Qualys CloudView v1.x

Version 1.19.0

November 08, 2021

Here's what's new in Qualys CloudView 1.19.0!

Amazon Web Services

New controls for AWS Best Practices Policy
New Permissions Needed for Elastic File System, Step Functions, and API Gateway Resources

Microsoft Azure

New controls for Azure Best Practices Policy
New controls for Azure Database Service Best Practices Policy

Google Cloud Platform

New controls for CIS Google Cloud Platform Foundation Benchmark
New controls for GCP Cloud SQL Best Practices Policy
New controls for GCP Kubernetes Engine Best Practices Policy
New API Library Access for GCP Connectors

Common Feature

Update To Mandates
New Tokens Added

API Features and Enhancements

Qualys CloudView 1.19 brings you many more Improvements and updates! Learn more

Amazon Web Services

New controls for AWS Best Practices Policy

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

CID	Service	Resource	Title
197	Workspace	Workspace	Ensure to encrypt the Volumes (Root and User) with the customer managed master keys in the same account and the region
198	Workspace	VPC	Ensure workspace directory must have a vpc endpoint so that the API traffic associated with the management of workspaces stays within the vpc
230	Config	Config	Ensure to enable config for the all resources for Config Service
231	Config	Config	Ensure to enable config for the global resources like IAM for Config Service
233	Config	Config	Ensure to configure s3 buckets which contains details for the resources that Config records
232	Config	Config	Ensure to configure data retention period for the configuration items for Config Service
200	Step Function	Step Function	Ensure to log state machine's execution history to CloudWatch Logs
373	Cloudwatch	Cloudwatch Log Group	Ensure to encrypt cloudwatch log groups
313	Cloudwatch	Cloudwatch Log Group	Ensure CloudWatch Log Group has a retention period set to 7 days or greater
290	SNS	SNS Topic	Ensure SNS Topics have encryption at rest enabled
182	SNS	SNS Topic	Ensure SNS Topics do not Allow 'Everyone' to Publish
183	SNS	SNS Topic	Ensure SNS Topics do not Allow 'Everyone' to Subscribe
291	SQS	SQS Queue	Ensure SNS Queue have encryption at rest enabled

New Permissions Needed for Elastic File System, Step Functions, and API Gateway Resources

The cross-account role associated with the AWS connector needs additional permissions to fetch information about Elastic File System (EFS), Step Functions, and API Gateway resources. To fetch information about these resources in your cloud environment, you need to assign these additional permissions to the IAM role associated with the AWS connector.

You can create a new policy with the required permissions and attach the policy to the IAM role associated with the AWS connector. The detailed steps for policy creation and associating with the IAM role are listed in the CloudView online help.

Microsoft Azure Cloud Platform

New controls for Azure Best Practices Policy

We have introduced the following 35 controls for Azure Best Practices Policy.

CID	Service	Resource	Title
50037	Virtual Machine	Virtual Machine	Ensure to enable virtual machines with end-to-end encryption using encryption at host
50182	Security Center	Security Policy	Ensure that monitoring of DDoS protection at the Azure virtual network level is enabled
50183	Security Center	Security Policy	Ensure that monitoring of deprecated accounts within your Azure subscription(s) is enabled
50184	Security Center	Security Policy	Ensure that IP forwarding enablement on your Azure virtual machines (VMs) is being monitored
50185	Security Center	Security Policy	Ensure that the external accounts with write permissions are monitored using Azure Security Center
50186	Storage Account	Storage Account	Ensure that critical Azure Blob Storage data is protected from accidental deletion or modification
50187	Storage Account	Storage Account	Ensure that Diagnostic Settings for Storage Accounts are configured with Log Analytics workspace
50188	Storage Account	Storage Account	Ensure that Diagnostic Settings for Storage Blobs are configured with Log Analytics workspace
50189	Storage Account	Storage Account	Ensure that Diagnostic Settings for Storage Files are configured with Log Analytics workspace
50190	Storage Account	Storage Account	Ensure that Diagnostic Settings for Storage Queues are configured with Log Analytics workspace
50191	Storage Account	Storage Account	Ensure that Diagnostic Settings for Storage Tables are configured with Log Analytics workspace
50208	Kubernetes Service	Kubernetes Cluster	Ensure that Kubernetes Services Management API server is configured with restricted access
50254	Kubernetes Service	Kubernetes Cluster	Ensure that Azure Kubernetes Service uses disk encryption set
50210	Kubernetes Service	Kubernetes Cluster	Ensure that Kube Dashboard is disabled

