



Qualys CloudView v1.x

Version 1.16.0

June 15, 2021

Here's what's new in Qualys CloudView 1.16.0!

Google Cloud Platform

[Control Update](#)

Common Feature

[Remediating Control Misconfigurations](#)

[API Features and Enhancements](#)

Google Cloud Platform

Control Update

We have updated the control logic/title for CID 52055 to accommodate the latest deprecated/decommissioned runtime version.

CID 52055

Title: Ensure that Runtime used in cloud function is not deprecated or decommissioned

Service Type: Cloud Function

Resource Type: Cloud Function

Common Feature

Remediating Control Misconfigurations

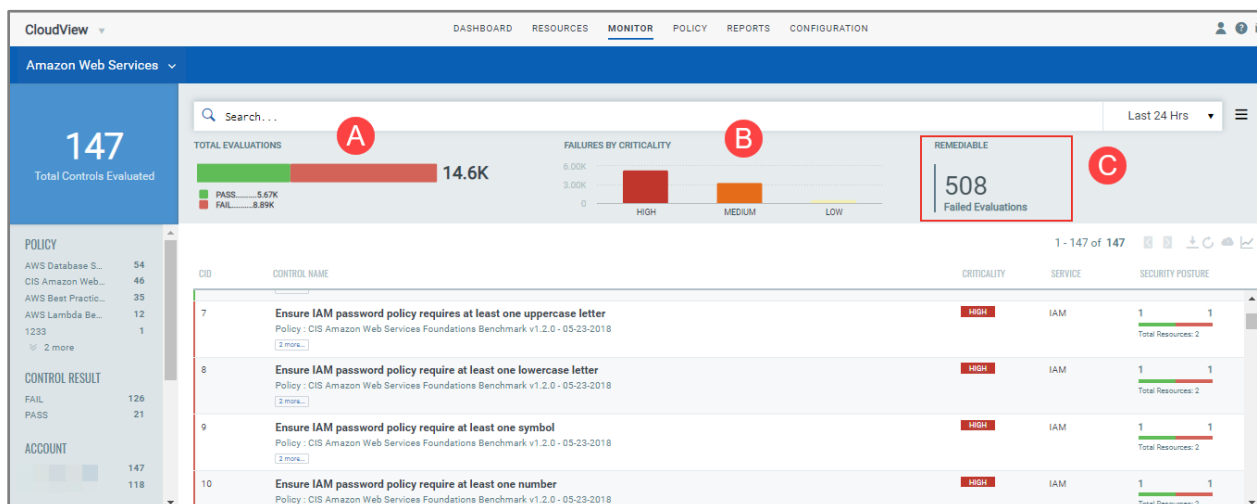
We are now introducing a new capability that allows you to remediate a control misconfiguration on a resource as well as a bulk of resources in a single click. As a result, this will simplify remediation of control misconfigurations and you will be able to quickly improve your compliance score.

Remediation allows you to select the resources you want to remediate and launch a remediation action that configures the required setting on your behalf.

Note: The remediation feature is available only to Cloud Security Assessment (CSA) subscribers and is enabled by default.


Single-Click Remediation

CSA provides you information on control misconfigurations. You can now remediate resource misconfigurations on multiple resources with single click.



To remediate the control misconfiguration, navigate to the Monitor tab. We have introduced widget cards on Monitor tab that provide total evaluations, failures by criticality, and the count of failed evaluations that can be fixed through remediation.



The “” icon indicates that these controls are available for remediation. For complete list of controls that are supported for remediation, refer to Remediable Control List topic in the CloudView online help.

Click on one of the controls to proceed with Remediation. Let us consider an example of CID 60.

RESOURCE	ACCOUNT ID	EVALUATED ON	RESULT	EVIDENCE	REMEDIATION
cf-templates-sr1r6kom4714-us-east-2	[REDACTED]	2 hours ago	FAIL	Evidence	Remediate Now
cf-templates-sr1r6kom4714-us-west-2	[REDACTED]	2 hours ago	FAIL	Evidence	Remediate Now
loadbalancertestcv-dev	[REDACTED]	2 hours ago	FAIL	Evidence	Remediate Now
conffilesdb	[REDACTED]	2 hours ago	FAIL	Evidence	Remediate Now

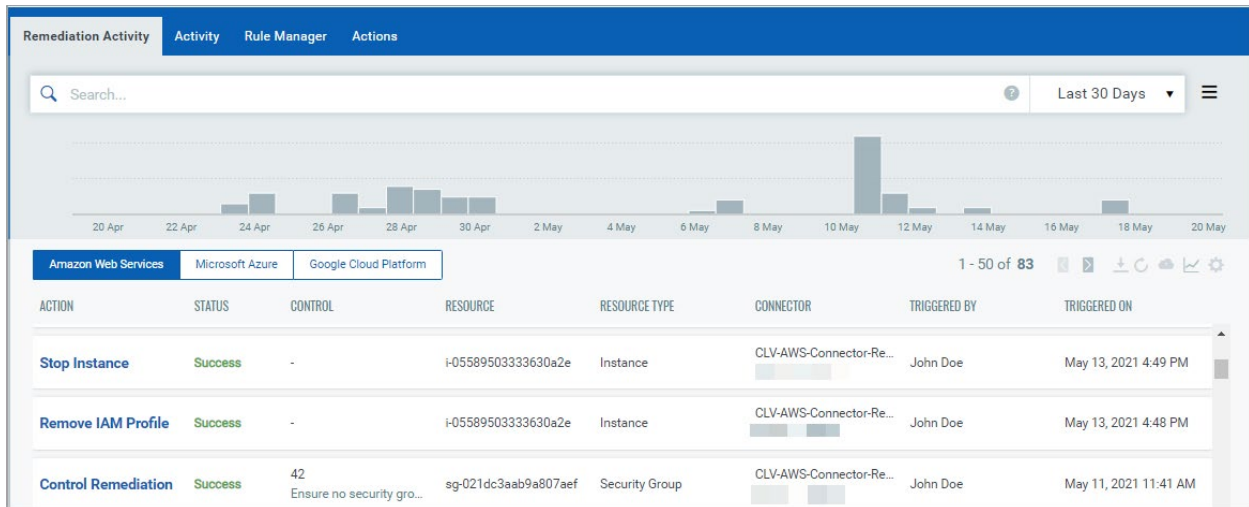
Click **Remediate Now** to trigger remediation process. The detailed steps are listed in the CloudView Online Help. All the remediation activities that you trigger are listed in Responses > Remediation Activity tab.

