

# Amazon-Web-Services

## Exam Questions SAP-C02

AWS Certified Solutions Architect - Professional



**NEW QUESTION 1**

- (Exam Topic 1)

A company is developing a new serverless API by using Amazon API Gateway and AWS Lambda. The company integrated the Lambda functions with API Gateway to use several shared libraries and custom classes.

A solutions architect needs to simplify the deployment of the solution and optimize for code reuse. Which solution will meet these requirements?

- A. Deploy the shared libraries and custom classes into a Docker image
- B. Store the image in an S3 bucket. Create a Lambda layer that uses the Docker image as the source
- C. Deploy the API's Lambda functions as Zip package
- D. Configure the packages to use the Lambda layer.
- E. Deploy the shared libraries and custom classes to a Docker image
- F. Upload the image to Amazon Elastic Container Registry (Amazon ECR). Create a Lambda layer that uses the Docker image as the source
- G. Deploy the API's Lambda functions as Zip package
- H. Configure the packages to use the Lambda layer.
- I. Deploy the shared libraries and custom classes to a Docker container in Amazon Elastic Container Service (Amazon ECS) by using the AWS Fargate launch type
- J. Deploy the API's Lambda functions as Zip package
- K. Configure the packages to use the deployed container as a Lambda layer.
- L. Deploy the shared libraries, custom classes, and code for the API's Lambda functions to a Docker image
- M. Upload the image to Amazon Elastic Container Registry (Amazon ECR). Configure the API's Lambda functions to use the Docker image as the deployment package.

**Answer:** B

**Explanation:**

Deploying the shared libraries and custom classes to a Docker image and uploading the image to Amazon Elastic Container Registry (Amazon ECR) and creating a Lambda layer that uses the Docker image as the source. Then, deploying the API's Lambda functions as Zip packages and configuring the packages to use the Lambda layer would meet the requirements for simplifying the deployment and optimizing for code reuse.

A Lambda layer is a distribution mechanism for libraries, custom runtimes, and other function dependencies. It allows you to manage your in-development function code separately from your dependencies, this way you can easily update your dependencies without having to update your entire function code.

By deploying the shared libraries and custom classes to a Docker image and uploading the image to Amazon Elastic Container Registry (ECR), it makes it easy to manage and version the dependencies. This way, the company can use the same version of the dependencies across different Lambda functions.

By creating a Lambda layer that uses the Docker image as the source, the company can configure the API's Lambda functions to use the layer, reducing the need to include the dependencies in each function package, and making it easy to update the dependencies across all functions at once.

Reference:

AWS Lambda Layers documentation: <https://docs.aws.amazon.com/lambda/latest/dg/configuration-layers.html>

AWS Elastic Container Registry (ECR) documentation: <https://aws.amazon.com/ecr/> Building Lambda Layers with Docker documentation:

<https://aws.amazon.com/blogs/compute/building-lambda-layers-with-docker/>

**NEW QUESTION 2**

- (Exam Topic 1)

An application is using an Amazon RDS for MySQL Multi-AZ DB instance in the us-east-1 Region. After a failover test, the application lost the connections to the database and could not re-establish the connections. After a restart of the application, the application re-established the connections.

A solutions architect must implement a solution so that the application can re-establish connections to the database without requiring a restart.

Which solution will meet these requirements?

- A. Create an Amazon Aurora MySQL Serverless v1 DB instance
- B. Migrate the RDS DB instance to the Aurora Serverless v1 DB instance
- C. Update the connection settings in the application to point to the Aurora reader endpoint.
- D. Create an RDS proxy
- E. Configure the existing RDS endpoint as a target
- F. Update the connection settings in the application to point to the RDS proxy endpoint.
- G. Create a two-node Amazon Aurora MySQL DB cluster
- H. Migrate the RDS DB instance to the Aurora DB cluster
- I. Create an RDS proxy
- J. Configure the existing RDS endpoint as a target
- K. Update the connection settings in the application to point to the RDS proxy endpoint.
- L. Create an Amazon S3 bucket
- M. Export the database to Amazon S3 by using AWS Database Migration Service (AWS DMS). Configure Amazon Athena to use the S3 bucket as a data store
- N. Install the latest Open Database Connectivity (ODBC) driver for the application
- O. Update the connection settings in the application to point to the Athena endpoint

**Answer:** B

**Explanation:**

Amazon RDS Proxy is a fully managed database proxy service for Amazon Relational Database Service (RDS) that makes applications more scalable, resilient, and secure. It allows applications to pool and share connections to an RDS database, which can help reduce database connection overhead, improve scalability, and provide automatic failover and high availability.

**NEW QUESTION 3**

- (Exam Topic 1)

A company runs a content management application on a single Windows Amazon EC2 instance in a development environment. The application reads and writes static content to a 2 TB Amazon Elastic Block Store (Amazon EBS) volume that is attached to the instance as the root device. The company plans to deploy this application in production as a highly available and fault-tolerant solution that runs on at least three EC2 instances across multiple Availability Zones.

A solutions architect must design a solution that joins all the instances that run the application to an Active Directory domain. The solution also must implement Windows ACLs to control access to file contents. The application always must maintain exactly the same content on all running instances at any given point in time.

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

- A. Create an Amazon Elastic File System (Amazon EFS) file share

- B. Create an Auto Scaling group that extends across three Availability Zones and maintains a minimum size of three instance
- C. Implement a user data script to install the application, join the instance to the AD domain, and mount the EFS file share.
- D. Create a new AMI from the current EC2 instance that is runnin
- E. Create an Amazon FSx for Lustre file syste
- F. Create an Auto Scaling group that extends across three Availability Zones and maintains a minimum size of three instance
- G. Implement a user data script to join the instance to the AD domain and mount the FSx for Lustre file system.
- H. Create an Amazon FSx for Windows File Server file syste
- I. Create an Auto Scaling group that extends across three Availability Zones and maintains a minimum size of three instance
- J. Implement a user data script to install the application and mount the FSx for Windows File Server file syste
- K. Perform a seamless domain join to join the instance to the AD domain.
- L. Create a new AMI from the current EC2 instance that is runnin
- M. Create an Amazon Elastic File System (Amazon EFS) file syste
- N. Create an Auto Scaling group that extends across three Availability Zones and maintains a minimum size of three instance
- O. Perform a seamless domain join to join the instance to the AD domain.

**Answer:** C

**Explanation:**

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/what-is.html> [https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms\\_ad\\_join\\_instance.html](https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_join_instance.html)

**NEW QUESTION 4**

- (Exam Topic 1)

A large mobile gaming company has successfully migrated all of its on-premises infrastructure to the AWS Cloud. A solutions architect is reviewing the environment to ensure that it was built according to the design and that it is running in alignment with the Well-Architected Framework.

While reviewing previous monthly costs in Cost Explorer, the solutions architect notices that the creation and subsequent termination of several large instance types account for a high proportion of the costs. The solutions architect finds out that the company's developers are launching new Amazon EC2 instances as part of their testing and that the developers are not using the appropriate instance types.

The solutions architect must implement a control mechanism to limit the instance types that only the developers can launch.

Which solution will meet these requirements?

- A. Create a desired-instance-type managed rule in AWS Confi
- B. Configure the rule with the instance types that are allowe
- C. Attach the rule to an event to run each time a new EC2 instance is launched.
- D. In the EC2 console, create a launch template that specifies the instance types that are allowe
- E. Assign the launch template to the developers' IAM accounts.
- F. Create a new IAM polic
- G. Specify the instance types that are allowe
- H. Attach the policy to an IAM group that contains the IAM accounts for the developers
- I. Use EC2 Image Builder to create an image pipeline for the developers and assist them in the creation of a golden image.

**Answer:** C

**Explanation:**

This is doable with IAM policy creation to restrict users to specific instance types. Found the below article. <https://blog.vizuri.com/limiting-allowed-aws-instance-type-with-iam-policy>

**NEW QUESTION 5**

- (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 SQ
- 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
- E. Configure the existing web server to publish to the new queu
- 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 EF
- H. Shut down the EC2 instance after the task is complete.
- I. Create a queue using Amazon M
- 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 SO
- M. Configure the existing web server to publish to the new queu
- 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 SOS queue lengt
- 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 6**

- (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 layer.

➤ 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 7**

- (Exam Topic 1)

A company is developing and hosting several projects in the AWS Cloud. The projects are developed across multiple AWS accounts under the same organization in AWS Organizations. The company requires the cost for cloud infrastructure to be allocated to the owning project. The team responsible for all of the AWS accounts has discovered that several Amazon EC2 instances are lacking the Project tag used for cost allocation.

Which actions should a solutions architect take to resolve the problem and prevent it from happening in the future? (Select THREE.)

- A. Create an AWS Config rule in each account to find resources with missing tags.
- B. Create an SCP in the organization with a deny action for `ec2:RunInstances` if the Project tag is missing.
- C. Use Amazon Inspector in the organization to find resources with missing tags.
- D. Create an IAM policy in each account with a deny action for `ec2:RunInstances` if the Project tag is missing.
- E. Create an AWS Config aggregator for the organization to collect a list of EC2 instances with the missing Project tag.
- F. Use AWS Security Hub to aggregate a list of EC2 instances with the missing Project tag.

**Answer:** ABE

**Explanation:**

<https://docs.aws.amazon.com/config/latest/developerguide/config-rule-multi-account-deployment.html>

<https://docs.aws.amazon.com/config/latest/developerguide/aggregate-data.html>

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scps\\_examples\\_tagging.htm](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_tagging.htm)

**NEW QUESTION 8**

- (Exam Topic 1)

A company has a serverless application comprised of Amazon CloudFront, Amazon API Gateway, and AWS Lambda functions. The current deployment process of the application code is to create a new version number of the Lambda function and run an AWS CLI script to update. If the new function version has errors, another CLI script reverts by deploying the previous working version of the function. The company would like to decrease the time to deploy new versions of the application logic provided by the Lambda functions, and also reduce the time to detect and revert when errors are identified.

How can this be accomplished?

