Qualys CloudView v1.x

Version 1.9.2.0
March 24, 2020

Here's what's new in Qualys CloudView 1.9.2!

Amazon Web Services

New Controls Added in AWS Best Practices Policy

New Control Added to AWS Lambda Best Practices Policy

Drill down to Vulnerability Details for Instances

Microsoft Azure

New Control Added to Azure Best Practices Policy

Inventory Support for Web App Resource (App Service)

New Azure Best Practices Policy for Function App

Azure Control Updates

Google Cloud Platform

New GCP Best Practices Policy

New GCP Best Practices Policy for Function App

GCP Control Updates

Common Features

New Resource Drop-Down

Qualys CloudView 1.9.2 brings you many more Improvements and updates! Learn more

Amazon Web Services

New Controls Added to AWS Best Practices Policy

We have added the following new controls to AWS Best Practices Policy.

CID	Resource	Service	Control Title
108	Redshift Clusters	Redshift	Ensure Version Upgrade is enabled for AWS Redshift clusters to automatically receive upgrades
109	Redshift Clusters	Redshift	Ensure that AWS Redshift database clusters are not using default endpoint port
110	Redshift Clusters	Redshift	Ensure that Redshift clusters are not publicly accessible
111	Redshift Clusters	Redshift	Ensure that AWS Redshift clusters master username is not set to well-known/default
112	Redshift Clusters	Redshift	Ensure that AWS Redshift clusters encryption is set for data at rest
113	Redshift Clusters	Redshift	Ensure audit logging is enabled for AWS Redshift clusters for security and troubleshooting purposes
114	EC2 Images	EC2	Ensure Images (AMIs) owned by an AWS account are not public
115	EBS Volumes	EC2	Ensure that EBS Volumes attached to EC2 instances are encrypted
116	EBS Volumes	EC2	Ensure that Unattached EBS Volumes are encrypted
117	RDS	RDS	Ensure that RDS Instances certificates are rotated
118	Document DB	Document DB	Ensure that documentDB Instances certificates are rotated
119	KMS Key	IAM	Ensure no AWS Managed CMKs is present
120	KMS Key	IAM	Ensure no CMK is marked for deletion
121	KMS Key	IAM	Ensure only Root user of the AWS Account should be allowed full access on the CMK
122	KMS Key	IAM	Permissions to delete key is not granted to any Principal other than the Root user of AWS Account
123	KMS Key	IAM	Ensure CMK administrators are not the user of the key
124	KMS Key Store	IAM	Ensure all Custom key stores are connected to their CloudHSM clusters

New Control Added to AWS Lambda Best Practices Policy

We have added control ID 125 to AWS Lambda Best Practices Policy for Lambda resource.

CID	Resource	Service	Control Title
125	Lambda	Lambda	Ensure that multiple triggers are not configured for Lambda Function Aliases

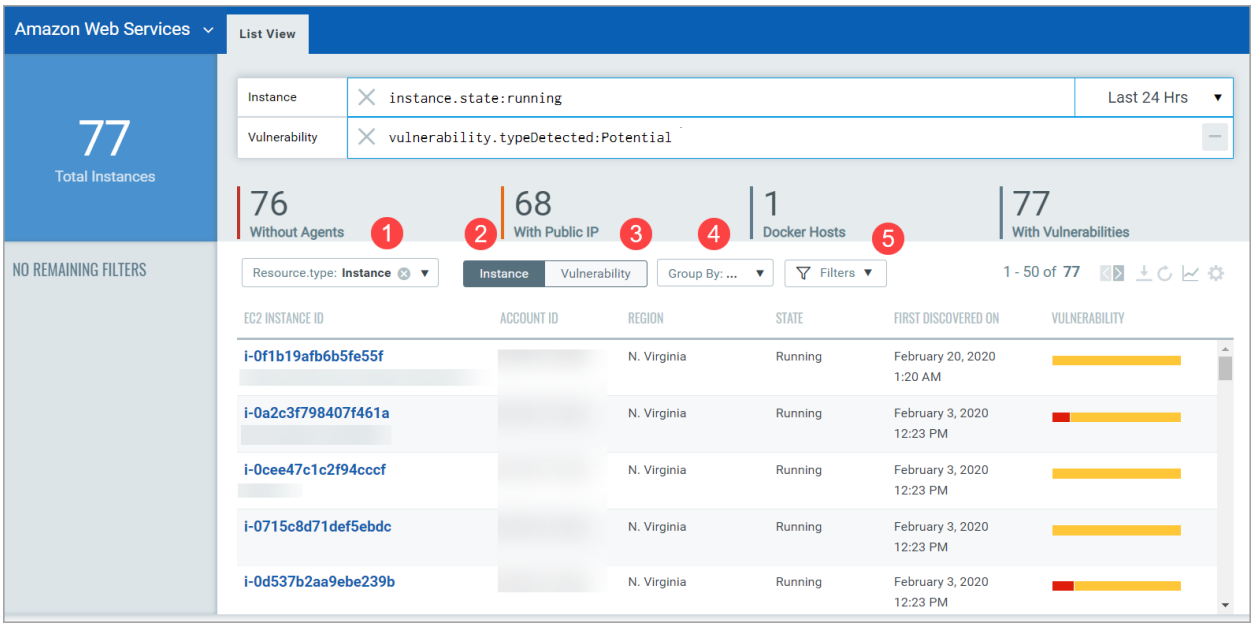
Drill down to Vulnerability Details for Instances

