Vendor: Amazon

Exam Code:SOA-C02

Exam Name:AWS Certified SysOps Administrator - Associate (SOA-C02)

Version: Demo

QUESTION 1

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 2

A company is supposed to receive a data file every hour in an Amazon S3 bucket. An S3 event notification invokes an AWS Lambda function each time a file arrives. The function processes the data for use by an application.

The application team notices that sometimes the file does not arrive. The application team wants to receive a notification whenever the file does not arrive.

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

A. Add an S3 Lifecycle rule on the S3 bucket with a scope that is limited to objects that were created in the last hour.

Configure another S3 event notification to be invoked by the lifecycle transition when the number of objects transitioned is zero. Publish a message to an Amazon Simple Notification Service (Amazon SNS) topic to notify the application team.

B. Configure another S3 event notification to invoke a Lambda function that posts a message to an Amazon Simple Queue Service (Amazon SQS) queue. Create an Amazon CloudWatch alarm to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic to notify the application team when the ApproximateAgeOfOldestMessage metric of the queue is greater than 1 hour.

C. Create an Amazon CloudWatch alarm to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic to alert the application team when the Invocations metric of the Lambda function is zero for an hour. Configure the alarm to treat missing data as breaching.

D. Create a new Lambda function to get the timestamp of the newest file in the S3 bucket. If the timestamp is more than 1 hour ago, publish a message to an Amazon Simple Notification Service (Amazon SNS) topic to notify the application team. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke the new function hourly.

Correct Answer: C

QUESTION 3

With the threat of ransomware viruses encrypting and holding company data hostage, which action should be taken to protect an Amazon S3 bucket?

A. Deny Post. Put. and Delete on the bucket.

B. Enable server-side encryption on the bucket.

C. Enable Amazon S3 versioning on the bucket.

D. Enable snapshots on the bucket.

Correct Answer: B

QUESTION 4

A company stores its data in an Amazon S3 bucket. The company is required to classify the data and find any sensitive personal information in its S3 files. Which solution will meet these requirements?

A. Create an AWS Config rule to discover sensitive personal information in the S3 files and mark them as noncompliant.

B. Create an S3 event-driven artificial intelligence/machine learning (AI/ML) pipeline to classify sensitive personal information by using Amazon Recognition.

C. Enable Amazon GuardDuty. Configure S3 protection to monitor all data inside Amazon S3.

D. Enable Amazon Macie. Create a discovery job that uses the managed data identifier.

Correct Answer: D

Amazon Macie is a security service designed to help organizations find, classify, and protect sensitive data stored in Amazon S3. Amazon Macie uses machine learning to automatically discover, classify, and protect sensitive data in

Amazon S3. Creating a discovery job with the managed data identifier will allow Macie to identify sensitive personal information in the S3 files and classify it accordingly. Enabling AWS Config and Amazon GuardDuty will not help with this requirement as they are not designed to automatically classify and protect data.

QUESTION 5

A company hosts an internal application on Amazon EC2 instances. All application data and requests route through an AWS Site-to-Site VPN connection between the on-premises network and AWS. The company must monitor the application for changes that allow network access outside of the corporate network. Any change that exposes the application externally must be restricted automatically.

Which solution meets these requirements in the MOST operationally efficient manner?

A. Create an AWS Lambda function that updates security groups that are associated with the elastic network interface to remove inbound rules with noncorporate CIDR ranges. Turn on VPC Flow Logs, and send the logs to Amazon CloudWatch Logs. Create an Amazon CloudWatch alarm that matches traffic from noncorporate CIDR ranges, and publish a message to an Amazon Simple Notification Service (Amazon SNS) topic with the Lambda function as a target.

B. Create a scheduled Amazon EventBridge (Amazon CloudWatch Events) rule that targets an AWS Systems Manager Automation document to check for public IP addresses on the EC2 instances. If public IP addresses are found on the EC2 instances, initiate another Systems Manager Automation document to terminate the instances.

