

# Amazon-Web-Services

## Exam Questions SAP-C02

AWS Certified Solutions Architect - Professional



**NEW QUESTION 1**

- (Exam Topic 1)

A company wants to migrate its data analytics environment from on premises to AWS. The environment consists of two simple Node.js applications. One of the applications collects sensor data and loads it into a MySQL database. The other application aggregates the data into reports. When the aggregation jobs run, some of the load jobs fail to run correctly.

The company must resolve the data loading issue. The company also needs the migration to occur without interruptions or changes for the company's customers. What should a solutions architect do to meet these requirements?

- A. Set up an Amazon Aurora MySQL database as a replication target for the on-premises database. Create an Aurora Replica for the Aurora MySQL database, and move the aggregation jobs to run against the Aurora Replica. Set up collection endpoints as AWS Lambda functions behind a Network Load Balancer (NLB), and use Amazon RDS Proxy to write to the Aurora MySQL database. When the databases are synced, disable the replication job and restart the Aurora Replica as the primary instance.
- B. Point the collector DNS record to the NLB.
- C. Set up an Amazon Aurora MySQL database. Use AWS Database Migration Service (AWS DMS) to perform continuous data replication from the on-premises database to Aurora. Move the aggregation jobs to run against the Aurora MySQL database. Set up collection endpoints behind an Application Load Balancer (ALB) as Amazon EC2 instances in an Auto Scaling group. When the databases are synced, point the collector DNS record to the ALB. Disable the AWS DMS sync task after the cutover from on premises to AWS.
- D. Set up an Amazon Aurora MySQL database. Use AWS Database Migration Service (AWS DMS) to perform continuous data replication from the on-premises database to Aurora. Create an Aurora Replica for the Aurora MySQL database and move the aggregation jobs to run against the Aurora Replica. Set up collection endpoints as AWS Lambda functions behind an Application Load Balancer (ALB) and use Amazon RDS Proxy to write to the Aurora MySQL database. When the databases are synced, point the collector DNS record to the ALB. Disable the AWS DMS sync task after the cutover from on premises to AWS.
- E. Set up an Amazon Aurora MySQL database. Create an Aurora Replica for the Aurora MySQL database and move the aggregation jobs to run against the Aurora Replica. Set up collection endpoints as an Amazon Kinesis data stream. Use Amazon Kinesis Data Firehose to replicate the data to the Aurora MySQL database. When the databases are synced, disable the replication job and restart the Aurora Replica as the primary instance. Point the collector DNS record to the Kinesis data stream.

**Answer: C**

**Explanation:**

Set up an Amazon Aurora MySQL database. Use AWS Database Migration Service (AWS DMS) to perform continuous data replication from the on-premises database to Aurora. Create an Aurora Replica for the Aurora MySQL database, and move the aggregation jobs to run against the Aurora Replica. Set up collection endpoints as AWS Lambda functions behind an Application Load Balancer (ALB), and use Amazon RDS Proxy to write to the Aurora MySQL database. When the databases are synced, point the collector DNS record to the ALB. Disable the AWS DMS sync task after the cutover from on premises to AWS.

Amazon RDS Proxy allows applications to pool and share connections established with the database, improving database efficiency and application scalability. With RDS Proxy, failover times for Aurora and RDS databases are reduced by up to 66%.

**NEW QUESTION 2**

- (Exam Topic 1)

A solutions architect needs to advise a company on how to migrate its on-premises data processing application to the AWS Cloud. Currently, users upload input files through a web portal. The web server then stores the uploaded files on NAS and messages the processing server over a message queue. Each media file can take up to 1 hour to process. The company has determined that the number of media files awaiting processing is significantly higher during business hours, with the number of files rapidly declining after business hours.

What is the MOST cost-effective migration recommendation?

- A. Create a queue using Amazon SQS.
- B. Configure the existing web server to publish to the new queue. When there are messages in the queue, invoke an AWS Lambda function to pull requests from the queue and process the file.
- C. Store the processed files in an Amazon S3 bucket.
- D. Create a queue using Amazon SNS.
- E. Configure the existing web server to publish to the new queue.
- F. When there are messages in the queue, create a new Amazon EC2 instance to pull requests from the queue and process the file.
- G. Store the processed files in Amazon EFS.
- H. Shut down the EC2 instance after the task is complete.
- I. Create a queue using Amazon MQ.
- J. Configure the existing web server to publish to the new queue. When there are messages in the queue, invoke an AWS Lambda function to pull requests from the queue and process the file.
- K. Store the processed files in Amazon EFS.
- L. Create a queue using Amazon SNS.
- M. Configure the existing web server to publish to the new queue.
- N. Use Amazon EC2 instances in an EC2 Auto Scaling group to pull requests from the queue and process the file.
- O. Scale the EC2 instances based on the SQS queue length.
- P. Store the processed files in an Amazon S3 bucket.

**Answer: D**

**Explanation:**

<https://aws.amazon.com/blogs/compute/operating-lambda-performance-optimization-part-1/>

**NEW QUESTION 3**

- (Exam Topic 1)

A company runs an IoT platform on AWS. IoT sensors in various locations send data to the company's Node.js API servers on Amazon EC2 instances running behind an Application Load Balancer. The data is stored in an Amazon RDS MySQL DB instance that uses a 4 TB General Purpose SSD volume.

The number of sensors the company has deployed in the field has increased over time and is expected to grow significantly. The API servers are consistently overloaded, and RDS metrics show high write latency.

Which of the following steps together will resolve the issues permanently and enable growth as new sensors are provisioned, while keeping this platform cost-efficient? (Select TWO.)

- A. Resize the MySQL General Purpose SSD storage to 6 TB to improve the volume's IOPS.
- B. Re-architect the database tier to use Amazon Aurora instead of an RDS MySQL DB instance and add read replicas.

- C. Leverage Amazon Kinesis Data Streams and AWS Lambda to ingest and process the raw data
- D. Use AWS X-Ray to analyze and debug application issues and add more API servers to match the load
- E. Re-architect the database tier to use Amazon DynamoDB instead of an RDS MySQL DB instance

**Answer:** CE

**Explanation:**

➤ Option C is correct because leveraging Amazon Kinesis Data Streams and AWS Lambda to ingest and process the raw data resolves the issues permanently and enable growth as new sensors are provisioned. Amazon Kinesis Data Streams is a serverless streaming data service that simplifies the capture, processing, and storage of data streams at any scale. Kinesis Data Streams can handle any amount of streaming data and process data from hundreds of thousands of sources with very low latency. AWS Lambda is a serverless compute service that lets you run code without provisioning or managing servers. Lambda can be triggered by Kinesis Data Streams events and process the data records in real time. Lambda can also scale automatically based on the incoming data volume. By using Kinesis Data Streams and Lambda, the company can reduce the load on the API servers and improve the performance and scalability of the data ingestion and processing layer3

➤ Option E is correct because re-architecting the database tier to use Amazon DynamoDB instead of an RDS MySQL DB instance resolves the issues permanently and enable growth as new sensors are provisioned. Amazon DynamoDB is a fully managed key-value and document database that delivers single-digit millisecond performance at any scale. DynamoDB supports auto scaling, which automatically adjusts read and write capacity based on actual traffic patterns. DynamoDB also supports on-demand capacity mode, which instantly accommodates up to double the previous peak traffic on a table. By using DynamoDB instead of RDS MySQL DB instance, the company can eliminate high write latency and improve scalability and performance of the database tier.

References: 1: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html> 2:

[https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/CHAP\\_AuroraOverview.html](https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/CHAP_AuroraOverview.html) 3:

<https://docs.aws.amazon.com/streams/latest/dev/introduction.html> : <https://docs.aws.amazon.com/lambda/latest/dg/welcome.html> :

<https://docs.aws.amazon.com/xray/latest/devguide/aws-xray.html> : <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html> :

**NEW QUESTION 4**

- (Exam Topic 1)

A company is refactoring its on-premises order-processing platform in the AWS Cloud. The platform includes a web front end that is hosted on a fleet of VMs RabbitMQ to connect the front end to the backend, and a Kubernetes cluster to run a containerized backend system to process the orders. The company does not want to make any major changes to the application

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

- A. Create an AMI of the web server VM Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer Set up Amazon MQ to replace the on-premises messaging queue Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend
- B. Create a custom AWS Lambda runtime to mimic the web server environment Create an Amazon API Gateway API to replace the front-end web servers Set up Amazon MQ to replace the on-premises messaging queue Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend
- C. Create an AMI of the web server VM Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer Set up Amazon MQ to replace the on-premises messaging queue Install Kubernetes on a fleet of different EC2 instances to host the order-processing backend
- D. Create an AMI of the web server VM Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer Set up an Amazon Simple Queue Service (Amazon SQS) queue to replace the on-premises messaging queue Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend

**Answer:** A

**Explanation:**

<https://aws.amazon.com/about-aws/whats-new/2020/11/announcing-amazon-mq-rabbitmq/>

**NEW QUESTION 5**

- (Exam Topic 1)

A software as a service (SaaS) based company provides a case management solution to customers A3 part of the solution. The company uses a standalone Simple Mail Transfer Protocol (SMTP) server to send email messages from an application. The application also stores an email template for acknowledgement email messages that populate customer data before the application sends the email message to the customer.

The company plans to migrate this messaging functionality to the AWS Cloud and needs to minimize operational overhead.

Which solution will meet these requirements MOST cost-effectively?

- A. Set up an SMTP server on Amazon EC2 instances by using an AMI from the AWS Marketplac
- B. Store the email template in an Amazon S3 bucke
- C. Create an AWS Lambda function to retrieve the template from the S3 bucket and to merge the customer data from the application with the templat
- D. Use an SDK in the Lambda function to send the email message.
- E. Set up Amazon Simple Email Service (Amazon SES) to send email message
- F. Store the email template in an Amazon S3 bucke
- G. Create an AWS Lambda function to retrieve the template from the S3 bucket and to merge the customer data from the application with the templat
- H. Use an SDK in the Lambda function to send the email message.
- I. Set up an SMTP server on Amazon EC2 instances by using an AMI from the AWS Marketplac
- J. Store the email template in Amazon Simple Email Service (Amazon SES) with parameters for the customer dat
- K. Create an AWS Lambda function to call the SES template and to pass customer data to replace the parameter
- L. Use the AWS Marketplace SMTP server to send the email message.
- M. Set up Amazon Simple Email Service (Amazon SES) to send email message
- N. Store the email template on Amazon SES with parameters for the customer dat
- O. Create an AWS Lambda function to call the SendTemplatedEmail API operation and to pass customer data to replace the parameters and the email destination.

**Answer:** D

**Explanation:**

In this solution, the company can use Amazon SES to send email messages, which will minimize operational overhead as SES is a fully managed service that handles sending and receiving email messages. The company can store the email template on Amazon SES with parameters for the customer data and use an AWS Lambda function to call the SendTemplatedEmail API operation, passing in the customer data to replace the parameters and the email destination. This solution eliminates the need to set up and manage an SMTP server on EC2 instances, which can be costly and time-consuming.

**NEW QUESTION 6**

- (Exam Topic 1)

An international delivery company hosts a delivery management system on AWS. Drivers use the system to upload confirmation of delivery. Confirmation includes the recipient's signature or a photo of the package with the recipient. The driver's handheld device uploads signatures and photos through FTP to a single Amazon EC2 instance. Each handheld device saves a file in a directory based on the signed-in user, and the file name matches the delivery number. The EC2 instance then adds metadata to the file after querying a central database to pull delivery information. The file is then placed in Amazon S3 for archiving.

As the company expands, drivers report that the system is rejecting connections. The FTP server is having problems because of dropped connections and memory issues. In response to these problems, a system engineer schedules a cron task to reboot the EC2 instance every 30 minutes. The billing team reports that files are not always in the archive and that the central system is not always updated.

A solutions architect needs to design a solution that maximizes scalability to ensure that the archive always receives the files and that systems are always updated. The handheld devices cannot be modified, so the company cannot deploy a new application.

Which solution will meet these requirements?

- A. Create an AMI of the existing EC2 instance
- B. Create an Auto Scaling group of EC2 instances behind an Application Load Balance
- C. Configure the Auto Scaling group to have a minimum of three instances.
- D. Use AWS Transfer Family to create an FTP server that places the files in Amazon Elastic File System (Amazon EFS). Mount the EFS volume to the existing EC2 instance
- E. Point the EC2 instance to the new path for file processing.
- F. Use AWS Transfer Family to create an FTP server that places the files in Amazon S3. Use an S3 event notification through Amazon Simple Notification Service (Amazon SNS) to invoke an AWS Lambda function
- G. Configure the Lambda function to add the metadata and update the delivery system.
- H. Update the handheld devices to place the files directly in Amazon S3. Use an S3 event notification through Amazon Simple Queue Service (Amazon SQS) to invoke an AWS Lambda function
- I. Configure the Lambda function to add the metadata and update the delivery system.

