



Amazon-Web-Services

Exam Questions SOA-C02

AWS Certified SysOps Administrator - Associate (SOA-C02)

NEW QUESTION 1

A company is running an application on premises and wants to use AWS for data backup. All of the data must be available locally. The backup application can write only to block-based storage that is compatible with the Portable Operating System Interface (POSIX). Which backup solution will meet these requirements?

- A. Configure the backup software to use Amazon S3 as the target for the data backups.
- B. Configure the backup software to use Amazon S3 Glacier as the target for the data backups.
- C. Use AWS Storage Gateway, and configure it to use gateway-cached volumes.
- D. Use AWS Storage Gateway, and configure it to use gateway-stored volumes.

Answer: D

NEW QUESTION 2

A company is running a flash sale on its website. The website is hosted on burstable performance Amazon EC2 instances in an Auto Scaling group. The Auto Scaling group is configured to launch instances when the CPU utilization is above 70%. A couple of hours into the sale, users report slow load times and error messages for refused connections. A SysOps administrator reviews Amazon CloudWatch metrics and notices that the CPU utilization is at 20% across the entire fleet of instances. The SysOps administrator must restore the website's functionality without making changes to the network infrastructure. Which solution will meet these requirements?

- A. Activate unlimited mode for the instances in the Auto Scaling group.
- B. Implement an Amazon CloudFront distribution to offload the traffic from the Auto Scaling group.
- C. Move the website to a different AWS Region that is closer to the users.
- D. Reduce the desired size of the Auto Scaling group to artificially increase CPU average utilization.

Answer: C

NEW QUESTION 3

A company has launched a social media website that gives users the ability to upload images directly to a centralized Amazon S3 bucket. The website is popular in areas that are geographically distant from the AWS Region where the S3 bucket is located. Users are reporting that uploads are slow. A SysOps administrator must improve the upload speed. What should the SysOps administrator do to meet these requirements?

- A. Create S3 access points in Regions that are closer to the users.
- B. Create an accelerator in AWS Global Accelerator for the S3 bucket.
- C. Enable S3 Transfer Acceleration on the S3 bucket.
- D. Enable cross-origin resource sharing (CORS) on the S3 bucket.

Answer: A

NEW QUESTION 4

A company using AWS Organizations requires that no Amazon S3 buckets in its production accounts should ever be deleted. What is the SIMPLEST approach the SysOps administrator can take to ensure S3 buckets in those accounts can never be deleted?

- A. Set up MFA Delete on all the S3 buckets to prevent the buckets from being deleted.
- B. Use service control policies to deny the s3:DeleteBucket action on all buckets in production accounts.
- C. Create an IAM group that has an IAM policy to deny the s3:DeleteBucket action on all buckets in production accounts.
- D. Use AWS Shield to deny the s3:DeleteBucket action on the AWS account instead of all S3 buckets.

Answer: B

NEW QUESTION 5

A company hosts its website on Amazon EC2 instances behind an Application Load Balancer. The company manages its DNS with Amazon Route 53, and wants to point its domain's zone apex to the website. Which type of record should be used to meet these requirements?

- A. An AAAA record for the domain's zone apex
- B. An A record for the domain's zone apex
- C. A CNAME record for the domain's zone apex
- D. An alias record for the domain's zone apex

Answer: D

NEW QUESTION 6

A SysOps administrator is maintaining a web application using an Amazon CloudFront web distribution, an Application Load Balancer (ALB), Amazon RDS, and Amazon EC2 in a VPC. All services have logging enabled. The administrator needs to investigate HTTP Layer 7 status codes from the web application. Which log sources contain the status codes? (Choose two.)

- A. VPC Flow Logs
- B. AWS CloudTrail logs
- C. ALB access logs
- D. CloudFront access logs
- E. RDS logs

Answer: CD

NEW QUESTION 7

A SysOps administrator is deploying a test site running on Amazon EC2 instances. The application requires both incoming and outgoing connectivity to the internet. Which combination of steps are required to provide internet connectivity to the EC2 instances? (Choose two.)

- A. Add a NAT gateway to a public subnet.
- B. Attach a private address to the elastic network interface on the EC2 instance.
- C. Attach an Elastic IP address to the internet gateway.
- D. Add an entry to the route table for the subnet that points to an internet gateway.
- E. Create an internet gateway and attach it to a VPC.

