
Appendix: List of Policies and Controls
AWS Policies

SQS Queue
CID 382: Ensure SQS queue policy is not public by only allowing specific services or principals to access it

Network ACL
CID 386: Ensure that all NACL are attached to subnets

DynamoDB Table
CID 396: Ensure that Auto Scaling is enabled on your DynamoDB tables

Route 53 Record
CID 401: Ensure that Route53 A Record has Attached Resource

EC2 Instance
CID 328: Ensure that EC2 instance have no public IP
CID 350: Ensure that detailed monitoring is enabled for EC2 instances
CID 357: Ensure that EC2 is EBS optimized

EC2
CID 398: Ensure that all EIP addresses allocated to a VPC are attached to EC2 instances

Transfer Server
CID 378: Ensure Transfer Server is not exposed publicly

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

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

RDS

RedShift Clusters

Amazon Aurora

DocumentDB Instance

Document DB Clusters

Neptune DB Clusters

DynamoDB

QLDB Ledger

DAX Cluster

DynamoDB Table

RDS Cluster

RDS

CID 51: Ensure that Public Accessibility is set to No for Database Instances
CID 52: Ensure DB snapshot is not publicly visible
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 97: Ensure that RDS Instances certificates are rotated
CID 257: Ensure status of the 'log_destination' parameter for PostgreSQL instance is set to 'csvlog'
CID 258: Ensure status of the 'log_rotation_age' parameter for PostgreSQL instance is set to 60(minutes)
CID 259: Ensure status of the 'log_connections' parameter for PostgreSQL instance is set to ON(1)
CID 260: Ensure status of the 'log_disconnections' parameter for PostgreSQL instance is set to ON(1)
CID 261: Ensure status of the 'log_hostname' parameter for PostgreSQL instance is set to OFF(0)
CID 262: Ensure status of the 'log_statement' parameter for PostgreSQL instance is set to 'ddl' or stricter
CID 263: Ensure the 'pgaudit.log' parameter for PostgreSQL instance is set to appropriate value
CID 250: Ensure RDS instances should not have be open to a large scope
CID 201: Ensure RDS Instance should not have an Interface open to a public scope
CID 402: Ensure that Postgres RDS has Query Logging enabled

**RedShift Clusters**
CID 108: Ensure Version Upgrade is enabled for AWS Redshift clusters to automatically receive upgrades
CID 109: Ensure that AWS Redshift database clusters are not using default endpoint port
CID 110: Ensure that Redshift clusters are not publicly accessible
CID 111: Ensure that AWS Redshift clusters master username is not set to well-known/default
CID 112: Ensure that AWS Redshift clusters encryption is set for data at rest
CID 113: Ensure audit logging is enabled for AWS Redshift clusters for security and troubleshooting purposes
CID 189: Ensure Automated backup retention is set for Redshift Cluster
CID 190: Ensure Redshift Cluster is configured to require an SSL connection
CID 191: Ensure database audit logging is enabled for Redshift Cluster
CID 192: Ensure Redshift Cluster are encrypted with customer managed keys
CID 371: Ensure Redshift is not deployed outside of a VPC

**Amazon Aurora**
CID 254: Ensure that backup retention is set between 3 to 7 days for Aurora postgresQL clusters
CID 265: Ensure status of the 'log_destination' parameter for Aurora PostgreSQL cluster is set to 'csvlog'
CID 266: Ensure status of the 'log_rotation_age' parameter for Aurora PostgreSQL cluster is set to 60(minutes)
CID 267: Ensure status of the 'log_connections' parameter for Aurora PostgreSQL cluster is set to ON(1)
CID 268: Ensure status of the 'log_disconnections' parameter for Aurora PostgreSQL cluster is set to ON(1)
CID 269: Ensure status of the 'log_hostname' parameter for Aurora PostgreSQL cluster is set to OFF(0)
CID 270: Ensure status of the 'log_statement' parameter for Aurora PostgreSQL cluster is set to 'ddl' or stricter
CID 271: Ensure the 'pgaudit.log' parameter for Aurora PostgreSQL cluster is set to appropriate value

**DocumentDB Instance**
CID 118: Ensure that DocumentDB Instances certificates are rotated
Appendix: List of Policies and Controls

AWS Policies

**Document DB Clusters**
CID 132: Ensure DocumentDB database cluster master username is not set to well-known/default
CID 133: Ensure backup retention is set to minimum of 7 days for DocumentDB clusters
CID 134: Ensure audit logs is enabled for Log export to CloudWatch for DocumentDB clusters
CID 135: Ensure deletion protection is enabled for DocumentDB clusters
CID 136: Ensure DocumentDB Cluster is not listening on default port
CID 206: Ensure Document DB Cluster snapshots are encrypted
CID 207: Ensure Document database Cluster snapshots are not public
CID 330: Ensure DocDB TLS is not disabled

