

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.leads4pass.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 solutions architect is determining the DNS strategy for an existing VPC. The VPC is provisioned to use the 10.24.34.0/24 CIDR block. The VPC also uses Amazon Route 53 Resolver for DNS. New requirements mandate that DNS queries

must use private hosted zones. Additionally, instances that have public IP addresses must receive corresponding public hostnames.

Which solution will meet these requirements to ensure that the domain names are correctly resolved within the VPC?

- A. Create a private hosted zone. Activate the `enableDnsSupport` attribute and the `enableDnsHostnames` attribute for the VPC. Update the VPC DHCP options set to include `domain-name-servers-10.24.34.2`.
- B. Create a private hosted zone. Associate the private hosted zone with the VPC. Activate the `enableDnsSupport` attribute and the `enableDnsHostnames` attribute for the VPC. Create a new VPC DHCP options set, and configure `domain-name-servers=AmazonProvidedDNS`. Associate the new DHCP options set with the VPC.
- C. Deactivate the `enableDnsSupport` attribute for the VPC. Activate the `enableDnsHostnames` attribute for the VPC. Create a new VPC DHCP options set, and configure `domain-name-servers=10.24.34.2`. Associate the new DHCP options set with the VPC.
- D. Create a private hosted zone. Associate the private hosted zone with the VPC. Activate the `enableDnsSupport` attribute for the VPC. Deactivate the `enableDnsHostnames` attribute for the VPC. Update the VPC DHCP options set to include `domain-name-servers=AmazonProvidedDNS`.

Correct Answer: B

This option allows the solutions architect to use a private hosted zone to host DNS records that are only accessible within the VPC1. By associating the private hosted zone with the VPC, the solutions architect can ensure that DNS queries from the VPC are routed to the private hosted zone2. By activating the `enableDnsSupport` attribute and the `enableDnsHostnames` attribute for the VPC, the solutions architect can enable DNS resolution and hostname assignment for instances in the VPC3. By creating a new VPC DHCP options set, and configuring `domain-name-servers=AmazonProvidedDNS`, the solutions architect can use Amazon-provided DNS servers to resolve DNS queries from instances in the VPC4. By associating the new DHCP options set with the VPC, the solutions architect can apply the DNS settings to all instances in the VPC5. References: What is Amazon Route 53 Resolver? Associating a private hosted zone with your VPC Using DNS with your VPC DHCP options sets Modifying your DHCP options

QUESTION 2

An online retail company hosts its stateful web-based application and MySQL database in an on-premises data center on a single server. The company wants to increase its customer base by conducting more marketing campaigns and promotions. In preparation, the company wants to migrate its application and database to AWS to increase the reliability of its architecture.

Which solution should provide the HIGHEST level of reliability?

- A. Migrate the database to an Amazon RDS MySQL Multi-AZ DB instance. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer. Store sessions in Amazon Neptune.
- B. Migrate the database to Amazon Aurora MySQL. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer. Store sessions in an Amazon ElastiCache for Redis replication group.

C. Migrate the database to Amazon DocumentDB (with MongoDB compatibility). Deploy the application in an Auto Scaling group on Amazon EC2 instances behind a Network Load Balancer. Store sessions in Amazon Kinesis Data Firehose.

D. Migrate the database to an Amazon RDS MariaDB Multi-AZ DB instance. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer. Store sessions in Amazon ElastiCache for Memcached.

Correct Answer: B

This option allows the company to use Amazon Aurora MySQL, which is a fully managed relational database service that is compatible with MySQL and offers up to five times better performance than standard MySQL¹. By migrating the database to Aurora MySQL, the company can benefit from its high availability, durability, scalability, and security features¹. By deploying the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load

Balancer, the company can ensure that the application can handle varying levels of traffic and distribute the requests across multiple instances². By storing sessions in an Amazon ElastiCache for Redis replication group, the company can

improve the performance and reliability of the session data by using a fast, in-memory data store that supports replication and failover³.

References:

What is Amazon Aurora?

What is Auto Scaling?

What is Amazon ElastiCache?

QUESTION 3

A company needs to create and manage multiple AWS accounts for a number of departments from a central location. The security team requires read-only access to all accounts from its own AWS account. The company is using AWS Organizations and created an account for the security team.

How should a solutions architect meet these requirements?

A. Use the OrganizationAccountAccessRole IAM role to create a new IAM policy with read-only access in each member account. Establish a trust relationship between the IAM policy in each member account and the security account. Ask the security team to use the IAM policy to gain access.

B. Use the OrganizationAccountAccessRole IAM role to create a new IAM role with read-only access in each member account. Establish a trust relationship between the IAM role in each member account and the security account. Ask the security team to use the IAM role to gain access.