CID	Service	Resource	Title
50241	Virtual Machine Scale Sets	Virtual Machine Scale Set	Ensure that Virtual Machine Scale Sets have encryption at host enabled
50198	Storage Account	Storage Account	Ensure that Storage Accounts use private link connections
50202	App Service	API App	Ensure that FTPS is enforced in API Apps
50203	App Service	API App	Ensure that Managed Identity is used in API Apps
50204	App Service	API App	Ensure that API Apps are only accessible over HTTPS
50205	App Service	API App	Ensure that API Apps have Incoming Client Certificates is set to On
50206	App Service	API App	Ensure that HTTP Logging is enabled in API Apps
50058	App Service	API App	Ensure that Detailed Error Logging is enabled in API Apps
50097	App Service	API App	Ensure that Request Tracing is enabled in API Apps
50255	Network Interface	Network Interface	Ensure that IP forwarding is disabled for Network Interfaces
50248	API Management Services	API Management Service	Ensure that API Management services use virtual networks
50101	Integration Service Environments	Integration Service Environment	Ensure that Logic Apps Integration Service Environments are encrypted with customer-managed keys
50260	Cognitive Services	Cognitive Service	Ensure that public network access is disabled for Cognitive Services accounts
50114	Cognitive Services	Cognitive Service	Ensure that network access is restricted in Cognitive Services accounts
50194	Event Grid Topics	Event Grid Topic	Ensure that Azure Event Grid topics use private links

CID	Service	Resource	Title
50195	Azure Cache for Redis	Redis Cache	Ensure that Azure Cache for Redis resides within virtual network
50257	Azure Front Door	Front Door	Ensure that Web Application Firewall (WAF) is enabled in Azure Front Door Services
50242	Container Instances	Container Group	Ensure that Azure Container Instance container groups are deployed in a virtual network
50224	Azure Synapse Analytics	Synapse Workspace	Ensure that managed virtual network is enabled in Azure Synapse workspaces
50196	Virtual Machine Scale Sets	Virtual Machine Scale Set	Ensure that Diagnostic logs are enabled in Virtual Machine Scale Sets
50197	Security Center	Security Policy	Ensure that Azure Defender for DNS is enabled
50226	Security Center	Security Policy	Ensure that Azure Defender for Resource Manager is enabled
50277	App Service	Logic App	Ensure that Diagnostic logs are enabled in Logic Apps
50274	Data Lake Analytics	Data Lake Analytics	Ensure that Diagnostic logs are enabled in Data Lake Analytics accounts
50275	Data Lake Storage	Data Lake Storage	Ensure that Diagnostic logs are enabled in Azure Data Lake Storage accounts
50276	Cognitive Search	Cognitive Search	Ensure that Diagnostic logs are enabled in Search Services
50253	Key Vault	Secret	Ensure that Key Vault Secrets have 'Content-Type' set
50251	Key Vault	Key	Ensure that Key Vault keys are backed by HSM
50250	Key Vault	Key Vault	Ensure that Firewall is enabled on Key Vaults

New controls for Azure Database Service Best Practices Policy

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

CID	Service	Resource	Title
50177	PostgreSQL server	PostgreSQL server	Ensure that encryption with customer-managed key is enabled in PostgreSQL servers
50178	Azure SQL	SQL Server	Ensure that public network access is disabled on Azure SQL databases
50179	MySQL server	MySQL server	Ensure that public network access is disabled for MySQL flexible servers
50180	PostgreSQL server	PostgreSQL server	Ensure that public network access is disabled for PostgreSQL flexible servers
50099	Cosmos DB	Cosmos DB	Ensure that Azure Cosmos DB accounts have firewall rules
50243	Cosmos DB	Cosmos DB	Ensure that Cosmos DB accounts have customer-managed keys to encrypt data at rest
50100	Azure SQL	SQL Server	Ensure that Azure SQL Database have private endpoint connections enabled
50268	MySQL server	MySQL server	Ensure that encryption with customer-managed key is enabled in MySQL Servers

Google Cloud Platform

New controls for CIS Google Cloud Platform Foundation Benchmark

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

CID	Service	Resource	Title
52148	Cloud SQL	SQL Server	Ensure 'user connections' database flag for Cloud SQL SQL Server instance is set as appropriate

New controls for GCP Cloud SQL Best Practices Policy

We have introduced the following control for GCP Cloud SQL Best Practices Policy.

