



Vendor: Amazon

Exam Code: SOA-C03

Exam Name: AWS Certified CloudOps Engineer - Associate
(SOA-C03)

Version: DEMO

QUESTION 1

A company has an internal web application that runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group in a single Availability Zone. A CloudOps engineer must make the application highly available.

Which action should the CloudOps engineer take to meet this requirement?

- A. Increase the maximum number of instances in the Auto Scaling group to meet the capacity that is required at peak usage.
- B. Increase the minimum number of instances in the Auto Scaling group to meet the capacity that is required at peak usage.
- C. Update the Auto Scaling group to launch new instances in a second Availability Zone in the same AWS Region.
- D. Update the Auto Scaling group to launch new instances in an Availability Zone in a second AWS Region.

Answer: C

Explanation:

High availability within AWS is achieved by distributing resources across multiple Availability Zones in the same Region. By updating the Auto Scaling group to span at least two Availability Zones, the application can continue serving traffic even if one zone becomes unavailable. This configuration works seamlessly with the Application Load Balancer, which automatically routes traffic only to healthy instances across those zones.

QUESTION 2

A CloudOps engineer is creating a simple, public-facing website running on Amazon EC2. The CloudOps engineer created the EC2 instance in an existing public subnet and assigned an Elastic IP address to the instance. Next, the CloudOps engineer created and applied a new security group to the instance to allow incoming HTTP traffic from 0.0.0.0/0. Finally, the CloudOps engineer created a new network ACL and applied it to the subnet to allow incoming HTTP traffic from 0.0.0.0/0. However, the website cannot be reached from the internet.

What is the cause of this issue?

- A. The CloudOps engineer did not create an outbound rule that allows ephemeral port return traffic in the new network ACL.
- B. The CloudOps engineer did not create an outbound rule in the security group that allows HTTP traffic from port 80.
- C. The Elastic IP address assigned to the EC2 instance has changed.
- D. There is an additional network ACL associated with the subnet that includes a rule that denies inbound HTTP traffic from port 80.

Answer: A

Explanation:

Network ACLs are stateless, meaning that return traffic for allowed inbound connections must be explicitly permitted by outbound rules. Although the inbound rule allows HTTP (port 80) from 0.0.0.0/0, if the outbound rule does not allow ephemeral ports (typically 1024–65535), return traffic from the web server to clients will be blocked, preventing users from accessing the website.

QUESTION 3

A company wants to use AWS Systems Manager to manage a large fleet of Amazon EC2 instances. The company hosts the instances in private subnets. The company follows the principle of least privilege to assign access permissions. All private subnets have internet

connectivity through a NAT gateway.

A CloudOps engineer installs the latest version of the Systems Manager Agent (SSM Agent). However, the EC2 instances do not appear in Systems Manager Fleet Manager. The CloudOps engineer must resolve this issue.

Which solution will meet this requirement?

- A. Replace the NAT gateway with a NAT instance that is deployed in the public subnet. Update the private subnet's route table to use the NAT instance.
- B. Create a VPC endpoint for Systems Manager. Remove routes to the internet through the NAT gateway from the private subnet's route table.
- C. Attach the AmazonSSMManagedInstanceCore AWS managed policy to the EC2 instance profile that is associated with the instances.
- D. Attach a custom policy that allows all actions to ssm* to the EC2 instance profile that is associated with the instances.

Answer: C

Explanation:

For EC2 instances to register and appear in AWS Systems Manager (Fleet Manager, Run Command, Patch Manager, etc.), the instance's IAM instance profile must have the correct permissions. The recommended least-privilege policy is AmazonSSMManagedInstanceCore, which grants SSM Agent the necessary access to Systems Manager, AWS Identity and Access Management, and (optionally) CloudWatch Logs. Without this policy, the agent cannot register the instance, even if network connectivity through a NAT gateway is present.

QUESTION 4

A company has an application that collects notifications from thousands of alarm systems. The notifications include alarm notifications and information notifications. The information notifications include the system arming processes, disarming processes, and sensor status.

All notifications are kept as messages in an Amazon Simple Queue Service (Amazon SQS) queue. Amazon EC2 instances that are in an Auto Scaling group process the messages. A CloudOps engineer needs to implement a solution that prioritizes alarm notifications over information notifications.

Which solution will meet these requirements?

- A. Adjust the Auto Scaling group to scale faster when a high number of messages is in the queue.
- B. Use the Amazon Simple Notification Service (Amazon SNS) fanout feature with Amazon SQS to send the notifications in parallel to all the EC2 instances.
- C. Add an Amazon DynamoDB stream to accelerate the message processing.
- D. Create a queue for alarm notifications and a queue for information notifications. Update the application to collect messages from the alarm notifications queue first.

