Qualys CloudView v1.x

Version 1.18.0

August 23, 2021

Here's what's new in Qualys CloudView 1.18.0!

Amazon Web Services

New control for CIS Amazon Web Services Foundations Benchmark
New controls for AWS Best Practices Policy
New controls for AWS Database Service Best Practices
Migrated Controls

Microsoft Azure

New controls for Azure Best Practices Policy
New controls for Azure Function App Best Practices Policy

Google Cloud Platform

New controls for CIS Google Cloud Platform Foundation Benchmark
New controls for GCP GKE Best Practices Policy
New controls for GCP Best Practices Policy
New controls for GCP Cloud SQL Best Practices Policy

Common Feature

Quick Navigation to Connector-Specific Control Evaluation

Qualys CloudView 1.18 brings you many more Improvements and updates! Learn more

Amazon Web Services

New control for CIS Amazon Web Services Foundations Benchmark

We have introduced the following new control for CIS Amazon Web Services Foundations Benchmark.

CID	Service	Resource	Title
255	S3	S3 Bucket	Ensure MFA Delete is enabled on S3 buckets

New controls for AWS Best Practices Policy

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

Note: Few additional permissions are needed for control evaluation of API Gateway and EFS resources. Learn more

CID	Service	Resource	Title
221	Workspace	Directory	Ensure ChangeComputeType is Disabled in all regions for Workspace Directories
222	Workspace	Directory	Ensure SwitchRunningMode is Disabled in all regions for Workspace Directories
223	Workspace	Directory	Ensure RebuildWorkspace is Disabled in all regions for Workspace Directories
224	Workspace	Directory	Ensure only AD Connector directory type is allowed for AWS Directories
225	Workspace	Workspace	Ensure to enable the encryption of the Root volumes for Workspaces in all regions
226	Workspace	Workspace	Ensure to enable the encryption of the User volumes for Workspaces in all regions
228	VPC	Transit gateway	Ensure to disable default route table association for Transit Gateways in all regions
229	VPC	Transit gateway	Ensure to disable default route table propagation for Transit Gateways in all regions
252	EFS	EFS	Ensure to encrypt the data in transit when using NFS between the client and EFS service
245	EC2	Load Balancer	Ensure there are no Internet facing Network load balancers
246	EC2	Load Balancer	Ensure NLB using listener type TLS must have SSL Security Policy

CID	Service	Resource	Title
247	EC2	Load Balancer	Ensure that NLB listeners using TLS have TLS enabled Target Groups configured
248	EC2	Load Balancer	Ensure that NLB listeners using default insecure ports are not configured for passthrough
249	EC2	Load Balancer	Ensure AWS NLB logging is enabled
227	API Gateway	Rest API Gateway	Ensure Amazon API Gateway APIs are only accessible through private API endpoints in all regions
242	API Gateway	Rest API Gateway	Ensure logging is not set to OFF for Rest APIs Stage in all regions
244	API Gateway	Rest API Gateway	Ensure accessLogSettings exists with the destinationArn and in the json format for Rest API Stage in all regions
243	API Gateway	Rest API Gateway	Ensure to enable encryption if caching is enabled for Rest API Stage in all regions
234	EMR	EMR	Ensure to configure certificate provider type to custom in EMR security configuration
235	EMR	EMR	Ensure to enable data in transit encryption for EMR security configurations
237	EMR	EMR	Ensure termination protection is enabled for EMR Clusters
238	ACM	ACM	Ensure ACM uses imported certificates only and does not create/issue certificates
239	ACM	ACM	Ensure expired certificates are removed from AWS ACM
240	ACM	ACM	Ensure ACM certificates should not have domain with wildcard(*)
241	ACM	ACM	Ensure that the certificate use appropriate algorithms and Key size
193	EC2	Load Balancer	Ensure that NLB balancer listener is not using unencrypted protocol
194	EC2	Load Balancer	Ensure that Classic Elastic load balancer is not internet facing
195	EC2	Load Balancer	Ensure Classic Elastic Load balancer must have SSL Security Policy

New Permissions for EFS and API Gateway Resources

To evaluate controls related to Elastic File System (EFS) and API Gateway resources, you need to assign additional permissions to the IAM role associated with the AWS connector in your cloud environment. You need to create a new policy with the required permissions and attach the policy to the IAM role associated with the AWS connector.

