Qualys CloudView v2.x

Version 2.1.0
February 03, 2023

What's new?

Common Features

Amazon Web Services

Microsoft Azure

Google Cloud Platform

Qualys CloudView 2.1.0 brings you improvements and updates! Learn More

Common Features

New Tokens

We have introduced the following new tokens for GCP labels on the Resource tab.

- label.name: Use a text value to define the name of a GCP label assigned to the resource (case sensitive).
- label.value: Use a text value to define the value of a GCP label tag assigned to the resource (case sensitive).

We have introduced the following new token to find the VM instances with Cloud Agent installed. The token can be found in the Resource tab.

- instance.agentInstalled: Use true to view the list of GCP VMs with Qualys Agent installed.

We have introduced the following new tokens to search for exceptions based on account ID (AWS), subscription ID (Azure) and project ID (GCP). These tokens can be found on the policy tab under Exceptions.

- resource.accountId: Use a text value to find exceptions for AWS resources based on the unique account ID assigned to it.
- resource.subscriptionId: Use a text value to find exceptions for Azure resources based on the unique account ID assigned to it.
- resource.projectId: Use a text value to find exceptions for GCP resources based on the unique account ID assigned to it.

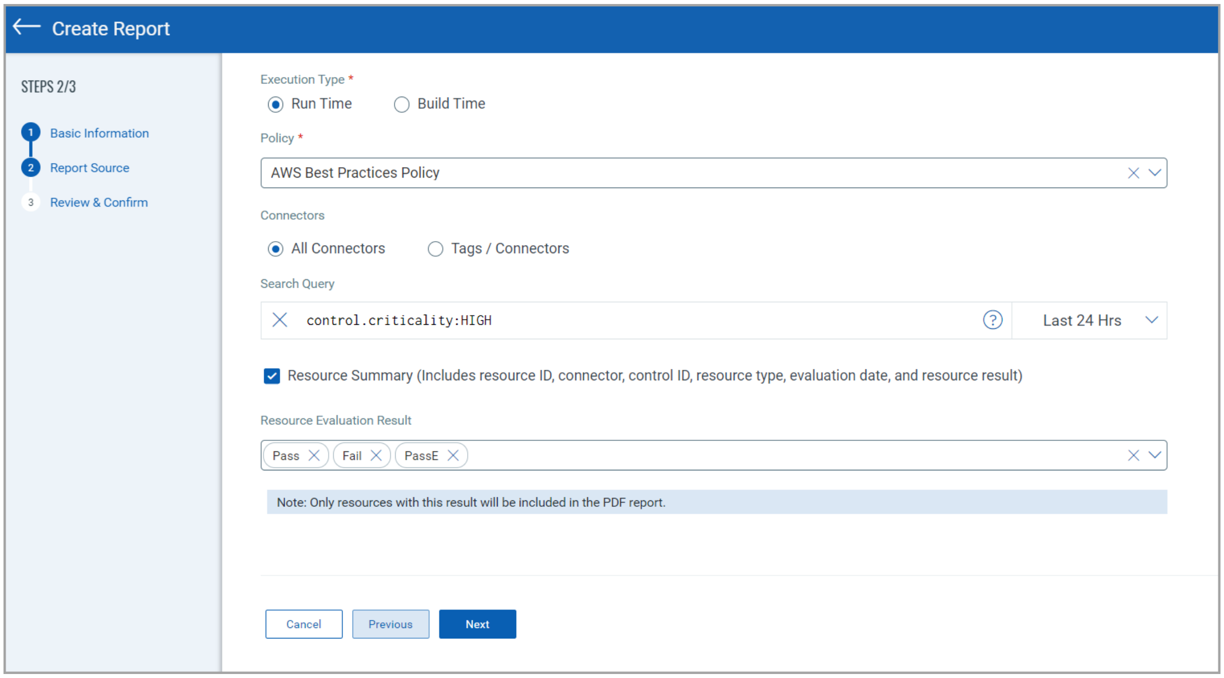
Enhanced Support for Mandates

We have now added support for a new mandate in this release.

New Mandate: New Zealand Information Security Manual (NZISM)

Introducing Support for Search Tokens in PDF Reports

We have now added support for search tokens when generating PDF assessment reports. Use search token query to filter the data you want to include in the report. For example, use the *control.criticality* search query token to find controls with a certain criticality for the report you want to generate.



Create Report

STEPS 2/3

1 Basic Information
2 Report Source
3 Review & Confirm

Execution Type *

● Run Time ○ Build Time

Policy *

AWS Best Practices Policy

Connectors

● All Connectors ○ Tags / Connectors

Search Query

```
control.criticality:HIGH
```

Last 24 Hrs

☑ Resource Summary (Includes resource ID, connector, control ID, resource type, evaluation date, and resource result)

Resource Evaluation Result

Pass Fail PassE

Note: Only resources with this result will be included in the PDF report.

Amazon Web Services

Deleted controls from AWS Best Practice:

We have deleted the following controls from Amazon Web Services.

