Qualys CloudView v1.x

Version 1.9.3.0
May 15, 2020

Here's what's new in Qualys CloudView 1.9.3!

Amazon Web Services

Microsoft Azure

Google Cloud Platform

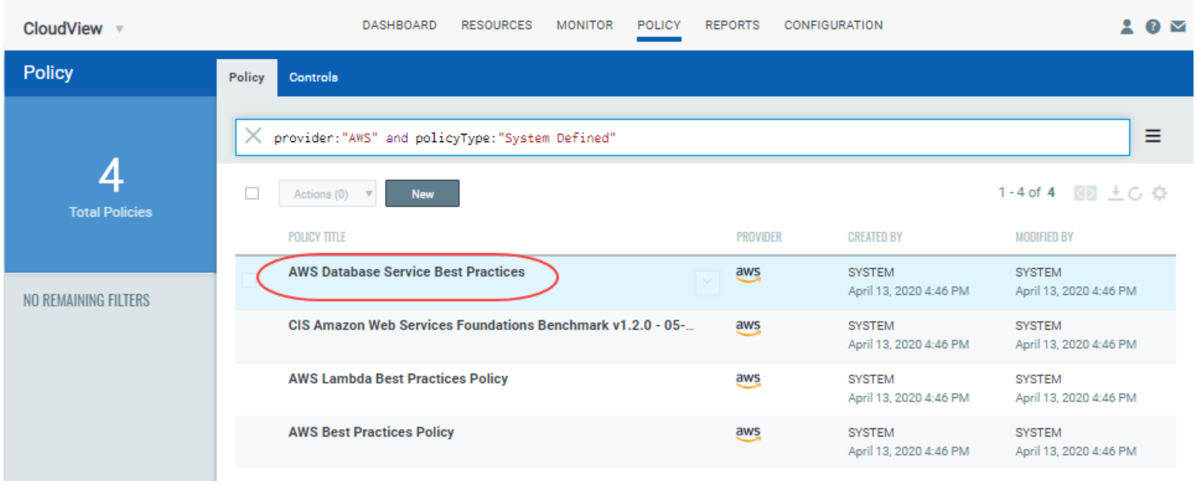
Common Feature

Qualys CloudView 1.9.3 brings you many more Improvements and updates! Learn more

Amazon Web Services

New AWS Database Service Best Practices Policy

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



```
provider:"AWS" and policyType:"System Defined"
```

4 Total Policies

1 - 4 of 4

POLICY TITLE	PROVIDER	CREATED BY	MODIFIED BY
AWS Database Service Best Practices	aws	SYSTEM April 13, 2020 4:46 PM	SYSTEM April 13, 2020 4:46 PM
CIS Amazon Web Services Foundations Benchmark v1.2.0 - 05-...	aws	SYSTEM April 13, 2020 4:46 PM	SYSTEM April 13, 2020 4:46 PM
AWS Lambda Best Practices Policy	aws	SYSTEM April 13, 2020 4:46 PM	SYSTEM April 13, 2020 4:46 PM
AWS Best Practices Policy	aws	SYSTEM April 13, 2020 4:46 PM	SYSTEM April 13, 2020 4:46 PM

New Controls

The pre-defined AWS Database Service Best Practices Policy is loaded with 54 controls. The 12 new system-defined controls are listed below. All the other controls are migrated from other.

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

New Controls Added to AWS Best Practices Policy

We have added the following new controls to AWS Best Practices Policy.

CID	Resource	Service	Control Title
126	EC2 Images	EC2	Ensure AMIs owned by an AWS account are encrypted
127	EBS Snapshots	EC2	Ensure AWS EBS Volume snapshots are encrypted
128	Load Balancer	EC2	Ensure access log is enabled for Elastic load balancer
129	Load Balancer	EC2	Ensure access log is enabled for Classic Elastic load balancer
130	Load Balancer	EC2	Ensure Classic Elastic load balancer is not using unencrypted protocol
131	Load Balancer	EC2	Ensure Elastic load balancer listener is not using unencrypted protocol
144	EFS	EFS	Ensure EFS Encryption is enabled for data at rest

Migrated Controls of AWS

We have now moved the following AWS related controls from AWS Best Practices Policy to our new AWS Database Service Best Practices policy. The following table lists all such controls that have been migrated.

