



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.geekcert.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

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 2

A company has a new requirement stating that all resources in AWS must be tagged according to a set policy.

Which AWS service should be used to enforce and continually identify all resources that are not in compliance with the policy?

- A. AWS CloudTrail
- B. Amazon Inspector
- C. AWSConfig
- D. AWS Systems Manager

Correct Answer: C

QUESTION 3

A company is using Amazon CloudFront to serve static content for its web application to its users. The CloudFront distribution uses an existing on-premises website as a custom origin.

The company requires the use of TLS between CloudFront and the origin server. This configuration has worked as expected for several months. However, users are now experiencing HTTP 502 (Bad Gateway) errors when they view webpages that include content from the CloudFront distribution.

What should a SysOps administrator do to resolve this problem?

- A. Examine the expiration date on the certificate on the origin site. Validate that the certificate has not expired. Replace the certificate if necessary.
- B. Examine the hostname on the certificate on the origin site. Validate that the hostname matches one of the hostnames on the CloudFront distribution. Replace the certificate if necessary.



C. Examine the firewall rules that are associated with the origin server. Validate that port 443 is open for inbound traffic from the internet. Create an inbound rule if necessary.

D. Examine the network ACL rules that are associated with the CloudFront distribution. Validate that port 443 is open for outbound traffic to the origin server. Create an outbound rule if necessary.

Correct Answer: A

HTTP 502 errors from CloudFront can occur because of the following reasons:

There's an SSL negotiation failure because the origin is using SSL/TLS protocols and ciphers that aren't supported by CloudFront.

There's an SSL negotiation failure because the SSL certificate on the origin is expired or invalid, or because the certificate chain is invalid. There's a host header mismatch in the SSL negotiation between your CloudFront distribution and the

custom origin.

The custom origin isn't responding on the ports specified in the origin settings of the CloudFront distribution.

The custom origin is ending the connection to CloudFront too quickly.

<https://aws.amazon.com/premiumsupport/knowledge-center/resolve-cloudfront-connection-error/>

QUESTION 4

A developer creates a web application that runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are in an Auto Scaling group. The developer reviews the deployment and notices some suspicious traffic to the application. The traffic is malicious and is coming from a single public IP address. A SysOps administrator must block the public IP address.

Which solution will meet this requirement?

A. Create a security group rule to deny all inbound traffic from the suspicious IP address. Associate the security group with the ALB.

B. Implement Amazon Detective to monitor traffic and to block malicious activity from the internet. Configure Detective to integrate with the ALB.

C. Implement AWS Resource Access Manager (AWS RAM) to manage traffic rules and to block malicious activity from the internet. Associate AWS RAM with the ALB.

D. Add the malicious IP address to an IP set in AWS WAF. Create a web ACL. Include an IP set rule with the action set to BLOCK. Associate the web ACL with the ALB.

Correct Answer: D

Add the malicious IP address to an IP set in AWS WAF. Create a web ACL. Include an IP set rule with the action set to BLOCK. Associate the web ACL with the ALB.

QUESTION 5



A SysOps administrator receives an alert that a production Auto Scaling group has been scaled down to two Amazon EC2 instances. The Auto Scaling group was originally configured with a minimum capacity of three instances. However, the SysOps administrator confirms that the configuration now reflects a minimum capacity of two instances.

Which AWS service will help identify who made the change?

- A. AWS Config
- B. Amazon Inspector
- C. Amazon Macie
- D. Amazon Cloud Watch Logs

Correct Answer: A

[SOA-C02 PDF Dumps](#)

[SOA-C02 Study Guide](#)

[SOA-C02 Exam Questions](#)