**Answer:** C

**Explanation:**

Using AWS Transfer Family to create an FTP server that places the files in Amazon S3 and using S3 event notifications through Amazon Simple Notification Service (Amazon SNS) to invoke an AWS Lambda function will ensure that the archive always receives the files and that the central system is always updated. This solution maximizes scalability and eliminates the need for manual intervention, such as rebooting the EC2 instance.

**NEW QUESTION 7**

- (Exam Topic 1)

A company is hosting a three-tier web application in an on-premises environment. Due to a recent surge in traffic that resulted in downtime and a significant financial impact, company management has ordered that the application be moved to AWS. The application is written in .NET and has a dependency on a MySQL database. A solutions architect must design a scalable and highly available solution to meet the demand of 200,000 daily users.

Which steps should the solutions architect take to design an appropriate solution?

- A. Use AWS Elastic Beanstalk to create a new application with a web server environment and an Amazon RDS MySQL Multi-AZ DB instance. The environment should launch a Network Load Balancer (NLB) in front of an Amazon EC2 Auto Scaling group in multiple Availability Zones. Use an Amazon Route 53 alias record to route traffic from the company's domain to the NLB.
- B. Use AWS CloudFormation to launch a stack containing an Application Load Balancer (ALB) in front of an Amazon EC2 Auto Scaling group spanning three Availability Zones
- C. The stack should launch a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a Retain deletion policy
- D. Use an Amazon Route 53 alias record to route traffic from the company's domain to the ALB
- E. Use AWS Elastic Beanstalk to create an automatically scaling web server environment that spans two separate Regions with an Application Load Balancer (ALB) in each Region
- F. Create a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a cross-Region read replica. Use Amazon Route 53 with a geoproximity routing policy to route traffic between the two Regions.
- G. Use AWS CloudFormation to launch a stack containing an Application Load Balancer (ALB) in front of an Amazon ECS cluster of Spot Instances spanning three Availability Zones. The stack should launch an Amazon RDS MySQL DB instance with a Snapshot deletion policy. Use an Amazon Route 53 alias record to route traffic from the company's domain to the ALB.

**Answer:** C

**Explanation:**

Using AWS CloudFormation to launch a stack with an Application Load Balancer (ALB) in front of an Amazon EC2 Auto Scaling group spanning three Availability Zones, a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a Retain deletion policy, and an Amazon Route 53 alias record to route traffic from the company's domain to the ALB will ensure that

**NEW QUESTION 8**

- (Exam Topic 1)

A software company hosts an application on AWS with resources in multiple AWS accounts and Regions. The application runs on a group of Amazon EC2 instances in an application VPC located in the us-east-1 Region with an IPv4 CIDR block of 10.10.0.0/16. In a different AWS account, a shared services VPC is located in the us-east-2 Region with an IPv4 CIDR block of 10.10.10.0/24. When a cloud engineer uses AWS CloudFormation to attempt to peer the application VPC with the shared services VPC, an error message indicates a peering failure. Which factors could cause this error? (Choose two.)

- A. The IPv4 CIDR ranges of the two VPCs overlap
- B. The VPCs are not in the same Region
- C. One or both accounts do not have access to an Internet gateway
- D. One of the VPCs was not shared through AWS Resource Access Manager
- E. The IAM role in the peer acceptor account does not have the correct permissions

**Answer:** AE

**Explanation:**

<https://aws.amazon.com/about-aws/whats-new/2017/11/announcing-support-for-inter-region-vpc-peering/>



**NEW QUESTION 9**

- (Exam Topic 1)

A company has 50 AWS accounts that are members of an organization in AWS Organizations. Each account contains multiple VPCs. The company wants to use AWS Transit Gateway to establish connectivity between the VPCs in each member account. Each time a new member account is created, the company wants to automate the process of creating a new VPC and a transit gateway attachment.

Which combination of steps will meet these requirements? (Select TWO)

- A. From the management account, share the transit gateway with member accounts by using AWS Resource Access Manager
- B. From the management account, share the transit gateway with member accounts by using an AWS Organizations SCP
- C. Launch an AWS CloudFormation stack set from the management account that automatically creates a new VPC and a VPC transit gateway attachment in a member account
- D. Associate the attachment with the transit gateway in the management account by using the transit gateway ID.
- E. Launch an AWS CloudFormation stack set from the management account that automatically creates a new VPC and a peering transit gateway attachment in a member account
- F. Share the attachment with the transit gateway in the management account by using a transit gateway service-linked role.
- G. From the management account, share the transit gateway with member accounts by using AWS Service Catalog

**Answer:** AC

**Explanation:**

<https://aws.amazon.com/blogs/mt/self-service-vpcs-in-aws-control-tower-using-aws-service-catalog/> <https://docs.aws.amazon.com/vpc/latest/tgw/tgw-transit-gateways.html>

[https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-ec2-transitgatewayattachme](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-ec2-transitgatewayattachment.html)

**NEW QUESTION 10**

- (Exam Topic 1)

A company manages multiple AWS accounts by using AWS Organizations. Under the root OU, the company has two OUs: Research and DataOps.

Because of regulatory requirements, all resources that the company deploys in the organization must reside in the ap-northeast-1 Region. Additionally, EC2 instances that the company deploys in the DataOps OU must use a predefined list of instance types.

A solutions architect must implement a solution that applies these restrictions. The solution must maximize operational efficiency and must minimize ongoing maintenance.

Which combination of steps will meet these requirements? (Select TWO)

- A. Create an IAM role in one account under the DataOps OU. Use the ec2 Instance Type condition key in an inline policy on the role to restrict access to specific instance types.
- B. Create an IAM user in all accounts under the root OU. Use the aws:RequestedRegion condition key in an inline policy on each user to restrict access to all AWS Regions except ap-northeast-1.
- C. Create an SCP. Use the aws:RequestedRegion condition key to restrict access to all AWS Regions except ap-northeast-1. Apply the SCP to the root OU.
- D. Create an SCP. Use the ec2:InstanceType condition key to restrict access to all AWS Regions except ap-northeast-1. Apply the SCP to the root OU.
- E. the DataOps OU.
- F. and the Research OU.
- G. Create an SCP. Use the ec2:InstanceType condition key to restrict access to specific instance types. Apply the SCP to the DataOps OU.

**Answer:** CE

**Explanation:**

[https://docs.aws.amazon.com/IAM/latest/UserGuide/reference\\_policies\\_examples\\_aws\\_deny-requested-region.h](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_aws_deny-requested-region.html)

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scps\\_examples\\_ec2.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_ec2.html)

**NEW QUESTION 10**

- (Exam Topic 1)

A finance company hosts a data lake in Amazon S3. The company receives financial data records over SFTP each night from several third parties. The company runs its own SFTP server on an Amazon EC2 instance in a public subnet of a VPC. After the files are uploaded, they are moved to the data lake by a cron job that runs on the same instance. The SFTP server is reachable on DNS `sftp.example.com` through the use of Amazon Route 53.

What should a solutions architect do to improve the reliability and scalability of the SFTP solution?

- A. Move the EC2 instance into an Auto Scaling group
- B. Place the EC2 instance behind an Application Load Balancer (ALB). Update the DNS record `sftp.example.com` in Route 53 to point to the ALB.
- C. Migrate the SFTP server to AWS Transfer for SFTP
- D. Update the DNS record `sftp.example.com` in Route 53 to point to the server endpoint hostname.
- E. Migrate the SFTP server to a file gateway in AWS Storage Gateway
- F. Update the DNS record `sftp.example.com` in Route 53 to point to the file gateway endpoint.
- G. Place the EC2 instance behind a Network Load Balancer (NLB). Update the DNS record `sftp.example.com` in Route 53 to point to the NLB.

**Answer:** B

**Explanation:**

<https://aws.amazon.com/aws-transfer-family/faqs/> <https://docs.aws.amazon.com/transfer/latest/userguide/what-is-aws-transfer-family.html>

[https://aws.amazon.com/about-aws/whats-new/2018/11/aws-transfer-for-sftp-fully-managed-sftp-for-s3/?nc1=h\\_](https://aws.amazon.com/about-aws/whats-new/2018/11/aws-transfer-for-sftp-fully-managed-sftp-for-s3/?nc1=h_)

**NEW QUESTION 14**

- (Exam Topic 1)

A company is running a critical application that uses an Amazon RDS for MySQL database to store data. The RDS DB instance is deployed in Multi-AZ mode.

A recent RDS database failover test caused a 40-second outage to the application. A solutions architect needs to design a solution to reduce the outage time to less than 20 seconds.

Which combination of steps should the solutions architect take to meet these requirements? (Select THREE.)

- A. Use Amazon ElastiCache for Memcached in front of the database
- B. Use Amazon ElastiCache for Redis in front of the database.
- C. Use RDS Proxy in front of the database

- D. Migrate the database to Amazon Aurora MySQL
- E. Create an Amazon Aurora Replica
- F. Create an RDS for MySQL read replica

**Answer:** CDE

**Explanation:**

Migrate the database to Amazon Aurora MySQL. - Create an Amazon Aurora Replica. - Use RDS Proxy in front of the database. - These options are correct because they address the requirement of reducing the failover time to less than 20 seconds. Migrating to Amazon Aurora MySQL and creating an Aurora replica can reduce the failover time to less than 20 seconds. Aurora has a built-in, fault-tolerant storage system that can automatically detect and repair failures. Additionally, Aurora has a feature called "Aurora Global Database" which allows you to create read-only replicas across multiple AWS regions which can further help to reduce the failover time. Creating an Aurora replica can also help to reduce the failover time as it can take over as the primary DB instance in case of a failure. Using RDS proxy can also help to reduce the failover time as it can route the queries to the healthy DB instance, it also helps to balance the load across multiple DB instances.

**NEW QUESTION 17**

- (Exam Topic 1)

An enterprise company wants to allow its developers to purchase third-party software through AWS Marketplace. The company uses an AWS Organizations account structure with full features enabled, and has a shared services account in each organizational unit (OU) that will be used by procurement managers. The procurement team's policy indicates that developers should be able to obtain third-party software from an approved list only and use Private Marketplace in AWS Marketplace to achieve this requirement. The procurement team wants administration of Private Marketplace to be restricted to a role named procurement-manager-role, which could be assumed by procurement managers. Other IAM users, groups, roles, and account administrators in the company should be denied Private Marketplace administrative access.

What is the MOST efficient way to design an architecture to meet these requirements?

- A. Create an IAM role named procurement-manager-role in all AWS accounts in the organization. Add the PowerUserAccess managed policy to the role. Apply an inline policy to all IAM users and roles in every AWS account to deny permissions on the AWSPPrivateMarketplaceAdminFullAccess managed policy.
- B. Create an IAM role named procurement-manager-role in all AWS accounts in the organization. Add the AdministratorAccess managed policy to the role. Define a permissions boundary with the AWSPPrivateMarketplaceAdminFullAccess managed policy and attach it to all the developer roles.
- C. Create an IAM role named procurement-manager-role in all the shared services accounts in the organization. Add the AWSPPrivateMarketplaceAdminFullAccess managed policy to the role. Create an organization root-level SCP to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role. Create another organization root-level SCP to deny permissions to create an IAM role named procurement-manager-role to everyone in the organization.
- D. Create an IAM role named procurement-manager-role in all AWS accounts that will be used by developer.
- E. Add the AWSPPrivateMarketplaceAdminFullAccess managed policy to the role.
- F. Create an SCP in Organizations to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role.
- G. Apply the SCP to all the shared services accounts in the organization.

**Answer:** C

**Explanation:**

SCP to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role.

<https://aws.amazon.com/blogs/aws/marketplace/controlling-access-to-a-well-architected-private-marketplace-use-case/>

This approach allows the procurement managers to assume the procurement-manager-role in shared services accounts, which have the AWSPPrivateMarketplaceAdminFullAccess managed policy attached to it and can then manage the Private Marketplace. The organization root-level SCP denies the permission to administer Private Marketplace to everyone except the role named procurement-manager-role and another SCP denies the permission to create an IAM role named procurement-manager-role to everyone in the organization, ensuring that only the procurement team can assume the role and manage the Private Marketplace. This approach provides a centralized way to manage and restrict access to Private Marketplace while maintaining a high level of security.

