Qualys CloudView v1.x

Version 1.14.0

March 10, 2021

Here’s what’s new in Qualys CloudView 1.14.0!

Amazon Web Services

Secure Configurable External ID Format for AWS Connectors
New controls for CIS Amazon Web Services Foundations Benchmark

Microsoft Azure

Subscription Name for Azure Connectors
New controls for CIS Microsoft Azure Foundations Benchmark
Controls Migrated for Microsoft Azure
Microsoft Azure Control Updates

Common Feature

Enable - Disable Connectors
Configure Rule-Based Alerts
PDF Format for Assessment Reports

Qualys CloudView 1.14 brings you many more Improvements and updates! Learn more

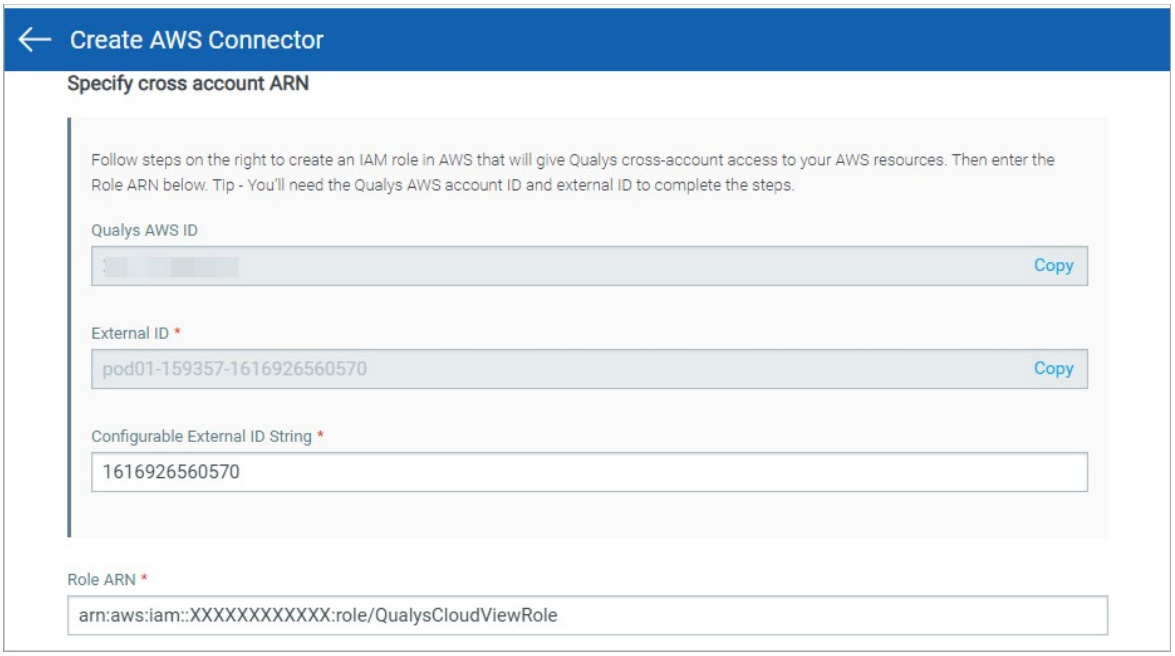
Amazon Web Services

Secure Configurable External ID Format for AWS Connectors

We have now updated the external ID format for AWS connectors to adhere to the AWS vendor requirement best practices. 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 new external ID format.

Note: All previously created connectors continue to work as configured. If the customer has to update an existing connector or create a new connector, they need to provide the external ID in the new format.

Go to **Configuration** > **Amazon Web Services** > **Create Connector** to create a new connector. The external ID consists of three parts. Two parts are pre-set by Qualys and the third part is editable by the customer.



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 Qualys AWS account ID and external ID to complete the steps.

Qualys AWS ID: [redacted]

External ID *: pod01-159357-1616926560570

Configurable External ID String *: 1616926560570

Role ARN *: arn:aws:iam::XXXXXXXXXXXX:role/QualysCloudViewRole

External ID: <Qualys POD>-<Qualys Subscription ID>-<Configurable External ID String>

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.

Configurable External ID String: Unique random alphanumeric number You can use a combination of alphabets (a-z, A-Z) and numbers to generate the unique number. You could use minimum 5 or maximum 13 digits to complete the external ID combination in the new format.

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

New controls for CIS Amazon Web Services Foundations Benchmark

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

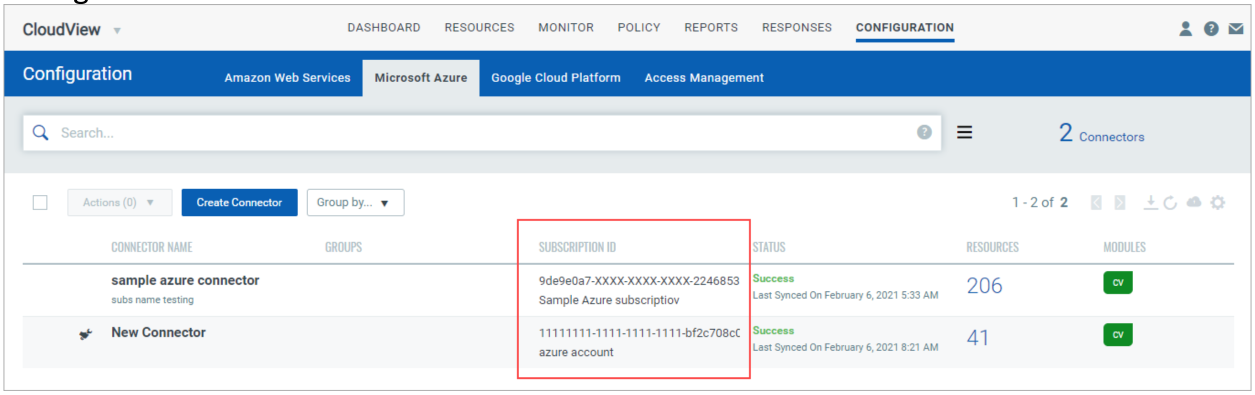
CID	Resource	Service	Control Title
177	Bucket	S3	Ensure that Object-level logging for write events is enabled for S3 bucket
178	Bucket	S3	Ensure that Object-level logging for read events is enabled for S3 bucket

