Leads4Pass

SOA-C02^{Q&As}

AWS Certified SysOps Administrator - Associate (SOA-C02)

Pass Amazon SOA-C02 Exam with 100% Guarantee

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

https://www.leads4pass.com/soa-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

A company asks a SysOps administrator to ensure that AWS CloudTrail files are not tampered with after they are created. Currently, the company uses AWS Identity and Access Management (IAM) to restrict access to specific trails. The company\\'s security team needs the ability to trace the integrity of each file.

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

A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function when a new file is delivered. Configure the Lambda function to compute an MD5 hash check on the file and store the result in an Amazon DynamoDB table. The security team can use the values that are stored in DynamoDB to verify the integrity of the delivered files.

B. Create an AWS Lambda function that is invoked each time a new file is delivered to the CloudTrail bucket. Configure the Lambda function to compute an MD5 hash check on the file and store the result as a tag in an Amazon S3 object. The security team can use the information in the tag to verify the integrity of the delivered files.

C. Enable the CloudTrail file integrity feature on an Amazon S3 bucket. Create an IAM policy that grants the security team access to the file integrity logs that are stored in the S3 bucket.

D. Enable the CloudTrail file integrity feature on the trail. The security team can use the digest file that is created by CloudTrail to verify the integrity of the delivered files.

Correct Answer: D

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html "When you enable log file integrity validation, CloudTrail creates a hash for every log file that it delivers. Every hour, CloudTrail also creates and delivers a file that references the log files for the last hour and contains a hash of each. This file is called a digest file. Validated log files are invaluable in security and forensic investigations"

QUESTION 2

A SysOps administrator creates a new VPC that includes a public subnet and a private subnet. The SysOps administrator successfully launches 11 Amazon EC2 instances in the private subnet. The SysOps administrator attempts to launch one more EC2 instance in the same subnet. However, the SysOps administrator receives an error message that states that not enough free IP addresses are available.

What must the SysOps administrator do to deploy more EC2 instances?

A. Edit the private subnet to change the CIDR block to /27.

B. Edit the private subnet to extend across a second Availability Zone.

C. Assign additional Elastic IP addresses to the private subnet.

D. Create a new private subnet to hold the required EC2 instances.

Correct Answer: D

Add an additional IPv4 CIDR block as a secondary CIDR to your VPC.

Create a new VPC with your preferred CIDR block and then migrate the resources from your old VPC to the new VPC (if applicable).

QUESTION 3

An errant process is known to use an entire processor and run at 100% A SysOps administrator wants to automate restarting the instance once the problem occurs for more than 2 minutes. How can this be accomplished?

A. Create an Amazon CloudWatch alarm for the Amazon EC2 instance with basic monitoring Enable an action to restart the instance

B. Create a CloudWatch alarm for the EC2 instance with detailed monitoring Enable an action to restart the instance

C. Create an AWS Lambda function to restart the EC2 instance triggered on a scheduled basis every 2 minutes

D. Create a Lambda function to restart the EC2 instance, triggered by EC2 health checks

Correct Answer: B

QUESTION 4

A company creates custom AMI images by launching new Amazon EC2 instances from an AWS CloudFormation template it installs and configure necessary software through AWS OpsWorks and takes images of each EC2 instance. The

process of installing and configuring software can take between 2 to 3 hours but at limes the process stalls due to installation errors.

The SysOps administrator must modify the CloudFormation template so if the process stalls, the entire stack will tail and roil back.

Based on these requirements what should be added to the template?

A. Conditions with a timeout set to 4 hours.

B. CreationPolicy with timeout set to 4 hours.

C. DependsOn a timeout set to 4 hours.

D. Metadata with a timeout set to 4 hours

Correct Answer: B

When you provision an Amazon EC2 instance in an AWS CloudFormation stack, you might specify additional actions to configure the instance, such as install software packages or bootstrap applications. Normally, CloudFormation proceeds with stack creation after the instance has been successfully created. However, you can use a CreationPolicy so that CloudFormation proceeds with stack creation only after your configuration actions are done. That way you'll know your applications are ready to go after stack creation succeeds.

A CreationPolicy instructs CloudFormation to wait on an instance until CloudFormation receives the specified number of signals. This policy takes effect only when CloudFormation creates the instance.

Ref link: https://aws.amazon.com/blogs/devops/use-a-creationpolicy-to-wait-for-on-instance-configurations/ Ref link: https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-creationpolicy.html

QUESTION 5

A company runs an application on an Amazon EC2 instance A SysOps administrator creates an Auto Scaling group and an Application Load Balancer (ALB) to handle an increase in demand However, the EC2 instances are failing tie health check.

What should the SysOps administrator do to troubleshoot this issue?

A. Verity that the Auto Scaling group is configured to use all AWS Regions.

B. Verily that the application is running on the protocol and the port that the listens is expecting.

C. Verify the listener priority in the ALB Change the priority if necessary.

D. Verify the maximum number of instances in the Auto Scaling group Change the number if necessary

Correct Answer: B

[Latest SOA-C02 Dumps](#)   [SOA-C02 Exam Questions](#)   [SOA-C02 Braindumps](#)