CID	Title
513	Ensure IMDv1 is disabled for AWS EC2 instances

Microsoft Azure

New controls for CIS Microsoft Azure Foundations Benchmark

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

CID	Title	Service	Resource
50443	Ensure that 'Enable key rotation reminders' is enabled for each Storage Account (Manual)	Storage Account	Storage Account
50445	Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL Database Server (Manual)	MYSQL Server	MYSQL Server
50446	Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL Database Server (Manual)	MYSQL Server	MYSQL Server
50447	Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL Flexible Database Server	MYSQL Flexible Server	MYSQL Flexible Server
50448	Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL Flexible Database Server	MYSQL Flexible Server	MYSQL Flexible Server
50440	Ensure that private endpoints are configured for Cosmos DB (Manual)	Cosmo DB	Cosmo DB
50444	Ensure that logging for Azure Web AppService 'AppServiceHTTPLogs' is enabled. (Manual)	App Service	Web App
50449	Ensure that logging for Azure Api AppService 'AppServiceHTTPLogs' is enabled. (Manual)	App Service	API App
50437	Ensure that Activity Log Alert exists for Create or Update Public IP Address rule	Monitor	Activity Log Alert
50436	Ensure that Activity Log Alert exists for Delete Public IP Address rule	Monitor	Activity Log Alert

50438	Ensure Virtual Machines are utilizing Managed Disks (Manual)	Virtual Machines	Disks
50442	Ensure that the Expiration Date is set for all Keys in Non-RBAC Key Vaults.	Key Vaults	Keys
50441	Enable Role Based Access Control for Azure Key Vault	Key Vaults	Key Vault

Updated controls for CIS Microsoft Azure Foundations Benchmark

We have updated the following controls for CIS Microsoft Azure Foundations Benchmark.

CID	Title
50032 (Modified check)	Ensure that 'Unattached disks' are encrypted with 'Customer Managed Key' (CMK)
50218 (Modified check)	Ensure that the Expiration Date is set for all Keys in RBAC Key Vaults

Migrated controls from Azure Best Practices Policy to CIS Microsoft Azure Foundations Benchmark

We have migrated the following controls from Azure Best Practices Policy to CIS Microsoft Azure Foundations Benchmark.

CID	Title
50005	Ensure that Microsoft Defender Recommendation for Apply system updates status is Completed
50008	Ensure that Disk encryption should be applied on virtual machines is set to On
50016	Ensure that Access through Internet facing endpoint should be restricted is set to On
50036	Ensure that Resource Locks are set for Mission-Critical Azure Resources
50175	Ensure that Storage Accounts have infrastructure encryption enabled
50176	Ensure that Azure Key Vaults use Private Links
50181	Ensure Storage Accounts are using the latest version of TLS encryption
50197	Ensure that Azure Defender for DNS is enabled
50223	Ensure that Only Approved Extensions Are Installed
50226	Ensure that Azure Defender for Resource Manager is enabled

50231	Ensure that Azure Defender is set to On for SQL servers on machines
50237	Ensure that Auditing Retention is greater than 90 days for Azure MSSQL Server
50256	Ensure that Public IP addresses are Evaluated on a Periodic Basis
50343	Ensure that Auditing is Enabled for Azure SQL Server
50363	Ensure that Network Security Group Flow logs are captured and sent to Log Analytics
50059	Ensure Activity Log Alert for Delete SQL server firewall rule
50218	Ensure the Storage Account naming rules

Migrated controls from Azure Database Service Best Practices Policy to CIS Microsoft Azure Foundations Benchmark

We have migrated the following controls from Azure Database Service Best Practices Policy to CIS Microsoft Azure Foundations Benchmark.

CID	Title
50099	Ensure that Azure Cosmos DB accounts have firewall rules

Migrated controls from CIS Microsoft Azure Foundations Benchmark to Azure Database Service Best Practices Policy

We have migrated the following controls from CIS Microsoft Azure Foundations Benchmark to Azure Database Service Best Practices Policy

CID	Title
50013	Ensure that default Auditing policy for a SQL Server is configured to capture and retain the activity logs
50046	Enable RBAC within Azure Kubernetes Services
50054	Ensure that logging for Azure KeyVault is Enabled
50066	Ensure Activity Log Alert exists for Create or Update Network Security Group Rule
50067	Ensure Activity Log Alert exists for Delete Network Security Group Rule
50139	Ensure that Azure Defender is set to On for Kubernetes

Google Cloud Platform

New controls for CIS Google Cloud Platform Foundation Benchmark

We have introduced the following controls for CIS Google Cloud Platform Foundation Benchmark.

CID	Title
52177	Ensure API Keys are rotated every 90 days
52178	Ensure Cloud SQL PostgreSQL Instance IP assignment is set to private

Migrated controls from GCP Best Practices Policy to CIS Google Cloud Platform Foundation Benchmark

We have migrated the following controls from GCP Best Practices Policy to CIS Google Cloud Platform Foundation Benchmark.

CID	Title
52132	Ensure API keys are not created for a project
52172	Ensure API keys are restricted to only APIs that application needs access
52173	Ensure API keys are restricted to use by only specified Hosts and Apps61
52161	Ensure that your Dataproc clusters are encrypted using Customer-Managed Keys (CMKs)
52174	Ensure that logging is enabled for Google Cloud global load balancing backend services

Issues Fixed in This Release

- We have updated the title of CID 95 so that the evaluation description and title both refer to the same configuration.
- We have fixed an issue where the CloudView Runtime reports weren’t displaying the CIS references.
- We have fixed an issue where last synced date of member connectors were not getting updated after creation.