C. Ask the security team to use AWS Security Token Service (AWS STS) to call the AssumeRole API for the OrganizationAccountAccessRole IAM role in the management account from the security account. Use the generated temporary credentials to gain access.

D. Ask the security team to use AWS Security Token Service (AWS STS) to call the AssumeRole API for the OrganizationAccountAccessRole IAM role in the member account from the security account. Use the generated temporary credentials to gain access.

Correct Answer: B

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_access.html#orgs_manage_accounts_access-cross-account-role "When you create a member account using the AWS Organizations console, AWS Organizations automatically creates an IAM role named OrganizationAccountAccessRole in the account" you need OrganizationAccountAccessRole in member account to create a read-only role and use role from security team to assume this read-only role.

QUESTION 4

A company is using AWS CloudFormation to deploy its infrastructure. The company is concerned that if a production CloudFormation stack is deleted, important data stored in Amazon RDS databases or Amazon EBS volumes might also be deleted.

Now can the company prevent users from accidentally deleting data in this way?

- A. Modify the CloudFormation templates to add a DeletionPolicy attribute to RDS and EBS resources.
- B. Configure a stack policy that disallows the deletion of RDS and EBS resources.
- C. Modify IAM policies to deny deleting RDS and EBS resources that are tagged with an "aws:cloudformation:stack-name" tag.
- D. Use AWS Config rules to prevent deleting RDS and EBS resources.

Correct Answer: A

With the DeletionPolicy attribute you can preserve or (in some cases) backup a resource when its stack is deleted. You specify a DeletionPolicy attribute for each resource that you want to control. If a resource has no DeletionPolicy attribute, AWS CloudFormation deletes the resource by default. To keep a resource when its stack is deleted, specify Retain for that resource. You can use retain for any resource. For example, you can retain a nested stack, Amazon S3 bucket, or EC2 instance so that you can continue to use or modify those resources after you delete their stacks.

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-deletionpolicy.html>

QUESTION 5

A financial services company sells its software-as-a-service (SaaS) platform for application compliance to large global banks. The SaaS platform runs on AWS and uses multiple AWS accounts that are managed in an organization in AWS Organizations. The SaaS platform uses many AWS resources globally.

For regulatory compliance, all API calls to AWS resources must be audited, tracked for changes, and stored in a durable and secure data store.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Create a new AWS CloudTrail trail. Use an existing Amazon S3 bucket in the organization's management account to store the logs. Deploy the trail to all AWS Regions. Enable MFA delete and encryption on the S3 bucket.
- B. Create a new AWS CloudTrail trail in each member account of the organization. Create new Amazon S3 buckets to store the logs. Deploy the trail to all AWS Regions. Enable MFA delete and encryption on the S3 buckets.
- C. Create a new AWS CloudTrail trail in the organization's management account. Create a new Amazon S3 bucket

with versioning turned on to store the logs. Deploy the trail for all accounts in the organization. Enable MFA delete and encryption on the S3 bucket.

D. Create a new AWS CloudTrail trail in the organization's management account. Create a new Amazon S3 bucket to store the logs. Configure Amazon Simple Notification Service (Amazon SNS) to send log-file delivery notifications to an external management system that will track the logs. Enable MFA delete and encryption on the S3 bucket.

Correct Answer: C

The correct answer is C. This option uses AWS CloudTrail to create a trail in the organization's management account that applies to all accounts in the organization. This way, the company can centrally manage and audit all API calls to AWS resources across multiple accounts and regions. The company also needs to create a new Amazon S3 bucket with versioning turned on to store the logs. Versioning helps protect against accidental or malicious deletion of log files by keeping multiple versions of each object in the bucket. The company also needs to enable MFA delete and encryption on the S3 bucket to further enhance the security and durability of the data store. Option A is incorrect because it uses an existing S3 bucket in the organization's management account to store the logs. This may not be optimal for regulatory compliance, as the existing bucket may have different permissions, encryption settings, or lifecycle policies than a dedicated bucket for CloudTrail logs. Option B is incorrect because it requires creating a new CloudTrail trail in each member account of the organization. This adds operational overhead and complexity, as the company would need to manage multiple trails and S3 buckets across multiple accounts and regions. Option D is incorrect because it requires configuring Amazon SNS to send log-file delivery notifications to an external management system that will track the logs. This adds unnecessary complexity and cost, as CloudTrail already provides log-file integrity validation and log-file digest delivery features that can help verify the authenticity and integrity of log files. Reference: Creating a Trail for an Organization

[SAP-C02 VCE Dumps](#)

[SAP-C02 Practice Test](#)

[SAP-C02 Study Guide](#)