**Neptune DB Clusters**
CID 137: Ensure multi-AZ high availability is enabled for neptune database cluster
CID 138: Ensure neptune database cluster is not listening on default port
CID 139: Ensure IAM db authentication is enabled for neptune database cluster
CID 140: Ensure backup retention is set to minimum of 7 days for neptune database cluster
CID 141: Ensure Audit logs is enabled for log exports to cloudwatch for neptune database cluster
CID 142: Ensure Auto minor version upgrade is enabled for neptune database instances
CID 143: Ensure deletion protection is enabled for neptune database cluster
CID 219: Ensure Neptune DB Cluster snapshots are encrypted
CID 220: Ensure Neptune database Cluster snapshots are not public

**DynamoDB**
CID 169: Ensure DynamoDB tables are encrypted using KMS Customer managed Keys
CID 173: Ensure DynamoDB tables are not configured using DEFAULT encryption

**QLDB Ledger**
CID 180: Ensure QLDB ledger has deletion protection enabled
CID 251: Ensure QLDB ledger has encryption enabled using accessible Customer managed KMS key
CID 384: Ensure QLDB ledger permissions mode is set to STANDARD

**DAX Cluster**
CID 302: Ensure DAX is encrypted at rest (default is unencrypted)
**DynamoDB Table**
CID 292: Ensure Dynamodb point in time recovery (backup) is enabled

**RDS Cluster**
CID 333: Ensure all data stored in Aurora is securely encrypted at rest
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
Disks
Network Security Group

Security Centre
CID 50004: Ensure that ‘Automatic provisioning of monitoring agent’ is set to ‘On’
CID 50022: Ensure that ‘Send me emails about alerts’ is set to ‘On’
CID 50023: Ensure that ‘Send email also to subscription owners’ is set to ‘On’
CID 50078: Ensure that Settings - Threat Detection for Windows Defender ATP (WDATP) is selected
CID 50079: Ensure that Standard pricing tier is enabled for PaaS SQL servers
CID 50080: Ensure that Standard pricing tier is enabled for App Service
CID 50081: Ensure that Standard pricing tier is enabled for Storage Accounts
CID 50082: Ensure any of the ASC Default policy setting is not set to “Disabled”
CID 50139: Ensure that Azure Defender is set to On for Kubernetes
CID 50140: Ensure that Azure Defender is set to On for Container Registries
Appendix: List of Policies and Controls
Azure Policies

CID 50141: Ensure that Azure Defender is set to On for Key Vault

Storage Accounts
CID 50011: Ensure that Secure transfer required for a Storage Account is set to Enabled
CID 50012: Ensure that 'Public access level' is set to Private for blob containers
CID 50052: Ensure default network access rule for Storage Accounts is set to deny
CID 50053: Ensure 'Trusted Microsoft Services' is enabled for Storage Account access
CID 50133: Ensure soft delete is enabled for Azure Storage.
CID 50134: Ensure Storage Service Encryption is enabled for Storage Accounts.

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

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

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

PostgreSQL Server
CID 50040: Ensure Enforce SSL connection" is set to "ENABLED“ for PostgreSQL Database Server"
CID 50041: Ensure server parameter log_checkpoints" is set to "ON" for PostgreSQL Database Server"
CID 50042: Ensure server parameter log_connections" is set to "ON" for PostgreSQL Database Server"
CID 50043: Ensure server parameter log_disconnections" is set to "ON" for PostgreSQL Database Server"
CID 50045: Ensure server parameter log_retention_days" is greater than 3 days for PostgreSQL Database Server"
Appendix: List of Policies and Controls

**Azure Policies**

CID 50074: Ensure server parameter `connection_throttling` is set to "ON" for PostgreSQL Database Server

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

**Logging and Monitoring**

CID 50063: Ensure Activity Log Alert exists for Create Policy Assignment
CID 50064: Ensure Activity Log Alert exists for Create or Update Network Security Group
CID 50065: Ensure Activity Log Alert exists for Delete Network Security Group
CID 50066: Ensure Activity Log Alert exists for Create or Update Network Security Group Rule
CID 50067: Ensure Activity Log Alert exists for Delete Network Security Group Rule
CID 50068: Ensure Activity Log Alert exists for Create or Update Security Solution
CID 50069: Ensure Activity Log Alert exists for Delete Security Solution
CID 50070: Ensure Activity Log Alert exists for Create or Update SQL Server Firewall Rule
CID 50071: Ensure Activity Log Alert exists for Update Security Policy
CID 50056: Ensure Storage account containing container with activity logs is encrypted with BYOK
CID 50076: Ensure storage container storing activity logs is not publicly accessible
CID 50135: Ensure that Activity Log Alert exists for Delete Policy Assignment
CID 50142: Ensure Diagnostic Setting captures appropriate categories