- A. Create and deploy nested AWS CloudFormation stacks with the parent stack consisting of the AWS CloudFront distribution and API Gateway, and the child stack containing the Lambda function
- B. For changes to Lambda, create an AWS CloudFormation change set and deploy; if errors are triggered, revert the AWS CloudFormation change set to the previous version.
- C. Use AWS SAM and built-in AWS CodeDeploy to deploy the new Lambda version, gradually shift traffic to the new version, and use pre-traffic and post-traffic test functions to verify code
- D. Rollback if Amazon CloudWatch alarms are triggered.
- E. Refactor the AWS CLI scripts into a single script that deploys the new Lambda version
- F. When deployment is completed, the script tests execution
- G. If errors are detected, revert to the previous Lambda version.
- H. Create and deploy an AWS CloudFormation stack that consists of a new API Gateway endpoint that references the new Lambda version
- I. Change the CloudFront origin to the new API Gateway endpoint, monitor errors and if detected, change the AWS CloudFront origin to the previous API Gateway endpoint.

**Answer:** B

**Explanation:**

<https://aws.amazon.com/about-aws/whats-new/2017/11/aws-lambda-supports-traffic-shifting-and-phased-deploy>



**NEW QUESTION 9**

- (Exam Topic 1)

A company recently deployed an application on AWS. The application uses Amazon DynamoDB. The company measured the application load and configured the RCUs and WCUs on the DynamoDB table to match the expected peak load. The peak load occurs once a week for a 4-hour period and is double the average load. The application load is close to the average load for the rest of the week. The access pattern includes many more writes to the table than reads of the table. A solutions architect needs to implement a solution to minimize the cost of the table. Which solution will meet these requirements?

- A. Use AWS Application Auto Scaling to increase capacity during the peak period.
- B. Purchase reserved RCUs and WCUs to match the average load.
- C. Configure on-demand capacity mode for the table.
- D. Configure DynamoDB Accelerator (DAX) in front of the table.
- E. Reduce the provisioned read capacity to match the new peak load on the table.
- F. Configure DynamoDB Accelerator (DAX) in front of the table.
- G. Configure on-demand capacity mode for the table.

**Answer:** D

**Explanation:**

This solution meets the requirements by using Application Auto Scaling to automatically increase capacity during the peak period, which will handle the double the average load. And by purchasing reserved RCUs and WCUs to match the average load, it will minimize the cost of the table for the rest of the week when the load is close to the average.

**NEW QUESTION 10**

- (Exam Topic 1)

A company is migrating some of its applications to AWS. The company wants to migrate and modernize the applications quickly after it finalizes networking and security strategies. The company has set up an AWS Direct Connect connection in a central network account. The company expects to have hundreds of AWS accounts and VPCs in the near future. The corporate network must be able to access the resources on AWS seamlessly and also must be able to communicate with all the VPCs. The company also wants to route its cloud resources to the internet through its on-premises data center. Which combination of steps will meet these requirements? (Choose three.)

- A. Create a Direct Connect gateway in the central account
- B. In each of the accounts, create an association proposal by using the Direct Connect gateway and the account ID for every virtual private gateway.
- C. Create a Direct Connect gateway and a transit gateway in the central network account
- D. Attach the transit gateway to the Direct Connect gateway by using a transit VIF.
- E. Provision an internet gateway
- F. Attach the internet gateway to subnet
- G. Allow internet traffic through the gateway.
- H. Share the transit gateway with other account
- I. Attach VPCs to the transit gateway.
- J. Provision VPC peering as necessary.
- K. Provision only private subnet
- L. Open the necessary route on the transit gateway and customer gateway to allow outbound internet traffic from AWS to flow through NAT services that run in the data center.

**Answer:** BDF

**Explanation:**

- Option A is incorrect because creating a Direct Connect gateway in the central account and creating an association proposal by using the Direct Connect gateway and the account ID for every virtual private gateway does not enable active-passive failover between the regions. A Direct Connect gateway is a globally available resource that enables you to connect your AWS Direct Connect connection over a private virtual interface (VIF) to one or more VPCs in any AWS Region. A virtual private gateway is the VPN concentrator on the Amazon side of a VPN connection. You can associate a Direct Connect gateway with either a transit gateway or a virtual private gateway. However, a Direct Connect gateway does not provide any load balancing or failover capabilities by itself.
- Option B is correct because creating a Direct Connect gateway and a transit gateway in the central network account and attaching the transit gateway to the Direct Connect gateway by using a transit VIF meets the requirement of enabling the corporate network to access the resources on AWS seamlessly and also to communicate with all the VPCs. A transit VIF is a type of private VIF that you can use to connect your AWS Direct Connect connection to a transit gateway or a Direct Connect gateway. A transit gateway is a network transit hub that you can use to interconnect your VPCs and on-premises networks. By using a transit VIF, you can route traffic between your on-premises network and multiple VPCs across different AWS accounts and Regions through a single connection.
- Option C is incorrect because provisioning an internet gateway, attaching the internet gateway to subnets, and allowing internet traffic through the gateway does not meet the requirement of routing cloud resources to the internet through its on-premises data center. An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet. An internet gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses. By using an internet gateway, you are routing cloud resources directly to the internet, not through your on-premises data center.
- Option D is correct because sharing the transit gateway with other accounts and attaching VPCs to the transit gateway meets the requirement of enabling the corporate network to access the resources on AWS seamlessly and also to communicate with all the VPCs. You can share your transit gateway with other AWS accounts within the same organization by using AWS Resource Access Manager (AWS RAM). This allows you to centrally manage connectivity from multiple accounts without having to create individual peering connections between VPCs or duplicate network appliances in each account. You can attach VPCs from different accounts and Regions to your shared transit gateway and enable routing between them.
- Option E is incorrect because provisioning VPC peering as necessary does not meet the requirement of enabling the corporate network to access the resources on AWS seamlessly and also to communicate with all the VPCs. VPC peering is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account within a single Region. However, VPC peering does not allow you to route traffic from your on-premises network to your VPCs or between multiple Regions. You would need to create multiple VPN connections or Direct Connect connections for each VPC peering connection, which increases operational complexity and costs.
- Option F is correct because provisioning only private subnets, opening the necessary route on the transit gateway and customer gateway to allow outbound internet traffic from AWS to flow through NAT services that run in the data center meets the requirement of routing cloud resources to the internet through its on-premises data center. A private subnet is a subnet that's associated with a route table that has no route to an internet gateway. Instances in a private subnet can

communicate with other instances in the same VPC but cannot access resources on the internet directly. To enable outbound internet access from instances in private subnets, you can use NAT devices such as NAT gateways or NAT instances that are deployed in public subnets. A public subnet is a subnet that's associated with a route table that has a route to an internet gateway. Alternatively, you can use your on-premises data center as a NAT device by configuring routes on your transit gateway and customer gateway that direct outbound internet traffic from your private subnets through your VPN connection or Direct Connect connection. This way, you can route cloud resources to the internet through your on-premises data center instead of using an internet gateway.

References: 1:

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html> 2:

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-transit-virtual-interfaces.html> 3: <https://docs.aws.amazon.com/vpc/latest/tgw/what-is-transit-gateway.html> :

[https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_Internet\\_Gateway.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html) : <https://docs.aws.amazon.com/vpc/latest/tgw/tgw-sharing.html> : <https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html> : [https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_Scenario2.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html) :

[https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_Scenario3.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario3.html) : [https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_NAT\\_Instance.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_NAT_Instance.html) :

[https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_NAT\\_Gateway.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_NAT_Gateway.html)

#### NEW QUESTION 10

- (Exam Topic 1)

A company is running an application in the AWS Cloud. The application runs on containers in an Amazon Elastic Container Service (Amazon ECS) cluster. The ECS tasks use the Fargate launch type. The application's data is relational and is stored in Amazon Aurora MySQL. To meet regulatory requirements, the application must be able to recover to a separate AWS Region in the event of an application failure. In case of a failure, no data can be lost. Which solution will meet these requirements with the LEAST amount of operational overhead?

- A. Provision an Aurora Replica in a different Region.
- B. Set up AWS DataSync for continuous replication of the data to a different Region.
- C. Set up AWS Database Migration Service (AWS DMS) to perform a continuous replication of the data to a different Region.
- D. Use Amazon Data Lifecycle Manager (Amazon DLM) to schedule a snapshot every 5 minutes.

**Answer:** A

#### Explanation:

Provision an Aurora Replica in a different Region will meet the requirement of the application being able to recover to a separate AWS Region in the event of an application failure, and no data can be lost, with the least amount of operational overhead.

#### NEW QUESTION 12

- (Exam Topic 1)

A company has an application that runs on Amazon EC2 instances. A solutions architect is designing VPC infrastructure in an AWS Region where the application needs to access an Amazon Aurora DB cluster. The EC2 instances are all associated with the same security group. The DB cluster is associated with its own security group.

The solutions architect needs to add rules to the security groups to provide the application with least privilege access to the DB cluster.

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

- A. Add an inbound rule to the EC2 instances' security group
- B. Specify the DB cluster's security group as the source over the default Aurora port.
- C. Add an outbound rule to the EC2 instances' security group
- D. Specify the DB cluster's security group as the destination over the default Aurora port.
- E. Add an inbound rule to the DB cluster's security group
- F. Specify the EC2 instances' security group as the source over the default Aurora port.
- G. Add an outbound rule to the DB cluster's security group
- H. Specify the EC2 instances' security group as the destination over the default Aurora port.
- I. Add an outbound rule to the DB cluster's security group
- J. Specify the EC2 instances' security group as the destination over the ephemeral ports.

**Answer:** AB

#### Explanation:

\* B. Add an outbound rule to the EC2 instances' security group. Specify the DB cluster's security group as the destination over the default Aurora port. This allows the instances to make outbound connections to the DB cluster on the default Aurora port. C. Add an inbound rule to the DB cluster's security group. Specify the EC2 instances' security group as the source over the default Aurora port. This allows connections to the DB cluster from the EC2 instances on the default Aurora port.

#### NEW QUESTION 14

- (Exam Topic 1)

A solutions architect has developed a web application that uses an Amazon API Gateway Regional endpoint and an AWS Lambda function. The consumers of the web application are all close to the AWS Region where the application will be deployed. The Lambda function only queries an Amazon Aurora MySQL database. The solutions architect has configured the database to have three read replicas.

During testing, the application does not meet performance requirements. Under high load, the application opens a large number of database connections. The solutions architect must improve the application's performance.

