



Qualys CloudView v1.x

Version 1.25

August 24, 2022

Here's what's new in Qualys CloudView 1.25!

Amazon Web Services

[New Controls for AWS Database Best Practices Policy](#)
[New Controls for AWS Best Practices Policy](#)

Microsoft Azure

[New Controls for Azure Best Practices Policy](#)
[Launching Azure User Defined Control with QFlow](#)

Qualys CloudView 1.25 brings you many more improvements and updates! [Learn more](#)

Amazon Web Services

New Controls for AWS Database Best Practices Policy

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

CID	Service	Resource	Title
507	DocumentDB	DocumentDB	Ensure encryption at rest is enabled for AWS DocumentDB clusters
512	Neptune	Neptune	Ensure storage encryption is enabled for AWS Neptune cluster

New Controls for AWS Best Practices Policy

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

CID	Service	Resource	Title
463	System Manager	System Manager	Ensure session logs for system manager are stored in only Encrypted Cloudwatch log groups or S3 Buckets
466	ECS	ECS	Ensure transit encryption is enabled for EFS volumes in AWS ECS Task Definition
472	SageMaker	SageMaker	Ensure ML storage volume attached to training jobs are encrypted with customer managed master key
477	SageMaker	SageMaker	Ensure ML storage volume attached to Hyperparameter Tuning jobs (if configured) are encrypted with customer managed master key
497	Elasticsearch	Elasticsearch	Ensure KMS customer managed keys are used for encryption for AWS ElasticSearch Domains
517	KMS	KMS	Ensure customer master key (CMK) is not disabled for AWS Key Management Service (KMS)
529	Launch Configuration	Launch Configuration	Ensure detailed monitoring is enabled for AWS Launch Configuration

Microsoft Azure

New Controls for Azure Best Practices Policy

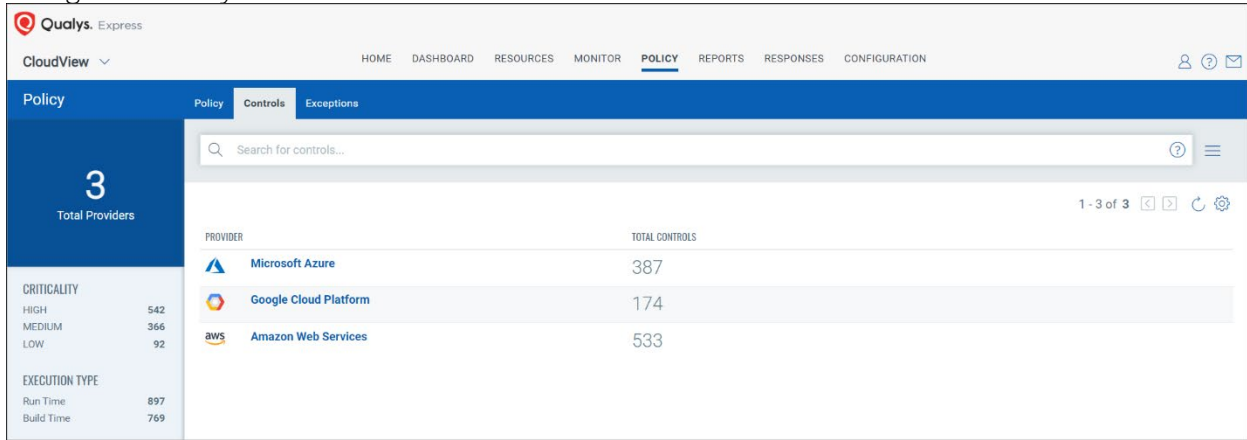
We have introduced the following new controls for Azure Best Practices Policy.

CID	Service	Resource	Title
50372	Access Control	Access Control	Ensure that a resource locking administrator role is available for each Azure subscription.