**NEW QUESTION 19**

- (Exam Topic 1)

A company has developed APIs that use Amazon API Gateway with Regional endpoints. The APIs call AWS Lambda functions that use API Gateway authentication mechanisms. After a design review, a solutions architect identifies a set of APIs that do not require public access. The solutions architect must design a solution to make the set of APIs accessible only from a VPC. All APIs need to be called with an authenticated user. Which solution will meet these requirements with the LEAST amount of effort?

- A. Create an internal Application Load Balancer (ALB). Create a target group.
- B. Select the Lambda function to call.
- C. Use the ALB DNS name to call the API from the VPC.
- D. Remove the DNS entry that is associated with the API in API Gateway.
- E. Create a hosted zone in Amazon Route 53. Create a CNAME record in the hosted zone.
- F. Update the API in API Gateway with the CNAME record.
- G. Use the CNAME record to call the API from the VPC.
- H. Update the API endpoint from Regional to private in API Gateway.
- I. Create an interface VPC endpoint in the VPC.
- J. Create a resource policy, and attach it to the API.
- K. Use the VPC endpoint to call the API from the VPC.
- L. Deploy the Lambda functions inside the VPC.
- M. Provision an EC2 instance, and install an Apache server. From the Apache server, call the Lambda function.
- N. Use the internal CNAME record of the EC2 instance to call the API from the VPC.

**Answer:** C

**Explanation:**

This solution requires the least amount of effort as it only requires to update the API endpoint to private in API Gateway and create an interface VPC endpoint. Then create a resource policy and attach it to the API. This will make the API only accessible from the VPC and still keep the authentication mechanism intact.

Reference:

➤ <https://aws.amazon.com/api-gateway/features/>

**NEW QUESTION 20**

- (Exam Topic 1)

A security engineer determined that an existing application retrieves credentials to an Amazon RDS for MySQL database from an encrypted file in Amazon S3. For the next version of the application, the security engineer wants to implement the following application design changes to improve security:

- The database must use strong, randomly generated passwords stored in a secure AWS managed service.
- The application resources must be deployed through AWS CloudFormation.
- The application must rotate credentials for the database every 90 days.

A solutions architect will generate a CloudFormation template to deploy the application.

Which resources specified in the CloudFormation template will meet the security engineer's requirements with the LEAST amount of operational overhead?

- A. Generate the database password as a secret resource using AWS Secrets Manager
- B. Create an AWS Lambda function resource to rotate the database password
- C. Specify a Secrets Manager RotationSchedule resource to rotate the database password every 90 days.
- D. Generate the database password as a SecureString parameter type using AWS Systems Manager Parameter Store
- E. Create an AWS Lambda function resource to rotate the database password
- F. Specify a Parameter Store RotationSchedule resource to rotate the database password every 90 days.
- G. Generate the database password as a secret resource using AWS Secrets Manager
- H. Create an AWS Lambda function resource to rotate the database password
- I. Create an Amazon EventBridge scheduled rule resource to trigger the Lambda function password rotation every 90 days.
- J. Generate the database password as a SecureString parameter type using AWS Systems Manager Parameter Store
- K. Specify an AWS AppSync DataSource resource to automatically rotate the database password every 90 days.

**Answer: B**

**Explanation:**

<https://aws.amazon.com/blogs/security/how-to-securely-provide-database-credentials-to-lambda-functions-by-us>

<https://docs.aws.amazon.com/secretsmanager/latest/userguide/rotating-secrets.html>

[https://docs.aws.amazon.com/secretsmanager/latest/userguide/integrating\\_cloudformation.html](https://docs.aws.amazon.com/secretsmanager/latest/userguide/integrating_cloudformation.html)

**NEW QUESTION 22**

- (Exam Topic 1)

A retail company is hosting an ecommerce website on AWS across multiple AWS Regions. The company wants the website to be operational at all times for online purchases. The website stores data in an Amazon RDS for MySQL DB instance.

Which solution will provide the HIGHEST availability for the database?

- A. Configure automated backups on Amazon RDS
- B. In the case of disruption, promote an automated backup to be a standalone DB instance
- C. Direct database traffic to the promoted DB instance
- D. Create a replacement read replica that has the promoted DB instance as its source.
- E. Configure global tables and read replicas on Amazon RDS
- F. Activate the cross-Region scope
- G. In the case of disruption, use AWS Lambda to copy the read replicas from one Region to another Region.
- H. Configure global tables and automated backups on Amazon RDS
- I. In the case of disruption, use AWS Lambda to copy the read replicas from one Region to another Region.
- J. Configure read replicas on Amazon RDS
- K. In the case of disruption, promote a cross-Region read replica to be a standalone DB instance
- L. Direct database traffic to the promoted DB instance
- M. Create a replacement read replica that has the promoted DB instance as its source.

**Answer: D**

**Explanation:**

This solution will provide the highest availability for the database, as the read replicas will allow the database to be available in multiple Regions, thus reducing the chances of disruption. Additionally, the promotion of the cross-Region read replica to become a standalone DB instance will ensure that the database is still available even if one of the Regions experiences disruptions.

**NEW QUESTION 24**

- (Exam Topic 1)

A company uses Amazon S3 to store files and images in a variety of storage classes. The company's S3 costs have increased substantially during the past year.

A solutions architect needs to review data trends for the past 12 months and identify the appropriate storage class for the objects.

Which solution will meet these requirements?

- A. Download AWS Cost and Usage Reports for the last 12 months of S3 usage
- B. Review AWS Trusted Advisor recommendations for cost savings.
- C. Use S3 storage class analysis
- D. Import data trends into an Amazon QuickSight dashboard to analyze storage trends.
- E. Use Amazon S3 Storage Lens
- F. Upgrade the default dashboard to include advanced metrics for storage trends.
- G. Use Access Analyzer for S3. Download the Access Analyzer for S3 report for the last 12 months
- H. Import the csv file to an Amazon QuickSight dashboard.

**Answer: B**

**Explanation:**

[https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage\\_lens.html](https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage_lens.html)

**NEW QUESTION 27**

- (Exam Topic 1)

A company developed a pilot application by using AWS Elastic Beanstalk and Java. To save costs during development, the company's development team



deployed the application into a single-instance environment. Recent tests indicate that the application consumes more CPU than expected. CPU utilization is regularly greater than 85%, which causes some performance bottlenecks.

A solutions architect must mitigate the performance issues before the company launches the application to production.

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

- A. Create a new Elastic Beanstalk applicatio
- B. Select a load-balanced environment typ
- C. Select all Availability Zone
- D. Add a scale-out rule that will run if the maximum CPU utilization is over 85% for 5 minutes.
- E. Create a second Elastic Beanstalk environmen
- F. Apply the traffic-splitting deployment polic
- G. Specify a percentage of incoming traffic to direct to the new environment in the average CPU utilization is over 85% for 5 minutes.
- H. Modify the existing environment's capacity configuration to use a load-balanced environment type.Select all Availability Zone
- I. Add a scale-out rule that will run if the average CPU utilization is over 85% for 5 minutes.
- J. Select the Rebuild environment action with the load balancing option Select an Availability Zones Add a scale-out rule that will run if the sum CPU utilization is over 85% for 5 minutes.

**Answer: C**

**Explanation:**

This solution will meet the requirements with the least operational overhead because it allows the company to modify the existing environment's capacity configuration, so it becomes a load-balanced environment type. By selecting all availability zones, the company can ensure that the application is running in multiple availability zones, which can help to improve the availability and scalability of the application. The company can also add a scale-out rule that will run if the average CPU utilization is over 85% for 5 minutes, which can help to mitigate the performance issues. This solution does not require creating new Elastic Beanstalk environments or rebuilding the existing one, which reduces the operational overhead.

You can refer to the AWS Elastic Beanstalk documentation for more information on how to use this service: <https://aws.amazon.com/elasticbeanstalk/> You can refer to the AWS documentation for more information on how to use autoscaling: <https://aws.amazon.com/autoscaling/>

**NEW QUESTION 32**

- (Exam Topic 1)

A company is subject to regulatory audits of its financial information. External auditors who use a single AWS account need access to the company's AWS account. A solutions architect must provide the auditors with secure, read-only access to the company's AWS account. The solution must comply with AWS security best practices.

Which solution will meet these requirements?

- A. In the company's AWS account, create resource policies for all resources in the account to grant access to the auditors' AWS accoun
- B. Assign a unique external ID to the resource policy.
- C. In the company's AWS account create an IAM role that trusts the auditors' AWS account Create an IAM policy that has the required permission
- D. Attach the policy to the rol
- E. Assign a unique external ID to the role's trust policy.
- F. In the company's AWS account, create an IAM use
- G. Attach the required IAM policies to the IAM user.Create API access keys for the IAM use
- H. Share the access keys with the auditors.
- I. In the company's AWS account, create an IAM group that has the required permissions Create an IAM user in the company s account for each audito
- J. Add the IAM users to the IAM group.

**Answer: B**

**Explanation:**

This solution will allow the external auditors to have read-only access to the company's AWS account while being compliant with AWS security best practices. By creating an IAM role, which is a secure and flexible way of granting access to AWS resources, and trusting the auditors' AWS account, the company can ensure that the auditors only have the permissions that are required for their role and nothing more. Assigning a unique external ID to the role's trust policy, it will ensure that only the auditors' AWS account can assume the role.

Reference:

AWS IAM Roles documentation: <https://aws.amazon.com/iam/features/roles/> AWS IAM Best practices: <https://aws.amazon.com/iam/security-best-practices/>

**NEW QUESTION 37**

- (Exam Topic 1)

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 protoco
- B. Grant access to the AWS accounts by using attribute-based access controls (ABACs).
- C. Configure AWS Single Sign-On (AWS SSO) by using AWS SSO as an identity sourc
- D. Enable automatic provisioning by using the System for Cross-domain Identity Management (SCIM) v2.0 protoco
- E. Grant access to the AWS accounts by using AWS SSO permission sets.
- F. In one of the company's AWS accounts, configure AWS Identity and Access Management (IAM) to use a SAML 2.0 identity provide
- G. Provision IAM users that are mapped to the federated user
- H. Grant access that corresponds to appropriate groups in Active Director
- I. Grant access to the required AWS accounts by using cross-account IAM users.
- J. In one of the company's AWS accounts, configure AWS Identity and Access Management (IAM) to use an OpenID Connect (OIDC) identity provide
- K. Provision IAM roles that grant access to the AWS account for the federated users that correspond to appropriate groups in Active Director
- L. Grant access to the required AWS accounts by using cross-account IAM roles.

**Answer: D**

**Explanation:**



<https://aws.amazon.com/blogs/aws/new-attributes-based-access-control-with-aws-single-sign-on/>

#### NEW QUESTION 42

- (Exam Topic 1)

A company has developed a web application. The company is hosting the application on a group of Amazon EC2 instances behind an Application Load Balancer. The company wants to improve the security posture of the application and plans to use AWS WAF web ACLs. The solution must not adversely affect legitimate traffic to the application.

How should a solutions architect configure the web ACLs to meet these requirements?

- A. Set the action of the web ACL rules to Count
- B. Enable AWS WAF logging Analyze the requests for false positives Modify the rules to avoid any false positive Over time change the action of the web ACL rules from Count to Block.
- C. Use only rate-based rules in the web ACL
- D. and set the throttle limit as high as possible Temporarily block all requests that exceed the limit
- E. Define nested rules to narrow the scope of the rate tracking.
- F. Set the action of the web ACL rules to Block
- G. Use only AWS managed rule groups in the web ACLs Evaluate the rule groups by using Amazon CloudWatch metrics with AWS WAF sampled requests or AWS WAF logs.
- H. Use only custom rule groups in the web ACL
- I. and set the action to Allow Enable AWS WAF logging Analyze the requests for false positives Modify the rules to avoid any false positive Over time, change the action of the web ACL rules from Allow to Block.

**Answer:** A

#### Explanation:

<https://aws.amazon.com/premiumsupport/knowledge-center/waf-analyze-count-action-rules/>

#### NEW QUESTION 46

- (Exam Topic 1)

A company runs its application in the eu-west-1 Region and has one account for each of its environments development, testing, and production All the environments are running 24 hours a day 7 days a week by using stateful Amazon EC2 instances and Amazon RDS for MySQL databases The databases are between 500 GB and 800 GB in size

The development team and testing team work on business days during business hours, but the production environment operates 24 hours a day. 7 days a week. The company wants to reduce costs All resources are tagged with an environment tag with either development, testing, or production as the key. What should a solutions architect do to reduce costs with the LEAST operational effort?

