



Qualys CloudView v1.x

Version 1.13.0

December 15, 2020

Here's what's new in Qualys CloudView 1.13.0!

Amazon Web Services

[New Controls for CIS Amazon Web Services Foundations Benchmark Control Migrated for AWS](#)

Google Cloud Platform

[GCP Control Updates](#)

Common Feature

[Exceptions For Failed Control Evaluations](#)

Qualys CloudView 1.13 brings you many more improvements and updates! [Learn more](#)

Amazon Web Services

New Controls for CIS Amazon Web Services Foundations Benchmark

We have added the following 3 new controls to CIS Amazon Web Services Foundations Benchmark.

CID	Resource	Service	Control Title
160	IAM Access analyzer	IAM	Ensure that IAM Access analyzer is enabled
175	IAM Users	IAM	Ensure no Inline Policies are attached to IAM Users directly
176	IAM Users	IAM	Ensure no Managed Policies are attached to IAM Users directly

Control Migrated for AWS

We have migrated the following control from AWS Best Practices Policy to CIS Amazon Web Services Foundations Benchmark.

Old Policy: AWS Best Practices Policy

New Policy: CIS Amazon Web Services Foundations Benchmark

CID	Resource	Service	Control Title
68	IAM Server Certificate	IAM	Ensure all the expired SSL/TLS certificates stored in AWS IAM are removed

Google Cloud Platform

GCP Control Updates

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

CID	Service	Resource	Title	Sections Updated
52029	Compute Engine	VM Disk	Ensure VM disks for critical VMs are encrypted with Customer-Supplied Encryption Keys (CSEK)	Updated control logic to filter GKE node disk
52098	BigQuery	Dataset	Ensure that BigQuery datasets are not anonymously or publicly accessible	Updated control logic

Common Feature

Exceptions For Failed Control Evaluations

We have now introduced Exceptions that allow you to exempt resources that have failed controls evaluations. You may want to create exceptions to exempt certain cloud resources from a particular control or temporarily change the status of a resource for a particular control from Fail to PassE (Pass with Exception).

For example, it may be the policy in an organization that the a particular cloud resource is not allowed on any server or port. However, there could be a business need for the organization to provide an exception for one or more resources on a temporary basis. This may be required to support a custom application or other business need. You could use exceptions in such scenarios.

Create Exception

Go to Monitor tab and select the failed resource for which you want to create an exception and select Create Exception from the quick actions menu.

Note: The Create Exception option is available in the quick action menu only for resources with failed control evaluations (FAIL).

The screenshot shows the 'Create Exception' form in the Qualys CloudView interface. The form is titled 'Basic Details' and includes the following fields and options:

- Exception Name ***: A text input field containing 'Sample Exception'.
- Reason ***: Radio button options for 'False Positive' (selected), 'Risk Accepted', and 'Other'.
- Explanation ***: A text area containing 'Sample explanation' with a character count of 232/250.
- Exception Start Date ***: A date picker showing '12/02/2020'.
- Exception End Date ***: A date picker showing '12/03/2020'.
- Information Security Policy**: A text area with the placeholder 'Please provide additional explanation for tracking purpose' and a character count of 250/250.
- Information Security Procedure**: A text area with the placeholder 'Please provide additional explanation for tracking purpose' and a character count of 250/250.

At the bottom of the form, there are 'Cancel' and 'Next' buttons.

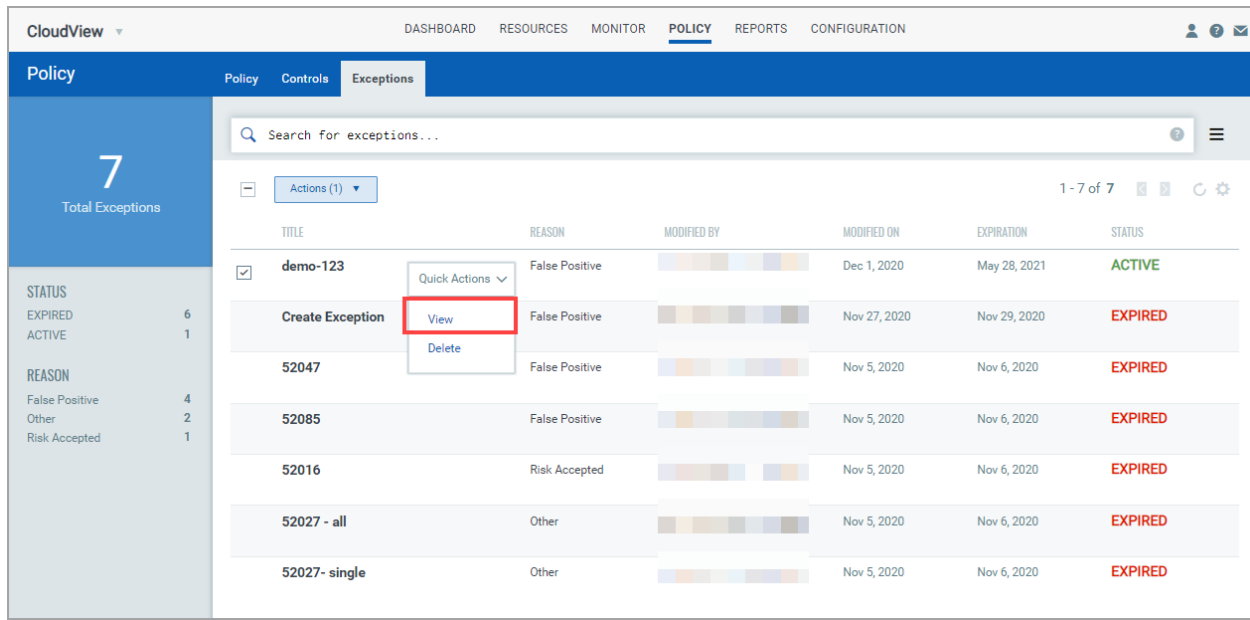
Simply follow the exception creation steps, provide the required details for the exception and click Create Exception.

That's it! The exception is created.

You can edit exceptions when they are in active status. You cannot edit exceptions that are expired.

Note: You can associate maximum 200 resources with an exception during creation.

You can view all the exceptions you create in Exceptions tab that we have newly introduced. Go to Policy > Exceptions to see exceptions.



Select View from the quick actions menu to view complete details and history log for the exception. All actions are logged in the exception history with the name of the user who performed the action and a time stamp for when the action took place.

New Search Tokens

We have introduced the following new search tokens to simplify your search related to exceptions.

The following tokens are available on Exceptions tab (Policy > Exceptions).

- exception.provider
- exception.reason
- exception.status
- exception.name
- resource.result (only on Monitor Tab)

You could use the new token on Monitor tab to view resources as per evaluations results.

Sort and Filter Connector List Using APIs

We have now introduced new parameters for Get Connectors APIs to simplify connector search results by supporting sorting or filtering connectors. For detailed information, refer to [CloudView 1.13 API Release Notes](#).

Issue addressed in this release

- We have now fixed the "elb.dnsName" search token so that the search results provide accurate results.