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

- A. Use the cluster endpoint of the Aurora database.
- B. Use RDS Proxy to set up a connection pool to the reader endpoint of the Aurora database.
- C. Use the Lambda Provisioned Concurrency feature.
- D. Move the code for opening the database connection in the Lambda function outside of the event handler.
- E. Change the API Gateway endpoint to an edge-optimized endpoint.

**Answer:** BD

#### Explanation:

Connect to RDS outside of Lambda handler method to improve performance <https://awstut.com/en/2022/04/30/connect-to-rds-outside-of-lambda-handler-method-to-improve-performance-en>

Using RDS Proxy, you can handle unpredictable surges in database traffic. Otherwise, these surges might cause issues due to oversubscribing connections or creating new connections at a fast rate. RDS Proxy establishes a database connection pool and reuses connections in this pool. This approach avoids the memory

and CPU overhead of opening a new database connection each time. To protect the database against oversubscription, you can control the number of database connections that are created. <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html>

**NEW QUESTION 17**

- (Exam Topic 1)

A company gives users the ability to upload images from a custom application. The upload process invokes an AWS Lambda function that processes and stores the image in an Amazon S3 bucket. The application invokes the Lambda function by using a specific function version ARN.

The Lambda function accepts image processing parameters by using environment variables. The company often adjusts the environment variables of the Lambda function to achieve optimal image processing output. The company tests different parameters and publishes a new function version with the updated environment variables after validating results. This update process also requires frequent changes to the custom application to invoke the new function version ARN. These changes cause interruptions for users.

A solutions architect needs to simplify this process to minimize disruption to users. Which solution will meet these requirements with the LEAST operational overhead?

- A. Directly modify the environment variables of the published Lambda function version
- B. Use the LATEST version to test image processing parameters.
- C. Create an Amazon DynamoDB table to store the image processing parameter
- D. Modify the Lambda function to retrieve the image processing parameters from the DynamoDB table.
- E. Directly code the image processing parameters within the Lambda function and remove the environment variable
- F. Publish a new function version when the company updates the parameters.
- G. Create a Lambda function alias
- H. Modify the client application to use the function alias ARN
- I. Reconfigure the Lambda alias to point to new versions of the function when the company finishes testing.

**Answer: D**

**Explanation:**

A Lambda function alias allows you to point to a specific version of a function and also can be updated to point to a new version of the function without modifying the client application. This way, the company can test different versions of the function with different environment variables and, once the optimal parameters are found, update the alias to point to the new version, without the need to update the client application.

By using this approach, the company can simplify the process of updating the environment variables, minimize disruption to users, and reduce the operational overhead.

Reference:

AWS Lambda documentation: <https://aws.amazon.com/lambda/>

AWS Lambda Aliases documentation: <https://docs.aws.amazon.com/lambda/latest/dg/aliases-intro.html> AWS Lambda versioning and aliases documentation:

<https://aws.amazon.com/blogs/compute/versioning-aliases-in-aws-lambda/>

**NEW QUESTION 22**

- (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 account
- 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 role
- E. Assign a unique external ID to the role's trust policy.
- F. In the company's AWS account, create an IAM user
- G. Attach the required IAM policies to the IAM user. Create API access keys for the IAM user
- 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 auditor
- 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 27**

- (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 protocol
- 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 source
- D. Enable automatic provisioning by using the System for Cross-domain Identity Management (SCIM) v2.0 protocol
- 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 provider



- 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 32**

- (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 33**

- (Exam Topic 1)

A company that uses AWS Organizations allows developers to experiment on AWS. As part of the landing zone that the company has deployed, developers use their company email address to request an account. The company wants to ensure that developers are not launching costly services or running services unnecessarily. The company must give developers a fixed monthly budget to limit their AWS costs.

Which combination of steps will meet these requirements? (Choose three.)

- A. Create an SCP to set a fixed monthly account usage limit
- B. Apply the SCP to the developer accounts.
- C. Use AWS Budgets to create a fixed monthly budget for each developer's account as part of the account creation process.
- D. Create an SCP to deny access to costly services and components
- E. Apply the SCP to the developer accounts.
- F. Create an IAM policy to deny access to costly services and components
- G. Apply the IAM policy to the developer accounts.
- H. Create an AWS Budgets alert action to terminate services when the budgeted amount is reached. Configure the action to terminate all services.
- I. Create an AWS Budgets alert action to send an Amazon Simple Notification Service (Amazon SNS) notification when the budgeted amount is reached
- J. Invoke an AWS Lambda function to terminate all services.

**Answer:** BCF

**Explanation:**

- Option A is incorrect because creating an SCP to set a fixed monthly account usage limit is not possible. SCPs are policies that specify the services and actions that users and roles can use in the member accounts of an AWS Organization. SCPs cannot enforce budget limits or prevent users from launching costly services or running services unnecessarily
- Option B is correct because using AWS Budgets to create a fixed monthly budget for each developer's account as part of the account creation process meets the requirement of giving developers a fixed monthly budget to limit their AWS costs. AWS Budgets allows you to plan your service usage, service costs, and instance reservations. You can create budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount
- Option C is correct because creating an SCP to deny access to costly services and components meets the requirement of ensuring that developers are not launching costly services or running services unnecessarily. SCPs can restrict access to certain AWS services or actions based on conditions such as region, resource tags, or request time. For example, an SCP can deny access to Amazon Redshift clusters or Amazon EC2 instances with certain instance types
- Option D is incorrect because creating an IAM policy to deny access to costly services and components is not sufficient to meet the requirement of ensuring that developers are not launching costly services or running services unnecessarily. IAM policies can only control access to resources within a single AWS account. If developers have multiple accounts or can create new accounts, they can bypass the IAM policy restrictions. SCPs can apply across multiple accounts within an AWS Organization and prevent users from creating new accounts that do not comply with the SCP rules
- Option E is incorrect because creating an AWS Budgets alert action to terminate services when the budgeted amount is reached is not possible. AWS Budgets alert actions can only perform one of the following actions: apply an IAM policy, apply an SCP, or send a notification through Amazon SNS. AWS Budgets alert actions cannot terminate services directly.
- Option F is correct because creating an AWS Budgets alert action to send an Amazon SNS notification when the budgeted amount is reached and invoking an AWS Lambda function to terminate all services meets the requirement of giving developers a fixed monthly budget to limit their AWS costs. AWS Budgets alert actions can send notifications through Amazon SNS when a budget threshold is breached. Amazon SNS can trigger an AWS Lambda function that can perform



custom logic such as terminating all services in the developer's account. This way, developers cannot exceed their budget limit and incur additional costs.

References: 1: [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) 2

: <https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/budgets-create.html> 3: <https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html> :

<https://docs.aws.amazon.com/cost-management/latest/userguide/budgets-actions.html> : <https://docs.aws.amazon.com/sns/latest/dg/sns-lambda.html> :

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

#### NEW QUESTION 34

- (Exam Topic 1)

A company's solutions architect is reviewing a new internally developed application in a sandbox AWS account. The application uses an AWS Auto Scaling group of Amazon EC2 instances that have an IAM instance profile attached. Part of the application logic creates and accesses secrets from AWS Secrets Manager. The company has an AWS Lambda function that calls the application API to test the functionality. The company also has created an AWS CloudTrail trail in the account. The application's developer has attached the `SecretsManagerReadWnte` AWS managed IAM policy to an IAM role. The IAM role is associated with the instance profile that is attached to the EC2 instances. The solutions architect has invoked the Lambda function for testing. The solutions architect must replace the `SecretsManagerReadWnte` policy with a new policy that provides least privilege access to the Secrets Manager actions that the application requires.

What is the MOST operationally efficient solution that meets these requirements?

- A. Generate a policy based on CloudTrail events for the IAM role. Use the generated policy output to create a new IAM policy. Use the newly generated IAM policy to replace the `SecretsManagerReadWnte` policy that is attached to the IAM role.
- B. Create an analyzer in AWS Identity and Access Management Access Analyzer. Use the IAM role's Access Advisor findings to create a new IAM policy. Use the newly created IAM policy to replace the `SecretsManagerReadWnte` policy that is attached to the IAM role.
- C. Use the `aws cloudtrail lookup-events` AWS CLI command to filter and export CloudTrail events that are related to Secrets Manager. Use a new IAM policy that contains the actions from CloudTrail to replace the `SecretsManagerReadWnte` policy that is attached to the IAM role.
- D. Use the IAM policy simulator to generate an IAM policy for the IAM role. Use the newly generated IAM policy to replace the `SecretsManagerReadWnte` policy that is attached to the IAM role.

**Answer:** B

#### Explanation:

The IAM policy simulator will generate a policy that contains only the necessary permissions for the application to access Secrets Manager, providing the least privilege necessary to get the job done. This is the most efficient solution as it will not require additional steps such as analyzing CloudTrail events or manually creating and testing an IAM policy.

You can use the IAM policy simulator to generate an IAM policy for an IAM role by specifying the role and the API actions and resources that the application or service requires. The simulator will then generate an IAM policy that grants the least privilege access to those actions and resources.

Once you have generated an IAM policy using the simulator, you can replace the existing `SecretsManagerReadWnte` policy that is attached to the IAM role with the newly generated policy. This will ensure that the application or service has the least privilege access to the Secrets Manager actions that it requires.

You can access the IAM policy simulator through the IAM console, AWS CLI, and AWS SDKs. Here is the link for more information:

[https://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies\\_simulator.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_simulator.html)

#### NEW QUESTION 35

- (Exam Topic 1)

A company is hosting a critical application on a single Amazon EC2 instance. The application uses an Amazon ElastiCache for Redis single-node cluster for an in-memory data store. The application uses an Amazon RDS for MariaDB DB instance for a relational database. For the application to function, each piece of the infrastructure must be healthy and must be in an active state.

A solutions architect needs to improve the application's architecture so that the infrastructure can automatically recover from failure with the least possible downtime.

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

- A. Use an Elastic Load Balancer to distribute traffic across multiple EC2 instances.
- B. Ensure that the EC2 instances are part of an Auto Scaling group that has a minimum capacity of two instances.
- C. Use an Elastic Load Balancer to distribute traffic across multiple EC2 instances. Ensure that the EC2 instances are configured in unlimited mode.
- D. Modify the DB instance to create a read replica in the same Availability Zone.
- E. Promote the read replica to be the primary DB instance in failure scenarios.
- F. Modify the DB instance to create a Multi-AZ deployment that extends across two Availability Zones.
- G. Create a replication group for the ElastiCache for Redis cluster.
- H. Configure the cluster to use an Auto Scaling group that has a minimum capacity of two instances.
- I. Create a replication group for the ElastiCache for Redis cluster.
- J. Enable Multi-AZ on the cluster.

