Qualys CloudView v1.x

Version 1.21.0

January 24, 2022

Here’s what’s new in Qualys CloudView 1.21.0!

Amazon Web Services

Common Feature

Qualys CloudView 1.21 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
285	Elasticsearch Service	ES Domain	Ensure all data stored in the Elasticsearch is securely encrypted at rest
286	EC2	Auto Scaling Group	Ensure all data stored in the Launch configuration EBS is securely encrypted
295	CloudFront	CloudFront	Ensure cloudfront distribution ViewerProtocolPolicy is set to HTTPS
303	MQ	MQ Broker	Ensure MQ Broker logging is enabled
314	CloudFront	CloudFront	Ensure that CloudFront Distribution has WAF enabled
315	MQ	MQ Broker	Ensure MQ Broker is not publicly exposed
318	API Gateway	Rest API Gateway	Ensure API Gateway has X-Ray Tracing enabled
319	Global Accelerator	Global Accelerator	Ensure Global Accelerator accelerator has flow logs enabled
321	CodeBuild	CodeBuild	Ensure that CodeBuild Project encryption is not disabled
325	Athena	Athena Workgroup	Ensure Athena Workgroup should enforce configuration to prevent client disabling encryption
326	Elasticsearch Service	ES Domain	Ensure Elasticsearch Domain enforces HTTPS
327	CloudFront	CloudFront	Ensure Cloudfront distribution has Access Logging enabled
328	EC2	EC2 Instance	Ensure that EC2 instance have no public IP
329	DMS	DMS Replication	Ensure that DMS replication instance is not publicly accessible
334	SageMaker	SageMaker Notebook	Ensure all data stored in the Sagemaker Endpoint is securely encrypted at rest

CID	Service	Resource	Title
338	EC2	Load Balancer	Ensure that load balancer is using TLS 1.2
348	VPC	VPC Endpoints	Ensure that VPC Endpoint Service is configured for Manual Acceptance
349	Cloud Formation	Cloud Formation Stack	Ensure that CloudFormation stacks are sending event notifications to an SNS topic
350	EC2	EC2 Instance	Ensure that detailed monitoring is enabled for EC2 instances
351	EC2	Load Balancer	Ensure that Elastic Load Balancer(s) uses SSL certificates provided by AWS Certificate Manager
354	EC2	Load Balancer	Ensure that ALB drops HTTP headers
357	EC2	EC2 Instance	Ensure that EC2 is EBS optimized
359	Elasticsearch Service	ES Domain	Ensure that Elasticsearch is configured inside a VPC
360	EC2	Load Balancer	Ensure that ELB is cross-zone-load-balancing enabled
366	Secrets Manager	Secrets	Ensure that Secrets Manager secret is encrypted using KMS
367	EC2	Load Balancer	Ensure that Load Balancer has deletion protection enabled
369	EC2	Load Balancer	Ensure that Load Balancer (Network/Gateway) has cross-zone load balancing enabled
370	EC2	Auto Scaling Group	Ensure that Autoscaling groups supply tags to launch configurations
374	Athena	Athena Workgroup	Ensure that Athena Workgroup is encrypted
378	Transfer Server	Transfer Server	Ensure Transfer Server is not exposed publicly
380	AWS Backup	Backup Vaults	Ensure Backup Vault is encrypted at rest using KMS CMK
381	S3 Glacier	Glacier Vault	Ensure Glacier Vault access policy is not public by only allowing specific services or principals to access it

CID	Service	Resource	Title
382	SQS	SQS Queue	Ensure SQS queue policy is not public by only allowing specific services or principals to access it
383	SNS	SNS Topic	Ensure SNS topic policy is not public by only allowing specific services or principals to access it
386	VPC	Network ACL	Ensure that all NACL are attached to subnets
388	API Gateway	API Gateway	Ensure API Gateway stage have logging level defined as appropriate and have metrics enabled
395	EC2	Load Balancer	Ensure that auto Scaling groups that are associated with a load balancer, are using Elastic Load Balancing health checks.
396	DynamoDB	DynamoDB Table	Ensure that Auto Scaling is enabled on your DynamoDB tables
398	EC2	EC2	Ensure that all EIP addresses allocated to a VPC are attached to EC2 instances
401	Route 53	Route 53 Record	Ensure that Route53 A Record has Attached Resource
403	EC2	Load Balancer	Ensure public-facing ALB are protected by WAF

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
292	DynamoDB	DynamoDB Table	Ensure Dynamodb point in time recovery (backup) is enabled
302	DynamoDB	DAX Cluster	Ensure DAX is encrypted at rest (default is unencrypted)
330	DocumentDB	DocumentDB Clusters	Ensure DocDB TLS is not disabled
333	RDS	RDS Cluster	Ensure all data stored in Aurora is securely encrypted at rest
371	Redshift	Redshift Clusters	Ensure Redshift is not deployed outside of a VPC
402	RDS	RDS	Ensure that Postgres RDS has Query Logging enabled

New Control for CIS Amazon Web Services Foundations Benchmark

We have introduced the following new control for CIS Amazon Web Services Foundations Benchmark Policy.