Microsoft Azure

Subscription Name for Azure Connectors

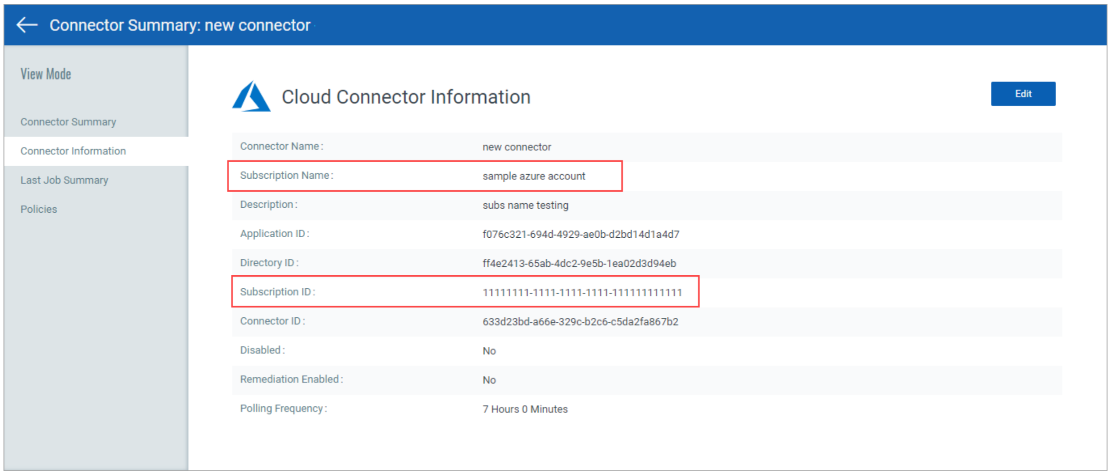
We now display the subscription name details for Microsoft Azure connectors. The Suscription ID column now displays subscription name below the subscription ID. You can also view the subscription name associated with the Azure connectors on multiple screens such as Azure Configurations, Azure Resources, Control evaluations of Azure resources, Dashboards, Assessment Reports. Let us view few examples.

Configuration > Microsoft Azure tab



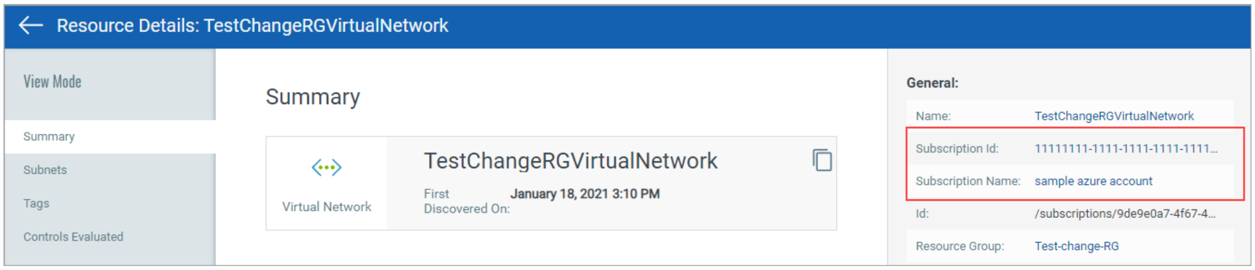
CONNECTOR NAME	GROUPS	SUBSCRIPTION ID	STATUS	RESOURCES	MODULES
sample azure connector subs name testing		9de9e0a7-XXXX-XXXX-XXXX-2246853 Sample Azure subscriptiov	Success Last Synced On February 6, 2021 5:33 AM	206	CV
New Connector		11111111-1111-1111-1111-bf2c708c0 azure account	Success Last Synced On February 6, 2021 8:21 AM	41	CV

Azure Connector Details



Connector Name :	new connector
Subscription Name :	sample azure account
Description :	subs name testing
Application ID :	f076c321-694d-4929-ae0b-d2bd14d1a4d7
Directory ID :	ff4e2413-65ab-4dc2-9e5b-1ea02d3d94eb
Subscription ID :	11111111-1111-1111-1111-111111111111
Connector ID :	633d23bd-a66e-329c-b2c6-c5da2fa867b2
Disabled :	No
Remediation Enabled :	No
Polling Frequency :	7 Hours 0 Minutes

