Qualys CloudView v1.x

Version 1.23.0
June 03, 2022

Here's what's new in Qualys CloudView 1.23.0!

Amazon Web Services

New controls for AWS Best Practices Policy
Permissions Needed for Directory Service Resource

Microsoft Azure

New controls for Azure Best Practices Policy

Common Feature

Reporting Permission
Tag-based Access Configuration
Connector Configuration
Build-Time Report Creation
New Tokens

Qualys CloudView 1.23 brings you many more Improvements and updates! Learn more

Amazon Web Services

New controls for AWS Best Practices Policy

We have introduced the following new controls for AWS Best Practices Policy.

CID	Service	Resource	Title
447	DataSync	DataSync Task	Ensure to enable data integrity checks for only files transferred in datasync task
446	DataSync	DataSync Task	Ensure a loggroup is created to upload logs of datasync task to the cloudwatch log group
448	IAM	IAM Server Certificate	Ensure that all your SSL/TLS IAM certificates are using 2048 or higher bit RSA keys
449	API Gateway	Rest API Gateway	Ensure to disable default endpoint for all the APIs
450	Microsoft AD Directory	Microsoft AD Directory	Ensure that Microsoft AD directory forward domain controller security event logs to cloudwatch logs
451	SQS	SQS Queue	Ensure SQS queues uses KMS customer managed master key
452	SQS	SQS Queue	Ensure SQS queues are encrypted in transit
453	EFS	EFS	Ensure to block public access to Amazon EFS file systems
407	Elasticache	Elasticache	Ensure all data stored in the Elasticache Replication Group is securely encrypted at transit and has auth token
256	CloudTrail	CloudTrail	Ensure that trail is configured on organization level
264	CloudTrail	CloudTrail	Ensure a Trail includes the global services
272	CloudTrail	CloudTrail	Ensure to log KMS events to the trail
355	CloudTrail	CloudTrail	Ensure Trail is configured to log Data events for s3 buckets

Permissions Needed for Directory Service Resources

The cross-account role associated with the AWS connector needs additional permissions to fetch information about the Directory Service resource. To fetch information about the resource 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 Connector online help.

Microsoft Azure

New controls for Azure Best Practices Policy

We have introduced the following new controls for Azure Best Practices Policy.

CID	Service	Resource	Title
50221	CosmosDB	CosmosDB	Ensure consistency level is not set to "eventual" for Azure CosmosDB account
50237	SQL	SQL Server	Ensure that Auditing Retention is greater than 90 days for Azure MSSQL Server
50337	SQL	SQL Server	Ensure access to Azure SQL Servers is restricted within Azure Infrastructure via Azure SQL Firewall Rule
50338	SQL	SQL Server	Ensure public accessibility is not enabled for Azure MSSQL Server
50343	SQL	SQL Server	Ensure that Auditing is set to "On" for Azure SQL Server
50349	PostgreSQL	PostgreSQL	Ensure missing service endpoints are disabled for Azure PostgreSQL Virtual Network Rule
50350	CosmosDB	CosmosDB	Ensure tags are associated with Azure CosmosDB account
50351	Storage Account	Storage Account	Ensure age in days after create to delete snapshot is more than 90 in Azure Storage Management Policy
50352	VM Scale Set	VM Scale Set	Ensure overprovisioning is disabled for Azure Linux Virtual Machine Scale Set
50354	Azure Container Instance	Azure Container Group	Ensure user ids are system managed for Azure Container Group
50355	Virtual WAN	Virtual WAN	Ensure that VPN Encryption is enabled for Azure Virtual WAN

