



SAP-C01^{Q&As}

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.pass4itsure.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 company wants to replace its call center system with a solution built using AWS managed services. The company call center would like the solution to receive calls, create contact flows, and scale to handle growth projections. The call center would also like the solution to use deep learning capabilities to recognize the intent of the callers and handle basic tasks, reducing the need to speak to an agent. The solution should also be able to query business applications and provide relevant information back to callers as requested.

Which services should the Solutions Architect use to build this solution? (Choose three.)

- A. Amazon Rekognition to identify who is calling.
- B. Amazon Connect to create a cloud-based contact center.
- C. Amazon Alexa for Business to build conversational interfaces.
- D. AWS Lambda to integrate with internal systems.
- E. Amazon Lex to recognize the intent of the caller.
- F. Amazon SQS to add incoming callers to a queue.

Correct Answer: BDE

QUESTION 2

A company has a new security policy. The policy requires the company to log any event that retrieves data from Amazon S3 buckets. The company must save these audit logs in a dedicated S3 bucket.

The company created the audit logs S3 bucket in an AWS account that is designated for centralized logging. The S3 bucket has a bucket policy that allows write-only cross-account access.

A solutions architect must ensure that all S3 object-level access is being logged for current S3 buckets and future S3 buckets.

Which solution will meet these requirements?

- A. Enable server access logging for all current S3 buckets. Use the audit logs S3 bucket as a destination for audit logs.
- B. Enable replication between all current S3 buckets and the audit logs S3 bucket. Enable S3 Versioning in the audit logs S3 bucket.
- C. Configure S3 Event Notifications for all current S3 buckets to invoke an AWS Lambda function every time objects are accessed. Store Lambda logs in the audit logs S3 bucket.
- D. Enable AWS CloudTrail, and use the audit logs S3 bucket to store logs. Enable data event logging for S3 event sources, current S3 buckets, and future S3 buckets.

Correct Answer: D

QUESTION 3



A company with global offices has a single 1 Gbps AWS Direct Connect connection to a single AWS Region. The company's on-premises network uses the connection to communicate with the company's resources in the AWS Cloud. The connection has a single private virtual interface that connects to a single VPC.

A solutions architect must implement a solution that adds a redundant Direct Connect connection in the same Region. The solution also must provide connectivity to other Regions through the same pair of Direct Connect connections as the company expands into other Regions.

Which solution meets these requirements?

- A. Provision a Direct Connect gateway. Delete the existing private virtual interface from the existing connection. Create the second Direct Connect connection. Create a new private virtual interface on each connection, and connect both private virtual interfaces to the Direct Connect gateway. Connect the Direct Connect gateway to the single VPC.
- B. Keep the existing private virtual interface. Create the second Direct Connect connection. Create a new private virtual interface on the new connection, and connect the new private virtual interface to the single VPC.
- C. Keep the existing private virtual interface. Create the second Direct Connect connection. Create a new public virtual interface on the new connection and connect the new public virtual interface to the single VPC.
- D. Provision a transit gateway. Delete the existing private virtual interface from the existing connection. Create the second Direct Connect connection. Create a new private virtual interface on each connection, and connect both private virtual interfaces to the transit gateway. Associate the transit gateway with the single VPC.

Correct Answer: A

A Direct Connect gateway is a globally available resource. You can create the Direct Connect gateway in any Region and access it from all other Regions. The following describe scenarios where you can use a Direct Connect gateway.

Reference: <https://docs.aws.amazon.com/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.html>
<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html>

QUESTION 4

A company uses Amazon S3 to host a web application. Currently, the company uses a continuous integration tool running on an Amazon EC2 instance that builds and deploys the application by uploading it to an S3 bucket. A Solutions Architect needs to enhance the security of the company's platform with the following requirements:

1.

A build process should be run in a separate account from the account hosting the web application.

2.

A build process should have minimal access in the account it operates in.

3.

Long-lived credentials should not be used.

As a start, the Development team created two AWS accounts: one for the application named web account process; other is a named build account.



Which solution should the Solutions Architect use to meet the security requirements?

A. In the build account, create a new IAM role, which can be assumed by Amazon EC2 only. Attach the role to the EC2 instance running the continuous integration process. Create an IAM policy to allow s3: PutObject calls on the S3 bucket in the web account. In the web account, create an S3 bucket policy attached to the S3 bucket that allows the build account to use s3:PutObject calls.