C. Configure AWS Config and a custom rule to monitor whether a security group allows inbound requests from noncorporate CIDR ranges. Create an AWS Systems Manager Automation document to remove any noncorporate CIDR ranges from the application security groups.

D. Configure AWS Config and the managed rule for monitoring public IP associations with the EC2 instances by tag. Tag the EC2 instances with an identifier. Create an AWS Systems Manager Automation document to remove the public IP association from the EC2 instances.

Correct Answer: C

https://aws.amazon.com/blogs/security/how-to-auto-remediate-internet-accessible-ports-with-aws-config-and-aws-system-manager/

QUESTION 6

CORRECT TEXT Update an existing AWS CloudFormation stack. If needed, a copy 0t the CloudFormation template is available in an Amazon SB bucket named cloudformation-bucket

1.

Use the us-east-2 Region for all resources.

2.

Unless specified below, use the default configuration settings.

3.

update the Amazon EQ instance named Devinstance by making the following changes to the stack named 1700182:

a) Change the EC2 instance type to us-east-t2.nano.

b) Allow SSH to connect to the EC2 instance from the IP address range 192.168.100.0/30.

c) Replace the instance profile IAM role with IamRoleB.

4.

Deploy the changes by updating the stack using the CFServiceR01e role.

5.

Edit the stack options to prevent accidental deletion.

6.

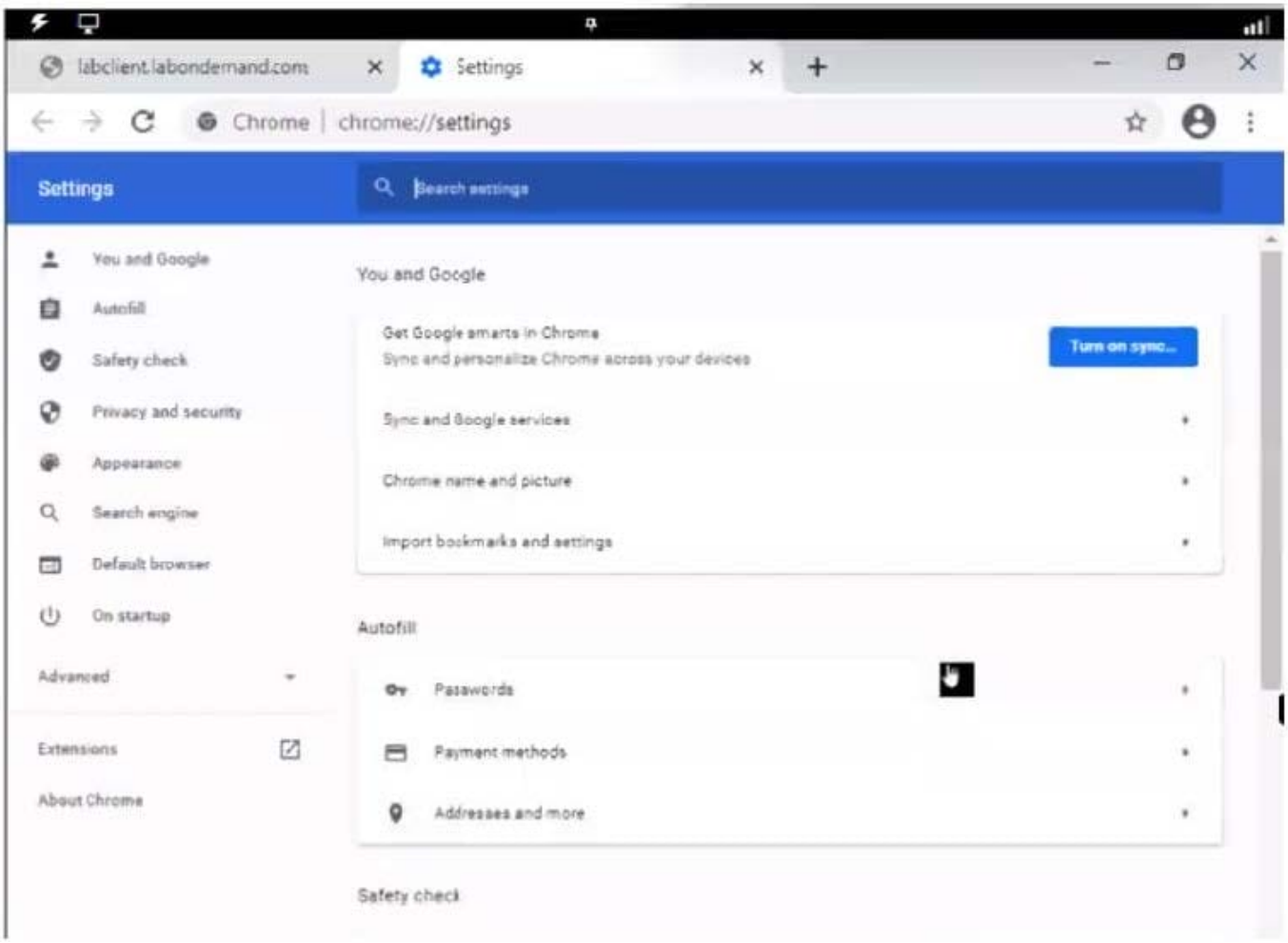
Using the output from the stack, enter the value of the ProdInstanceId in the text box below:

A. Check the answer in explanation.

B. Place Holder

Correct Answer: A

Solution as given below.



QUESTION 7

A company has a web application with a database tier that consists of an Amazon EC2 instance that runs MySQL. A SysOps administrator needs to minimize potential data loss and the time that is required to recover in the event of a database failure.

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

A. Create an Amazon CloudWatch alarm for the StatusCheckFailed_System metric to invoke an AWS Lambda function that stops and starts the EC2 instance.

B. Create an Amazon RDS for MySQL Multi-AZ DB instance. Use a MySQL native backup that is stored in Amazon S3 to restore the data to the new database. Update the connection string in the web application.

C. Create an Amazon RDS for MySQL Single-AZ DB instance with a read replica. Use a MySQL native backup that is stored in Amazon S3 to restore the data to the new database. Update the connection string in the web application.

D. Use Amazon Data Lifecycle Manager (Amazon DLM) to take a snapshot of the Amazon Elastic Block Store (Amazon EBS) volume every hour. In the event of an EC2 instance failure, restore the EBS volume from a snapshot.

Correct Answer: D

To me both BandD minimize potential data loss.

However, the question is not specifying availability (Multi-AZ is B)

Instead, the question is emphasizing quick recovery from backup (not active/active recovery)

Therefore, I think only option D meets both criteria for minimizing potential data loss and quick recovery.

-1 Hour RPO (only D specifies hourly snapshots and hourly RPO)

-Snapshots (D) have faster RTO than native backup restore from S3 (B)

In the real world, I\\'ve used both backups (regularly/scheduled) and snapshots (prior to scheduled changes, etc.)

QUESTION 8

An Amazon EC2 instance is running an application that uses Amazon Simple Queue Service (Amazon SQS} queues A SysOps administrator must ensure that the application can read, write, and delete messages from the SQS queues

Which solution will meet these requirements in the MOST secure manner?

A. Create an IAM user with an IAM policy that allows the sqs SendMessage permission, the sqs ReceiveMessage permission, and the sqs DeleteMessage permission to the appropriate queues Embed the IAM user\\'s credentials in the application\\'s configuration

B. Create an IAM user with an IAM policy that allows the sqs SendMessage permission, the sqs ReceiveMessage permission, and the sqs DeleteMessage permission to the appropriate queues Export the IAM user\\'s access key and secret access key as environment variables on the EC2 instance

C. Create and associate an IAM role that allows EC2 instances to call AWS services Attach an IAM policy to the role that allows sqs." permissions to the appropriate queues

D. Create and associate an IAM role that allows EC2 instances to call AWS services Attach an IAM policy to the role that allows the sqs SendMessage permission, the sqs ReceiveMessage permission, and the sqs DeleteMessage permission to the appropriate queues

Correct Answer: D

QUESTION 9

A SysOps administrator has enabled AWS CloudTrail in an AWS account If CloudTrail is disabled it must be re-enabled immediately.