Answer: DE

NEW QUESTION 8

A large company is using AWS Organizations to manage its multi-account AWS environment. According to company policy, all users should have read-level access to a particular Amazon S3 bucket in a central account. The S3 bucket data should not be available outside the organization. A SysOps administrator must set up the permissions and add a bucket policy to the S3 bucket. Which parameters should be specified to accomplish this in the MOST efficient manner?

- A. Specify "*" as the principal and PrincipalOrgId as a condition.
- B. Specify all account numbers as the principal.
- C. Specify PrincipalOrgId as the principal.
- D. Specify the organization's master account as the principal.

Answer: A

NEW QUESTION 9

A company must ensure that any objects uploaded to an S3 bucket are encrypted. Which of the following actions will meet this requirement? (Choose two.)

- A. Implement AWS Shield to protect against unencrypted objects stored in S3 buckets.
- B. Implement Object access control list (ACL) to deny unencrypted objects from being uploaded to the S3 bucket.
- C. Implement Amazon S3 default encryption to make sure that any object being uploaded is encrypted before it is stored.
- D. Implement Amazon Inspector to inspect objects uploaded to the S3 bucket to make sure that they are encrypted.
- E. Implement S3 bucket policies to deny unencrypted objects from being uploaded to the buckets.

Answer: CE

NEW QUESTION 10

An organization created an Amazon Elastic File System (Amazon EFS) volume with a file system ID of fs-85ba41fc, and it is actively used by 10 Amazon EC2 hosts. The organization has become concerned that the file system is not encrypted. How can this be resolved?

- A. Enable encryption on each host's connection to the Amazon EFS volume.
- B. Each connection must be recreated for encryption to take effect.
- C. Enable encryption on the existing EFS volume by using the AWS Command Line Interface.
- D. Enable encryption on each host's local drive.
- E. Restart each host to encrypt the drive.
- F. Enable encryption on a newly created volume and copy all data from the original volume.
- G. Reconnect each host to the new volume.

Answer: D

NEW QUESTION 10

A company has a stateful web application that is hosted on Amazon EC2 instances in an Auto Scaling group. The instances run behind an Application Load Balancer (ALB) that has a single target group. The ALB is configured as the origin in an Amazon CloudFront distribution. Users are reporting random logouts from the web application. Which combination of actions should a SysOps administrator take to resolve this problem? (Choose two.)

- A. Change to the least outstanding requests algorithm on the ALB target group.
- B. Configure cookie forwarding in the CloudFront distribution cache behavior.
- C. Configure header forwarding in the CloudFront distribution cache behavior.
- D. Enable group-level stickiness on the ALB listener rule.
- E. Enable sticky sessions on the ALB target group.

Answer: CE

NEW QUESTION 14

A company uses an AWS CloudFormation template to provision an Amazon EC2 instance and an Amazon RDS DB instance. A SysOps administrator must update the template to ensure that the DB instance is created before the EC2 instance is launched. What should the SysOps administrator do to meet this requirement?

- A. Add a wait condition to the template.
- B. Update the EC2 instance user data script to send a signal after the EC2 instance is started.
- C. Add the DependsOn attribute to the EC2 instance resource, and provide the logical name of the RDS resource.
- D. Change the order of the resources in the template so that the RDS resource is listed before the EC2 instance resource.
- E. Create multiple templates.
- F. Use AWS CloudFormation StackSets to wait for one stack to complete before the second stack is created.

Answer: B

NEW QUESTION 18

A SysOps administrator needs to design a high-traffic static website. The website must be highly available and must provide the lowest possible latency to users across the globe. Which solution will meet these requirements?

- A. Create an Amazon S3 bucket, and upload the website content to the S3 bucket
- B. Create an Amazon CloudFront distribution in each AWS Region, and set the S3 bucket as the origin
- C. Use Amazon Route 53 to create a DNS record that uses a geolocation routing policy to route traffic to the correct CloudFront distribution based on where the request originates.
- D. Create an Amazon S3 bucket, and upload the website content to the S3 bucket
- E. Create an Amazon CloudFront distribution, and set the S3 bucket as the origin
- F. Use Amazon Route 53 to create an alias record that points to the CloudFront distribution.
- G. Create an Application Load Balancer (ALB) and a target group
- H. Create an Amazon EC2 Auto Scaling group with at least two EC2 instances in the associated target group
- I. Store the website content on the EC2 instance
- J. Use Amazon Route 53 to create an alias record that points to the ALB.
- K. Create an Application Load Balancer (ALB) and a target group in two Regions
- L. Create an Amazon EC2 Auto Scaling group in each Region with at least two EC2 instances in each target group
- M. Store the website content on the EC2 instance
- N. Use Amazon Route 53 to create a DNS record that uses a geolocation routing policy to route traffic to the correct ALB based on where the request originates.