B. In the build account, create a new IAM role, which can be assumed by Amazon EC2 only. Attach the role to the EC2 instance running the continuous integration process. Create an IAM policy to allow s3: PutObject calls on the S3 bucket in the web account. In the web account, create an S3 bucket policy

attached to the S3 bucket that allows the newly created IAM role to use s3:PutObject calls.

C. In the build account, create a new IAM user. Store the access key and secret access key in AWS Secrets Manager. Modify the continuous integration process to perform a lookup of the IAM user credentials from Secrets Manager. Create an IAM policy to allow s3: PutObject calls on the S3 bucket in the web account, and attach it to the user. In the web account, create an S3 bucket policy attached to the S3 bucket that allows the newly created IAM user to use s3:PutObject calls.

D. In the build account, modify the continuous integration process to perform a lookup of the IAM user credentials from AWS Secrets Manager. In the web account, create a new IAM user. Store the access key and secret access key in Secrets Manager. Attach the PowerUserAccess IAM policy to the IAM user.

Correct Answer: A

QUESTION 5

In Amazon Cognito, your mobile app authenticates with the Identity Provider (IdP) using the provider's SDK. Once the end user is authenticated with the IdP, the OAuth or OpenID Connect token returned from the IdP is passed by your app to Amazon Cognito, which returns a new _____ for the user and a set of temporary, limited-privilege AWS credentials.

A. Cognito Key Pair

B. Cognito API

C. Cognito ID

D. Cognito SDK

Correct Answer: C

Your mobile app authenticates with the identity provider (IdP) using the provider's SDK. Once the end user is authenticated with the IdP, the OAuth or OpenID Connect token returned from the IdP is passed by your app to Amazon Cognito, which returns a new Cognito ID for the user and a set of temporary, limited-privilege AWS credentials.

Reference: <http://aws.amazon.com/cognito/faqs/>

QUESTION 6

A company that provisions job boards for a seasonal workforce is seeing an increase in traffic and usage. The backend services run on a pair of Amazon EC2 instances behind an Application Load Balancer with Amazon DynamoDB as the datastore. Application read and write traffic is slow during peak seasons.



Which option provides a scalable application architecture to handle peak seasons with the LEAST development effort?

- A. Migrate the backend services to AWS Lambda. Increase the read and write capacity of DynamoDB
- B. Migrate the backend services to AWS Lambda. Configure DynamoDB to use global tables
- C. Use Auto Scaling groups for the backend services. Use DynamoDB auto scaling
- D. Use Auto Scaling groups for the backend services. Use Amazon Simple Queue Service (Amazon SQS) and an AWS Lambda function to write to DynamoDB

Correct Answer: C

QUESTION 7

A company has an application that runs on Amazon EC2 instances in an Amazon EC2 Auto Scaling group. The company uses AWS CodePipeline to deploy the application. The instances that run in the Auto Scaling group are constantly changing because of scaling events.

When the company deploys new application code versions, the company installs the AWS CodeDeploy agent on any new target EC2 instances and associates the instances with the CodeDeploy deployment group. The application is set to go live within the next 24 hours.

What should a solutions architect recommend to automate the application deployment process with the LEAST amount of operational overhead?

- A. Configure Amazon EventBridge (Amazon CloudWatch Events) to invoke an AWS Lambda function when a new EC2 instance is launched into the Auto Scaling group. Code the Lambda function to associate the EC2 instances with the CodeDeploy deployment group.
- B. Write a script to suspend Amazon EC2 Auto Scaling operations before the deployment of new code. When the deployment is complete, create a new AMI and configure the Auto Scaling group's launch template to use the new AMI for new launches. Resume Amazon EC2 Auto Scaling operations.
- C. Create a new AWS CodeBuild project that creates a new AMI that contains the new code. Configure CodeBuild to update the Auto Scaling group's launch template to the new AMI. Run an Amazon EC2 Auto Scaling instance refresh operation.
- D. Create a new AMI that has the CodeDeploy agent installed. Configure the Auto Scaling group's launch template to use the new AMI. Associate the CodeDeploy deployment group with the Auto Scaling group instead of the EC2 instances.

Correct Answer: C

QUESTION 8

A company is using AWS Organizations to manage multiple accounts. Due to regulatory requirements, the company wants to restrict specific member accounts to certain AWS Regions, where they are permitted to deploy resources. The resources in the accounts must be tagged, enforced based on a group standard, and centrally managed with minimal configuration.