CID	Service	Resource	Title
199	IAM	IAM User	Ensure not to setup access keys during initial user setup for all IAM users that have a console password except for the master account

Permissions Needed for AWS Backup, WAF, and CodeBuild Resources

The cross-account role associated with the AWS connector needs additional permissions to fetch information about AWS Backup, WAF, and CodeBuild 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.

Common Feature

Updates to Mandate Configurations

Qualys CloudView application is extending mandate coverage by introducing new mandates and upgrading versions of the existing ones.

Updated Mandates (New Versions)

Sr No	Mandate Name	Current Version	Version Post 1.21 release
1	The Australian Signals Directorate - The Essential 8 Strategies (ASD 8)	February 2017	June 2020

Updated Mandates (Fixed sort order)

(no other change in mapping)

Sr No	Mandate Name	Version
1	Federal Risk and Authorization Management Program (FedRAMP H) - High Security Baseline	Rev. 4
2	Federal Risk and Authorization Management Program (FedRAMP M) - Moderate Security Baseline	Rev. 4

Infrastructure as Code (IaC) Security Posture

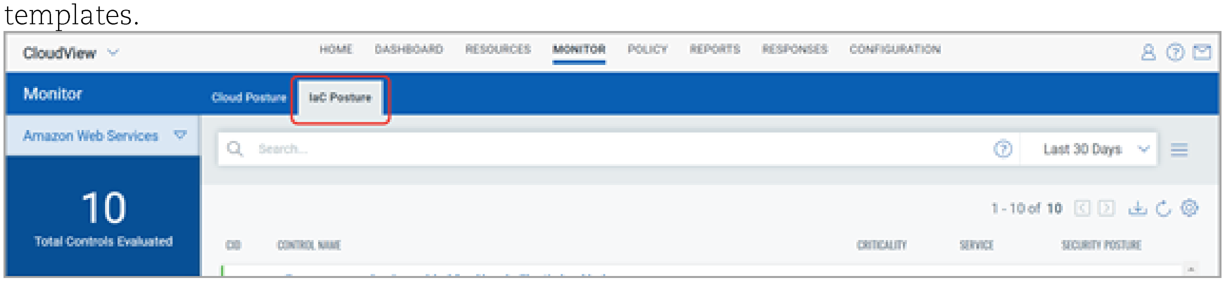
You can now view the compliance posture of resources residing in your Infrastructure as Code (IaC) templates. We have now introduced a new sub-tab named IaC Posture under the Monitor tab. The IaC Posture tab provides a complete picture of the compliance posture and helps you prevent misconfigurations before the resources are deployed in your cloud environment.

For IaC security posture, we have introduced the following things on CloudView UI.

- IaC Posture Tab
- New Search Tokens
- New Columns
- Assessment Reports for Build Time Controls
- Exceptions for Build Time Controls

IaC Posture Tab

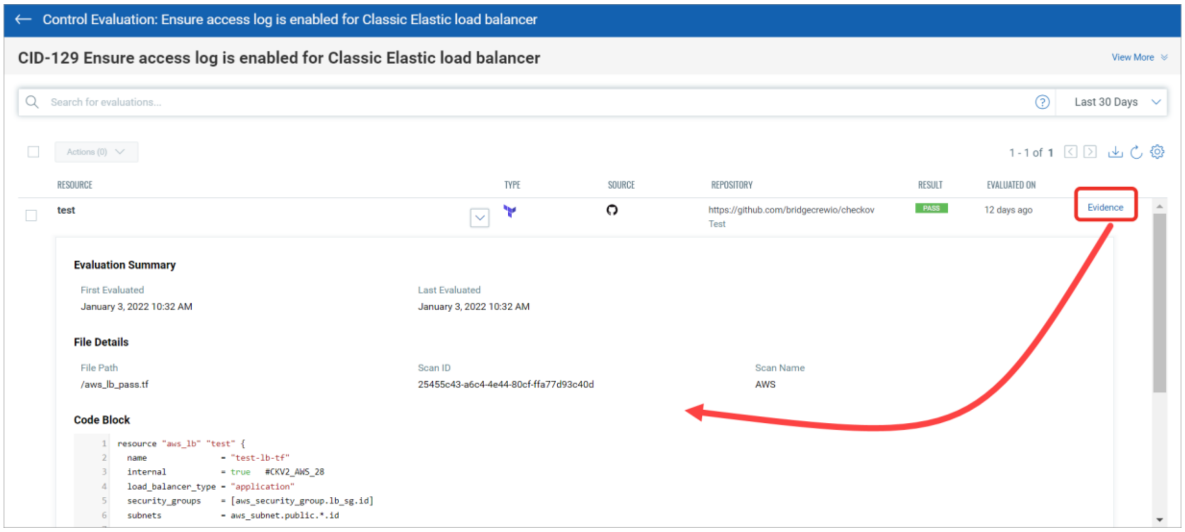
The IaC Posture tab lists all the build time control evaluations of the resources within your IaC templates.