Note: These additional permissions are not required for Cloud Inventory users.

You can assign the policy with additional permissions to a connector while creating a new connector or edit the policy associated with the IAM role.

For the detailed steps on custom policy creation and attaching the policy to the IAM role, refer to the CloudView Online help.

New controls for AWS Database Service Best Practices

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

CID	Service	Resource	Title
190	Redshift	Redshift Clusters	Ensure Redshift Cluster is configured to require an SSL connection
191	Redshift	Redshift Clusters	Ensure database audit logging is enabled for Redshift Cluster
192	Redshift	Redshift Clusters	Ensure Redshift Cluster are encrypted with customer managed keys
265	RDS	Amazon Aurora	Ensure status of the 'log_destination' parameter for Aurora PostgreSQL cluster is set to 'csvlog'
266	RDS	Amazon Aurora	Ensure status of the 'log_rotation_age' parameter for Aurora PostgreSQL cluster is set to 60(minutes)
267	RDS	Amazon Aurora	Ensure status of the 'log_connections' parameter for Aurora PostgreSQL cluster is set to ON(1)
268	RDS	Amazon Aurora	Ensure status of the 'log_disconnections' parameter for Aurora PostgreSQL cluster is set to ON(1)
269	RDS	Amazon Aurora	Ensure status of the 'log_hostname' parameter for Aurora PostgreSQL cluster is set to OFF(0)
270	RDS	Amazon Aurora	Ensure status of the 'log_statement' parameter for Aurora PostgreSQL cluster is set to 'ddl' or stricter
271	RDS	Amazon Aurora	Ensure the 'pgaudit.log' parameter for Aurora PostgreSQL cluster is set to appropriate value

CID	Service	Resource	Title
257	RDS	RDS	Ensure status of the 'log_destination' parameter for PostgreSQL instance is set to 'csvlog'
258	RDS	RDS	Ensure status of the 'log_rotation_age' parameter for PostgreSQL instance is set to 60(minutes)
259	RDS	RDS	Ensure status of the 'log_connections' parameter for PostgreSQL instance is set to ON(1)
260	RDS	RDS	Ensure status of the 'log_disconnections' parameter for PostgreSQL instance is set to ON(1)
261	RDS	RDS	Ensure status of the 'log_hostname' parameter for PostgreSQL instance is set to OFF(0)
262	RDS	RDS	Ensure status of the 'log_statement' parameter for PostgreSQL instance is set to 'ddl' or stricter
263	RDS	RDS	Ensure the 'pgaudit.log' parameter for PostgreSQL instance is set to appropriate value
254	RDS	Amazon Aurora	Ensure that backup retention is set between 3 to 7 days for Aurora postgreSQL clusters

Migrated Controls

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

CID	Title	Service	Resource
53	Ensure Encryption is enabled for the database Instance	RDS	RDS

