



Qualys CloudView v1.x

Version 1.9.4.0

July 10, 2020

Here's what's new in Qualys CloudView 1.9.4!

Amazon Web Services

[New Controls Added to AWS Best Practices Policy](#)
[Support for Two New Regions](#)

Microsoft Azure

[Inventory Support for Function App Resource \(App Service\)](#)
[New Azure Database Service Best Practices Policy](#)
[New Controls Added to Microsoft Azure Best Practices Policy](#)
[Azure Control Updates](#)

Google Cloud Platform

[Inventory Support for Cloud Function Resource](#)
[New Controls Added to GCP Kubernetes Engine Best Practices Policy](#)
[GCP Control Updates](#)

Common Feature

[Configure Connector Polling Frequency](#)
[Configure and Generate Alerts Using APIs \(Beta\)](#)

Amazon Web Services

New Controls Added to AWS Best Practices Policy

We have added the following 11 new controls to AWS Best Practices Policy.

CID	Resource	Service	Control Title
145	EFS	EFS	Ensure CMK is used to encrypt data at rest for EFS
146	EBS Snapshots	EC2	Ensure that AWS Elastic Block Store (EBS) volume snapshots are not public
147	MEMCAC HED	ELASTIC ACHE	Ensure that AWS ElastiCache Memcached clusters are not associated with default VPC
148	REDIS	ELASTIC ACHE	Ensure that AWS ElastiCache Redis clusters are not associated with default VPC
149	REDIS	ELASTIC ACHE	Ensure that AWS ElastiCache redis clusters are not using their default endpoint ports
150	MEMCAC HED	ELASTIC ACHE	Ensure that AWS ElastiCache memcached clusters are not using their default endpoint ports
151	REDIS	ELASTIC ACHE	Ensure AWS ElastiCache Redis cluster with MultiAZ Automatic Failover feature is set to enabled
152	REDIS	ELASTIC ACHE	Ensure AWS ElastiCache Redis cluster with Redis AUTH feature is enabled
153	REDIS	ELASTIC ACHE	Ensure that AWS ElastiCache Redis clusters are In-Transit encrypted
154	REDIS	ELASTIC ACHE	Ensure that AWS ElastiCache Redis clusters are Data At-Rest encrypted
155	REDIS	ELASTIC ACHE	Ensure that AWS ElastiCache Redis clusters are Data At-Rest encrypted with CMK

Support for Two New Regions

We have now added support for two new regions: Africa (Cape Town), Europe (Milan). Our AWS connectors now discover and assess resources from Africa (Cape Town) and Europe (Milan).

