

## Exam Questions SAP-C02

AWS Certified Solutions Architect - Professional

<https://www.2passeasy.com/dumps/SAP-C02/>



**NEW QUESTION 1**

- (Exam Topic 1)

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

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

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

**Answer: C**

**Explanation:**

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

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

**NEW QUESTION 2**

- (Exam Topic 1)

A 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 instances.
- 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 running.
- E. Create an Amazon FSx for Lustre file system.
- F. Create an Auto Scaling group that extends across three Availability Zones and maintains a minimum size of three instances.
- 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 system.
- I. Create an Auto Scaling group that extends across three Availability Zones and maintains a minimum size of three instances.
- J. Implement a user data script to install the application and mount the FSx for Windows File Server file system.
- 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 running.
- M. Create an Amazon Elastic File System (Amazon EFS) file system.
- N. Create an Auto Scaling group that extends across three Availability Zones and maintains a minimum size of three instances.
- 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 3**

- (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 Config.
- B. Configure the rule with the instance types that are allowed.

- 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 allowed.
- E. Assign the launch template to the developers' IAM accounts.
- F. Create a new IAM policy.
- G. Specify the instance types that are allowed.
- 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 4**

- (Exam Topic 1)

A company has migrated its forms-processing application to AWS. When users interact with the application, they upload scanned forms as files through a web application. A database stores user metadata and references to files that are stored in Amazon S3. The web application runs on Amazon EC2 instances and an Amazon RDS for PostgreSQL database.

When forms are uploaded, the application sends notifications to a team through Amazon Simple Notification Service (Amazon SNS). A team member then logs in and processes each form. The team member performs data validation on the form and extracts relevant data before entering the information into another system that uses an API.

A solutions architect needs to automate the manual processing of the forms. The solution must provide accurate form extraction, minimize time to market, and minimize long-term operational overhead.

Which solution will meet these requirements?

- A. Develop custom libraries to perform optical character recognition (OCR) on the form.
- B. Deploy the libraries to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster as an application tier.
- C. Use this tier to process the forms when forms are uploaded.
- D. Store the output in Amazon S3. Parse this output by extracting the data into an Amazon DynamoDB table.
- E. Submit the data to the target system's API.
- F. Host the new application tier on EC2 instances.
- G. Extend the system with an application tier that uses AWS Step Functions and AWS Lambda.
- H. Configure this tier to use artificial intelligence and machine learning (AI/ML) models that are trained and hosted on an EC2 instance to perform optical character recognition (OCR) on the forms when forms are uploaded.
- I. Store the output in Amazon S3. Parse this output by extracting the data that is required within the application tier.
- J. Submit the data to the target system's API.
- K. Host a new application tier on EC2 instance.
- L. Use this tier to call endpoints that host artificial intelligence and machine learning (AI/ML) models that are trained and hosted in Amazon SageMaker to perform optical character recognition (OCR) on the form.
- M. Store the output in Amazon ElastiCache.
- N. Parse this output by extracting the data that is required within the application tier.
- O. Submit the data to the target system's API.
- P. Extend the system with an application tier that uses AWS Step Functions and AWS Lambda.
- Q. Configure this tier to use Amazon Textract and Amazon Comprehend to perform optical character recognition (OCR) on the forms when forms are uploaded.
- R. Store the output in Amazon S3. Parse this output by extracting the data that is required within the application tier.
- S. Submit the data to the target system's API.

**Answer:** D

**Explanation:**

Extend the system with an application tier that uses AWS Step Functions and AWS Lambda. Configure this tier to use Amazon Textract and Amazon Comprehend to perform optical character recognition (OCR) on the forms when forms are uploaded. Store the output in Amazon S3. Parse this output by extracting the data that is required within the application tier. Submit the data to the target system's API. This solution meets the requirements of accurate form extraction, minimal time to market, and minimal long-term operational overhead. Amazon Textract and Amazon Comprehend are fully managed and serverless services that can perform OCR and extract relevant data from the forms, which eliminates the need to develop custom libraries or train and host models. Using AWS Step Functions and Lambda allows for easy automation of the process and the ability to scale as needed.