- A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that runs once every day Configure the rule to invoke one AWS Lambda function that starts or stops instances based on the tag day and time.
- B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that runs every business day in the evening
- C. Configure the rule to invoke an AWS Lambda function that stops instances based on the tag Create a second EventBridge (CloudWatch Events) rule that runs every business day in the morning Configure the second rule to invoke another Lambda function that starts instances based on the tag
- D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that runs every business day in the evening Configure the rule to invoke an AWS Lambda function that terminates instances based on the tag Create a second EventBridge (CloudWatch Events) rule that runs every business day in the morning Configure the second rule to invoke another Lambda function that restores the instances from their last backup based on the tag.
- E. Create an Amazon EventBridge rule that runs every hour
- F. Configure the rule to invoke one AWS Lambda function that terminates or restores instances from their last backup based on the tag
- G. day, and time.

**Answer:** B

#### Explanation:

Creating an Amazon EventBridge rule that runs every business day in the evening to stop instances and another rule that runs every business day in the morning to start instances based on the tag will reduce costs with the least operational effort. This approach allows for instances to be stopped during non-business hours when they are not in use, reducing the costs associated with running them. It also allows for instances to be started again in the morning when the development and testing teams need to use them.

#### NEW QUESTION 49

- (Exam Topic 1)

A company is in the process of implementing AWS Organizations to constrain its developers to use only Amazon EC2. Amazon S3 and Amazon DynamoDB. The developers account resides in a dedicated organizational unit (OU). The solutions architect has implemented the following SCP on the developers account:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowEC2",
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*"
    },
    {
      "Sid": "AllowDynamoDB",
      "Effect": "Allow",
      "Action": "dynamodb:*",
      "Resource": "*"
    },
    {
      "Sid": "AllowS3",
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

When this policy is deployed, IAM users in the developers account are still able to use AWS services that are not listed in the policy. What should the solutions architect do to eliminate the developers' ability to use services outside the scope of this policy?

- A. Create an explicit deny statement for each AWS service that should be constrained
- B. Remove the Full AWS Access SCP from the developer account's OU
- C. Modify the Full AWS Access SCP to explicitly deny all services
- D. Add an explicit deny statement using a wildcard to the end of the SCP

**Answer: B**

**Explanation:**

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_inheritance\\_auth.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_inheritance_auth.html)

**NEW QUESTION 50**

- (Exam Topic 1)

A company is hosting a monolithic REST-based API for a mobile app on five Amazon EC2 instances in public subnets of a VPC. Mobile clients connect to the API by using a domain name that is hosted on Amazon Route 53. The company has created a Route 53 multivalue answer routing policy with the IP addresses of all the EC2 instances. Recently, the app has been overwhelmed by large and sudden increases to traffic. The app has not been able to keep up with the traffic. A solutions architect needs to implement a solution so that the app can handle the new and varying load. Which solution will meet these requirements with the LEAST operational overhead?

- A. Separate the API into individual AWS Lambda function
- B. Configure an Amazon API Gateway REST API with Lambda integration for the backen
- C. Update the Route 53 record to point to the API Gateway API.
- D. Containerize the API logi
- E. Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluste
- F. Run the containers in the cluster by using Amazon EC2. Create a Kubernetes ingres
- G. Update the Route 53 record to point to the Kubernetes ingress.
- H. Create an Auto Scaling grou
- I. Place all the EC2 instances in the Auto Scaling grou
- J. Configure the Auto Scaling group to perform scaling actions that are based on CPU utilizatio
- K. Create an AWS Lambda function that reacts to Auto Scaling group changes and updates the Route 53 record.
- L. Create an Application Load Balancer (ALB) in front of the AP
- M. Move the EC2 instances to private subnets in the VP
- N. Add the EC2 instances as targets for the AL
- O. Update the Route 53 record to point to the ALB.

**Answer: D**

**Explanation:**

By breaking down the monolithic API into individual Lambda functions and using API Gateway to handle the incoming requests, the solution can automatically scale to handle the new and varying load without the need for manual scaling actions. Additionally, this option will automatically handle the traffic without the need of having EC2 instances running all the time and only pay for the number of requests and the duration of the execution of the Lambda function.

By updating the Route 53 record to point to the API Gateway, the solution can handle the traffic and also it will direct the traffic to the correct endpoint.

**NEW QUESTION 51**

- (Exam Topic 1)

A company is using multiple AWS accounts The DNS records are stored in a private hosted zone for Amazon Route 53 in Account A The company's applications and databases are running in Account B.

A solutions architect win deploy a two-net application In a new VPC To simplify the configuration, the db.example com CNAME record set tor the Amazon RDS endpoint was created in a private hosted zone for Amazon Route 53.

During deployment, the application failed to start. Troubleshooting revealed that db.example.com is not resolvable on the Amazon EC2 instance. The solutions architect confirmed that the record set was created correctly in Route 53.

Which combination of steps should the solutions architect take to resolve this issue? (Select TWO)

- A. Deploy the database on a separate EC2 instance in the new VPC. Create a record set for the instance's private IP in the private hosted zone.
- B. Use SSH to connect to the application tier EC2 instance. Add an RDS endpoint IP address to the /etc/resolv.conf file.
- C. Create an authorization to associate the private hosted zone in Account A with the new VPC in Account B.
- D. Create a private hosted zone for the example.com domain in Account B. Configure Route 53 replication between AWS accounts.
- E. Associate a new VPC in Account B with a hosted zone in Account A.
- F. Delete the association authorization in Account A.

**Answer:** CE

**Explanation:**

<https://aws.amazon.com/premiumsupport/knowledge-center/private-hosted-zone-different-account/>

#### NEW QUESTION 56

- (Exam Topic 1)

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.
- B. Delete the existing private virtual interface from the existing connection.
- C. Create the second Direct Connect connection.
- D. Create a new private virtual interface on each connection, and connect both private virtual interfaces to the Direct Connect gateway.
- E. Connect the Direct Connect gateway to the single VPC.
- F. Keep the existing private virtual interface.
- G. Create the second Direct Connect connection.
- H. Create a new private virtual interface on the new connection, and connect the new private virtual interface to the single VPC.
- I. Keep the existing private virtual interface.
- J. Create the second Direct Connect connection.
- K. Create a new public virtual interface on the new connection, and connect the new public virtual interface to the single VPC.
- L. Provision a transit gateway.
- M. Delete the existing private virtual interface from the existing connection. Create the second Direct Connect connection.
- N. Create a new private virtual interface on each connection, and connect both private virtual interfaces to the transit gateway.
- O. Associate the transit gateway with the single VPC.

**Answer:** A

**Explanation:**

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.

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

#### NEW QUESTION 57

- (Exam Topic 1)

A company has its cloud infrastructure on AWS. A solutions architect needs to define the infrastructure as code. The infrastructure is currently deployed in one AWS Region. The company's business expansion plan includes deployments in multiple Regions across multiple AWS accounts.

What should the solutions architect do to meet these requirements?

- A. Use AWS CloudFormation templates. Add IAM policies to control the various accounts. Deploy the templates across the multiple Regions.
- B. Use AWS Organizations. Deploy AWS CloudFormation templates from the management account. Use AWS Control Tower to manage deployments across accounts.
- C. Use AWS Organizations and AWS CloudFormation StackSets. Deploy a CloudFormation template from an account that has the necessary IAM permissions.
- D. Use nested stacks with AWS CloudFormation templates. Change the Region by using nested stacks.

**Answer:** C

**Explanation:**

<https://aws.amazon.com/blogs/aws/new-use-aws-cloudformation-stacksets-for-multiple-accounts-in-an-aws-org/> AWS Organizations allows the management of multiple AWS accounts as a single entity and AWS

CloudFormation StackSets allows creating, updating, and deleting stacks across multiple accounts and regions in an organization. This solution allows creating a single CloudFormation template that can be deployed across multiple accounts and regions, and also allows for the management of access and permissions for the different accounts through the use of IAM roles and policies in the management account.

#### NEW QUESTION 59

- (Exam Topic 1)

A company built an application based on AWS Lambda deployed in an AWS CloudFormation stack. The last production release of the web application introduced an issue that resulted in an outage lasting several minutes. A solutions architect must adjust the deployment process to support a canary release.

Which solution will meet these requirements?

- A. Create an alias for every new deployed version of the Lambda function.
- B. Use the AWS CLI update-alias command with the routing-config parameter to distribute the load.
- C. Deploy the application into a new CloudFormation stack.
- D. Use an Amazon Route 53 weighted routing policy to distribute the load.
- E. Create a version for every new deployed Lambda function.
- F. Use the AWS CLI update-function-configuration command with the routing-config parameter to distribute the load.



G. Configure AWS CodeDeploy and use CodeDeployDefault.OneAtATime in the Deployment configuration to distribute the load.

**Answer:** A

**Explanation:**

<https://aws.amazon.com/blogs/compute/implementing-canary-deployments-of-aws-lambda-functions-with-alias->  
<https://docs.aws.amazon.com/lambda/latest/dg/configuration-aliases.html>

**NEW QUESTION 63**

- (Exam Topic 1)

A retail company is operating its ecommerce application on AWS. The application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The company uses an Amazon RDS DB instance as the database backend. Amazon CloudFront is configured with one origin that points to the ALB. Static content is cached. Amazon Route 53 is used to host all public zones.

After an update of the application, the ALB occasionally returns a 502 status code (Bad Gateway) error. The root cause is malformed HTTP headers that are returned to the ALB. The webpage returns successfully when a solutions architect reloads the webpage immediately after the error occurs.

While the company is working on the problem, the solutions architect needs to provide a custom error page instead of the standard ALB error page to visitors. Which combination of steps will meet this requirement with the LEAST amount of operational overhead? (Choose two.)

- A. Create an Amazon S3 bucket
- B. Configure the S3 bucket to host a static webpage
- C. Upload the custom error pages to Amazon S3.
- D. Create an Amazon CloudWatch alarm to invoke an AWS Lambda function if the ALB health check response Target.FailedHealthChecks is greater than 0. Configure the Lambda function to modify the forwarding rule at the ALB to point to a publicly accessible web server.
- E. Modify the existing Amazon Route 53 records by adding health check
- F. Configure a fallback target if the health check fails
- G. Modify DNS records to point to a publicly accessible webpage.
- H. Create an Amazon CloudWatch alarm to invoke an AWS Lambda function if the ALB health check response Elb.InternalError is greater than 0. Configure the Lambda function to modify the forwarding rule at the ALB to point to a public accessible web server.
- I. Add a custom error response by configuring a CloudFront custom error page
- J. Modify DNS records to point to a publicly accessible web page.

**Answer:** CE

**Explanation:**

"Save your custom error pages in a location that is accessible to CloudFront. We recommend that you store them in an Amazon S3 bucket, and that you don't store them in the same place as the rest of your website or application's content. If you store the custom error pages on the same origin as your website or application, and the origin starts to return 5xx errors, CloudFront can't get the custom error pages because the origin server is unavailable."

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/GeneratingCustomErrorResponses.htm>

**NEW QUESTION 67**

- (Exam Topic 1)

A solutions architect needs to implement a client-side encryption mechanism for objects that will be stored in a new Amazon S3 bucket. The solutions architect created a CMK that is stored in AWS Key Management Service (AWS KMS) for this purpose.

The solutions architect created the following IAM policy and attached it to an IAM role:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DownloadUpload",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::BucketName/*"
    },
    {
      "Sid": "KMSAccess",
      "Action": [
        "kms:Decrypt",
        "kms:Encrypt"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:kms:us-east-1:123456789012:key/*"
    }
  ]
}
```

During tests, the solutions architect was able to successfully get existing test objects in the S3 bucket. However, attempts to upload a new object resulted in an error message. The error message stated that the action was forbidden.

Which action must the solutions architect add to the IAM policy to meet all the requirements?

- A. kms:GenerateDataKey
- B. kms:GetKeyPolicy
- C. kms:GetPublicKey
- D. kms:Sign

**Answer:** A

**Explanation:**

<https://aws.amazon.com/premiumsupport/knowledge-center/s3-access-denied-error-kms/>

"An error occurred (AccessDenied) when calling the PutObject operation: Access Denied" This error message indicates that your IAM user or role needs

permission for the kms:GenerateDataKey action.

#### NEW QUESTION 68

- (Exam Topic 1)

A company with several AWS accounts is using AWS Organizations and service control policies (SCPs). An Administrator created the following SCP and has attached it to an organizational unit (OU) that contains AWS account 1111-1111-1111:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowsAllActions",
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    },
    {
      "Sid": "DenyCloudTrail",
      "Effect": "Deny",
      "Action": "cloudtrail:*",
      "Resource": "*"
    }
  ]
}
```

Developers working in account 1111-1111-1111 complain that they cannot create Amazon S3 buckets. How should the Administrator address this problem?