What should the SysOps administrator do to meet these requirements WITHOUT writing custom code\\'\\'

A. Add the AWS account to AWS Organizations Enable CloudTrail in the management account

B. Create an AWS Config rule that is invoked when CloudTrail configuration changes Apply the AWS-ConfigureCloudTrailLogging automatic remediation action

C. Create an AWS Config rule that is invoked when CloudTrail configuration changes Configure the rule to invoke an AWS Lambda function to enable CloudTrail

D. Create an Amazon EventBridge (Amazon CloudWatch Events) hourly rule with a schedule pattern to run an AWS Systems Manager Automation document to enable CloudTrail

Correct Answer: B

QUESTION 10

A company is implementing a monitoring solution that is based on machine learning. The monitoring solution consumes Amazon EventBridge (Amazon CloudWatch Events) events that are generated by Amazon EC2 Auto Scaling. The monitoring solution provides detection of anomalous behavior such as unanticipated scaling events and is configured as an EventBridge (CloudWatch Events) API destination.

During initial testing, the company discovers that the monitoring solution is not receiving events. However, Amazon CloudWatch is showing that the EventBridge (CloudWatch Events) rule is being invoked. A SysOps administrator must implement a solution to retrieve client error details to help resolve this issue. Which solution will meet these requirements with the LEAST operational effort?

A. Create an EventBridge (CloudWatch Events) archive for the event pattern to replay the events. Increase the logging on the monitoring solution. Use replay to invoke the monitoring solution. Examine the error details.

B. Add an Amazon Simple Queue Service (Amazon SQS) standard queue as a dead-letter queue for the target. Process the messages in the dead-letter queue to retrieve error details.

C. Create a second EventBridge (CloudWatch Events) rule for the same event pattern to target an AWS Lambda function. Configure the Lambda function to invoke the monitoring solution and to record the results to Amazon CloudWatch Logs. Examine the errors in the logs.

D. Configure the EventBridge (CloudWatch Events) rule to send error messages to an Amazon Simple Notification Service (Amazon SNS) topic.

Correct Answer: A

You can now create an encrypted archive of the events published to an event bus. You can archive all events, or filter them using the same pattern matching syntax used by EventBridge rules. You can store events indefinitely, or set up a

retention period after which older events are automatically removed from the archive.

You can also replay the events stored in an archive. Events are replayed to all rules defined for the event bus (but not to managed rules created by other AWS services) or to the rules you specify. Replayed events contain an extra replay-

name field in case you need to recognize them. When starting a replay, you define a time frame, and only events within that time frame are replayed. Currently, you can only replay events to the same event bus from which they were archived.

QUESTION 11

A company uses Amazon Elasticsearch Service (Amazon ES) to analyze sales and customer usage data. Members of the company\\'s geographically dispersed sales team are traveling. They need to log in to Kibana by using their existing corporate credentials that are stored in Active Directory. The company has deployed Active Directory Federation Services (AD FS) to enable authentication to cloud services.

Which solution will meet these requirements?

A. Configure Active Directory as an authentication provider in Amazon ES. Add the Active Directory server\\'s domain

name to Amazon ES. Configure Kibana to use Amazon ES authentication.

B. Deploy an Amazon Cognito user pool. Configure Active Directory as an external identity provider for the user pool. Enable Amazon Cognito authentication for Kibana on Amazon ES.

C. Enable Active Directory user authentication in Kibana. Create an IP-based custom domain access policy in Amazon ES that includes the Active Directory server\\'s IP address.

D. Establish a trust relationship with Kibana on the Active Directory server. Enable Active Directory user authentication in Kibana. Add the Active Directory server\\'s IP address to Kibana.

Correct Answer: B

https://aws.amazon.com/blogs/security/how-to-enable-secure-access-to-kibana-using-aws-single-sign-on/
https://docs.aws.amazon.com/elasticsearch-service/latest/developerguide/es-cognito-auth.html

---

QUESTION 12

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