We now provide you with multiple meta data filters to narrow down your search for vulnerability details. Using the new filters, you can get a complete view of vulnerability posture from an asset and vulnerability point of view.

Under Resources tab, select the Instance type of resource (AWS). Choose Instance resource type from the Resource drop-down.

The Resource Type drop-down is available to quickly view resource inventory of different types of resources. You can use the various metadata filters, group by options and custom query capabilities to find what you are interested in.

Note: The vulnerability data is available only for Instance type of resource (AWS cloud provider) and only after the Instances have been scanned.



1 - Indicates the type of resource
2 - Click to view instances in your inventory
3 - Click to view vulnerabilities that affect the instances in your cloud environment
4 - Various group-by filters to narrow down your search
5 - Filters for Type of vulnerabilities

Using the various filters, you can drill down to view vulnerabilities that exists on instances. The search tokens give you further flexibility to narrow down your search results.

Microsoft Azure

New Control Added to Azure Best Practices Policy

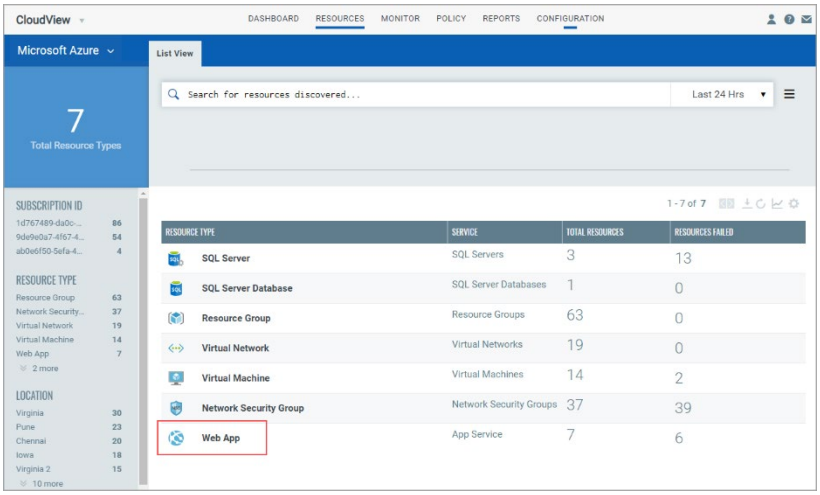
We have added the one new control to Azure Best Practices Policy.