Launching Azure User Defined Control with QFlow

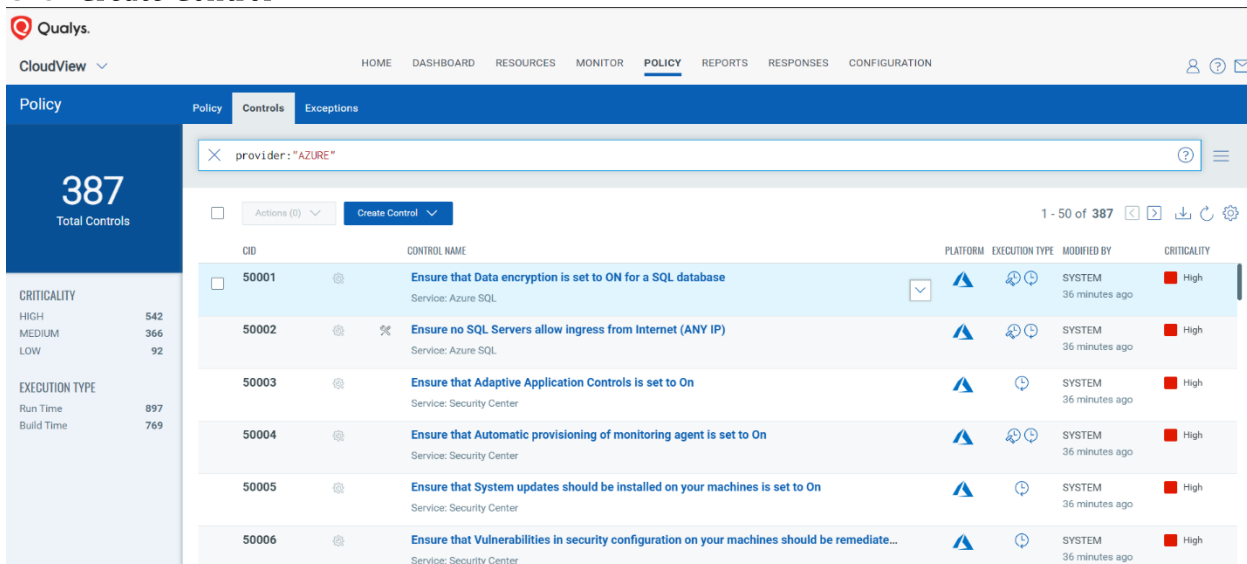
You can create your own Azure custom control and associate it to a custom policy to be evaluated against the policy.

Navigate to Policy > Control > Click **Microsoft Azure**



PROVIDER	TOTAL CONTROLS
Microsoft Azure	387
Google Cloud Platform	174
Amazon Web Services	533

Click **Create Control**



CID	CONTROL NAME	PLATFORM	EXECUTION TYPE	MODIFIED BY	CRITICALITY
50001	Ensure that Data encryption is set to ON for a SQL database Service: Azure SQL		SYSTEM	36 minutes ago	High
50002	Ensure no SQL Servers allow ingress from Internet (ANY IP) Service: Azure SQL		SYSTEM	36 minutes ago	High
50003	Ensure that Adaptive Application Controls is set to On Service: Security Center		SYSTEM	36 minutes ago	High
50004	Ensure that Automatic provisioning of monitoring agent is set to On Service: Security Center		SYSTEM	36 minutes ago	High
50005	Ensure that System updates should be installed on your machines is set to On Service: Security Center		SYSTEM	36 minutes ago	High
50006	Ensure that Vulnerabilities in security configuration on your machines should be remediate... Service: Security Center		SYSTEM	36 minutes ago	High

Provide the basic details and customize the control as you need. You can also include QFlow in the control. Select from the list of QFlows that have CloudView Nodes added in them. Associate the Azure custom control to a user-defined policy to be evaluated for the custom policy.

Issues Fixed In This Release

We fixed an issue where the CloudView UI was showing a lower number of assets than existed in the AWS environment.