CID	Service	Resource	Title
50356	VM Scale Set	VM Scale Set	Ensure use of NSG with Azure Virtual Machine Scale Set
50357	Network Watcher	Network Watcher Flow Log	Ensure flow logging is enabled for Azure Network Watcher via Azure Network Watcher Flow Log
50358	Azure Container Registry	Azure Container Registry	Ensure that admin user is disabled for Azure Container Registry
50359	Log Analytics Workspace	Log Analytics Workspace	Ensure queries are not supported over the public internet for Azure Log Analytics Workspace
50360	Load Balancer	Load Balancer	Ensure that standard sku is used to enforce TLS for Azure Load Balancer
50361	VM Scale Set	VM Scale Set	Ensure overprovisioning is disabled for Azure Windows Virtual Machine Scale Set
50362	Log Analytics Workspace	Log Analytics Workspace	Ensure log analytics workspace has daily quota value set for Azure Log Analytics Workspace
50363	Network Watcher	Network Watcher Flow Log	Ensure that traffic analytics is enabled via Azure Network Watcher Flow Log
50365	Application Gateway	Application Gateway	Ensure end-to-end TLS is enabled to encrypt and securely transmit sensitive data to the backend for Azure Application Gateway
50366	Azure CDN	Azure CDN Endpoint	Ensure HTTP is disallowed for Azure CDN Endpoint
50367	Eventhub	Eventhub Namespace	Ensure auto inflate is enabled for Azure Eventhub Namespace
50368	Azure Analysis Services	Azure Analysis Services Server	Ensure data backup is enabled using "blob container uri" for Azure Analysis Services Servers
50369	Azure CDN	Azure CDN Endpoint	Ensure compression is enabled for Azure CDN Endpoint
50370	Azure Analysis Services	Azure Analysis Services Server	Ensure Power BI analysis services are defined for Azure Analysis Services Server

Common Feature

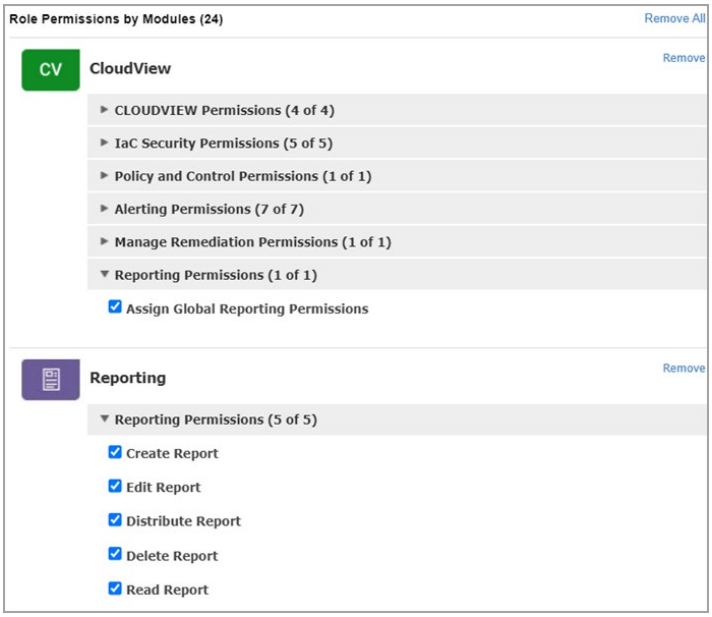
Reporting Permission

We have added new permission – Assign Global Reporting Permissions to provide users the permissions to create, read, edit, and delete reports in CloudView. By default, the Manager users have the global reporting permissions and CloudView reporting permissions.

All existing sub-users with the write permissions to CloudView will have the new reporting permissions enabled. All existing sub-users with read-only permissions do not have the reporting permissions.