- A. Add s3:CreateBucket with `Allow` effect to the SCP.
- B. Remove the account from the OU, and attach the SCP directly to account 1111-1111-1111.
- C. Instruct the Developers to add Amazon S3 permissions to their IAM entities.
- D. Remove the SCP from account 1111-1111-1111.

**Answer: C**

#### Explanation:

However A's explanation is incorrect - [https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scps.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html)

"SCPs are similar to AWS Identity and Access Management (IAM) permission policies and use almost the same syntax. However, an SCP never grants permissions."

SCPs alone are not sufficient to granting permissions to the accounts in your organization. No permissions are granted by an SCP. An SCP defines a guardrail, or sets limits, on the actions that the account's administrator can delegate to the IAM users and roles in the affected accounts. The administrator must still attach identity-based or resource-based policies to IAM users or roles, or to the resources in your accounts to actually grant permissions. The effective permissions are the logical intersection between what is allowed by the SCP and what is allowed by the IAM and resource-based policies.

#### NEW QUESTION 69

- (Exam Topic 1)

A financial company is planning to migrate its web application from on premises to AWS. The company uses a third-party security tool to monitor the inbound traffic to the application. The company has used the security tool for the last 15 years, and the tool has no cloud solutions available from its vendor. The company's security team is concerned about how to integrate the security tool with AWS technology.

The company plans to deploy the application migration to AWS on Amazon EC2 instances. The EC2 instances will run in an Auto Scaling group in a dedicated VPC. The company needs to use the security tool to inspect all packets that come in and out of the VPC. This inspection must occur in real time and must not affect the application's performance. A solutions architect must design a target architecture on AWS that is highly available within an AWS Region.

Which combination of steps should the solutions architect take to meet these requirements? (Select TWO.)

- A. Deploy the security tool on EC2 instances in a new Auto Scaling group in the existing VPC.
- B. Deploy the web application behind a Network Load Balancer.
- C. Deploy an Application Load Balancer in front of the security tool instances.
- D. Provision a Gateway Load Balancer for each Availability Zone to redirect the traffic to the security tool.
- E. Provision a transit gateway to facilitate communication between VPCs.

**Answer: AD**

#### Explanation:

Option A, Deploy the security tool on EC2 instances in a new Auto Scaling group in the existing VPC, allows the company to use its existing security tool while still running it within the AWS environment. This ensures that all packets coming in and out of the VPC are inspected by the security tool in real time. Option D, Provision a Gateway Load Balancer for each Availability Zone to redirect the traffic to the security tool, allows for high availability within an AWS Region. By provisioning a Gateway Load Balancer for each Availability Zone, the traffic is redirected to the security tool in the event of any failures or outages. This ensures that the security tool is always available to inspect the traffic, even in the event of a failure.

#### NEW QUESTION 73

- (Exam Topic 1)

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 main 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 main AWS account Establish connectivity between the Client VPN endpoint and the AWS Site-to-Site VPN

**Answer:** C

**Explanation:**

<https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/scenario-peered.html>

**NEW QUESTION 74**

- (Exam Topic 1)

A solutions architect is designing the data storage and retrieval architecture for a new application that a company will be launching soon. The application is designed to ingest millions of small records per minute from devices all around the world. Each record is less than 4 KB in size and needs to be stored in a durable location where it can be retrieved with low latency. The data is ephemeral and the company is required to store the data for 120 days only, after which the data can be deleted.

The solutions architect calculates that, during the course of a year, the storage requirements would be about 10-15 TB.

Which storage strategy is the MOST cost-effective and meets the design requirements?

- A. Design the application to store each incoming record as a single .csv file in an Amazon S3 bucket to allow for indexed retrieval
- B. Configure a lifecycle policy to delete data older than 120 days.
- C. Design the application to store each incoming record in an Amazon DynamoDB table properly configured for the scale
- D. Configure the DynamoDB Time to Live (TTL) feature to delete records older than 120 days.
- E. Design the application to store each incoming record in a single table in an Amazon RDS MySQL database
- F. Run a nightly cron job that executes a query to delete any records older than 120 days.
- G. Design the application to batch incoming records before writing them to an Amazon S3 bucket
- H. Update the metadata for the object to contain the list of records in the batch and use the Amazon S3 metadata search feature to retrieve the data
- I. Configure a lifecycle policy to delete the data after 120 days.

**Answer:** B

**Explanation:**

DynamoDB with TTL, cheaper for sustained throughput of small items + suited for fast retrievals. S3 cheaper for storage only, much higher costs with writes. RDS not designed for this use case.

**NEW QUESTION 75**

- (Exam Topic 1)

A company has registered 10 new domain names. The company uses the domains for online marketing. The company needs a solution that will redirect online visitors to a specific URL for each domain. All domains and target URLs are defined in a JSON document. All DNS records are managed by Amazon Route 53. A solutions architect must implement a redirect service that accepts HTTP and HTTPS requests.

Which combination of steps should the solutions architect take to meet these requirements with the LEAST amount of operational effort? (Choose three.)

- A. Create a dynamic webpage that runs on an Amazon EC2 instance
- B. Configure the webpage to use the JSON document in combination with the event message to look up and respond with a redirect URL.
- C. Create an Application Load Balancer that includes HTTP and HTTPS listeners.
- D. Create an AWS Lambda function that uses the JSON document in combination with the event message to look up and respond with a redirect URL.
- E. Use an Amazon API Gateway API with a custom domain to publish an AWS Lambda function.
- F. Create an Amazon CloudFront distribution
- G. Deploy a Lambda@Edge function.
- H. Create an SSL certificate by using AWS Certificate Manager (ACM). Include the domains as Subject Alternative Names.

**Answer:** CEF

**Explanation:**

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-edge-how-it-works-tutorial.html>

**NEW QUESTION 77**

- (Exam Topic 1)

The company needs to determine which costs on the monthly AWS bill are attributable to each application or team. The company also must be able to create reports to compare costs from the last 12 months and to help forecast costs for the next 12 months. A solutions architect must recommend an AWS Billing and Cost Management solution that provides these cost reports.

Which combination of actions will meet these requirements? (Select THREE.)

- A. Activate the user-defined cost allocation tags that represent the application and the team.
- B. Activate the AWS generated cost allocation tags that represent the application and the team.
- C. Create a cost category for each application in Billing and Cost Management.
- D. Activate IAM access to Billing and Cost Management.
- E. Create a cost budget.
- F. Enable Cost Explorer.

**Answer:** ACF

**Explanation:**

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/manage-cost-categories.html> <https://aws.amazon.com/premiumsupport/knowledge-center/cost-explorer-analyze-spending-and-usage/> <https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/manage-cost-categories.html>  
<https://docs.aws.amazon.com/cost-management/latest/userguide/ce-enable.html>

The best combination of actions to meet the company's requirements is Options A, C, and F.

Option A involves activating the user-defined cost allocation tags that represent the application and the team. This will allow the company to assign costs to different applications or teams, and will allow them to be tracked in the monthly AWS bill.



Option C involves creating a cost category for each application in Billing and Cost Management. This will allow the company to easily identify and compare costs across different applications and teams.

Option F involves enabling Cost Explorer. This will allow the company to view the costs of their AWS resources over the last 12 months and to create forecasts for the next 12 months.

These recommendations are in line with the official Amazon Textbook and Resources for the AWS Certified Solutions Architect - Professional certification. In particular, the book states that "You can use cost allocation tags to group your costs by application, team, or other categories" (Source: [https://d1.awsstatic.com/training-and-certification/docs-sa-pro/AWS\\_Certified\\_Solutions\\_Architect\\_Professiona](https://d1.awsstatic.com/training-and-certification/docs-sa-pro/AWS_Certified_Solutions_Architect_Professiona)). Additionally, the book states that "Cost Explorer enables you to view the costs of your AWS resources over the last 12 months and to create forecasts for the next 12 months" (Source: [https://d1.awsstatic.com/training-and-certification/docs-sa-pro/AWS\\_Certified\\_Solutions\\_Architect\\_Professiona](https://d1.awsstatic.com/training-and-certification/docs-sa-pro/AWS_Certified_Solutions_Architect_Professiona)).

**NEW QUESTION 81**

- (Exam Topic 1)

A weather service provides high-resolution weather maps from a web application hosted on AWS in the eu-west-1 Region. The weather maps are updated frequently and stored in Amazon S3 along with static HTML content. The web application is fronted by Amazon CloudFront.

The company recently expanded to serve users in the us-east-1 Region, and these new users report that viewing their respective weather maps is slow from time to time.

Which combination of steps will resolve the us-east-1 performance issues? (Choose two.)

- A. Configure the AWS Global Accelerator endpoint for the S3 bucket in eu-west-1. Configure endpoint groups for TCP ports 80 and 443 in us-east-1.
- B. Create a new S3 bucket in us-east-1. Configure S3 cross-Region replication to synchronize from the S3 bucket in eu-west-1.
- C. Use Lambda@Edge to modify requests from North America to use the S3 Transfer Acceleration endpoint in us-east-1.
- D. Use Lambda@Edge to modify requests from North America to use the S3 bucket in us-east-1.
- E. Configure the AWS Global Accelerator endpoint for us-east-1 as an origin on the CloudFront distributio
- F. Use Lambda@Edge to modify requests from North America to use the new origin.

**Answer: BD**

**Explanation:**

<https://aws.amazon.com/about-aws/whats-new/2016/04/transfer-files-into-amazon-s3-up-to-300-percent-faster/>

**NEW QUESTION 84**

- (Exam Topic 1)

A company has hundreds of AWS accounts. The company recently implemented a centralized internal process for purchasing new Reserved Instances and modifying existing Reserved Instances. This process requires all business units that want to purchase or modify Reserved Instances to submit requests to a dedicated team for procurement. Previously, business units directly purchased or modified Reserved Instances in their own respective AWS accounts autonomously.

A solutions architect needs to enforce the new process in the most secure way possible.

Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)

- A. Ensure that all AWS accounts are part of an organization in AWS Organizations with all features enabled.
- B. Use AWS Config to report on the attachment of an IAM policy that denies access to the ec2:PurchaseReservedInstancesOffering action and the ec2:ModifyReservedInstances action.
- C. In each AWS account, create an IAM policy that denies the ec2:PurchaseReservedInstancesOffering action and the ec2:ModifyReservedInstances action.
- D. Create an SCP that denies the ec2:PurchaseReservedInstancesOffering action and the ec2:ModifyReservedInstances actio
- E. Attach the SCP to each OU of the organization.
- F. Ensure that all AWS accounts are part of an organization in AWS Organizations that uses the consolidated billing feature.

**Answer: AD**

**Explanation:**

All features – The default feature set that is available to AWS Organizations. It includes all the functionality of consolidated billing, plus advanced features that give you more control over accounts in your organization. For example, when all features are enabled the management account of the organization has full control over what member accounts can do. The management account can apply SCPs to restrict the services and actions that users (including the root user) and roles in an account can access. [https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_getting-started\\_concepts.html#feature-set](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html#feature-set)

**NEW QUESTION 86**

- (Exam Topic 1)

A company has an organization in AWS Organizations. The company is using AWS Control Tower to deploy a landing zone for the organization. The company wants to implement governance and policy enforcement. The company must implement a policy that will detect Amazon RDS DB instances that are not encrypted at rest in the company's production OU.

Which solution will meet this requirement?

- A. Turn on mandatory guardrails in AWS Control Towe
- B. Apply the mandatory guardrails to the production OU.
- C. Enable the appropriate guardrail from the list of strongly recommended guardrails in AWS Control Towe
- D. Apply the guardrail to the production OU.
- E. Use AWS Config to create a new mandatory guardrai
- F. Apply the rule to all accounts in the production OU.
- G. Create a custom SCP in AWS Control Towe
- H. Apply the SCP to the production OU.

**Answer: B**

**Explanation:**

AWS Control Tower provides a set of "strongly recommended guardrails" that can be enabled to implement governance and policy enforcement. One of these guardrails is "Encrypt Amazon RDS instances" which will detect RDS DB instances that are not encrypted at rest. By enabling this guardrail and applying it to the production OU, the company will be able to enforce encryption for RDS instances in the production environment.

**NEW QUESTION 88**

- (Exam Topic 1)

A global media company is planning a multi-Region deployment of an application. Amazon DynamoDB global tables will back the deployment to keep the user experience consistent across the two continents where users are concentrated. Each deployment will have a public Application Load Balancer (ALB). The company manages public DNS internally. The company wants to make the application available through an apex domain. Which solution will meet these requirements with the LEAST effort?

