



Qualys CloudView v1.x

Version 1.9.0.0

October 17, 2019

Here's what's new in Qualys CloudView 1.9!

Amazon Web Services

[Base Account Support for AWS Connectors](#)

[GovCloud and China Support for AWS](#)

[Inventory Support for Lambda Function Resource](#)

[New Controls Added in AWS Best Practices Policy](#)

[New Best Practices Policy for Lambda Function](#)

[Search Resources Using Account Alias](#)

[Identifying Instances with Vulnerability Using Search Tokens](#)

Microsoft Azure

[GovCloud Support for Azure Connectors](#)

[New Controls for CIS Microsoft Azure Foundations Benchmark](#)

[New Azure Best Practices Policy](#)

[Azure Control Updates](#)

GCP

[New Controls in CIS Google Cloud Platform Foundation Benchmark](#)

Common Features

[Customizing Out of the Box Control Parameter Values and Criticality](#)

[Group Connectors and Assign Access to Sub Users](#)

[Enhanced Details for Instance type of Resource](#)

Qualys CloudView 1.9 brings you many more improvements and updates! [Learn more](#)

Amazon Web Services

Base Account Support for AWS Connectors

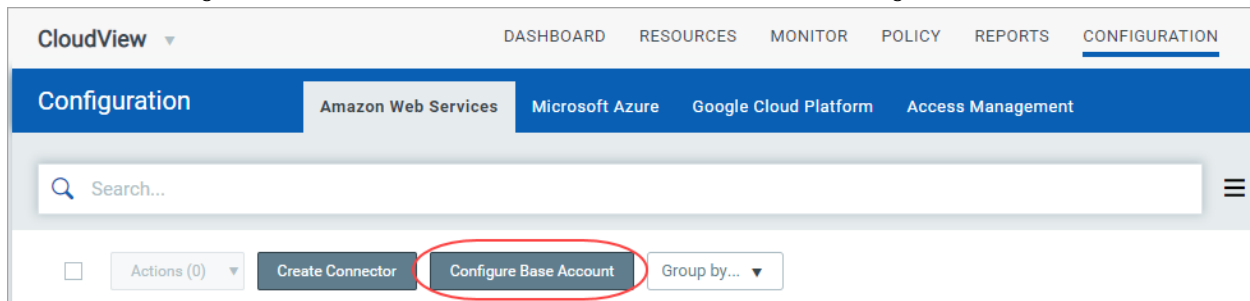
The AWS connectors uses Qualys accounts to query the AWS APIs. If you do not wish to use the Qualys accounts, you can use the base account feature to use your own AWS account for AWS API queries from CloudView. You need to configure your AWS account ID and user credential for each base account type.

For example, you have 3 AWS accounts: Central Security Account, Production and Development. You can designate the Central Security Account as a base account to set up an AWS connector in CloudView to pull the resources from Production & Development account.

Tell me the steps

Before you create a new connector, create a base account for the same account type (region). In AWS console, create a IAM user with API access and associate IAM policies with AssumeRole permissions.

Go to the Configuration > Amazon Web Services and then click Configure Base Account.



Provide title, AWS account ID, access and secret keys and then select the account type. You can create only one base account per account type.

Click Save.

That's it!

A screenshot of the 'Create Base Account' form. The form has the following fields: 'Title' (text input, required), 'AWS Account ID' (text input, required), 'Access Key' (password input, required), and 'Secret Key' (password input, required). Below these fields is a 'Select Account Type' section with three radio buttons: 'Global' (selected), 'GovCloud', and 'China'. There is also a checkbox for 'Use in Assetview'. At the bottom are 'Cancel' and 'Save' buttons.

Note: If you plan to move the existing connectors from Qualys account to new base account, ensure that you update the cross-account role on AWS console to reflect the new base account. Else, it could result in failure of connectors.

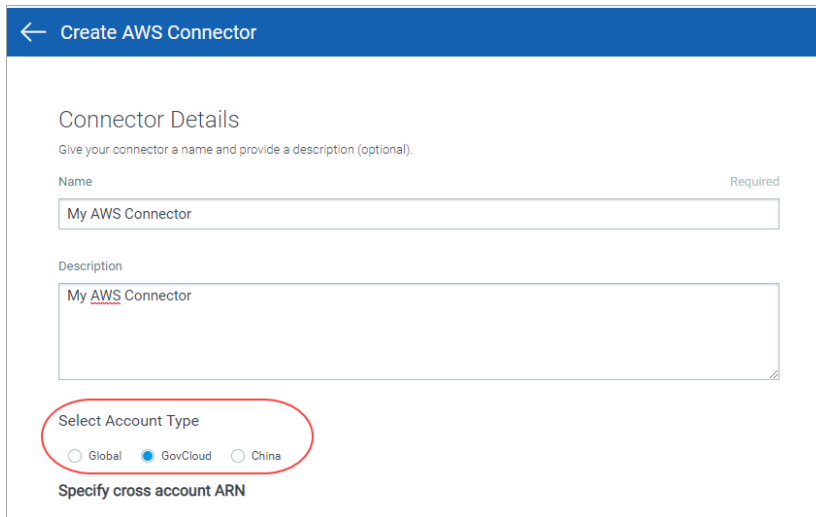
GovCloud and China Support for AWS

You can now discover and assess resources from GovCloud and China region. We have added a new option in connector creation process to choose account types: GovCloud or China.

You can create connector for each account type (Global, GovCloud, or China) and start discovering resources from each region and evaluate them against policies. If you do not see China region available in base account creation, submit a Qualys support ticket to have this enabled for your subscription.

Tell me the steps

Go to the Configuration > Amazon Web Services and then click Create Connector. Enter a name and description (optional) for your connector.



Select an account type for your connector: Global, GovCloud or China. You can choose only one account type per connector.

Note: If you plan to use connector for China account type, ensure that you set up a base account.

Provide other connector details as needed.

Click Create Connector.

That's it! The connector will establish a connection with AWS to start discovering resources from each region and evaluate them against policies.

All controls for AWS also support GovCloud except the controls CID 15, CID 16, and CID 107, which are not applicable for GovCloud region.