**Networking**

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

**Virtual Machines**

CID 50032: Ensure that all unattached VM disks are encrypted
CID 50033: Ensure that all attached VM disks are encrypted
CID 50034: Ensure disks are encrypted for Windows VMs with ADE version 1.1
CID 50130: Ensure that the endpoint protection for all Virtual Machines is installed

**Web App**

CID 50047: Ensure App Service Authentication is set on Azure App Service
CID 50048: Ensure web app redirects all HTTP traffic to HTTPS in Azure App Service
CID 50049: Ensure web app has 'Client Certificates (Incoming client certificates)' set to 'On'
CID 50050: Ensure that 'Register with Azure Active Directory' is enabled on App Service
CID 50051: Ensure web app is using the latest version of TLS encryption version
CID 50061: Ensure that 'HTTP Version' is latest, if used to run the web app
CID 50136: Ensure FTP deployments are disabled for web apps.

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

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

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

**Disks**
CID 50137: Ensure that 'OS and Data' disks are encrypted with CMK

**Network Security Group**
CID 50138: Ensure that UDP services are restricted from the Internet
Azure Best Practices Policy

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

- Web App
- Redis Cache
- Key Vault
- Disk
- Disk Access
- Event Hub/Namespace/Grid Topic
- Service Bus Namespace
- Virtual Machines/Scale Set
- Container Group
- Cosmos DB
- Storage Account
- Storage Sync Service
- Snapshot
- PostgreSQL Servers
- SQL Servers
- Kubernetes
- Kubernetes Cluster
- Application Gateway
- Container Registries
- Monitor
- Virtual Network Subnet
- Resource Group
- Security Centre/Policy/Policy
- Logging and Monitoring
- API App
- API Management Service
- Cognitive Search/Service
- Data Lake Analytics/Storage
- Synapse Workspace
Appendix: List of Policies and Controls

Azure Policies

Network Interface
Integration Service Environment
Front Door
Logic App
VPC
Data Factory
Data Explorer
Batch Account
IOT Hub
Service Fabric
Automation Account
Device Provisioning Service
Integration Runtime
Batch Pool
Event Grid Domain
Activity Log

Web App
CID 50144: Ensure that CORS does not allow every resource to access the Web apps
CID 50145: Ensure that Diagnostic logs is enabled in Web apps
CID 50148: Ensure that Managed identity is used in Web apps
CID 50150: Ensure that Remote debugging is turned off for Web apps
CID 50152: Ensure that routing of outbound non-RFC 1918 traffic to Azure Virtual Network is enabled in Web apps
CID 50236: Ensure that Web Apps use Azure Files

Redis Cache
CID 50153: Ensure that public network access is disabled in Redis Cache
CID 50154: Ensure that Redis Cache uses private link
CID 50155: Ensure that only secure connections to Redis Cache is enabled
CID 50171: Ensure that Azure Redis Cache servers are using the latest version of the TLS protocol
CID 50195: Ensure that Azure Cache for Redis resides within virtual network
Appendix: List of Policies and Controls

Azure Policies

**Key Vault**
CID 50172: Ensure that public network access is disabled for Azure Key Vaults
CID 50176: Ensure that Azure Key Vaults use Private Links
CID 50250: Ensure that Firewall is enabled on Key Vaults
CID 50251: Ensure that Key Vault keys are backed by HSM
CID 50253: Ensure that Key Vault Secrets have 'Content-Type' set
CID 50218: Ensure that the expiry date is set on all keys

**Disk**
CID 50156: Ensure that public network access is disabled in Managed Disks

**Disk Access**
CID 50157: Ensure that Disk Access resources are configured with private endpoints

**Event Hub/Namespace/Grid Topic**
CID 50158: Ensure that all Authorization Rules except RootManageSharedAccessKey are removed from Event Hub Namespaces
CID 50159: Ensure that Authorization rules are defined in Event Hub instances
CID 50160: Ensure that Event Hub Namespaces use Customer-Managed Key for encryption
CID 50161: Ensure that Event Hub Namespaces use private links
CID 50162: Ensure that Resource Logs are enabled in Event Hub Namespaces
CID 50194: Ensure that Azure Event Grid topics use private links
CID 50301: Ensure that public network access is disabled in Azure Event Grid topics

**Service Bus Namespace**
CID 50163: Ensure that all Authorization Rules except RootManageSharedAccessKey are removed from Service Bus Namespaces
CID 50164: Ensure that Service Bus Namespaces use private links
CID 50165: Ensure that Resource Logs are enabled in Service Bus Namespaces