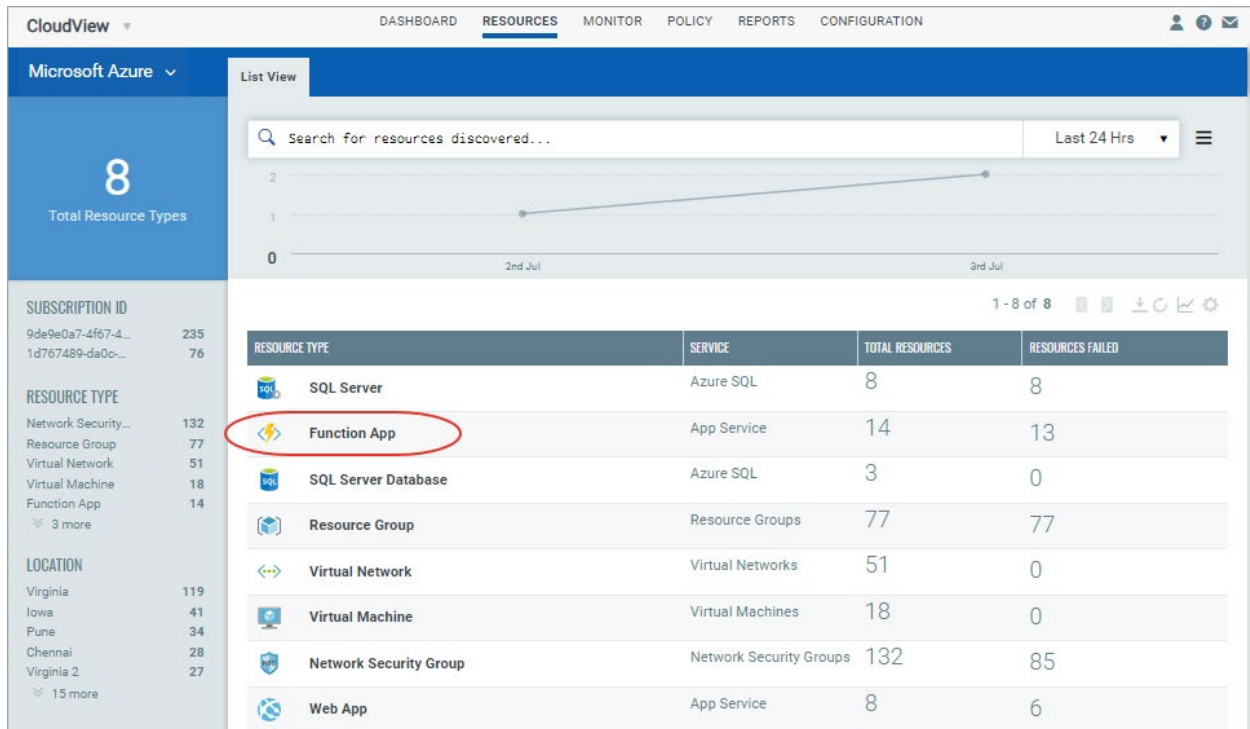
Once you create AWS connector, the connector will establish a connection with AWS to start discovering resources from each region and evaluate them against policies.

Microsoft Azure

Inventory Support for Function App Resource (App Service)

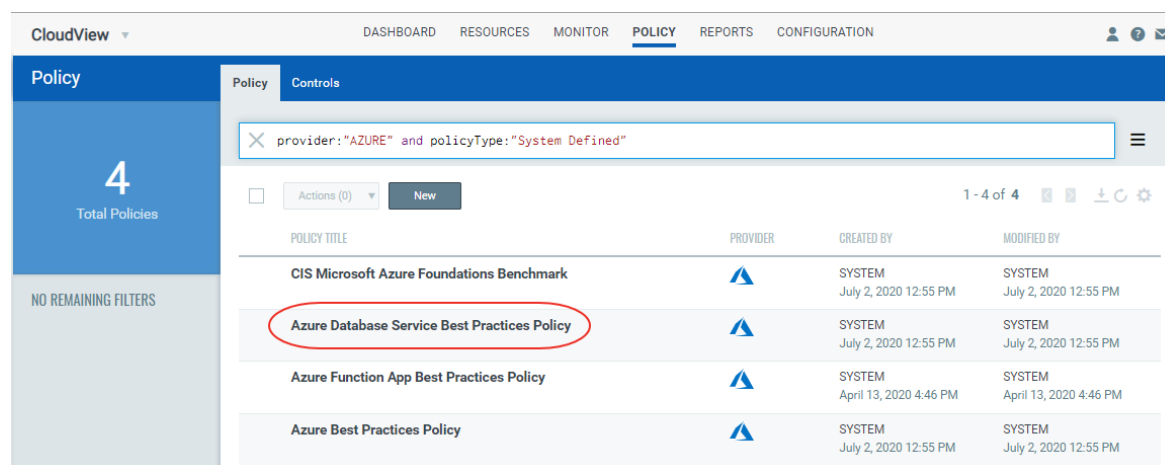
You can now monitor Function App resources and view its details. You can filter further using the tokens and view the resource information.

Go to Resources tab and select Microsoft Azure from the dropdown. You can view the newly supported resource in the List View.



New Azure Database Service Best Practices Policy

We have introduced a new 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.



New Controls

We have added the following 21 new controls to Azure Database Service Best Practices Policy.