**NEW QUESTION 5**

- (Exam Topic 1)

A company is running an application in the AWS Cloud. The company's security team must approve the creation of all new IAM users. When a new IAM user is created, all access for the user must be removed automatically. The security team must then receive a notification to approve the user. The company has a multi-Region AWS CloudTrail trail in the AWS account.

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

- A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule.
- B. Define a pattern with the detail-type value set to AWS API Call via CloudTrail and an eventName of CreateUser.
- C. Configure CloudTrail to send a notification for the CreateUser event to an Amazon Simple Notification Service (Amazon SNS) topic.
- D. Invoke a container that runs in Amazon Elastic Container Service (Amazon ECS) with AWS Fargate technology to remove access.
- E. Invoke an AWS Step Functions state machine to remove access.
- F. Use Amazon Simple Notification Service (Amazon SNS) to notify the security team.
- G. Use Amazon Pinpoint to notify the security team.

**Answer:** ADE

**Explanation:**

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/send-a-notification-when-an-iam-user-is-created.html>

**NEW QUESTION 6**

- (Exam Topic 1)

A software as a service (SaaS) based company provides a case management solution to customers A3 part of the solution. The company uses a standalone Simple Mail Transfer Protocol (SMTP) server to send email messages from an application. The application also stores an email template for acknowledgement email messages that populate customer data before the application sends the email message to the customer. The company plans to migrate this messaging functionality to the AWS Cloud and needs to minimize operational overhead. Which solution will meet these requirements MOST cost-effectively?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 7**

- (Exam Topic 1)

A company uses AWS Organizations for a multi-account setup in the AWS Cloud. The company uses AWS Control Tower for governance and uses AWS Transit Gateway for VPC connectivity across accounts.

In an AWS application account, the company's application team has deployed a web application that uses AWS Lambda and Amazon RDS. The company's database administrators have a separate DBA account and use the account to centrally manage all the databases across the organization. The database administrators use an Amazon EC2 instance that is deployed in the DBA account to access an RDS database that is deployed in the application account. The application team has stored the database credentials as secrets in AWS Secrets Manager in the application account. The application team is manually sharing the secrets with the database administrators. The secrets are encrypted by the default AWS managed key for Secrets Manager in the application account. A solutions architect needs to implement a solution that gives the database administrators access to the database and eliminates the need to manually share the secrets.

Which solution will meet these requirements?

- A. Use AWS Resource Access Manager (AWS RAM) to share the secrets from the application account with the DBA account
- B. In the DBA account, create an IAM role that is named DBA-Admi
- C. Grant the role the required permissions to access the shared secret
- D. Attach the DBA-Admin role to the EC2 instance for access to the cross-account secrets.
- E. In the application account, create an IAM role that is named DBA-Secre
- F. Grant the role the required permissions to access the secret
- G. In the DBA account, create an IAM role that is named DBA-Admi
- H. Grant the DBA-Admin role the required permissions to assume the DBA-Secret role in the application account
- I. Attach the DBA-Admin role to the EC2 instance for access to the cross-account secrets.
- J. In the DBA account, create an IAM role that is named DBA-Admi
- K. Grant the role the required permissions to access the secrets and the default AWS managed key in the application account
- L. In the application account, attach resource-based policies to the key to allow access from the DBA account
- M. Attach the DBA-Admin role to the EC2 instance for access to the cross-account secrets.
- N. In the DBA account, create an IAM role that is named DBA-Admi
- O. Grant the role the required permissions to access the secrets in the application account
- P. Attach an SCP to the application account to allow access to the secrets from the DBA account
- Q. Attach the DBA-Admin role to the EC2 instance for access to the cross-account secrets.

**Answer:** B

**Explanation:**

➤ Option B is correct because creating an IAM role in the application account that has permissions to access the secrets and creating an IAM role in the DBA account that has permissions to assume the role in the application account eliminates the need to manually share the secrets. This approach uses cross-account IAM roles to grant access to the secrets in the application account. The database administrators can assume the role in the application account from their EC2 instance in the DBA

account and retrieve the secrets without having to store them locally or share them manually2

References: 1: <https://docs.aws.amazon.com/ram/latest/userguide/what-is.html> 2:

[https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial\\_cross-account-with-roles.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html) 3:

<https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html> : [https://docs.aws.amazon.com/secretsmanager/latest/userguide/tutorials\\_basic.html](https://docs.aws.amazon.com/secretsmanager/latest/userguide/tutorials_basic.html) :

<https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html>

**NEW QUESTION 8**

- (Exam Topic 1)

A company has migrated an application from on premises to AWS. The application frontend is a static website that runs on two Amazon EC2 instances behind an Application Load Balancer (ALB). The application backend is a Python application that runs on three EC2 instances behind another ALB. The EC2 instances are large, general purpose On-Demand Instances that were sized to meet the on-premises specifications for peak usage of the application.

