DOP-C02 Q&As

AWS Certified DevOps Engineer - Professional

Pass Amazon DOP-C02 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/dop-c02.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

When logging with Amazon CloudTrail, API call information for services with regional end points is ____.

A. captured and processed in the same region as to which the API call is made and delivered to the region associated with your Amazon S3 bucket

B. captured, processed, and delivered to the region associated with your Amazon S3 bucket

C. captured in the same region as to which the API call is made and processed and delivered to the region associated with your Amazon S3 bucket

D. captured in the region where the end point is located, processed in the region where the CloudTrail trail is configured, and delivered to the region associated with your Amazon S3 bucket

Correct Answer: A

When logging with Amazon CloudTrail, API call information for services with regional end points (EC2, RDS etc.) is captured and processed in the same region as to which the API call is made and delivered to the region associated with your Amazon S3 bucket. API call information for services with single end points (IAM, STS etc.) is captured in the region where the end point is located, processed in the region where the CloudTrail trail is configured, and delivered to the region associated with your Amazon S3 bucket.

Reference: https://aws.amazon.com/cloudtrail/faqs/

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

When logging with Amazon CloudTrail, API call information for services with single end points is ____.

A. captured and processed in the same region as to which the API call is made and delivered to the region associated with your Amazon S3 bucket

B. captured, processed, and delivered to the region associated with your Amazon S3 bucket

C. captured in the same region as to which the API call is made and processed and delivered to the region associated with your Amazon S3 bucket

D. captured in the region where the end point is located, processed in the region where the CloudTrail trail is configured, and delivered to the region associated with your Amazon S3 bucket

Correct Answer: D

When logging with Amazon CloudTrail, API call information for services with regional end points (EC2, RDS etc.) is captured and processed in the same region as to which the API call is made and delivered to the region associated with your Amazon S3 bucket. API call information for services with single end points (IAM, STS etc.) is captured in the region where the end point is located, processed in the region where the CloudTrail trail is configured, and delivered to the region associated with your Amazon S3 bucket.

Reference: https://aws.amazon.com/cloudtrail/faqs/

QUESTION 4

A company has developed a serverless web application that is hosted on AWS. The application consists of Amazon S3. Amazon API Gateway, several AWS Lambda functions, and an Amazon RDS for MySQL database. The company is using AWS CodeCommit to store the source code. The source code is a combination of AWS Serverless Application Model (AWS SAM) templates and Python code.

A security audit and penetration test reveal that user names and passwords for authentication to the database are hardcoded within CodeCommit repositories. A DevOps engineer must implement a solution to automatically detect and prevent hardcoded secrets.

What is the MOST secure solution that meets these requirements?

A. Enable Amazon CodeGuru Profiler. Decorate the handler function with @with_lambda_profiler(). Manually review the recommendation report. Write the secret to AWS Systems Manager Parameter Store as a secure string. Update the SAM templates and the Python code to pull the secret from Parameter Store.

B. Associate the CodeCommit repository with Amazon CodeGuru Reviewer. Manually check the code review for any recommendations. Choose the option to protect the secret. Update the SAM templates and the Python code to pull the secret from AWS Secrets Manager.

C. Enable Amazon CodeGuru Profiler. Decorate the handler function with @with_lambda_profiler(). Manually review the recommendation report. Choose the option to protect the secret. Update the SAM templates and the Python code to pull the secret from AWS Secrets Manager.

D. Associate the CodeCommit repository with Amazon CodeGuru Reviewer. Manually check the code review for any recommendations. Write the secret to AWS Systems Manager Parameter Store as a string. Update the SAM templates and the Python code to pull the secret from Parameter Store.

Correct Answer: B

https://docs.aws.amazon.com/codecommit/latest/userguide/how-to-amazon-codeguru-reviewer.html

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.