Inventory Support for Lambda Function Resource

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

Go to Resources tab and you can view the newly supported resource in the List View.

The screenshot shows the CloudView interface with the 'RESOURCES' tab selected. On the left, a sidebar displays '14 Total Resource Types' and lists various AWS resources categorized by ACCOUNT, RESOURCE TYPE, and REGIONS. The main area shows a table of resources with columns: RESOURCE TYPE, SERVICE, TOTAL RESOURCES, and RESOURCES FAILED. The 'Lambda Function' resource is highlighted with a red circle, and a red arrow points to it from the text 'New Resource Type Support'.

RESOURCE TYPE	SERVICE	TOTAL RESOURCES	RESOURCES FAILED
RDS	RDS	63	0
Network ACL	VPC	182	0
S3 Bucket	S3	247	0
IAM User	IAM	1.80K	0
VPC	VPC	143	0
Security Group	VPC	1.41K	0
Lambda Function	Lambda Function	169	169
Subnet	VPC	399	0
Internet Gateway	VPC	120	0

New Controls Added in AWS Best Practices Policy

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

Note: The controls CID 15, CID 16, and CID 107 are not applicable for GovCloud region.

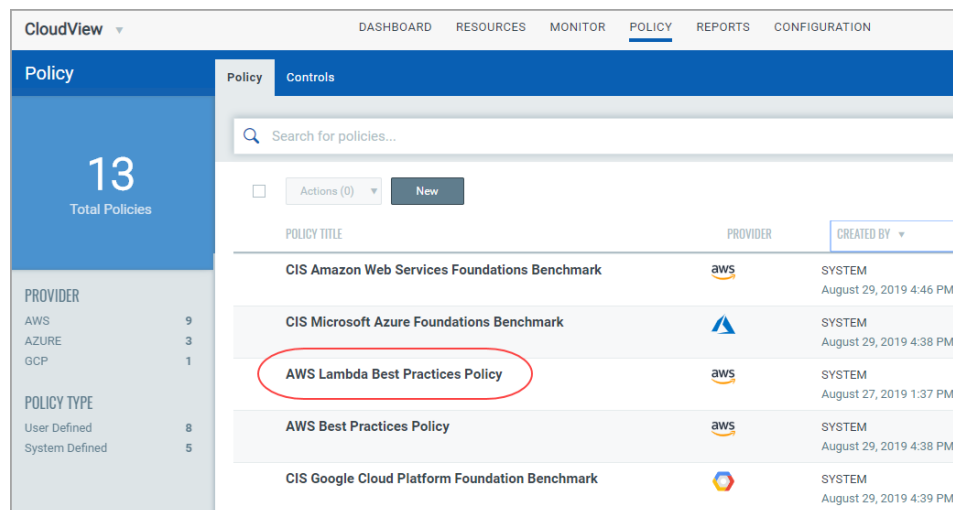
CID	Resource	Control Title
69	RDS	Ensure automated backups are enabled for RDS database instances
70	RDS	Ensure that Deletion Protection is enabled for RDS DB Cluster
71	RDS	Ensure that Deletion Protection is enabled for RDS Database instances
72	RDS	Ensure that IAM Database Authentication is Enabled for the DB Cluster
73	RDS	Ensure that IAM Database Authentication is Enabled for the DB Instances
74	RDS	Ensure that AWS RDS Log Exports is enabled for DB Cluster
75	RDS	Ensure that AWS RDS Log Exports is enabled for DB Instances
76	RDS	Ensure that RDS Database Master username is not set to well-known/default
77	RDS	Ensure VPC security group attached to RDS Database Instance does not allows Inbound traffic from ANY source IP
78	RDS	Ensure RDS DB instances are not present in public subnets
79	RDS	Ensure RDS DB Cluster are not present in public subnets
80	RDS	Ensure Event Subscriptions for Instance Level Events is Enabled for DB Instances
81	RDS	Ensure RDS Microsoft SQL instance enforces encrypted connections only
82	RDS	Ensure RDS PostgreSQL instance enforces encrypted connections only
83	RDS	Ensure RDS PostgreSQL Cluster enforces encrypted connections only
84	RDS	Ensure that Encryption is enabled for the RDS DB Cluster
85	RDS	Ensure RDS DB Cluster snapshots are encrypted
86	RDS	Ensure CMK is used to protect RDS DB Cluster encryption key
87	RDS	Ensure CMK is used to protect RDS Db Instance encryption key
88	RDS	Ensure DB instance replication is set to the another Zone for High Availability
89	RDS	Ensure that DB Cluster replication is set to the another Zone for High Availability
90	RDS	Ensure RDS database Cluster snapshots are not public
91	RDS	Ensure that Enhance monitoring is enabled for RDS Database Instance
92	RDS	Ensure that AWS RDS DB Cluster with copy tags to snapshots option is enabled
93	RDS	Ensure AWS RDS instances with copy tags to snapshots option is enabled
94	RDS	Ensure Event Subscriptions for cluster Level Events is Enabled for DB Clusters
95	RDS	Ensure MYSQL DB Instance backup Binary logs configuration is not enabled
96	RDS	Ensure backup configuration is enabled for MSSQL DB Instances

Control Updated

We have updated AWS control CID 24. While evaluating CID24, the CloudTrail log bucket configured in different AWS account (other than CloudView connector) triggers authentication errors in AWS account. We now prevent any other API calls to the S3 resources from accounts other than the connector.

New Best Practice Policy for Lambda Function

We have introduced AWS Lambda Best Practices Policy specifically for Lambda resources. The pre-defined system policy is loaded with 11 system-defined controls.



