Qualys CloudView v1.x

Version 1.24
August 19, 2022

Here's what's new in Qualys CloudView 1.24!

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
New controls for Azure Function App Practices Policy

Google Cloud Platform

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

Qualys CloudView 1.24 brings you many more improvements and updates! Learn More

Copyright 2022 by Qualys, Inc. All Rights Reserved.

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
393	RDS	RDS	Ensure the option group attached to the RDS Oracle Instance have TLSv1.2 and the required ciphers configured
409	RDS Aurora PostgreSQL	RDS Cluster	Ensure that 'ssl_max_protocol_version' parameter for Aurora PostgreSQL cluster is set to latest version
410	RDS Aurora PostgreSQL	RDS Cluster	Ensure that 'ssl_min_protocol_version' parameter for Aurora PostgreSQL cluster is set to latest version
413	RDS	RDS	Ensure that your Amazon Relational Database Service (RDS) instances have Storage AutoScaling feature enabled
435	RDS	RDS	Ensure the Performance Insights feature is enabled for your Amazon RDS database instances
531	Neptune DB	Neptune DB Instances	Ensure that your Amazon Neptune database instances are using KMS Customer Master Keys (CMKs)
530	Neptune DB	Neptune DB Instances	Ensure that encryption is enabled for AWS Neptune instances
455	RDS	RDS	Ensure backtracking is enabled for AWS RDS cluster
456	RDS	RDS	Ensure database retention is set to 7 days or more for AWS RDS cluster
457	RDS	RDS	Ensure Aurora Serverless AutoPause is enabled for RDS cluster
459	Redshift	Redshift	Ensure Enhanced VPC routing should be enabled for AWS Redshift Clusters

New Controls for AWS Best Practices Policy

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

CID	Service	Resource	Title
503	API Gateway	Custom Domain	Ensure TLS security policy is using 1.2 version for the custom domains
379	S3	Bucket	Ensure S3 bucket must not allow "WRITE" permissions for server access logs from all the principals on the buckets
411	ECS	ECS Task Definition	Ensure that a log driver has been defined for each active Amazon ECS task definition.
436	SNS	SNS Topic	Ensure to encrypt data in transit for the SNS topic
438	SNS	SNS Topic	Ensure AWS SNS topics do not allow HTTP subscriptions
504	SQS	SQS	Ensure there is a Dead Letter Queue configured for each Amazon SQS queue
505	EMR	EMR Cluster	Ensure that EMR cluster is configured with security configuration
506	EMR	EMR Cluster	Ensure AWS Elastic MapReduce (EMR) clusters capture detailed log data to Amazon S3
533	ACM	ACM	Ensure that ACM Certificate is validated
458	ELB	ELB	Ensure connection draining is enabled for AWS ELB
460	API Gateway	API Gateway	Ensure that content encoding is enabled for API Gateway Rest API
461	System Manager	System Manager	Ensure to configure idle session timeout in all regions
462	System Manager	System Manager	Ensure session logs for system manager are stored in CloudWatch log groups or S3 buckets
464	System Manager	System Manager	Ensure "Block public sharing setting" is ON for the documents in all regions
465	API Gateway	API Gateway	Ensure stage caching is enabled for AWS API Gateway Method Settings
467	SageMaker	SageMaker	Ensure to disable root access for all notebook instance users
468	SageMaker	SageMaker	Ensure to enable inter-container traffic encryption for Processing jobs(if configured)
469	SageMaker	SageMaker	Ensure processing jobs(if configured) are running inside a VPC

