

# SAP-C01<sup>Q&As</sup>

AWS Certified Solutions Architect - Professional (SAP-C01)

## Pass Amazon SAP-C01 Exam with 100% Guarantee

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

<https://www.pass2lead.com/aws-solution-architect-professional.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 media company is serving video files stored in Amazon S3 using Amazon CloudFront. The development team needs access to the logs to diagnose faults and perform service monitoring. The log files from CloudFront may contain sensitive information about users.

The company uses a log processing service to remove sensitive information before making the logs available to the development team. The company has the following requirements for the unprocessed logs:

1.

The logs must be encrypted at rest and must be accessible by the log processing service only.

2.

Only the data protection team can control access to the unprocessed log files.

3.

AWS CloudFormation templates must be stored in AWS CodeCommit.

4.

AWS CodePipeline must be triggered on commit to perform updates made to CloudFormation templates.

5.

CloudFront is already writing the unprocessed logs to an Amazon S3 bucket, and the log processing service is operating against this S3 bucket.

Which combination of steps should a solutions architect take to meet the company's requirements? (Choose two.)

A. Create an AWS KMS key that allows the AWS Logs Delivery account to generate data keys for encryption. Configure S3 default encryption to use server-side encryption with KMS managed keys (SSE-KMS) on the log storage bucket using the new KMS key. Modify the KMS key policy to allow the log processing service to perform decrypt operations.

B. Create an AWS KMS key that follows the CloudFront service role to generate data keys for encryption. Configure S3 default encryption to use KMS managed keys (SSE-KMS) on the log storage bucket using the new KMS key. Modify the KMS key policy to allow the log processing service to perform decrypt operations.

C. Configure S3 default encryption to use AWS KMS managed keys (SSE-KMS) on the log storage bucket using the AWS Managed S3 KMS key. Modify the KMS key policy to allow the CloudFront service role to generate data keys for encryption. Modify the KMS key policy to allow the log processing service to perform decrypt operations.

D. Create a new CodeCommit repository for the AWS KMS key template. Create an IAM policy to allow commits to the new repository and attach it to the data protection team's users. Create a new CodePipeline pipeline with a custom IAM role to perform KMS key updates using CloudFormation. Modify the KMS key policy to allow the CodePipeline IAM role to modify the key policy.

E. Use the existing CodeCommit repository for the AWS KMS key template. Create an IAM policy to allow commits to the new repository and attach it to the data protection team's users. Modify the existing CodePipeline pipeline to use a custom IAM role and to perform KMS key updates using CloudFormation. Modify the KMS key policy to allow the CodePipeline IAM role to modify the key policy.

Correct Answer: AD

## QUESTION 2

A company provides AWS solutions to its users with AWS CloudFormation templates. Users launch the templates in their accounts to have different solutions provisioned for them. The users want to improve the deployment strategy for solutions while retaining the ability to do the following:

1.

Add their own features to a solution for their specific deployments.

2.

Run unit tests on their changes.

3.

Turn features on and off for their deployments.

4.

Automatically update with code changes.

5.

Run security scanning tools for their deployments.

Which strategies should the Solutions Architect use to meet the requirements?

A. Allow users to download solution code as Docker images. Use AWS CodeBuild and AWS CodePipeline for the CI/CD pipeline. Use Docker images for different solution features and the AWS CLI to turn features on and off. Use AWS CodeDeploy to run unit tests and security scans, and for deploying and updating a solution with changes.

B. Allow users to download solution code artifacts. Use AWS CodeCommit and AWS CodePipeline for the CI/CD pipeline. Use AWS Amplify plugins for different solution features and user prompts to turn features on and off. Use AWS Lambda to run unit tests and security scans, and AWS CodeBuild for deploying and updating a solution with changes.

C. Allow users to download solution code artifacts in their Amazon S3 buckets. Use Amazon S3 and AWS CodePipeline for the CI/CD pipelines. Use CloudFormation StackSets for different solution features and to turn features on and off. Use AWS Lambda to run unit tests and security scans, and CloudFormation for deploying and updating a solution with changes.