**Virtual Machines/Scale Set**
CID 50034: Ensure disks are encrypted for Windows VMs with ADE version 1.1
CID 50166: Ensure that Azure Linux-based virtual machines (VMs) are configured to use SSH keys
CID 50037: Ensure to enable virtual machines with end-to-end encryption using encryption at host
CID 50241: Ensure that Virtual Machine Scale Sets have encryption at host enabled
CID 50196: Ensure that Diagnostic logs are enabled in Virtual Machine Scale Sets
CID 50239: Ensure that automatic OS image patching is enabled for Virtual Machine Scale Sets
CID 50223: Ensure that Virtual Machine disallows Extensions

**Container Group**
CID 50167: Ensure that Azure Container Instance container groups use customer-managed key for encryption
CID 50242: Ensure that Azure Container Instance container groups are deployed in a virtual network

**Cosmos DB**
CID 50168: Ensure that Advanced Threat Protection is enabled for all Microsoft Azure Cosmos DB accounts

**Storage Account**
CID 50169: Ensure that Advanced Threat Protection is enabled on Storage Accounts
CID 50173: Ensure that Geo-redundant storage is enabled for Storage Accounts
CID 50175: Ensure that Storage Accounts have infrastructure encryption enabled
CID 50181: Ensure Storage Accounts are using the latest version of TLS encryption
CID 50186: Ensure that critical Azure Blob Storage data is protected from accidental deletion or modification
CID 50187: Ensure that Diagnostic Settings for Storage Accounts are configured with Log Analytics workspace
CID 50188: Ensure that Diagnostic Settings for Storage Blobs are configured with Log Analytics workspace
CID 50189: Ensure that Diagnostic Settings for Storage Files are configured with Log Analytics workspace
CID 50190: Ensure that Diagnostic Settings for Storage Queues are configured with Log Analytics workspace
CID 50191: Ensure that Diagnostic Settings for Storage Tables are configured with Log Analytics workspace
CID 50198: Ensure that Storage Accounts use private link connections
CID 50225: Ensure that Storage accounts disallow Blob public access

**Storage Sync Service**
CID 50170: Ensure that Azure File Sync uses private link
CID 50174: Ensure that Public network access is disabled for Azure File Sync

**Snapshot**
CID 50038: Ensure disk snapshots are encrypted.
**PostgreSQL Servers**
CID 50044: Ensure server parameter log_duration" is set to "ON" for PostgreSQL Database Server"

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

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

**Kubernetes Cluster**
CID 50192: Ensure that Azure Kubernetes Service Private Clusters is enabled
CID 50193: Ensure that Azure Policy Add-on for Kubernetes service (AKS) is installed and enabled on your clusters
CID 50208: Ensure that Kubernetes Services Management API server is configured with restricted access
CID 50254: Ensure that Azure Kubernetes Service uses disk encryption set
CID 50210: Ensure that Kube Dashboard is disabled
CID 50279: Ensure that Azure Kubernetes Service (AKS) cluster has Network Policy configured

**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
CID 50199: Ensure that Container Registries are configured to disable public network access
CID 50200: Ensure that Container Registries are configured with private endpoints
CID 50201: Ensure that Container Registries are encrypted with a customer-managed key
CID 50278: Ensure that Container Registry disallows unrestricted network access

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

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

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

**Security Centre/Policy**
CID 50003: Ensure ASC Default policy setting Monitor Application Whitelisting is not Disabled
CID 50005: Ensure ASC Default policy setting Monitor System Updates is not Disabled
CID 50006: Ensure that Vulnerabilities in security configuration on your machines should be remediated is set to On
CID 50007: Ensure ASC Default policy setting Monitor Endpoint Protection is not Disabled
CID 50008: Ensure ASC Default policy setting Monitor Disk Encryption is not Disabled
CID 50009: Ensure ASC Default policy setting Monitor Network Security Groups is not Disabled
CID 50010: Ensure ASC Default policy setting Monitor Web Application Firewall is not Disabled
CID 50014: Ensure ASC Default policy setting Monitor SQL Auditing is not Disabled
CID 50015: Ensure that standard pricing tier is selected
CID 50016: Ensure ASC Default policy setting Enable Next Generation Firewall(NGFW) Monitoring is not Disabled
CID 50017: Ensure that Vulnerabilities should be remediated by a Vulnerability Assessment solution
CID 50018: Ensure ASC Default policy setting Monitor Storage Blob Encryption is not Disabled
CID 50019: Ensure ASC Default policy setting Monitor JIT Network Access is not Disabled
CID 50021: Ensure that security contact 'Phone number' is set
CID 50025: Ensure ASC Default policy setting Monitor SQL Encryption is not Disabled
CID 50071: Ensure that Activity Log Alert exists for Update Security Policy
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'
CID 50182: Ensure that monitoring of DDoS protection at the Azure virtual network level is enabled
CID 50183: Ensure that monitoring of deprecated accounts within your Azure subscription(s) is enabled
CID 50184: Ensure that IP forwarding enablement on your Azure virtual machines (VMs) is being monitored
CID 50185: Ensure that the external accounts with write permissions are monitored using Azure Security Center
CID 50197: Ensure that Azure Defender for DNS is enabled
CID 50226: Ensure that Azure Defender for Resource Manager is enabled
CID 50231: Ensure that Azure Defender is set to On for SQL servers on machines

