Qualys CloudView v1.x

Version 1.9.1.0

December 17, 2019

Here's what's new in Qualys CloudView 1.9.1!

Amazon Web Services

AWS Control Updates

Microsoft Azure

Azure Control Updates

Google Cloud Platform

GCP Control Updates

Common Features

Search Using Resource Parameter Information

Qualys CloudView 1.9.1 brings you many more Improvements and updates! Learn more

Control Updates

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

AWS Control Updates

CID	Resource	Title	Sections Updated
3	IAM	Ensure access keys unused for 90 days or greater are disabled	Remediation
4	IAM	Ensure access key1 is rotated every 90 days or less	Remediation
5	IAM	Ensure access key2 is rotated every 90 days or less	Remediation
8	IAM	Ensure IAM password policy require at least one lowercase letter	Remediation
9	IAM	Ensure IAM password policy require at least one symbol	Remediation
10	IAM	Ensure IAM password policy require at least one number	Remediation
11	IAM	Ensure IAM password policy requires minimum length of 14 or greater	Remediation
12	IAM	Ensure IAM password policy prevents password reuse	Remediation
13	IAM	Ensure IAM password policy expires passwords within 90 days or less	Rationale
17	IAM	Ensure IAM policies are attached only to groups or roles	Remediation
18	IAM	Avoid the use of the root account	Remediation
19	CLOUD_TRAIL	Ensure CloudTrail is enabled in all regions	Remediation
20	CLOUD_TRAIL	Ensure CloudTrail log file validation is enabled	Remediation
23	CONFIG	Ensure AWS Config is enabled in all regions	Remediation
25	CLOUD_TRAIL	Ensure CloudTrail logs are encrypted at rest using KMS CMKs	Remediation
26	CLOUD_TRAIL	Ensure rotation is enabled for customer created CMK with AWS managed key material	Remediation
41	VPC	Ensure no security groups allow ingress from 0.0.0.0/0 to port 22	Remediation
42	VPC	Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389	Remediation
45	S3	S3 Bucket Access Control List Grant Access to Everyone or Authenticated Users	Reference Added
46	S3	S3 Bucket Policy Grant Access to Everyone	Reference Added

47	S3	Ensure access logging is enabled for S3 buckets	Reference Added
48	S3	Ensure versioning is enabled for S3 buckets	Reference Added
56	RDS	Ensure database Instance is not listening on to a standard/default port	Reference Added, Fail text
58	IAM	Ensure that the key expiry is set for CMK with external key material	Remediation
59	S3	Ensure Block new public bucket policies" for a bucket is set to true"	Remediation and Specification
60	S3	Ensure that Block public and cross-account access" if bucket has public policies for bucket is set to true"	Remediation and Specification
61	S3	Ensure that Block new public ACLs and uploading public objects" for a bucket is set to true."	Remediation and Specification
62	S3	Ensure that Remove public access granted through public ACLs" for a bucket is set to true"	Remediation and Specification
63	S3	Ensure Block new public bucket policies" for an account is set to true"	Remediation and Specification
64	S3	Ensure that Block public and cross-account access" if bucket has public policies for the account is set to true"	Remediation and Specification
65	S3	Ensure that Block new public ACLs and uploading public objects" for the account is set to true"	Remediation and Specification
66	S3	Ensure that Remove public access granted through public ACLs" for the account is enabled"	Remediation and Specification
98	Lambda Function	Ensure that Lambda Function is not using An IAM role for more than one Lambda Function	Reference
99	Lambda Function	Ensure that Multiple Triggers are not configured in Lambda Function	Specifications, Evaluation
100	Lambda Function	Ensure that Lambda Runtime Version is latest and not custom	Specifications, Evaluation, Rationale
101	Lambda Function	Ensure that Lambda function does not have Admin Privileges	Reference
102	Lambda Function	Ensure that Lambda function does not have Cross Account Access	Remediation
103	Lambda Function	Ensure that Lambda Environment Variables at-rest are encrypted with CMK	Specifications, Evaluation
104	Lambda Function	Ensure that Lambda Environment Variables are encrypted using AWS encryption helpers for encryption in transit	Specifications, Evaluation
105	Lambda Function	Ensure that Lambda function does not allows anonymous invocation	Specifications, Evaluation
107	Lambda Function	Ensure that AWS Lambda excess Permissions are removed	Reference Added