CID	Resource	Service	Control Title
50034	Virtual Machine	Virtual Machine	Ensure disks are encrypted for Windows VMs with ADE version 1.1

Inventory Support for Web App Resource (App Service)

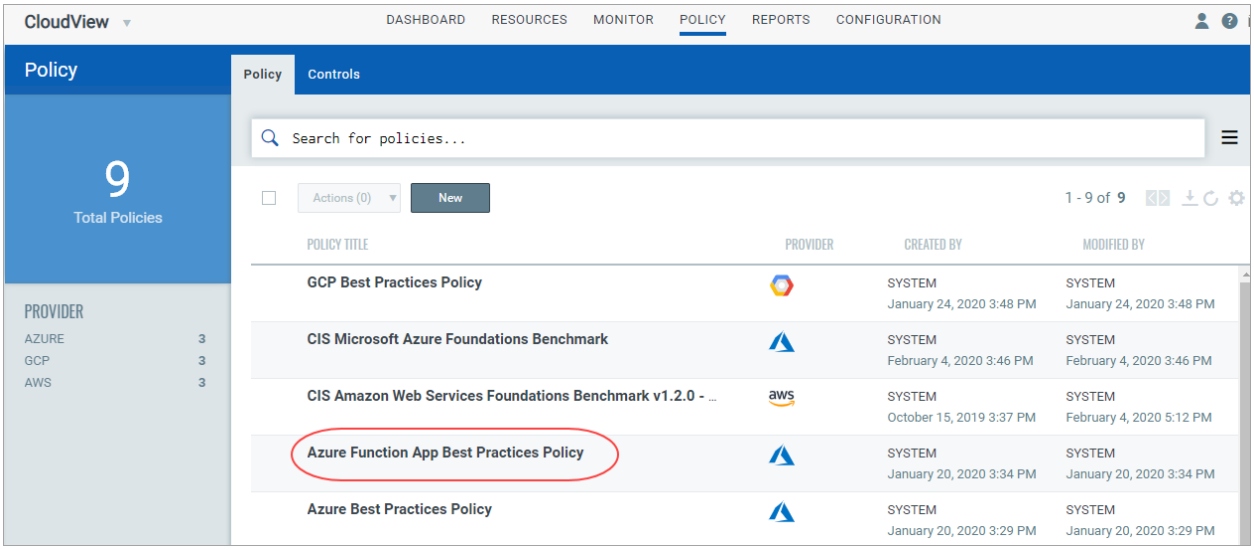
You can now monitor Web App resources and view its details. You can filter further using the tokens and view the resource information.

Go to Resources tab and select Microsoft Azure from the dropdown. You can view the newly supported resource in the List View.



New Azure Best Practices Policy for Function App

We have introduced Azure Function App Best Practices Policy to help you in automated auditing and reporting on the Azure Function app misconfigurations, unwarranted access, and non-standard deployments, and provide remediation steps to manage risks.



New Controls

The pre-defined Azure Function App Best Practices Policy is loaded with the following 6 system-defined controls.

CID	Resource	Service	Control Title
50084	Function App	App Service	Ensure App Service Authentication is set on Function Apps
50085	Function App	App Service	Ensure Function app redirects all HTTP traffic to HTTPS
50086	Function App	App Service	Ensure function app has 'Client Certificates (Incoming client certificates)' set to 'On'
50087	Function App	App Service	Ensure that 'Register with Azure Active Directory' is enabled on Function app
50088	Function App	App Service	Ensure function app is using the latest version of TLS encryption version
50089	Function App	App Service	Ensure that 'HTTP Version' is latest, if used to run the function app

Control Updates

We have updated the static content for the following controls to match with the changes on Azure portal. The static content for the control includes title, summary, specification, evaluation, rationale, remediation, references.

Note: Due to changes in API on Azure portal, control 50055 may display incorrect evaluations. The corrections will be available soon.

Azure Control Updates

CID	Resource	Service	Title	Sections Updated
50047	Web App	App Service	Ensure App Service Authentication is set on web apps	Control Logic
50048	Web App	App Service	Ensure web app redirects all HTTP traffic to HTTPS in Azure App Service	
50049	Web App	App Service	Ensure web app has 'Client Certificates (Incoming client certificates)' set to 'On'	
50050	Web App	App Service	Ensure that 'Register with Azure Active Directory' is enabled on web apps	
50051	Web App	App Service	Ensure web app is using the latest version of TLS encryption version	
50061	Web App	App Service	Ensure that 'HTTP Version' is latest, if used to run the web app	