CID	Service	Resource	Title
470	SageMaker	SageMaker	Ensure to enable network isolation for processing jobs(if configured)
471	SageMaker	SageMaker	Ensure ML storage volume attached to training jobs are encrypted
473	SageMaker	SageMaker	Ensure to encrypt the output of the training jobs in s3 with customer managed master key
474	SageMaker	SageMaker	Ensure to enable inter-container traffic encryption for training jobs
475	SageMaker	SageMaker	Ensure to enable network isolation for training jobs
476	SageMaker	SageMaker	Ensure ML storage volume attached to Hyperparameter Tuning jobs are encrypted
478	SageMaker	SageMaker	Ensure to encrypt the output of Hyperparameter tuning jobs in s3
479	SageMaker	SageMaker	Ensure to encrypt the output of Hyperparameter tuning jobs(if configured) in s3 with customer managed master key
480	SageMaker	SageMaker	Ensure to enable inter-container traffic encryption for Hyperparameter tuning jobs(if configured)
481	SageMaker	SageMaker	Ensure Hyperparameter tuning jobs(if configured) are running inside a VPC
482	SageMaker	SageMaker	Ensure to enable network isolation for Hyperparameter tuning jobs(if configured)
483	SageMaker	SageMaker	Ensure to enable network isolation for models
485	Kinesis	Kinesis	Ensure to enable CloudWatch logging in the audit logging account
489	DMS	DMS	Ensure multi-az is enabled for AWS DMS instances
490	DMS	DMS	Ensure auto minor version upgrade is enabled for AWS DMS instances
491	MQ Brokers	MQ Brokers	Ensure auto minor version upgrade is enabled for AWS MQ Brokers
492	MQ Brokers	MQ Brokers	Ensure active/standby deployment mode is used for AWS MQ Brokers
495	ElasticSearch	ElasticSearch	Ensure advanced security options are enabled for AWS ElasticSearch Domain

CID	Service	Resource	Title
496	ElasticSearch	ElasticSearch	Ensure general purpose SSD node type is not used for AWS ElasticSearch Domains - Strikedthrough
498	ElasticSearch	ElasticSearch	Ensure ElasticSearch Zone Awareness is enabled - Strikethrough Text Ensure Zone Awareness is enabled for AWS ElasticSearch Domain
499	ElasticSearch	ElasticSearch	Ensure Amazon cognito authentication is enabled for AWS ElasticSearch Domain
500	ElasticSearch	ElasticSearch	Ensure dedicated master nodes are enabled for AWS ElasticSearch Domains
501	CloudFormation	CloudFormation	Ensure policies are used for AWS CloudFormation Stacks
502	CloudFormation	CloudFormation	Ensure termination protection is enabled for AWS CloudFormation Stack
508	EBS	EBS	Ensure AWS EBS Volume has a corresponding AWS EBS Snapshot
509	Application Mesl	Application Mesh	Ensure egress filter is set as 'DROP_ALL' for AWS Application Mesh
510	Secrets	Secrets	Ensure secrets should be auto rotated after not more than 90 days
511	API Gateway	API Gateway	Ensure CORS is configured to prevent sharing across all domains for AWS API Gateway V2 API
513	EC2	EC2	Ensure IMDv1 is disabled for AWS EC2 instances
514	Kinesis Streams	Kinesis Streams	Ensure sufficient data retention period is set for AWS Kinesis Streams (7 days or More)
516	ACM	ACM	Ensure AWS ACM certificates are renewed 7 days before expiration date
518	SNS	SNS	Ensure SNS Topics are encrypted with customer managed master key
519	SageMaker	SageMaker	Ensure ML storage volume attached to notebooks are encrypted
520	SageMaker	SageMaker	Ensure ML storage volume attached to notebooks are encrypted with customer managed master key
521	SageMaker	SageMaker	Ensure ML storage volume attached to processing jobs are encrypted

CID	Service	Resource	Title
522	SageMaker	SageMaker	Ensure ML storage volume attached to processing jobs(if configured) are encrypted with customer managed master key
523	SageMaker	SageMaker	Ensure to encrypt the output of processing jobs
524	SageMaker	SageMaker	Ensure to encrypt the output of processing jobs(if configured)in s3 with customer managed master key
527	Kinesis	Kinesis	Ensure to encrypt the destination bucket in s3 in the audit logging account
528	Kinesis	Kinesis	Ensure to encrypt the destination bucket in s3 with customer managed master keys in the audit logging account