Azure Control Updates

CID	Resource	Title	Sections Updated
50002	SQL Servers	Ensure no SQL Servers allow ingress from Internet (ANY IP)	Remediation
50003	Security Center	Ensure that Adaptive Application Controls is set to On	Evaluation text, Rationale, Remediation, Pass/Fail text
50004	Security Center	Ensure that Automatic provisioning of monitoring agent is set to On	Remediation
50006	Security Center	Ensure that Vulnerabilities in security configuration on your machines should be remediated is set to On	Evaluation text, Rationale, Remediation, Pass/Fail text
50007	Security Center	Ensure that Monitor missing Endpoint Protection in Azure Security Center is set to On	Evaluation text, Rationale, Remediation, Pass/Fail text
50008	Security Center	Ensure that Disk encryption should be applied on virtual machines is set to On	Evaluation text, Rationale, Remediation, Pass/Fail text
50009	Security Center	Ensure that Network security groups is set to On	Evaluation text, Rationale, Remediation, Pass/Fail text
50010	Security Center	Ensure that NSGs rules for web applications on IaaS should be hardened is set to ON	Evaluation text, Rationale, Remediation, Pass/Fail text
50012	Storage Account	Ensure that Public access level is set to Private for blob containers	Remediation
50014	Security Center	Ensure that Monitor unaudited SQL databases in Azure Security Center is set to On	Evaluation text, Rationale, Remediation, Pass/Fail text
50016	Security Center	Ensure that Access through Internet facing endpoint should be restricted is set to On	Evaluation text, Rationale, Remediation, Pass/Fail text
50017	Security Center	Ensure that Vulnerabilities in security configuration on your machines should be remediated is to On	Evaluation text, Rationale, Remediation, Pass/Fail text
50018	Security Center	Ensure that Audit missing blob encryption for storage account is set to On	Evaluation text, Rationale, Remediation, Pass/Fail text
50019	Security Center	Ensure that Just-In-Time network access control should be applied on virtual machines is set to On	Evaluation text, Rationale, Remediation, Pass/Fail text
50024	Monitor	Ensure that Just-In-Time network access control should be applied on virtual machines is set to On	Remediation
50025	Security Center	Ensure that Monitor unencrypted SQL databases in Azure Security Center is set to On	Evaluation text, Rationale, Remediation, Pass/Fail text
50038	Snapshot	Ensure that all disk snapshots are encrypted	Specification and References
50076	Activity Log	Ensure storage container storing activity logs is not publicly accessible	Remediation
50077	Security Center	Ensure that Settings - Threat Detection for Microsoft Cloud App Security (MCAS) is selected	Remediation

50078	Security Center	Ensure that Settings - Threat Detection for Windows Defender ATP (WDATP) is selected	Remediation
50083	SQL Servers	Ensure that ADS - Vulnerability Assessment (VA) is enabled and configured properly	Remediation

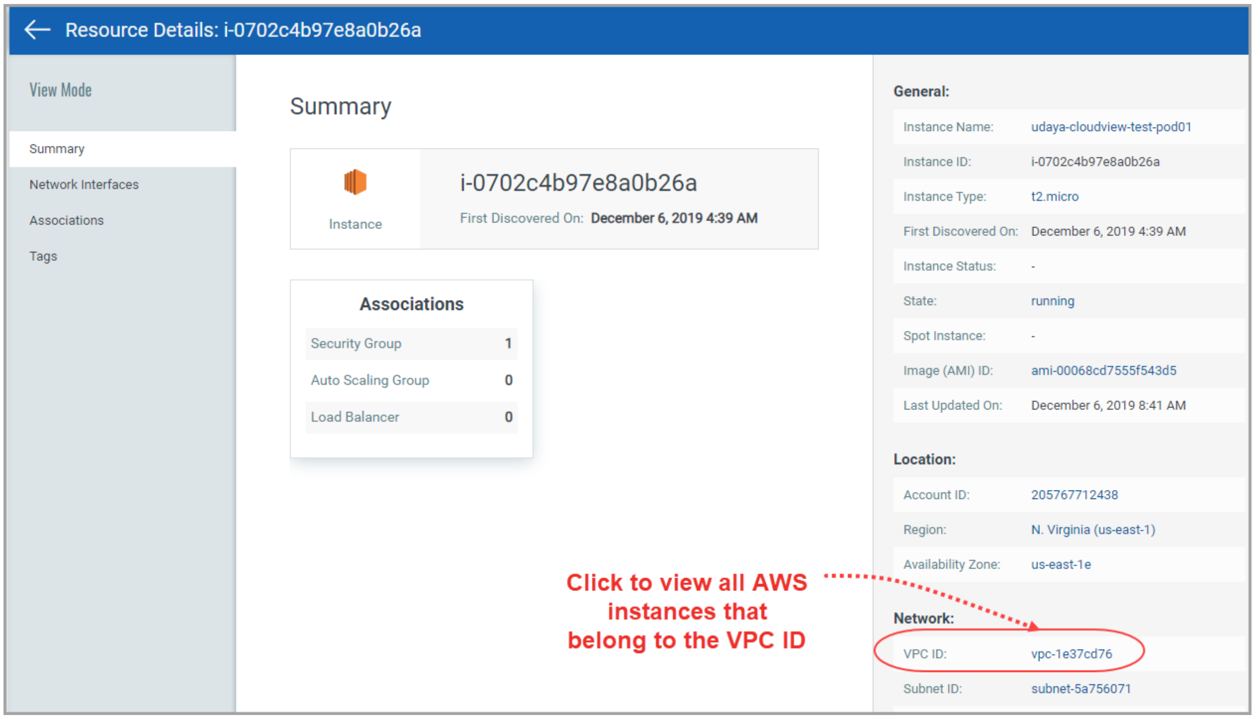
GCP Control Updates

CID	Resource	Title	Sections Updated
52005	IAM & Admin	Ensure Encryption keys are rotated within a period of 365 days	Remediation
52040	Kubernetes Engine	Ensure Automatic node repair is enabled for Kubernetes Clusters	Remediation

Search Using Resource Parameter Information

You can now search for all resources that match with the parameter information of a resource. For example, if you have a resource with certain specific parameter such as an AWS instance with specific VPC. You could now search for all resources that belong to the same VPC ID and resource type.