D. Allow users to download solution code artifacts. Use AWS CodeCommit and AWS CodePipeline for the CI/CD pipeline. Use the AWS Cloud Development Kit constructs for different solution features, and use the manifest file to turn features on and off. Use AWS CodeBuild to run unit tests and security scans, and for deploying and updating a solution with changes.

Correct Answer: A

Reference: <https://www.slideshare.net/AmazonWebServices/cicd-for-containers-a-way-forward-for-yourdevops-pipeline>

## QUESTION 3

A company's solution architect is designing a disaster recovery (DR) solution for an application that runs on AWS.

The application uses PostgreSQL 11.7 as its database. The company has an RPO of 30 seconds. The solutions architect must design a DR solution with the primary database in the us-east-1 Region and the database in the us-west-2 Region.

What should the solution architect do to meet these requirements with minimum application change?

- A. Migrate the database to Amazon RDS for PostgreSQL in us-east-1. Set up a read replica in us-west-2. Set the managed RPO for the RDS database to 30 seconds.
- B. Migrate the database to Amazon for PostgreSQL in us-east-1. Set up a standby replica in an Availability Zone in us-west-2, Set the managed RPO for the RDS database to 30 seconds.
- C. Migrate the database to an Amazon Aurora PostgreSQL global database with the primary Region as us-east-1 and the secondary Region as us-west-2. Set the managed RPO for the Aurora database to 30 seconds.
- D. Migrate the database to Amazon DynamoDB in us-east-1. Set up global tables with replica tables that are created in us-west-2.

Correct Answer: A

#### QUESTION 4

A user is planning to launch multiple EC2 instance same as current running instance.

Which of the below mentioned parameters is not copied by Amazon EC2 in the launch wizard when the user has selected the option "Launch more like this"?

- A. Termination protection
- B. Tenancy setting
- C. Storage
- D. Shutdown behavior

Correct Answer: C

The Amazon EC2 console provides a "Launch more like this" wizard option that enables the user to use a current instance as a template for launching other instances. This option automatically populates the Amazon EC2 launch wizard with certain configuration details from the selected instance. The following configuration details are copied from the selected instance into the launch wizard: AMI ID Instance type Availability Zone, or the VPC and subnet in which the selected instance is located Public IPv4 address. If the selected instance currently has a public IPv4 address, the new instance receives a public IPv4 address

- regardless of the selected instance's default public IPv4 address setting. For more information about public IPv4 addresses, see Public IPv4 Addresses and External DNS Hostnames. Placement group, if applicable IAM role associated with the instance, if applicable Shutdown behavior setting (stop or terminate) Termination protection setting (true or false) CloudWatch monitoring (enabled or disabled) Amazon EBS-optimization setting (true or false) Tenancy setting, if launching into a VPC (shared or dedicated) Kernel ID and RAM disk ID, if applicable User data, if specified Tags associated with the instance, if applicable Security groups associated with the instance The following configuration details are not copied from your selected instance; instead, the wizard applies their default settings or behavior: (VPC only) Number of network interfaces: The default is one network interface, which is the primary network interface (eth0). Storage: The default storage configuration is determined by the AMI and the instance type.

Reference: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html>

## QUESTION 5

A company is developing a web application that runs on Amazon EC2 instances in an Auto Scaling group behind a public-facing Application Load Balancer (ALB). Only users from a specific country are allowed to access the application. The company needs the ability to log the access requests that have been blocked. The solution should require the least possible maintenance.

Which solution meets these requirements?

- A. Create an IPSet containing a list of IP ranges that belong to the specified country. Create an AWS WAF web ACL. Configure a rule to block any requests that do not originate from an IP range in the IPSet. Associate the rule with the web ACL. Associate the web ACL with the ALB.
- B. Create an AWS WAF web ACL. Configure a rule to block any requests that do not originate from the specified country. Associate the rule with the web ACL. Associate the web ACL with the ALB.
- C. Configure AWS Shield to block any requests that do not originate from the specified country. Associate AWS Shield with the ALB.
- D. Create a security group rule that allows ports 80 and 443 from IP ranges that belong to the specified country. Associate the security group with the ALB.

Correct Answer: A

[Latest SAP-C01 Dumps](#)

[SAP-C01 Study Guide](#)

[SAP-C01 Braindumps](#)