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
50144	App Service	Web App	Ensure that CORS does not allow every resource to access the Web apps
50145	App Service	Web App	Ensure that Diagnostic logs is enabled in Web apps
50148	App Service	Web App	Ensure that Managed identity is used in Web apps
50150	App Service	Web App	Ensure that Remote debugging is turned off for Web apps
50152	App Service	Web App	Ensure that routing of outbound non-RFC 1918 traffic to Azure Virtual Network is enabled in Web apps
50153	Azure Cache for Redis	Redis Cache	Ensure that public network access is disabled in Redis Cache
50154	Azure Cache for Redis	Redis Cache	Ensure that Redis Cache uses private link
50155	Azure Cache for Redis	Redis Cache	Ensure that only secure connections to Redis Cache is enabled
50156	Disk	Disk	Ensure that public network access is disabled in Managed Disks
50157	Disk Accesses	Disk Access	Ensure that Disk Access resources are configured with private endpoints
50158	Event Hubs	Event Hub Namespace	Ensure that all Authorization Rules except RootManageSharedAccessKey are removed from Event Hub Namespaces
50159	Event Hubs	Event Hub	Ensure that Authorization rules are defined in Event Hub instances
50160	Event Hubs	Event Hub Namespace	Ensure that Event Hub Namespaces use Customer-Managed Key for encryption
50161	Event Hubs	Event Hub Namespace	Ensure that Event Hub Namespaces use private links
50162	Event Hubs	Event Hub Namespace	Ensure that Resource Logs are enabled in Event Hub Namespaces

CID	Service	Resource	Title
50163	Service Bus	Service Bus Namespace	Ensure that all Authorization Rules except RootManageSharedAccessKey are removed from Service Bus Namespaces
50164	Service Bus	Service Bus Namespace	Ensure that Service Bus Namespaces use private links
50165	Service Bus	Service Bus Namespace	Ensure that Resource Logs are enabled in Service Bus Namespaces
50166	Virtual Machine	Virtual Machine	Ensure that Azure Linux-based virtual machines (VMs) are configured to use SSH keys
50167	Container Instances	Container Group	Ensure that Azure Container Instance container groups use customer-managed key for encryption
50168	Cosmos DB	Cosmos DB	Ensure that Advanced Threat Protection is enabled for all Microsoft Azure Cosmos DB accounts
50169	Storage Account	Storage Account	Ensure that Advanced Threat Protection is enabled on Storage Accounts
50170	Storage Sync Services	Storage Sync Service	Ensure that Azure File Sync uses private link
50171	Azure Cache for Redis	Redis Cache	Ensure that Azure Redis Cache servers are using the latest version of the TLS protocol
50172	Key Vault	Key Vault	Ensure that public network access is disabled for Azure Key Vaults
50173	Storage Account	Storage Account	Ensure that Geo-redundant storage is enabled for Storage Accounts
50174	Storage Sync Services	Storage Sync Service	Ensure that Public network access is disabled for Azure File Sync
50175	Storage Account	Storage Account	Ensure that Storage Accounts have infrastructure encryption enabled
50176	Key Vault	Key Vault	Ensure that Azure Key Vaults use Private Links
50181	Storage Account	Storage Account	Ensure Storage Accounts are using the latest version of TLS encryption

CID	Service	Resource	Title
50192	Kubernetes Service	Kubernetes Cluster	Ensure that Azure Kubernetes Service Private Clusters is enabled
50193	Kubernetes Service	Kubernetes Cluster	Ensure that Azure Policy Add-on for Kubernetes service (AKS) is installed and enabled on your clusters
50199	Container Registry	Container Registry	Ensure that Container Registries are configured to disable public network access
50200	Container Registry	Container Registry	Ensure that Container Registries are configured with private endpoints
50201	Container Registry	Container Registry	Ensure that Container Registries are encrypted with a customer-managed key
50166	Virtual Machine	Virtual Machine	Ensure that Azure Linux-based virtual machines (VMs) are configured to use SSH keys

New controls for Azure Function App Best Practices Policy

We have introduced the following 5 controls for Azure Function App Best Practices Policy.

CID	Service	Resource	Title
50143	App Service	Function App	Ensure that CORS does not allow every resource to access the Function Apps
50146	App Service	Function App	Ensure that Function apps enforce FTPS-only access to FTP traffic
50147	App Service	Function App	Ensure that Managed identity is used in Function apps
50149	App Service	Function App	Ensure that Remote debugging is turned off for Function apps
50151	App Service	Function App	Ensure that routing of outbound non-RFC 1918 traffic to Azure Virtual Network is enabled in Function apps

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
52116	VPC Network	Networks	Ensure that Cloud DNS logging is enabled for all VPC networks

New controls for GCP GKE Best Practices Policy

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

CID	Service	Resource	Title
52117	Kubernetes Cluster	Kubernetes Engine	Ensure that data at rest available on your GKE clusters is encrypted with Customer-Managed Keys.