Answer: A

NEW QUESTION 19

A company has just launched a gamification feature on its mobile app that stores the score of the players to a DynamoDB table. You have been tasked to design a solution to trigger a Lambda function whenever the LeaderBoard attribute of the PlayerScore table is updated. The Lambda function would post a congratulatory message on a social media network.

What's the best solution that can be implemented to trigger the Lambda function on specific events?

- A. Enable DynamoDB Streams to capture table activity and automatically trigger the Lambda function
- B. Create a CloudWatch alarm and automatically trigger the Lambda function
- C. Use Amazon Simple Notification Service to trigger Lambda function
- D. Use AWS Device Farm

Answer: A

Explanation:

Enable DynamoDB Streams to capture table activity and automatically trigger the Lambda function is the correct answer.

Amazon DynamoDB is integrated with AWS Lambda so that you can create triggers—pieces of code that automatically respond to events in DynamoDB Streams. With triggers, you can build applications that react to data modifications in DynamoDB tables.

If you enable DynamoDB Streams on a table, you can associate the stream Amazon Resource Name (ARN) with an AWS Lambda function that you write. Immediately after an item in the table is modified, a new record appears in the table's stream. AWS Lambda polls the stream and invokes your Lambda function synchronously when it detects new stream records.

Create a CloudWatch alarm and automatically trigger the Lambda function is incorrect. Amazon CloudWatch monitors your Amazon Web Services (AWS) resources and the applications you run on AWS in real-time. You can use CloudWatch to collect and track metrics, which are variables you can measure for your resources and applications.

You can create alarms that watch metrics and send notifications or automatically make changes to the resources you are monitoring when a threshold is breached, but can't monitor changes in DynamoDB table data.

Use Amazon Simple Notification Service to trigger Lambda function is incorrect. Amazon Simple Notification Service (Amazon SNS) is a web service that coordinates and manages the delivery or sending of messages to subscribing endpoints or clients. Subscribers (that is, web servers, email addresses, Amazon SQS queues, AWS Lambda functions) consume or receive the message or notification over one of the supported protocols (that is, Amazon SQS, HTTP/S, email, SMS, Lambda) when they are subscribed to the topic.

The Amazon SNS answer can be considered as correct but requires more configuration and is not the best solution.

Use AWS Device Farm is incorrect. Device Farm is an app testing service that you can use to test and interact with your Android, iOS, and web apps on real, physical phones and tablets that are hosted by Amazon Web Services (AWS).

There are two main ways to use Device Farm:

- * 1. Automated testing of apps using a variety of testing frameworks.
- * 2. Remote access of devices onto which you can load, run and interact with apps in real-time.

The Device Farm can't trigger Lambda functions.

NEW QUESTION 21

Which of the following AWS service is a security management service which allows you to centrally configure and manage firewall rules across your accounts and applications in AWS Organization?

- A. AWS Shield
- B. AWS Secrets Manager
- C. AWS WAF
- D. AWS Firewall Manager

Answer: D

Explanation:

AWS Firewall Manager is the correct answer. AWS Firewall Manager is a security management service that allows you to centrally configure and manage firewall rules across your accounts and applications in AWS Organization. As new applications are created, Firewall Manager makes it easy to bring new applications and resources into compliance by enforcing a common set of security rules. Now you have a single service to build firewall rules, create security policies, and enforce them in a consistent, hierarchical manner across your entire infrastructure.

Using AWS Firewall Manager, you can easily roll out AWS WAF rules for your Application Load Balancers, API Gateways, and Amazon CloudFront distributions. Similarly, you can create AWS Shield Advanced protections for your Application Load Balancers, ELB Classic Load Balancers, Elastic IP Addresses and CloudFront distributions. Finally, with AWS Firewall Manager, you can enable security groups for your Amazon EC2 and ENI resource types in Amazon VPCs.