CID	Control Name	Service	Resource	Old Policy	New Policy
51	Ensure that Public Accessibility is set to No for Database Instances	RDS	RDS	AWS Best Practices Policy	AWS Database Service Best Practices
52	Ensure DB snapshot is not publicly visible	RDS	RDS		
53	Ensure Encryption is enabled for the database Instance	RDS	RDS		
54	Ensure database Instance snapshot is encrypted	RDS	RDS		
55	Ensure auto minor version upgrade is enabled for a Database Instance	RDS	RDS		
56	Ensure database Instance is not listening on to a standard/default port	RDS	RDS		
69	Ensure automated backups are enabled for RDS database instances	RDS	RDS		
70	Ensure Deletion Protection is enabled for RDS DB Cluster	RDS	RDS		
71	Ensure Deletion Protection is enabled for RDS Database instances	RDS	RDS		
72	Ensure IAM Database Authentication is Enabled for the DB Cluster	RDS	RDS		

CID	Control Name	Service	Resource	Old Policy	New Policy
73	Ensure IAM Database Authentication is Enabled for the DB Instances	RDS	RDS	AWS Best Practices Policy	AWS Database Service Best Practices
74	Ensure AWS RDS Log Exports is enabled for DB Cluster	RDS	RDS		
75	Ensure AWS RDS Log Exports is enabled for DB Instances	RDS	RDS		
76	Ensure RDS Database Master username is not set to well-known/default	RDS	RDS		
77	Ensure VPC security group attached to RDS Database Instance does not allows Inbound traffic from ANY source IP	RDS	RDS		
78	Ensure RDS DB instances are not present in public subnets	RDS	RDS		
79	Ensure RDS DB Cluster are not present in public subnets	RDS	RDS		
80	Ensure Event Subscriptions for Instance Level Events is Enabled for DB Instances	RDS	RDS		
81	Ensure RDS Microsoft SQL instance enforces encrypted connections only	RDS	RDS		
82	Ensure RDS PostgreSQL instance enforces encrypted connections only	RDS	RDS		
83	Ensure RDS PostgreSQL Cluster enforces encrypted connections only	RDS	RDS		
84	Ensure Encryption is enabled for the RDS DB Cluster	RDS	RDS		
85	Ensure RDS DB Cluster snapshots are encrypted	RDS	RDS		
86	Ensure CMK is used to protect RDS DB Cluster encryption key	RDS	RDS		
87	Ensure CMK is used to protect RDS Db Instance encryption key	RDS	RDS		
88	Ensure DB instance replication is set to the another Zone for High Availability	RDS	RDS		
89	Ensure DB Cluster replication is set to the another Zone for High Availability	RDS	RDS		
90	Ensure RDS database Cluster snapshots are not public	RDS	RDS		

CID	Control Name	Service	Resource	Old Policy	New Policy
91	Ensure Enhance monitoring is enabled for RDS Database Instance	RDS	RDS	AWS Best Practices Policy	AWS Database Service Best Practices
92	Ensure AWS RDS DB Cluster with copy tags to snapshots option is enabled	RDS	RDS		
93	Ensure AWS RDS instances with copy tags to snapshots option is enabled	RDS	RDS		
94	Ensure Event Subscriptions for cluster Level Events is Enabled for DB Clusters	RDS	RDS		
95	Ensure MYSQL DB Instance backup Binary logs configuration is not enabled	RDS	RDS		
96	Ensure backup configuration is enabled for MSSQL DB Instances	RDS	RDS		
108	Ensure Version Upgrade is enabled for AWS Redshift clusters to automatically receive upgrades	Redshift	Redshift clusters		
109	Ensure AWS Redshift clusters are not using default endpoint port	Redshift	Redshift clusters		
110	Ensure AWS Redshift clusters are not publicly accessible	Redshift	Redshift clusters		
111	Ensure AWS Redshift clusters master username is not set to well-known/default	Redshift	Redshift clusters		
112	Ensure that AWS Redshift clusters encryption is set for data at rest	Redshift	Redshift clusters		
113	Ensure audit logging is enabled for AWS Redshift clusters for security and troubleshooting purposes	Redshift	Redshift clusters		
117	Ensure that RDS Instances certificates are rotated	RDS	RDS		
118	Ensure that DocumentDB Instances certificates are rotated	DocumentDB	Document DB Instance		

AWS Control Updates

We have updated the static content and logic for the following controls to match with the changes on AWS portal. The static content for the control includes title, summary, specification, evaluation, rationale, remediation, references.

CID	Resource	Service	Title	Sections Updated
119	Secrets Manager	Secrets	Ensure no AWS default KMS Key is used to protect Secrets	Updated control to evaluate on specific service such as "secrets manager". Updated static content, service type and resource type.
121	KMS	KMS	Ensure only Root user of the AWS Account should be allowed full access on the CMK	Control Logic & Rationale
122	KMS	KMS	Permissions to delete key is not granted to any Principal other than the Root user of AWS Account	
123	KMS	KMS	Ensure CMK administrators are not the user of the key	

Microsoft Azure

New Controls Added to Azure Best Practices Policy

We have added the following five new controls to Azure Best Practices Policy.