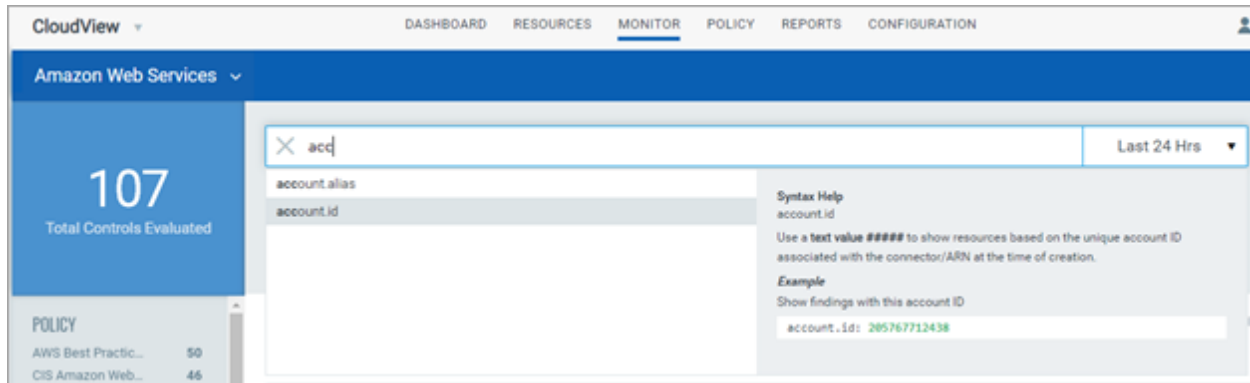
New Controls for Lambda Function

We have also introduced 11 new controls for Lambda Function in AWS Lambda Best Practices Policy. You can view control evaluation in Monitor tab and control details in Policies tab.

CID	Resource	Control Name
97	Lambda	Ensure that Lambda function has tracing enabled
98	Lambda	Ensure that Lambda Function is not using An IAM role for more than one Lambda Function
99	Lambda	Ensure that Multiple Triggers are not configured in Lambda Function
100	Lambda	Ensure that Lambda Runtime Version is latest and not custom
101	Lambda	Ensure that Lambda function does not have Admin Privileges
102	Lambda	Ensure that Lambda function does not have Cross Account Access
103	Lambda	Ensure that Lambda Environment Variables at-rest are encrypted with CMK
104	Lambda	Ensure that Lambda Environment Variables are encrypted using AWS encryption helpers for encryption in transit
105	Lambda	Ensure that Lambda function is not Exposed (Ensure that Lambda function does not allows anonymous invocation)
106	Lambda	Ensure that VPC access for Lambda Function is not set to default(Null)
107	Lambda	Ensure that AWS Lambda excess Permissions are removed
		Note: This control is not applicable for GovCloud region.

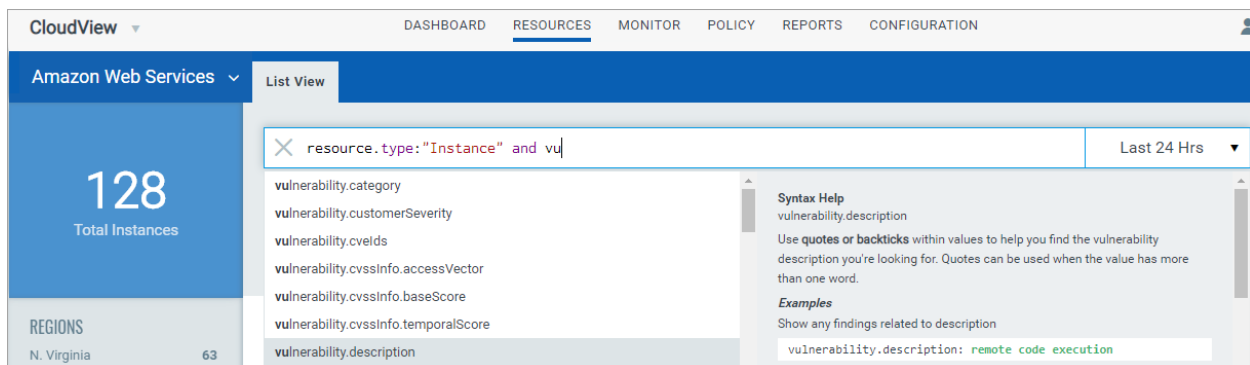
Search Resources Using Account Alias

We now fetch the account alias details from AWS. You can view the account alias details using our new token `account.alias` in the simplified search for a resource in AWS. In Monitor tab, you can search AWS resources with their alias names rather than `account.id` or any other property.



Identifying Instances with Vulnerability Using Search Tokens

We have introduced several new tokens to find vulnerabilities on instances having vulnerability scan results from Qualys scanners or Cloud Agent.



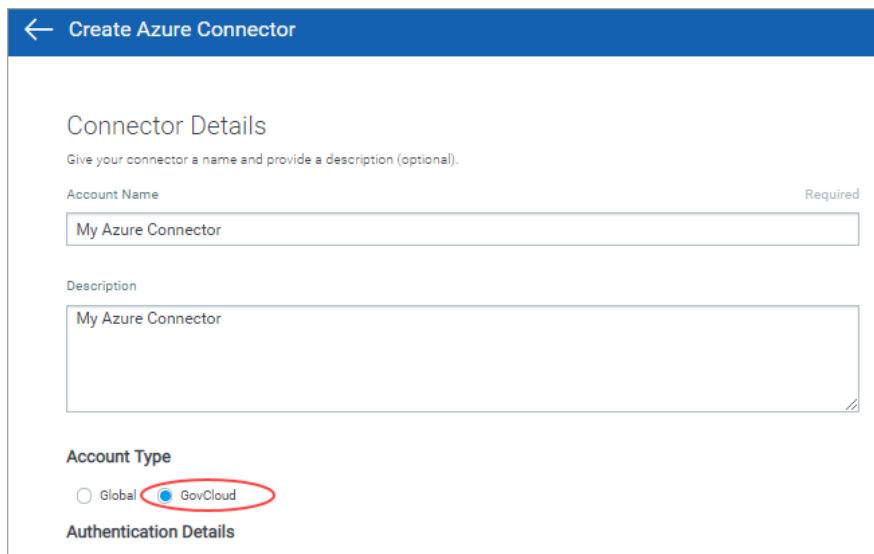
Microsoft Azure Updates

GovCloud Support for Azure Connectors

You can now discover and assess resources in GovCloud region. We have added a new option in Azure connector creation process to choose account type: GovCloud. You can create connectors for each account type (Global or GovCloud) and start discovering resources from Global and GovCloud region and evaluate them against policies.