Logging and Monitoring
CID 50024: Ensure that LogProfile for a subscription is configured properly

API App
CID 50202: Ensure that FTPS is enforced in API Apps
CID 50203: Ensure that Managed Identity is used in API Apps
CID 50204: Ensure that API Apps are only accessible over HTTPS
CID 50205: Ensure that API Apps have Incoming Client Certificates is set to On
CID 50206: Ensure that HTTP Logging is enabled in API Apps
CID 50058: Ensure that Detailed Error Logging is enabled in API Apps

API Management Service
CID 50248: Ensure that API Management services use virtual networks
CID 50303: Ensure that API Management Services use latest protocol for Client Side Security
CID 50304: Ensure that API Management Services use latest protocol for Backend Side Transport Security
CID 50305: Ensure that API Management services use a SKU that supports virtual networks
CID 50306: Ensure that Cipher Triple DES (3DES) is enabled for API Management resource
CID 50307: Ensure that HTTP/2 client side protocol is enabled for API Management resource
CID 50308: Ensure that System assigned Managed Identity is enabled for API Management Service

**Cognitive Search/Service**
CID 50276: Ensure that Diagnostic logs are enabled in Search Services
CID 50260: Ensure that public network access is disabled for Cognitive Services accounts
CID 50114: Ensure that network access is restricted in Cognitive Services accounts
CID 50296: Ensure that Cognitive Services enable data encryption with customer-managed keys
CID 50297: Ensure that Cognitive Services have local authentication methods disabled
CID 50298: Ensure that Managed identity is used in Cognitive Services
CID 50299: Ensure that Cognitive Services use private links

**Data Lake Analytics/Storage**
CID 50274: Ensure that Diagnostic logs are enabled in Data Lake Analytics accounts
CID 50275: Ensure that Diagnostic logs are enabled in Azure Data Lake Storage accounts
CID 50246: Ensure that encryption is enabled for Data Lake Store accounts

**Synapse Workspace**
CID 50224: Ensure that managed virtual network is enabled in Azure Synapse workspace

**Network Interface**
CID 50255: Ensure that IP forwarding is disabled for Network Interfaces
CID 50256: Ensure that Network Interfaces don’t use public IPs

**Integration Service Environment**
CID 50101: Ensure that Logic Apps Integration Service Environments are encrypted with customer-managed keys

**Front Door**
CID 50257: Ensure that Web Application Firewall (WAF) is enabled in Azure Front Door Services

**Logic App**
CID 50277: Ensure that Diagnostic logs are enabled in Logic Apps
CID 50309: Ensure that Logic Apps are deployed into Integration Service Environment

**VPC**
CID 198: Ensure workspace directory must have a vpc endpoint so that the API traffic associated with the management of workspaces stays within the vpc
Appendix: List of Policies and Controls

Azure Policies

Data Factory
CID 50267: Ensure that Azure Data Factory is encrypted with a customer-managed key
CID 50245: Ensure that public network access is disabled in Azure Data Factory
CID 50244: Ensure that Azure Data Factory uses Git repository for source control
CID 50284: Ensure that Azure Data Factory uses private link

Data Explorer
CID 50265: Ensure that encryption at rest uses customer-managed key in Azure Data Explorer
CID 50229: Ensure that Azure Data Explorer uses double encryption
CID 50228: Ensure that Azure Data Explorer uses disk encryption
CID 50286: Ensure that Virtual network injection is enabled for Azure Data Explorer

Batch Account
CID 50230: Ensure that Azure Batch account uses key vault to encrypt data
CID 50291: Ensure that Azure Batch accounts have local authentication methods disabled
CID 50292: Ensure that Metric alert rules are configured on Batch accounts
CID 50293: Ensure that Batch accounts have private endpoint connections enabled
CID 50294: Ensure that public network access is disabled for Batch accounts
CID 50295: Ensure that Resource logs are enabled in Batch accounts