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
50373	Activity Log	Activity Log	Ensure that an activity log alert is created for "Create or Update Load Balancer" events.
50376	Activity Log	Activity Log	Ensure there is an activity log alert created for the "Delete Key Vault" events.
50377	Activity Log	Activity Log	Ensure there is an Azure activity log alert created for "Delete Load Balancer" events.
50378	Activity Log	Activity Log	Ensure that an activity log alert exists for "Power Off Virtual Machine" events.
50380	Activity Log	Activity Log	Ensure that an activity log alert is created for "Update Key Vault (Microsoft.KeyVault/vaults)" events.
50389	VMSS	VMSS	Ensure that Azure virtual machine scale sets are configured for zone redundancy.
50390	Monitor	Monitor	Ensure that Azure Log Profile is configured to export all control & management activities.
50391	Search	Search	Ensure that Azure Search Service instances are configured to use system-assigned managed identities.
50392	Storage Accounts	Storage Accounts	Ensure that Azure Blob Storage service has a lifecycle management policy configured.
50393	Storage Accounts	Storage Accounts	Ensure that Azure Storage account access is limited only to specific IP address(es).
50375	Activity Log	Activity Log	Ensure that an activity log alert is created for "Delete Azure SQL Database" events.
50374	Activity Log	Activity Log	Ensure that an activity log alert is created for "Create or Update Azure SQL Database" events.
50381	Activity Log	Activity Log	Ensure that an activity log alert is created for “Create/Update MySQL Database” events.
50382	Activity Log	Activity Log	Ensure that an activity log alert is created for “Create/Update PostgreSQL Database” events.
50383	Activity Log	Activity Log	Ensure that an activity log alert is created for “Delete MySQL Database” events.
50384	Activity Log	Activity Log	Ensure that an activity log alert is created for “Delete PostgreSQL Database” events.
50379	Activity Log	Activity Log	Ensure that an activity log alert is created for "Rename Azure SQL Database" events.

CID	Service	Resource	Title
50394	Subscriptions	Subscriptions	Ensure there are budget alerts configured to warn about forthcoming budget overages within your Azure cloud account.

New Controls for Azure Function App Practices Policy

We have introduced the following new controls Azure Function App Practices Policy.

CID	Service	Resource	Title
50385	AppService	AppService	Ensure there is a sufficient backup retention period configured for Azure Api App Services applications.
50386	AppService	AppService	Ensure there is a sufficient backup retention period configured for Azure Web App Services applications.
50387	AppService	AppService	Ensure that all your Azure Api App Services applications are using the Backup and Restore feature.
50388	AppService	AppService	Ensure that all your Azure App Services applications are using the Backup and Restore feature in Web App

Google Cloud Platform

New Controls in CIS Google Cloud Platform Foundation Benchmark

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

CID	Service	Resource	Title
52176	SQL	Postgresql	Ensure that 'cloudsql.enable_pgaudit' database flag for each Cloud Sql Postgresql Instance is Set to 'on' for Centralized Logging
52175	API & Services	APIs	Ensure Cloud Asset Inventory Is Enabled

New Controls in GCP Cloud SQL Best Practices Policy

We have introduced the following new controls in GCP Cloud SQL Best Practices Policy.

CID	Service	Resource	Title
52169	Cloud SQL	Cloud SQL	Ensure that automatic storage increase is enabled for your Cloud SQL database instances.

New Controls in GCP Best Practices Policy

We have introduced the following new controls in GCP Best Practices Policy

CID	Service	Resource	Title
52172	API & Services	API Key	Ensure that API keys are restricted to only those APIs that your application needs access to
52173	API & Services	API Key	Ensure there are no unrestricted API keys available within your Google Cloud Platform (GCP) project
52174	Network	Load Balancing	Ensure that logging is enabled for Google Cloud load balancing backend services.
52170	PubSub	PubSub	Ensure there is a dead-letter topic configured for each Pub/Sub subscription.
52171	Compute Engine	Instance Group	Ensure that your Google Cloud instance groups are using autohealing to proactively replace failing instances
52132	API & Services	API Keys	Ensure there are no API keys associated with your Google Cloud Platform (GCP) projects

Issues addressed in this release

- We have fixed an issue where service accounts without external keys no longer continue to be evaluated by GCP controls.
- We have removed double quotes from control titles so that they do not break the query when entered in monitor query search.