DUMPSBOSS.COM

# Associate AWS Certified SysOps Administrator - Associate (SOA-C02)

## Amazon AWS SOA-C02

## Version Demo

**Total Demo Questions: 15**

**Total Premium Questions: 305**

**Buy Premium PDF**

https://dumpsboss.com

support@dumpsboss.com

# Topic Break Down

| Topic | No. of Questions |
|---|---|
| Topic 1, Mix Questions | 301 |
| Topic 2, Simulation | 4 |
| Total | 305 |

## QUESTION NO: 1

A company has a critical serverless application that uses multiple AWS Lambda functions. Each Lambda function generates 1 GB of log data daily in its own Amazon CloudWatch Logs log group. The company's security team asks for a count of application errors, grouped by type, across all of the log groups.

What should a SysOps administrator do to meet this requirement?

**A.** Perform a CloudWatch Logs Insights query that uses the stats command and count function.

**B.** Perform a CloudWatch Logs search that uses the groupby keyword and count function.

**C.** Perform an Amazon Athena query that uses the SELECT and GROUP BY keywords.

**D.** Perform an Amazon RDS query that uses the SELECT and GROUP BY keywords.

**ANSWER: A**

## QUESTION NO: 2

A company has an existing web application that runs on two Amazon EC2 instances behind an Application Load Balancer (ALB) across two Availability Zones The application uses an Amazon RDS Multi-AZ DB Instance Amazon Route 53 record sets route requests tor dynamic content to the load balancer and requests for static content to an Amazon S3 bucket Site visitors are reporting extremely long loading times.

Which actions should be taken to improve the performance of the website? (Select TWO )

**A.** Add Amazon CloudFront caching for static content

**B.** Change the load balancer listener from HTTPS to TCP

**C.** Enable Amazon Route 53 latency-based routing

**D.** Implement Amazon EC2 Auto Scaling for the web servers

**E.** Move the static content from Amazon S3 to the web servers

**ANSWER: A D**

## QUESTION NO: 3

A SysOps administrator needs to delete an AWS CloudFormation stack that is no longer in use. The CloudFormation stack is in the DELETE_FAILED state. The SysOps administrator has validated the permissions that are required to delete the Cloud Formation stack.

**A.** The configured timeout to delete the stack was too low for the delete operation to complete.

**B.** The stack contains nested stacks that must be manually deleted fast.

**C.** The stack was deployed with the -disable rollback option.

**D.** There are additional resources associated with a security group in the stack

**E.** There are Amazon S3 buckets that still contain objects in the stack.

**ANSWER: D E**

## QUESTION NO: 4

A company is using an AWS KMS customer master key (CMK) with imported key material The company references the CMK by its alias in the Java application to encrypt data The CMK must be rotated every 6 months

What is the process to rotate the key?

**A.** Enable automatic key rotation for the CMK and specify a period of 6 months

**B.** Create a new CMK with new imported material, and update the key alias to point to the new CMK.

**C.** Delete the current key material, and import new material into the existing CMK

**D.** Import a copy of the existing key material into a new CMK as a backup, and set the rotation schedule for 6 months

**ANSWER: B**

## QUESTION NO: 5

A company's reporting job that used to run in 15 minutes is now taking an hour to run. An application generates the reports. The application runs on Amazon EC2 instances and extracts data from an Amazon RDS for MySQL database.

A SysOps administrator checks the Amazon CloudWatch dashboard for the RDS instance and notices that the Read IOPS metrics are high, even when the reports are not running. The SysOps administrator needs to improve the performance and the availability of the RDS instance.

Which solution will meet these requirements?

**A.** Configure an Amazon ElastiCache cluster in front of the RDS instance. Update the reporting job to query the ElastiCache cluster.

**B.** Deploy an RDS read replica. Update the reporting job to query the reader endpoint.

**C.** Create an Amazon CloudFront distribution. Set the RDS instance as the origin. Update the reporting job to query the CloudFront distribution.

**D.** Increase the size of the RDS instance.

**ANSWER: B**

**Explanation:**

Using an RDS read replica will improve the performance and availability of the RDS instance by offloading read queries to the replica. This will also ensure that the reporting job completes in a timely manner and does not affect the performance of other queries that might be running on the RDS instance. Additionally, updating the reporting job to query the reader endpoint will ensure that all read queries are directed to the read replica.