Benefits

- * 1. Simplify management of firewall rules across your accounts
- * 2. Ensure compliance of existing and new applications
- * 3. Easily deploy managed rules across accounts
- * 4. Enable rapid response to internet attacks

AWS Secrets Manager is incorrect. AWS Secrets Manager helps you to securely encrypt, store, and retrieve credentials for your databases and other services. Instead of hardcoding credentials in your apps, you can make calls to Secrets Manager to retrieve your credentials whenever needed. Secrets Manager helps you protect access to your IT resources and data by enabling you to rotate and manage access to your secrets.

AWS Shield is incorrect. AWS provides two levels of protection against DDoS attacks: AWS Shield Standard and AWS Shield Advanced. AWS Shield Standard is automatically included at no extra cost beyond what you already pay for AWS WAF and your other AWS services. For added protection against DDoS attacks, AWS offers AWS Shield Advanced.

AWS WAF is incorrect. AWS WAF is a web application firewall that lets you monitor web requests that are forwarded to Amazon CloudFront distributions or an Application Load Balancer. You can also use AWS WAF to block or allow requests based on conditions that you specify, such as the IP addresses that requests originate from or values in the requests.

NEW QUESTION 23

A company is using IAM with Amazon EC2 to control whether users can perform a task using specific Amazon EC2 API actions and whether they can use specific AWS resources. A SysOps administrator attempts to launch an instance with a role, but he gets an AccessDenied error.

Which actions should the SysOps administrator take to fix this issue?

- A. Modify the bucket policy to allow root user access from the Amazon S3 console or the AWS CLI
- B. Call the IAM GetInstanceProfile action to ensure that you are using a valid instance profile name
- C. Verify that you have the identity-based policy permission to call the action and resource that you have requested
- D. Verify that your temporary security credentials haven't expired

Answer: B

Explanation:

Call the IAM GetInstanceProfile action to ensure that you are using a valid instance profile name is the correct answer. When you attempt to launch an instance with a role and get an AccessDenied error check the following:

- * 1. Launch an instance without an instance profile. This will help ensure that the problem is limited to IAM roles for Amazon EC2 instances.
- * 2. If you are making requests as an IAM user, verify that you have the following permissions: ec2:RunInstances with a wildcard resource ("*") iam:PassRole with the resource matching the role ARN (for example, arn:aws:iam::999999999999:role/ExampleRoleName)
- * 3. Call the IAM GetInstanceProfile action to ensure that you are using a valid instance profile name or a valid instance profile ARN.
- * 4. Call the IAM GetInstanceProfile action to ensure that the instance profile has a role. Empty instance profiles will fail with an AccessDenied error.

NEW QUESTION 26

A company for compliance purposes needs to assess how well its resource configurations comply with internal practices, industry guidelines, and regulations. Which tool should a SysOps administrator use to meet these requirements?

- A. AWS Security Hub
- B. AWS Shield
- C. AWS Health
- D. AWS Config

Answer: D

Explanation:

AWS Config is the correct answer. AWS Config can be used to assess how well your resource configurations comply with internal practices, industry guidelines, and regulations.

AWS Security Hub is incorrect. AWS Security Hub provides you with a comprehensive view of your security state in AWS and helps you check your environment against security industry standards and best practices.

Security Hub collects security data from across AWS accounts, services, and supported third-party partner products and helps you analyze your security trends and identify the highest priority security issues.

AWS Shield is incorrect. AWS provides two levels of protection against DDoS attacks: AWS Shield Standard and AWS Shield Advanced. AWS Shield Standard is automatically included at no extra cost beyond what you already pay for AWS WAF and your other AWS services.

For added protection against DDoS attacks, AWS offers AWS Shield Advanced. AWS Shield Advanced provides expanded DDoS attack protection for your Amazon EC2 instances, Elastic Load Balancing load balancers, Amazon CloudFront distributions, and Amazon Route 53 hosted zones. AWS Health is incorrect. AWS Health provides personalized information about events that can affect your AWS infrastructure, guides you through scheduled changes, and accelerates the troubleshooting of issues that affect your AWS resources and accounts.

NEW QUESTION 30

Which of the following recommendations is NOT considered a best practice for using AWS CloudFormation more effectively and securely throughout its entire workflow?

- A. Reuse templates to replicate stacks in multiple environments
- B. Use nested stacks to reuse common template patterns
- C. Embed credentials in your templates
- D. Use IAM to control access

Answer: C

Explanation:

Embed credentials in your templates is the correct answer as it is not considered a best practice for using AWS CloudFormation effectively. Best practices are recommendations that can help you use AWS CloudFormation more effectively and securely throughout its entire workflow. Learn how to plan and organize your stacks, create templates that describe your resources and the software applications that run on them, and manage your stacks and their resources. The following best practices are based on real-world experience from current AWS CloudFormation customers.