Azure Resource Details



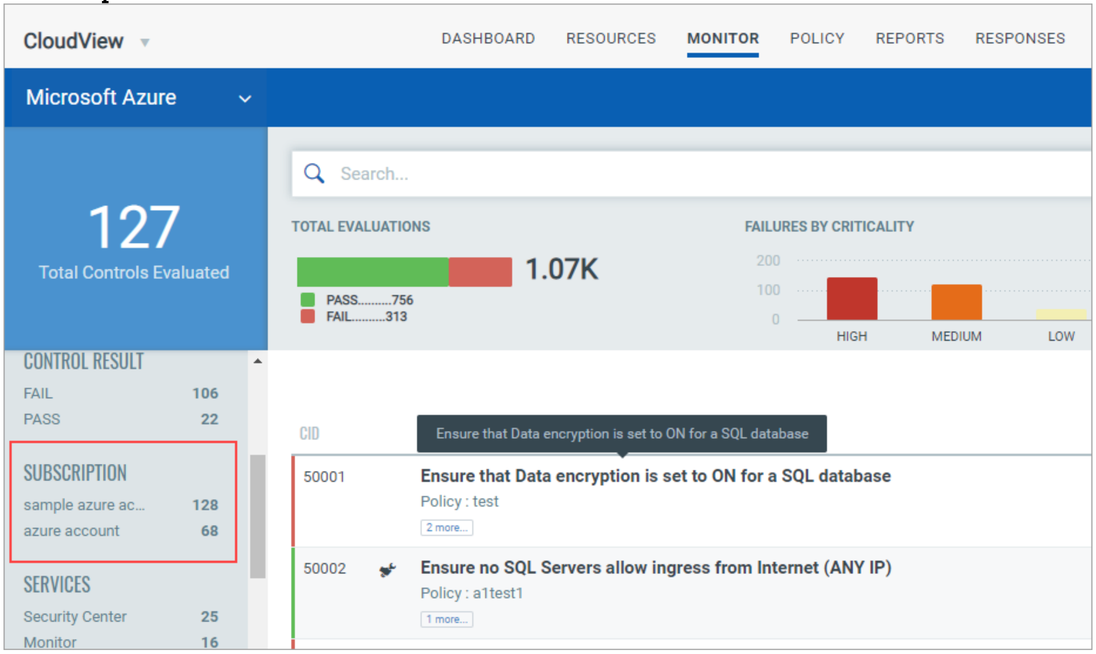
TestChangeRGVirtualNetwork

First Discovered On: January 18, 2021 3:10 PM

General:

Name:	TestChangeRGVirtualNetwork
Subscription Id:	11111111-1111-1111-1111-1111...
Subscription Name:	sample azure account
Id:	/subscriptions/9de9e0a7-4f67-4...
Resource Group:	Test-change-RG

Subscription Name Filter in Monitor Tab



Ensure that Data encryption is set to ON for a SQL database

CID	
50001	Ensure that Data encryption is set to ON for a SQL database Policy : test 2 more...
50002	Ensure no SQL Servers allow ingress from Internet (ANY IP) Policy : a1test1 1 more...

New controls for CIS Microsoft Azure Foundations Benchmark

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

CID	Resource	Service	Control Title
50133	Storage	Storage	Ensure soft delete is enabled for Azure Storage.
50134	Storage	Storage	Ensure Storage Service Encryption is enabled for Storage Accounts.
50136	Web App	App Service	Ensure FTP deployments are disabled for web apps.

Controls Migrated for Microsoft Azure

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

Old Policy: CIS Microsoft Azure Foundations Benchmark

New Policy: Azure Best Practices Policy

CID	Service	Resource	Control Title
50003	Security Center	Security Policy	Ensure ASC Default policy setting "Monitor Adaptive Application Whitelisting" is not "Disabled"
50005	Security Center	Security Policy	Ensure ASC Default policy setting "Monitor System Updates" is not "Disabled"
50006	Security Center	Security Policy	Ensure ASC Default policy setting "Monitor OS Vulnerabilities" is not "Disabled"
50007	Security Center	Security Policy	Ensure ASC Default policy setting "Monitor Endpoint Protection" is not "Disabled"

CID	Service	Resource	Control Title
50008	Security Center	Security Policy	Ensure ASC Default policy setting "Monitor Disk Encryption" is not "Disabled"
50009	Security Center	Security Policy	Ensure ASC Default policy setting "Monitor Network Security Groups" is not "Disabled"
50010	Security Center	Security Policy	Ensure ASC Default policy setting "Monitor Web Application Firewall" is not "Disabled"
50014	Security Center	Security Policy	Ensure ASC Default policy setting "Monitor SQL Auditing" is not "Disabled"
50016	Security Center	Security Policy	Ensure ASC Default policy setting "Enable Next Generation Firewall(NGFW) Monitoring" is not "Disabled"
50017	Security Center	Security Policy	Ensure ASC Default policy setting "Monitor Vulnerability Assessment" is not "Disabled"
50018	Security Center	Security Policy	Ensure ASC Default policy setting "Monitor Storage Blob Encryption" is not "Disabled"
50019	Security Center	Security Policy	Ensure ASC Default policy setting "Monitor JIT Network Access" is not "Disabled"
50021	Security Center	Security Policy	Ensure that security contact 'Phone number' is set
50071	Security Center	Security Policy	Ensure that Activity Log Alert exists for Update Security Policy

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

Old Policy: Azure Best Practices Policy

New Policy: CIS Microsoft Azure Foundations Benchmark

CID	Service	Resource	Control Title
50077	Security Center	Security Policy	Ensure that Settings - Threat Detection for Microsoft Cloud App Security (MCAS) is selected
50078	Security Center	Security Policy	Ensure that Settings - Threat Detection for Windows Defender ATP (WDATP) is selected
50082	Security Center	Security Policy	Ensure any of the ASC Default policy setting is not set to 'Disabled'
50083	Azure SQL	SQL Server	Ensure that ADS - Vulnerability Assessment (VA) is enabled and configured properly
50130	Virtual Machine	Virtual Machine	Ensure that the endpoint protection for all Virtual Machines is installed