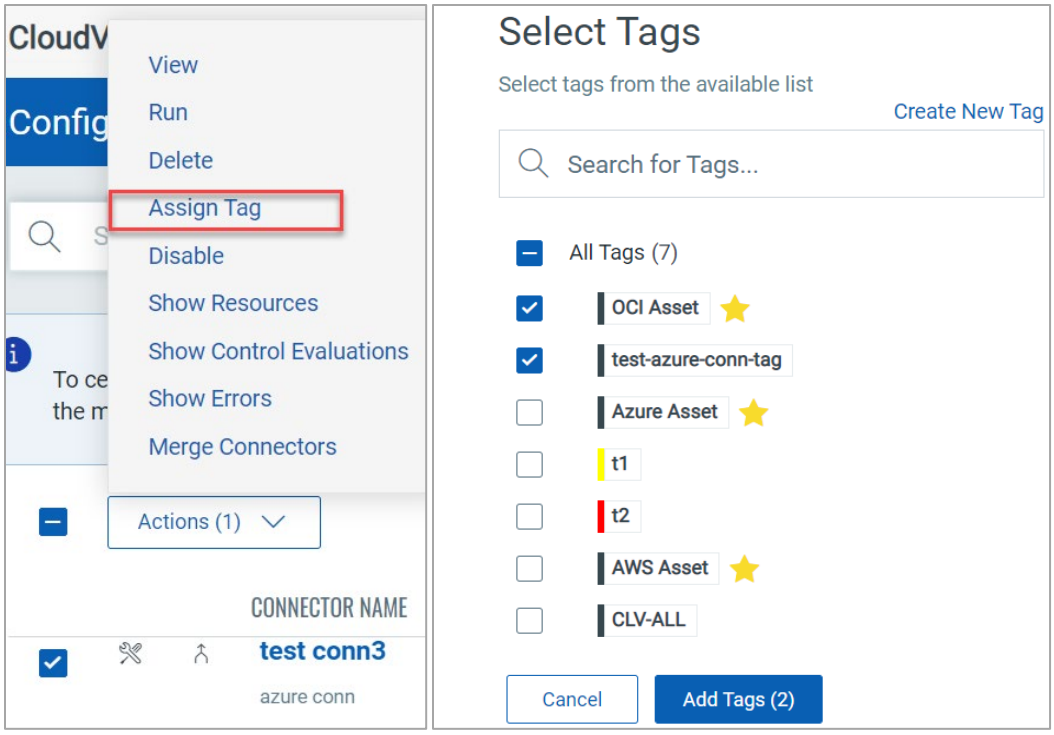
We have provided a new pre-defined role 'CloudView - only Reports' which has the 'Assign Global Reporting Permissions' enabled. You can assign this role to any sub-user to provide access to CloudView reports.

The manager user can choose to enable or disable the reporting access to CloudView reports for sub-users For a sub-user to be able to perform reporting actions, a user with the Manager role needs to assign the permission to the sub-users from the Administration utility.



