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.certbus.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

Regarding Identity and Access Management (IAM), Which type of special account belonging to your application allows your code to access Google services programmatically?

A. Service account

B. Simple Key

C. OAuth

D. Code account

Correct Answer: A

A service account is a special Google account that can be used by applications to access Google services programmatically. This account belongs to your application or a virtual machine (VM), instead of to an individual end user. Your application uses the service account to call the Google API of a service, so that the users aren\\'t directly involved. A service account can have zero or more pairs of service account keys, which are used to authenticate to Google. A service account key is a public/private key pair generated by Google. Google retains the public key, while the user is given the private key.

Reference: https://cloud.google.com/iam/docs/service-accounts

QUESTION 2

An organization is planning to use NoSQL DB for its scalable data needs. The organization wants to host

an application securely in AWS VPC.

What action can be recommended to the organization?

A. The organization should setup their own NoSQL cluster on the AWS instance and configure route tables and subnets.

B. The organization should only use a DynamoDB because by default it is always a part of the default subnet provided by AWS.

C. The organization should use a DynamoDB while creating a table within the public subnet.

D. The organization should use a DynamoDB while creating a table within a private subnet.

Correct Answer: A

The Amazon Virtual Private Cloud (Amazon VPC) allows the user to define a virtual networking environment in a private, isolated section of the Amazon Web Services (AWS) cloud. The user has complete control over the virtual networking environment. Currently VPC does not support DynamoDB. Thus, if the user wants to implement VPC, he has to setup his own NoSQL DB within the VPC.

Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Introduction.html

QUESTION 3

A solutions architect is migrating an existing workload to AWS Fargate. The task can only run in a private subnet within the VPC where there is no direct connectivity from outside the system to the application. When the Fargate task is launched, the task fails with the following error:

CannotPullContainerError: API error (500): Get https://111122223333.dkr.ecr.us-east-1.amazonaws.com/ v2/: net/http: request canceled while waiting for connection

How should the solutions architect correct this error?

A. Ensure the task is set to ENABLED for the auto-assign public IP setting when launching the task.

B. Ensure the task is set to DISABLED for the auto-assign public IP setting when launching the task. Configure a NAT gateway in the public subnet in the VPC to route requests to the internet.

C. Ensure the task is set to DISABLED for the auto-assign public IP setting when launching the task. Configure a NAT gateway in the private subnet in the VPC to route requests to the internet.

D. Ensure the network mode is set to bridge in the Fargate task definition.

Correct Answer: B

QUESTION 4

A company is running a large containerized workload in the AWS Cloud. The workload consists of approximately 100 different services. The company uses Amazon Elastic Container Service (Amazon ECS) to orchestrate the workload.

Recently, the company\\'s development team started using AWS Fargate instead of Amazon EC2 instances in the ECS cluster. In the past, the workload has come close to running the maximum number of EC2 instances that are available in the account.

The company is worried that the workload could reach the maximum number of ECS tasks that are allowed. A solutions architect must implement a solution that will notify the development team when Fargate reaches 80% of the maximum number of tasks.

What should the solutions architect do to meet this requirement?

A. Use Amazon CloudWatch to monitor the Sample Count statistic for each service in the ECS cluster. Set an alarm for when the math expression sample count/SERVICE_QUOTA(service)*100 is greater than

80. Notify the development team by using Amazon Simple Notification Service (Amazon SNS).

B. Use Amazon CloudWatch to monitor service quotas that are published under the AWS/Usage metric namespace. Set an alarm for when the math expression metric/SERVICE_QUOTA(metric)*100 is greater than 80. Notify the development team by using Amazon Simple Notification Service (Amazon SNS).

C. Create an AWS Lambda function to poll detailed metrics form the ECS cluster. When the number of running Fargate tasks is greater than 80, invoke Amazon Simple Email Service (Amazon SES) to notify the development team.

D. Create an AWS Config rule to evaluate whether the Fargate SERVICE_QUOTA is greater than 80. Use Amazon Simple Email Service (Amazon SES) to notify the development team when the AWS Config rule is not compliant.