**Answer:** ADF

#### Explanation:

➤ Option A is correct because using an Elastic Load Balancer and an Auto Scaling group with a minimum capacity of two instances can improve the availability and scalability of the EC2 instances that host the application. The load balancer can distribute traffic across multiple instances and the Auto Scaling group can replace any unhealthy instances automatically.

➤ Option D is correct because modifying the DB instance to create a Multi-AZ deployment that extends across two Availability Zones can improve the availability and durability of the RDS for MariaDB database. Multi-AZ deployments provide enhanced data protection and minimize downtime by automatically failing over to a standby replica in another Availability Zone in case of a planned or unplanned outage.

➤ Option F is correct because creating a replication group for the ElastiCache for Redis cluster and enabling Multi-AZ on the cluster can improve the availability and fault tolerance of the in-memory data store. A replication group consists of a primary node and up to five read-only replica nodes that are synchronized with the primary node using asynchronous replication. Multi-AZ allows automatic failover to one of the replicas if the primary node fails or becomes unreachable.

References: 1:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/how-elastic-load-balancing-works.html> 2:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/burstable-performance-instances-unlimited-mode.htm> 3:

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_ReadRepl.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html) 4:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html> 5:

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/AutoScaling.html> 6: <https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/Replication.Redis.Groups.html>

**NEW QUESTION 39**

- (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 41**

- (Exam Topic 1)

A financial services company in North America plans to release a new online web application to its customers on AWS . The company will launch the application in the us-east-1 Region on Amazon EC2 instances. The application must be highly available and must dynamically scale to meet user traffic. The company also wants to implement a disaster recovery environment for the application in the us-west-1 Region by using active-passive failover. Which solution will meet these requirements?

- A. Create a VPC in us-east-1 and a VPC in us-west-1 Configure VPC peering In the us-east-1 VP
- B. create an Application Load Balancer (ALB) that extends across multiple Availability Zones in both VPCs Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in both VPCs Place the Auto Scaling group behind the ALB.
- C. Create a VPC in us-east-1 and a VPC in us-west-1. In the us-east-1 VP
- D. create an Application Load Balancer (ALB) that extends across multiple Availability Zones in that VP
- E. Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in the us-east-1 VPC Place the Auto Scaling group behind the ALB Set up the same configuration in the us-west-1 VP
- F. Create an Amazon Route 53 hosted zone Create separate records for each ALB Enable health checks to ensure high availability between Regions.
- G. Create a VPC in us-east-1 and a VPC in us-west-1 In the us-east-1 VP
- H. create an Application Load Balancer (ALB) that extends across multiple Availability Zones in that VPC Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in the us-east-1 VPC Place the Auto Scaling group behind the ALB Set up the same configuration in the us-west-1 VPC Create an Amazon Route 53 hosted zon
- I. Create separate records for each ALB Enable health checks and configure a failover routing policy for each record.
- J. Create a VPC in us-east-1 and a VPC in us-west-1 Configure VPC peering In the us-east-1 VP
- K. create an Application Load Balancer (ALB) that extends across multiple Availability Zones in Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in both VPCs Place the Auto Scaling group behind the ALB Create an Amazon Route 53 host.. Create a record for the ALB.

**Answer:** C

**Explanation:**

it's the one that handles failover while B (the one shown as the answer today) it almost the same but does not handle failover.

**NEW QUESTION 46**

- (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 lo 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 m Account B Configure Route 53 replication between AWS accounts
- E. Associate a new VPC in Account B with a hosted zone in Account
- 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 50

- (Exam Topic 1)

A company has a multi-tier web application that runs on a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are in an Auto Scaling group. The ALB and the Auto Scaling group are replicated in a backup AWS Region. The minimum value and the maximum value for the Auto Scaling group are set to zero. An Amazon RDS Multi-AZ DB instance stores the application's data. The DB instance has a read replica in the backup Region. The application presents an endpoint to end users by using an Amazon Route 53 record.

The company needs to reduce its RTO to less than 15 minutes by giving the application the ability to automatically fail over to the backup Region. The company does not have a large enough budget for an active-active strategy.

What should a solutions architect recommend to meet these requirements?

- A. Reconfigure the application's Route 53 record with a latency-based routing policy that load balances traffic between the two ALB
- B. Create an AWS Lambda function in the backup Region to promote the read replica and modify the Auto Scaling group value
- C. Create an Amazon CloudWatch alarm that is based on the HTTPCode\_Target\_5XX\_Count metric for the ALB in the primary Region
- D. Configure the CloudWatch alarm to invoke the Lambda function.
- E. Create an AWS Lambda function in the backup Region to promote the read replica and modify the Auto Scaling group value
- F. Configure Route 53 with a health check that monitors the web application and sends an Amazon Simple Notification Service (Amazon SNS) notification to the Lambda function when the health check status is unhealthy
- G. Update the application's Route 53 record with a failover policy that routes traffic to the ALB in the backup Region when a health check failure occurs.
- H. Configure the Auto Scaling group in the backup Region to have the same values as the Auto Scaling group in the primary Region
- I. Reconfigure the application's Route 53 record with a latency-based routing policy that load balances traffic between the two ALB
- J. Remove the read replica
- K. Replace the read replica with a standalone RDS DB instance
- L. Configure Cross-Region Replication between the RDS DB instances by using snapshots and Amazon S3.
- M. Configure an endpoint in AWS Global Accelerator with the two ALBs as equal weighted targets
- N. Create an AWS Lambda function in the backup Region to promote the read replica and modify the Auto Scaling group value
- O. Create an Amazon CloudWatch alarm that is based on the HTTPCode\_Target\_5XX\_Count metric for the ALB in the primary Region
- P. Configure the CloudWatch alarm to invoke the Lambda function.

**Answer: B**

#### Explanation:

an AWS Lambda function in the backup region to promote the read replica and modify the Auto Scaling group values, and then configuring Route 53 with a health check that monitors the web application and sends an Amazon SNS notification to the Lambda function when the health check status is unhealthy. Finally, the application's Route 53 record should be updated with a failover policy that routes traffic to the ALB in the backup region when a health check failure occurs. This approach provides automatic failover to the backup region when a health check failure occurs, reducing the RTO to less than 15 minutes. Additionally, this approach is cost-effective as it does not require an active-active strategy.

### NEW QUESTION 52

- (Exam Topic 1)

A company is using Amazon OpenSearch Service to analyze data. The company loads data into an OpenSearch Service cluster with 10 data nodes from an Amazon S3 bucket that uses S3 Standard storage. The data resides in the cluster for 1 month for read-only analysis. After 1 month, the company deletes the index that contains the data from the cluster. For compliance purposes, the company must retain a copy of all input data.

The company is concerned about ongoing costs and asks a solutions architect to recommend a new solution. Which solution will meet these requirements MOST cost-effectively?

- A. Replace all the data nodes with UltraWarm nodes to handle the expected capacity
- B. Transition the input data from S3 Standard to S3 Glacier Deep Archive when the company loads the data into the cluster.
- C. Reduce the number of data nodes in the cluster to 2. Add UltraWarm nodes to handle the expected capacity
- D. Configure the indexes to transition to UltraWarm when OpenSearch Service ingests the data
- E. Transition the input data to S3 Glacier Deep Archive after 1 month by using an S3 Lifecycle policy.
- F. Reduce the number of data nodes in the cluster to 2. Add UltraWarm nodes to handle the expected capacity
- G. Configure the indexes to transition to UltraWarm when OpenSearch Service ingests the data
- H. Add cold storage nodes to the cluster. Transition the indexes from UltraWarm to cold storage
- I. Delete the input data from the S3 bucket after 1 month by using an S3 Lifecycle policy.
- J. Reduce the number of data nodes in the cluster to 2. Add instance-backed data nodes to handle the expected capacity
- K. Transition the input data from S3 Standard to S3 Glacier Deep Archive when the company loads the data into the cluster.

**Answer: B**

#### Explanation:

By reducing the number of data nodes in the cluster to 2 and adding UltraWarm nodes to handle the expected capacity, the company can reduce the cost of running the cluster. Additionally, configuring the indexes to transition to UltraWarm when OpenSearch Service ingests the data will ensure that the data is stored in the most cost-effective manner. Finally, transitioning the input data to S3 Glacier Deep Archive after 1 month by using an S3 Lifecycle policy will ensure that the data is retained for compliance purposes, while also reducing the ongoing costs.

### NEW QUESTION 57

- (Exam Topic 1)

An AWS customer has a web application that runs on premises. The web application fetches data from a third-party API that is behind a firewall. The third party accepts only one public CIDR block in each client's allow list.

The customer wants to migrate their web application to the AWS Cloud. The application will be hosted on a set of Amazon EC2 instances behind an Application Load Balancer (ALB) in a VPC. The ALB is located in public subnets. The EC2 instances are located in private subnets. NAT gateways provide internet access to the private subnets.

How should a solutions architect ensure that the web application can continue to call the third-party API after the migration?

- A. Associate a block of customer-owned public IP addresses to the VPC
- B. Enable public IP addressing for public subnets in the VPC.
- C. Register a block of customer-owned public IP addresses in the AWS account
- D. Create Elastic IP addresses from the address block and assign them to the NAT gateways in the VPC.



- E. Create Elastic IP addresses from the block of customer-owned IP addresses
- F. Assign the static Elastic IP addresses to the ALB.
- G. Register a block of customer-owned public IP addresses in the AWS account
- H. Set up AWS Global Accelerator to use Elastic IP addresses from the address block
- I. Set the ALB as the accelerator endpoint.