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

Old Policy: Azure Database Service Best Practices Policy

New Policy: CIS Microsoft Azure Foundations Benchmark

CID	Service	Resource	Control Title
50117	Postgre SQL	Postgre SQL	Ensure 'Allow access to Azure services' for PostgreSQL Database Server is disabled

Microsoft Azure Control Updates

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

CID	Service	Resource	Title	Sections Updated
50015	Security Center	Security Policy	Ensure that Azure Defender is set to On for Servers	Updated Title, static content and service type / resource type change
50020	Security Center	Security Policy	Ensure 'Additional email addresses' is configured with a security contact email	Updated Title, static content and service type / resource type change
50022	Security Center	Security Policy	Ensure that 'Notify about alerts with the following severity' is set to 'High'	Updated Title, static content and service type / resource type change
50023	Security Center	Security Policy	Ensure that 'All users with the following roles' is set to 'Owner'	Updated Title, static content and service type / resource type change
50072	Azure Active Directory	User	Ensure guest users are reviewed on a monthly basis	Updated Title
50077	Security Center	Security Policy	Ensure that Settings - Threat Detection for Microsoft Cloud App Security (MCAS) is selected	Updated Title
50078	Security Center	Security Policy	Ensure that Settings - Threat Detection for Windows Defender ATP (WDATP) is selected	Updated Title
50079	Security Center	Security Policy	Ensure that Azure Defender is set to On for Azure SQL database servers	Updated Title, static content and service type / resource type change
50080	Security Center	Security Policy	Ensure that Azure Defender is set to On for App Service	Updated Title, static content and service type / resource type change
50081	Security Center	Security Policy	Ensure that Azure Defender is set to On for Storage	Updated Title, static content and service type / resource type change
50117	PostgreSQL	PostgreSQL	Ensure 'Allow access to Azure services' for PostgreSQL Database Server is disabled	Updated Title

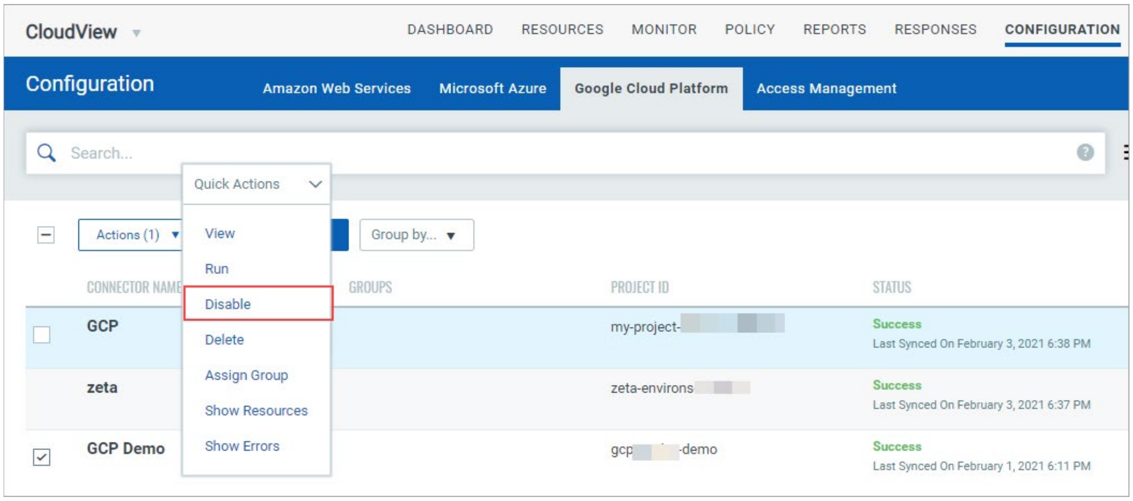
Common Feature

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. By default, all connectors you create are in enabled state.

Disable Connector

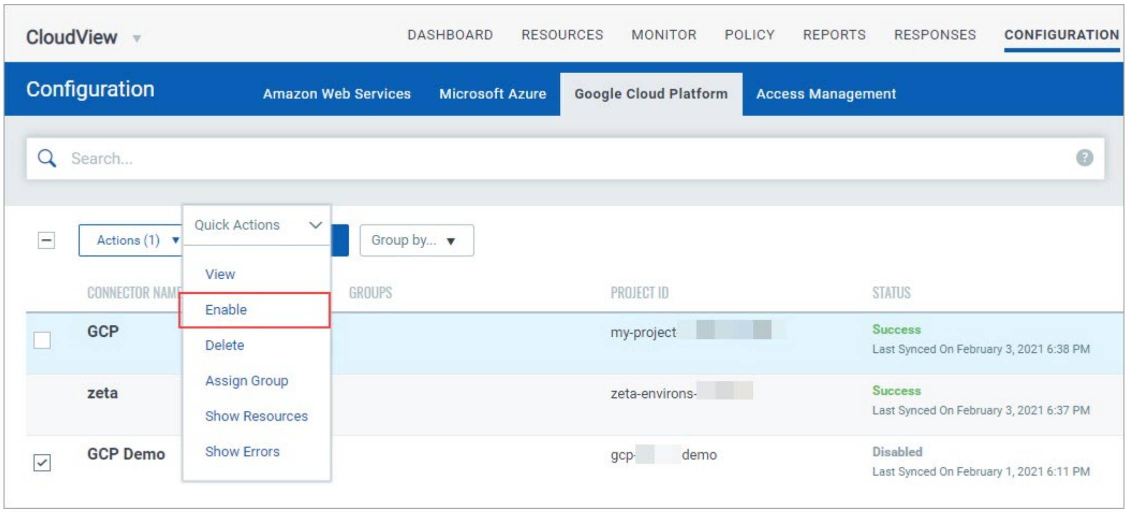
Go to Configuration tab and then the cloud provider tab, where the connector belongs. Select the connector to be disabled and from the quick actions menu, select Disable from the quick actions menu. Click on the confirmation message. The connector gets disabled.