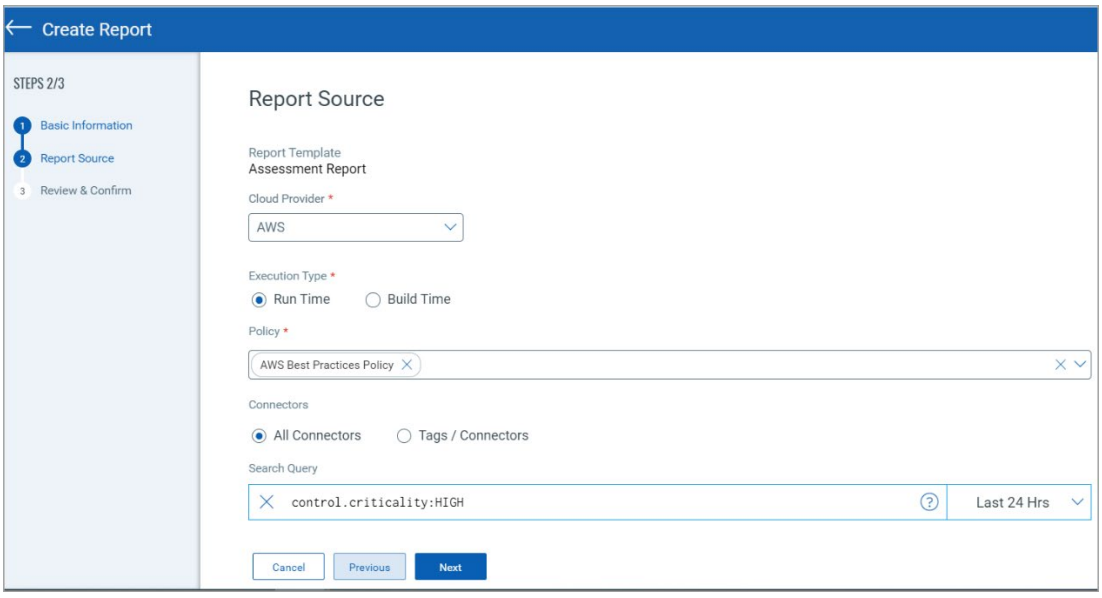
Tag-based Access Configuration

With the introduction of the Connector app, all the CloudView groups that were assigned to CloudView connectors are migrated to Qualys tags with the prefix 'CLV-'. Connector groups that were not assigned to any connectors are not migrated. You can control access to connectors by assigning tags.



Previous configurations involving groups are now replaced with tags.

For example, in Assessment Report, the Report Source allows users to choose connectors from 'All connectors' or 'Tags/Connectors'.

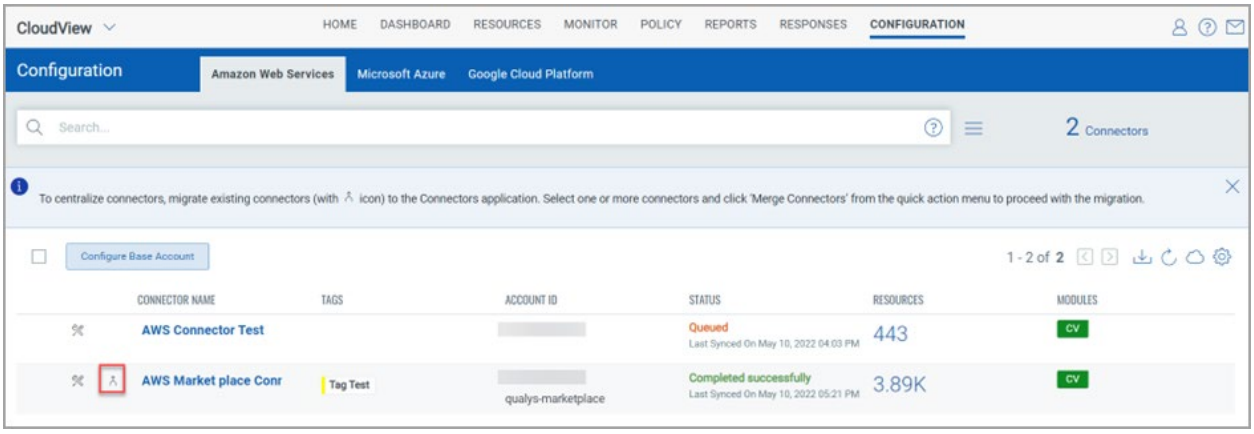


With the removal of Groups, we will also have removed the Access Management tab from CloudView Configuration. Now user access management can be done by assigning the necessary tags to connectors/users.

Connector Configuration

We have launched one centralized application – Connector, to create connectors for AssetView and CloudView. Thus, connector creation can only be done through the Connector app.

The changes to the CloudView connector configuration will not be allowed until you merge the CloudView connectors to the Connectors application. You are requested to merge CloudView connectors to the Connectors application by using the merge feature.



Select the connectors with the icon to merge them with the Connector app. After merging the connectors from CloudView, you can update the connectors in the Connectors application.

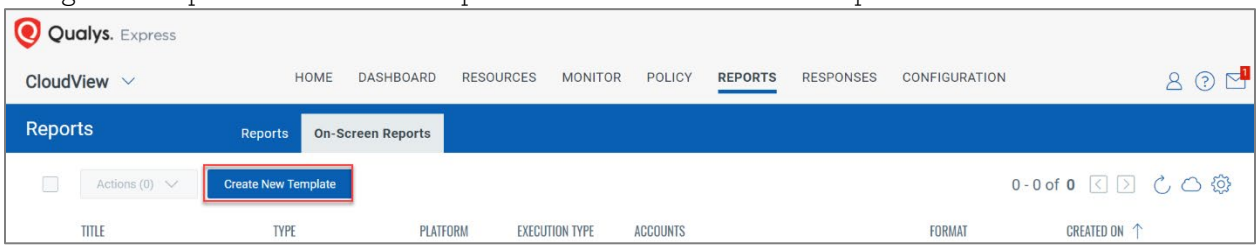
For merged connectors, tags can be assigned from the Connectors app. For unmerged connectors, tags can be assigned from the CloudView CONFIGURATION tab.

