



Qualys CloudView v1.x

Version 1.15.0

April 7, 2021 (updated on June 1, 2021)

Here's what's new in Qualys CloudView 1.15.0!

Amazon Web Services

[Inventory Support for EKS Resources](#)
[New Tokens Introduced](#)

Microsoft Azure

[New controls for CIS Microsoft Azure Foundations Benchmark](#)
[Control Migrated for Microsoft Azure](#)

Google Cloud Platform

[Project ID for GCP Connectors](#)

Common Feature

[API Features and Enhancements](#)

**Qualys CloudView 1.15 brings you many more
Improvements and updates! [Learn more](#)**

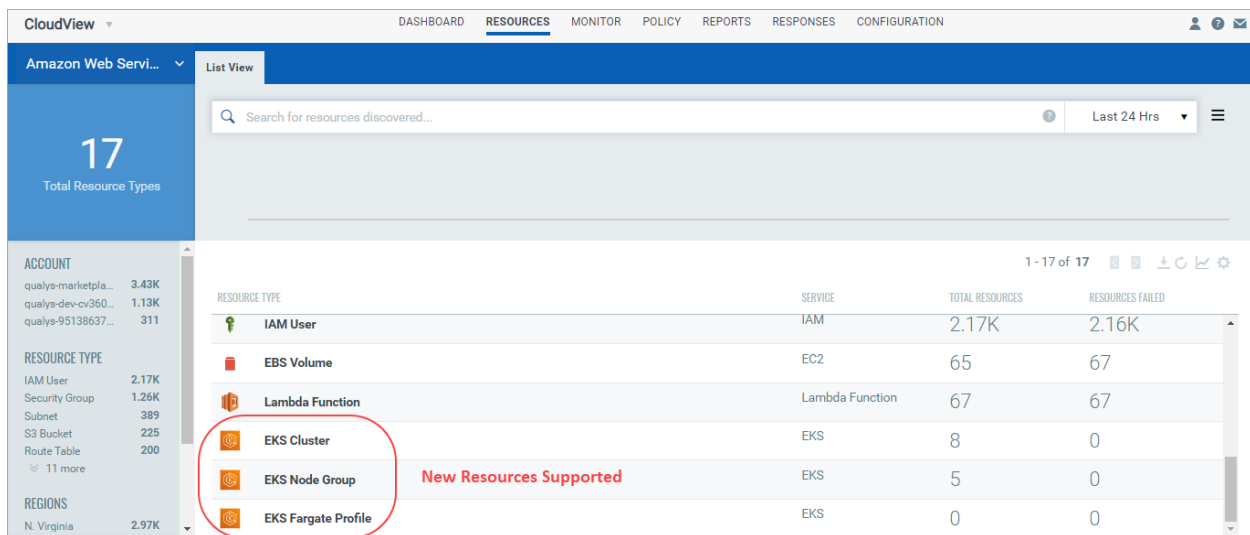
Amazon Web Services

Inventory Support for EKS Resources

You can now monitor EKS resources and view its details. You can filter further using the tokens and view the resource information.

Go to Resources tab. You can view the newly supported resource in the List View for Amazon Web Services.

- EKS Cluster
- EKS Node Group
- EKS Fargate Profile



The screenshot shows the CloudView interface with the 'RESOURCES' tab selected. On the left, a sidebar shows '17 Total Resource Types'. The main table lists resources with columns for 'RESOURCE TYPE', 'SERVICE', 'TOTAL RESOURCES', and 'RESOURCES FAILED'. The following table represents the data shown in the screenshot:

RESOURCE TYPE	SERVICE	TOTAL RESOURCES	RESOURCES FAILED
IAM User	IAM	2.17K	2.16K
EBS Volume	EC2	65	67
Lambda Function	Lambda Function	67	67
EKS Cluster	EKS	8	0
EKS Node Group	EKS	5	0
EKS Fargate Profile	EKS	0	0

New Permissions Needed to Fetch Fargate Profile Resources

The cross-account role associated with the AWS connector needs additional permissions to fetch information about Fargate profile. To fetch information about the Fargate profile resources in your cloud environment, you need to assign these additional permissions to the IAM role associated with the AWS connector

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

The detailed steps for policy creation and associating with the IAM role are listed in the CloudView online help.

New Tokens Introduced

We have added the following search tokens for the new resources that we have introduced:

EKS Cluster

- ekscluster.name
- ekscluster.status
- ekscluster.version
- ekscluster.platformVersion
- ekscluster.endpointPublicAccess
- ekscluster.endpointPrivateAccess
- ekscluster.endpoint
- ekscluster.role.name
- ekscluster.eksnodegroup.name
- ekscluster.fargateprofile.name
- ekscluster.subnetId
- ekscluster.vpcId

EKS Node Group

- eksnodegroup.name
- eksnodegroup.version
- eksnodegroup.status
- eksnodegroup.desiredSize
- eksnodegroup.amiType
- eksnodegroup.instanceType
- eksnodegroup.diskSize
- eksnodegroup.minSize
- eksnodegroup.maxSize
- eksnodegroup.labels.key
- eksnodegroup.labels.value
- eksnodegroup.role.name
- eksnodegroup.subnetId
- eksnodegroup.autoScalingGroup.Name
- eksnodegroup.ekscluster.name
- eksnodegroup.securityGroup

EKS Fargate Profile

- eksfargateprofile.name
- eksfargateprofile.status
- eksfargateprofile.selectors.namespace.name
- eksfargateprofile.selectors.namespace.labels.key
- eksfargateprofile.selectors.namespace.labels.value
- eksfargateprofile.role.name
- eksfargateprofile.ekscluster.name
- eksfargateprofile.subnetId

New controls for CIS Amazon Web Services Foundations Benchmark

We have added the following 2 new controls to CIS Amazon Web Services Foundations Benchmark.