CID	Resource	Service	Control Title
50090	Kubernetes Cluster	Kubernetes Services	Ensure that Azure AKS cluster monitoring is enabled
50091	Kubernetes Cluster	Kubernetes Services	Ensure that Azure AKS cluster HTTP application routing is disabled
50092	Kubernetes Cluster	Kubernetes Services	Ensure that Azure AKS cluster Azure CNI networking is enabled
50093	Application Gateway	Application Gateway	Ensure that Azure Application Gateway have Web application firewall (WAF) enabled
50094	Application Gateway	Application Gateway	Ensure that Azure Application Gateway allows TLSv1.2 or above

Microsoft Azure Control Updates

We have updated the static content and control logic for some controls to match with the changes on Microsoft Azure portal. The static content for the control includes title, summary, specification, evaluation, rationale, remediation, references.

CID	Service	Resource	Title	Sections Updated
50034	Virtual Machines	Virtual Machines	Ensure disks are encrypted for Windows VMs with ADE version 1.1	Control Logic Updated
50055	Network Security Group	Network Security Group	Ensure Network Security Group Flow Log retention is greater than 90 days	Control Logic Updated
50010	Security Center	Security Policy	Ensure that NSGs rules for web applications on IaaS should be hardened is set to ON	Control Logic Updated
50014	Security Center	Security Policy	Ensure that Monitor unaudited SQL databases in Azure Security Center is set to On	Control Logic Updated
50016	Security Center	Security Policy	Ensure that Access through Internet facing endpoint should be restricted is set to On	Control Logic Updated
50017	Security Center	Security Policy	Ensure that Vulnerabilities in security configuration on your machines should be remediated is to On	Control Logic Updated
50018	Security Center	Security Policy	Ensure that Audit missing blob encryption for storage account is set to On	Control Logic Updated
50019	Security Center	Security Policy	Ensure that Just-In-Time network access control should be applied on virtual machines is set to On	Control Logic Updated

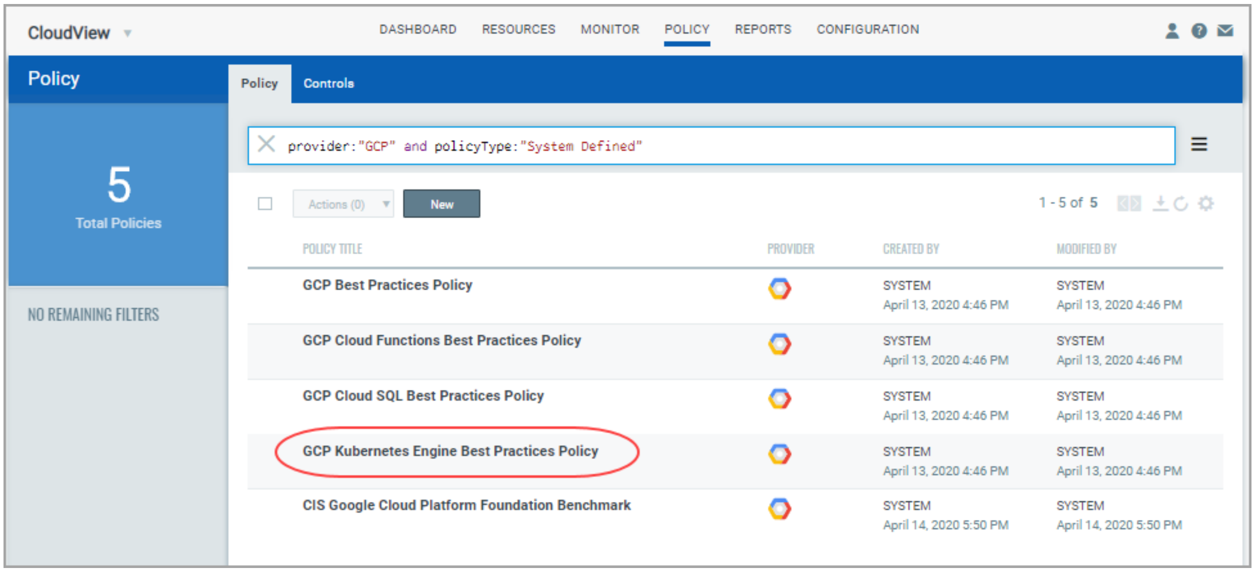
CID	Service	Resource	Title	Sections Updated
50025	Security Center	Security Policy	Ensure that Monitor unencrypted SQL databases in Azure Security Center is set to On	Control Logic Updated
50082	Security Center	Security Policy	Ensure any of the ASC Default policy setting is not set to "Disabled"	Control Logic Updated