IOT Hub
CID 50249: Ensure that public network access is disabled for Azure IoT Hub
CID 50282: Ensure that Resource logs are enabled in IoT Hub

Service Fabric
CID 50261: Ensure that Service Fabric cluster has the ClusterProtectionLevel property set to EncryptAndSign
CID 50262: Ensure that Service Fabric cluster uses Azure Active Directory for authentication

Automation Account
CID 50227: Ensure that Automation account variables are encrypted
CID 50287: Ensure that public network access is disabled for Automation accounts
CID 50288: Ensure that Automation account uses customer-managed keys to encrypt data at rest
CID 50289: Ensure that Automation account has private endpoint connections enabled
Device Provisioning Service
CID 50280: Ensure that public network access is disabled for IoT Hub Device Provisioning Service instances
CID 50281: Ensure that IoT Hub Device Provisioning Service instances use private links

Integration Runtime
CID 50283: Ensure that Azure Data Factory Integration Runtimes have a limit for the number of cores
CID 50285: Ensure that SQL Server Integration Services Integration Runtimes on Azure Data Factory are joined to a virtual network

Batch Pool
CID 50290: Ensure that Azure Batch pools have disk encryption enabled

Event Grid Domain
CID 50300: Ensure that Azure Event Grid domains are configured to disable public network access
CID 50302: Ensure that Azure Event Grid domains use private links

Activity Log
CID 50217: Ensure that audit profile captures all the activities

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
CID 50143: Ensure that CORS does not allow every resource to access the Function Apps
CID 50146: Ensure that Function apps enforce FTPS-only access to FTP traffic
CID 50147: Ensure that Managed identity is used in Function apps
CID 50149: Ensure that Remote debugging is turned off for Function apps
CID 50151: Ensure that routing of outbound non-RFC 1918 traffic to Azure Virtual Network is enabled in Function apps
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

CID 50178: Ensure that public network access is disabled on Azure SQL databases

CID 50180: Ensure that public network access is disabled for PostgreSQL flexible servers

CID 50100: Ensure that Azure SQL Database have private endpoint connections enabled

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
CID 50179: Ensure that public network access is disabled for MySQL flexible servers
CID 50268: Ensure that encryption with customer-managed key is enabled in MySQL Servers
CID 50263: Ensure that MySQL server has infrastructure encryption enabled

**MariDB Server**
CID 50108: Ensure that Advanced Threat Protection settings is configured properly for Azure Database for MariaDB Server
CID 50109: Ensure 'Enforce SSL connection' is set to 'ENABLED' for Azure Database for MariaDB server
CID 50110: Ensure that TLS is enforced and the minimum version be set to 1.2 for Azure Database for MariaDB server
CID 50111: Ensure no MariaDB Server allow ingress from Internet (ANY IP)
CID 50112: Ensure that 'geo_redundant_backup_enabled' is set to Enabled for Azure Database for MariaDB server
CID 50113: Ensure that Public Network Access is Disabled for Azure Database for MariaDB server

**PostgreSQL Server**
CID 50115: Ensure that Advanced Threat Protection settings is configured properly for Azure Database for PostgreSQL Server
CID 50116: Ensure that TLS is enforced and the minimum version be set to 1.2 for Azure Database for PostgreSQL server
CID 50118: Ensure that 'geo_redundant_backup_enabled' is set to Enabled for Azure Database for PostgreSQL server
CID 50119: Ensure that Public Network Access is Disabled for Azure Database for PostgreSQL server
CID 50120: Ensure that Azure Database for PostgreSQL server diagnostic setting is configured properly
CID 50132: Ensure that Azure Active Directory authentication is configured for PostgreSQL server
CID 50177: Ensure that encryption with customer-managed key is enabled in PostgreSQL servers
CID 50240: Ensure that PostgreSQL server has infrastructure encryption enabled

**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
CID 50099: Ensure that Azure Cosmos DB accounts have firewall rules
CID 50243: Ensure that Cosmos DB accounts have customer-managed keys to encrypt data at rest
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
VM Instances
Dataset
Table
Cloud DNS

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

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

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

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

**Network**
CID 52019: Ensure the default network does not exist in a project
CID 52034: Ensure legacy networks do not exist for a project
CID 52116: Ensure that Cloud DNS logging is enabled for all VPC networks

**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
Appendix: List of Policies and Controls

GCP Policies

Cloud SQL- Mysql
CID 52032: Ensure that Cloud SQL - Mysql database Instance requires all incoming connections to use SSL
CID 52033: Ensure that Cloud SQL - Mysql database Instances are not open to the world
CID 52075: Ensure 'skip_show_database' database flag for Cloud SQL - Mysql instance is set to 'on'
CID 52076: Ensure 'local_infile' database flag for Cloud SQL - Mysql instance is set to 'off'
CID 52084: Ensure Cloud SQL - MySQL Instance do not have public IP addresses
CID 52087: Ensure Cloud SQL- MySQL instance is configured with automated backups