Remediation Activity

You can view the all the remediation activities that are triggered in your Qualys account for all the 3 cloud providers.

Note: Before you trigger remediation for resource, ensure you have the necessary permissions needed for every cloud provider. The permission related details are listed in CloudView online help.

Go to Responses > Remediation Activity. Activities for every cloud are listed under the respective sub tabs.



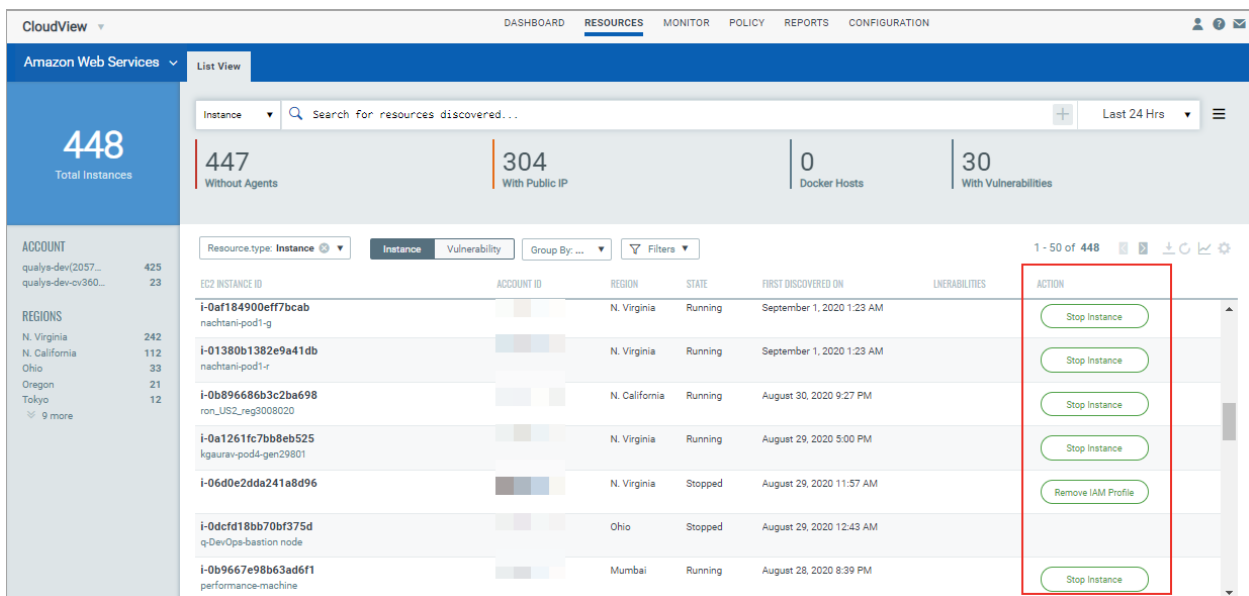
You could use filters listed in the left pane or form search queries using the search tokens supported by Qualys Query Language (QQL) to filter the activities. To view the complete list of search tokens supported for Remediation Activity, refer to “Search for Remediation Activity” topic of the Cloudview online help.

Actions for AWS Instances

We provide actions that you can execute on compromised instance from accessing AWS services and stopping it to quarantine it. These actions typically can be used as first level of response in the following use cases:

- Stopping an instance that is created in a AWS region, which is not used in your organization.
- Stopping an instance as a first level of response to AWS Abuse Alerts.
- Removing an IAM Profile, associated with instances having critical vulnerability to ensure access to AWS services is blocked.

We support the following actions for AWS instance resources.



Stop Instance

You can use the Stop Instance action as an immediate response on a newly detected unknown instance. You can initiate the actions on such instances from Resources tab.

For example, if you operate only in Mumbai region, but instances are detected in North Carolina region (where you do not operate). In such cases, the first response action towards such unknown instance would be to stop the instance and then troubleshoot it.

Remove IAM Profile:

The Remove IAM profile action allows you disassociate an IAM profile from the instance. You can initiate the actions on such instances from Resources tab.

For example, if you have special IAM roles for specific purposes or intended for specific instances. You discover an instance is using the IAM role (not applicable for that instance). In such cases, the first response action towards such instance would be to remove the IAM profile and then troubleshoot it.

API Features and Enhancements

We have introduced API changes for Remediation Activity. For detailed information, refer to [CloudView 1.16 API Release Notes](#).