What should a solutions architect do to meet these requirements?



- A. Create an AWS Config rule in the specific member accounts to limit Regions and apply a tag policy.
- B. From the AWS Billing and Cost Management console, in the master account, disable Regions for the specific member accounts and apply a tag policy on the root.
- C. Associate the specific member accounts with the root. Apply a tag policy and an SCP using conditions to limit Regions.
- D. Associate the specific member accounts with a new OU. Apply a tag policy and an SCP using conditions to limit Regions.

Correct Answer: D

QUESTION 9

A 3-Ber e-commerce web application is currently deployed on-premises, and will be migrated to AWS for greater scalability and elasticity. The web tier currently shares read-only data using a network distributed file system. The app server tier uses a clustering mechanism for discovery and shared session state that depends on IP multicast. The database tier uses shared-storage clustering to provide database failover capability, and uses several read slaves for scaling. Data on all servers and the distributed file system directory is backed up weekly to off-site tapes.

Which AWS storage and database architecture meets the requirements of the application?

- A. Web servers: store read-only data in S3, and copy from S3 to root volume at boot time. App servers: share state using a combination of DynamoDB and IP unicast. Database: use RDS with multi-AZ deployment and one or more read replicas. Backup: web servers, app servers, and database backed up weekly to Glacier using snapshots.
- B. Web servers: store read-only data in an EC2 NFS server, mount to each web server at boot time. App servers: share state using a combination of DynamoDB and IP multicast. Database: use RDS with multi-AZ deployment and one or more Read Replicas. Backup: web and app servers backed up weekly via AMIs, database backed up via DB snapshots.
- C. Web servers: store read-only data in S3, and copy from S3 to root volume at boot time. App servers: share state using a combination of DynamoDB and IP unicast. Database: use RDS with multi-AZ deployment and one or more Read Replicas. Backup: web and app servers backed up weekly via AMIs, database backed up via DB snapshots.
- D. Web servers: store read-only data in S3, and copy from S3 to root volume at boot time App servers: share state using a combination of DynamoDB and IP unicast. Database: use RDS with multi-AZ deployment. Backup: web and app servers backed up weekly via AMIs, database backed up via DB snapshots.

Correct Answer: A

Amazon Glacier doesn't suit all storage situations. Listed following are a few storage needs for which you should consider other AWS storage options instead of Amazon Glacier. Data that must be updated very frequently might be better served by a storage solution with lower read/write latencies, such as Amazon EBS, Amazon RDS, Amazon DynamoDB, or relational databases running on EC2. Reference:

<https://d0.awsstatic.com/whitepapers/Storage/AWS%20Storage%20Services%20Whitepaper-v9.pdf>

QUESTION 10

How can a user list the IAM Role configured as a part of the launch config?

- A. `as-describe-launch-configs -iam-profile`



B. `as-describe-launch-configs -show-long`

C. `as-describe-launch-configs -iam-role`

D. `as-describe-launch-configs -role`

Correct Answer: B

`As-describe-launch-configs` describes all the launch config parameters created by the AWS account in the specified region. Generally, it returns values, such as Launch Config name, Instance Type and AMI ID. If the user wants additional parameters, such as the IAM Profile used in the config, he has to run command: `as-describe-launch-configs --show-long`

QUESTION 11

A Solutions Architect is building a containerized .NET Core application that will run in AWS Fargate. The backend of the application requires Microsoft SQL Server with high availability. All tiers of the application must be highly available. The credentials used for the connection string to SQL Server should not be stored on disk within the .NET Core front-end containers.

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

A. Set up SQL Server to run in Fargate with Service Auto Scaling. Create an Amazon ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to SQL Server running in Fargate. Specify the ARN of the secret in AWS Secrets Manager in the secrets section of the Fargate task definition so the sensitive data can be injected into the containers as environment variables on startup for reading into the application to construct the connection string. Set up the .NET Core service using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones.

B. Create a Multi-AZ deployment of SQL Server on Amazon RDS. Create a secret in AWS Secrets Manager for the credentials to the RDS database. Create an Amazon ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to the RDS database in Secrets Manager. Specify the ARN of the secret in Secrets Manager in the secrets section of the Fargate task definition so the sensitive data can be injected into the containers as environment variables on startup for reading into the application to construct the connection string. Set up the .NET Core service in Fargate using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones.