New controls for GCP Best Practices Policy

We have introduced the following two controls for GCP Best Practices Policy.

CID	Service	Resource	Title
52118	Pub/Sub	Pub/Sub	Ensure that Pub/Sub topics are encrypted using Customer-Managed Keys (CMKs).
52120	Compute Engine	Compute	Ensure that "On Host Maintenance" configuration setting is set to "Migrate" for all VM instances.

New controls for GCP Cloud SQL Best Practices Policy

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

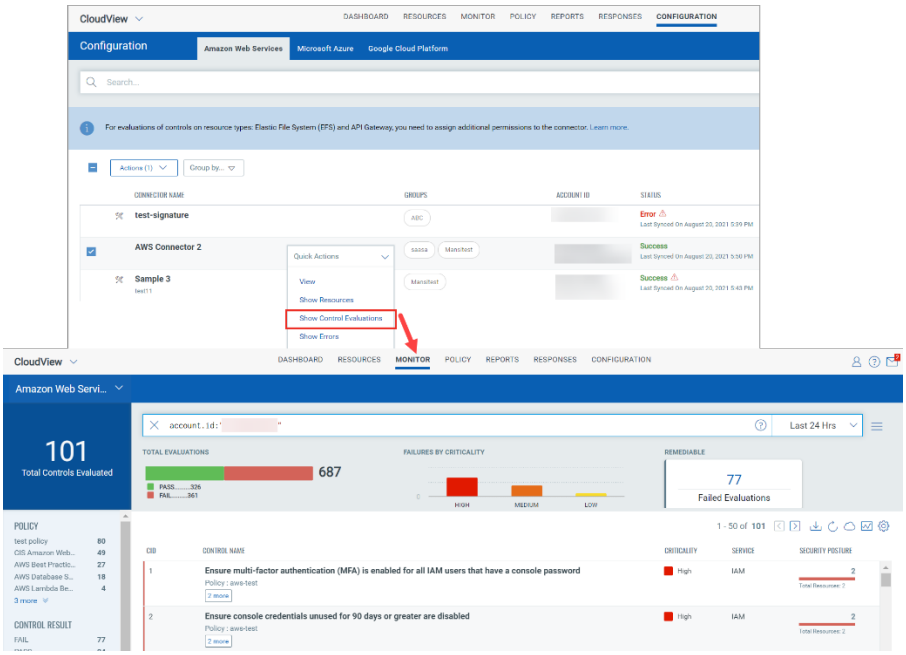
CID	Service	Resource	Title
52119	Cloud SQL	SQL	Ensure that MySQL database instances have the "slow_query_log" flag set to On (enabled)

Common Feature

Quick Navigation to Connector-Specific Control Evaluation

You can now quickly view the control evaluation results for a specific connector. We have now introduced a new quick action menu option named Show Control Evaluation. This option quickly navigates you to the Monitor tab and provides a glance of all the control evaluations associated with the connector.

On the Configuration tab, select the cloud provider, select the connector and then select **Show Control Evaluations** from the quick actions menu. The Monitor tab is displayed. The search bar is pre-populated with the filter query that displays control evaluations associated with the connector.



Issues addressed in this release

- Updated the check for CID 117 to include other CA certificate identifiers.
- Previously the controls would only check the logging condition as defined by CIS. It resulted in a failure if the customer added any extra field. The following controls were updated to check the CIS condition and ignore any additional values.
  - 52013
  - 52014
  - 52015
  - 52017
  - 52018
- Updated the title for CID 52095.