Answer: D

Explanation:

By separating alarm and information notifications into two SQS queues, the application can always poll and process the alarm queue first, ensuring high-priority alarm messages are handled before lower-priority informational ones. This achieves true prioritization with minimal architectural change and without relying on scaling behavior or unrelated services.

QUESTION 5

A company is implementing security and compliance by using AWS Trusted Advisor. The company's CloudOps team is validating the list of Trusted Advisor checks that it can access.

Which factor will affect the quantity of available Trusted Advisor checks?

- A. Whether at least one Amazon EC2 instance is in the running state
- B. The AWS Support plan
- C. An AWS Organizations service control policy (SCP)
- D. Whether the AWS account root user has multi-factor authentication (MFA) enabled

Answer: B

Explanation:

The number and depth of Trusted Advisor checks available depend on the AWS Support plan level.

Basic and Developer Support plans only provide a limited set of checks (mainly Service Limits and Security).

Business and Enterprise Support plans provide access to the full set of Trusted Advisor checks, including cost optimization, performance, and fault tolerance.

QUESTION 6

A CloudOps engineer has successfully deployed a VPC with an AWS CloudFormation template. The CloudOps engineer wants to deploy the same template across multiple accounts that are managed through AWS Organizations.

Which solution will meet this requirement with the LEAST operational overhead?

- A. Assume the OrganizationAccountAccessRole IAM role from the management account. Deploy the template in each of the accounts.
- B. Create an AWS Lambda function to assume a role in each account. Deploy the template by using the AWS CloudFormation CreateStack API call.
- C. Create an AWS Lambda function to query for a list of accounts. Deploy the template by using the AWS CloudFormation CreateStack API call.
- D. Use AWS CloudFormation StackSets from the management account to deploy the template in each of the accounts.

Answer: D

Explanation:

AWS CloudFormation StackSets is purpose-built for deploying CloudFormation templates across multiple AWS accounts and Regions from a central management account. When integrated with AWS Organizations, StackSets automatically handles account targeting and stack synchronization with minimal manual effort, providing the lowest operational overhead compared to scripting or manual deployment approaches.

QUESTION 7

A company's application is hosted by an internet provider at app.example.com. The company wants to access the application by using www.company.com, which the company owns and manages with Amazon Route 53.

Which Route 53 record should be created to address this?

- A. A record
- B. Alias record
- C. CNAME record
- D. Pointer (PTR) record

Answer: C

Explanation:

A CNAME (Canonical Name) record maps one domain name (e.g., www.company.com) to another domain name (e.g., app.example.com). This allows users to access the application using the company's custom domain while DNS resolution automatically points to the external hostname. Alias records are used for AWS resources like CloudFront or ELB, not external domains.

QUESTION 8

A company uses Amazon ElastiCache (Redis OSS) to cache application data. A CloudOps engineer must implement a solution to increase the resilience of the cache. The solution also must minimize the recovery time objective (RTO).

Which solution will meet these requirements?

- A. Replace ElastiCache (Redis OSS) with ElastiCache (Memcached).
- B. Create an Amazon EventBridge rule to initiate a backup every hour. Restore the backup when necessary.
- C. Create a read replica in a second Availability Zone. Enable Multi-AZ for the ElastiCache (Redis OSS) replication group.
- D. Enable automatic backups. Restore the backups when necessary.

Answer: C

Explanation:

Enabling Multi-AZ with automatic failover for ElastiCache for Redis provides high availability and the lowest possible RTO, as Redis automatically promotes a replica to primary if the primary node fails. This ensures near-instant recovery without manual intervention, unlike backup-based solutions, which involve downtime and manual restores.

QUESTION 9

A company has multiple AWS accounts. A CloudOps engineer uses a sandbox account to create and verify IAM policies for use in a production account. The CloudOps engineer uses AWS CloudFormation to deploy policies to the sandbox account for testing. When tests pass, the CloudOps engineer deploys the policies to production. The CloudOps engineer has configured AWS CloudTrail in both the sandbox account and the production account.

The CloudOps engineer wants to detect any changes to the IAM policies after the policies have been deployed by CloudFormation. The CloudOps engineer must receive notifications for any changes to the policies.

Which solution will meet these requirements with the LEAST administrative effort?

- A. Configure CloudTrail to send email notifications to the CloudOps engineer when CloudTrail detects changes to the IAM policies.
- B. Create an Amazon EventBridge rule to invoke an AWS Lambda function to check the CloudFormation stack for drift. Configure the function to use Amazon Simple Notification Service (Amazon SNS) to notify the CloudOps engineer if the function detects any drift.