CID	Service	Resource	Title
52121	Cloud SQL	MySQL	Ensure that production MySQL database instances are configured to automatically fail over to another zone within the selected cloud region.
52152	Cloud SQL	PostgreSQL	Ensure that production PostgreSQL database instances are configured to automatically fail over to another zone within the selected cloud region.
52153	Cloud SQL	SQL Server	Ensure that production SQL Server database instances are configured to automatically fail over to another zone within the selected cloud region.
52122	Cloud SQL	MySQL	Ensure that MySQL database servers are using the latest major version of MySQL database.
52128	Cloud SQL	PostgreSQL	Ensure that PostgreSQL database instances have the appropriate configuration set for the "max_connections" flag.
52146	Cloud SQL	MySQL	Ensure that MySQL instances are encrypted with Customer-Managed Keys (CMKs).
52154	Cloud SQL	PostgreSQL	Ensure that PostgreSQL instances are encrypted with Customer-Managed Keys (CMKs).
52155	Cloud SQL	SQL Server	Ensure that SQL Server instances are encrypted with Customer-Managed Keys (CMKs).
52149	Cloud SQL	PostgreSQL	Ensure that Cloud SQL PostgreSQL instance server certificates are rotated (renewed) before their expiration.
52150	Cloud SQL	MySQL	Ensure that Cloud SQL MySQL instance server certificates are rotated (renewed) before their expiration.
52151	Cloud SQL	SQL Server	Ensure that Cloud SQL - SQL Server instance certificates are rotated (renewed) before their expiration

New controls for GCP Kubernetes Engine Best Practices Policy

We have introduced the following control for GCP Kubernetes Engine Best Practices Policy.

CID	Service	Resource	Title
52129	Kubernetes Engine	Kubernetes Cluster	Ensure that your GKE clusters nodes are shielded to protect against impersonation attacks.
52130	Kubernetes Engine	Kubernetes Node Pool	Ensure that Integrity Monitoring is enabled for your Google Kubernetes Engine (GKE) cluster nodes.
52142	Kubernetes Engine	Kubernetes Node Pool	Ensure that the Secure Boot feature is enabled for your Google Kubernetes Engine (GKE) cluster nodes.
52131	Kubernetes Engine	Kubernetes Node Pool	Ensure that Google Kubernetes Engine (GKE) clusters have sandbox enabled
52079	Kubernetes Engine	Kubernetes Cluster	Ensure that Google Kubernetes Engine (GKE) clusters have workload identity enabled
52147	Kubernetes Engine	Kubernetes Cluster	Ensure Image Vulnerability Scanning using GCR Container Analysis or a third-party provider
52143	Kubernetes Engine	Kubernetes Node Pool	Ensure the GKE Metadata Server is Enabled

New API Library Access for GCP Connectors

The new controls we have introduced in 1.19 need additional API access enabled for the service account associated with the GCP connector. You need to enable Service Usage API from the API library for the new controls to be executed.

Common Feature

Update To Mandates

We have introduced new mandates, upgraded version for few mandates and changed name for few mandates. All the details related to mandate updates are listed below.

Introduction on New Mandates

Sr. No.	Mandate Name	Version
1	NIST 800-53 (Special Publication)	Rev 5

Mandates with Version Upgrades

Sr. No.	Mandate Name	Current Version	New Version
1	NIST Special Publication 800-171	Ver 1.0	Rev. 2
2	CIS Controls Version 8	Ver 7.1	Ver 8
3	Criminal Justice Information Services (CJIS) Security Policy	Ver. 5.8	Ver. 5.9
4	Payment Card Industry Data Security Standard (PCI-DSS) v3.2.1	Ver 3.2	Ver. 3.2.1
5	SWIFT Customer Security Controls Framework - Customer Security Programme v2019	Ver. 1.0	Ver. 2019
6	Federal Risk and Authorization Management Program (FedRAMP H) - High Security Baseline	Ver. 1.0	Rev. 4
7	Federal Risk and Authorization Management Program (FedRAMP M) - Moderate Security Baseline	Ver. 1.0	Rev. 4

Mandates with Name change (version is still same)