**Answer:** B

**Explanation:**

When EC2 instances reach third-party API through internet, their private IP addresses will be masked by NAT Gateway public IP address.  
<https://aws.amazon.com/blogs/networking-and-content-delivery/introducing-bring-your-own-ip-byoip-for-amaz>

**NEW QUESTION 60**

- (Exam Topic 1)

A retail company has an on-premises data center in Europe. The company also has a multi-Region AWS presence that includes the eu-west-1 and us-east-1 Regions. The company wants to be able to route network traffic from its on-premises infrastructure into VPCs in either of those Regions. The company also needs to support traffic that is routed directly between VPCs in those Regions. No single points of failure can exist on the network. The company already has created two 1 Gbps AWS Direct Connect connections from its on-premises data center. Each connection goes into a separate Direct Connect location in Europe for high availability. These two locations are named DX-A and DX-B, respectively. Each Region has a single AWS Transit Gateway that is configured to route all inter-VPC traffic within that Region. Which solution will meet these requirements?

- A. Create a private VIF from the DX-A connection into a Direct Connect gateway
- B. Create a private VIF from the DX-B connection into the same Direct Connect gateway for high availability
- C. Associate both the eu-west-1 and us-east-1 transit gateways with the Direct Connect gateway
- D. Peer the transit gateways with each other to support cross-Region routing.
- E. Create a transit VIF from the DX-A connection into a Direct Connect gateway
- F. Associate the eu-west-1 transit gateway with this Direct Connect gateway
- G. Create a transit VIF from the DX-B connection into a separate Direct Connect gateway
- H. Associate the us-east-1 transit gateway with this separate Direct Connect gateway
- I. Peer the Direct Connect gateways with each other to support high availability and cross-Region routing.
- J. Create a transit VIF from the DX-A connection into a Direct Connect gateway
- K. Create a transit VIF from the DX-B connection into the same Direct Connect gateway for high availability
- L. Associate both the eu-west-1 and us-east-1 transit gateways with this Direct Connect gateway
- M. Configure the Direct Connect gateway to route traffic between the transit gateways.
- N. Create a transit VIF from the DX-A connection into a Direct Connect gateway
- O. Create a transit VIF from the DX-B connection into the same Direct Connect gateway for high availability
- P. Associate both the eu-west-1 and us-east-1 transit gateways with this Direct Connect gateway
- Q. Peer the transit gateways with each other to support cross-Region routing.

**Answer:** D

**Explanation:**

In this solution, two transit VIFs are created - one from the DX-A connection and one from the DX-B connection - into the same Direct Connect gateway for high availability. Both the eu-west-1 and us-east-1 transit gateways are then associated with this Direct Connect gateway. The transit gateways are then peered with each other to support cross-Region routing. This solution meets the requirements of the company by creating a highly available connection between the on-premises data center and the VPCs in both the eu-west-1 and us-east-1 regions, and by enabling direct traffic routing between VPCs in those regions.

