Qualys CloudView v1.x

Version 1.20.0

January 3, 2022

Here's what's new in Qualys CloudView 1.20.0!

Amazon Web Services

New controls for AWS Best Practices Policy
New controls for AWS Database Service Best Practices Policy
Permissions Needed for QLDB and MSK Resources

Microsoft Azure

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

Google Cloud Platform

New controls for GCP Kubernetes Engine Best Practices Policy
New controls for GCP Best Practices Policy

Qualys CloudView 1.20 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
181	Workspace	Workspace	Ensure proper protocol is configured for Radius server in AWS Directory
179	Workspace	Workspace	Ensure MFA is enabled in AWS Directory
236	System Manager	System Manager	Ensure that all AWS Systems Manager (SSM) parameters are encrypted
196	VPC	Security Group	Ensure AWS VPC subnets have automatic public IP assignment disabled
202	EC2	Network Load Balancer	Ensure to update the Security Policy of the Network Load Balance
288	SageMaker	SageMaker Notebook	Ensure SageMaker Notebook is encrypted at rest using KMS CMK
377	ECR	ECR Images	Ensure ECR image scanning on push is enabled
324	MSK	MSK_CLUSTER	Ensure MSK Cluster encryption at rest and in transit is enabled
358	ECR	ECR Repository	Ensure that ECR repositories are encrypted using KMS
305	ECR	ECR Repository	Ensure ECR Image Tags are immutable
347	SageMaker	SageMaker Notebook	Ensure that direct internet access is disabled for an Amazon SageMaker Notebook Instance
312	ECS	ECS Cluster	Ensure container insights are enabled on ECS cluster
293	ECR	ECR Repository	Ensure ECR repository policy is not set to public
385	EMR	EMR Cluster	Ensure that EMR Cluster security configuration encryption is using SSE-KMS
342	EMR	EMR Cluster	Ensure that EMR clusters with Kerberos have Kerberos Realm set

New controls for AWS Database Service Best Practices Policy

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

CID	Service	Resource	Title
180	QLDB	QLDB Ledger	Ensure QLDB ledger has deletion protection enabled
251	QLDB	QLDB Ledger	Ensure QLDB ledger has encryption enabled using accessible Customer managed KMS key
250	RDS	RDS	Ensure RDS instances should not have be open to a large scope
201	RDS	RDS	Ensure RDS Instance should not have an Interface open to a public scope
384	QLDB	QLDB Ledger	Ensure QLDB ledger permissions mode is set to STANDARD

Permissions Needed for QLDB and MSK Resources

The cross-account role associated with the AWS connector needs additional permissions to fetch information about Amazon Quantum Ledger Database (QLDB) and Managed Streaming for Apache Kafka (MSK) 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 15 controls for Azure Best Practices Policy.

CID	Service	Resource	Title
50303	API MANAGE MENT	API MANAGEM ENT	Ensure that API Management Services use latest protocol for Client Side Security
50304	API MANAGE MENT	API MANAGEM ENT	Ensure that API Management Services use latest protocol for Backend Side Transport Security
50305	API MANAGE MENT	API MANAGEM ENT	Ensure that API Management services use a SKU that supports virtual networks
50306	API MANAGE MENT	API MANAGEM ENT	Ensure that Cipher Triple DES (3DES) is enabled for API Management resource
50307	API MANAGE MENT	API MANAGEM ENT	Ensure that HTTP/2 client side protocol is enabled for API Management resource
50308	API MANAGE MENT	API MANAGEM ENT	Ensure that System assigned Managed Identity is enabled for API Management Service
50309	LOGIC APP	LOGIC APP	Ensure that Logic Apps are deployed into Integration Service Environment
50267	Data Factories	Data Factory	Ensure that Azure Data Factory is encrypted with a customer-managed key
50245	Data Factories	Data Factory	Ensure that public network access is disabled in Azure Data Factory
50244	Data Factories	Data Factory	Ensure that Azure Data Factory uses Git repository for source control
50265	Data Explorer	Data Explorer	Ensure that encryption at rest uses customer-managed key in Azure Data Explorer
50229	Data Explorer	Data Explorer	Ensure that Azure Data Explorer uses double encryption
50228	Data Explorer	Data Explorer	Ensure that Azure Data Explorer uses disk encryption

CID	Service	Resource	Title
50261	Service Fabric	Service Fabric	Ensure that Service Fabric cluster has the ClusterProtectionLevel property set to EncryptAndSign
50262	Service Fabric	Service Fabric	Ensure that Service Fabric cluster uses Azure Active Directory for authentication
50256	Network Interfaces	Network Interface	Ensure that Network Interfaces don't use public IPs
50279	Kubernetes service	Kubernetes cluster	Ensure that Azure Kubernetes Service (AKS) cluster has Network Policy configured
50249	IOT Hub	IOT Hub	Ensure that public network access is disabled for Azure IoT Hub
50246	Data Lake Storage	Data Lake Storage	Ensure that encryption is enabled for Data Lake Store accounts
50239	Virtual Machine Scale Sets	Virtual Machine Scale Set	Ensure that automatic OS image patching is enabled for Virtual Machine Scale Sets
50236	App Service	Web App	Ensure that Web Apps use Azure Files
50231	Security Center	Security Policy	Ensure that Azure Defender is set to On for SQL servers on machines
50230	Batch Accounts	Batch Account	Ensure that Azure Batch account uses key vault to encrypt data
50227	Automation Accounts	Automation Account	Ensure that Automation account variables are encrypted
50225	Storage Account	Storage Account	Ensure that Storage accounts disallow Blob public access
50223	Virtual Machine	Virtual Machine	Ensure that Virtual Machine disallows Extensions
50218	Key Vault	Key	Ensure that the expiry date is set on all keys
50217	Monitor	Log Profiles	Ensure that audit profile captures all the activities
50280	Device Provisioning Services	Device Provisioning Service	Ensure that public network access is disabled for IoT Hub Device Provisioning Service instances