Tell me the steps

Go to the Configuration > Microsoft Azure and then click Create Connector. Enter a name and description (optional) for your connector.



← Create Azure Connector

Connector Details
Give your connector a name and provide a description (optional).

Account Name Required
My Azure Connector

Description
My Azure Connector

Account Type
☐ Global ☒ GovCloud

Authentication Details

Select an account type for your connector: Global, GovCloud. You can choose only one account type per connector.

Provide other connector details for Azure as needed.

Click Create Connector.

That's it! The connector will establish a connection with Azure to start discovering resources from each region and evaluate them against policies.

New Controls for CIS Microsoft Azure Foundations Benchmark

We have now added 38 new controls to the policy titled CIS Microsoft Azure Foundations Benchmark for Microsoft Azure. All the scored controls from CIS for Microsoft Azure Foundations Benchmarks v1.1.0 are now supported within CIS policy for Azure.

Navigate to Policy > Policy tab and then click CIS Microsoft Azure Foundations Benchmark. You can view the policy information and the all the controls associated with the policy.

New Controls

We have added the following controls to the CIS Microsoft Azure Foundations Benchmark Policy.

Note: The newly added control CID 50046 is not applicable for Azure GovCloud.

CID	CIS Reference	Resource	Control Title
50033	7.1, 7.2	Virtual Machine	Ensure that all attached VM Data disks are encrypted
50039	4.11	SQL	Ensure 'Enforce SSL connection' is set to 'ENABLED' for MySQL Database Server
50040	4.13	SQL	Ensure 'Enforce SSL connection' is set to 'ENABLED' for PostgreSQL Database Server
50041	4.12	SQL	Ensure server parameter 'log_checkpoints' is set to 'ON' for PostgreSQL Database Server
50042	4.14	SQL	Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL Database Server
50043	4.15	SQL	Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server
50044	4.16	SQL	Ensure server parameter 'log_duration' is set to 'ON' for PostgreSQL Database Server
50045	4.18	SQL	Ensure server parameter 'log_retention_days' is greater than 3 days for PostgreSQL Database Server
50046	8.5	Kubernetes	Enable RBAC within Azure Kubernetes Services
			Note: This control is not applicable for GovCloud

CID	CIS Reference	Resource	Control Title
50047	9.1	App service	Ensure App Service Authentication is set on Azure App Service
50048	9.2	App service	Ensure web app redirects all HTTP traffic to HTTPS in Azure App Service
50049	9.4	App service	Ensure web app has 'Client Certificates (Incoming client certificates)' set to 'On'
50050	9.5	App service	Ensure that 'Register with Azure Active Directory' is enabled on App Service
50051	9.3	App service	Ensure web app is using the latest version of TLS encryption version
50052	3.7	Storage Accounts	Ensure default network access rule for Storage Accounts is set to deny
50053	3.8	Storage Accounts	Ensure 'Trusted Microsoft Services' is enabled for Storage Account access
50054	5.1.7	Key vault	Ensure that logging for Azure KeyVault is 'Enabled'
50055	6.4	Network - NSG	Ensure Network Security Group Flow Log retention is greater than 90 days
50056	5.1.6	Activity Logging	Ensure Storage account containing container with activity logs is encrypted with BYOK
50061	9.10	App service	Ensure that 'HTTP Version' is latest, if used to run the web app
50062	6.5	Network	Ensure Network Watcher is Enabled for your Subscription
50063	5.2.1	Monitor	Ensure Activity Log Alert exists for Create Policy Assignment
50064	5.2.2	Monitor	Ensure Activity Log Alert exists for Create or Update Network Security Group
50065	5.2.3	Monitor	Ensure Activity Log Alert exists for Delete Network Security Group
50066	5.2.4	Monitor	Ensure Activity Log Alert exists for Create or Update Network Security Group Rule
50067	5.2.5	Monitor	Ensure Activity Log Alert exists for Delete Network Security Group Rule
50068	5.2.6	Monitor	Ensure Activity Log Alert exists for Create or Update Security Solution
50069	5.2.7	Monitor	Ensure Activity Log Alert exists for Delete Security Solution
50070	5.2.8	Monitor	Ensure Activity Log Alert exists for Create or Update SQL Server Firewall Rule
50071	5.2.9	Monitor	Ensure Activity Log Alert exists for Update Security Policy
50072	1.3	Azure AD/IAM	Ensure that there are no guest users
			Note: This control is not applicable for GovCloud. Select Application Permission and expand User permissions and select User.Read.All permission and click Add permissions instead of AccessReview.Read.All permission as mentioned in the online help and connector creation steps in CloudView UI.

CID	CIS Reference	Resource	Control Title
50073	1.23	Azure AD/IAM	Ensure no custom subscription owner roles are created
50074	4.17	SQL	Ensure server parameter 'connection_throttling' is set to 'ON' for PostgreSQL Database Server
50075	5.1.7	Key vault	Ensure that diagnostic settings for Azure KeyVault is set to ON
50076	5.1.5	Activity Logging	Ensure storage container storing activity logs is not publicly accessible
50079	2.1	Security Center	Ensure that Standard pricing tier is enabled for PaaS SQL servers
50080	2.1	Security Center	Ensure that Standard pricing tier is enabled for App Service
50081	2.1	Security Center	Ensure that Standard pricing tier is enabled for Storage Accounts

New Azure Best Practices Policy

We have now introduced a new policy for Azure titled Azure Best Practices Policy. Currently the policy evaluates the following 5 new controls.

CID	Resource	Control Name
50038	Snapshot	Ensure disk snapshots are encrypted.
50077	Security Center	Ensure that Settings - Threat Detection for Microsoft Cloud App Security (MCAS) is selected
50078	Security Center	Ensure that Settings - Threat Detection for Windows Defender ATP (WDATP) is selected
50083	Security Center	Ensure that ADS - Vulnerability Assessment (VA) is enabled and configured properly
50082	Security Center	Ensure any of the ASC Default policy setting is not set to 'Disabled'

Azure 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.