**NEW QUESTION 62**

- (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:Region:Account:key/Key ID"
    }
  ]
}
```

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. kmsGetKeyPolpcy
- C. kmsGetPubKKey
- D. kms:SKjn

**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 64**

- (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 company is planning to migrate 1,000 on-premises servers to AWS. The servers run on several VMware clusters in the company's data center. As part of the migration plan, the company wants to gather server metrics such as CPU details, RAM usage, operating system information, and running processes. The company then wants to query and analyze the data.

Which solution will meet these requirements?

- A. Deploy and configure the AWS Agentless Discovery Connector virtual appliance on the on-premises host
- B. Configure Data Exploration in AWS Migration Hub
- C. Use AWS Glue to perform an ETL job against the data
- D. Query the data by using Amazon S3 Select.
- E. Export only the VM performance information from the on-premises host
- F. Directly import the required data into AWS Migration Hub
- G. Update any missing information in Migration Hub
- H. Query the data by using Amazon QuickSight.
- I. Create a script to automatically gather the server information from the on-premises host
- J. Use the AWS CLI to run the put-resource-attributes command to store the detailed server data in AWS Migration Hub
- K. Query the data directly in the Migration Hub console.
- L. Deploy the AWS Application Discovery Agent to each on-premises server
- M. Configure Data Exploration in AWS Migration Hub
- N. Use Amazon Athena to run predefined queries against the data in Amazon S3.

**Answer:** D

**Explanation:**

➤ it covers all the requirements mentioned in the question, it will allow collecting the detailed metrics, including process information and it provides a way to query and analyze the data using Amazon Athena.

**NEW QUESTION 70**

- (Exam Topic 1)

A company has an asynchronous HTTP application that is hosted as an AWS Lambda function. A public Amazon API Gateway endpoint invokes the Lambda function. The Lambda function and the API Gateway endpoint reside in the us-east-1 Region. A solutions architect needs to redesign the application to support failover to another AWS Region.

Which solution will meet these requirements?

- A. Create an API Gateway endpoint in the us-west-2 Region to direct traffic to the Lambda function in us-east-1. Configure Amazon Route 53 to use a failover routing policy to route traffic for the two API Gateway endpoints.
- B. Create an Amazon Simple Queue Service (Amazon SQS) queue
- C. Configure API Gateway to direct traffic to the SQS queue instead of to the Lambda function
- D. Configure the Lambda function to pull messages from the queue for processing.
- E. Deploy the Lambda function to the us-west-2 Region
- F. Create an API Gateway endpoint in us-west-2 to direct traffic to the Lambda function in us-west-2. Configure AWS Global Accelerator and an Application Load Balancer to manage traffic across the two API Gateway endpoints.
- G. Deploy the Lambda function and an API Gateway endpoint to the us-west-2 Region
- H. Configure Amazon Route 53 to use a failover routing policy to route traffic for the two API Gateway endpoints.

**Answer: B**

**Explanation:**

This solution allows for deploying the Lambda function and API Gateway endpoint to another region, providing a failover option in case of any issues in the primary region. Using Route 53's failover routing policy allows for automatic routing of traffic to the healthy endpoint, ensuring that the application is available even in case of issues in one region. This solution provides a cost-effective and simple way to implement failover while minimizing operational overhead.

**NEW QUESTION 75**

- (Exam Topic 1)

A company is running several workloads in a single AWS account. A new company policy states that engineers can provision only approved resources and that engineers must use AWS CloudFormation to provision these resources. A solutions architect needs to create a solution to enforce the new restriction on the IAM role that the engineers use for access.

What should the solutions architect do to create the solution?

- A. Upload AWS CloudFormation templates that contain approved resources to an Amazon S3 bucket. Update the IAM policy for the engineers' IAM role to only allow access to Amazon S3 and AWS CloudFormation
- B. Use AWS CloudFormation templates to provision resources.
- C. Update the IAM policy for the engineers' IAM role with permissions to only allow provisioning of approved resources and AWS CloudFormation
- D. Use AWS CloudFormation templates to create stacks with approved resources.
- E. Update the IAM policy for the engineers' IAM role with permissions to only allow AWS CloudFormation action
- F. Create a new IAM policy with permission to provision approved resources, and assign the policy to a new IAM service role
- G. Assign the IAM service role to AWS CloudFormation during stack creation.
- H. Provision resources in AWS CloudFormation stack
- I. Update the IAM policy for the engineers' IAM role to only allow access to their own AWS CloudFormation stack.

**Answer: B**

**Explanation:**

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/security-best-practices.html#use-iam-to-c>  
<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-iam-servicerole.html>

**NEW QUESTION 77**

- (Exam Topic 1)

A company needs to implement a patching process for its servers. The on-premises servers and Amazon EC2 instances use a variety of tools to perform patching. Management requires a single report showing the patch status of all the servers and instances.

Which set of actions should a solutions architect take to meet these requirements?

- A. Use AWS Systems Manager to manage patches on the on-premises servers and EC2 instance
- B. Use Systems Manager to generate patch compliance reports.
- C. Use AWS OpsWorks to manage patches on the on-premises servers and EC2 instance
- D. Use Amazon QuickSight integration with OpsWorks to generate patch compliance reports.
- E. Use an Amazon EventBridge (Amazon CloudWatch Events) rule to apply patches by scheduling an AWS Systems Manager patch remediation job
- F. Use Amazon Inspector to generate patch compliance reports.
- G. Use AWS OpsWorks to manage patches on the on-premises servers and EC2 instance
- H. Use AWS X-Ray to post the patch status to AWS Systems Manager OpsCenter to generate patch compliance reports.

**Answer: A**

**Explanation:**

<https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html>

**NEW QUESTION 78**

- (Exam Topic 1)

A company is planning to store a large number of archived documents and make the documents available to employees through the corporate intranet. Employees will access the system by connecting through a client VPN service that is attached to a VPC. The data must not be accessible to the public.

The documents that the company is storing are copies of data that is held on physical media elsewhere. The number of requests will be low. Availability and speed of retrieval are not concerns of the company.



Which solution will meet these requirements at the LOWEST cost?

- A. Create an Amazon S3 bucket
- B. Configure the S3 bucket to use the S3 One Zone-Infrequent Access (S3 One Zone-IA) storage class as default
- C. Configure the S3 bucket for website hosting
- D. Create an S3 interface endpoint
- E. Configure the S3 bucket to allow access only through that endpoint.
- F. Launch an Amazon EC2 instance that runs a web server
- G. Attach an Amazon Elastic File System (Amazon EFS) file system to store the archived data in the EFS One Zone-Infrequent Access (EFS One Zone-IA) storage class. Configure the instance security groups to allow access only from private networks.
- H. Launch an Amazon EC2 instance that runs a web server. Attach an Amazon Elastic Block Store (Amazon EBS) volume to store the archived data.
- I. Use the Cold HDD (sc1) volume type
- J. Configure the instance security groups to allow access only from private networks.
- K. Create an Amazon S3 bucket
- L. Configure the S3 bucket to use the S3 Glacier Deep Archive storage class as default
- M. Configure the S3 bucket for website hosting
- N. Create an S3 interface endpoint
- O. Configure the S3 bucket to allow access only through that endpoint.

**Answer:** D

**Explanation:**

The S3 Glacier Deep Archive storage class is the lowest-cost storage class offered by Amazon S3, and it is designed for archival data that is accessed infrequently and for which retrieval time of several hours is acceptable. S3 interface endpoint for the VPC ensures that access to the bucket is only from resources within the VPC and this will meet the requirement of not being accessible to the public. And also, S3 bucket can be configured for website hosting, and this will allow employees to access the documents through the corporate intranet. Using an EC2 instance and a file system or block store would be more expensive and unnecessary because the number of requests to the data will be low and availability and speed of retrieval are not concerns. Additionally, using Amazon S3 bucket will provide durability, scalability and availability of data.

**NEW QUESTION 82**

- (Exam Topic 1)

A company is storing data on premises on a Windows file server. The company produces 5 GB of new data daily.

The company migrated part of its Windows-based workload to AWS and needs the data to be available on a file system in the cloud. The company already has established an AWS Direct Connect connection between the on-premises network and AWS.

Which data migration strategy should the company use?

- A. Use the file gateway option in AWS Storage Gateway to replace the existing Windows file server, and point the existing file share to the new file gateway.
- B. Use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows file server and Amazon FSx.
- C. Use AWS Data Pipeline to schedule a daily task to replicate data between the on-premises Windows file server and Amazon Elastic File System (Amazon EFS).
- D. Use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows file server and Amazon Elastic File System (Amazon EFS).

**Answer:** B

**Explanation:**

<https://aws.amazon.com/storagegateway/file/>

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/migrate-files-to-fsx-datasync.html> <https://docs.aws.amazon.com/systems-manager/latest/userguide/prereqs-operating-systems.html#prereqs-os-win>

**NEW QUESTION 86**

- (Exam Topic 1)

A company has many AWS accounts and uses AWS Organizations to manage all of them. A solutions architect must implement a solution that the company can use to share a common network across multiple accounts.

The company's infrastructure team has a dedicated infrastructure account that has a VPC. The infrastructure team must use this account to manage the network. Individual accounts cannot have the ability to manage their own networks. However, individual accounts must be able to create AWS resources within subnets.

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

- A. Create a transit gateway in the infrastructure account.
- B. Enable resource sharing from the AWS Organizations management account.
- C. Create VPCs in each AWS account within the organization in AWS Organization
- D. Configure the VPCs to share the same CIDR range and subnets as the VPC in the infrastructure account
- E. Peer the VPCs in each individual account with the VPC in the infrastructure account.
- F. Create a resource share in AWS Resource Access Manager in the infrastructure account
- G. Select the specific AWS Organizations OU that will use the shared network
- H. Select each subnet to associate with the resource share.
- I. Create a resource share in AWS Resource Access Manager in the infrastructure account
- J. Select the specific AWS Organizations OU that will use the shared network
- K. Select each prefix list to associate with the resource share.

**Answer:** AE

**Explanation:**

<https://docs.aws.amazon.com/vpc/latest/userguide/sharing-managed-prefix-lists.html>

**NEW QUESTION 88**

- (Exam Topic 1)

A company is storing data in several Amazon DynamoDB tables. A solutions architect must use a serverless architecture to make the data accessible publicly through a simple API over HTTPS. The solution must scale automatically in response to demand.

Which solutions meet these requirements? (Choose two.)

- A. Create an Amazon API Gateway REST AP
- B. Configure this API with direct integrations to DynamoDB by using API Gateway's AWS integration type.
- C. Create an Amazon API Gateway HTTP AP
- D. Configure this API with direct integrations to Dynamo DB by using API Gateway's AWS integration type.
- E. Create an Amazon API Gateway HTTP AP
- F. Configure this API with integrations to AWS Lambda functions that return data from the DynamoDB tables.
- G. Create an accelerator in AWS Global Accelerato
- H. Configure this accelerator with AWS Lambda@Edge function integrations that return data from the DynamoDB tables.
- I. Create a Network Load Balance
- J. Configure listener rules to forward requests to the appropriate AWS Lambda functions

**Answer:** AC

**Explanation:**

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-overview-developer-experience.htm>

**NEW QUESTION 91**

- (Exam Topic 1)

A video processing company has an application that downloads images from an Amazon S3 bucket, processes the images, stores a transformed image in a second S3 bucket, and updates metadata about the image in an Amazon DynamoDB table. The application is written in Node.js and runs by using an AWS Lambda function. The Lambda function is invoked when a new image is uploaded to Amazon S3.

The application ran without incident for a while. However, the size of the images has grown significantly. The Lambda function is now failing frequently with timeout errors. The function timeout is set to its maximum value. A solutions architect needs to refactor the application's architecture to prevent invocation failures. The company does not want to manage the underlying infrastructure.

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

- A. Modify the application deployment by building a Docker image that contains the application code. Publish the image to Amazon Elastic Container Registry (Amazon ECR).
- B. Create a new Amazon Elastic Container Service (Amazon ECS) task definition with a compatibility type of AWS Fargat
- C. Configure the task definition to use the new image in Amazon Elastic Container Registry (Amazon ECR). Adjust the Lambda function to invoke an ECS task by using the ECS task definition when a new file arrives in Amazon S3.
- D. Create an AWS Step Functions state machine with a Parallel state to invoke the Lambda function. Increase the provisioned concurrency of the Lambda function.
- E. Create a new Amazon Elastic Container Service (Amazon ECS) task definition with a compatibility type of Amazon EC2. Configure the task definition to use the new image in Amazon Elastic Container Registry (Amazon ECR). Adjust the Lambda function to invoke an ECS task by using the ECS task definition when a new file arrives in Amazon S3.
- F. Modify the application to store images on Amazon Elastic File System (Amazon EFS) and to store metadata on an Amazon RDS DB instanc
- G. Adjust the Lambda function to mount the EFS file share.

**Answer:** AB

**Explanation:**

A. Modify the application deployment by building a Docker image that contains the application code. Publish the image to Amazon Elastic Container Registry (Amazon ECR). - This step is necessary to package the application code in a container and make it available for running on ECS. B. Create a new Amazon Elastic Container Service (Amazon ECS) task definition with a compatibility type of AWS Fargate. Configure the task definition to use the new image in Amazon Elastic Container Registry (Amazon ECR). Adjust the Lambda function to invoke an ECS task by using the ECS task definition when a new file arrives in Amazon S3.