	CONNECTOR NAME	GROUPS	PROJECT ID	STATUS
□	GCP		my-project-[redacted]	Success Last Synced On February 3, 2021 6:38 PM
	zeta		zeta-environs[redacted]	Success Last Synced On February 3, 2021 6:37 PM
☑	GCP Demo		gcp[redacted]-demo	Success Last Synced On February 1, 2021 6:11 PM

Enable Connector

After you disable a connectors, you can enable the connector. From the quick actions menu, select Enable from the quick actions menu. The connector gets enabled.



	CONNECTOR NAME	GROUPS	PROJECT ID	STATUS
□	GCP		my-project [redacted]	Success Last Synced On February 3, 2021 6:38 PM
	zeta		zeta-environs-[redacted]	Success Last Synced On February 3, 2021 6:37 PM
☑	GCP Demo		gcp-[redacted]demo	Disabled Last Synced On February 1, 2021 6:11 PM

Note: Automatic or manual connector run skips the disabled connectors. Only connectors with enabled state are executed during connector run.

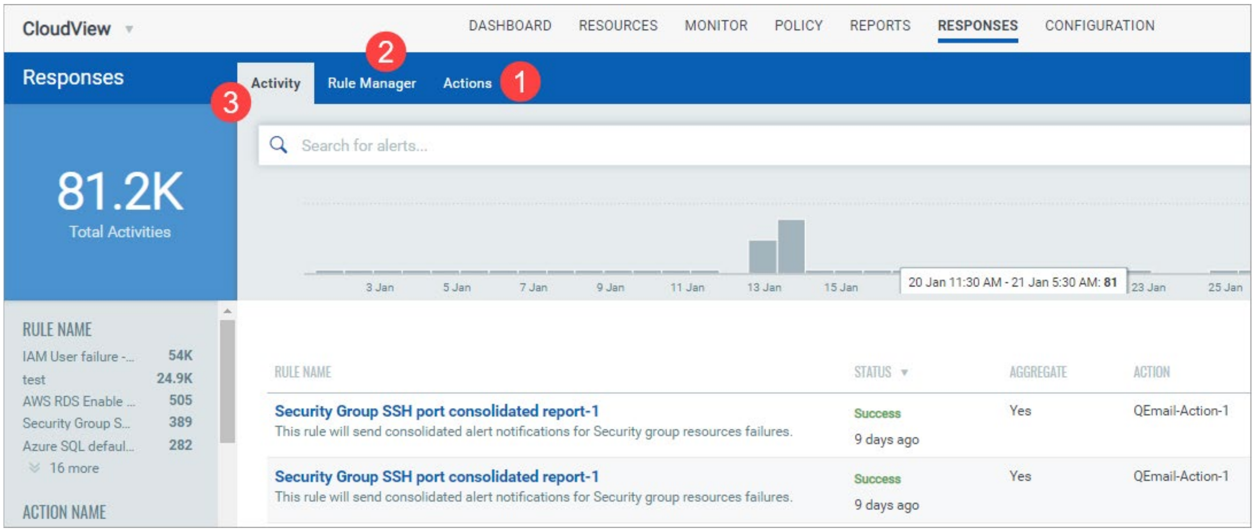
Configure Rule-Based Alerts

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

How to set up 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.



RULE NAME	
IAM User failure -...	54K
test	24.9K
AWS RDS Enable ...	505
Security Group S...	389
Azure SQL defaul...	282

RULE NAME	STATUS	AGGREGATE	ACTION
Security Group SSH port consolidated report-1 This rule will send consolidated alert notifications for Security group resources failures.	Success 9 days ago	Yes	QEmail-Action-1
Security Group SSH port consolidated report-1 This rule will send consolidated alert notifications for Security group resources failures.	Success 9 days ago	Yes	QEmail-Action-1

Step 1 - Define actions that the rule must implement in response to the alert.

Define the method in which you want to be alerted once any rule created by you is triggered.

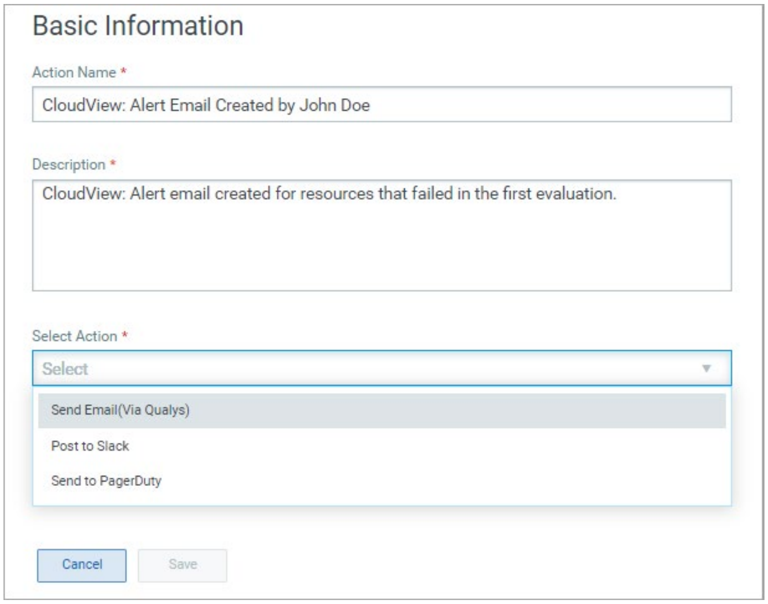
Navigate to **Rules** > **Actions** > **New Action** and provide details required to create a new action:
- In the Basic Information section, provide name and description of the action in the Action Name and Description fields respectively.
- Select an action from the **Select Action** drop-down and provide the settings for configuring the messaging system to send alerts.