CID	Service	Resource	Title
50281	Device Provisioning Services	Device Provisioning Service	Ensure that IoT Hub Device Provisioning Service instances use private links
50282	IOT Hub	IOT Hub	Ensure that Resource logs are enabled in IoT Hub
50283	Data Factories	Integration Runtime	Ensure that Azure Data Factory Integration Runtimes have a limit for the number of cores
50284	Data Factories	Data Factory	Ensure that Azure Data Factory uses private link
50285	Data Factories	Integration Runtime	Ensure that SQL Server Integration Services Integration Runtimes on Azure Data Factory are joined to a virtual network
50286	Data Explorer	Data Explorer	Ensure that Virtual network injection is enabled for Azure Data Explorer
50287	Automation Accounts	Automation Account	Ensure that public network access is disabled for Automation accounts
50288	Automation Accounts	Automation Account	Ensure that Automation account uses customer-managed keys to encrypt data at rest
50289	Automation Accounts	Automation Account	Ensure that Automation account has private endpoint connections enabled
50290	Batch Accounts	Batch Pool	Ensure that Azure Batch pools have disk encryption enabled
50291	Batch Accounts	Batch Account	Ensure that Azure Batch accounts have local authentication methods disabled
50292	Batch Accounts	Batch Account	Ensure that Metric alert rules are configured on Batch accounts
50293	Batch Accounts	Batch Account	Ensure that Batch accounts have private endpoint connections enabled
50294	Batch Accounts	Batch Account	Ensure that public network access is disabled for Batch accounts
50295	Batch Accounts	Batch Account	Ensure that Resource logs are enabled in Batch accounts
50296	Cognitive Services	Cognitive Service	Ensure that Cognitive Services enable data encryption with customer-managed keys

CID	Service	Resource	Title
50297	Cognitive Services	Cognitive Service	Ensure that Cognitive Services have local authentication methods disabled
50298	Cognitive Services	Cognitive Service	Ensure that Managed identity is used in Cognitive Services
50299	Cognitive Services	Cognitive Service	Ensure that Cognitive Services use private links
50300	Event Grid Domains	Event Grid Domain	Ensure that Azure Event Grid domains are configured to disable public network access
50301	Event Grid Topics	Event Grid Topic	Ensure that public network access is disabled in Azure Event Grid topics
50302	Event Grid Domains	Event Grid Domain	Ensure that Azure Event Grid domains use private links
50278	Container Registry	Container Registry	Ensure that Container Registry disallows unrestricted network access

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
50240	PostgreSQL server	PostgreSQL server	Ensure that PostgreSQL server has infrastructure encryption enabled
50263	MySQL server	MySQL	Ensure that MySQL server has infrastructure encryption enabled

Updated controls for Azure Database Service Best Practices Policy

We have updated the control title, control logic for the following controls.

CID	Service	Resource	New Title	Old Title
50096	PostgreSQL server	PostgreSQL server	Ensure Storage Auto-Growth is enabled on PostgreSQL server	Ensure that Advanced Data Security is enabled and Advanced Threat Protection settings is configured properly for a SQL Database
50108	SQL server	SQL server	Ensure SQL server has Auto-Failover group enabled	Ensure that Advanced Threat Protection settings is configured properly for Azure Database for MariaDB Server

Google Cloud Platform

New controls for GCP Kubernetes Engine Best Practices Policy

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

CID	Service	Resource	Title
52127	Kubernetes Engine	Kubernetes Cluster	Ensure Kubernetes Clusters are configured with Labels
52144	Kubernetes Engine	Kubernetes Cluster	Ensure the GKE Release Channel is set

New controls for GCP Best Practices Policy

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

ID	Service	Resource	Title
52135	IAM	Project IAM	Ensure Default Service account is not used at a project level
52138	IAM	Project IAM	Ensure no roles that enable to impersonate and manage all service accounts are used at a project level
52140	Storage	Storage	Ensure that Bucket should not log to itself
52156	Cloud Storage	Cloud Storage	Ensure that Google Cloud Storage objects are using a lifecycle configuration for cost management.
52157	Compute Engine	VM Instance	Ensure that the Auto-Delete feature is disabled for the disks attached to your VM instances.
52158	Compute Engine	VM Instance	Ensure that your production Google Cloud virtual machine instances are not preemptible.
52159	Compute Engine	VM Instance	Ensure that deletion protection is enabled for your Google Cloud virtual machine (VM) instances.
52160	Compute Engine	VM Disk	Ensure that your virtual machine (VM) instance disks are encrypted using Customer-Managed Keys (CMKs).
52161	Dataproc	Dataproc Cluster	Ensure that your Dataproc clusters are encrypted using Customer-Managed Keys (CMKs).
52162	Compute Engine	VM Instance	Ensure that automatic restart is enabled for VM instances

Issues addressed in this release

- Updated the remediation steps for making exceptions for some resources and also updated evidence for more clarity for CID 24.
- Updated evidence for more clarity for CID 12.
- Updated control signature to check expired certificates for CID: 239.