Google Cloud Platform

We have introduced two new policies for Google Cloud Platform (GCP):

New GCP Kubernetes Engine Best Practices Policy

We have introduced New 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.



```
provider:"GCP" and policyType:"System Defined"
```

POLICY TITLE	PROVIDER	CREATED BY	MODIFIED BY
GCP Best Practices Policy		SYSTEM April 13, 2020 4:46 PM	SYSTEM April 13, 2020 4:46 PM
GCP Cloud Functions Best Practices Policy		SYSTEM April 13, 2020 4:46 PM	SYSTEM April 13, 2020 4:46 PM
GCP Cloud SQL Best Practices Policy		SYSTEM April 13, 2020 4:46 PM	SYSTEM April 13, 2020 4:46 PM
GCP Kubernetes Engine Best Practices Policy		SYSTEM April 13, 2020 4:46 PM	SYSTEM April 13, 2020 4:46 PM
CIS Google Cloud Platform Foundation Benchmark		SYSTEM April 14, 2020 5:50 PM	SYSTEM April 14, 2020 5:50 PM

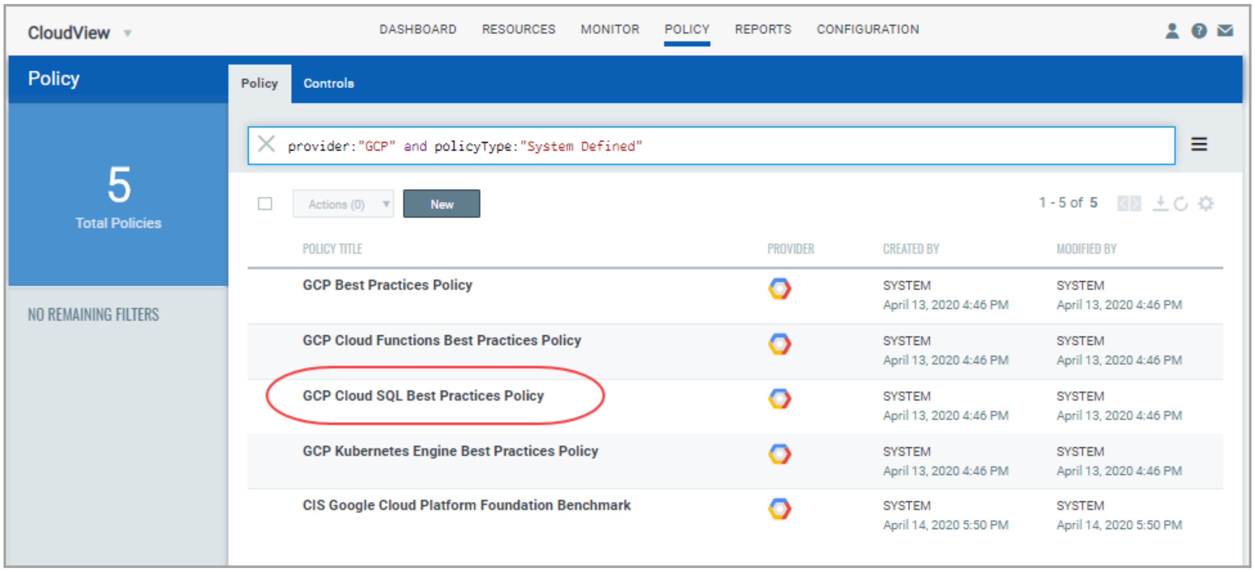
New Controls

The pre-defined GCP Kubernetes Engine Best Practices is loaded with the 17 system-defined controls. Of the 17 controls, the following three controls are new controls. All the other 14 controls are migrated from other policies.