Google Cloud Platform

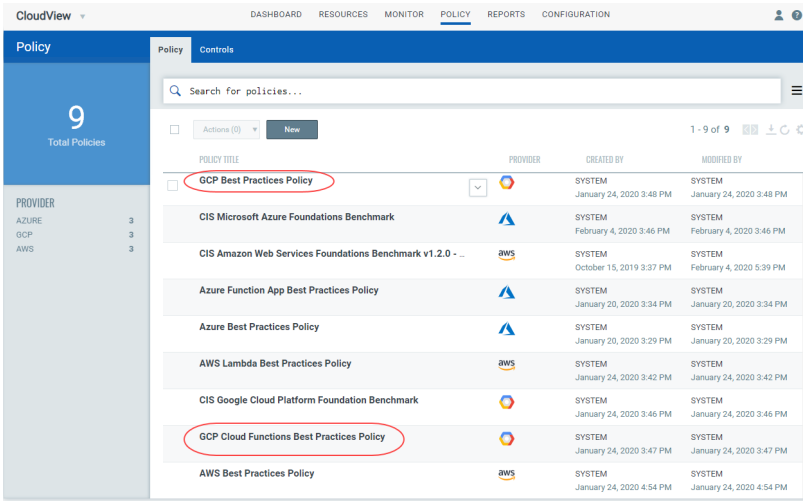
We have introduced two new policies for GCP:

New GCP Best Practices Policy

We have introduced GCP Best Practices Policy that covers Cloud Functions Services of Google Cloud Platform. The controls in this policy are targeted only for Cloud Functions service.

New Controls

The pre-defined GCP Best Practices Policy is loaded with the following 4 system-defined controls.



CID	Resource	Service	Control Title
52052	Cluster	Google Kubernetes Engine	Ensure that Application-Layer secret encryption is enabled for Kubernetes cluster
52053	Cluster	Google Kubernetes Engine	Ensure that Master authorized network is enabled for Kubernetes cluster
52057	Bucket	Storage	Ensure that there are no harmful object life cycle rules are created
52058	Bucket	Storage	Ensure that object retention policy is set on buckets

New GCP Best Practices Policy for Function App

We have introduced GCP Function App Best Practices Policy that covers Cloud Functions Services of Google Cloud Platform. The controls in this policy are targeted only for Cloud Functions service.

New Controls

The pre-defined GCP Function App Best Practices Policy is loaded with the following 3 system-defined controls.

CID	Resource	Service	Control Title
52054	Cloud Functions	Functions	Ensure that Default service account is not used for the function
52055	Cloud Functions	Functions	Ensure that Runtime used in function is not deprecated
52056	Cloud Functions	Functions	Ensure that function is not anonymously or publicly accessible