The application averages hundreds of thousands of requests each month. However, the application is used mainly during lunchtime and receives minimal traffic during the rest of the day.

A solutions architect needs to optimize the infrastructure cost of the application without negatively affecting the application availability.

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

- A. Change all the EC2 instances to compute optimized instances that have the same number of cores as the existing EC2 instances.
- B. Move the application frontend to a static website that is hosted on Amazon S3.
- C. Deploy the application frontend by using AWS Elastic Beanstalk
- D. Use the same instance type for the nodes.
- E. Change all the backend EC2 instances to Spot Instances.
- F. Deploy the backend Python application to general purpose burstable EC2 instances that have the same number of cores as the existing EC2 instances.

**Answer:** BD

**Explanation:**

Moving the application frontend to a static website that is hosted on Amazon S3 will save cost as S3 is cheaper than running EC2 instances.

Using Spot instances for the backend EC2 instances will also save cost, as they are significantly cheaper than On-Demand instances. This will be suitable for the application, as it has minimal traffic during the rest of the day, and the availability of spot instances will not negatively affect the application's availability.

Reference:

Amazon S3 pricing: <https://aws.amazon.com/s3/pricing/>

Amazon EC2 Spot Instances documentation: <https://aws.amazon.com/ec2/spot/> AWS Elastic Beanstalk documentation: <https://aws.amazon.com/elasticbeanstalk/>

Amazon Elastic Compute Cloud (EC2) pricing: <https://aws.amazon.com/ec2/pricing/>

**NEW QUESTION 9**

- (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 10**

- (Exam Topic 1)

A company wants to migrate its workloads from on premises to AWS. The workloads run on Linux and Windows. The company has a large on-premises infrastructure that consists of physical machines and VMs that host numerous applications.

The company must capture details about the system configuration, system performance, running processes and network connections of its on-premises servers. The company also must divide the on-premises applications into groups for AWS migrations. The company needs recommendations for Amazon EC2 instance types so that the company can run its workloads on AWS in the most cost-effective manner.

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

- A. Assess the existing applications by installing AWS Application Discovery Agent on the physical machines and VMs.
- B. Assess the existing applications by installing AWS Systems Manager Agent on the physical machines and VMs
- C. Group servers into applications for migration by using AWS Systems Manager Application Manager.
- D. Group servers into applications for migration by using AWS Migration Hub.
- E. Generate recommended instance types and associated costs by using AWS Migration Hub.
- F. Import data about server sizes into AWS Trusted Advisor
- G. Follow the recommendations for cost optimization.

**Answer:** ADE

**Explanation:**

<https://docs.aws.amazon.com/application-discovery/latest/userguide/discovery-agent.html>

<https://docs.aws.amazon.com/migrationhub/latest/ug/ec2-recommendations.html>

**NEW QUESTION 10**

- (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 14

- (Exam Topic 1)

A company is building a solution in the AWS Cloud. Thousands of devices will connect to the solution and send data. Each device needs to be able to send and receive data in real time over the MQTT protocol. Each device must authenticate by using a unique X.509 certificate. Which solution will meet these requirements with the LEAST operational overhead?

- A. Set up AWS IoT Core
- B. For each device, create a corresponding Amazon MQ queue and provision a certificate
- C. Connect each device to Amazon MQ.
- D. Create a Network Load Balancer (NLB) and configure it with an AWS Lambda authorizer
- E. Run an MQTT broker on Amazon EC2 instances in an Auto Scaling group
- F. Set the Auto Scaling group as the target for the NLB
- G. Connect each device to the NLB.
- H. Set up AWS IoT Core
- I. For each device, create a corresponding AWS IoT thing and provision a certificate
- J. Connect each device to AWS IoT Core.
- K. Set up an Amazon API Gateway HTTP API and a Network Load Balancer (NLB). Create integration between API Gateway and the NLB
- L. Configure a mutual TLS certificate authorizer on the HTTP API
- M. Run an MQTT broker on an Amazon EC2 instance that the NLB target
- N. Connect each device to the NLB.