CID	Resource	Service	Control Title
52037	Kubernetes Cluster	Kubernetes Engine	Ensure that GCP Kubernetes cluster intra-node visibility is enabled
52042	Kubernetes Cluster	Kubernetes Engine	Ensure that GCP Kubernetes Engine Clusters have HTTP load balancing enabled
52044	Kubernetes Cluster	Kubernetes Engine	Ensure that GCP Kubernetes Engine Clusters have Alpha cluster feature disabled

New GCP Cloud SQL Best Practices Policy

We have introduced 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.



provider:"GCP" and policyType:"System Defined"

POLICY TITLE	PROVIDER	CREATED BY	MODIFIED BY
GCP Best Practices Policy		SYSTEM April 13, 2020 4:46 PM	SYSTEM April 13, 2020 4:46 PM
GCP Cloud Functions Best Practices Policy		SYSTEM April 13, 2020 4:46 PM	SYSTEM April 13, 2020 4:46 PM
GCP Cloud SQL Best Practices Policy		SYSTEM April 13, 2020 4:46 PM	SYSTEM April 13, 2020 4:46 PM
GCP Kubernetes Engine Best Practices Policy		SYSTEM April 13, 2020 4:46 PM	SYSTEM April 13, 2020 4:46 PM
CIS Google Cloud Platform Foundation Benchmark		SYSTEM April 14, 2020 5:50 PM	SYSTEM April 14, 2020 5:50 PM

New Controls

The pre-defined GCP Cloud SQL Best Practices Policy is loaded 12 system-defined controls. The following 11 controls are new controls. One control is migrated from other policy.

CID	Resource	Service	Control Title
52061	Cloud SQL PostgreSQL	SQL	Ensure 'log_duration' database flag for Cloud SQL PostgreSQL instance is set to 'on'
52062	Cloud SQL PostgreSQL	SQL	Ensure 'log_error_verbosity' database flag for Cloud SQL - PostgreSQL instance is set to 'DEFAULT' or stricter
52063	Cloud SQL PostgreSQL	SQL	Ensure log_statement" database flag for Cloud SQL - PostgreSQL instance is set to "ddl" or stricter"
52064	Cloud SQL PostgreSQL	SQL	Ensure 'log_hostname' database flag for Cloud SQL - PostgreSQL instance is set to 'off'
52071	Cloud SQL PostgreSQL	SQL	Ensure 'log_min_error_statement' database flag for Cloud SQL - PostgreSQL instance is set to 'Error' or stricter
52075	Cloud SQL Mysql	SQL	Ensure 'skip_show_database' database flag for Cloud SQL - Mysql instance is set to 'on'
52077	Cloud SQL SQL Server	SQL	Ensure 'external scripts enabled' database flag for Cloud SQL - SQL Server instance is set to 'off'
52080	Cloud SQL SQL Server	SQL	Ensure 'user options' database flag for Cloud SQL - SQL Server instance is not configured
52081	Cloud SQL SQL Server	SQL	Ensure 'remote access' database flag for Cloud SQL - SQL Server instance is set to 'off'
52082	Cloud SQL SQL Server	SQL	Ensure '3625 (trace flag)' database flag for Cloud SQL - SQL Server instance is set to 'off'
52097	Cloud SQL SQL Server	SQL	Ensure 'default trace enabled' database flag for Cloud SQL - SQL Server instance is set to 'on'

New Controls Added to GCP Best Practices Policy

We have added the following 3 new controls to GCP Best Practices Policy.

CID	Resource	Service	Control Title
52092	VM Instance	Compute Engine	Ensure oslogin is enabled for VM instance
52095	Dataset	BigQuery	Ensure that BigQuery Dateset is encrypted with Customer-managed key
52096	Table	BigQuery	Ensure that BigQuery Table is encrypted with Customer-managed key

New Controls Added to CIS Google Cloud Platform Foundation Benchmark Policy

We have added the following 40 new controls to CIS Google Cloud Platform Foundation Benchmark policy.

CID	Resource	Service	Control Title
52007	IAM	Project	Ensure that IAM users are not assigned Service Account Token Creator role at project level
52009	Logs Router	Logging	Ensure that sinks are configured for all Log entries
52011	Logs-based metrics	Stackdriver Logging	Ensure log metric filter and alerts exists for Project Ownership assignments/changes
52012	Logs-based metrics	Stackdriver Logging	Ensure log metric filter and alerts exists for Audit Configuration Changes
52013	Logs-based metrics	Stackdriver Logging	Ensure log metric filter and alerts exists for Custom Role changes
52014	Logs-based metrics	Stackdriver Logging	Ensure log metric filter and alerts exists for VPC Network Firewall rule changes
52015	Logs-based metrics	Stackdriver Logging	Ensure log metric filter and alerts exists for VPC network route changes
52016	Logs-based metrics	Stackdriver Logging	Ensure log metric filter and alerts exists for VPC network changes
52017	Logs-based metrics	Stackdriver Logging	Ensure log metric filter and alerts exists for Cloud Storage IAM permission changes
52018	Logs-based metrics	Stackdriver Logging	Ensure log metric filter and alerts exists for SQL instance configuration changes
52020	VM Instance	Compute Engine	Ensure that IP forwarding is not enabled on Instances
52034	Network	Project	Ensure legacy networks do not exist for a project
52036	Storage	Storage	Ensure that Cloud Storage buckets have uniform bucket-level access enabled
52059	Cloud SQL PostgreSQL	SQL	Ensure 'log_connections' database flag for Cloud SQL - PostgreSQL instance is set to 'on'
52060	Cloud SQL PostgreSQL	SQL	Ensure 'log_disconnections' database flag for Cloud SQL - PostgreSQL instance is set to 'on'
52065	Cloud SQL PostgreSQL	SQL	Ensure that Cloud SQL - PostgreSQL database instance requires all incoming connections to use SSL
52066	Cloud SQL PostgreSQL	SQL	Ensure that Cloud SQL - PostgreSQL database Instances are not open to the world