CID	Resource	Old Title	New Title
50003	Security Center	Ensure that 'Adaptive Application Controls' is set to On	Ensure that Adaptive Application Controls is set to On
50005	Security Center	Ensure that 'System updates' is set to On	Ensure that System updates should be installed on your machines is set to On
50006	Security Center	Ensure that 'Security Configurations' is set to On	Ensure that Vulnerabilities in security configuration on your machines should be remediated is set to On
50007	Security Center	Ensure that Endpoint protection is set to On	Ensure that Monitor missing Endpoint Protection in Azure Security Center is set to On
50008	Security Center	Ensure that 'Disk encryption' is set to On	Ensure that Disk encryption should be applied on virtual machines is set to On
50010	Security Center	Ensure that 'Web application firewall' is set to On	Ensure that NSGs rules for web applications on IaaS should be hardened is set to On
50014	Security Center	Ensure that 'SQL auditing' is set to On	Ensure that Monitor unaudited SQL databases in Azure Security Center is set to On
50015	Security Center	Ensure that standard pricing tier is selected	Ensure that Standard pricing tier is enabled for Virtual Machines
50016	Security Center	Ensure that 'Next generation firewall' is set to On	Ensure that Access through Internet facing endpoint should be restricted is set to On
50017	Security Center	Ensure that 'Vulnerability assessment' is set to On	Ensure that Vulnerabilities in security configuration on your machines should be remediated is set to On
50018	Security Center	Ensure that 'Storage Encryption' is set to On	Ensure that Audit missing blob encryption for storage account is set to On
50019	Security Center	Ensure that 'JIT Network Access' is set to On	Ensure that Just-In-Time network access control should be applied on virtual machines is set to On
50025	Security Center	Ensure that 'SQL Encryption' is set to On	Ensure that Monitor unencrypted SQL databases in Azure Security Center is set to On

GCP

New Controls in CIS Google Cloud Platform Foundation Benchmark

We have added 21 new controls to CIS Google Cloud Platform Foundation Benchmark Policy. The control list is given below.

CID	CIS Reference	Resource	Control Title
52000	1.1	IAM	Ensure that corporate login credentials are used instead of Gmail accounts
52002	1.4	IAM	Ensure that ServiceAccount has no Admin privileges.
52003	1.5	IAM	Ensure that IAM users are not assigned Service Account User role at project level
52004	1.6	IAM	Ensure user-managed/external keys for service accounts are rotated every 90 days or less
52005	1.8	IAM	Ensure Encryption keys are rotated within a period of 365 days
52006	1.9	IAM	Ensure that Separation of duties is enforced while assigning KMS related roles to users
52008	2.1	Logging	Ensure that Cloud Audit Logging is configured properly across all services and all users from a project
52019	3.1	Networks	Ensure the default network does not exist in a project
52021	3.6	Firewall	Ensure that SSH access is restricted from the internet
52022	3.7	Firewall	Ensure that RDP access is restricted from the internet
52025	4.1	VM	Ensure that instances are not configured to use the default service account with full access to all Cloud APIs
52026	4.2	VM	Ensure "Block Project-wide SSH keys" enabled for VM instances
52027	4.3	VM	Ensure oslogin is enabled for a Project
52028	4.4	VM	Ensure 'Enable connecting to serial ports' is not enabled for VM Instance
52033	6.2	SQL	Ensure that Cloud SQL database Instances are not open to the world
52035	6.4	SQL	Ensure that MySQL Database Instance does not allows root login from any Host
52036	7.1	Kubernetes	Ensure Stackdriver Logging is set to Enabled on Kubernetes Engine Clusters
52048	7.16	Kubernetes	Ensure Private Google Access is set on Kubernetes Engine Cluster Subnets
52050	7.18	Kubernetes	Ensure Kubernetes Clusters created with limited service account Access scopes for Project access
52051	7.3	Kubernetes	Ensure Stackdriver Monitoring is set to Enabled on Kubernetes Engine Clusters

Customizing Out of the Box Control Parameter Values and Criticality

We allow you to customize the controls to suit your need and associate them with the policy. You can now customize control parameters and change criticality of existing controls.


We now provide to build your own policies by adding the required controls to it. You could either use the pre-defined controls or change parameter values of pre-defined control to make your own user-defined controls.


Customize Controls

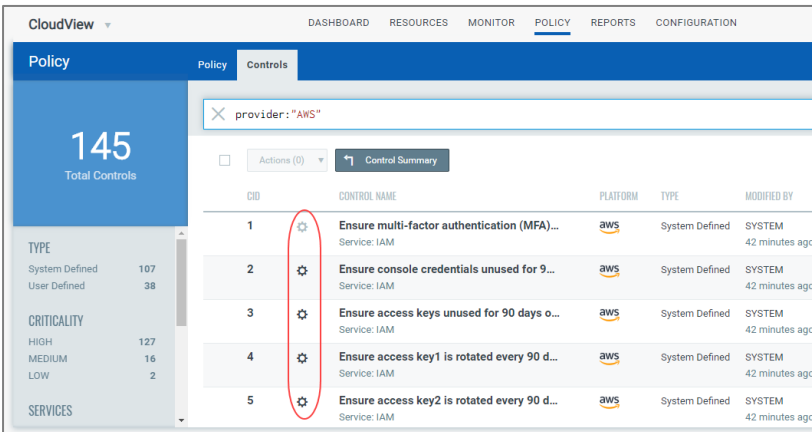
Controls are the building blocks of the policies used to measure and report compliance for a set of cloud resources. We provide many controls for you to choose from and you can customize them too. Controls play the key part in the compliance posture of resource.

System Defined Controls

System-defined Control is a predefined control provided by Qualys. Few system-defined controls are customizable while others are not. The control indicator icon tells us if the control is customizable or not.

 - control cannot be customized.

 - control can be customized to suit your need.