C. Create an Auto Scaling group to run SQL Server on Amazon EC2. Create a secret in AWS Secrets Manager for the credentials to SQL Server running on EC2. Create an Amazon ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to SQL Server on EC2. Specify the ARN of the secret in Secrets Manager in the secrets section of the Fargate task definition so the sensitive data can be injected into the containers as environment variables on startup for reading into the application to construct the connection string. Set up the .NET Core service using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones.

D. Create a Multi-AZ deployment of SQL Server on Amazon RDS. Create a secret in AWS Secrets Manager for the credentials to the RDS database. Create non-persistent empty storage for the .NET Core containers in the Fargate task definition to store the sensitive information. Create an Amazon ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to the RDS database in Secrets Manager. Specify the ARN of the secret in Secrets Manager in the secrets section of the Fargate task definition so the sensitive data can be written to the non-persistent empty storage on startup for reading into the application to construct the connection string. Set up the .NET Core service using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones.

Correct Answer: B

Secrets Manager natively supports SQL Server on RDS. No real need to create additional '\ephemeral storage\' to



fetch credentials, as these can be injected to containers as environment variables.

<https://aws.amazon.com/premiumsupport/knowledge-center/ecs-data-security-container-task/>

QUESTION 12

ABC has three separate departments and each department has their own AWS accounts. The HR department has created a file sharing site where all the on roll employees' data is uploaded. The Admin department uploads data about the employee presence in the office to their DB hosted in the VPC. The Finance department needs to access data from the HR department to know the on roll employees to calculate the salary based on the number of days that an employee is present in the office. How can ABC setup this scenario?

- A. It is not possible to configure VPC peering since each department has a separate AWS account.
- B. Setup VPC peering for the VPCs of Admin and Finance.
- C. Setup VPC peering for the VPCs of Finance and HR as well as between the VPCs of Finance and Admin.
- D. Setup VPC peering for the VPCs of Admin and HR

Correct Answer: C

A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. It enables the user to launch AWS resources into a virtual network that the user has defined. A VPC peering connection allows the user to route traffic between the peer VPCs using private IP addresses as if they are a part of the same network. This is helpful when one VPC from the same or different AWS account wants to connect with resources of the other VPC.

Reference: <http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/peering-configurations-fullaccess.html#three-vpcs-full-access>.

QUESTION 13

Which EC2 functionality allows the user to place the Cluster Compute instances in clusters?

- A. Cluster group
- B. Cluster security group
- C. GPU units
- D. Cluster placement group

Correct Answer: D

The Amazon EC2 cluster placement group functionality allows users to group cluster compute instances in clusters.

Reference: <https://aws.amazon.com/ec2/faqs/>

QUESTION 14

A user has configured two security groups which allow traffic as given below: 1: SecGrp1:



Inbound on port 80 for 0.0.0.0/0 Inbound on port 22 for 0.0.0.0/0 2: SecGrp2:

Inbound on port 22 for 10.10.10.1/32

If both the security groups are associated with the same instance, which of the below mentioned statements is true?

- A. It is not possible to have more than one security group assigned to a single instance
- B. It is not possible to create the security group with conflicting rules. AWS will reject the request
- C. It allows inbound traffic for everyone on both ports 22 and 80
- D. It allows inbound traffic on port 22 for IP 10.10.10.1 and for everyone else on port 80

Correct Answer: C

A user can attach more than one security group to a single EC2 instance. In this case, the rules from each security group are effectively aggregated to create one set of rules. AWS uses this set of rules to determine whether to allow access or not. Thus, here the rule for port 22 with IP 10.10.10.1/32 will merge with IP 0.0.0.0/0 and open ports 22 and 80 for all.

Reference: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html>

QUESTION 15

A company wants to migrate its on-premises data center to the AWS Cloud. This includes thousands of virtualized Linux and Microsoft Windows servers, SAN storage, Java and PHP applications with MYSQL, and Oracle databases. There are many department services hosted either in the same data center or externally. The technical documentation is incomplete and outdated. A solutions architect needs to understand the current environment and estimate the cloud resource costs after the migration.

Which tools or services should solutions architect use to plan the cloud migration (Choose three.)

- A. AWS Application Discovery Service
- B. AWS SMS
- C. AWS x-Ray
- D. AWS Cloud Adoption Readiness Tool (CART)
- E. Amazon Inspector
- F. AWS Migration Hub

Correct Answer: ADF

[Latest SAP-C01 Dumps](#)

[SAP-C01 Practice Test](#)

[SAP-C01 Exam Questions](#)