![Qualys logo]

Qualys CloudView v2.x
Release Notes

Version 2.3.0
May 20, 2023

What's new?

Microsoft Azure

New Controls

Control Check Modified

Migrated Controls from Azure Best Practices to CIS Microsoft Azure Foundation Benchmark

Deprecated Controls

Common Features

Exception Management

Updated Tokens

Qualys CloudView 2.3.0 brings you improvements and updates! Learn More!

Microsoft Azure

New Controls
We have introduced the following controls for CIS Microsoft Azure Foundations Benchmark.

CID	Title	Service	Resource
50455	Ensure Storage logging is enabled for Blob service for read, write and delete requests	STORAGE ACCOUNT	STORAGE ACCOUNT
50456	Ensure Storage logging is enabled for Table service for read, write and delete requests	STORAGE ACCOUNT	STORAGE ACCOUNT
50439	Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults	KEY VAULT	SECRET

Control Check Modified
We have updated the following control check for CIS Microsoft Azure Foundations Benchmark.

CID	Title	Service	Resource
50030	Ensure that the Expiration Date is set for all Secrets in Non RBAC Key Vaults	KEY VAULT	SECRET
50091	Ensure that Azure AKS cluster HTTP application routing is disabled	KUBERNETES CLUSTER	KUBERNETES CLUSTER

Migrated Control from Azure Best Practices to CIS Microsoft Azure Foundation Benchmark

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

CID	Title	Service	Resource
50030	Ensure that the Expiration Date is set for all Secrets in Non RBAC Key Vaults	KEY VAULT	SECRET

Deprecated Controls

We have deprecated the following Azure controls because of behaviour changes from Azure side.

| CID	Title	Service	Resource
50083	Ensure that Vulnerability Assessment Setting Also send email notifications to admins and subscription owners is set to On for SQL Server	AZURE_SQL	SQL_SERVER
50313	Ensure that Vulnerability Assessment (VA) is enabled on a SQL server by setting a Storage Account	AZURE_SQL	SQL_SERVER
50314	Ensure that Vulnerability Assessment setting Periodic recurring scans is set to on for SQL server	AZURE_SQL	SQL_SERVER
50315	Ensure that the Vulnerability Assessment setting Send scan reports to is configured for a SQL server	AZURE_SQL	SQL_SERVER

Common Features

Exception Management

We have introduced an option to create exceptions from the **Exceptions** tab of CloudView. You can continue to create exceptions through failed controls but now, you can also leverage the new **Create Exception** action to create exceptions for resources, connectors, and Qualys Tags of your choice. With Qualys Tags, you can create exceptions for multiple evaluations together.

You can find the new create exception option under **Policy** -> **Exceptions** -> **New.**
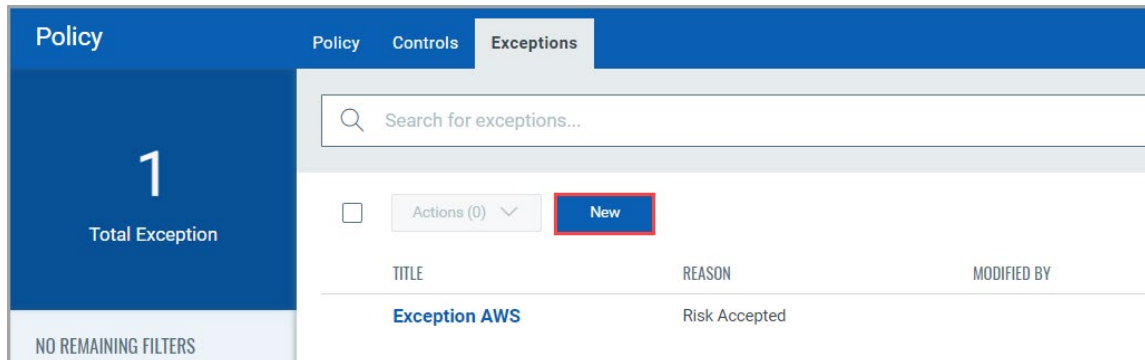
Provide Exception scope information for the new exception.
- Connector scope – The exception is associated with the selected connector and its control Ids.
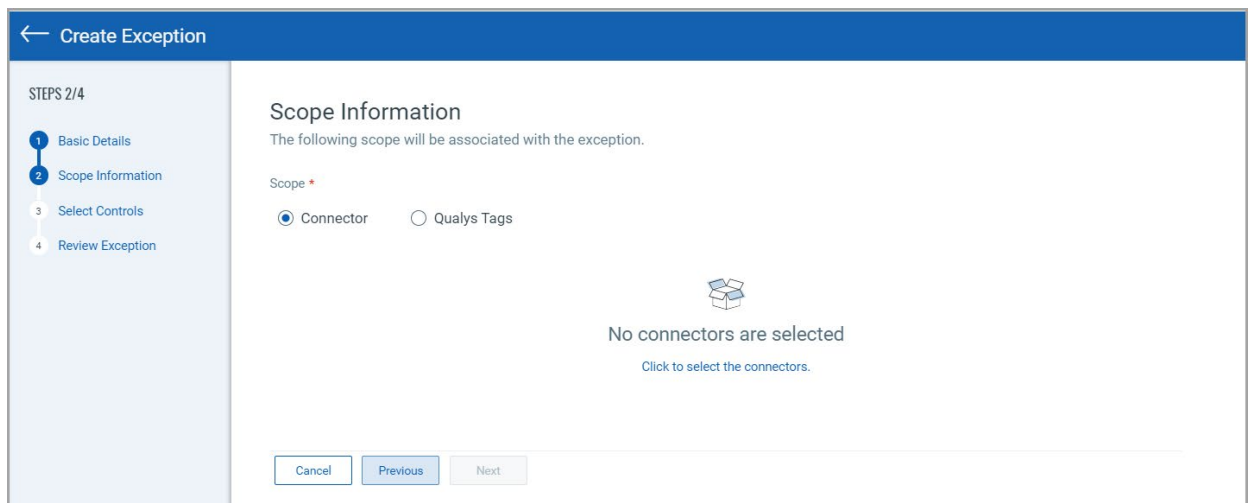
- QualysTags – The exception is associated with the selected Resource Tags and its controlIds.

NOTE: When selecting QualysTags, choose resource tags applied through the Exception Management APIs. Do not select connector tags. Refer to the CloudView API guide for more information on Exception Management APIs.

Refer to the CloudView Online Help for detailed instructions.

Updated Tokens
We have introduced a token to other tabs in CloudView and added new scope to an existing token.

tags.name: Use values within quotes or backticks to help you find the resources and evaluations with the specified tag you want.

This token can now be found in Monitor, Report, and Dashboard.

exception.scope: Select the scope of exception (CONNECTOR, RESOURCE, QUALYSTAG). Select scope from the drop-down options.

This token has an additional scope, QUALYSTAG, to find the exceptions created through QUALYSTAG scope.

Issues Addressed

-We fixed an issue where CID 50091 was not evaluating properly due to a missing field in the response.

-We have optimized the connector creation logic to prevent time-outs from Connectors application when creating new connectors.

- We have fixed an issue where connectors selected for custom policies were not displaying in the edit policy page.

- We have fixed an issue where control evaluations took too long to produce results.

- We have fixed an issue where the customer could not find the accurate count of Lambda functions in CloudView resources.