Free Questions for DOP-C01 by dumpssheet

Shared by Sanford on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A DevOps engineer has been tasked with ensuring that all Amazon S3 buckets, except for those with the word "public" in the name, allow access only to authorized users utilizing S3 bucket policies. The security team wants to be notified when a bucket is created without the proper policy and for the policy to be automatically updated.

Which solutions will meet these requirements?

Options:

A- Create a custom AWS Config rule that will trigger an AWS Lambda function when an S3 bucket is created or updated. Use the Lambda function to look for S3 buckets that should be private, but that do not have a bucket policy that enforces privacy. When such a bucket is found, invoke a remediation action and use Amazon SNS to notify the security team.

B- Create an Amazon EventBridge (Amazon CloudWatch Events) rule that triggers when an S3 bucket is created. Use an AWS Lambda function to determine whether the bucket should be private. If the bucket should be private, update the PublicAccessBlock configuration. Configure a second EventBridge (CloudWatch Events) rule to notify the security team using Amazon SNS when PutBucketPolicy is called.

C- Create an Amazon S3 event notification that triggers when an S3 bucket is created that does not have the word 'public' in the name. Define an AWS Lambda function as a target for this notification and use the function to apply a new default policy to the S3 bucket. Create an additional notification with the same filter and use Amazon SNS to send an email to the security team.

D- Create an Amazon EventBridge (Amazon CloudWatch Events) rule that triggers when a new object is created in a bucket that does not have the word 'public' in the name. Target and use an AWS Lambda function to update the PublicAccessBlock configuration. Create an additional notification with the same filter and use Amazon SNS to send an email to the security team.

Answer:

A

Question 2

Question Type: **MultipleChoice**

A company is migrating its public-facing software to AWS. The company plans to use Amazon EC2 to run application code and Amazon RDS to store all application dat

a. The company wants to primarily use one Region with failover capabilities to a secondary Region and Amazon Route 53 to route traffic. The RPO is 2 hours and the RTO is 4 hours.

Which combination of steps should be used to meet these requirements while MINIMIZING cost? {Select THREE.)

Options:

A- Create an AWS CloudFormation template to provision the application server and database instance in a single Region.

B- Create an AWS CloudFormation template to provision the application tier of the application and a multi-Region database instance.

C- Configure Amazon CloudWatch Events rules to run every hour. Trigger AWS Lambda functions to create an RDS snapshot and copy it to the secondary Region.

D- Configure Amazon CloudWatch Events rules to run every 3 hours. Trigger AWS Lambda functions to create an RDS snapshot and copy it to the secondary Region.

E- In the event of a failure, deploy a new AWS CloudFormation stack in a secondary region to provision the application resources and a new RDS instance using the copied snapshot and a Route 53 failover routing policy.

F- In the event of a failure, deploy a new AWS CloudFormation stack in a secondary region to provision the application resources and a replica of the RDS database using the copied snapshot and a Route 53 latency-based routing policy.

Answer:

C, D, E

Question 3

Question Type: **MultipleChoice**

A company is deploying a container-based application using AWS CodeBuild. The security team mandates that all containers are scanned for vulnerabilities prior to deployment using a password-protected endpoint. All sensitive information must be stored securely.

Which solution should be used to meet these requirements?

Options:

A- Encrypt the password using AWS KMS. Store the encrypted password in the buildspec.yml file as an environment variable under the variables mapping. Reference the environment variable to initiate scanning.

B- Import the password into an AWS CloudHSM key. Reference the CloudHSM key in the buildpec.yml file as an environment variable under the variables mapping. Reference the environment variable to initiate scanning.

C- Store the password in the AWS Systems Manager Parameter Store as a secure string. Add the Parameter Store key to the buildspec.yml file as an environment variable under the parameter-store mapping. Reference the environment variable to initiate scanning.

D- Use the AWS Encryption SDK to encrypt the password and embed in the buildspec.yml file as a variable under the secrets mapping. Attach a policy to CodeBuild to enable access to the required decryption key.

Answer:

C

Question 4

Question Type: **MultipleChoice**

A company is running an application on Amazon EC2 instances in an Auto Scaling group. Recently, an issue occurred that prevented EC2 instances from launching successfully, and it took several hours for the support team to discover the issue. The support team wants to be notified by email whenever an EC2 instance does not start successfully.

Which action will accomplish this?

Options:

A- Add a health check to the Auto Scaling group to invoke an AWS Lambda function whenever an instance status is impaired.

B- Configure the Auto Scaling group to send a notification to an Amazon SNS topic whenever a failed instance launch occurs.

C- Create an Amazon CloudWatch alarm that invokes an AWS Lambda function when a failed AttachInstances Auto Scaling API call is made.

D- Create a status check alarm on Amazon EC2 to send a notification to an Amazon SNS topic whenever a status check fail occurs.

Answer:

B

Question 5

Question Type: **MultipleChoice**

A development team is using AWS CodeCommit to version control application code and AWS CodePipeline to orchestrate software deployments. The team has decided to use a remote master branch as the trigger (or the pipeline to integrate code changes. A developer has pushed code changes to the CodeCommit repository, but noticed that the pipeline had no reaction, even after 10 minutes.

Which of the following actions should be taken to troubleshoot this issue?

Options:

A- Check that an Amazon CloudWatch Events rule has been created for the master branch to trigger the pipeline.

B- Check that the CodePipeline service role has permission to access the CodeCommit repository.

C- Check that the developer's IAM role has permission to push to the CodeCommit repository.

D- Check to see if the pipeline failed to start because of CodeCommit errors in Amazon CloudWatch Logs.