We support the following three actions for alerting:
- **Send Email (Via Qualys)** 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 that is required to connect to your PagerDuty account.

- **Post to Slack** to post alert messages to your Slack account. Provide the Webhook

URI that will be used to connect to your slack account to post alert messages.



Basic Information

Action Name *

CloudView: Alert Email Created by John Doe

Description *

CloudView: Alert email created for resources that failed in the first evaluation.

Select Action *

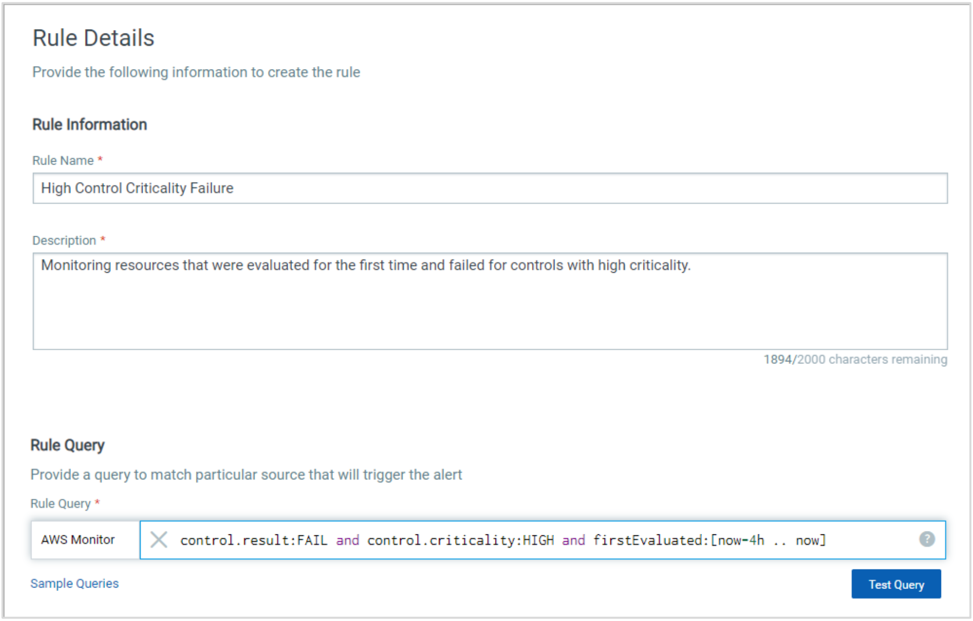
Select

View and manage the newly created actions in the **Actions** tab with details such as name of the action, type of the action, etc.

Step 2 - Set up your rules in the Rule Manager tab

Define the conditions, significant finding or event that should trigger the rules and send you alerts.

Navigate to **Rules** > **Rule Manager** > **New Rule** and provide required details in the respective sections to create a new rule:
- In the Rule Information section, provide a name and description of the new rule.
- 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 to select from predefined queries.



Rule Details

Provide the following information to create the rule

Rule Information

Rule Name *

High Control Criticality Failure

Description *

Monitoring resources that were evaluated for the first time and failed for controls with high criticality.

1894/2000 characters remaining

Rule Query

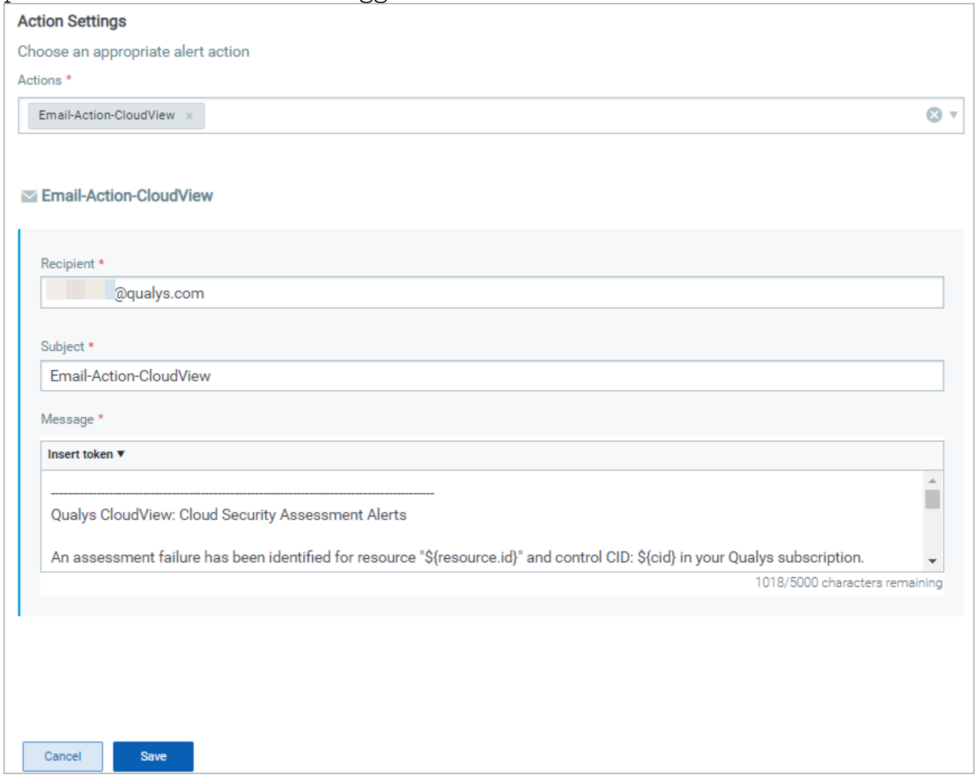
Provide a query to match particular source that will trigger the alert

Rule Query *

AWS Monitor

```
control.result:FAIL and control.criticality:HIGH and firstEvaluated:[now-4h .. now]
```

- In the Action Settings section, choose the actions that you want the system to perform when an alert is triggered.



