DOP-C02$^{\text{Q\&As}}$

AWS Certified DevOps Engineer - Professional

Pass Amazon DOP-C02 Exam with 100% Guarantee

Following Questions and Answers are all new published by Amazon Official Exam Center

QUESTION 1

The security team depends on AWS CloudTrail to detect sensitive security issues in the company\\'s AWS account. The DevOps engineer needs a solution to auto-remediate CloudTrail being turned off in an AWS account.

What solution ensures the LEAST amount of downtime for the CloudTrail log deliveries?

A. Create an Amazon EventBridge rule for the CloudTrail StopLogging event. Create an AWS Lambda (unction that uses the AWS SDK to call StartLogging on the ARN of the resource in which StopLogging was called. Add the Lambda function ARN as a target to the EventBridge rule.

B. Deploy the AWS-managed CloudTrail-enabled AWS Config rule set with a periodic interval to 1 hour. Create an Amazon EventBridge rule tor AWS Config rules compliance change. Create an AWS Lambda function that uses the AWS SDK to call StartLogging on the ARN of the resource in which StopLoggmg was called. Add the Lambda function ARN as a target to the EventBridge rule.

C. Create an Amazon EventBridge rule for a scheduled event every 5 minutes. Create an AWS Lambda function that uses the AWS SDK to call StartLogging on a CloudTrail trail in the AWS account. Add the Lambda function ARN as a target to the EventBridge rule.

D. Launch a t2 nano instance with a script running every 5 minutes that uses the AWS SDK to query CloudTrail in the current account. If the CloudTrail trail is disabled have the script re-enable the trail.

Correct Answer: A

https://aws.amazon.com/blogs/mt/monitor-changes-and-auto-enable-logging-in-aws-cloudtrail/

QUESTION 2

Which statement is true about configuring proxy support for Amazon Inspector agent on a Windows-based system?

A. Amazon Inspector agent supports proxy usage on Windows-based systems through the use of the WinHTTP proxy.

B. Amazon Inspector agent supports proxy usage on Linux-based systems but not on Windows.

C. Amazon Inspector proxy support on Windows-based systems is achieved through installing proxy-enabled version of the agent which comes with preconfigured files that you need to edit to match your environment.

D. Amazon Inspector agent supports proxy usage on Windows-based systems through awsagent.env configuration file.

Correct Answer: A

Proxy support for AWS agents is achieved through the use of the WinHTTP proxy.

Reference: https://docs.aws.amazon.com/inspector/latest/userguide/inspector_agents-on-win.html#inspectoragent-proxy

QUESTION 3

A company has enabled all features for its organization in AWS Organizations. The organization contains 10 AWS accounts. The company has turned on AWS CloudTrail in all the accounts. The company expects the number of AWS accounts in the organization to increase to 500 during the next year. The company plans to use multiple OUs for these accounts.

The company has enabled AWS Config in each existing AWS account in the organization. A DevOps engineer must implement a solution that enables AWS Config automatically for all future AWS accounts that are created in the organization.

Which solution will meet this requirement?

A. In the organization\\'s management account, create an Amazon EventBridge rule that reacts to a CreateAccount API call. Configure the rule to invoke an AWS Lambda function that enables trusted access to AWS Config for the organization.

B. In the organization\\'s management account, create an AWS CloudFormation stack set to enable AWS Config. Configure the stack set to deploy automatically when an account is created through Organizations.

C. In the organization\\'s management account, create an SCP that allows the appropriate AWS Config API calls to enable AWS Config. Apply the SCP to the root-level OU.

D. In the organization\\'s management account, create an Amazon EventBridge rule that reacts to a CreateAccount API call. Configure the rule to invoke an AWS Systems Manager Automation runbook to enable AWS Config for the account.

Correct Answer: B

https://aws.amazon.com/about-aws/whats-new/2020/02/aws-cloudformation-stacksets-introduces-automatic-deployments-across-accounts-and-regions-through-aws-organizations/

QUESTION 4

A company is running a number of internet-facing APIs that use an AWS Lambda authorizer to control access. A security team wants to be alerted when a large number of requests are failing authorization, as this may indicate API abuse. Given the magnitude of API requests, the team wants to be alerted only if the number of HTTP 403 Forbidden responses goes above 2% of overall API calls.

Which solution will accomplish this?

A. Use the default Amazon API Gateway 403Error and Count metrics sent to Amazon CloudWatch, and use metric math to create a CloudWatch alarm. Use the (403Error/Count)*100 mathematical expression when defining the alarm. Set the alarm threshold to be greater than 2.

B. Write a Lambda function that fetches the default Amazon API Gateway 403Error and Count metrics sent to Amazon CloudWatch, calculate the percentage of errors, then push a custom metric to CloudWatch named Custorn403Percent. Create a CloudWatch alarm based on this custom metric. Set the alarm threshold to be greater than 2.

C. Configure Amazon API Gateway to send custom access logs to Amazon CloudWatch Logs. Create a log filter to produce a custom metric for the HTTP 403 response code named Custom403Error. Use this custom metric and the default API Gateway Count metric sent to CloudWatch, and use metric match to create a CloudWatch alarm. Use the (Custom403Error/Count)*100 mathematical expression when defining the alarm. Set the alarm threshold to be greater than 2.

D. Configure Amazon API Gateway to enable custom Amazon CloudWatch metrics, enable the ALL_STATUS_CODE option, and define an APICustom prefix. Use CloudWatch metric math to create a CloudWatch alarm. Use the

(APICustom403Error/Count)*100 mathematical expression when defining the alarm. Set the alarm threshold to be greater than 2.

Correct Answer: C

Reference: https://aws.amazon.com/blogs/compute/analyzing-api-gateway-custom-access-logs-for-custom-domain-names/

QUESTION 5

A company\\'s security team requires that all external Application Load Balancers (ALBs) and Amazon API Gateway APIs are associated with AWS WAF web ACLs. The company has hundreds of AWS accounts, all of which are included in a single organization in AWS Organizations. The company has configured AWS Config for the organization. During an audit, the company finds some externally facing ALBs that are not associated with AWS WAF web ACLs.

Which combination of steps should a DevOps engineer take to prevent future violations? (Choose two.)

A. Delegate AWS Firewall Manager to a security account.

B. Delegate Amazon GuardDuty to a security account.

C. Create an AWS Firewall Manager policy to attach AWS WAF web ACLs to any newly created ALBs and API Gateway APIs.

D. Create an Amazon GuardDuty policy to attach AWS WAF web ACLs to any newly created ALBs and API Gateway APIs.

E. Configure an AWS Config managed rule to attach AWS WAF web ACLs to any newly created ALBs and API Gateway APIs.

Correct Answer: AC

If instead you want to automatically apply the policy to existing in-scope resources, choose Auto remediate any noncompliant resources. This option creates a web ACL in each applicable account within the AWS organization and associates the web ACL with the resources in the accounts. When you choose Auto remediate any noncompliant resources, you can also choose to remove existing web ACL associations from in-scope resources, for the web ACLs that aren\\'t managed by another active Firewall Manager policy. If you choose this option, Firewall Manager first associates the policy\\'s web ACL with the resources, and then removes the prior associations. If a resource has an association with another web ACL that\\'s managed by a different active Firewall Manager policy, this choice doesn\\'t affect that association.