Answer:

C

Question 6

Question Type: **MultipleChoice**

A DevOps engineer used an AWS CloudFormation custom resource to set up AD Connector. The AWS Lambda function executed and created AD Connector, but CloudFormation is not transitioning from CREATE_IN_PROGRESS to CREATE.COMPLETE.

Which action should the engineer take to resolve this issue?

Options:

A- Ensure the Lambda function code has exiled successfully.

B- Ensure the Lambda function code returns a response to the pre-signed URL.

C- Ensure the Lambda function IAM role has cloudformation:UpdateStack permissions for the stack ARN.

D- Ensure the Lambda function IAM role has ds:ConnectDirectory permissions for the AWS account.

Answer:

A

Question 7

Question Type: MultipleChoice

A company wants to ensure that their EC2 instances are secure. They want to be notified if any new vulnerabilities are discovered on their instances, and they also want an audit trail of all login activities on the instances.

Which solution will meet these requirements?

Options:

A- Use AWS Systems Manager to detect vulnerabilities on the EC2 instances. Install the Amazon Kinesis Agent to capture system logs and deliver them to Amazon S3.

B- Use AWS Systems Manager to detect vulnerabilities on the EC2 instances. Install the Systems Manager Agent to capture system logs and view login activity in the CloudTrail console.

C- Configure Amazon CloudWatch to detect vulnerabilities on the EC2 instances. Install the AWS Config daemon to capture system logs and view them in the AWS Config console.

D- Configure Amazon Inspector to detect vulnerabilities on the EC2 instances. Install the Amazon CloudWatch Agent to capture system logs and record them via Amazon CloudWatch Logs.

Answer:

D

Question 8

Question Type: **MultipleChoice**

A DevOps engineer is creating a CI/CD pipeline for an Amazon ECS service. The ECS container instances run behind an Application Load Balancer as the web tier of a three-tier application. An acceptance criterion (or a successful deployment is the verification that the web tier can communicate with the database and middleware tiers of the application upon deployment.

How can this be accomplished in an automated fashion?

Options:

A- Create a health check endpoint in the web application that tests connectivity to the data and middleware tiers. Use this endpoint as the health check URL for the load balancer.

B- Create an approval step for the quality assurance team to validate connectivity. Reject changes in the pipeline if there is an issue with connecting to the dependent tiers.

C- Use an Amazon RDS active connection count and an Amazon CloudWatch ELB metric to alarm on a significant change to the number of open connections.

D- Use Amazon Route 53 health checks to detect issues with the web service and roll back the CI/CD pipeline if there is an error.

Answer:

A

Question 9

Question Type: MultipleChoice

A company uses Amazon S3 to store proprietary information. The development team creates buckets for new projects on a daily basis. The security team wants to ensure that all existing and future buckets have encryption, logging, and versioning enabled. Additionally, no buckets should ever be publicly read or write accessible.

What should a DevOps engineer do to meet these requirements?

Options:

A- Enable AWS CloudTrail and configure automatic remediation using AWS Lambda.

B- Enable AWS Config rules and configure automatic remediation using AWS Systems Manager documents.

C- Enable AWS Trusted Advisor and configure automatic remediation using Amazon CloudWatch Events.

D- Enable AWS Systems Manager and configure automatic remediation using Systems Manager documents.

Answer:

B

Question 10

Question Type: **MultipleChoice**

A company has 100 GB of log data in an Amazon S3 bucket stored in .csv format. SQL developers want to query this data and generate graphs to visualize it. They also need an efficient, automated way to store metadata from the .csv file.

Which combination of steps should be taken to meet these requirements with the LEAST amount of effort? (Select THREE.)

Options:

A- Filter the data through AWS X-Ray to visualize the data.

B- Filter the data through Amazon QuickSight to visualize the data.

C- Query the data with Amazon Athena.

D- Query the data with Amazon Redshift.

E- Use AWS Glue as the persistent metadata store.

F- Use Amazon S3 as the persistent metadata store.

Answer:

B, C, E

Question 11

Question Type: **MultipleChoice**

A DevOps engineer is assisting with a multi-Region disaster recovery solution for a new application. The application consists of Amazon EC2 instances running in an Auto Scaling group and an Amazon Aurora MySQL DB cluster. The application must be available with an RTO of 120 minutes and an RPO of 60 minutes.

What is the MOST cost-effective way to meet these requirements?

Options:

A- Launch an Aurora DB cluster as an Aurora Replica in a different Region. Create an AWS CloudFormation template for all compute resources and create a stack in two Regions. Write a script that promotes the Aurora Replica to the primary instance in the event of a failure.

B- Launch an Aurora DB cluster as an Aurora Replica in a different Region and configure automatic cross-Region failover. Create an AWS CloudFormation template that includes an Auto Scaling group, and create a stack in two Regions. Write a script that updates the CloudFormation stack in the disaster recovery Region to increase the number of instances.

C- Use AWS Lambda to create and copy a snapshot of the Aurora DB cluster to the destination Region hourly. Create an AWS CloudFormation template that includes an Auto Scaling group, and create a stack in two Regions. Restore the Aurora DB cluster from a snapshot and update the Auto Scaling group to start launching instances.

D- Configure Amazon DynamoDB cross-Region replication. Create an AWS CloudFormation template that includes an Auto Scaling group, and create a stack in two Regions. Write a script that will update the CloudFormation stack in the disaster recovery Region and promote the DynamoDB replica to the primary instance in the event of a failure.

Answer:

D

20%
DISCOUNT