**NEW QUESTION 94**

- (Exam Topic 1)

A company has an organization that has many AWS accounts in AWS Organizations. A solutions architect must improve how the company manages common security group rules for the AWS accounts in the organization.

The company has a common set of IP CIDR ranges in an allow list in each AWS account to allow access to and from the company's on-premises network.

Developers within each account are responsible for adding new IP CIDR ranges to their security groups. The security team has its own AWS account. Currently, the security team notifies the owners of the other AWS accounts when changes are made to the allow list.

The solutions architect must design a solution that distributes the common set of CIDR ranges across all accounts.

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

- A. Set up an Amazon Simple Notification Service (Amazon SNS) topic in the security team's AWS account
- B. Deploy an AWS Lambda function in each AWS account
- C. Configure the Lambda function to run every time an SNS topic receives a messag
- D. Configure the Lambda function to take an IP address as input and add it to a list of security groups in the account
- E. Instruct the security team to distribute changes by publishing messages to its SNS topic.
- F. Create new customer-managed prefix lists in each AWS account within the organizatio
- G. Populate the prefix lists in each account with all internal CIDR range
- H. Notify the owner of each AWS account to allow the new customer-managed prefix list IDs in their accounts in their security group
- I. Instruct the security team to share updates with each AWS account owner.
- J. Create a new customer-managed prefix list in the security team's AWS account
- K. Populate the customer-managed prefix list with all internal CIDR range
- L. Share the customer-managed prefix listwith the organization by using AWS Resource Access Manage
- M. Notify the owner of each AWS account to allow the new customer-managed prefix list ID in their security groups.
- N. Create an IAM role in each account in the organizatio
- O. Grant permissions to update security groups. Deploy an AWS Lambda function in the security team's AWS account
- P. Configure the Lambda function to take a list of internal IP addresses as input, assume a role in each organization account, and add the list of IP addresses to the security groups in each account.

**Answer:** C

**Explanation:**

Create a new customer-managed prefix list in the security team's AWS account. Populate the customer-managed prefix list with all internal CIDR ranges. Share the customer-managed prefix list with the organization by using AWS Resource Access Manager. Notify the owner of each AWS account to allow the new customer-managed prefix list ID in their security groups. This solution meets the requirements

with the least amount of operational overhead as it requires the security team to create and maintain a single customer-managed prefix list, and share it with the organization using AWS Resource Access Manager. The owners of each AWS account are then responsible for allowing the prefix list in their security groups, which eliminates the need for the security team to manually notify each account owner when changes are made. This solution also eliminates the need for a separate AWS Lambda function in each account, reducing the overall complexity of the solution.

**NEW QUESTION 99**

- (Exam Topic 1)

A company is running an event ticketing platform on AWS and wants to optimize the platform's cost-effectiveness. The platform is deployed on Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 and is backed by an Amazon RDS for MySQL DB instance. The company is developing new application features to run on Amazon EKS with AWS Fargate. The platform experiences infrequent high peaks in demand. The surges in demand depend on event dates. Which solution will provide the MOST cost-effective setup for the platform?

- A. Purchase Standard Reserved Instances for the EC2 instances that the EKS cluster uses in its baseline load
- B. Scale the cluster with Spot Instances to handle peak
- C. Purchase 1-year All Upfront Reserved Instances for the database to meet predicted peak load for the year.
- D. Purchase Compute Savings Plans for the predicted medium load of the EKS cluster
- E. Scale the cluster with On-Demand Capacity Reservations based on event dates for peak
- F. Purchase 1-year No Upfront Reserved Instances for the database to meet the predicted base load
- G. Temporarily scale out database read replicas during peaks.
- H. Purchase EC2 Instance Savings Plans for the predicted base load of the EKS cluster
- I. Scale the cluster with Spot Instances to handle peak
- J. Purchase 1-year All Upfront Reserved Instances for the database to meet the predicted base load
- K. Temporarily scale up the DB instance manually during peaks.
- L. Purchase Compute Savings Plans for the predicted base load of the EKS cluster
- M. Scale the cluster with Spot Instances to handle peak
- N. Purchase 1-year All Upfront Reserved Instances for the database to meet the predicted base load
- O. Temporarily scale up the DB instance manually during peaks.

**Answer:** B

**Explanation:**

They all mention using spot instances and EKS based on EC2. A spot instance is not appropriate for a production server and the company is developing new application designed for AWS Fargate, which means we must plan the future cost improvement including AWS Fargate.  
<https://aws.amazon.com/savingsplans/compute-pricing/>

**NEW QUESTION 104**

- (Exam Topic 2)

A company needs to audit the security posture of a newly acquired AWS account. The company's data security team requires a notification only when an Amazon S3 bucket becomes publicly exposed. The company has already established an Amazon Simple Notification Service (Amazon SNS) topic that has the data security team's email address subscribed. Which solution will meet these requirements?

- A. Create an S3 event notification on all S3 buckets for the isPublic event
- B. Select the SNS topic as the target for the event notifications.
- C. Create an analyzer in AWS Identity and Access Management Access Analyzer
- D. Create an Amazon EventBridge rule for the event type "Access Analyzer Finding" with a filter for "isPublic: true." Select the SNS topic as the EventBridge rule target.
- E. Create an Amazon EventBridge rule for the event type "Bucket-Level API Call via CloudTrail" with a filter for "PutBucketPolicy." Select the SNS topic as the EventBridge rule target.
- F. Activate AWS Config and add the cloudtrail-s3-dataevents-enabled rule
- G. Create an Amazon EventBridge rule for the event type "Config Rules Re-evaluation Status" with a filter for "NON\_COMPLIANT." Select the SNS topic as the EventBridge rule target.

**Answer:** B

**Explanation:**

Access Analyzer is to assess the access policy. [https://docs.aws.amazon.com/ja\\_jp/AmazonS3/latest/userguide/access-control-block-public-access.html](https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/access-control-block-public-access.html)

**NEW QUESTION 105**

- (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 110**



- (Exam Topic 2)

A company is running a compute workload by using Amazon EC2 Spot Instances that are in an Auto Scaling group. The launch template uses two placement groups and a single instance type.

Recently, a monitoring system reported Auto Scaling instance launch failures that correlated with longer wait times for system users. The company needs to improve the overall reliability of the workload.

Which solution will meet this requirement?

- A. Replace the launch template with a launch configuration to use an Auto Scaling group that uses attribute-based instance type selection.
- B. Create a new launch template version that uses attribute-based instance type selectio
- C. Configure the Auto Scaling group to use the new launch template version.
- D. Update the launch template Auto Scaling group to increase the number of placement groups.
- E. Update the launch template to use a larger instance type.

**Answer: B**

**Explanation:**

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/create-asg-instance-type-requirements.html#use-attribut>

#### NEW QUESTION 111

- (Exam Topic 2)

A company has five development teams that have each created five AWS accounts to develop and host applications. To track spending, the development teams log in to each account every month, record the current cost from the AWS Billing and Cost Management console, and provide the information to the company's finance team.

The company has strict compliance requirements and needs to ensure that resources are created only in AWS Regions in the United States. However, some resources have been created in other Regions.

A solutions architect needs to implement a solution that gives the finance team the ability to track and consolidate expenditures for all the accounts. The solution also must ensure that the company can create resources only in Regions in the United States.

Which combination of steps will meet these requirements in the MOST operationally efficient way? (Select THREE.)

- A. Create a new account to serve as a management account
- B. Create an Amazon S3 bucket for the finance team. Use AWS Cost and Usage Reports to create monthly reports and to store the data in the finance team's S3 bucket.
- C. Create a new account to serve as a management account
- D. Deploy an organization in AWS Organizations with all features enable
- E. Invite all the existing accounts to the organizatio
- F. Ensure that each account accepts the invitation.
- G. Create an OU that includes all the development team
- H. Create an SCP that allows the creation of resources only in Regions that are in the United State
- I. Apply the SCP to the OU.
- J. Create an OU that includes all the development team
- K. Create an SCP that denies the creation of resources in Regions that are outside the United State
- L. Apply the SCP to the OU.
- M. Create an IAM role in the management account. Attach a policy that includes permissions to view the Billing and Cost Management console.
- N. Allow the finance team users to assume the role.
- O. Use AWS Cost Explorer and the Billing and Cost Management console to analyze cost.
- P. Create an IAM role in each AWS account
- Q. Attach a policy that includes permissions to view the Billing and Cost Management console
- R. Allow the finance team users to assume the role.

**Answer: BCE**

**Explanation:**

AWS Organizations is a service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage. By creating a management account and inviting all the existing accounts to join the organization, the solutions architect can track and consolidate expenditures for all the accounts using AWS Cost Management tools such as AWS Cost Explorer and AWS Budgets. An organizational unit (OU) is a group of accounts within an organization that can be used to apply policies and simplify management. A service control policy (SCP) is a type of policy that you can use to manage permissions in your organization. By creating an OU that includes all the development teams and applying an SCP that allows the creation of resources only in Regions that are in the United States, the solutions architect can ensure that the company meets its compliance requirements and avoids unwanted charges from other Regions. An IAM role is an identity with permission policies that determine what the identity can and cannot do in AWS. By creating an IAM role in the management account and allowing the finance team users to assume it, the solutions architect can give them access to view the Billing and Cost Management console without sharing credentials or creating additional users. References:

- > [https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_introduction.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_introduction.html)
- > [https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scp.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html)
- > [https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html)
- > <https://docs.aws.amazon.com/aws-cost-management/latest/userguide/what-is-costmanagement.html>

#### NEW QUESTION 114

- (Exam Topic 2)

A solutions architect is designing a solution to process events. The solution must have the ability to scale in and out based on the number of events that the solution receives. If a processing error occurs, the event must move into a separate queue for review.

Which solution will meet these requirements?

- A. Send event details to an Amazon Simple Notification Service (Amazon SNS) topic
- B. Configure an AWS Lambda function as a subscriber to the SNS topic to process the event
- C. Add an on-failure destination to the function
- D. Set an Amazon Simple Queue Service (Amazon SQS) queue as the target.
- E. Publish events to an Amazon Simple Queue Service (Amazon SQS) queue
- F. Create an Amazon EC2 Auto Scaling group
- G. Configure the Auto Scaling group to scale in and out based on the ApproximateAgeOfOldestMessage metric of the queue

- H. Configure the application to write failed messages to a dead-letter queue.
- I. Write events to an Amazon DynamoDB tabl
- J. Configure a DynamoDB stream for the tabl
- K. Configure the stream to invoke an AWS Lambda functio
- L. Configure the Lambda function to process the events.
- M. Publish events to an Amazon EventBridge event bu
- N. Create and run an application on an Amazon EC2 instance with an Auto Scaling group that isbehind an Application Load Balancer (ALB). Set the ALB as the event bus targe
- O. Configure the event bus to retry event
- P. Write messages to a dead-letter queue if the application cannot process the messages.

**Answer: A**

**Explanation:**

Amazon Simple Notification Service (Amazon SNS) is a fully managed pub/sub messaging service that enables users to send messages to multiple subscribers<sup>1</sup>. Users can send event details to an Amazon SNS topic and configure an AWS Lambda function as a subscriber to the SNS topic to process the events. Lambda is a serverless compute service that runs code in response to events and automatically manages the underlying compute resources<sup>2</sup>. Users can add an on-failure destination to the function and set an Amazon Simple Queue Service (Amazon SQS) queue as the target. Amazon SQS is a fully managed message queuing service that enables users to decouple and scale microservices, distributed systems, and serverless applications<sup>3</sup>. This way, if a processing error occurs, the event will move into the separate queue for review.

Option B is incorrect because publishing events to an Amazon SQS queue and creating an Amazon EC2 Auto Scaling group will not have the ability to scale in and out based on the number of events that the solution receives. Amazon EC2 is a web service that provides secure, resizable compute capacity in the cloud. Auto Scaling is a feature that helps users maintain application availability and allows them to scale their EC2 capacity up or down automatically according to conditions they define. However, for this use case, using SQS and EC2 will not take advantage of the serverless capabilities of Lambda and SNS.

Option C is incorrect because writing events to an Amazon DynamoDB table and configuring a DynamoDB stream for the table will not have the ability to move events into a separate queue for review if a processing error occurs. Amazon DynamoDB is a fully managed key-value and document database that delivers single-digit millisecond performance at any scale. DynamoDB Streams is a feature that captures data modification events in DynamoDB tables. Users can configure the stream to invoke a Lambda function, but they cannot configure an on-failure destination for the function.