- C. Use AWS Identity and Access Management Access Analyzer to generate a policy based on CloudTrail activity for the IAM role that is attached to the IAM policies in the production account. Compare the results to the IAM policies that are in the sandbox account. Send a notification to the CloudOps engineer if the policies are different.
- D. Store the IAM policies as a JSON document in an Amazon S3 bucket. Use an AWS Lambda function to periodically compare the IAM policies with the JSON document that is stored in the S3 bucket.

Answer: B

Explanation:

CloudFormation drift detection is designed to detect any configuration changes made outside CloudFormation (such as manual edits to IAM policies). By wiring CloudTrail → EventBridge → Lambda → Drift Detection → SNS, you automatically trigger drift checks when relevant changes occur and notify the CloudOps engineer if the actual IAM policies differ from the CloudFormation template. This leverages managed services and avoids building your own comparison logic, providing the least administrative effort among the options.

QUESTION 10

A finance company stores confidential data in an Amazon S3 bucket. The company uses Amazon QuickSight to analyze the data and create dashboard reports. The company requires that all data access and connections to QuickSight remain within the company's VPC network boundary.

Which solution will meet these requirements?

- A. Create an interface VPC endpoint for QuickSight. Configure the endpoint to connect to QuickSight within the VPC by using AWS PrivateLink. Create a manifest file that points to the S3 data. Grant QuickSight permission to access the S3 bucket.
- B. Set up a VPC endpoint for QuickSight. Use an Amazon EC2 instance as a proxy to establish a direct connection between the VPC and QuickSight. Create a manifest file that points to the S3 data. Store the manifest on the EC2 instance. Grant QuickSight permission to access the EC2 instance.
- C. Configure an Amazon S3 VPC gateway endpoint. Route all data from QuickSight through the endpoint to transfer data. Grant QuickSight permission to access the S3 bucket.
- D. Configure a NAT gateway in the company's VPC. Route all data from QuickSight through the NAT gateway to transfer data. Grant QuickSight permission to access the S3 bucket.

Answer: A

Explanation:

To keep all QuickSight traffic and data access within the VPC boundary, you must use an interface VPC endpoint for QuickSight via AWS PrivateLink. This provides a private connection from your VPC to the QuickSight service without traversing the public internet. Then QuickSight can read data from S3 (referenced via a manifest file) while staying within the VPC path, as long as the proper S3 permissions are granted.

QUESTION 11

A company is migrating its production file server to AWS. All data that is stored on the file server must remain accessible if an Availability Zone becomes unavailable or when system maintenance is performed. Users must be able to interact with the file server through the SMB protocol. Users also must have the ability to manage file permissions by using Windows ACLs.

Which solution will meet these requirements?

- A. Create a single AWS Storage Gateway file gateway.

- B. Create an Amazon FSx for Windows File Server Multi-AZ file system.
- C. Deploy two AWS Storage Gateway file gateways across two Availability Zones. Configure an Application Load Balancer in front
- D. Deploy two Amazon FSx for Windows File Server Single-AZ 2 file systems Configure Microsoft Distributed File System Replication (DFS-R).

Answer: B

Explanation:

Amazon FSx for Windows File Server is a fully managed Windows file system that supports SMB and Windows ACLs natively. The Multi-AZ deployment option provides built-in high availability across two Availability Zones, with automatic failover during AZ outages or maintenance, ensuring continuous access to the file share without additional custom replication or load balancing.

QUESTION 12

A company has a web application that is experiencing performance problems many times each night. A root cause analysis reveals sudden increases in CPU utilization that last 5 minutes on an Amazon EC2 Linux instance. A CloudOps engineer must find the process ID (PID) of the service or process that is consuming more CPU.

What should the CloudOps engineer do to collect the process utilization information with the LEAST amount of effort?

- A. Configure the Amazon CloudWatch agent procstat plugin to capture CPU process metrics.
- B. Configure an AWS Lambda function to run every minute to capture the PID and send a notification.
- C. Log in to the EC2 instance by using a .pem key each night. Then run the top command.
- D. Use the default Amazon CloudWatch CPU utilization metric to capture the PID in CloudWatch.

Answer: A

Explanation:

The CloudWatch agent procstat plugin can be configured to automatically collect detailed per-process CPU utilization metrics, including process IDs (PIDs), with minimal setup effort. This eliminates the need for manual monitoring or custom scripts, and integrates directly with CloudWatch for visualization, alerting, and analysis - making it the most efficient and scalable solution.