Reference: [1] https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

## QUESTION NO: 6

A SysOps administrator has an AWS CloudFormation template of the company's existing infrastructure in us-west-2. The administrator attempts to use the template to launch a new stack in eu-west-1, but the stack only partially deploys, receives an error message, and then rolls back.

Why would this template fail to deploy? (Select TWO.)

**A.** The template referenced an IAM user that is not available in eu-west-1.

**B.** The template referenced an Amazon Machine Image (AMI) that is not available in eu-west-1.

**C.** The template did not have the proper level of permissions to deploy the resources.

**D.** The template requested services that do not exist in eu-west-1.

**E.** CloudFormation templates can be used only to update existing services.

**ANSWER: B D**

## QUESTION NO: 7

A company's SysOps administrator has created an Amazon EC2 instance with custom software that will be used as a template for all new EC2 instances across multiple AWS accounts. The Amazon Elastic Block Store (Amazon EBS) volumes that are attached to the EC2 instance are encrypted with AWS managed keys.

The SysOps administrator creates an Amazon Machine Image (AMI) of the custom EC2 instance and plans to share the AMI with the company's other AWS accounts. The company requires that all AMIs are encrypted with AWS Key Management Service (AWS KMS) keys and that only authorized AWS accounts can access the shared AMIs.

Which solution will securely share the AMI with the other AWS accounts?

**A.** In the account where the AMI was created, create a customer master key (CMK). Modify the key policy to provide kms:DescribeKey, kms ReEncrypf, kms:CreateGrant, and kms:Decrypt permissions to the AWS accounts that the AMI will be shared with. Modify the AMI permissions to specify the AWS account numbers that the AMI will be shared with.

**B.** In the account where the AMI was created, create a customer master key (CMK). Modify the key policy to provide kms:DescribeKey, kms:ReEncrypt*. kms:CreateGrant, and kms;Decrypt permissions to the AWS accounts that the AMI will be shared with. Create a copy of the AMI. and specify the CMK. Modify the permissions on the copied AMI to specify the AWS account numbers that the AMI will be shared with.

**C.** In the account where the AMI was created, create a customer master key (CMK). Modify the key policy to provide kms:DescrlbeKey, kms:ReEncrypt\ kms:CreateGrant, and kms:Decrypt permissions to the AWS accounts that the AMI will be shared with. Create a copy of the AMI. and specify the CMK. Modify the permissions on the copied AMI to make it public.

**D.** In the account where the AMI was created, modify the key policy of the AWS managed key to provide kms:DescnbeKey. kms:ReEncrypt\ kms:CreateGrant, and kms:Decrypt permissions to the AWS accounts that the AMI will be shared with. Modify the AMI permissions to specify the AWS account numbers that the AMI will be shared with.

**ANSWER: B**

**Explanation:**

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sharingamis-explicit.html

## QUESTION NO: 8

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: C D**

**Explanation:**

"C" because Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html

"D" because "you can configure CloudFront to create log files that contain detailed information about every user request that CloudFront receives"

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html

## QUESTION NO: 9

A SysOps administrator noticed that the cache hit ratio for an Amazon CloudFront distribution is less than 10%.

Which collection of configuration changes will increase the cache hit ratio for the distribution? (Select TWO.)

**A.** Ensure that only required cookies, query strings, and headers are forwarded in the Cache Behavior Settings.

**B.** Change the Viewer Protocol Policy to use HTTPS only.

**C.** Configure the distribution to use presigned cookies and URLs to restrict access to the distribution.

**D.** Enable automatic compression of objects in the Cache Behavior Settings.

**E.** Increase the CloudFront time to live (TTL) settings in the Cache Behavior Settings.

**ANSWER: A E**

**Explanation:**

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cache-hit-ratio.html#cache-hit-ratio-http-streaming

## QUESTION NO: 10

A SysOps administrator launches an Amazon EC2 Linux instance in a public subnet. When the instance is running, the SysOps administrator obtains the public IP address and attempts to remotely connect to the instance multiple times. However, the SysOps administrator always receives a timeout error.

Which action will allow the SysOps administrator to remotely connect to the instance?