Correct Answer: B

To visualize a service quota and optionally set an alarm.

Reference: https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-QuotasVisualize-Alarms.html

QUESTION 5

A solutions architect is implementing infrastructure as code for a two-tier web application in an AWS CloudFormation template. The web frontend application will be deployed on Amazon EC2 instances in an Auto Scaling group. The backend database will be an Amazon RDS for MySQL DB instance. The database password will be rotated every 60 days.

How can the solutions architect MOST securely manage the configuration of the application\\'s database credentials?

A. Provide the database password as a parameter in the CloudFormation template. Create an initialization script in the Auto Scaling group\\'s launch configuration UserData property to reference the password parameter using the Ref intrinsic function. Store the password on the EC2 instances. Reference the parameter for the value of the MasterUserPassword property in the AWS::RDS::DBInstance resource using the Ref intrinsic function.

B. Create a new AWS Secrets Manager secret resource in the CloudFormation template to be used as the database password. Configure the application to retrieve the password from Secrets Manager when needed. Reference the secret resource for the value of the MasterUserPassword property in the AWS::RDS::DBInstance resource using a dynamic reference.

C. Create a new AWS Secrets Manager secret resource in the CloudFormation template to be used as the database password. Create an initialization script in the Auto Scaling group\\'s launch configuration UserData property to reference the secret resource using the Ref intrinsic function. Reference the secret resource for the value of the MasterUserPassword property in the AWS::RDS::DBInstance resource using the Ref intrinsic function.

D. Create a new AWS Systems Manager Parameter Store parameter in the CloudFormation template to be used as the database password. Create an initialization script in the Auto Scaling group\\'s launch configuration UserData property to reference the parameter. Reference the parameter for the value of the MasterUserPassword property in the AWS::RDS::DBInstance resource using the Fn::GetAtt intrinsic function.

Correct Answer: D

QUESTION 6

You are developing a new mobile application and are considering storing user preferences in AWS.2w This would provide a more uniform cross-device experience to users using multiple mobile devices to access the application. The preference data for each user is estimated to be 50KB in size Additionally 5 million customers are expected to use the application on a regular basis.

The solution needs to be cost-effective, highly available, scalable and secure, how would you design a solution to meet the above requirements?

A. Setup an RDS MySQL instance in 2 availability zones to store the user preference data. Deploy a public facing application on a server in front of the database to manage security and access credentials

B. Setup a DynamoDB table with an item for each user having the necessary attributes to hold the user preferences. The mobile application will query the user preferences directly from the DynamoDB table. Utilize STS. Web Identity Federation, and DynamoDB Fine Grained Access Control to authenticate and authorize access.

C. Setup an RDS MySQL instance with multiple read replicas in 2 availability zones to store the user preference data .The mobile application will query the user preferences from the read replicas. Leverage the MySQL user management and access privilege system to manage security and access credentials.

D. Store the user preference data in S3 Setup a DynamoDB table with an item for each user and an item attribute pointing to the user\\' S3 object. The mobile application will retrieve the S3 URL from DynamoDB and then access the S3 object directly utilize STS, Web identity Federation, and S3 ACLs to authenticate and authorize access.

Correct Answer: B

Here are some of the things that you can build using fine-grained access control:

A mobile app that displays information for nearby airports, based on the user\\'s location. The app can

access and display attributes such airline names, arrival times, and flight numbers. However, it cannot

access or display pilot names or passenger counts.

A mobile game which stores high scores for all users in a single table. Each user can update their own

scores, but has no access to the other ones.

Reference:

https://aws.amazon.com/blogs/aws/fine-grained-access-control-for-amazon-dynamodb/

QUESTION 7

A company hosts a large on-premises MySQL database at its main office that supports an issue tracking system used by employees around the world. The company already uses AWS for some workloads and has created an Amazon Route 53 entry for the database endpoint that points to the on-premises database. Management is concerned about the database being a single point of failure and wants a solutions architect to migrate the database to AWS without any data loss or downtime.