Action Settings

Choose an appropriate alert action

Actions *: Email-Action-CloudView ×

Email-Action-CloudView

Recipient *: [redacted]@qualys.com

Subject *: Email-Action-CloudView

Message *

Insert token ▾

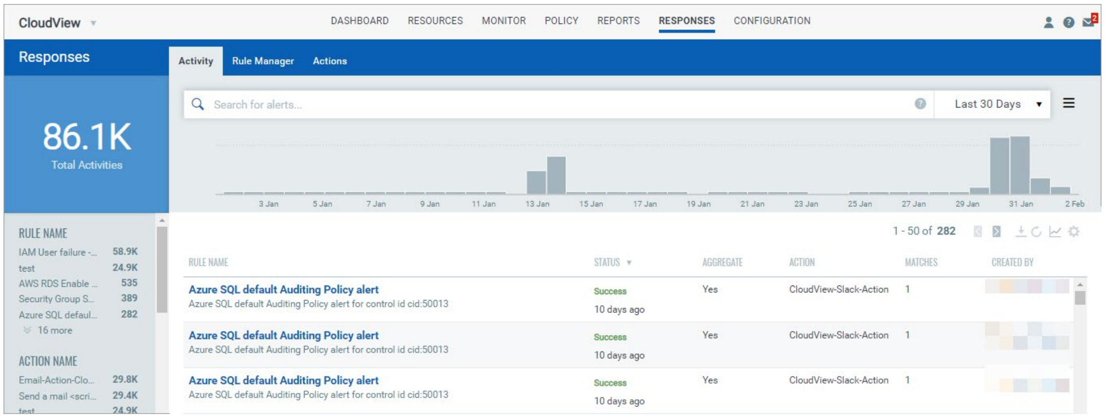
```
-----------------------------------------------------------------------------------------
Qualys CloudView: Cloud Security Assessment Alerts

An assessment failure has been identified for resource "${resource.id}" and control CID: ${cid} in your Qualys subscription.
```

1018/5000 characters remaining

You can also customize the message text by inserting tokens to the alert message.

Step 3 - Monitor all the alerts that were sent after the rules were triggered

Once a rule condition is met an action is triggered and the stakeholders are alerted. These alerts are listed in the **Activity** tab for you view. Here, you will see for each alert, rule name, success or failure in sending the alert message, action chosen for the rule, matches found for the rule etc.



RULE NAME	
IAM User failure -...	58.9K
test	24.9K
AWS RDS Enable ...	535
Security Group S...	389
Azure SQL defaul...	282
16 more	

ACTION NAME	
Email-Action-Clo...	29.8K
Send a mail <scri...	29.4K
test	24.9K

RULE NAME	STATUS ▾	AGGREGATE	ACTION	MATCHES	CREATED BY
Azure SQL default Auditing Policy alert Azure SQL default Auditing Policy alert for control id cid:50013	Success 10 days ago	Yes	CloudView-Slack-Action	1	[redacted]
Azure SQL default Auditing Policy alert Azure SQL default Auditing Policy alert for control id cid:50013	Success 10 days ago	Yes	CloudView-Slack-Action	1	[redacted]
Azure SQL default Auditing Policy alert Azure SQL default Auditing Policy alert for control id cid:50013	Success 10 days ago	Yes	CloudView-Slack-Action	1	[redacted]