- A. Migrate public DNS to Amazon Route 53. Create CNAME records for the apex domain to point to the AL
- B. Use a geolocation routing policy to route traffic based on user location.
- C. Place a Network Load Balancer (NLB) in front of the AL
- D. Migrate public DNS to Amazon Route 53. Create a CNAME record for the apex domain to point to the NLB's static IP address
- E. Use a geolocation routing policy to route traffic based on user location.
- F. Create an AWS Global Accelerator accelerator with multiple endpoint groups that target endpoints in appropriate AWS Region
- G. Use the accelerator's static IP address to create a record in public DNS for the apex domain.
- H. Create an Amazon API Gateway API that is backed by AWS Lambda in one of the AWS Regions. Configure a Lambda function to route traffic to application deployments by using the round robin method
- I. Create CNAME records for the apex domain to point to the API's URL.

**Answer: C**

**Explanation:**

AWS Global Accelerator is a service that directs traffic to optimal endpoints (in this case, the Application Load Balancer) based on the health of the endpoints and network routing. It allows you to create an accelerator that directs traffic to multiple endpoint groups, one for each Region where the application is deployed. The accelerator uses the AWS global network to optimize the traffic routing to the healthy endpoint.

By using Global Accelerator, the company can use a single static IP address for the apex domain, and traffic will be directed to the optimal endpoint based on the user's location, without the need for additional load balancers or routing policies.

Reference:

AWS Global Accelerator documentation: <https://aws.amazon.com/global-accelerator/Routing-User-Traffic-to-the-Optimal-AWS-Region-using-Global-Accelerator-documentation/>

<https://aws.amazon.com/blogs/networking-and-content-delivery/routing-user-traffic-to-the-optimal-aws-region-u>

**NEW QUESTION 92**

- (Exam Topic 1)

A company wants to deploy an AWS WAF solution to manage AWS WAF rules across multiple AWS accounts. The accounts are managed under different OUs in AWS Organizations.

Administrators must be able to add or remove accounts or OUs from managed AWS WAF rule sets as needed. Administrators also must have the ability to automatically update and remediate noncompliant AWS WAF rules in all accounts.

Which solution meets these requirements with the LEAST amount of operational overhead?

- A. Use AWS Firewall Manager to manage AWS WAF rules across accounts in the organization
- B. Use an AWS Systems Manager Parameter Store parameter to store account numbers and OUs to manage. Update the parameter as needed to add or remove accounts or OUs. Use an Amazon EventBridge (Amazon CloudWatch Events) rule to identify any changes to the parameter and to invoke an AWS Lambda function to update the security policy in the Firewall Manager administrative account
- C. Deploy an organization-wide AWS Config rule that requires all resources in the selected OUs to associate the AWS WAF rule
- D. Deploy automated remediation actions by using AWS Lambda to fix noncompliant resources. Deploy AWS WAF rules by using an AWS CloudFormation stack set to target the same OUs where the AWS Config rule is applied.
- E. Create AWS WAF rules in the management account of the organization. Use AWS Lambda environment variables to store account numbers and OUs to manage. Update environment variables as needed to add or remove accounts or OUs. Create cross-account IAM roles in member accounts. Assume the roles by using AWS Security Token Service (AWS STS) in the Lambda function to create and update AWS WAF rules in the member accounts.
- F. Use AWS Control Tower to manage AWS WAF rules across accounts in the organization. Use AWS Key Management Service (AWS KMS) to store account numbers and OUs to manage. Update AWS KMS as needed to add or remove accounts or OUs. Create IAM users in member accounts. Allow AWS Control Tower in the management account to use the access key and secret access key to create and update AWS WAF rules in the member accounts.

**Answer: A**

**Explanation:**

<https://aws.amazon.com/solutions/implementations/automations-for-aws-firewall-manager/>

In this solution, AWS Firewall Manager is used to manage AWS WAF rules across accounts in the organization. An AWS Systems Manager Parameter Store parameter is used to store account numbers and OUs to manage. This parameter can be updated as needed to add or remove accounts or OUs. An Amazon EventBridge rule is used to identify any changes to the parameter and to invoke an AWS Lambda function to update the security policy in the Firewall Manager administrative account. This solution allows for easy management of AWS WAF rules across multiple accounts with minimal operational overhead.

**NEW QUESTION 96**

- (Exam Topic 1)

A retail company has structured its AWS accounts to be part of an organization in AWS Organizations. The company has set up consolidated billing and has mapped its departments to the following OUs: Finance, Sales, Human Resources (HR), Marketing, and Operations. Each OU has multiple AWS accounts, one for each environment within a department. These environments are development, test, pre-production, and production.

The HR department is releasing a new system that will launch in 3 months. In preparation, the HR department has purchased several Reserved Instances (RIs) in its production AWS account. The HR department will install the new application on this account. The HR department wants to make sure that other departments cannot share the RI discounts.

Which solution will meet these requirements?

- A. In the AWS Billing and Cost Management console for the HR department's production account, turn off R1 sharing.
- B. Remove the HR department's production AWS account from the organization
- C. Add the account to the consolidating billing configuration only.
- D. In the AWS Billing and Cost Management console, use the organization's management account to turn off R1 sharing for the HR department's production AWS account.
- E. Create an SCP in the organization to restrict access to the RI
- F. Apply the SCP to the OUs of the other departments.

**Answer: C**

**Explanation:**

You can use the management account of the organization in AWS Billing and Cost Management console to turn off RI sharing for the HR department's production AWS account. This will prevent other departments from sharing the RI discounts and ensure that only the HR department can use the RIs purchased in their production account.

**NEW QUESTION 100**

- (Exam Topic 1)

A company runs a proprietary stateless ETL application on an Amazon EC2 Linux instance. The application is a Linux binary, and the source code cannot be modified. The application is single-threaded, uses 2 GB of RAM, and is highly CPU intensive. The application is scheduled to run every 4 hours and runs for up to 20 minutes. A solutions architect wants to revise the architecture for the solution.

Which strategy should the solutions architect use?

- A. Use AWS Lambda to run the application.
- B. Use Amazon CloudWatch Logs to invoke the Lambda function every 4 hours.
- C. Use AWS Batch to run the application.
- D. Use an AWS Step Functions state machine to invoke the AWS Batch job every 4 hours.
- E. Use AWS Fargate to run the application.
- F. Use Amazon EventBridge (Amazon CloudWatch Events) to invoke the Fargate task every 4 hours.
- G. Use Amazon EC2 Spot Instances to run the application.
- H. Use AWS CodeDeploy to deploy and run the application every 4 hours.

**Answer:** C

**Explanation:**

Step function could run a scheduled task when triggered by EventBridge, but why would you add that layer of complexity just to run AWS Batch when you could directly invoke it through EventBridge. The link provided - <https://aws.amazon.com/pt/blogs/compute/orchestrating-high-performance-computing-with-aws-step-functions/> - makes sense only for HPC, this is a single instance that needs to be run.

**NEW QUESTION 103**

- (Exam Topic 1)

A company has deployed an application on AWS Elastic Beanstalk. The application uses Amazon Aurora for the database layer. An Amazon CloudFront distribution serves web requests and includes the Elastic Beanstalk domain name as the origin server. The distribution is configured with an alternate domain name that visitors use when they access the application.

Each week, the company takes the application out of service for routine maintenance. During the time that the application is unavailable, the company wants visitors to receive an informational message instead of a CloudFront error message.

A solutions architect creates an Amazon S3 bucket as the first step in the process.

Which combination of steps should the solutions architect take next to meet the requirements? (Choose three.)

- A. Upload static informational content to the S3 bucket.
- B. Create a new CloudFront distribution.
- C. Set the S3 bucket as the origin.
- D. Set the S3 bucket as a second origin in the original CloudFront distribution.
- E. Configure the distribution and the S3 bucket to use an origin access identity (OAI).
- F. During the weekly maintenance, edit the default cache behavior to use the S3 origin.
- G. Revert the change when the maintenance is complete.
- H. During the weekly maintenance, create a cache behavior for the S3 origin on the new distribution.
- I. Set the path pattern to \. Set the precedence to 0. Delete the cache behavior when the maintenance is complete.
- J. During the weekly maintenance, configure Elastic Beanstalk to serve traffic from the S3 bucket.

**Answer:** ACD

**Explanation:**

The company wants to serve static content from an S3 bucket during the maintenance period. To do this, the following steps are required:

- Upload static informational content to the S3 bucket. This will provide the source of the content that will be served to the visitors.
  - Set the S3 bucket as a second origin in the original CloudFront distribution. Configure the distribution and the S3 bucket to use an origin access identity (OAI). This will allow CloudFront to access the S3 bucket securely and prevent public access to the bucket.
  - During the weekly maintenance, edit the default cache behavior to use the S3 origin. Revert the change when the maintenance is complete. This will redirect all web requests to the S3 bucket instead of the Elastic Beanstalk domain name.
- The other options are not correct because:
- Creating a new CloudFront distribution is not necessary and would require changing the alternate domain name configuration.
  - Creating a cache behavior for the S3 origin on a new distribution would not work because the visitors would still access the original distribution using the alternate domain name.
  - Configuring Elastic Beanstalk to serve traffic from the S3 bucket is not possible and would not achieve the desired result.

References:

- <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-values-specify>.

**NEW QUESTION 104**

- (Exam Topic 2)

A company's solutions architect is analyzing costs of a multi-application environment. The environment is deployed across multiple Availability Zones in a single AWS Region. After a recent acquisition, the company manages two organizations in AWS Organizations. The company has created multiple service provider applications as AWS PrivateLink-powered VPC endpoint services in one organization. The company has created multiple service consumer applications in the other organization.

Data transfer charges are much higher than the company expected, and the solutions architect needs to reduce the costs. The solutions architect must recommend guidelines for developers to follow when they deploy services. These guidelines must minimize data transfer charges for the whole environment.

Which guidelines meet these requirements? (Select TWO.)



- A. Use AWS Resource Access Manager to share the subnets that host the service provider applications with other accounts in the organization.
- B. Place the service provider applications and the service consumer applications in AWS accounts in the same organization.
- C. Turn off cross-zone load balancing for the Network Load Balancer in all service provider application deployments.
- D. Ensure that service consumer compute resources use the Availability Zone-specific endpoint service by using the endpoint's local DNS name.
- E. Create a Savings Plan that provides adequate coverage for the organization's planned inter-Availability Zone data transfer usage.

**Answer:** CD

**Explanation:**

Cross-zone load balancing enables traffic to be distributed evenly across all registered instances in all enabled Availability Zones. However, this also increases data transfer charges between Availability Zones. By turning off cross-zone load balancing, the service provider applications can reduce inter-Availability Zone data transfer costs. Similarly, by using the Availability Zone-specific endpoint service, the service consumer applications can ensure that they connect to the nearest service provider application in the same Availability Zone, avoiding cross-Availability Zone data transfer charges. References:

➤ <https://docs.aws.amazon.com/vpc/latest/userguide/vpce-interface.html#vpce-interface-dns>

**NEW QUESTION 109**

- (Exam Topic 2)

A company provides auction services for artwork and has users across North America and Europe. The company hosts its application in Amazon EC2 instances in the us-east-1 Region. Artists upload photos of their work as large-size, high-resolution image files from their mobile phones to a centralized Amazon S3 bucket created in the us-east-1 Region. The users in Europe are reporting slow performance for their Image uploads.

How can a solutions architect improve the performance of the image upload process?

- A. Redeploy the application to use S3 multipart uploads.
- B. Create an Amazon CloudFront distribution and point to the application as a custom origin
- C. Configure the buckets to use S3 Transfer Acceleration.
- D. Create an Auto Scaling group for the EC2 instances and create a scaling policy.

**Answer:** C

**Explanation:**

Transfer acceleration. S3 Transfer Acceleration utilizes the Amazon CloudFront global network of edge locations to accelerate the transfer of data to and from S3 buckets. By enabling S3 Transfer Acceleration on the centralized S3 bucket, the users in Europe will experience faster uploads as their data will be routed through the closest CloudFront edge location.

**NEW QUESTION 113**

- (Exam Topic 2)

A company processes environment data. The has a set up sensors to provide a continuous stream of data from different areas in a city. The data is available in JSON format.

The company wants to use an AWS solution to send the data to a database that does not require fixed schemas for storage. The data must be send in real time. Which solution will meet these requirements?

- A. Use Amazon Kinesis Data Firehouse to send the data to Amazon Redshift.
- B. Use Amazon Kinesis Data streams to send the data to Amazon DynamoDB.
- C. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) to send the data to Amazon Aurora.
- D. Use Amazon Kinesis Data firehouse to send the data to Amazon Keyspaces (for Apache Cassandra).