Which set of actions should the solutions architect implement?

A. Create an Amazon Aurora DB cluster. Use AWS Database Migration Service (AWS DMS) to do a full load from the on-premises database to Aurora. Update the Route 53 entry for the database to point to the Aurora cluster endpoint, and shut down the on-premises database.

B. During nonbusiness hours, shut down the on-premises database and create a backup. Restore this backup to an Amazon Aurora DB cluster. When the restoration is complete, update the Route 53 entry for the database to point to the Aurora cluster endpoint, and shut down the on-premises database.

C. Create an Amazon Aurora DB cluster. Use AWS Database Migration Service (AWS DMS) to do a full load with continuous replication from the on-premises database to Aurora. When the migration is complete, update the Route 53 entry for the database to point to the Aurora cluster endpoint, and shut down the on-premises database.

D. Create a backup of the database and restore it to an Amazon Aurora multi-master cluster. This Aurora cluster will be in a master-master replication configuration with the on-premises database. Update the Route 53 entry for the database to point to the Aurora cluster endpoint, and shut down the on-premises database.

Correct Answer: C

"Around the world" eliminates possibility for the maintenance window at night. The other difference is ability to leverage

continuous replication in MySQL to Aurora case.

QUESTION 8

A company wants to use Amazon S3 to back up its on-premises file storage solution. The company\\'s on-premises file storage solution supports NFS, and the company wants its new solution to support NFS. The company wants to archive the backup files after 5 days. If the company needs archived files for disaster recovery, the company is willing to wait a few days for the retrieval of those files.

Which solution meets these requirements MOST cost-effectively?

A. Deploy an AWS Storage Gateway files gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the file gateway. Create an S3 Lifecycle rule to move the file to S3 Standard-Infrequent Access (S3 Standard-IA) after 5 days.

B. Deploy an AWS Storage Gateway volume gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the volume gateway. Create an S3 Lifecycle rule to move the files to S3 Glacier Deep Archive after 5 days.

C. Deploy an AWS Storage Gateway tape gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the tape gateway. Create an S3 Lifecycle rule to move the files to S3 Standard-Infrequent Access (S3 Standard-IA) after 5 days.

D. Deploy an AWS Storage Gateway file gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the file gateway. Create an S3 Lifecycle rule to move the files to S3 Glacier Deep Archive after 5 days.

Correct Answer: D

QUESTION 9

Your company hosts a social media site supporting users in multiple countries. You have been asked to provide a highly available design tor the application that leverages multiple regions tor the most recently accessed content and latency sensitive portions of the wet) site The most latency sensitive component of the application involves reading user preferences to support web site personalization and ad selection.

In addition to running your application in multiple regions, which option will support this application\\'s requirements?

A. Serve user content from S3. CloudFront and use Route53 latency-based routing between ELBs in each region Retrieve user preferences from a local DynamoDB table in each region and leverage SQS to capture changes to user preferences with SOS workers for propagating updates to each table.

B. Use the S3 Copy API to copy recently accessed content to multiple regions and serve user content from S3. CloudFront with dynamic content and an ELB in each region Retrieve user preferences from an ElasticCache cluster in each region and leverage SNS notifications to propagate user preference changes to a worker node in each region.

C. Use the S3 Copy API to copy recently accessed content to multiple regions and serve user content from S3 CloudFront and Route53 latency-based routing Between ELBs In each region Retrieve user preferences from a DynamoDB table and leverage SQS to capture changes to user preferences with SOS workers for propagating DynamoDB updates.

D. Serve user content from S3. CloudFront with dynamic content, and an ELB in each region Retrieve user preferences from an ElastiCache cluster in each region and leverage Simple Workflow (SWF) to manage the propagation of user

preferences from a centralized OB to each ElastiCache cluster.

Correct Answer: A

QUESTION 10

A manufacturing company is growing exponentially and has secured funding to improve its IT infrastructure and ecommerce presence. The company\\'s ecommerce platform consists of:

1.

