(https://www.whizlabs.com/learn) > My Courses (https://www.whizlabs.com/learn/my-courses)
> AWS Certified SysOps Administrator Associate (https://www.whizlabs.com/learn/course/aws-csyopaa-practice-tests#section-1)
> AWS Config (https://www.whizlabs.com/learn/course/aws-csyopaa-practice-tests/quiz/14887)
> Report

AWS CONFIG

Attempt	1
Marks Obtained	0 / 10
Your score is	0.0%
Completed on	Tuesday , 29 January 2019 , 02:29 PM
Time Taken	00 H 00 M 07 S
Result	Fail

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Monitoring and Reporting	10	0	1	9

10 Questions	**0** Correct	**1** Incorrect	**9** Unattempted

Show Answers

All ▼

QUESTION 1 INCORRECT MONITORING AND REPORTING

You are setting AWS Config via AWS CLI & you have created S3 Bucket in your account named as 12345. You are not receiving any change configuration notifications in this bucket. What could be the reason for this? Select any two options.

☑ **A.** Verify that S3 bucket is created in region where AWS config is created. ✖

☑ **B.** Create an IAM user name AWSCONFIG & assign full permission to access S3 bucket 12345. ✖

☐ **C.** If you have S3 bucket policies attached to your buckets, verify that it allows AWS Config permission to record changes to buckets. ✔

☐ **D.** Verify that the IAM role assigned to AWS Config has the AWSConfigRole managed policy. ✔

☐ **E.** Create a new S3 bucket name as AWSCONFIG.

Explanation :

Correct Answer – C, D.
To record AWS resource configurations, AWS Config requires IAM permissions to get the configuration details about your resources. Use the AWS managed policy AWSConfigRole and attach it to the IAM role that you assign to AWS Config. AWS updates this policy each time AWS Config adds support for an AWS resource type, which means AWS Config will continue to have the required permissions to get configuration details as long as the role has this managed policy attached. Also, if custom bucket policies are assigned to S3 bucket 12345, you must allow AWS Config permissions to record changes to bucket.
Option A is incorrect as S3 bucket can be in different regions as well. Option B is incorrect as IAM user is not required to be created.
Option E is incorrect as S3 bucket name can be any standard name & not specific name as AWSCONFIG.
For troubleshooting AWS Configs change notifications, check following link,
https://docs.aws.amazon.com/config/latest/developerguide/iamrole-permissions.html
(https://docs.aws.amazon.com/config/latest/developerguide/iamrole-permissions.html)

Ask our Experts

👍 👎

QUESTION 2 UNATTEMPTED MONITORING AND REPORTING

You are working as SysOps architect with a global advertising firm. Information for all clients is stored in RDS DB instance using Oracle database. Last month due to natural disaster, AZ ap-southeast-2a was down which cause outage in RDS DB instance. To avoid such outage in future, you are concerned about RDS DB instance running in production environment within single AZ & are not Multi-AZ enabled. Which of the following tool can be used to determine RDS DB instance across all regions which are not Multi-AZ enabled?

○ **A.** AWS CloudTrail

○ **B.** AWS Config ✓

○ **C.** AWS CloudWatch

○ **D.** AWS Trusted Advisor

Explanation :

Correct Answer – B

AWS Config rule “rds-multi-az-support” can be used to check whether high availability is enabled for your RDS DB instances.

Option A is incorrect CloudTrail is a logging service that records all API calls to any AWS service. It reports on who made the change, when, and from which location. It would not gather information on whether Multi-AZ is enabled on RDS DB Instance.

Option C is incorrect as CloudWatch is monitoring tool which monitors AWS resources in real-time. It would not gather information on whether Multi-AZ is enabled on RDS DB Instance.

Option D is incorrect as Trusted Advisor is online tool to reduce cost, increase performance, and improve security by optimizing your AWS environment. It would not gather information on whether Multi-AZ is enabled on RDS DB Instance.

For more information on setting config rules, check following link,
https://docs.aws.amazon.com/config/latest/developerguide/rds-multi-az-support.html
(https://docs.aws.amazon.com/config/latest/developerguide/rds-multi-az-support.html)

Ask our Experts

👍 👎

QUESTION 3 UNATTEMPTED MONITORING AND REPORTING

You are working as SysOps architect with a start-up company. A mission critical application is deployed on EC2 instance. Last week there were changes in Security Group for this EC2 instance, which caused blocking of remote access for all users to these servers. To avoid such issues in future, CTO is looking for a notification post security group changes to these EC2 instance. Which of the following can be configured to meet this requirement?

