SAP-C02 Q&As

AWS Certified Solutions Architect - Professional

Pass Amazon SAP-C02 Exam with 100% Guarantee

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

https://www.passapply.com/sap-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 is rearchitecting its applications to run on AWS. The company\\'s infrastructure includes multiple Amazon EC2 instances. The company\\'s development team needs different levels of access. The company wants to implement a policy that requires all Windows EC2 instances to be joined to an Active Directory domain on AWS. The company also wants to Implement enhanced security processes such as multi-factor authentication (MFA). The company wants to use managed AWS services wherever possible.

Which solution will meet these requirements?

A. Create an AWS Directory Service for Microsoft Active Directory implementation. Launch an Amazon Workspace. Connect to and use the Workspace for domain security configuration tasks.

B. Create an AWS Directory Service for Microsoft Active Directory implementation. Launch an EC2 instance. Connect to and use the EC2 instance for domain security configuration tasks.

C. Create an AWS Directory Service Simple AD implementation. Launch an EC2 instance. Connect to and use the EC2 instance for domain security configuration tasks.

D. Create an AWS Directory Service Simple AD implementation. Launch an Amazon Workspace. Connect to and use the Workspace for domain security configuration tasks.

Correct Answer: A

A is the correct answer because it uses AWS Directory Service for Microsoft Active Directory to join the Windows EC2 instances to an Active Directory domain on AWS and enable MFA. AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, is a fully managed service that is powered by Windows Server 2019. It allows you to run directory-aware workloads in the AWS Cloud, including Microsoft SharePoint and custom .NET and SQL Server-based applications. You can also configure a trust relationship between AWS Managed Microsoft AD in the AWS Cloud and your existing on-premises Microsoft Active Directory. AWS Managed Microsoft AD supports MFA by integrating with your existing RADIUS-based MFA infrastructure. To join the Windows EC2 instances to an Active Directory domain on AWS, you can use an Amazon Workspace, which is a fully managed, secure desktop computing service that runs on AWS. You can connect to and use the Workspace for domain security configuration tasks.

References: https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_microsoft_ad.html
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_join_instance.html
https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces.html

QUESTION 2

A company runs applications on Amazon EC2 instances. The company plans to begin using an Auto Scaling group for the instances. As part of this transition, a solutions architect must ensure that Amazon CloudWatch Logs automatically collects logs from all new instances The new Auto Scaling group will use a launch template that includes the Amazon Linux 2 AMI and no key pair.

Which solution meets these requirements?

A. Create an Amazon CloudWatch agent configuration for the workload Store the CloudWatch agent configuration in an Amazon S3 bucket Write an EC2 user data script to fetch the configuration He from Amazon S3. Configure the cloudWatch agent on the instance during Initial boot.

B. Create an Amazon CloudWatch agent configuration for the workload In AWS Systems Manager Parameter Store

Create a Systems Manager document that Installs and configures the CloudWatch agent by using the configuration Create an Amazon EventBridge (Amazon CloudWatch Events) rule on the default event bus with a Systems Manager Run Command target that runs the document whenever an instance enters the running state.

C. Create an Amazon CloudWatch agent configuration for the workload Create an AWS Lambda function to Install and configure CloudWatch agent by using AWS Systems Manager Session Manager. Include the agent configuration inside the Lambda package Create an AWS Config custom rule to identify changes to the EC2 instances and invoke the Lambda function

D. Create an Amazon CloudWatch agent configuration for the workload. Save the CloudWatch agent configuration as pan of an AWS Lambda deployment package. Use AWS CloudTrail to capture EC2 tagging events and initiate agent installation. Use AWS CodeBuild to configure the CloudWatch agent on the instances that run the workload.

Correct Answer: B

QUESTION 3

A company runs a Python script on an Amazon EC2 instance to process data. The script runs every 10 minutes. The script ingests files from an Amazon S3 bucket and processes the files. On average, the script takes approximately 5 minutes to process each file The script will not reprocess a file that the script has already processed.

The company reviewed Amazon CloudWatch metrics and noticed that the EC2 instance is idle for approximately 40% of the time because of the file processing speed. The company wants to make the workload highly available and scalable. The company also wants to reduce long-term management overhead.

Which solution will meet these requirements MOST cost-effectively?