Cloud SQL- SQL Server
CID 52035: Ensure that MySQL Database Instance does not allows root login from any Host
CID 52067: Ensure that Cloud SQL - SQL Server database instance requires all incoming connections to use SSL
CID 52068: Ensure that Cloud SQL - SQL Server database Instances are not open to the world
CID 52077: Ensure 'external scripts enabled' database flag for Cloud SQL - SQL Server instance is set to 'off'
CID 52078: Ensure 'cross db ownership chaining' database flag for Cloud SQL - SQL Server instance is set to 'off'
CID 52081: Ensure 'remote access' database flag for Cloud SQL - SQL Server instance is set to 'off'
CID 52082: Ensure '3625 (trace flag)' database flag for Cloud SQL - SQL Server instance is set to 'off'
CID 52083: Ensure 'contained database authentication' database flag for Cloud SQL SQL Server instance is set to 'off'
CID 52085: Ensure Cloud SQL - SQL server Instance do not have public IP addresses
CID 52088: Ensure Cloud SQL- SQL server is configured with automated backups
CID 52080: Ensure 'user options' database flag for Cloud SQL - SQL Server instance is not configured
CID 52148: Ensure 'user connections' database flag for Cloud SQL SQL Server instance is set as appropriate

Cloud SQL- PostgreSQL
CID 52059: Ensure 'log_connections' database flag for Cloud SQL - PostgreSQL instance is set to 'on'
CID 52060: Ensure 'log_disconnections' database flag for Cloud SQL - PostgreSQL instance is set to 'on'
CID 52061: Ensure 'log_duration' database flag for Cloud SQL PostgreSQL instance is set to 'on'
CID 52062: Ensure 'log_errorVerbosity' 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 'logHostname' database flag for Cloud SQL - PostgreSQL instance is set to 'off'
CID 52065: Ensure that Cloud SQL - PostgreSQL database instance requires all incoming connections to use SSL
CID 52066: Ensure that Cloud SQL - PostgreSQL database Instances are not open to the world
CID 52069: Ensure 'logLockWaits' database flag for Cloud SQL - PostgreSQL instance is set to 'on'
CID 52070: Ensure 'logTempFiles' database flag for Cloud SQL - PostgreSQL instance is set to '0' (on)
CID 52071: Ensure 'logMinErrorStatement' database flag for Cloud SQL - PostgreSQL instance is set to 'Error' or stricter
CID 52072: Ensure 'logMinMessages' database flag for Cloud SQL - PostgreSQL instance is set to 'Error' or stricter
CID 52073: Ensure 'logMinDurationStatement' database flag for Cloud SQL - PostgreSQL instance is set to '-1'
  (disabled)
CID 52074: Ensure 'logCheckpoints' database flag for Cloud SQL - PostgreSQL instance is set to 'on'
CID 52086: Ensure Cloud SQL - PostgreSQL Instance do not have public IP addresses
CID 52089: Ensure Cloud SQL - PostgreSQL instance is configured with automated backups
CID 52112: Ensure logParserStats database flag for Cloud SQL PostgreSQL instance is set to off
CID 52113: Ensure logPlannerStats database flag for Cloud SQL PostgreSQL instance is set to off
CID 52114: Ensure logExecutorStats database flag for Cloud SQL PostgreSQL instance is set to off
CID 52115: Ensure 'logStatementStats' database flag for Cloud SQL PostgreSQL instance is set to off

**VM Instances**
CID 5220: Ensure that IP forwarding is not enabled on Instances
CID 52025: Ensure that instances are not configured to use the default service account with full access to all Cloud APIs
CID 52026: Ensure Block Project-wide SSH keys "enabled for VM instances"
CID 52027: Ensure oslogin is enabled for a Project
CID 52028: Ensure Enable connecting to serial ports "is not enabled for VM Instance"
CID 52029: Ensure VM disks for critical VMs are encrypted with Customer-Supplied Encryption Keys (CSEK)
CID 52091: Ensure Compute instances are launched with Shielded VM enabled
CID 52093: Ensure that instances are not configured to use default service account
CID 52094: Ensure that Compute instances do not have public IP addresses
CID 52111: Ensure that Compute instances have Confidential Computing enabled

**Dataset**
CID 52095: Ensure that BigQuery dataset is encrypted with Customer-managed key
CID 52098: Ensure that BigQuery datasets are not anonymously or publicly accessible