Static assets primarily comprised of product images stored in Amazon S3.

2.

Amazon DynamoDB tables that store product information, user information, and order information.

3.

Web servers containing the application\\'s front-end behind Elastic Load Balancers.

The company wants to set up a disaster recovery site in a separate Region.

Which combination of actions should the solutions architect take to implement the new design while meeting all the requirements? (Choose three.)

A. Enable Amazon Route 53 health checks to determine if the primary site is down, and route traffic to the disaster recovery site if there is an issue.

B. Enable Amazon S3 cross-Region replication on the buckets that contain static assets.

C. Enable multi-Region targets on the Elastic Load Balancer and target Amazon EC2 instances in both Regions.

D. Enable DynamoDB global tables to achieve a multi-Region table replication.

E. Enable Amazon CloudWatch and create CloudWatch alarms that route traffic to the disaster recovery site when application latency exceeds the desired threshold.

F. Enable Amazon S3 versioning on the source and destination buckets containing static assets to ensure there is a rollback version available in the event of data corruption.

Correct Answer: AEF

QUESTION 11

You\\'re running an application on-premises due to its dependency on non-x86 hardware and want to use AWS for data backup. Your backup application is only able to write to POSIX-compatible block-based storage. You have 140TB of data and would like to mount it as a single folder on your file server. Users must be able to access portions of this data while the backups are taking place.

What backup solution would be most appropriate for this use case?

A. Use Storage Gateway and configure it to use Gateway Cached volumes.

B. Configure your backup software to use S3 as the target for your data backups.

C. Configure your backup software to use Glacier as the target for your data backups.

D. Use Storage Gateway and configure it to use Gateway Stored volumes.

Correct Answer: D

Volume gateway provides an iSCSI target, which enables you to create volumes and mount them as iSCSI devices from your on-premises application servers. The volume gateway runs in either a cached or stored mode.

In the cached mode, your primary data is written to S3, while you retain some portion of it locally in a cache for frequently accessed data. In the stored mode, your primary data is stored locally and your entire dataset is available for low- latency access while asynchronously backed up to AWS. In either mode, you can take point-in-time snapshots of your volumes and store them in Amazon S3, enabling you to make space-efficient versioned copies of your volumes for data protection and various data reuse needs.

QUESTION 12

A healthcare company runs a production workload on AWS that stores highly sensitive personal information. The security team mandates that, for auditing purposes, any AWS API action using AWS account root user credentials must automatically create a high-priority ticket in the company\\'s ticketing system. The ticketing system has a monthly 3-hour maintenance window when no tickets can be created.

To meet security requirements, the company enabled AWS CloudTrail logs and wrote a scheduled AWS Lambda function that uses Amazon Athena to query API actions performed by the root user. The Lambda function submits any actions found to the ticketing system API. During a recent security audit, the security team discovered that several tickets were not created because the ticketing system was unavailable due to planned maintenance.

Which combination of steps should a solutions architect take to ensure that the incidents are reported to the ticketing system even during planned maintenance? (Choose two.)

A. Create an Amazon SNS topic to which Amazon CloudWatch alarms will be published. Configure a CloudWatch alarm to invoke the Lambda function.

B. Create an Amazon SQS queue to which Amazon CloudWatch alarms will be published. Configure a CloudWatch alarm to publish to the SQS queue.

C. Modify the Lambda function to be triggered by messages published to an Amazon SNS topic. Update the existing application code to retry every 5 minutes if the ticketing system\\'s API endpoint is unavailable.

D. Modify the Lambda function to be triggered when there are messages in the Amazon SQS queue and to return successfully when the ticketing system API has processed the request.

E. Create an Amazon EventBridge rule that triggers on all API events where the invoking user identity is root. Configure the EventBridge rule to write the event to an Amazon SQS queue.

Correct Answer: BD

QUESTION 13

A North American company with headquarters on the East Coast is deploying a new web application running on Amazon EC2 in the us-east-1 Region. The application should dynamically scale to meet user demand and maintain

resiliency. Additionally, the application must have disaster recover capabilities in an active-passive configuration with the us-west-1 Region.