○ **A.** AWS Config Change-triggered rule ✔

○ **B.** AWS Config Periodic rule with frequency of 6 hours.

○ **C.** AWS Config Change-triggered rule with frequency of 6 hours.

○ **D.** AWS Config Custom Rules with Lambda Function having EC2 instance in scope.

Explanation :

Correct Answer – A
A change-triggered rule is executed when AWS Config records a configuration change for any of the resources
specified. AWS Config runs the evaluation when it detects a change to a resource that matches the rule's scope. You can use the scope to constrain which resources trigger evaluations. Otherwise, evaluations are triggered when any recorded resource changes
Option B is incorrect - A periodic rule is triggered at a specified frequency. Available frequencies are 1hr, 3hr, 6hr, 12hr or 24hrs.This will not be correct option for requirement.
Option C is incorrect as AWS Config Change-triggered rule runs the evaluation when it detects a change to a resource that matches the rule's scope & not on periodic basis.

Option D is incorrect as Custom rules with Lambda functions can be created to evaluate additional resources that AWS Config doesn't record. For specified requirement we can use AWS Config Managed rule to check for Security Group configuration changes & also record compliance status.
For more information of AWS Config trigger types, check following link:
https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html (https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html)

Ask our Experts

👍 👎

QUESTION 4 UNATTEMPTED MONITORING AND REPORTING

You are working as SysOps architect with a financial company. You have a finance application on EC2 instance behind an application load balancer. There is third party audit to be schedule next month. As a pre-requisite, Auditors require complete report of configuration changes on EC2 servers regardless of changes made to these servers. Which of the following can be configured to meet this requirement?

○ **A.** AWS Config Change-triggered rule

○ **B.** AWS Config Periodic rule with frequency of 24 hours ✔

○ **C.** AWS Config Periodic rule with frequency of 4 hours

○ **D.** AWS CloudTrail

Explanation :

Correct Answer – B
A periodic rule can be configured for this requirement. A periodic rule is triggered at a specified frequency. Available frequencies are 1hr, 3hr, 6hr, 12hr or 24hrs.

Option A is incorrect - A change-triggered rule is executed when AWS Config records a configuration change for any of the resources specified. This will not suffice requirement of Auditors as they are looking for changes every 24 hours.
Option C is incorrect as AWS Config Periodic rule with frequency of 4 hours is not a valid frequency. Available frequencies are 1hr, 3hr, 6hr, 12hr or 24hrs.
Option D is incorrect as CloudTrail will record user API activity on your account. This will not record changes made to EC2 but will record who made changes.
For more information of AWS Config trigger types, check following link,
https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html
(https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html)

Ask our Experts

👍 👎

QUESTION 5 UNATTEMPTED MONITORING AND REPORTING

You are working as SysOps administrator for a global IT firm having IT infrastructure spread across multiple regions. Based upon business verticals a separate AWS account is created. Operations director wants a consolidated report of resources count & compliance in all accounts across all regions. Which of the following can be used to achieve this requirement?

○ **A.** AWS Config Aggregated view ✓

○ **B.** Gather information from each account/region & share with director.

○ **C.** Not possible with AWS Config.

○ **D.** AWS Config Custom rules.

Explanation :

Correct Answer – A

The Aggregated view displays the configuration data of AWS resources and provides an overview of your rules and their compliance state. It provides the total resource count of AWS resources. The resource types and source accounts are ranked by the highest number of resources. It also provides a count of compliant and noncompliant rules.
Option B is incorrect – Using AWS Aggregated view, we can pull resource details from multiple accounts & regions, no need to gather information from each region or account.
Option C is incorrect as Using AWS Aggregated view it is possible.
Option D is incorrect as AWS Config Custom rules are created for to evaluate additional resources that AWS Config doesn't record.
For troubleshooting AWS Configs change notifications, check following link,
https://docs.aws.amazon.com/config/latest/developerguide/viewing-the-aggregate-dashboard.html (https://docs.aws.amazon.com/config/latest/developerguide/viewing-the-aggregate-dashboard.html)

Ask our Experts

👍 👎

QUESTION 6 UNATTEMPTED MONITORING AND REPORTING

You are working as solution architect for a media firm. Your technical manager asks to evaluate cost for implementing AWS Config. Which of the following are component of AWS Config pricing? Select any two options.