Option D is incorrect because publishing events to an Amazon EventBridge event bus and setting an Application Load Balancer (ALB) as the event bus target will not have the ability to move events into a separate queue for review if a processing error occurs. Amazon EventBridge is a serverless event bus service that makes it easy to connect applications with data from a variety of sources. An ALB is a load balancer that distributes incoming application traffic across multiple targets, such as EC2 instances, containers, IP addresses, Lambda functions, and virtual appliances. Users can configure EventBridge to retry events, but they cannot configure an on-failure destination for the ALB.

**NEW QUESTION 116**

- (Exam Topic 2)

A company runs its sales reporting application in an AWS Region in the United States. The application uses an Amazon API Gateway Regional API and AWS Lambda functions to generate on-demand reports from data in an Amazon RDS for MySQL database. The frontend of the application is hosted on Amazon S3 and is accessed by users through an Amazon CloudFront distribution. The company is using Amazon Route 53 as the DNS service for the domain. Route 53 is configured with a simple routing policy to route traffic to the API Gateway API.

In the next 6 months, the company plans to expand operations to Europe. More than 90% of the database traffic is read-only traffic. The company has already deployed an API Gateway API and Lambda functions in the new Region.

A solutions architect must design a solution that minimizes latency for users who download reports. Which solution will meet these requirements?

- A. Use an AWS Database Migration Service (AWS DMS) task with full load to replicate the primary database in the original Region to the database in the new Regio
- B. Change the Route 53 record to latency-based routing to connect to the API Gateway API.
- C. Use an AWS Database Migration Service (AWS DMS) task with full load plus change data capture (CDC) to replicate the primary database in the original Region to the database in the new Regio
- D. Change the Route 53 record to geolocation routing to connect to the API Gateway API.
- E. Configure a cross-Region read replica for the RDS database in the new Regio
- F. Change the Route 53 record to latency-based routing to connect to the API Gateway API.
- G. Configure a cross-Region read replica for the RDS database in the new Regio
- H. Change the Route 53 record to geolocation routing to connect to the API

**Answer: C**

**Explanation:**

The company should configure a cross-Region read replica for the RDS database in the new Region. The company should change the Route 53 record to latency-based routing to connect to the API Gateway API. This solution will meet the requirements because a cross-Region read replica is a feature that enables you to create a MariaDB, MySQL, Oracle, PostgreSQL, or SQL Server read replica in a different Region from the source DB instance. You can use cross-Region read replicas to improve availability and disaster recovery, scale out globally, or migrate an existing database to a new Region<sup>1</sup>. By creating a cross-Region read replica for the RDS database in the new Region, the company can have a standby copy of its primary database that can serve read-only traffic from users in Europe. A latency-based routing policy is a feature that enables you to route traffic based on the latency between your users and your resources. You can use latency-based routing to route traffic to the resource that provides the best latency<sup>2</sup>. By changing the Route 53 record to latency-based routing, the company can minimize latency for users who download reports by connecting them to the API Gateway API in the Region that provides the best response time.

The other options are not correct because:

- Using AWS Database Migration Service (AWS DMS) to replicate the primary database in the original Region to the database in the new Region would not be as cost-effective or simple as using a cross-Region read replica. AWS DMS is a service that enables you to migrate relational databases, data warehouses, NoSQL databases, and other types of data stores. You can use AWS DMS to perform one-time migrations or continuous data replication with high availability and consolidate databases into a petabyte-scale data warehouse<sup>3</sup>. However, AWS DMS requires more configuration and management than creating a cross-Region read replica, which is fully managed by Amazon RDS. AWS DMS also incurs additional charges for replication instances and tasks.
- Creating an Amazon API Gateway Data API service integration with Amazon Redshift would not help with disaster recovery or minimizing latency. 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. It is useful for building applications that interact with Amazon Redshift, but not for replicating or recovering data from an RDS database.
- Creating an AWS Data Exchange datashare by connecting AWS Data Exchange to the Redshift cluster would not help with disaster recovery or minimizing latency. AWS Data Exchange is a service that makes it easy for AWS customers to exchange data in the cloud. You can use AWS Data Exchange to subscribe to a diverse selection of third-party data products or offer your own data products to other AWS customers. 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. It is useful for sharing query results and views with other users, but not for replicating or recovering data from an RDS database.

References:

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

#### NEW QUESTION 119

- (Exam Topic 2)

A company runs a customer service center that accepts calls and automatically sends all customers a managed, interactive, two-way experience survey by text message.

The applications that support the customer service center run on machines that the company hosts in an on-premises data center. The hardware that the company uses is old, and the company is experiencing downtime with the system. The company wants to migrate the system to AWS to improve reliability.

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

- A. Use Amazon Connect to replace the old call center hardware
- B. Use Amazon Pinpoint to send text message surveys to customers.
- C. Use Amazon Connect to replace the old call center hardware
- D. Use Amazon Simple Notification Service (Amazon SNS) to send text message surveys to customers.
- E. Migrate the call center software to Amazon EC2 instances that are in an Auto Scaling group
- F. Use the EC2 instances to send text message surveys to customers.
- G. Use Amazon Pinpoint to replace the old call center hardware and to send text message surveys to customers.

**Answer:** A

#### Explanation:

Amazon Connect is a cloud-based contact center service that allows you to set up a virtual call center for your business. It provides an easy-to-use interface for managing customer interactions through voice and chat. Amazon Connect integrates with other AWS services, such as Amazon S3 and Amazon Kinesis, to help you collect, store, and analyze customer data for insights into customer behavior and trends. On the other hand, Amazon Pinpoint is a marketing automation and analytics service that allows you to engage with your customers across different channels, such as email, SMS, push notifications, and voice. It helps you create personalized campaigns based on user behavior and enables you to track user engagement and retention. While both services allow you to communicate with your customers, they serve different purposes. Amazon Connect is focused on customer support and service, while Amazon Pinpoint is focused on marketing and engagement.

#### NEW QUESTION 124

- (Exam Topic 2)

A telecommunications company is running an application on AWS. The company has set up an AWS Direct Connect connection between the company's on-premises data center and AWS. The company deployed the application on Amazon EC2 instances in multiple Availability Zones behind an internal Application Load Balancer (ALB). The company's clients connect from the on-premises network by using HTTPS. The TLS terminates in the ALB. The company has multiple target groups and uses path-based routing to forward requests based on the URL path.

The company is planning to deploy an on-premises firewall appliance with an allow list that is based on IP address. A solutions architect must develop a solution to allow traffic flow to AWS from the on-premises network so that the clients can continue to access the application.

Which solution will meet these requirements?

- A. Configure the existing ALB to use static IP addresses
- B. Assign IP addresses in multiple Availability Zones to the ALB
- C. Add the ALB IP addresses to the firewall appliance.
- D. Create a Network Load Balancer (NLB). Associate the NLB with one static IP address in multiple Availability Zones
- E. Create an ALB-type target group for the NLB and add the existing ALB. Add the NLB IP addresses to the firewall appliance
- F. Update the clients to connect to the NLB.
- G. Create a Network Load Balancer (NLB). Associate the NLB with one static IP address in multiple Availability Zones
- H. Add the existing target groups to the NLB
- I. Update the clients to connect to the NLB
- J. Delete the ALB. Add the NLB IP addresses to the firewall appliance.
- K. Create a Gateway Load Balancer (GWLB). Assign static IP addresses to the GWLB in multiple Availability Zones
- L. Create an ALB-type target group for the GWLB and add the existing ALB
- M. Add the GWLB IP addresses to the firewall appliance
- N. Update the clients to connect to the GWLB.

**Answer:** B

#### Explanation:

The company should create a Network Load Balancer (NLB) and associate it with one static IP address in multiple Availability Zones. The company should also create an ALB-type target group for the NLB and add the existing ALB. The company should add the NLB IP addresses to the firewall appliance and update the clients to connect to the NLB. This solution will allow traffic flow to AWS from the on-premises network by using static IP addresses that can be added to the firewall appliance's allow list. The NLB will forward requests to the ALB, which will use path-based routing to forward requests to the target groups.

#### NEW QUESTION 126

- (Exam Topic 2)

A company has built a high performance computing (HPC) cluster in AWS for a tightly coupled workload that generates a large number of shared files stored in Amazon EFS. The cluster was performing well when the number of Amazon EC2 instances in the cluster was 100. However, when the company increased the cluster size to 1,000 EC2 instances, overall performance was well below expectations.

Which collection of design choices should a solutions architect make to achieve the maximum performance from the HPC cluster? (Select THREE.)

- A. Ensure the HPC cluster is launched within a single Availability Zone.
- B. Launch the EC2 instances and attach elastic network interfaces in multiples of four.
- C. Select EC2 Instance types with an Elastic Fabric Adapter (EFA) enabled.



- D. Ensure the cluster is launched across multiple Availability Zones.
- E. Replace Amazon EFS with multiple Amazon EBS volumes in a RAID array.
- F. Replace Amazon EFS with Amazon FSx for Lustre.

**Answer:** ACF

**Explanation:**

- \* A. High performance computing (HPC) workload cluster should be in a single AZ.
  - \* C. Elastic Fabric Adapter (EFA) is a network device that you can attach to your Amazon EC2 instances to accelerate High Performance Computing (HPC)
  - \* F. Amazon FSx for Lustre - Use it for workloads where speed matters, such as machine learning, high performance computing (HPC), video processing, and financial modeling.
- Cluster – packs instances close together inside an Availability Zone. This strategy enables workloads to achieve the low-latency network performance necessary for tightly-coupled node-to-node communication that is typical of HPC applications.
- <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

**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 132**

- (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. 1. A public VIF allows you to access AWS public services such as EC2. 2. 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 133**

- (Exam Topic 2)

A company uses a Grafana data visualization solution that runs on a single Amazon EC2 instance to monitor the health of the company's AWS workloads. The company has invested time and effort to create dashboards that the company wants to preserve. The dashboards need to be highly available and cannot be down for longer than 10 minutes. The company needs to minimize ongoing maintenance.

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

- A. Migrate to Amazon CloudWatch dashboard

- B. Recreate the dashboards to match the existing Grafana dashboard
- C. Use automatic dashboards where possible.
- D. Create an Amazon Managed Grafana workspace
- E. Configure a new Amazon CloudWatch data source. Export dashboards from the existing Grafana instance
- F. Import the dashboards into the new workspace.
- G. Create an AMI that has Grafana pre-installed
- H. Store the existing dashboards in Amazon Elastic File System (Amazon EFS). Create an Auto Scaling group that uses the new AMI
- I. Set the Auto Scaling group's minimum, desired, and maximum number of instances to one
- J. Create an Application Load Balancer that serves at least two Availability Zones.
- K. Configure AWS Backup to back up the EC2 instance that runs Grafana once each hour
- L. Restore the EC2 instance from the most recent snapshot in an alternate Availability Zone when required.

**Answer: C**

**Explanation:**

By creating an AMI that has Grafana pre-installed and storing the existing dashboards in Amazon Elastic File System (Amazon EFS) it allows for faster and more efficient scaling, and by creating an Auto Scaling group that uses the new AMI and setting the Auto Scaling group's minimum, desired, and maximum number of instances to one and creating an Application Load Balancer that serves at least two Availability Zones, it ensures high availability and minimized downtime.

**NEW QUESTION 137**

- (Exam Topic 2)

A company has several AWS accounts. A development team is building an automation framework for cloud governance and remediation processes. The automation framework uses AWS Lambda functions in a centralized account. A solutions architect must implement a least privilege permissions policy that allows the Lambda functions to run in each of the company's AWS accounts.

Which combination of steps will meet these requirements? (Choose two.)

- A. In the centralized account, create an IAM role that has the Lambda service as a trusted entity
- B. Add an inline policy to assume the roles of the other AWS accounts.
- C. In the other AWS accounts, create an IAM role that has minimal permission
- D. Add the centralized account's Lambda IAM role as a trusted entity.
- E. In the centralized account, create an IAM role that has roles of the other accounts as trusted entities. Provide minimal permissions.
- F. In the other AWS accounts, create an IAM role that has permissions to assume the role of the centralized account
- G. Add the Lambda service as a trusted entity.
- H. In the other AWS accounts, create an IAM role that has minimal permission
- I. Add the Lambda service as a trusted entity.

**Answer: AB**

**Explanation:**

<https://medium.com/@it.melnichenko/invoke-a-lambda-across-multiple-aws-accounts-8c094b2e70be>

**NEW QUESTION 141**

.....

## 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](#)**