CID	CONTROL NAME	PLATFORM	TYPE	MODIFIED BY
1	Ensure multi-factor authentication (MFA)...	aws	System Defined	SYSTEM 42 minutes ago
2	Ensure console credentials unused for 9...	aws	System Defined	SYSTEM 42 minutes ago
3	Ensure access keys unused for 90 days o...	aws	System Defined	SYSTEM 42 minutes ago
4	Ensure access key1 is rotated every 90 d...	aws	System Defined	SYSTEM 42 minutes ago
5	Ensure access key2 is rotated every 90 d...	aws	System Defined	SYSTEM 42 minutes ago

Use our new search query token “iscustomizable: yes” to view all controls that are customizable.

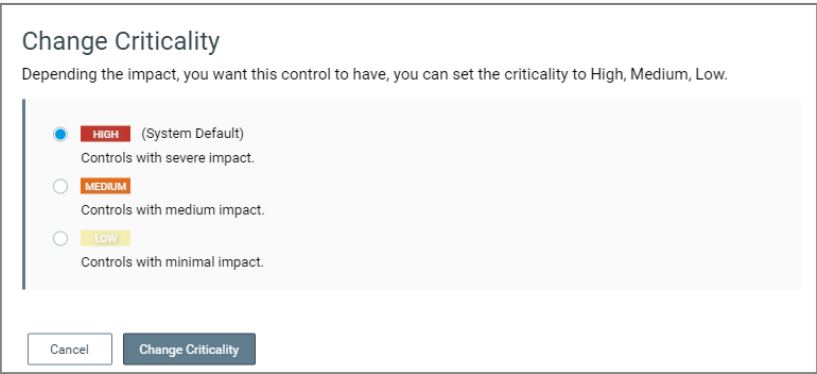
User-Defined Controls

You can copy any system-defined control to make your own user-defined controls that you can customize to meet your needs.

Control Criticality

You can modify the criticality of any control to suit your need. If the control criticality needs to be changed to match your environment, you can select the control, select Change Criticality from quick action menu.

Select the criticality you want to assign to the control and click Change Criticality.



Change Criticality


Depending the impact, you want this control to have, you can set the criticality to High, Medium, Low.

☒ **HIGH** (System Default)
Controls with severe impact.

☐ **MEDIUM**
Controls with medium impact.

☐ **LOW**
Controls with minimal impact.

Copy Control and Customize

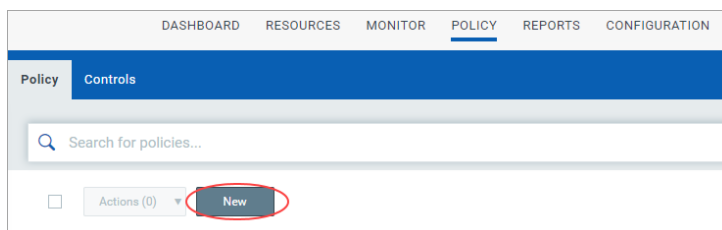
Go to Policy > Controls and select the control to be customized, select Copy Control from the quick action menu. The  icon indicates that the control is customizable. You can then modify the parameters of the control as per your requirement and save the customized control. The customized control is available to associate with policy and evaluate the resources.

Build Your Own Policy

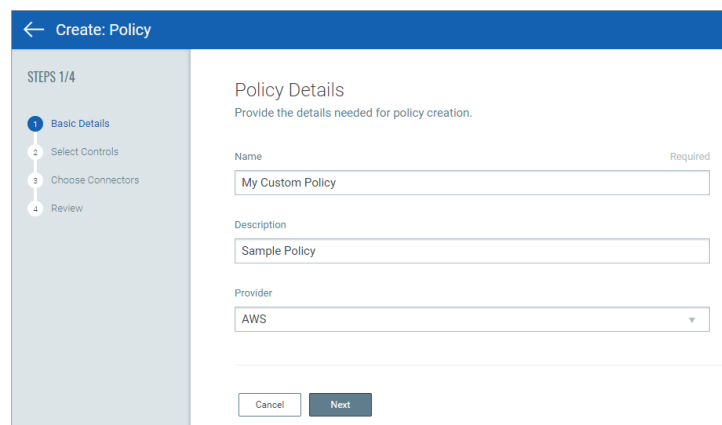
A policy is a collection of controls used to measure and report compliance for a set of resources. You can create your own custom policy and associate the required the controls to be evaluated for the custom policy.

Set Up Your Own Policy (Custom Policy)

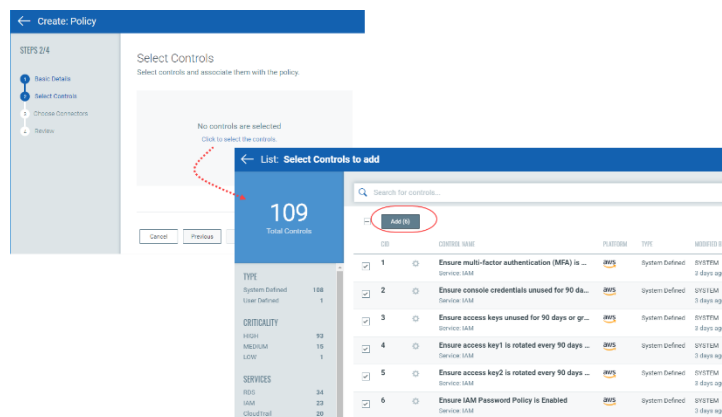
Navigate to Policy > Policy > New.



Provide the basic details for the custom policy such as name, description and select the cloud provider. Click Next



Select the controls to be associated with the policy and click Add. Click Next.



You can associate system-defined controls or create your own custom control using existing control to suit your need.

Select the connector groups or connectors that should be analyzed for policy compliance. Click Next.

That's it. Your custom policy is ready to use.

The screenshot shows the 'Create Policy' wizard in Qualys Express. The left sidebar indicates the current step is '3 Choose Connectors' out of 4 steps. The main area is titled 'Choose Connectors' and instructs the user to select connectors for analysis. It includes two dropdown menus: 'Groups' and 'Connectors'. At the bottom, there are 'Cancel', 'Previous', and 'Next' buttons.