For details, refer to the Configure Connectors topic in the CloudView online help.

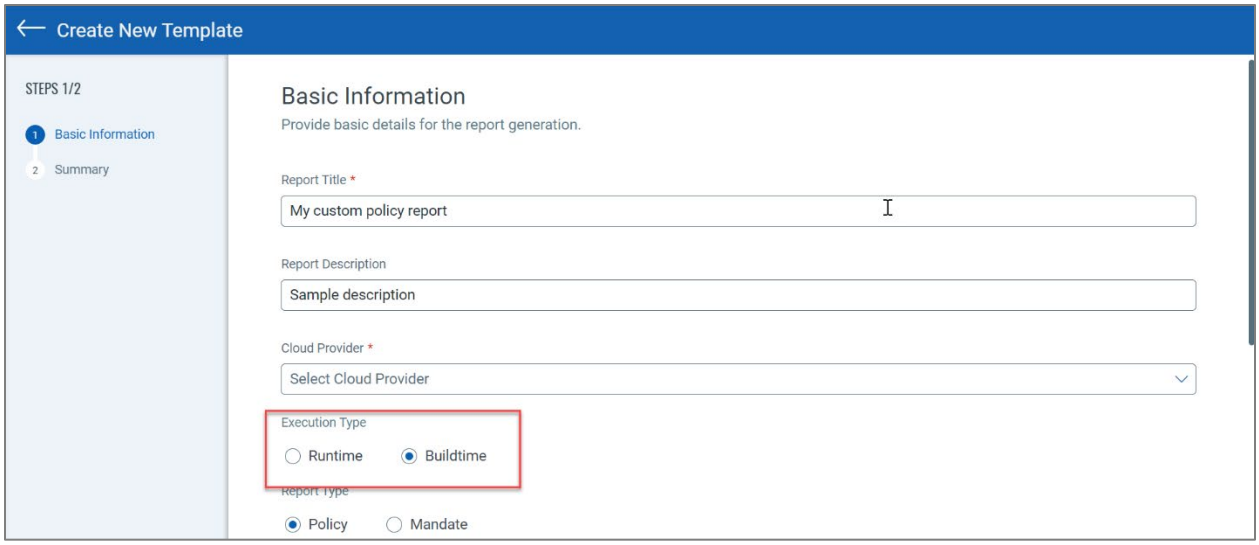
Build-Time Report Creation

CloudView has now introduced the option for users to generate On-Screen reports for build-time controls. A new parameter called "Execution Type" is introduced with two values ‘Runtime’ and ’Buildtime’ for users to choose from.

Navigate to Reports-> On-Screen Reports-> Click ‘Create New Template’



Select ‘Buildtime’ from the Basic Information page.



New Tokens

We have introduced the following new tokens for tags that are created as alternatives for groups. These tags can be found in the Resource tab

- tags.name: Use values within quotes to help you find connectors with the specified tag name.
- tag.key: Use a text value to define the key of an AWS or Azure tag assigned to the resource (case sensitive).
- tag.value: Use a text value to define the value of an AWS or Azure tag assigned to the resource (case sensitive).

These tags can be found in the Monitor tab

- mandate.name: Use the name of mandate policy to view controls that belong to the specified mandate policy.
- mandate.publisher: Use the name of mandate publisher to view controls that belong to the specified mandate policy.

Issues addressed in this release

- We have now fixed an issue where all the CloudView connector was picking up false information about port range for inbound and outbound rules of Security Groups.
- We fixed an issue where control CID 2 was failing and ID was displayed as non-compliant despite entering the correct credentials.
  We have rectified an issue where the queries for Azure VM status returned incorrect results.