□ **A.** AWS Config is free, you are charged only for data recorded in S3 bucket.

□ **B.** Total number of active Config rules. ✓

□ **C.** Total number of Config rules.

□ **D.** Number of configuration Items. ✓

Explanation :

Correct Answer – B, D
With AWS Config, you are charged based on the number of configuration items recorded and the number of

active AWS Config rules in your account. A configuration item is a record of the configuration of a resource, in your AWS account. There is no up-front commitment and you can stop recording configuration items at any time. An AWS Config rule is considered active during a month if it records a compliance result against at least one resource during a month.

Option A is incorrect – For AWS config, there is charge based upon configuration item & number of active config rules. For Data recorded in S3 bucket, there would be additional charge based upon standard rates in a region.

Option C is incorrect. AWS Config charges are only based upon Active rules not total number of rules. An AWS Config rule is considered active during a month if it records a compliance result against at least one resource during a month.

For more information on AWS Config Pricing, check following link

https://aws.amazon.com/config/pricing/ (https://aws.amazon.com/config/pricing/)

Ask our Experts

👍 👎

QUESTION 7 UNATTEMPTED MONITORING AND REPORTING

For a test setup of new application, Team members are initiating large number of EC2 instance. Finance Team wants to evaluate how many of these EC2 instance are m4. large EC2 instance for cost projection. You created an AWS Config custom rule along with Lambda function. After successful rule creation, under Compliance

section you are getting error as “No resources in scope”. Which of the following may be reason for this error?

○ **A.** Instead of Custom rule, use AWS managed rules.

○ **B.** Verify if custom rule is associated with Lambda function.

○ **C.** Verify custom rules, to confirm EC2 instance are part of its scope. ✓

○ **D.** All EC2 instance initiated are t2. micro, & none are m4. large, so this is valid response.

Explanation :

Correct Answer – C
AWS Config cannot evaluate your recorded AWS resources against this rule because none of your resources are within the rule’s scope. To get evaluation results, edit the rule and change its scope, or add resources for AWS Config to record by using the Settings page. Verify that AWS Config is recording EC2 instances.
Option A is incorrect – You need to create AWS config custom rules for this requirement.
Option B is incorrect – This error will not be generated if custom rules are not associated with Lambda function. Option D is incorrect - If EC2 instance are t2. micro it would display count in noncompliant resources & will not generate this error.
For more information on AWS Custom rules, check following link,
https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_develop-rules_getting- (https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_develop-rules_getting-started.html) started.html (https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_develop-rules_getting- started.html)

Ask our Experts

👍 👎

QUESTION 8 UNATTEMPTED MONITORING AND REPORTING

You are working as SysOps admin for a large pharma company. They are using infrastructure with large number of EC2 instance. You are concern for some critical EC2 servers for which any unplanned changes will be catastrophic. You want to be notify to an operations team whenever there are change to these instances. Notification mails should consist of user details performing those changes & changes made. Which of the following services will you use for this purpose.

○ **A.** AWS Config & Trusted advisor.

○ **B.** AWS CloudWatch & CloudTrail.

○ **C.** AWS Config & CloudTrail. ✔

○ **D.** AWS CloudWatch & Config.

Explanation :

Correct Answer – C
AWS Config is a fully managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance.
AWS CloudTrail records user API activity on your account and allows you to access information about this activity. You get full details about API actions, such as identity of the caller, the time of the API call, the request parameters, and the response elements returned by the AWS service.
Option A is incorrect – Trusted Advisor is online tool to reduce cost, increase performance, and improve security by optimizing your AWS environment. Using AWS Config, you can determine changes made to EC2, but AWS Trust Advisor will not gather user details performing changes. AWS CloudTrail will gather these details.
Option B is incorrect – Using Amazon CloudWatch, you gain system-wide visibility into resource utilization, application performance, and operational health. Using AWS CloudTrail, you can determine who made changes to your EC2 servers from which location & time. To determine configuration changes, you need to use AWS Config instead of AWS CloudWatch.
Option D is incorrect – Using Amazon CloudWatch, you gain system-wide visibility into resource utilization, application performance, and operational health. Using AWS Config, you can determine changes made to EC2, but AWS CloudWatch will not gather user details performing changes. AWS CloudTrail will gather these details.
For more information on using both AWS Config & CloudTrail, check following link,
https://aws.amazon.com/config/faq/ (https://aws.amazon.com/config/faq/)