Which steps should a solutions architect take after creating a VPC in the us-east-1 Region?

A. Create a VPC in the us-west-1 Region. Use inter-Region VPC peering to connect both VPCs. Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the useast-1 Region. Deploy EC2 instances across multiple AZs in each Region as part of an Auto Scaling group spanning both VPCs and served by the ALB.

B. Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region. Deploy EC2 instances across multiple AZs as part of an Auto Scaling group served by the ALB. Deploy the same solution to the us-west-1 Region. Create an Amazon Route 53 record set with a failover routing policy and health checks enabled to provide high availability across both Regions.

C. Create a VPC in the us-west-1 Region. Use inter-Region VPC peering to connect both VPCs. Deploy an Application Load Balancer (ALB) that spans both VPCs. Deploy EC2 instances across multiple Availability Zones as part of an Auto Scaling group in each VPC served by the ALB. Create an Amazon Route 53 record that points to the ALB.

D. Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region. Deploy EC2 instances across multiple AZs as part of an Auto Scaling group served by the ALB. Deploy the same solution to the us-west-1 Region. Create separate Amazon Route 53 records in each Region that point to the ALB in the Region. Use Route 53 health checks to provide high availability across both Regions.

Correct Answer: B

A new web application in a active-passive DR mode. a Route 53 record set with a failover routing policy.

QUESTION 14

A company is using an on-premises Active Directory service for user authentication. The company wants to use the same authentication service to sign in to the company\\'s AWS accounts, which are using AWS Organizations. AWS Site-to- Site VPN connectivity already exists between the on-premises environment and all the company\\'s AWS accounts.

The company\\'s security policy requires conditional access to the accounts based on user groups and roles. User identities must be managed in a single location.

Which solution will meet these requirements?

A. Configure AWS Single Sign-On (AWS SSO) to connect to Active Directory by using SAML 2.0. Enable automatic provisioning by using the System for Cross-domain Identity Management (SCIM) v2.0 protocol. Grant access to the AWS accounts by using attribute-based access controls (ABACs).

B. Configure AWS Single Sign-On (AWS SSO) by using AWS SSO as an identity source. Enable automatic provisioning by using the System for Cross-domain Identity Management (SCIM) v2.0 protocol. Grant access to the AWS accounts by using AWS SSO permission sets.

C. In one of the company\\'s AWS accounts, configure AWS Identity and Access Management (IAM) to use a SAML 2.0 identity provider. Provision IAM users that are mapped to the federated users. Grant access that corresponds to appropriate groups in Active Directory. Grant access to the required AWS accounts by using cross-account IAM users.

D. In one of the company\\'s AWS accounts, configure AWS Identity and Access Management (IAM) to use an OpenID Connect (OIDC) identity provider. Provision IAM roles that grant access to the AWS account for the federated users that correspond to appropriate groups in Active Directory. Grant access to the required AWS accounts by using cross-

account IAM roles.

Correct Answer: B

QUESTION 15

A company has introduced a new policy that allows employees to work remotely from their homes if they connect by using a VPN The company Is hosting Internal applications with VPCs in multiple AWS accounts Currently the applications are accessible from the company\\'s on-premises office network through an AWS Site-to-Site VPN connection The VPC in the company\\'s main AWS account has peering connections established with VPCs in other AWS accounts.

A solutions architect must design a scalable AWS Client VPN solution for employees to use while they work from home.

What is the MOST cost-effective solution that meets these requirements?

A. Create a Client VPN endpoint in each AWS account Configure required routing that allows access to internal applications

B. Create a Client VPN endpoint in the mam AWS account Configure required routing that allows access to internal applications

C. Create a Client VPN endpoint in the main AWS account Provision a transit gateway that is connected to each AWS account Configure required routing that allows access to internal applications

D. Create a Client VPN endpoint in the mam AWS account Establish connectivity between the Client VPN endpoint and the AWS Site-to-Site VPN

Correct Answer: C