**Answer:** B

**Explanation:**

Amazon Kinesis Data Streams is a service that enables real-time data ingestion and processing. Amazon DynamoDB is a NoSQL database that does not require fixed schemas for storage. By using Kinesis Data Streams and DynamoDB, the company can send the JSON data to a database that can handle schemaless data in real time. References:

➤ <https://docs.aws.amazon.com/streams/latest/dev/introduction.html>

➤ <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html>

**NEW QUESTION 117**

- (Exam Topic 2)

A company wants to containerize a multi-tier web application and move the application from an on-premises data center to AWS. The application includes web. application, and database tiers. The company needs to make the application fault tolerant and scalable. Some frequently accessed data must always be available across application servers. Frontend web servers need session persistence and must scale to meet increases in traffic.

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

- A. Run the application on Amazon Elastic Container Service (Amazon ECS) on AWS Fargat
- B. Use Amazon Elastic File System (Amazon EFS) for data that is frequently accessed between the web and application tier
- C. Store the frontend web server session data in Amazon Simple Queue Service (Amazon SQS).
- D. Run the application on Amazon Elastic Container Service (Amazon ECS) on Amazon EC2. Use Amazon ElastiCache for Redis to cache frontend web server session data
- E. Use Amazon Elastic Block Store (Amazon EBS) with Multi-Attach on EC2 instances that are distributed across multiple Availability Zones.
- F. Run the application on Amazon Elastic Kubernetes Service (Amazon EKS). Configure Amazon EKS to use managed node group
- G. Use ReplicaSets to run the web servers and application
- H. Create an Amazon Elastic File System (Amazon EFS) Me syste
- I. Mount the EFS file system across all EKS pods to store frontend web server session data.
- J. Deploy the application on Amazon Elastic Kubernetes Service (Amazon EKS) Configure Amazon EKS to use managed node group
- K. Run the web servers and application as Kubernetes deployments in the EKS cluste
- L. Store the frontend web server session data in an Amazon DynamoDB tabl
- M. Create an Amazon Elastic File System (Amazon EFS) volume that all applications will mount at the time of deployment.

**Answer:** D

**Explanation:**

Deploying the application on Amazon EKS with managed node groups simplifies the operational overhead of managing the Kubernetes cluster. Running the web servers and application as Kubernetes deployments ensures that the desired number of pods are always running and can scale up or down as needed. Storing the frontend web server session data in an Amazon DynamoDB table provides a fast, scalable, and durable storage option that can be accessed across multiple Availability Zones. Creating an Amazon EFS volume that all applications will mount at the time of deployment allows the application to share data that is frequently accessed between the web and application tiers. References:

- <https://docs.aws.amazon.com/eks/latest/userguide/managed-node-groups.html>
- <https://docs.aws.amazon.com/eks/latest/userguide/deployments.html>
- <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html>
- <https://docs.aws.amazon.com/efs/latest/ug/mounting-fs.html>

**NEW QUESTION 122**

- (Exam Topic 2)

A company has a website that runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are in an Auto Scaling group. The ALB is associated with an AWS WAF web ACL.

The website often encounters attacks in the application layer. The attacks produce sudden and significant increases in traffic on the application server. The access logs show that each attack originates from different IP addresses. A solutions architect needs to implement a solution to mitigate these attacks.

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

- A. Create an Amazon CloudWatch alarm that monitors server access
- B. Set a threshold based on access by IP address
- C. Configure an alarm action that adds the IP address to the web ACL's deny list.
- D. Deploy AWS Shield Advanced in addition to AWS WAF
- E. Add the ALB as a protected resource.
- F. Create an Amazon CloudWatch alarm that monitors user IP addresses
- G. Set a threshold based on access by IP address
- H. Configure the alarm to invoke an AWS Lambda function to add a deny rule in the application server's subnet route table for any IP addresses that activate the alarm.
- I. Inspect access logs to find a pattern of IP addresses that launched the attack
- J. Use an Amazon Route 53 geolocation routing policy to deny traffic from the countries that host those IP addresses.

**Answer: C**

**Explanation:**

"The AWS WAF API supports security automation such as blacklisting IP addresses that exceed request limits, which can be useful for mitigating HTTP flood attacks." >

<https://aws.amazon.com/blogs/security/how-to-protect-dynamic-web-applications-against-ddos-attacks-by-using>

**NEW QUESTION 123**

- (Exam Topic 2)

A solutions architect wants to cost-optimize and appropriately size Amazon EC2 instances in a single AWS account. The solutions architect wants to ensure that the instances are optimized based on CPU, memory, and network metrics.

Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)

- A. Purchase AWS Business Support or AWS Enterprise Support for the account.
- B. Turn on AWS Trusted Advisor and review any "Low Utilization Amazon EC2 Instances" recommendations.
- C. Install the Amazon CloudWatch agent and configure memory metric collection on the EC2 instances.
- D. Configure AWS Compute Optimizer in the AWS account to receive findings and optimization recommendations.
- E. Create an EC2 Instance Savings Plan for the AWS Regions, instance families, and operating systems of interest.

**Answer: BD**

**Explanation:**

AWS Trusted Advisor is a service that provides real-time guidance to help users provision their resources following AWS best practices<sup>1</sup>. One of the Trusted Advisor checks is "Low Utilization Amazon EC2 Instances", which identifies EC2 instances that appear to be underutilized based on CPU, network I/O, and disk I/O metrics<sup>1</sup>. This check can help users optimize the cost and size of their EC2 instances by recommending smaller or more appropriate instance types.

AWS Compute Optimizer is a service that analyzes the configuration and utilization metrics of AWS resources and generates optimization recommendations to reduce the cost and improve the performance of workloads<sup>2</sup>. Compute Optimizer supports four types of AWS resources: EC2 instances, EBS volumes, ECS services on AWS Fargate, and Lambda functions<sup>2</sup>. For EC2 instances, Compute Optimizer evaluates the vCPUs, memory, storage, and other specifications, as well as the CPU utilization, network in and out, disk read and write, and other utilization metrics of currently running instances<sup>3</sup>. It then recommends optimal instance types based on price-performance trade-offs.

Option A is incorrect because purchasing AWS Business Support or AWS Enterprise Support for the account will not directly help with cost-optimization and sizing of EC2 instances. However, these support plans do provide access to more Trusted Advisor checks than the basic support plan<sup>1</sup>.

Option C is incorrect because installing the Amazon CloudWatch agent and configuring memory metric collection on the EC2 instances will not provide any optimization recommendations by itself. However, memory metrics can be used by Compute Optimizer to enhance its recommendations if enabled<sup>3</sup>.

Option E is incorrect because creating an EC2 Instance Savings Plan for the AWS Regions, instance families, and operating systems of interest will not help with cost-optimization and sizing of EC2 instances. Savings Plans are a flexible pricing model that offer lower prices on Amazon EC2 usage in exchange for a commitment to a consistent amount of usage for a 1- or 3-year term<sup>4</sup>. Savings Plans do not affect the configuration or utilization of EC2 instances.

**NEW QUESTION 126**

- (Exam Topic 2)

A company has many separate AWS accounts and uses no central billing or management. Each AWS account hosts services for different departments in the company. The company has a Microsoft Azure Active Directory that is deployed.

A solution architect needs to centralize billing and management of the company's AWS accounts. The company wants to start using identity federation instead of manual user management. The company also wants to use temporary credentials instead of long-lived access keys.

Which combination of steps will meet these requirements? (Select THREE)

- A. Create a new AWS account to serve as a management account

- B. Deploy an organization in AWS Organization
- C. Invite each existing AWS account to join the organization
- D. Ensure that each account accepts the invitation.
- E. Configure each AWS Account's email address to be aws+<account id>@example.com so that account management email messages and invoices are sent to the same place.
- F. Deploy AWS IAM Identity Center (AWS Single Sign-On) in the management account
- G. Connect IAM Identity Center to the Azure Active Directory
- H. Configure IAM Identity Center for automatic synchronization of users and groups.
- I. Deploy an AWS Managed Microsoft AD directory in the management account
- J. Share the directory with all other accounts in the organization by using AWS Resource Access Manager (AWS RAM).
- K. Create AWS IAM Identity Center (AWS Single Sign-On) permission set
- L. Attach the permission sets to the appropriate IAM Identity Center groups and AWS accounts.
- M. Configure AWS Identity and Access Management (IAM) in each AWS account to use AWS Managed Microsoft AD for authentication and authorization.

**Answer:** ACE

#### NEW QUESTION 131

- (Exam Topic 2)

A company has millions of objects in an Amazon S3 bucket. The objects are in the S3 Standard storage class. All the S3 objects are accessed frequently. The number of users and applications that access the objects is increasing rapidly. The objects are encrypted with server-side encryption with AWS KMS Keys (SSE-KMS).

A solutions architect reviews the company's monthly AWS invoice and notices that AWS KMS costs are increasing because of the high number of requests from Amazon S3. The solutions architect needs to optimize costs with minimal changes to the application.

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

- A. Create a new S3 bucket that has server-side encryption with customer-provided keys (SSE-C) as the encryption type
- B. Copy the existing objects to the new S3 bucket
- C. Specify SSE-C.
- D. Create a new S3 bucket that has server-side encryption with Amazon S3 managed keys (SSE-S3) as the encryption type
- E. Use S3 Batch Operations to copy the existing objects to the new S3 bucket
- F. Specify SSE-S3.
- G. Use AWS CloudHSM to store the encryption key
- H. Create a new S3 bucket
- I. Use S3 Batch Operations to copy the existing objects to the new S3 bucket
- J. Encrypt the objects by using the keys from CloudHSM.
- K. Use the S3 Intelligent-Tiering storage class for the S3 bucket
- L. Create an S3 Intelligent-Tiering archive configuration to transition objects that are not accessed for 90 days to S3 Glacier Deep Archive.

**Answer:** B

#### Explanation:

To reduce the volume of Amazon S3 calls to AWS KMS, use Amazon S3 bucket keys, which are protected encryption keys that are reused for a limited time in Amazon S3. Bucket keys can reduce costs for AWS KMS requests by up to 99%. You can configure a bucket key for all objects in an Amazon S3 bucket, or for a specific object in an Amazon S3 bucket. [https://docs.aws.amazon.com/fr\\_fr/kms/latest/developerguide/services-s3.html](https://docs.aws.amazon.com/fr_fr/kms/latest/developerguide/services-s3.html)

#### NEW QUESTION 134

- (Exam Topic 2)

A company is building a hybrid environment that includes servers in an on-premises data center and in the AWS Cloud. The company has deployed Amazon EC2 instances in three VPCs. Each VPC is in a different AWS Region. The company has established an AWS Direct Connect connection to the data center from the Region that is closest to the data center.

The company needs the servers in the on-premises data center to have access to the EC2 instances in all three VPCs. The servers in the on-premises data center also must have access to AWS public services.

Which combination of steps will meet these requirements with the LEAST cost? (Select TWO.)

- A. Create a Direct Connect gateway in the Region that is closest to the data center
- B. Attach the Direct Connect connection to the Direct Connect gateway
- C. Use the
- D. Direct Connect gateway to connect the VPCs in the other two Regions.
- E. Set up additional Direct Connect connections from the on-premises data center to the other two Regions.
- F. Create a private VIF
- G. Establish an AWS Site-to-Site VPN connection over the private VIF to the VPCs in the other two Regions.
- H. Create a public VIF
- I. Establish an AWS Site-to-Site VPN connection over the public VIF to the VPCs in the other two Regions.
- J. Use VPC peering to establish a connection between the VPCs across the Region
- K. Create a private VIF with the existing Direct Connect connection to connect to the peered VPCs.

**Answer:** AE

#### Explanation:

A Direct Connect gateway allows you to connect multiple VPCs across different Regions to a Direct Connect connection. A public VIF allows you to access AWS public services such as EC2. A Site-to-Site VPN connection over the public VIF provides encryption and redundancy for the traffic between the on-premises data center and the VPCs. This solution is cheaper than setting up additional Direct Connect connections or using a private VIF with VPC peering.

#### NEW QUESTION 139

- (Exam Topic 2)

A company plans to migrate a three-tiered web application from an on-premises data center to AWS. The company developed the UI by using server-side JavaScript libraries. The business logic and API tier uses a Python-based web framework. The data tier runs on a MySQL database.

The company custom-built the application to meet business requirements. The company does not want to

re-architect the application. The company needs a solution to replatform the application to AWS with the least possible amount of development. The solution needs to be highly available and must reduce operational overhead.



Which solution will meet these requirements?