Ask our Experts

👍 👎

QUESTION 9 UNATTEMPTED MONITORING AND REPORTING

You are working as a SysOps architect for a media firm. All news footage files are uploaded in S3 buckets. To archive old video footage, you set S3 Lifecycle policies to move these files to STANDARD_IA after 30 days & to

S3 Glacier vaults after 90 days. For all compliance & audit requirements, you are looking for a tool which will gather records across all regions. Which of the following can be used to evaluate AWS Glacier vaults? Choose 2 options.

□ **A.** Enable Audit logging on Amazon S3 Glacier with AWS CloudTrail.

□ **B.** Create a AWS Config Custom rule & assign Lambda function to this rule. ✓

□ **C.** Create a AWS Config Managed rule & assign Lambda function to this rule.

□ **D.** Create a Lambda function to evaluate AWS S3 Glacier Vault. ✓

Explanation :

Correct Answer – B, D
AWS Config doesn't currently record Amazon S3 Glacier vaults. You can create custom rules to run evaluations for resource types not yet recorded by AWS Config. To create a custom rule, you first create an AWS Lambda function, which contains the evaluation logic for the rule. Then you associate the function with a custom rule that you create in AWS Config.
Option A is incorrect – Enabling Audit logging on Amazon S3 Glacier with AWS CloudTrail will provide record of actions taken by a user, role, or an AWS service in Glacier.
Option C is incorrect – AWS Config managed rules are predefined, customizable rules that AWS Config uses to evaluate whether your AWS resources comply with common best practices. Currently S3 Glaciers is not supported by these rules.
For more information on managed Config rules, you can check following link, https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_use-managed-rules.html (https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_use-managed-rules.html)
For more information on custom AWS config rules with Lambda function, check following link, https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_develop-rules_nodejs.html (https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_develop-rules_nodejs.html)

Ask our Experts

👍 👎

QUESTION 10 UNATTEMPTED MONITORING AND REPORTING

You are working as SysOps admin for a HR firm. They are storing resumes of all probable candidates in a S3 bucket. A separate bucket is being created based upon domain of each candidate.HR Head is concerned about policy violations which may grant public read / write access to these S3 buckets. He wants to have a tool for monitoring all these bucket & rectify if any violations. Which of the following may be used to achieve these processes? Select Three options.