Note: The IaC evaluations are displayed for scans initiated from Git integrations. For more information on Git integrations, refer to the Secure IaC section in CloudView User Guide.

Go to Monitor > IaC Posture tab. You'll notice a search bar above the controls list. Type your search query using our predefined-search tokens and filter controls as per your needs.

Click any control to get details of all the resources evaluated against the control.



Control Evaluation: Ensure access log is enabled for Classic Elastic load balancer

CID-129 Ensure access log is enabled for Classic Elastic load balancer

	RESOURCE	TYPE	SOURCE	REPOSITORY	RESULT	EVALUATED ON	
□	test			https://github.com/bridgecrewio/checkov Test	PASS	12 days ago	Evidence

Evaluation Summary

First Evaluated
January 3, 2022 10:32 AM

Last Evaluated
January 3, 2022 10:32 AM

File Details

File Path
/aws_lb_pass.tf

Scan ID
25455c43-a6c4-4e44-80cf-ffa77d93c40d

Scan Name
AWS

Code Block

```
resource "aws_lb" "test" {
  name               = "test-lb-tf"
  internal           = true    #CKV2_AWS_28
  load_balancer_type = "application"
  security_groups    = [aws_security_group.lb_sg.id]
  subnets            = aws_subnet.public.*.id
```

New Tokens

We have introduced the following new tokens for IaC related search on the IaC Posture tab.

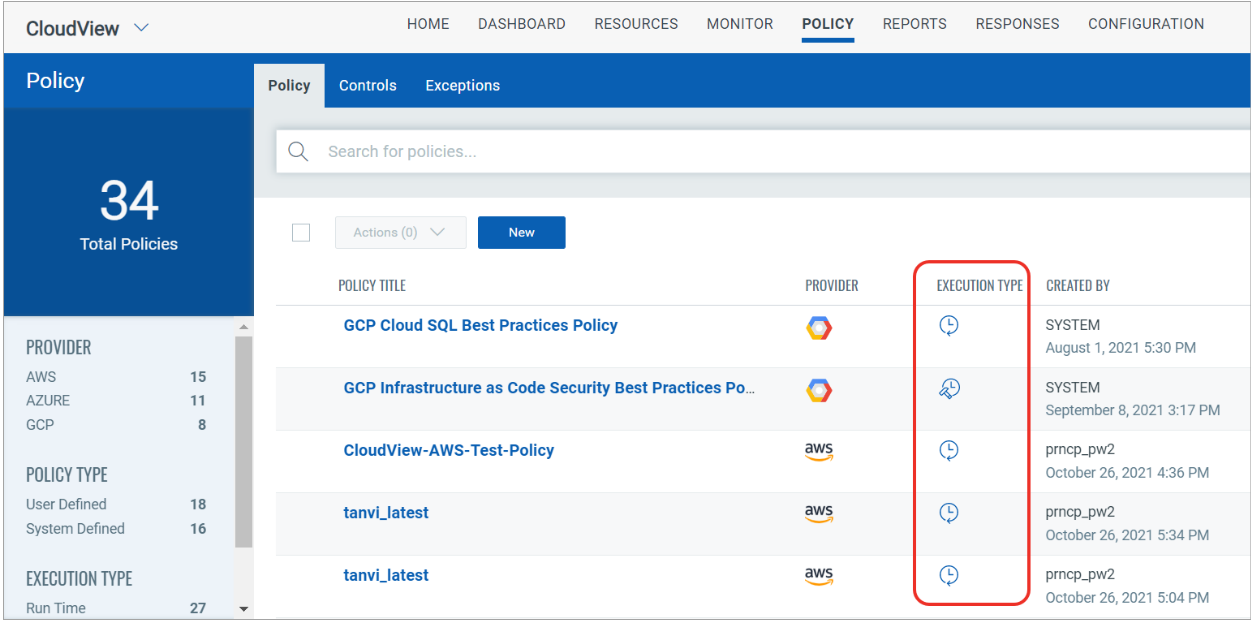
- iac.source: Use to filter IaC templates on the type of source they belong to
- iac.template.type: Use to filter IaC templates depending on the type of templates.
- iac.scan.id: Use to filter IaC scans using the unique IaC scan ID.
- iac.scan.name: Use to filter resources based on the unique scan name.
- git.reponame: Use to view resources belonging to a particular Git repository.
- git.branch: Use to view resources belonging to a particular branch of the Git repository.