Sr No	Old Mandate Name	New Mandate Name
1	Cybersecurity Maturity Model Certification (CMMC) - Maturity Level 1 (ML1)	Cybersecurity Maturity Model Certification (CMMC) Level 1
2	Cybersecurity Maturity Model Certification (CMMC) - Maturity Level 2 (ML2)	Cybersecurity Maturity Model Certification (CMMC) Level 2
3	Cybersecurity Maturity Model Certification (CMMC) - Maturity Level 3 (ML3)	Cybersecurity Maturity Model Certification (CMMC) Level 3
4	Cybersecurity Maturity Model Certification (CMMC) - Maturity Level 4 (ML4)	Cybersecurity Maturity Model Certification (CMMC) Level 4
5	Cybersecurity Maturity Model Certification (CMMC) - Maturity Level 5 (ML5)	Cybersecurity Maturity Model Certification (CMMC) Level 5

We updated the list of mandates that we support. Here is the updated list of mandates that we support:

Name	Version
ISO/IEC 27001:2013	Edition 2013-11
Cloud Controls Matrix (CCM)	Ver 3.0.1
NERC Critical Infrastructure Protection (CIP)	Ver. 5
Health Insurance Portability and Accountability (HIPAA) Security Rule 45 CFR Parts 160/164, Subparts A/C:1996	Ver. 2 Rev. 3, 2007
ANSSI 40 Essential Measures for a Healthy Network	Ver 1.0
The Australian Signals Directorate - The Essential 8 Strategies (ASD 8)	February 2017
Reserve Bank of India (RBI) - Baseline Cyber Security and Resilience Requirements (Annex 1)	Ver 1.0 (June 2, 2016)
NESA UAE Information Assurance Standards (IAS)	Ver 1.0
APRA Prudential Practice Guide (PPG): CPG 234 - Management of Security Risk in Information and Information Technology	Ver 1.0
IRDAI Guidelines On Information and Cyber Security for Insurers	Ver 1.0
General Data Protection Regulation (GDPR)	Regulation (EU) 2016/679
Minimum Acceptable Risk Standards for Exchanges (MARS-E)	Ver. 2.0
NCSC Basic Cyber Security Controls (BCSC)	1.0 (August 2017)
IRS Publication 1075	Rev. 11-2016
NIST Cyber Security Framework (CSF)	Ver 1.1
Sarbanes-Oxley Act: IT Security	2002
Monetary Authority of Singapore (MAS) - Notice 834: Cyber Hygiene Practices	Issue Date: 6 Aug, 2019
NIST Special Publication 800-171	Rev. 2
CIS Controls Version 8	Ver 8
Criminal Justice Information Services (CJIS) Security Policy	Ver. 5.9

Name	Version
Cybersecurity Maturity Model Certification (CMMC) Level 1	v1.02 (18 March 2020)
Cybersecurity Maturity Model Certification (CMMC) Level 2	v1.02 (18 March 2020)
Cybersecurity Maturity Model Certification (CMMC) Level 4	v1.02 (18 March 2020)
Cybersecurity Maturity Model Certification (CMMC) Level 5	v1.02 (18 March 2020)
Cybersecurity Maturity Model Certification (CMMC) Level 3	v1.02 (18 March 2020)
Payment Card Industry Data Security Standard (PCI-DSS) v3.2.1	Ver. 3.2.1
SWIFT Customer Security Controls Framework - Customer Security Programme v2019	Ver. 2019
Federal Risk and Authorization Management Program (FedRAMP H) - High Security Baseline	Rev. 4
Federal Risk and Authorization Management Program (FedRAMP M) - Moderate Security Baseline	Rev. 4
NIST 800-53 (Special Publication)	Rev 5

New Tokens Added

We have added two new tokens to this release.

policy.executionType: Select the policy by the execution type (Build Time, Run Time).

Examples:
Show policies created with controls used for resource evaluation.
`policy.executionType: Run Time`
Show policies created with controls used for IaC file evaluation.
`policy.executionType: Build Time`

control.executionType: Select the controls by the execution type (Build Time, Run Time).

Examples: Show controls used for resource evaluation.
`control.executionType: Run Time`
Show controls used for IaC file evaluation.
`control.executionType: Build Time`

API Features and Enhancements

We now support multiple policy names in the Fetch Remediation Activity API response. For detailed information, refer to CloudView 1.19 API Release Notes.

Issues addressed in this release

- We have now fixed an issue where the GET API (rest/v1/aws/connectors) displayed an error and did not return the list and count of all connectors when page size exceeded 800.
- We have now fixed an issue where you cannot add more than 21 resources to an exception. You should now be able to create an exception for up to 200 resources.
- We have now created a Knowledge-based article highlighting the difference between CloudView and AssetView connectors.
  Link: **https://success.qualys.com/support/s/article/000006782**
- We have now fixed the remediation steps for CIDs 50028 and 50083.