□ **A.** AWS Config. ✓

□ **B.** AWS CloudWatch Events. ✓

□ **C.** AWS Lambda. ✓

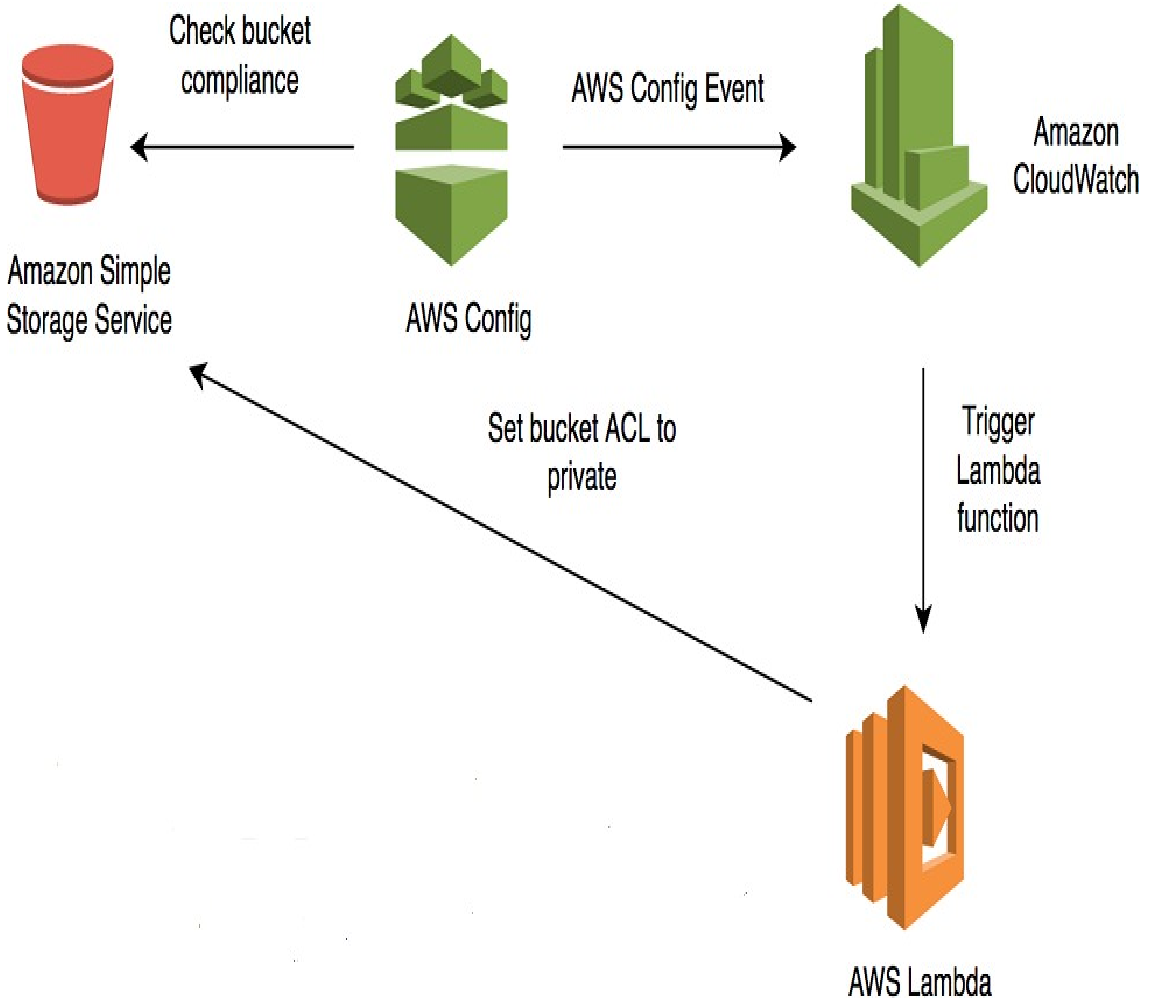
□ **D.** AWS Trusted advisor

□ **E.** AWS CloudTrail.

Explanation :

Correct Answer – A, B, C
AWS Config can be used to monitor Amazon Simple Storage Service (S3) bucket ACLs and policies for violations which allow public read or public write access. If AWS Config finds a policy violation, it can trigger an Amazon CloudWatch Event rule to trigger an AWS Lambda function which corrects the S3 bucket ACL. Following are steps to enable this,

- Enable AWS Config to monitor Amazon S3 bucket ACLs and policies for compliance violations.
- Create and configure a CloudWatch Events rule that triggers the Lambda function when AWS Config detects an S3 bucket ACL or policy violation.
- Create a Lambda function that uses the IAM role to review S3 bucket ACLs and policies, correct the ACLs, and also notify your team of out-of-compliance policies.



Option D is incorrect – Trusted Advisor is online tool to reduce cost, increase performance, and improve security by optimizing your AWS environment. This will not help to monitor policy violations in S3 buckets & rectify those.

Option E is incorrect - as CloudTrail will record user API activity on your account. This will not check bucket compliance.

For more information on AWS Custom rules, check following link,

https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-monitor-for-and-respond-to-amazon-s3- (https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-monitor-for-and-respond-to-amazon-s3-buckets-allowing-public-access/) buckets-allowing-public-access/ (https://aws.amazon.com/blogs/security/how-to-use-aws-config-to-monitor-for-and-respond-to-amazon-s3- buckets-allowing-public-access/)

Ask our Experts

👍 👎

Finish Review (https://www.whizlabs.com/learn/course/aws-csyopaa-practice-tests/quiz/14887)