QUESTION 13

A company needs to monitor its website's availability to end users. The company needs a solution to provide an Amazon Simple Notification Service (Amazon SNS) notification if the website's uptime decreases to less than 99%. The monitoring must provide an accurate view of the user experience on the website.

Which solution will meet these requirements?

- A. Create an Amazon CloudWatch alarm that is based on the website's logs that are published to a CloudWatch Logs log group. Configure the alarm to publish an SNS notification if the number of HTTP 4xx errors and 5xx errors exceeds a specified threshold.
- B. Create an Amazon CloudWatch alarm that is based on the website's published metrics in CloudWatch. Configure the alarm to publish an SNS notification that is based on anomaly detection.
- C. Create an Amazon CloudWatch Synthetics heartbeat monitoring canary. Associate the canary

with the website's URL for end users. Create a CloudWatch alarm for the canary. Configure the alarm to publish an SNS notification if the value of the

- D. Create an Amazon CloudWatch Synthetics broken link checker monitoring canary. Associate the canary with the website's URL for end users. Create a CloudWatch alarm for the canary. Configure the alarm to publish an SNS notification if the value of the SuccessPercent metric is less than 99%.

Answer: C

Explanation:

CloudWatch Synthetics heartbeat canaries simulate real user traffic to continuously monitor website availability and performance from an end-user perspective. By setting a CloudWatch alarm on the SuccessPercent metric and configuring it to send SNS notifications when uptime falls below 99%, the company gains accurate, automated monitoring of actual user experience with minimal operational effort.

QUESTION 14

A company uses Amazon EC2 Auto Scaling across multiple Availability Zones. The company must ensure that EC2 instances are provisioned in private subnets.

The company recently optimized its cloud infrastructure by reducing the number of NAT gateways in the company's VPC to one. Some EC2 instances lost internet connectivity after the infrastructure update. A CloudOps engineer must resolve the connectivity issue.

Which solution will meet this requirement?

- A. Replace the existing NAT gateway with a NAT instance in the same subnet.
- B. Update VPC route tables to target the existing NAT gateway for internet traffic.
- C. Update VPC route tables to target an internet gateway for internet traffic.
- D. Add secondary IP addresses to the existing NAT gateway.

Answer: B

Explanation:

After consolidating to a single NAT gateway, private subnets in other Availability Zones might still have routes pointing to old or deleted NAT gateways. To restore internet connectivity, the CloudOps engineer must update each private subnet's route table so that 0.0.0.0/0 points to the current NAT gateway. This ensures that all private subnets send outbound internet traffic correctly through the existing NAT gateway.

QUESTION 15

A company uses AWS CloudFormation to manage a stack of Amazon EC2 instances on AWS. A CloudOps engineer needs to keep the instances and all of the instances' data, even if someone deletes the stack.

Which solution will meet these requirements?

- A. Set the DeletionPolicy attribute to Snapshot for the EC2 instance resource in the CloudFormation template.
- B. Automate backups by using Amazon Data Lifecycle Manager (Amazon DLM).
- C. Create a backup plan in AWS Backup.
- D. Set the DeletionPolicy attribute to Retain for the EC2 instance resource in the CloudFormation template.

Answer: D

Explanation:

In AWS CloudFormation, setting the DeletionPolicy attribute to Retain ensures that the resource (in this case, the EC2 instance and its associated data) is not deleted when the stack is deleted. This preserves the instance and its data outside of the stack lifecycle, meeting the requirement to keep everything even if the stack is removed.

QUESTION 16

A CloudOps engineer is preparing to deploy an application to Amazon EC2 instances that are in an Auto Scaling group. The application requires dependencies to be installed. Application updates are issued weekly.

The CloudOps engineer needs to implement a solution to incorporate the application updates on a regular basis. The solution also must conduct a vulnerability scan during Amazon Machine Image (AMI) creation.

What is the MOST operationally efficient solution that meets these requirements?

- A. Create a script that uses Packer. Schedule a cron job to run the script.
- B. Install the application and its dependencies on an EC2 instance. Create an AMI of the EC2 instance.
- C. Use EC2 Image Builder with a custom recipe to install the application and its dependencies.
- D. Invoke the EC2 CreateImage API operation by using an Amazon EventBridge scheduled rule.

Answer: C

Explanation:

EC2 Image Builder is a managed service that automates AMI creation on a schedule, including installing dependencies, applying weekly application updates, and running steps such as vulnerability scans as part of the image build pipeline. It provides versioning, automated builds, and integration with scanners via components, giving a highly automated and operationally efficient solution compared to manual scripts or ad hoc AMI creation.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



10% Discount Coupon Code: ASTR14