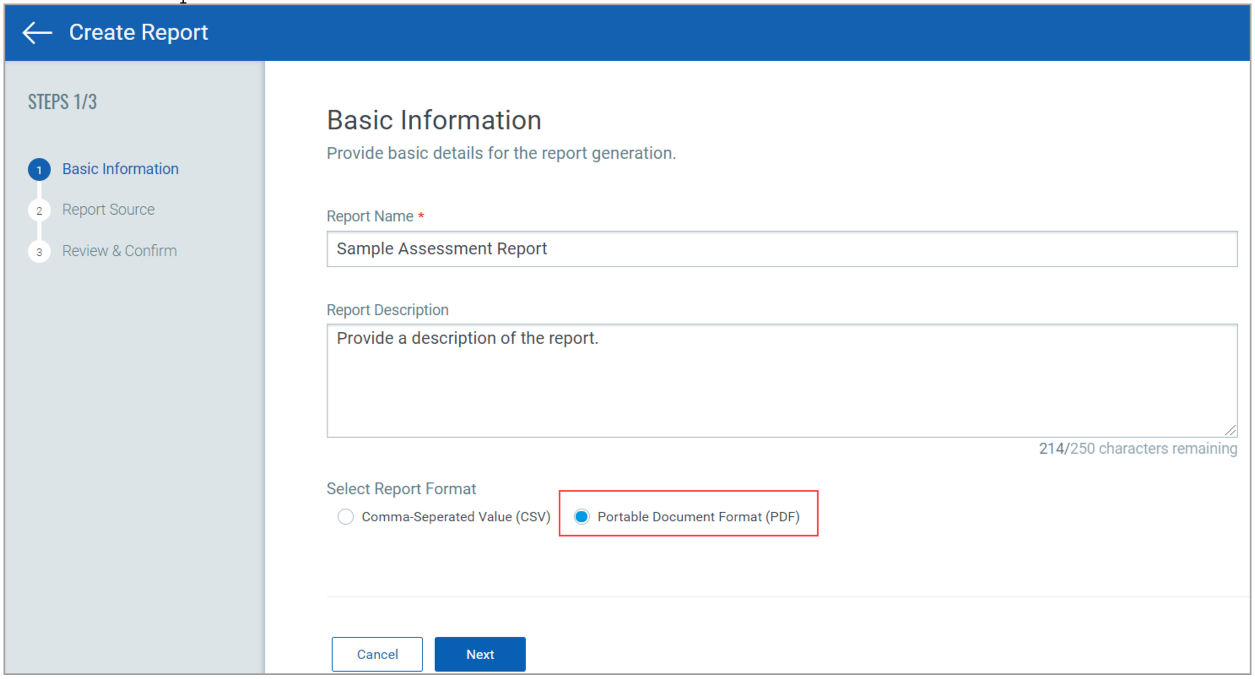
You can easily search for alerts using search tokens, select a period to view the rules triggered during that time frame, click a bar to jump to the alerts triggered in a certain time frame, use filters listed on left to group the alerts by rule name, action name, etc.

PDF Format for Assessment Reports

Use assessment reports to view the compliance of your resources for the defined policies in CloudView. Once you generate an assessment report, you can view and download the report now in PDF format.

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

Choose the report format as PDF.



Create Report

STEPS 1/3

1 Basic Information
2 Report Source
3 Review & Confirm

Basic Information

Provide basic details for the report generation.

Report Name *: Sample Assessment Report

Report Description: Provide a description of the report.

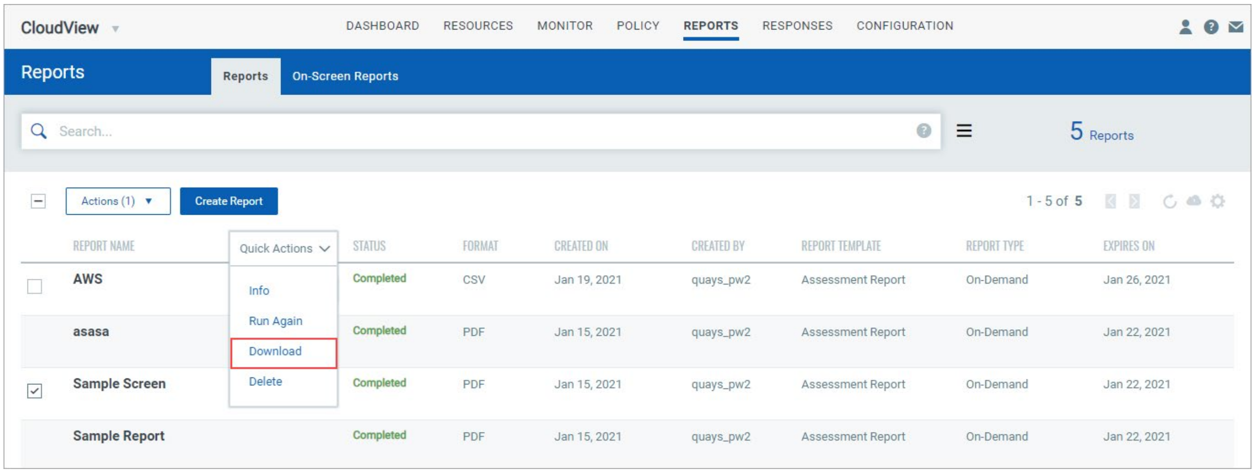
214/250 characters remaining

Select Report Format

○ Comma-Seperated Value (CSV) ● Portable Document Format (PDF)

Define the other settings as per your requirement for the assessment report. Review the configured report settings in the Summary pane and then click **Create and Run Report**.

Once the report is generated, you can download it from the Reports tab. Use **Download** from the quick actions menu to download the report.



	REPORT NAME	STATUS	FORMAT	CREATED ON	CREATED BY	REPORT TEMPLATE	REPORT TYPE	EXPIRES ON
□	AWS	Completed	CSV	Jan 19, 2021	quays_pw2	Assessment Report	On-Demand	Jan 26, 2021
	asasa	Completed	PDF	Jan 15, 2021	quays_pw2	Assessment Report	On-Demand	Jan 22, 2021
☑	Sample Screen	Completed	PDF	Jan 15, 2021	quays_pw2	Assessment Report	On-Demand	Jan 22, 2021
	Sample Report	Completed	PDF	Jan 15, 2021	quays_pw2	Assessment Report	On-Demand	Jan 22, 2021

Note: Assessment reports containing upto 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.

API Features and Enhancements

We have introduced the following API related features and enhancements:

- Unique Secure External ID for AWS connectors
- Assessment Reports in PDF Format
- Fetch Account Alias and Subscription Name
- Enable-Disable Connectors

For detailed information, refer to CloudView 1.14 API Release Notes.

Issues Addressed

- We have now added error logs with details if we encounter errors during processing of For Network Security Group resource related to Azure connectors.
- We have now fixed the pagination issue for connectors displayed for system-defined policies.
- We have rectified the curl commands for Delete connector API in CloudView API User Guide.