New Columns

We have introduced a new column ‘Execution Type’ for policies and controls with values as follows:

- **Run-Time**: category for listing controls and policies for evaluations on deployed cloud resources. Denoted by the 🕓 icon.
- **Build Time**: category for listing controls and policies for evaluations on IaC templates. Denoted in the execution type column by the 🔧 icon.

Policy Tab

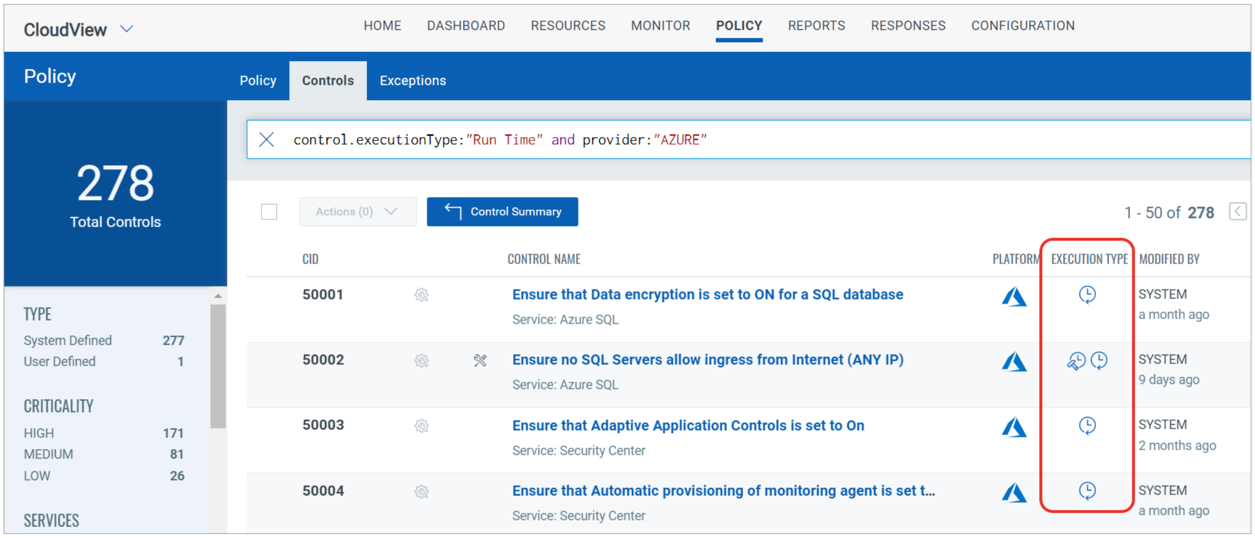


34
Total Policies

PROVIDER	
AWS	15
AZURE	11
GCP	8
POLICY TYPE	
User Defined	18
System Defined	16
EXECUTION TYPE	
Run Time	27

POLICY TITLE	PROVIDER	EXECUTION TYPE	CREATED BY
GCP Cloud SQL Best Practices Policy	⬡	🕓	SYSTEM August 1, 2021 5:30 PM
GCP Infrastructure as Code Security Best Practices Po...	⬡	🔧	SYSTEM September 8, 2021 3:17 PM
CloudView-AWS-Test-Policy	aws	🕓	prncp_pw2 October 26, 2021 4:36 PM
tanvi_latest	aws	🕓	prncp_pw2 October 26, 2021 5:34 PM
tanvi_latest	aws	🕓	prncp_pw2 October 26, 2021 5:04 PM

Controls Tab



```
control.executionType:"Run Time" and provider:"AZURE"
```

278 Total Controls

TYPE	
System Defined	277
User Defined	1
CRITICALITY	
HIGH	171
MEDIUM	81
LOW	26
SERVICES	