A. Migrate the data processing script to an AWS Lambda function. Use an S3 event notification to invoke the Lambda function to process the objects when the company uploads the objects.

B. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure Amazon S3 to send event notifications to the SQS queue. Create an EC2 Auto Scaling group with a minimum size of one instance. Update the data processing script to poll the SQS queue. Process the S3 objects that the SQS message identifies.

C. Migrate the data processing script to a container image. Run the data processing container on an EC2 instance. Configure the container to poll the S3 bucket for new objects and to process the resulting objects.

D. Migrate the data processing script to a container image that runs on Amazon Elastic Container Service (Amazon ECS) on AWS Fargate. Create an AWS Lambda function that calls the Fargate RunTaskAPI operation when the container processes the file. Use an S3 event notification to invoke the Lambda function.

Correct Answer: A

The correct answer is A, migrating the data processing script to an AWS Lambda function and using an S3 event notification to invoke the Lambda function to process the objects when the company uploads the objects. This solution meets

the company\\'s requirements of high availability and scalability, as well as reducing long-term management overhead, and is likely to be the most cost-effective option.

Option B involves creating an SQS queue and configuring S3 to send event notifications to it. The data processing script would then poll the SQS queue and process the S3 objects that the SQS message identifies. While this option also

provides high availability and scalability, it is less cost-effective than using Lambda, as it requires additional resources such as an SQS queue and an EC2 Auto Scaling group.

QUESTION 4

A company is expanding. The company plans to separate its resources into hundreds of different AWS accounts in multiple AWS Regions. A solutions architect must recommend a solution that denies access to any operations outside of specifically designated Regions.

Which solution will meet these requirements?

A. Create IAM roles for each account. Create IAM policies with conditional allow permissions that include only approved Regions for the accounts.

B. Create an organization in AWS Organizations. Create IAM users for each account. Attach a policy to each user to block access to Regions where an account cannot deploy infrastructure.

C. Launch an AWS Control Tower landing zone. Create OUs and attach SCPs that deny access to run services outside of the approved Regions.

D. Enable AWS Security Hub in each account. Create controls to specify the Regions where an account can deploy infrastructure.

Correct Answer: C

QUESTION 5

A company is deploying AWS Lambda functions that access an Amazon RDS for PostgreSQL database. The company needs to launch the Lambda functions in a QA environment and in a production environment.

The company must not expose credentials within application code and must rotate passwords automatically. Which solution will meet these requirements?

A. Store the database credentials for both environments in AWS Systems Manager Parameter Store. Encrypt the credentials by using an AWS Key Management Service (AWS KMS) key. Within the application code of the Lambda functions, pull the credentials from the Parameter Store parameter by using the AWS SDK for Python (Bot03). Add a role to the Lambda functions to provide access to the Parameter Store parameter.

B. Store the database credentials for both environments in AWS Secrets Manager with distinct key entry for the QA environment and the production environment. Turn on rotation. Provide a reference to the Secrets Manager key as an environment variable for the Lambda functions.

C. Store the database credentials for both environments in AWS Key Management Service (AWS KMS). Turn on rotation. Provide a reference to the credentials that are stored in AWS KMS as an environment variable for the Lambda functions.

D. Create separate S3 buckets for the QA environment and the production environment. Turn on server-side encryption with AWS KMS keys (SSE-KMS) for the S3 buckets. Use an object naming pattern that gives each Lambda function\\'s application code the ability to pull the correct credentials for the function\\'s corresponding environment. Grant each Lambda function\\'s execution role access to Amazon S3.

Correct Answer: B

The best solution is to store the database credentials for both environments in AWS Secrets Manager with distinct key entry for the QA environment and the production environment. AWS Secrets Manager is a web service that can securely store, manage, and retrieve secrets, such as database credentials. AWS Secrets Manager also supports automatic

rotation of secrets by using Lambda functions or built-in rotation templates. By storing the database credentials for both environments in AWS Secrets Manager, the company can avoid exposing credentials within application code and rotate passwords automatically. By providing a reference to the Secrets Manager key as an environment variable for the Lambda functions, the company can easily access the credentials from the code by using the AWS SDK. This solution meets all the requirements of the company. References: AWS Secrets Manager Documentation, Using AWS Lambda with AWS Secrets Manager, Using environment variables - AWS Lambda