SOA-C01 Q&As

AWS Certified SysOps Administrator - Associate (SOA-C01)

Pass Amazon SOA-C01 Exam with 100% Guarantee

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

https://www.pass4itsure.com/aws-sysops.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

A company wants to track Amazon EC2 usage charges that are based on the value of a tag that is named Business-Unit. Company leaders instruct developers to update all EC2 resources with the tag. The developers notify the leaders that they have completed this task.

Later that week, a finance team member checks Cost Explorer. The finance team member sees EC2 costs in the different accounts but cannot find the Business-Unit tag to filter by or group by.

What is the MOST likely reason that the Business-Unit tag is absent?

A. The Business-Unit tag is not activated as a cost allocation tag in the AWS Billing and Cost Management console.

B. The Business-Unit tag is not valid because tag key names do not support dashes (-).

C. The instances have been rebooted, and the developers neglected to re-add the Business-Unit tag after the reboot.

D. The IAM user does not have permission to view the tags in Cost Explorer.

Correct Answer: A

QUESTION 2

A SysOps Administrator needs to monitor all the object upload and download activity of a single Amazon S3 bucket. Monitoring must include tracking the AWS account of the caller, the IAM user role of the caller, the time of the API call, and the IP address of the API.

Where can the Administrator find this information?

A. AWS CloudTrail data event logging

B. AWS CloudTrail management event logging

C. Amazon Inspector bucket event logging

D. Amazon Inspector user event logging

Correct Answer: A

QUESTION 3

A company currently has a single AWS account used by all project teams. The company is migrating to a

multi-account strategy, where each project team will have its own account. The AWS IAM configuration

must have the same roles and policies for each of the accounts.

What is the MOST efficient way to implement and manage these new requirements?

A. Create a portfolio in the AWS Service Catalog for the IAM roles and policies. Have a specific product in the portfolio for each environment, project, and team that can be launched independently by each user.

B. Use AWS Organizations to create organizational units (OUs) for each group of projects and each team. Then leverage service control policies at the account level to restrict what services can used and what actions the users, groups, and roles can perform in those accounts.

C. Create an AWS Lambda script that leverages cross-account access to each AWS account, and create all the roles and policies needed using the IAM API and JSON documents stored in Amazon S3.

D. Create a single AWS CloudFormation template. Use CloudFormation StackSets to launch the CloudFormation template into each target account from the Administrator account.

Correct Answer: B

Explanation: Service control policies (SCPs) are one type of policy that you can use to manage your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization\\'s access control guidelines. SCPs are available only in an organization that has all features enabled. SCPs aren\\'t available if your organization has enabled only the consolidated billing features. Reference: https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html

QUESTION 4

What can an Administrator do to monitor whether an organization\\'s instances are compliant with corporate policies and guidelines?

A. Check the instances' metadata to determine what software is running.

B. Use AWS CloudTrail logs to identify the applications running on the instances.

C. Set CloudWatch alarms that are triggered with any software change on the instances.

D. Using Config Rules in the AWS Config service to check the instance\\'s configuration and applications.

Correct Answer: D

QUESTION 5

A user has created a launch configuration for Auto Scaling where CloudWatch detailed monitoring is disabled. The user wants to now enable detailed monitoring. How can the user achieve this?

A. Update the Launch config with CLI to set InstanceMonitoringDisabled = false

B. The user should change the Auto Scaling group from the AWS console to enable detailed monitoring

C. Update the Launch config with CLI to set InstanceMonitoring.Enabled = true

D. Create a new Launch Config with detail monitoring enabled and update the Auto Scaling group

Correct Answer: D

Explanation: CloudWatch is used to monitor AWS as well as the custom services. To enable detailed instance monitoring for a new Auto Scaling group, the user does not need to take any extra steps. When the user creates the AutoScaling launch config as the first step for creating an Auto Scaling group, each launch configuration contains a flag named InstanceMonitoring.Enabled. The default value of this flag is true. When the user has created a launch configuration with InstanceMonitoring.Enabled = false it will involve multiple steps to enable detail monitoring. The steps are: Create a new Launch config with detailed monitoring enabled Update the Auto Scaling group with a new launch config Enable detail monitoring on each EC2 instance