Qualys CloudView v1.x

Version 1.12.0

October 21, 2020

Here's what's new in Qualys CloudView 1.12.0!

Amazon Web Services

New Controls for AWS Best Practices Policy
New Controls for AWS Database Service Best Practices
New Controls for CIS Amazon Web Services Foundations Benchmark

Microsoft Azure

New controls for Azure Database Best Practices Policy
New controls for Azure Best Practices Policy:

Common Feature

Downloadable Assessment Reports
Generate Assessment Report Using APIs

Qualys CloudView 1.12 brings you many more Improvements and updates! Learn more

Amazon Web Services

New Controls for AWS Best Practices Policy

We have added the following 8 new controls to AWS Best Practices Policy.

CID	Resource	Service	Control Title
162	Route 53 Domain	Route 53	Ensure AWS Route 53 Registered domain has Transfer lock enabled
163	Route 53 Domain	Route 53	Ensure AWS Route 53 Registered domain has Auto renew Enabled
164	Route 53 Domain	Route 53	Ensure AWS Route 53 Registered domain is not expired
165	FireHose	Kinesis	Ensure AWS Kinesis Data Firehose delivery stream with Direct PUT and other sources as source has Server-side encryption configured
166	FireHose	Kinesis	Ensure AWS Kinesis Data Firehose delivery stream with Kinesis Data stream as source has Server-side encryption configured
167	FireHose	Kinesis	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
168	FireHose	Kinesis	Ensure AWS Kinesis Data Firehose delivery stream with Kinesis Data stream as source has Server-side encryption configured with KMS Customer Managed Keys
174	KMS	KMS	Ensure that Customer managed KMS keys use external key material

New Controls for AWS Database Service Best Practices

We have added the following 2 new controls to AWS Database Service Best Practices.

CID	Resource	Service	Control Title
169	DynamoDB Table	DynamoDB	Ensure DynamoDB tables are encrypted using KMS Customer managed Keys
173	DynamoDB Table	DynamoDB	Ensure DynamoDB tables are not configured using DEFAULT encryption

New Controls for CIS Amazon Web Services Foundations Benchmark

We have added the following 4 new controls to CIS Amazon Web Services Foundations Benchmark.

CID	Resource	Service	Control Title
161	Network ACLs	VPC	Ensure no Network ACLs allow ingress from 0.0.0.0/0 to port 22
170	Network ACLs	VPC	Ensure no Network ACLs allow ingress from 0.0.0.0/0 to port 3389
171	IAM	IAM	Ensure there is only one active access key available for any single IAM user

172	CloudTrail	CloudTrail	Ensure a log metric filter and alarm exists for AWS Organizations changes

Controls Migrated for AWS

We have migrated the following controls from CIS Amazon Web Services Foundations Benchmark to AWS Best Practices Policy.

Old Policy: CIS Amazon Web Services Foundations Benchmark

New Policy: AWS Best Practices Policy

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

We have migrated the following controls from AWS Best Practices Policy to CIS Amazon Web Services Foundations Benchmark.

Old Policy: AWS Best Practices Policy

New Policy: CIS Amazon Web Services Foundations Benchmark

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

Microsoft Azure

New controls for Azure Database Best Practices Policy

We have added the following 2 new controls to Azure Database Best Practices Policy.

CID	Resource	Service	Control Title
50131	MySQL	MySQL	Ensure that Azure Active Directory authentication is co nfigured for MySql server
50132	PostgreSQL	PostgreSQL	Ensure that Azure Active Directory authentication is co nfigured for PostgreSql server

New controls for Azure Best Practices Policy

We have added the following 6 new controls to Azure Best Practices Policy.