* 1. Organize your stacks by lifecycle and ownership

Use the lifecycle and ownership of your AWS resources to help you decide what resources should go in each stack. Initially, you might put all your resources in one stack, but as your stack grows in scale and broadens in scope, managing a single stack can be cumbersome and time-consuming.

* 2. Use IAM to control access

IAM is an AWS service that you can use to manage users and their permissions in AWS. You can use IAM with AWS CloudFormation to specify what AWS CloudFormation actions users can perform, such as viewing stack templates, creating stacks, or deleting stacks.

* 3. Verify quotas for all resource types

Before launching a stack, ensure that you can create all the resources that you want without hitting your AWS account limits. If you hit a limit, AWS CloudFormation won't create your stack successfully until you increase your quota or delete extra resources.

* 4. Reuse templates to replicate stacks in multiple environments

After you have your stacks and resources set up, you can reuse your templates to replicate your infrastructure in multiple environments. For example, you can create environments for development, testing, and production so that you can test changes before implementing them into production.

* 5. Do not embed credentials in your templates

Rather than embedding sensitive information in your AWS CloudFormation templates, we recommend you use dynamic references in your stack template. Dynamic references provide a compact, powerful way for you to reference external values that are stored and managed in other services, such as the AWS Systems Manager Parameter Store or AWS Secrets Manager.

NEW QUESTION 32

Suppose you have ELB load balancers in the US West (Oregon) Region and in the Asia Pacific (Singapore) Region and you created a latency record for each load balancer. What will happen when a user in London enters the name of your domain in a browser? (Choose all that apply.)

- A. If latency is lower between the London and Oregon regions, Route 53 responds to the query with the IP address for the Singapore load balancer
- B. If latency is lower between the London and Oregon regions, Route 53 responds to the query with the IP address for the Oregon load balancer
- C. DNS routes the query to a Route 53 name server
- D. Route 53 refers to its data on latency ONLY between London and the Singapore region
- E. Route 53 refers to its data on latency between London and the Singapore region and between London and the Oregon region

Answer: BCE

Explanation:

Explanation/Reference:

The correct answers are:

* 1. DNS routes the query to a Route 53 name server

* 2. Route 53 refers to its data on latency between London and the Singapore region and between London and the Oregon region

* 3. If latency is lower between the London and Oregon regions, Route 53 responds to the query with the IP address for the Oregon load balancer

If your application is hosted in multiple AWS Regions, you can improve performance for your users by serving their requests from the AWS Region that provides the lowest latency.

To use latency-based routing, you create latency records for your resources in multiple AWS Regions. When Route 53 receives a DNS query for your domain or subdomain (example.com or acme.example.com), it determines which AWS Regions you've created latency records for, determines which region gives the user the lowest latency, and then selects a latency record for that region. Route 53 responds with the value from the selected record, such as the IP address for a web server.

For example, suppose you have ELB load balancers in the US West (Oregon) Region and in the Asia Pacific (Singapore) Region. You created a latency record for each load balancer. Here's what happens when a user in London enters the name of your domain in a browser:

* 1. DNS routes the query to a Route 53 name server.

* 2. Route 53 refers to its data on latency between London and the Singapore region and between

London and the Oregon region.

* 3. If latency is lower between the London and Oregon regions, Route 53 responds to the query with the IP address for the Oregon load balancer. If latency is lower between London and the Singapore region, Route 53 responds with the IP address for the Singapore load balancer.

NEW QUESTION 36

A SysOps Administrator has implemented an Auto Scaling group with a step scaling policy. The Administrator notices that the additional instances have not been included in the aggregated metrics. Why are the additional instances missing from the aggregated metrics?

- A. The warm-up period has not expired
- B. The instances are still in the boot process
- C. The instances have not been attached to the Auto Scaling group
- D. The instances are included in a different set of metrics

Answer: B

NEW QUESTION 37

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SOA-C02 Practice Exam Features:

- * SOA-C02 Questions and Answers Updated Frequently
- * SOA-C02 Practice Questions Verified by Expert Senior Certified Staff
- * SOA-C02 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SOA-C02 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SOA-C02 Practice Test Here](#)