CID	Resource	Service	Control Title
52067	Cloud SQL SQL Server	SQL	Ensure that Cloud SQL - SQL Server database instance requires all incoming connections to use SSL
52068	Cloud SQL SQL Server	SQL	Ensure that Cloud SQL - SQL Server database Instances are not open to the world
52069	Cloud SQL PostgreSQL	SQL	Ensure 'log_lock_waits' database flag for Cloud SQL - PostgreSQL instance is set to 'on'
52070	Cloud SQL PostgreSQL	SQL	Ensure 'log_temp_files' database flag for Cloud SQL - PostgreSQL instance is set to '0' (on)
52072	Cloud SQL PostgreSQL	SQL	Ensure 'log_min_messages' database flag for Cloud SQL - PostgreSQL instance is set to 'Error' or stricter
52073	Cloud SQL PostgreSQL	SQL	Ensure 'log_min_duration_statement' database flag for Cloud SQL - PostgreSQL instance is set to '-1' (disabled)
52074	Cloud SQL PostgreSQL	SQL	Ensure 'log_checkpoints' database flag for Cloud SQL - PostgreSQL instance is set to 'on'
52076	Cloud SQL Mysql	SQL	Ensure 'local_infile' database flag for Cloud SQL - Mysql instance is set to 'off'
52078	Cloud SQL SQL Server	SQL	Ensure 'cross db ownership chaining' database flag for Cloud SQL - SQL Server instance is set to 'off'
52083	Cloud SQL SQL Server	SQL	Ensure 'contained database authentication' database flag for Cloud SQL SQL Server instance is set to 'off'
52084	Cloud SQL Mysql	SQL	Ensure Cloud SQL - MySql Instance do not have public IP addresses
52085	Cloud SQL SQL Server	SQL	Ensure Cloud SQL - SQL server Instance do not have public IP addresses
52086	Cloud SQL PostgreSQL	SQL	Ensure Cloud SQL - PostgreSQL Instance do not have public IP addresses
52087	Cloud SQL Mysql	SQL	Ensure Cloud SQL- MySql instance is configured with automated backups
52088	Cloud SQL SQL Server	SQL	Ensure Cloud SQL- SQL server is configured with automated backups
52089	Cloud SQL PostgreSQL	SQL	Ensure Cloud SQL SQL PostgreSQL is configured with automated backups
52090	Cryptographic Keys	IAM	Ensure that Cloud KMS cryptokeys are not anonymously or publicly accessible
52091	VM Instance	Compute Engine	Ensure Compute instances are launched with Shielded VM enabled
52093	VM Instance	Compute Engine	Ensure that instances are not configured to use default service account
52094	VM Instance	Compute Engine	Ensure that Compute instances do not have public IP addresses
52098	Dataset	BigQuery	Ensure that BigQuery datasets are not anonymously or publicly accessible
52099	Storage	Storage	Ensure that retention policies on log buckets are configured using Bucket Lock
52100	Cloud DNS	Network Services	Ensure that DNSSEC is enabled for Cloud DNS

Migrated Controls of GCP

We have moved few controls from an existing policy to a different policy of the same cloud provider. The following table lists all such controls that have been migrated from one policy to another.