1 - 50 of 278

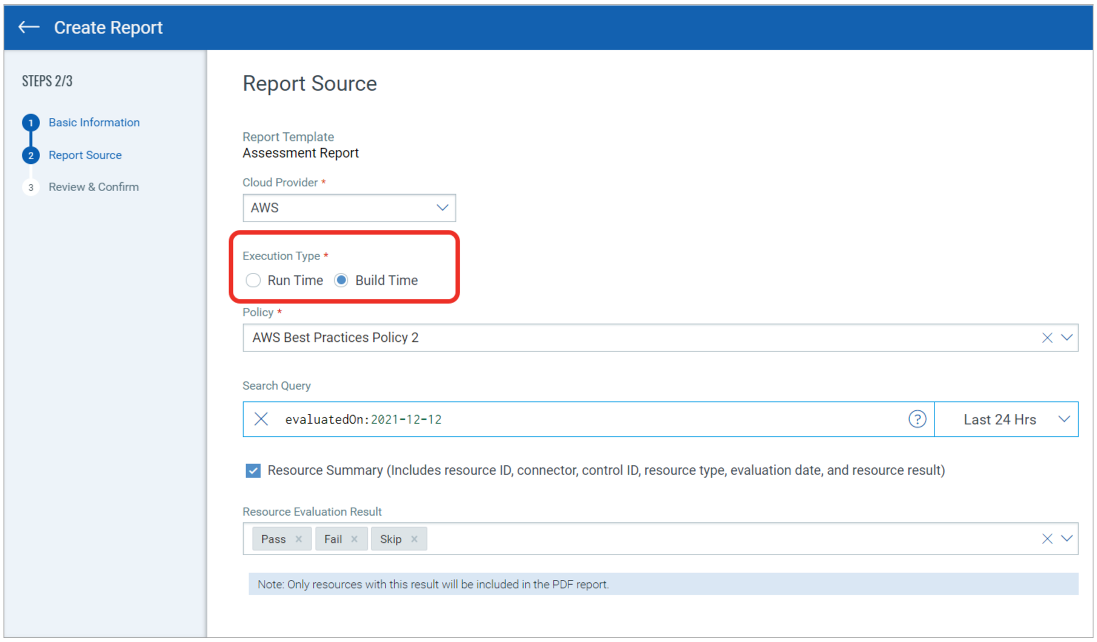
CID	CONTROL NAME	PLATFORM	EXECUTION TYPE	MODIFIED BY
50001	Ensure that Data encryption is set to ON for a SQL database Service: Azure SQL			SYSTEM a month ago
50002	Ensure no SQL Servers allow ingress from Internet (ANY IP) Service: Azure SQL			SYSTEM 9 days ago
50003	Ensure that Adaptive Application Controls is set to On Service: Security Center			SYSTEM 2 months ago
50004	Ensure that Automatic provisioning of monitoring agent is set t... Service: Security Center			SYSTEM a month ago

Assessment Reports for Build Time Control Evaluation

Use assessment reports to view the compliance of your cloud resources and resources within the IaC templates for the defined policies in CloudView. You can use Qualys Query Language (QQL) to generate the on-demand assessment reports.

Create an assessment report by telling us the settings. The report settings are saved and available to you. Once you generate an assessment report, you can view the report summary, reconfigure the report settings, and download the report in CSV or PDF format.

We have introduced a new option to generate a report depending on the control execution type. The detailed steps to generate the report are listed in the Assessment Reports topic of the CloudView online help.



Report Source

Report Template
Assessment Report

Cloud Provider *
AWS

Execution Type *
○ Run Time ● Build Time

Policy *
AWS Best Practices Policy 2

Search Query

```
evaluatedOn:2021-12-12
```

Last 24 Hrs

☑ Resource Summary (Includes resource ID, connector, control ID, resource type, evaluation date, and resource result)

Resource Evaluation Result
Pass × Fail × Skip ×

Note: Only resources with this result will be included in the PDF report.

Exceptions for Build Time Controls

You may want to create exceptions to exempt certain cloud resources from a particular run time of control or temporarily change the status of a resource for a particular run time of control from Failed to Skip (applicable for resources in IaC templates).

You need to add the following code to your template files and the controls are skipped during evaluation.

Code Snippet

```
"metadata":{
  "qiac-skip": [
    "iac:exempt=<cid>:<exception_comment>",
    "iac:exempt=<cid>:<exception_comment>"
  ]
}
```

For details, refer to the Exceptions topic in the CloudView online help.

Issues addressed in this release

- We have now fixed an issue where all the Lambda resources weren't being discovered and evaluated by controls in AWS Lambda Best Practices policy. We have now fixed the issue at the control level.
- We fixed an issue where the control was failing for AWS GovCloud accounts. The reason was that the GovCloud accounts didn’t have RDS 2019 certificates, only 2017 certificates are available. We fixed the issue by handling this case at the control level.