CID	Resource	Service	Control Title
50095	SQL Database	Azure SQL	Ensure that default Auditing policy for a SQL Database is configured to capture and retain the activity logs
50096	SQL Database	Azure SQL	Ensure that Advanced Data Security is enabled and Advanced Threat Protection settings is configured properly for a SQL Database
50098	SQL Server	Azure SQL	Ensure that 'ssl_minimal_tls_version_enforced' is set to '1.2' for SQL server
50102	MySQL Server	MySQL Server	Ensure that Advanced Threat Protection settings is configured properly for Azure Database for MySQL Server
50103	MySQL Server	MySQL Server	Ensure that TLS is enforced and the minimum version be set to 1.2 for Azure Database for MYSQL server
50104	MySQL Server	MySQL Server	Ensure no MySQL Server allow ingress from Internet (ANY IP)
50105	MySQL Server	MySQL Server	Ensure that 'geo_redundant_backup_enabled' is set to Enabled for Azure Database for MySQL server
50106	MySQL Server	MySQL Server	Ensure that Public Network Access is Disabled for Azure Database for MySQL server

CID	Resource	Service	Control Title
50107	MySQL Server	MySQL Server	Ensure that Azure Database for MySQL server diagnostic setting is configured properly
50108	MariaDB Server	MariaDB Server	Ensure that Advanced Threat Protection settings is configured properly for Azure Database for MariaDB Server
50109	MariaDB Server	MariaDB Server	Ensure 'Enforce SSL connection' is set to 'ENABLED' for Azure Database for MariaDB server
50110	MariaDB Server	MariaDB Server	Ensure that TLS is enforced and the minimum version be set to 1.2 for Azure Database for MariaDB server
50111	MariaDB Server	MariaDB Server	Ensure no MariaDB Server allow ingress from Internet (ANY IP)
50112	MariaDB Server	MariaDB Server	Ensure that 'geo_redundant_backup_enabled' is set to Enabled for Azure Database for MariaDB server
50113	MariaDB Server	MariaDB Server	Ensure that Public Network Access is Disabled for Azure Database for MariaDB server
50115	PostgreSQL Server	PostgreSQL Server	Ensure that Advanced Threat Protection settings is configured properly for Azure Database for PostgreSQL Server
50116	PostgreSQL Server	PostgreSQL Server	Ensure that TLS is enforced and the minimum version be set to 1.2 for Azure Database for PostgreSQL server
50117	PostgreSQL Server	PostgreSQL Server	Ensure no PostgreSQL Server allow ingress from Internet (ANY IP)
50118	PostgreSQL Server	PostgreSQL Server	Ensure that 'geo_redundant_backup_enabled' is set to Enabled for Azure Database for PostgreSQL server
50119	PostgreSQL Server	PostgreSQL Server	Ensure that Public Network Access is Disabled for Azure Database for PostgreSQL server
50120	PostgreSQL Server	PostgreSQL Server	Ensure that Azure Database for PostgreSQL server diagnostic setting is configured properly

New Controls Added to Microsoft Azure Best Practices Policy

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

CID	Resource	Service	Control Title
50057	Container Registries	Container Registries	Ensure that Azure Container Registry using the deprecated classic registry
50059	Monitor	Activity Log Alert	Ensure Activity Log Alert for Delete SQL server firewall rule
50060	Virtual Network	Virtual Network Subnet	Ensure that Azure Virtual Network subnet is configured with a Network Security Group

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.