Qualys Express

← Create Policy

STEPS 3/4

- 1 Basic Details
- 2 Select Controls
- 3 Choose Connectors
- 4 Review

Choose Connectors

Tell us the connectors you want to analyze for compliance with this policy.

You can select a combination of groups and connectors, and we'll evaluate the policy against all matching connectors.

Groups

Select the Groups...

Connectors

Select the Connectors...

Cancel Previous Next

Group Connectors and Assign Access to Sub Users

You can now control access to connectors for sub users with the usage of groups. The groups help you to organize your connectors and to manage user access to them.

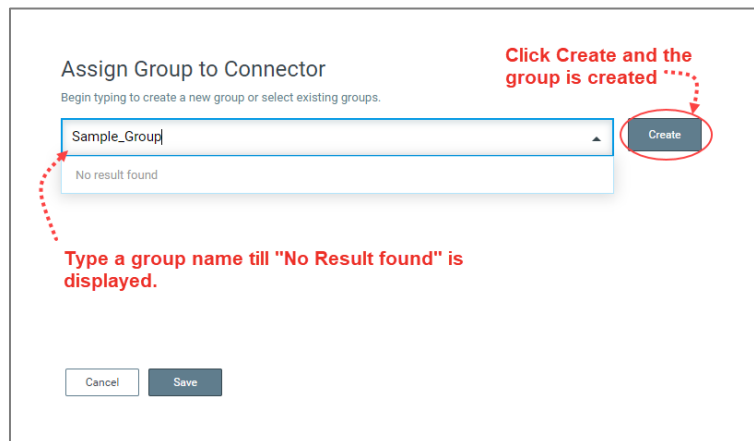
Assigning Groups to Connector

You can apply groups to connectors and form connector groups that can represent your business units or departments.

Note: Only user with Manager role can create and assign groups to connectors.

To create and assign a group to the connector, navigate to Configuration tab and then the Cloud Provider (AWS, Azure, or GCP).

Choose the connector for which you want to assign group and click Assign Group from the quick action menu. Type a name for the group and click Create and then click Save.



Assign Group to Connector
Begin typing to create a new group or select existing groups.

Sample_Group

No result found

Click Create and the group is created

Type a group name till "No Result found" is displayed.

Cancel Save

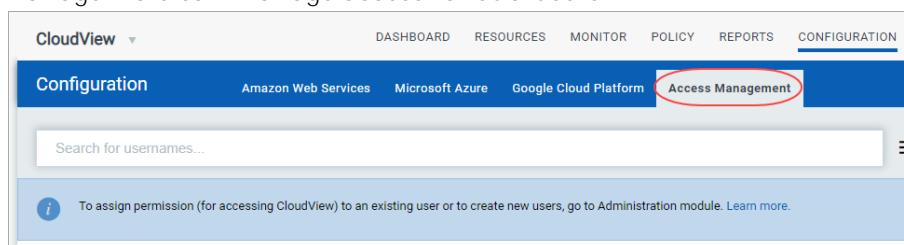
The group is created and associated with the connector. You can associate a group with one or more connectors.

Managing Access for Sub User

The user with Manager role can now assign access to sub users and decide which connectors are accessible to sub users. The Access Management tab lists all the sub users who can access the CloudView module.

If you do not see any sub users, you can create sub users. To create new sub user, visit the Administration utility and create new users and assign role to each user.

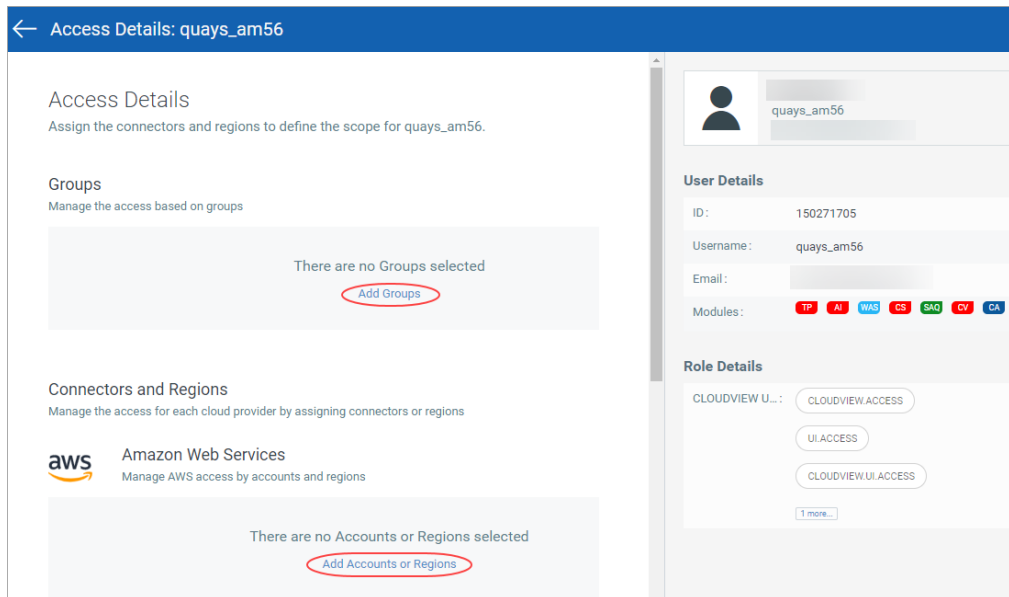
Note: The Access Management tab is available only to user with Manager role. The user with Manager role can manage access for sub-users.



How do I manage access for sub users?

Navigate to the Access Management tab, select the user and choose Manage Access from the quick action menu.

There are two options you could configure access for sub users:



- Using groups

To assign the groups to a sub user, you need to associate the group with the user.

Click Add Groups and select the group, and click Save to associate the group with the user.