CID	Control Title	Service	Resource	Old Policy	New Policy
52010	Ensure that object versioning is enabled on buckets	Storage	Storage	CIS Google Cloud Platform Foundation Benchmark	GCP Best Practices Policy
52023	Ensure Private Google Access is enabled for all subnetwork in VPC Network	VPC Network	Subnetwork		
52031	Ensure that logging is enabled for Cloud storage buckets	Storage	Storage		
52052	Ensure that Application-Layer secret encryption is enabled for Kubernetes cluster	Kubernetes Engine	Kubernetes Cluster	GCP Best Practices Policy	GCP Kubernetes Engine Best Practices Policy
52053	Ensure that Master authorized network is enabled for Kubernetes cluster	Kubernetes Engine	Kubernetes Cluster		
52035	Ensure that MySQL Database Instance does not allows root login from any Host	SQL	SQL	CIS Google Cloud Platform Foundation Benchmark	GCP Cloud SQL Best Practices Policy

CID	Control Name	Service	Resource	Old Policy	New Policy
52038	Ensure Legacy Authorization is set to Disabled on Kubernetes Engine Clusters	Kubernetes Engine	Kubernetes Cluster	CIS Google Cloud Platform Foundation Benchmark	GCP Kubernetes Engine Best Practices Policy
52939	Ensure Kubernetes web UI / Dashboard is disabled	Kubernetes Engine	Kubernetes Cluster		
52040	Ensure Automatic node repair is enabled for Kubernetes Clusters	Kubernetes Engine	Kubernetes Cluster		
52041	Ensure Automatic node upgrades is enabled on Kubernetes Engine Clusters nodes	Kubernetes Engine	Kubernetes Cluster		
52043	Ensure Network policy is enabled on Kubernetes Engine Clusters	Kubernetes Engine	Kubernetes Cluster		
52045	Ensure Kubernetes Cluster is created with Alias IP ranges enabled	Kubernetes Engine	Kubernetes Cluster		
52046	Ensure PodSecurityPolicy controller is enabled on the Kubernetes Engine Clusters	Kubernetes Engine	Kubernetes Cluster		
52047	Ensure Kubernetes Cluster is created with Private cluster enabled	Kubernetes Engine	Kubernetes Cluster		
52048	Ensure Private Google Access is set on Kubernetes Engine Cluster Subnets	Kubernetes Engine	Kubernetes Cluster		
52049	Ensure default Service account is not used for Project access in Kubernetes Clusters	Kubernetes Engine	Kubernetes Cluster		
52050	Ensure Kubernetes Clusters created with limited service account Access scopes for Project access	Kubernetes Engine	Kubernetes Cluster		
52051	Ensure Stackdriver Kubernetes Engine Monitoring is set to Enabled on Kubernetes Engine Clusters	Kubernetes Engine	Kubernetes Cluster		

GCP Control Updates

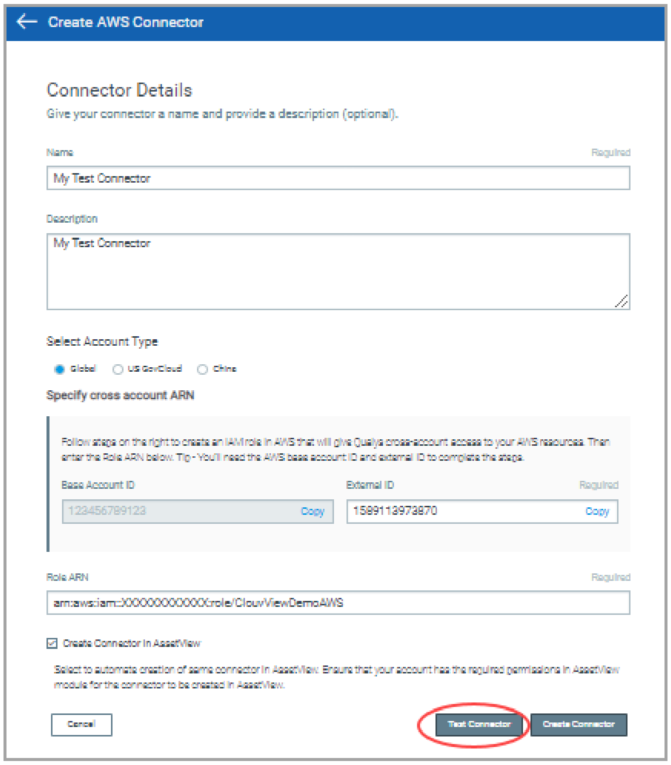
We have updated the static content and control logic for some controls to match with the changes on GCP portal. The static content for the control includes title, summary, specification, evaluation, rationale, remediation, references.