- A. Deploy the UI to a static website on Amazon S3 Use Amazon CloudFront to deliver the website Build the business logic in a Docker image Store the image in Amazon Elastic Container Registry (Amazon ECR) Use Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type to host the website with an Application Load Balancer in front Deploy the datalayer to an Amazon Aurora MySQL DB cluster
- B. Build the UI and business logic in Docker images Store the images in Amazon Elastic Container Registry (Amazon ECR) Use Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type to host the UI and business logic applications with an Application Load Balancer in front Migrate the database to an Amazon RDS for MySQL Multi-AZ DB instance
- C. Deploy the UI to a static website on Amazon S3 Use Amazon CloudFront to deliver the website Convert the business logic to AWS Lambda functions Integrate the functions with Amazon API Gateway Deploy the data layer to an Amazon Aurora MySQL DB cluster
- D. Build the UI and business logic in Docker images Store the images in Amazon Elastic Container Registry (Amazon ECR) Use Amazon Elastic Kubernetes Service (Amazon EKS) with Fargate profiles to host the UI and business logic Use AWS Database Migration Service (AWS DMS) to migrate the data layer to Amazon DynamoDB

**Answer:** A

**Explanation:**

This solution utilizes Amazon S3 and CloudFront to deploy the UI as a static website, which can be done with minimal development effort. The business logic and API tier can be containerized in a Docker image and stored in Amazon Elastic Container Registry (ECR) and run on Amazon Elastic Container Service (ECS) with the Fargate launch type, which allows the application to be highly available with minimal operational overhead. The data layer can be deployed on an Amazon Aurora MySQL DB cluster which is a fully managed relational database service. Amazon Aurora provides high availability and performance for the data layer without the need for managing the underlying infrastructure.

**NEW QUESTION 143**

- (Exam Topic 2)

A company is migrating its development and production workloads to a new organization in AWS Organizations. The company has created a separate member account for development and a separate member account for production. Consolidated billing is linked to the management account. In the management account, a solutions architect needs to create an IAM user that can stop or terminate resources in both member accounts.

Which solution will meet this requirement?

- A. Create an IAM user and a cross-account role in the management account
- B. Configure the cross-account role with least privilege access to the member accounts.
- C. Create an IAM user in each member account
- D. In the management account, create a cross-account role that has least privilege access
- E. Grant the IAM users access to the cross-account role by using a trust policy.
- F. Create an IAM user in the management account
- G. In the member accounts, create an IAM group that has least privilege access
- H. Add the IAM user from the management account to each IAM group in the member accounts.
- I. Create an IAM user in the management account
- J. In the member accounts, create cross-account roles that have least privilege access
- K. Grant the IAM user access to the roles by using a trust policy.

**Answer:** D

**Explanation:**

Cross account role should be created in destination(member) account. The role has trust entity to master account.

**NEW QUESTION 148**

- (Exam Topic 2)

A company runs an application on AWS. The company curates data from several different sources. The company uses proprietary algorithms to perform data transformations and aggregations. After the company performs ETL processes, the company stores the results in Amazon Redshift tables. The company sells this data to other companies. The company downloads the data as files from the Amazon Redshift tables and transmits the files to several data customers by using FTP. The number of data customers has grown significantly. Management of the data customers has become difficult.

The company will use AWS Data Exchange to create a data product that the company can use to share data with customers. The company wants to confirm the identities of the customers before the company shares data.

The customers also need access to the most recent data when the company publishes the data. Which solution will meet these requirements with the LEAST operational overhead?

- A. Use AWS Data Exchange for APIs to share data with customer
- B. Configure subscription verification In the AWS account of the company that produces the data, create an Amazon API Gateway Data API service integration with Amazon Redshift
- C. Require the data customers to subscribe to the data product In the AWS account of the company that produces the data, create an AWS Data Exchange datashare by connecting AWS Data Exchange to the Redshift cluster
- D. cluster
- E. Configure subscription verification
- F. Require the data customers to subscribe to the data product.
- G. Download the data from the Amazon Redshift tables to an Amazon S3 bucket periodically
- H. Use AWS Data Exchange for S3 to share data with customers.
- I. Configure subscription verification
- J. Require the data customers to subscribe to the data product Publish the Amazon Redshift data to an Open Data on AWS Data Exchange
- K. Require the customers to subscribe to the data product in AWS Data Exchange
- L. In the AWS account of the company that produces the data, attach IAM resource-based policies to the Amazon Redshift tables to allow access only to verified AWS accounts.

**Answer:** C

**Explanation:**

The company should download the data from the Amazon Redshift tables to an Amazon S3 bucket periodically and use AWS Data Exchange for S3 to share data with customers. The company should configure subscription verification and require the data customers to subscribe to the data product. This solution will meet the requirements with the least operational overhead because AWS Data Exchange for S3 is a feature that enables data subscribers to access third-party data files directly from data providers' Amazon S3 buckets. Subscribers can easily use these files for their data analysis with AWS services without needing to create or

manage data copies. Data providers can easily set up AWS Data Exchange for S3 on top of their existing S3 buckets to share direct access to an entire S3 bucket or specific prefixes and S3 objects. AWS Data Exchange automatically manages subscriptions, entitlements, billing, and payment<sup>1</sup>.

The other options are not correct because:

- Using AWS Data Exchange for APIs to share data with customers would not work because AWS Data Exchange for APIs is a feature that enables data subscribers to access third-party APIs directly from data providers' AWS accounts. Subscribers can easily use these APIs for their data analysis with AWS services without needing to manage API keys or tokens. Data providers can easily set up AWS Data Exchange for APIs on top of their existing API Gateway resources to share direct access to an entire API or specific routes and stages<sup>2</sup>. However, this feature is not suitable for sharing data from Amazon Redshift tables, which are not exposed as APIs.
- Creating an Amazon API Gateway Data API service integration with Amazon Redshift would not work because the Data API is a feature that enables you to query your Amazon Redshift cluster using HTTP requests, without needing a persistent connection or a SQL client<sup>3</sup>. It is useful for building applications that interact with Amazon Redshift, but not for sharing data files with customers.
- Creating an AWS Data Exchange datashare by connecting AWS Data Exchange to the Redshift cluster would not work because AWS Data Exchange does not support datashares for Amazon Redshift clusters. A datashare is a feature that enables you to share live and secure access to your Amazon Redshift data across your accounts or with third parties without copying or moving the underlying data<sup>4</sup>. It is useful for sharing query results and views with other users, but not for sharing data files with customers.
- Publishing the Amazon Redshift data to an Open Data on AWS Data Exchange would not work because Open Data on AWS Data Exchange is a feature that enables you to find and use free and public datasets from AWS customers and partners. It is useful for accessing open and free data, but not for confirming the identities of the customers or charging them for the data.

References:

- <https://aws.amazon.com/data-exchange/why-aws-data-exchange/s3/>
- <https://aws.amazon.com/data-exchange/why-aws-data-exchange/api/>
- <https://docs.aws.amazon.com/redshift/latest/mgmt/data-api.html>
- <https://docs.aws.amazon.com/redshift/latest/dg/datashare-overview.html>
- <https://aws.amazon.com/data-exchange/open-data/>

### NEW QUESTION 150

- (Exam Topic 2)

A company has a critical application in which the data tier is deployed in a single AWS Region. The data tier uses an Amazon DynamoDB table and an Amazon Aurora MySQL DB cluster. The current Aurora MySQL engine version supports a global database. The application tier is already deployed in two Regions. Company policy states that critical applications must have application tier components and data tier components deployed across two Regions. The RTO and RPO must be no more than a few minutes each. A solutions architect must recommend a solution to make the data tier compliant with company policy. Which combination of steps will meet these requirements? (Choose two.)

- A. Add another Region to the Aurora MySQL DB cluster
- B. Add another Region to each table in the Aurora MySQL DB cluster
- C. Set up scheduled cross-Region backups for the DynamoDB table and the Aurora MySQL DB cluster
- D. Convert the existing DynamoDB table to a global table by adding another Region to its configuration
- E. Use Amazon Route 53 Application Recovery Controller to automate database backup and recovery to the secondary Region

**Answer:** AD

#### Explanation:

The company should use Amazon Aurora global database and Amazon DynamoDB global table to deploy the data tier components across two Regions. Amazon Aurora global database is a feature that allows a single Aurora database to span multiple AWS Regions, enabling low-latency global reads and fast recovery from Region-wide outages<sup>1</sup>. Amazon DynamoDB global table is a feature that allows a single DynamoDB table to span multiple AWS Regions, enabling low-latency global reads and writes and fast recovery from Region-wide outages<sup>2</sup>.

References:

- <https://aws.amazon.com/rds/aurora/global-database/>
- [https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/globaltables\\_HowItWorks.html](https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/globaltables_HowItWorks.html)
- <https://aws.amazon.com/route53/application-recovery-controller/>

### NEW QUESTION 152

- (Exam Topic 2)

A company is running a containerized application in the AWS Cloud. The application is running by using Amazon Elastic Container Service (Amazon ECS) on a set of Amazon EC2 instances. The EC2 instances run in an Auto Scaling group.

The company uses Amazon Elastic Container Registry (Amazon ECR) to store its container images. When a new image version is uploaded, the new image version receives a unique tag.

The company needs a solution that inspects new image versions for common vulnerabilities and exposures. The solution must automatically delete new image tags that have Critical or High severity findings. The solution also must notify the development team when such a deletion occurs.

Which solution meets these requirements?

- A. Configure scan on push on the repository Use Amazon EventBridge to invoke an AWS Step Functions state machine when a scan is complete for images that have Critical or High severity finding
- B. Use the Step Functions state machine to delete the image tag for those images and to notify the development team through Amazon Simple Notification Service (Amazon SNS).
- C. Configure scan on push on the repository Configure scan results to be pushed to an Amazon Simple Queue Service (Amazon SQS) queue
- D. Invoke an AWS Lambda function when a new message is added to the SQS queue
- E. Use the Lambda function to delete the image tag for images that have Critical or High severity finding
- F. Notify the development team by using Amazon Simple Email Service (Amazon SES).
- G. Schedule an AWS Lambda function to start a manual image scan every hour
- H. Configure Amazon EventBridge to invoke another Lambda function when a scan is complete
- I. Use the second Lambda function to delete the image tag for images that have Critical or High severity finding
- J. Notify the development team by using Amazon Simple Notification Service (Amazon SNS).
- K. Configure periodic image scan on the repository
- L. Configure scan results to be added to an Amazon Simple Queue Service (Amazon SQS) queue
- M. Invoke an AWS Step Functions state machine when a new message is added to the SQS queue

- N. Use the Step Functions state machine to delete the image tag for images that have Critical or High severity finding
- O. Notify the development team by using Amazon Simple Email Service (Amazon SES).

**Answer:** A

**Explanation:**

<https://docs.aws.amazon.com/AmazonECR/latest/userguide/ecr-eventbridge.html> "Activating an AWS Step Functions state machine"  
<https://docs.aws.amazon.com/step-functions/latest/dg/tutorial-creating-lambda-state-machine.html>

**NEW QUESTION 157**

- (Exam Topic 2)

A company has an on-premises Microsoft SQL Server database that writes a nightly 200 GB export to a local drive. The company wants to move the backups to more robust cloud storage on Amazon S3. The company has set up a 10 Gbps AWS Direct Connect connection between the on-premises data center and AWS. Which solution meets these requirements MOST cost-effectively?

- A. Create a new S3 bucket
- B. Deploy an AWS Storage Gateway file gateway within the VPC that is connected to the Direct Connect connection
- C. Create a new SMB file share
- D. Write nightly database exports to the new SMB file share.
- E. Create an Amazon FSx for Windows File Server Single-AZ file system within the VPC that is connected to the Direct Connect connection
- F. Create a new SMB file share
- G. Write nightly database exports to an SMB file share on the Amazon FSx file system
- H. Enable nightly backups.
- I. Create an Amazon FSx for Windows File Server Multi-AZ file system within the VPC that is connected to the Direct Connect connection
- J. Create a new SMB file share
- K. Write nightly database exports to an SMB file share on the Amazon FSx file system
- L. Enable nightly backups.
- M. Create a new S3 bucket
- N. Deploy an AWS Storage Gateway volume gateway within the VPC that is connected to the Direct Connect connection
- O. Create a new SMB file share
- P. Write nightly database exports to the new SMB file share on the volume gateway, and automate copies of this data to an S3 bucket.

**Answer:** A

**Explanation:**

<https://docs.aws.amazon.com/filegateway/latest/files3/CreatingAnSMBFileShare.html>

**NEW QUESTION 158**

.....



## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### SAP-C02 Practice Exam Features:

- \* SAP-C02 Questions and Answers Updated Frequently
- \* SAP-C02 Practice Questions Verified by Expert Senior Certified Staff
- \* SAP-C02 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* SAP-C02 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The SAP-C02 Practice Test Here](#)**