Go to Resources, select Instance resource type and click on the EC2 Instance ID to view the details of the resource. All the searchable parameter information for that resource type is displayed with links on the right side.



Resource Details: i-0702c4b97e8a0b26a

Summary

i-0702c4b97e8a0b26a
Instance
First Discovered On: **December 6, 2019 4:39 AM**

Associations

Security Group	1
Auto Scaling Group	0
Load Balancer	0

General:

Instance Name:	udaya-cloudview-test-pod01
Instance ID:	i-0702c4b97e8a0b26a
Instance Type:	t2.micro
First Discovered On:	December 6, 2019 4:39 AM
Instance Status:	-
State:	running
Spot Instance:	-
Image (AMI) ID:	ami-00068cd7555f543d5
Last Updated On:	December 6, 2019 8:41 AM

Location:

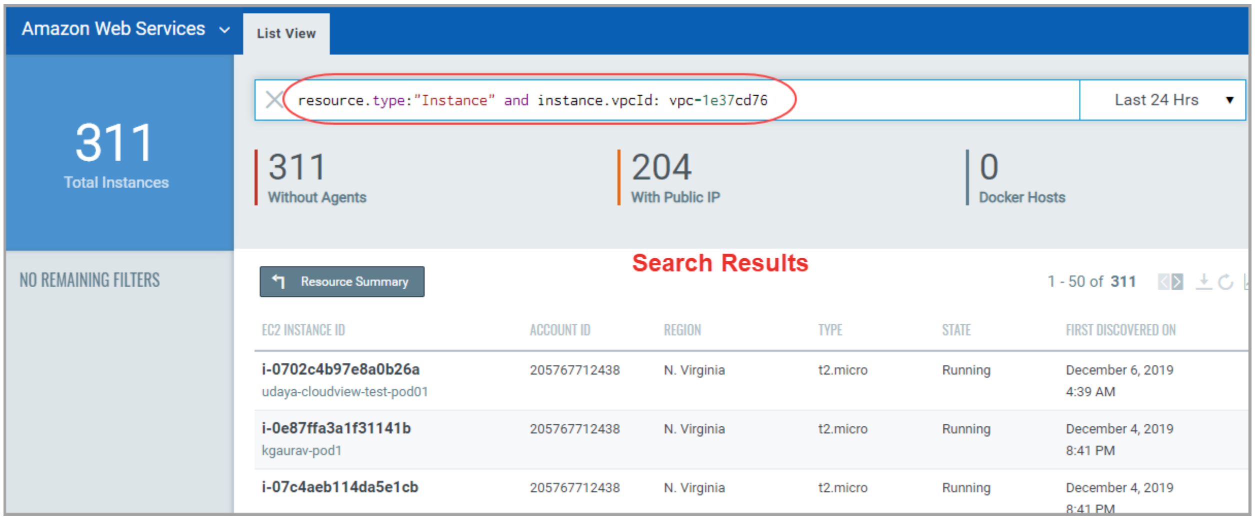
Account ID:	205767712438
Region:	N. Virginia (us-east-1)
Availability Zone:	us-east-1e

Network:

VPC ID:	vpc-1e37cd76
Subnet ID:	subnet-5a756071

Click to view all AWS instances that belong to the VPC ID

Click the link to automatically form the search query based on the VPC ID and view the search results.



resource.type:"Instance" and instance.vpcId: vpc-1e37cd76

311 Total Instances

311 Without Agents

204 With Public IP

0 Docker Hosts

Search Results

1 - 50 of 311

EC2 INSTANCE ID	ACCOUNT ID	REGION	TYPE	STATE	FIRST DISCOVERED ON
i-0702c4b97e8a0b26a udaya-cloudview-test-pod01	205767712438	N. Virginia	t2.micro	Running	December 6, 2019 4:39 AM
i-0e87ffa3a1f31141b kgaurav-pod1	205767712438	N. Virginia	t2.micro	Running	December 4, 2019 8:41 PM
i-07c4aeb114da5e1cb	205767712438	N. Virginia	t2.micro	Running	December 4, 2019 8:41 PM

Issues addressed in this release

We have fixed the following issues:

- We have now fixed the issue so that control evaluation results for associated resources of Lambda Function now displays correct results.
- The QQL search token "securitygroup.name" resulted in incorrect data. We have now fixed the issue so that the search displays correct results.
- We have now fixed pagination issue on Access Management tab. The pagination is now working as expected.