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

**Cloud DNS**
CID 52100: Ensure that DNSSEC is enabled for Cloud DNS
CID 52109: Ensure that GCP Cloud DNS zones is using RSASHA1 algorithm for DNSSEC key-signing
CID 52110: Ensure that GCP Cloud DNS zones is using RSASHA1 algorithm for DNSSEC zone-signing
GCP Best Practices Policy

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

**Storage**

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
CID 52140: Ensure that Bucket should not log to itself

**VM Instance**

CID 52092: Ensure oslogin is enabled for VM instance
CID 52157: Ensure that the Auto-Delete feature is disabled for the disks attached to your VM instances
CID 52158: Ensure that your production Google Cloud virtual machine instances are not preemptible
CID 52159: Ensure that deletion protection is enabled for your Google Cloud virtual machine (VM) instances
CID 52162: Ensure that automatic restart is enabled for VM instances

**Subnetwork**

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

**Pub/Sub**

CID 52118: Ensure that Pub/Sub topics are encrypted using Customer-Managed Keys (CMKs).
Appendix: List of Policies and Controls

GCP Policies

**Compute**
CID 52120: Ensure that "On Host Maintenance" configuration setting is set to "Migrate" for all VM instances.

**Project IAM**
CID 52135: Ensure Default Service account is not used at a project level
CID 52138: Ensure no roles that enable to impersonate and manage all service accounts are used at a project level

**Cloud Storage**
CID 52156: Ensure that Google Cloud Storage objects are using a lifecycle configuration for cost management

**VM Disk**
CID 52160: Ensure that your virtual machine (VM) instance disks are encrypted using Customer-Managed Keys (CMKs)

**Dataproc Cluster**
CID 52161: Ensure that your Dataproc clusters are encrypted using Customer-Managed Keys (CMKs)
**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
CID 52117: Ensure that data at rest available on your GKE clusters is encrypted with Customer-Managed Keys.
CID 52129: Ensure that your GKE clusters nodes are shielded to protect against impersonation attacks.
CID 52130: Ensure that Integrity Monitoring is enabled for your Google Kubernetes Engine (GKE) cluster nodes.
CID 52142: Ensure that the Secure Boot feature is enabled for your Google Kubernetes Engine (GKE) cluster nodes.
CID 52131: Ensure that Google Kubernetes Engine (GKE) clusters have sandbox enabled
CID 52079: Ensure that Google Kubernetes Engine (GKE) clusters have workload identity enabled
CID 52147: Ensure Image Vulnerability Scanning using GCR Container Analysis or a third-party provider
CID 52143: Ensure the GKE Metadata Server is Enabled
CID 52127: Ensure Kubernetes Clusters are configured with Labels
CID 52144: Ensure the GKE Release Channel is set

**GCP Cloud SQL Best Practices Policy**

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

- Cloud SQL - PostgreSQL
- Cloud SQL - Mysql
- Cloud SQL - SQL Server
- Cloud SQL - SQL
Cloud SQL - PostgreSQL
CID 52107: Ensure that Cloud SQL - PostgreSQL database instance Point-in-time recovery is enabled
CID 52152: Ensure that production PostgreSQL database instances are configured to automatically fail over to another zone within the selected cloud region.
CID 52128: Ensure that PostgreSQL database instances have the appropriate configuration set for the "max_connections" flag.
CID 52154: Ensure that PostgreSQL instances are encrypted with Customer-Managed Keys (CMKs).
CID 52149: Ensure that Cloud SQL PostgreSQL instance server certificates are rotated (renewed) before their expiration.

Cloud SQL - Mysql
CID 52106: Ensure that Cloud SQL Mysql database instance Binary logs configuration is enabled
CID 52121: Ensure that production MySQL database instances are configured to automatically fail over to another zone within the selected cloud region.
CID 52122: Ensure that MySQL database servers are using the latest major version of MySQL database.
CID 52146: Ensure that MySQL instances are encrypted with Customer-Managed Keys (CMKs).
CID 52150: Ensure that Cloud SQL MySQL instance server certificates are rotated (renewed) before their expiration.

Cloud SQL - SQL Server
CID 52097: Ensure 'default trace enabled' database flag for Cloud SQL - SQL Server instance is set to 'on'
CID 52153: Ensure that production SQL Server database instances are configured to automatically fail over to another zone within the selected cloud region.
CID 52155: Ensure that SQL Server instances are encrypted with Customer-Managed Keys (CMKs).
CID 52151: Ensure that Cloud SQL - SQL Server instance certificates are rotated (renewed) before their expiration.

Cloud SQL - SQL
CID 52119: Ensure that MySQL database instances have the "slow_query_log" flag set to On (enabled)