CID	Service	Resource	Title	Sections Updated
52045	Kubernetes Engine	Cluster	Ensure Kubernetes Cluster is created with Alias IP ranges enabled	Remediation
52047	Kubernetes Engine	Cluster	Ensure Kubernetes Cluster is created with Private cluster enabled	Remediation
52049	Kubernetes Engine	Cluster	Ensure default Service account is not used for Project access in Kubernetes Clusters	Remediation
52050	Kubernetes Engine	Cluster	Ensure Kubernetes Clusters created with limited service account Access scopes for Project access	Remediation
52025	Compute Engine	VM Instance	Ensure that instances are not configured to use the default service account with full access to all Cloud APIs	Control Logic
52050	Kubernetes Engine	Kubernetes Node Pool	Ensure Kubernetes Clusters created with limited service account Access scopes for Project access	Control Logic

Common Feature

Test Connectivity with Cloud Provider

We now provide a feature to check the connectivity of the connector with your cloud provider. We support this feature for all the three cloud providers: AWS, Microsoft Azure and GCP. You can check the connectivity for new as well as existing connectors. The test connector result provides a preview of the connector connectivity with your cloud provider.



Connector Details

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

Name: My Test Connector (Required)

Description: My Test Connector

Select Account Type

● Global ○ US GovCloud ○ China

Specify cross account ARN

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

Base Account ID: 123456789123 Copy

External ID: 1589113973870 Copy (Required)

Role ARN: arn:aws:iam::XXXXXXXXXXXX:role/ClouvViewDemoAWS (Required)

☑ Create Connector In AssetView

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

New Connectors

Let us see how to test connector for new connectors (example: AWS).

Go to the **Configuration > Amazon Web Services** and then click **Create Connector**. Once you provide all the necessary details required to create the connector, click **Test Connector**.

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.

Existing Connectors

Let us see how to test connectors for existing connectors (example: Microsoft Azure).

Go to **Configuration > Microsoft Azure** and select the connector. From the quick actions menu, select **View** and go to **Connector Information** tab and click **Edit**. Once you update the required details, you can click **Test Connector**.

If the test connection is successful, click **Save** and proceed. If the connection is fails, the failure message provides details that need to be updated to fix the connection failure.

Issues addressed in this release

We have fixed the following issues:

- The control signatures are updated to accommodate changes if organizational level CloudTrail is present in accounts other than master account. The master account in an organization has no impact, only the account that exists under an organization or organizational unit (OU) with multi region CloudTrail configured at organizational level will experience control signature improvement. The impact is listed below:
  - CID 19: Control signature now considers organizational trail for evaluation. (Now, AWS provides API to describe CloudTrail properties.)
  - CID 27-40: Control signature will not consider organizational trail as the connector cannot access resources across account.
  - CID: 21,24: Control Evaluation fails for organization trail error stating "S3 Bucket doesn't belong to the same account" as the connector cannot access resources across account.
- AWS doesn't allow to delete default KMS key. Due to this restriction, the remediation steps cannot be executed. The previous control signature avoids use of KMS default key. Now, the updated control signature avoids use of KMS default key based upon service consisting of sensitive data i.e Secrets Manager.
  CID 119: We have updated the static content. The resource id is now updated to secrets manager id.
- Control signature is updated to add support Service and Federated Principals in KMS resource policy. The control 121, 122 and 123 now can parse KMS resource policy with Service and Federated Principals defined. We have also updated the static text to define the supported policy elements and requirements.
- We have modified the control logic of CID 50034 to handle more cases in customer environments.
- We have updated control logic for CID 50003, 50005, 50004, 50005, 50006, 50007, 50008, 50009 to handle additional checks for ASC default policy.
- We have now fixed the sync discrepancy for EC2 Instances between AssetView and CloudView. Now, the EC2 instances between AssetView and CloudView will be in sync. The EC2 instances that are not detected by the connector run will be marked as Terminated.
- We have now fixed an issue so that the GCP Resources page displays the correct count of failed resources instead of 0 failed resources.
- We have updated the Step 6 in Generate Authentication Key section in Online Help to match the steps listed on UI.
- We have fixed an issue where duplicate connectors would be created on same account (AWS) or subscription (Microsoft Azure) or project (GCP) if a create connector API was fired concurrently.
- We have fixed an issue where the Microsoft Azure connector retained in Processing state in CloudView and AssetView:
  - if none of the resource groups had any Virtual Machines
  - If there were no resources in the subscription.

  Now, despite these conditions the Microsoft Azure connector is not stuck in Processing state, but displays success state after some time.
- We have fixed an issue where the Microsoft Azure connector retained in Processing state in CloudView if there are large number of resource groups and substantial number of Virtual Machines in each of these groups.
- We have now fixed an issue so that only CloudView Azure connector resources are displayed in CloudView module. Earlier, AssetView Azure connector resources were also displayed in CloudView module-

- We have now fixed and issue of loading connector list on Configuration tab. Earlier, the connector list was not loading intermittently.
- We have now fixed an issue so that you can now successfully create connectors for China region.