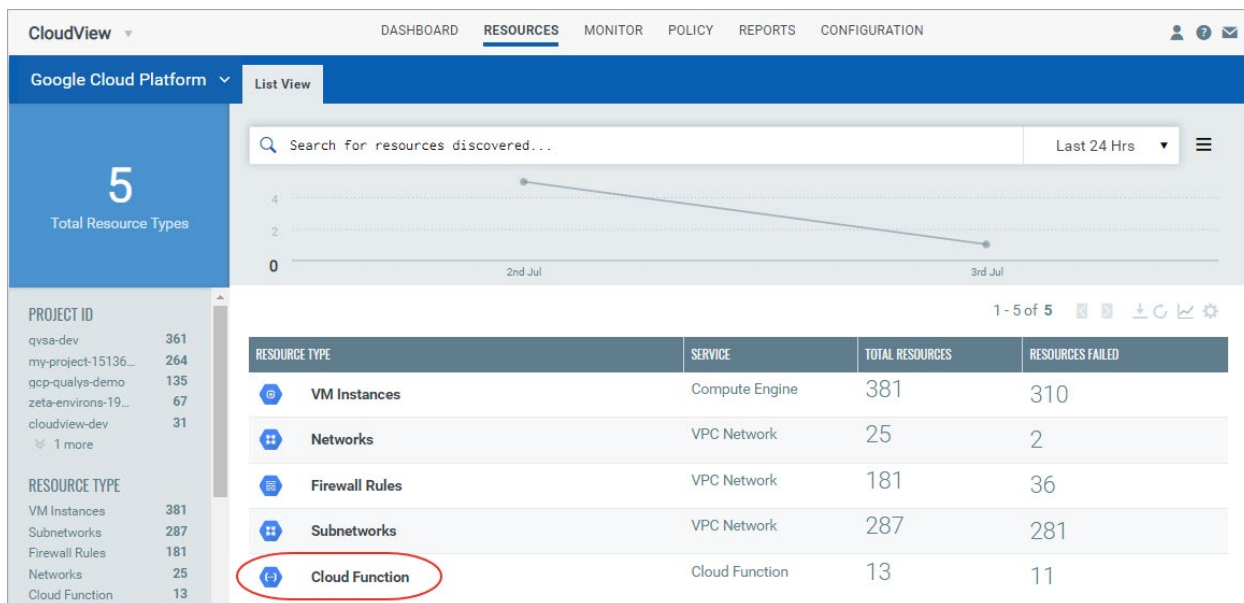
CID	Service	Resource	Title	Sections Updated
50075	Key Vault	Key Vault	Ensure that diagnostic settings for Azure KeyVault is set to 'ON'	Updated control logic
50049	App Service	Web App	Ensure Web app has "Client Certificates (Incoming client certificates)" set to "On"	Remediation Updated
50084	App Service	Function App	Ensure App Service Authentication is set on Function Apps	Remediation Updated
50085	App Service	Function App	Ensure Function app redirects all HTTP traffic to HTTPS	Remediation Updated
50086	App Service	Function App	Ensure Function app has "Client Certificates (Incoming client certificates)" set to "On"	Remediation Updated
50087	App Service	Function App	Ensure that "Register with Azure Active Directory" is enabled on Function apps	Remediation Updated
50088	App Service	Function App	Ensure Function app is using the latest version of TLS encryption version	Remediation Updated
50089	App Service	Function App	Ensure that "HTTP Version" used for Function app is latest	Remediation Updated

Google Cloud Platform

Inventory Support for Cloud Function Resource

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

Go to Resources tab and select Google Cloud Platform from the dropdown. You can view the newly supported resource in the List View.



New Controls Added to GCP Kubernetes Engine Best Practices Policy

We have added the following five new controls to GCP Kubernetes Engine Best Practices Policy.

CID	Resource	Service	Control Title
52101	Kubernetes Engine	Kubernetes Cluster	Ensure Binary Authorization is set to Enabled on Kubernetes Engine Clusters
52102	Kubernetes Engine	Kubernetes Cluster	Ensure Container-Optimized OS (cos) is used for Kubernetes Engine Clusters Node image
52103	Kubernetes Engine	Kubernetes Cluster	Ensure GCP Kubernetes Engine Clusters are not using the default network
52104	Kubernetes Engine	Kubernetes Cluster	Ensure that network traffic egress metering is enabled on Kubernetes Engine Clusters
52105	Kubernetes Engine	Kubernetes Cluster	Ensure that legacy compute engine metadata endpoint for GCP Kubernetes Engine Cluster Node is disabled