CID	Resource	Service	Control Title
50125	Activity Log Alert	Monitor	Ensure Activity Log Alert exists for Create/Update Storage Account
50126	Activity Log Alert	Monitor	Ensure Activity Log Alert exists for Delete Storage Account
50127	Activity Log Alert	Monitor	Ensure Activity Log Alert exists for Create or Update Virtual Machine
50128	Activity Log Alert	Monitor	Ensure Activity Log Alert exists for Deallocate Virtual Machine
50129	Activity Log Alert	Monitor	Ensure Activity Log Alert exists for Delete Virtual Machine
50130	Virtual Machine	Virtual Machine	Ensure that the endpoint protection for all Virtual Machines is installed

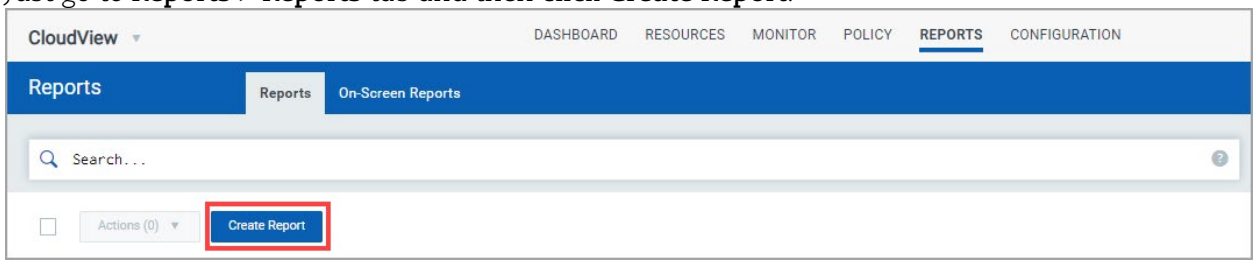
Common Feature

Downloadable Assessment Reports

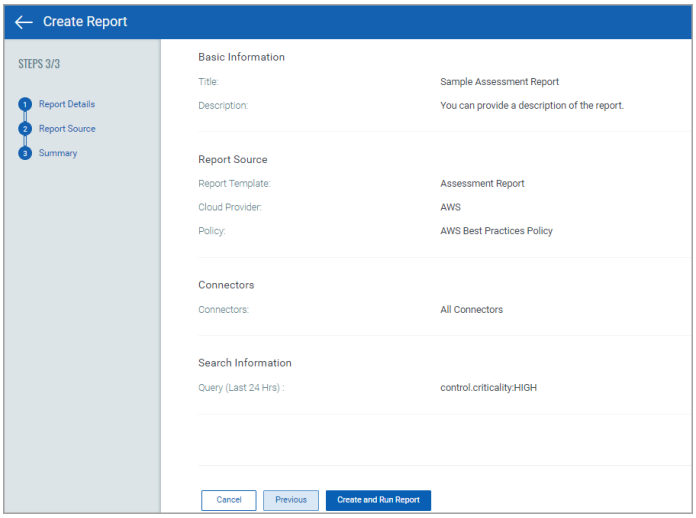
We now provide you with assessment reports to view the compliance evaluation of your resources for multiple policies in your cloud environment. You can use our Qualys Query Language (QQL) query to generate on-demand assessment report. When the report is successfully created, you can also download it in CSV format using our quick actions menu.

Create Assessment Report

Just go to **Reports** > **Reports** tab and then click **Create Report**.



Provide a title and description (optional) to the report template and configure other report settings such as cloud provider, compliance policy, connector you want to evaluate for compliance, and so on. You can also use Qualys Query Language (QQL) to define the report criteria. Review the configured report settings in the **Summary** pane and then click **Create and Run 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.

Can I download the assessment report?

Yes. To download assessment report, select the report from the **Reports** page and click **Download** from the quick actions menu. The report is downloaded in CSV format.

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

Generate Assessment Report Using APIs

We have now introduced new Assessment Report APIs to create, download, delete and view assessment reports.. For detailed information, refer to CloudView 1.12 API Release Notes.

Issues addressed in this release

- The GCP connector state now remains consistent on List Connectors page, Connector Summary, and Last Job Summary page. Earlier, the connector state displayed inconsistencies in certain scenarios.
- We have now fixed an issue where the EC2 Instance state was erroneously marked as terminated if the associated CloudView connector did not run in few hours.