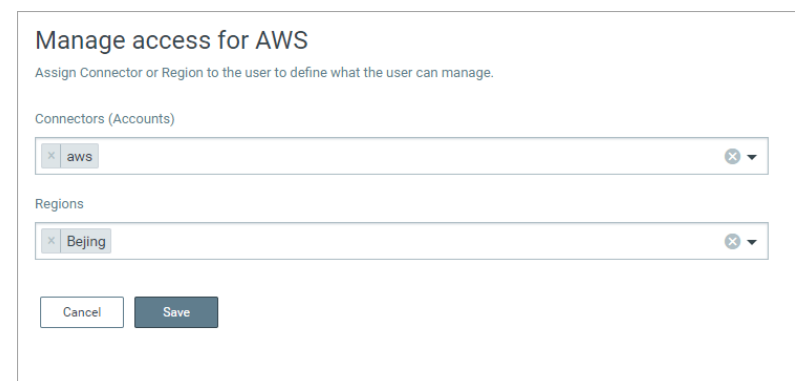
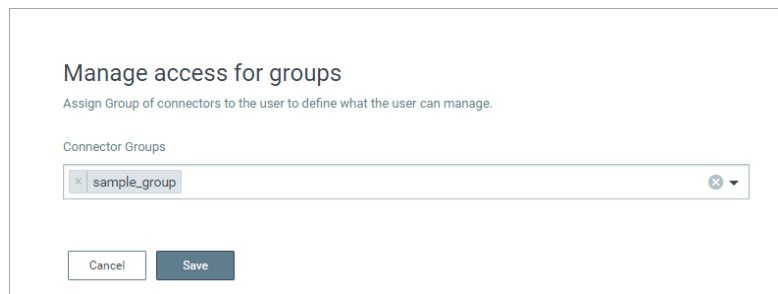
If a group is assigned to multiple connectors that belong to different Cloud Providers, the user can access all the connectors associated with the groups.

- Using connectors

When you define scope for a sub user, you could directly select the connectors for every Cloud Provider and associate it with the sub user. The sub user can then access all the connectors assigned to the sub user.

In the Connectors and Regions section, click the link for the specific Cloud Provider and then select the connector, and click Save.

You can select multiple connectors from multiple cloud providers as well. For AWS, you can select connector and region as well.



Enhanced Details for Instance type of Resource

We now show you additional details for instance type of resources in CloudView. The additional details include resource inventory, security details, compliance details, and sensor details.

Few points to note for the resource details to be visible:

- The details are displayed for only Instance type of resources.
AWS: Instance, Azure: Virtual Machine, GCP: VM Instances
- The resource (asset) must also be detected during Qualys scan or must have Qualys Cloud Agent installed on it. The resource (asset) must be available in Qualys Cloud Platform (AssetView).
- If the resource has Qualys Cloud Agent installed, the Agent Summary section displays corresponding details.

Where can I view the details?

Go to Resources and then select the Cloud Provider (AWS, Azure, or Google Cloud Platform). Now, select the resource of instance type and click the resource. The Resource Details page displays the enhanced details.

Resource Details: i-0fd5ad25d4aef1161

Summary

Instance **i-0fd5ad25d4aef1161**
First Discovered On: September 5, 2019 11:38 AM

Vulnerabilities

100 %
0 %
Potential: 1
Confirmed: 0

Associations

Security Group: 1
Auto Scaling Group: 0
Load Balancer: 0

General:

Instance Name: EC2_Plus_Agent1_qualys_b43
Instance ID: i-0fd5ad25d4aef1161
Instance Type: t2.micro
First Discovered On: September 5, 2019 11:38 AM
Instance Status: -
State: running
Spot Instance: -
Image (AMI) ID: ami-0cfee17793b08a293
Last Updated On: September 10, 2019 2:18 PM

Location:

Account ID: 383031256652
Region: N. Virginia (us-east-1)
Availability Zone: us-east-1b

Network:

VPC ID: vpc-caace657
Subnet ID: subnet-b358299f
DNS (Private): ip-172-31-85-154.ec2.internal
DNS (Public): ec2-52-55-244-224.compute-1.amazonaws.com
IP Address (Public): 52.55.244.224
IP Address (Private): 172.31.85.154

Note: If the resource does not exist in Qualys Cloud Platform, the View Mode is displayed for the resource.

Resource Details: i-0bfab06114a91e901

Summary

Instance **i-0bfab06114a91e901**
First Discovered On: September 10, 2019 9:10 AM

Associations

Security Group: 1
Auto Scaling Group: 0
Load Balancer: 0

General:

Instance Name: Test-scan-4
Instance ID: i-0bfab06114a91e901
Instance Type: t2.medium
First Discovered On: September 10, 2019 9:10 AM
Instance Status: -
State: running
Spot Instance: -
Image (AMI) ID: ami-0c566de751b1be85a
Last Updated On: September 10, 2019 1:38 PM

Location:

Account ID: 205767712438
Region: Canada Central (ca-central-1)
Availability Zone: ca-central-1b

Network:

VPC ID: vpc-2f638f46
Subnet ID: subnet-bc2929eca
DNS (Private): ip-172-31-14-85.ca-central-1.com

Issues addressed in this release

We have fixed the following issues:

- Users can now successfully download data list with 10000 records in CSV format.
- Recently Azure updated option/setting names for Azure Security Center. We have updated the static content for CIDs 50003, 50006-50008, 50010, 50014-50019 to match with the changes on Azure portal. The static content updated for the controls include title, summary, specification, evaluation, rationale, remediation, references.
- The Azure disk encryption extension, if running on older version of Azure VM, fails to update correct encryption status for VM disk on disk API resulting into false positive evaluations. Although older versions of Azure disk encryption extension on VM is not recommended, we have implemented fix to support such scenarios and suppress all such false positives.

CID50032 checked encryption setting for every VM disk (OS, Data, Unattached) within subscription. To support the above case, we have now split the logic in two different controls. CID50032 evaluates for OS and Data disks attached to the VM instances and the new control CID 50033 only evaluates for unattached disks within the subscription.

- We have updated the steps for Azure connector creation on UI to match the steps updated on Azure portal. We have updated the online help as well.
- The Cloud formation template to create cross-account access IAM role is now updated so that users can add connectors without any error.
- We now display details about Network Interfaces for Instance type of resources in Resource Details page. Earlier, although this information was fetched by the connectors, it was not displayed in the Resource Details page.