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
52038	Kubernetes Engine	Kubernetes Cluster	Ensure Legacy Authorization is set to Disabled on Kubernetes Engine Clusters	Remediation Updated
52041	Kubernetes Engine	Kubernetes Cluster	Ensure Automatic node upgrades is enabled on Kubernetes Engine Clusters nodes	Remediation Updated
52051	Kubernetes Engine	Kubernetes Cluster	Ensure Stackdriver Kubernetes Engine Monitoring is set to Enabled on Kubernetes Engine Clusters	Remediation Updated

Common Feature

Configure Connector Polling Frequency

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

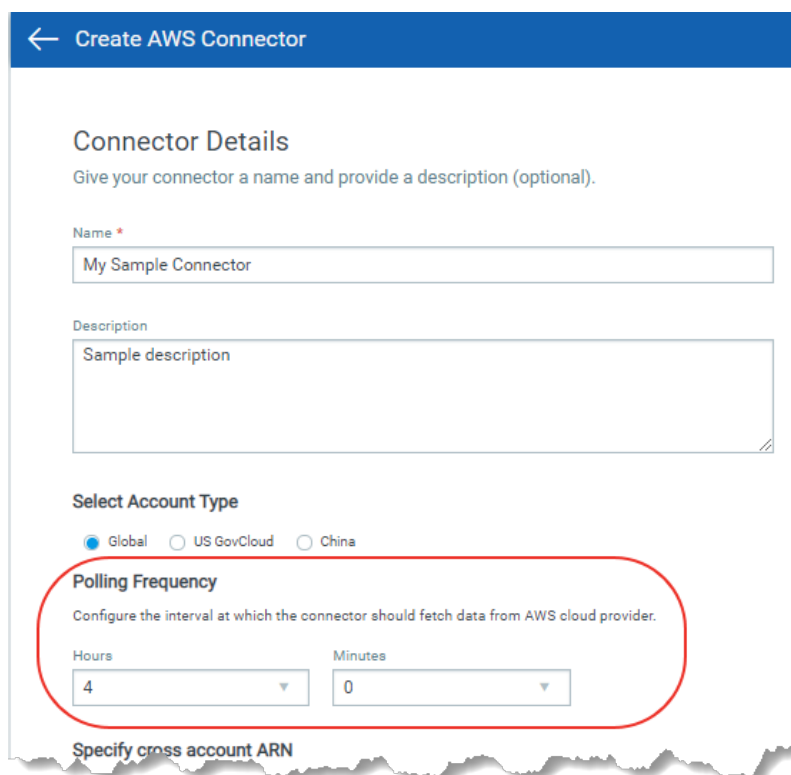
Earlier, Qualys pre-configured a fixed polling frequency for the connector. The polling frequency was set to 4 hours by default and was not configurable. We now give you the flexibility to configure the polling frequency of the connector as per your need.

Note: Configuration of connector polling frequency is available only for Cloud Security Assessment (CSA) users.

Go to the Configuration and select the cloud provider and click the respective tab. Click Create Connector and provide all the necessary details. Select a frequency at which the connector should poll the cloud provider and fetch data. You can configure frequency from minimum one hour to maximum 24 hours.

You can configure the connector polling frequency during connector creation process or edit an existing connector.

By default, all existing connectors are configured to polling frequency of 4 hours.



The screenshot shows the 'Create AWS Connector' form. The 'Polling Frequency' section is highlighted with a red circle. It includes a title 'Polling Frequency', a subtitle 'Configure the interval at which the connector should fetch data from AWS cloud provider.', and two dropdown menus for 'Hours' (set to 4) and 'Minutes' (set to 0). Below the highlighted section is a field for 'Specify cross account ARN'.

Configure and Generate Alerts Using APIs (Beta)

We have now introduced APIs to generate alert responses for the control assessment criteria you define. You can now configure monitoring of critical controls and triggering alert messages on detection of critical conditions. The alert messages you receive includes control assessment details. These alerts are notified through either Email, Slack or Pagerduty. For detailed information, refer to [CloudView 1.9.4 API Release Notes](#).