CID	Resource	Service	Control Title
175	IAM User	IAM	Ensure no Inline Policies are attached to IAM Users directly
176	IAM User	IAM	Ensure no Managed Policies are attached to IAM Users directly

Microsoft Azure

New controls for CIS Microsoft Azure Foundations Benchmark

We have added the following 7 new controls to CIS Microsoft Azure Foundations Benchmark.

CID	Resource	Service	Control Title
50135	Activity Log Alert	Monitor	Ensure that Activity Log Alert exists for Delete Policy Assignment
50137	Disks	Disks	Ensure that 'OS and Data' disks are encrypted with CMK
50138	Network Security Group	Network Security Group	Ensure that UDP services are restricted from the Internet
50139	Security Policy	Security Center	Ensure that Azure Defender is set to On for Kubernetes
50140	Security Policy	Security Center	Ensure that Azure Defender is set to On for Container Registries
50141	Security Policy	Security Center	Ensure that Azure Defender is set to On for Key Vault
50142	Activity Log Alert	Monitor	Ensure Diagnostic Setting captures appropriate categories

Control Migrated for Microsoft Azure

We have migrated the following control from CIS Microsoft Azure Foundations Benchmark to Azure Best Practices Policy.

Old Policy: CIS Microsoft Azure Foundations Benchmark

New Policy: Azure Best Practices Policy

CID	Resource	Service	Control Title
50024	Activity Log Alert	Monitor	Ensure that LogProfile for a subscription is configured properly
50025	Security Policy	Security Center	Ensure that Monitor unencrypted SQL databases in Azure Security Center is set to On
50044	PSQL server	PSQL server	Ensure server parameter 'log_duration' is set to 'ON' for PostgreSQL Database Server

Google Cloud Platform

Project ID for GCP Connectors

Google Cloud Platform allows usage of the same service account for multiple projects. To give users the same flexibility for GCP connectors, we now allow you to provide distinct project ID with same service account for creating GCP connectors. As a result, you can create multiple GCP connectors with same service account but distinct project IDs.

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

Provide a name, description, polling frequency for your GCP connector.

Provide a project Id for your GCP connector. Upload the configuration file and click Create Connector.

The screenshot shows the 'Create GCP Connector' form. It has a blue header with a back arrow and the title 'Create GCP Connector'. Below the header, there are several sections:

- Description:** A text area with the placeholder 'Sample GCP Connector description' and a character count '3968/4000 characters remaining'.
- Polling Frequency:** A section with the instruction 'Configure the interval at which the connector should fetch data from GCP cloud provider.' It contains two dropdown menus: 'Hours' (set to 4) and 'Minutes' (set to 0).
- Authentication Details:** A section with a red circle around the 'Project ID *' label and the text 'sample-project-id' in the input field.
- Configuration File:** A section with a dashed border and a cloud icon. It contains a file upload area with the text 'Drop file here to attach or browse'. Below this, there is a list of files: '1 file' and 'response_1594206461026.json' (31/Mar/2021 9:26 PM, 2 Bytes).

At the bottom of the form, there are three buttons: 'Cancel', 'Test Connector', and 'Create Connector'.

You can use the same service account for setting up connectors for additional projects. You can assign an existing service account to a member in IAM at the organization level or at the project level. The detailed steps for assigning service account to other projects or organization are listed in the CloudView online help.

API Features and Enhancements

We have introduced API changes for Project ID of GCP Connectors. For detailed information, refer to [CloudView 1.15 API Release Notes](#).

Issues Addressed

AWS

- Updated CIS Amazon Web Services Foundations Benchmark PDF with required missing controls.

Azure: Updated the control logic, title and content for following controls

- CID 50006 - Ensure that Vulnerabilities in security configuration on your machines should be remediated is set to On
- CID 50017 - Ensure that Vulnerabilities should be remediated by a Vulnerability Assessment solution

GCP

- Updated control logic for CID 52089 to filter read replicas. CID 52107 is updated to check point-in-recovery for postgresQL
- Updated control logic for CID 52021/52022 to filter out rules with direction EGRESS
- Rectified remediation steps for CID 52078.

Common

- We have now fixed an issue where on downloading CSV report (Vulnerability search token result on Monitor tab), the report with vulnerability details is downloaded. Earlier, the CSV report that was downloaded was empty.
- We have now fixed an issue so that the Name field displays correct data for all Azure virtual machines the Resource listing page.
- We have now fixed the connector count sync issue between AssetView and CloudView. Due to the sync issue earlier, an error was displayed when Create connector in CloudView checkbox was selected.