GCP Control Updates

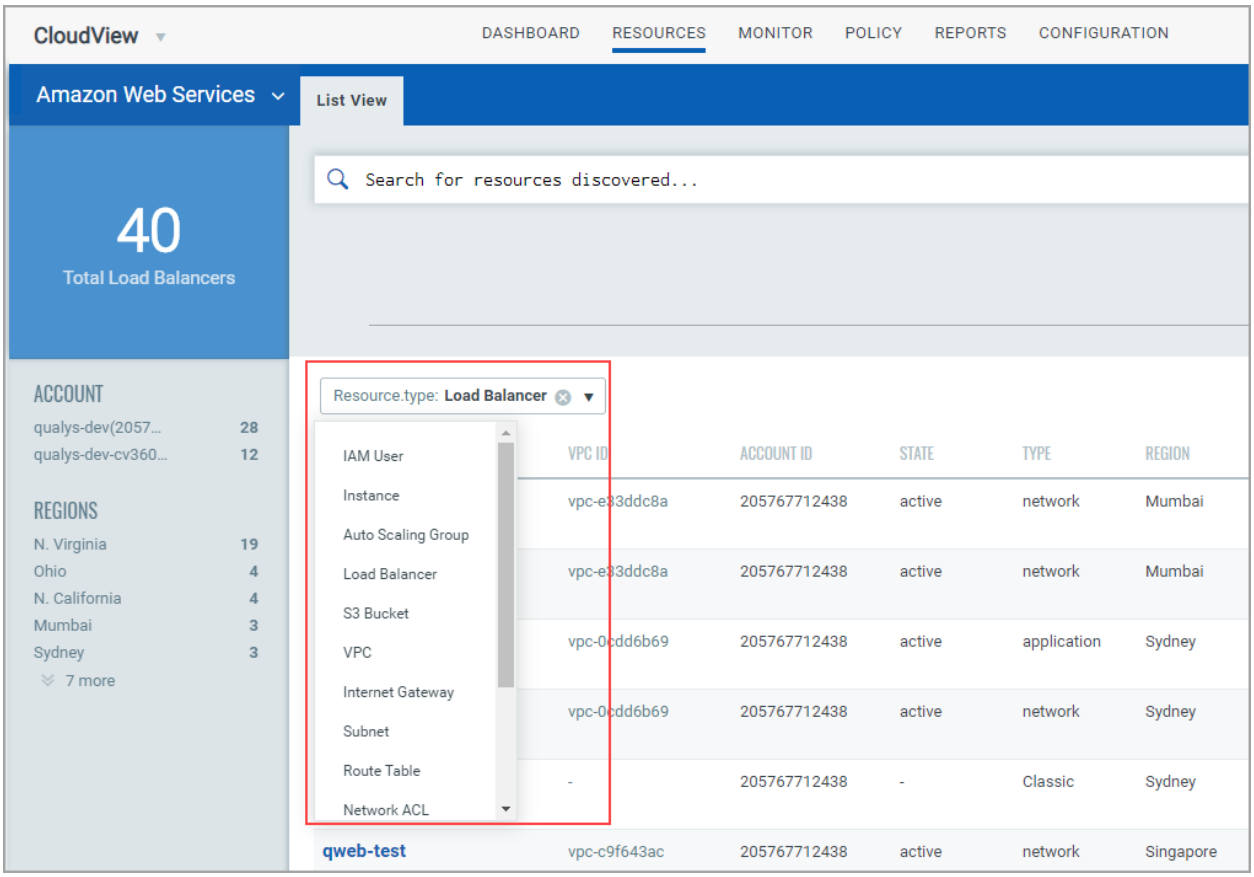
We have updated the following GCP related controls.

CID	Resource	Service	Title	Sections Updated
52021	Firewall Rules	VPC Network	Ensure that SSH access is restricted from the internet	Control Logic
52022	Firewall Rules	VPC Network	Ensure that RDP access is restricted from the internet	
52026	VM Instances	VM Instances	Ensure "Block Project-wide SSH keys" enabled for VM instances	
52050	Kubernetes Engine	Kubernetes Cluster	Ensure Kubernetes Clusters created with limited service account Access scopes for Project access	
52006	Project	IAM & Admin	Ensure that Separation of duties is enforced while assigning KMS related roles	Remediation
52002	Project	IAM & Admin	Ensure that ServiceAccount has no Admin privileges	
52008	Project	IAM & Admin	Ensure that Cloud Audit Logging is configured properly across all services and all users from a project	
52050	Kubernetes Engine	Kubernetes Cluster	Ensure Kubernetes Clusters created with limited service account Access scopes for Project access	

New Resource Drop-Down

We have introduced a resource dropdown filter that will fasten filtering of resources and switching between different resource types.

Go to Resources and choose the resource type. Resources belonging to the selected resource type are displayed. You could easily switch to other resource type using the drop-down.



Note: When you switch from one resource type to another resource type, the filters applied are cleared.

Issues addressed in this release

We have fixed the following issues:

- Updated the control logic and fixed the false positives for GCP controls 52002 , 52021 ,52022, 52001 and 52030.
- Due to API limitations, VMs with Legacy ADE cannot be covered for 50033 as the API result is not in expected format. A new control 50034 has been added for VMs with Legacy ADE versions, to mitigate this and avert false positives.
- Added a new control CID 125 to prevent false positives resulting due to CID 99 for AWS compliance.
- Updated the control logic for CID 52022 and CID 52021 to prevent the control failure for public access.
- Updated the information for CID 104 to include the steps that should help to surpass the error message.
- The connectors listing is now corrected for Azure and GCP so that even if there are large number of connectors in your subscription, they are all correctly listed.
- We have now fixed the issue so that the Azure connector is not permanently stuck in processing state. Although it may take longer time to process, it eventually converts to Successful state once all the resource information is successfully fetched.