**A.** Add a route table entry in the public subnet for the SysOps administrator's IP address.

**B.** Add an outbound network ACL rule to allow TCP port 22 for the SysOps administrator's IP address.

**C.** Modify the instance security group to allow inbound SSH traffic from the SysOps administrator's IP address.

**D.** Modify the instance security group to allow outbound SSH traffic to the SysOps administrator's IP address.

**ANSWER: C**

## QUESTION NO: 11

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. Create an Amazon CloudFront distribution in each AWS Region, and set the S3 bucket as the origin. 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.

**B.** Create an Amazon S3 bucket, and upload the website content to the S3 bucket. Create an Amazon CloudFront distribution, and set the S3 bucket as the origin. Use Amazon Route 53 to create an alias record that points to the CloudFront distribution.

**C.** Create an Application Load Balancer (ALB) and a target group. Create an Amazon EC2 Auto Scaling group with at least two EC2 instances in the associated target group. Store the website content on the EC2 instances. Use Amazon Route 53 to create an alias record that points to the ALB.

**D.** Create an Application Load Balancer (ALB) and a target group in two Regions. Create an Amazon EC2 Auto Scaling group in each Region with at least two EC2 instances in each target group. Store the website content on the EC2 instances. 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: B**

## QUESTION NO: 12 - (SIMULATION)

You need to update an existing AWS CloudFormation stack. If needed, a copy to 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:

See the Explanation for solution.

**Explanation:**

Here are the steps to update an existing AWS CloudFormation stack:

Note:

**ANSWER:**

**Explanation:**

Here are the steps to update an existing AWS CloudFormation stack:

Note:

## QUESTION NO: 13

A SysOps administrator is configuring an application on Amazon EC2 instances for a company Teams in other countries will use the application over the internet. The company requires the application endpoint to have a static pubic IP address.

How should the SysOps administrator deploy the application to meet this requirement?

**A.** Behind an Amazon API Gateway API

**B.** Behind an Application Load Balancer

**C.** Behind an internet-facing Network Load Balancer

**D.** In an Amazon CloudFront distribution

**ANSWER: C**

## QUESTION NO: 14

A new application runs on Amazon EC2 instances and accesses data in an Amazon RDS database instance. When fully deployed in production, the application fails. The database can be queried from a console on a bastion host. When looking at the web server logs, the following error is repeated multiple times:

"** Error Establishing a Database Connection

Which of the following may be causes of the connectivity problems? {Select TWO.)

**A.** The security group for the database does not have the appropriate egress rule from the database to the web server.

**B.** The certificate used by the web server is not trusted by the RDS instance.

**C.** The security group for the database does not have the appropriate ingress rule from the web server to the database.

**D.** The port used by the application developer does not match the port specified in the RDS configuration.

**E.** The database is still being created and is not available for connectivity.

**ANSWER: C D**

## QUESTION NO: 15

A company website contains a web tier and a database tier on AWS. The web tier consists of Amazon EC2 instances that run in an Auto Scaling group across two Availability Zones. The database tier runs on an Amazon ROS for MySQL Multi-AZ DB instance. The database subnet network ACLs are restricted to only the web subnets that need access to the database. The web subnets use the default network ACL with the default rules.

The company's operations team has added a third subnet to the Auto Scaling group configuration. After an Auto Scaling event occurs, some users report that they intermittently receive an error message. The error message states that the server cannot connect to the database. The operations team has confirmed that the route tables are correct and that the required ports are open on all security groups.

Which combination of actions should a SysOps administrator take so that the web servers can communicate with the DB instance? (Select TWO.)

**A.** On the default ACL. create inbound Allow rules of type TCP with the ephemeral port range and the source as the database subnets.

**B.** On the default ACL, create outbound Allow rules of type MySQL/Aurora (3306). Specify the destinations as the database subnets.

**C.** On the network ACLs for the database subnets, create an inbound Allow rule of type MySQL/Aurora (3306). Specify the source as the third web subnet.

**D.** On the network ACLs for the database subnets, create an outbound Allow rule of type TCP with the ephemeral port range and the destination as the third web subnet.

**E.** On the network ACLs for the database subnets, create an outbound Allow rule of type MySQL/Aurora (3306). Specify the destination as the third web subnet.

**ANSWER: C D**