**Answer: D**

**Explanation:**

This solution requires minimal operational overhead, as it only requires setting up AWS IoT Core and creating a thing for each device. (Reference: AWS Certified Solutions Architect - Professional Official Amazon Text Book, Page 537)

AWS IoT Core is a fully managed service that enables secure, bi-directional communication between internet-connected devices and the AWS Cloud. It supports the MQTT protocol and includes built-in device authentication and access control. By using AWS IoT Core, the company can easily provision and manage the X.509 certificates for each device, and connect the devices to the service with minimal operational overhead.

#### NEW QUESTION 16

- (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 Connection 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<sup>23</sup>

➤ 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 17

- (Exam Topic 1)

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

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

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

**Answer: B**

### Explanation:

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

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

## NEW QUESTION 20

- (Exam Topic 1)

A company wants to migrate to AWS. The company wants to use a multi-account structure with centrally managed access to all accounts and applications. The company also wants to keep the traffic on a private network. Multi-factor authentication (MFA) is required at login, and specific roles are assigned to user groups. The company must create separate accounts for development, staging, production, and shared network. The production account and the shared network account must have connectivity to all accounts. The development account and the staging account must have access only to each other.

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

- A. Deploy a landing zone environment by using AWS Control Tower
- B. Enroll accounts and invite existing accounts into the resulting organization in AWS Organizations.
- C. Enable AWS Security Hub in all accounts to manage cross-account access
- D. Collect findings through AWS CloudTrail to force MFA login.
- E. Create transit gateways and transit gateway VPC attachments in each account
- F. Configure appropriate route tables.
- G. Set up and enable AWS IAM Identity Center (AWS Single Sign-On). Create appropriate permission sets with required MFA for existing accounts.
- H. Enable AWS Control Tower in all accounts to manage routing between accounts
- I. Collect findings through AWS CloudTrail to force MFA login.
- J. Create IAM users and groups
- K. Configure MFA for all users
- L. Set up Amazon Cognito user pools and identity pools to manage access to accounts and between accounts.

**Answer: ACD**

### Explanation:

The correct answer would be options A, C and D, because they address the requirements outlined in the question. A. Deploying a landing zone environment using AWS Control Tower and enrolling accounts in an organization in AWS Organizations allows for a centralized management of access to all accounts and applications. C. Creating transit gateways and transit gateway VPC attachments in each account and configuring appropriate route tables allows for private network traffic, and ensures that the production account and shared network account have connectivity to all accounts, while the development and staging accounts have access only to each other. D. Setting up and enabling AWS IAM Identity Center (AWS Single Sign-On) and creating appropriate permission sets with required MFA for existing accounts allows for multi-factor authentication at login and specific roles to be assigned to user groups.

#### NEW QUESTION 24

- (Exam Topic 1)

A company has developed APIs that use Amazon API Gateway with Regional endpoints. The APIs call AWS Lambda functions that use API Gateway authentication mechanisms. After a design review, a solutions architect identifies a set of APIs that do not require public access.

The solutions architect must design a solution to make the set of APIs accessible only from a VPC. All APIs need to be called with an authenticated user.

Which solution will meet these requirements with the LEAST amount of effort?

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

**Answer:** C

#### Explanation:

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

Reference:

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

#### NEW QUESTION 26

- (Exam Topic 1)

A company has created an OU in AWS Organizations for each of its engineering teams. Each OU owns multiple AWS accounts. The organization has hundreds of AWS accounts. A solutions architect must design a solution so that each OU can view a breakdown of usage costs across its AWS accounts. Which solution meets these requirements?

- A. Create an AWS Cost and Usage Report (CUR) for each OU by using AWS Resource Access Manager. Allow each team to visualize the CUR through an Amazon QuickSight dashboard.
- B. Create an AWS Cost and Usage Report (CUR) from the AWS Organizations management account. Allow each team to visualize the CUR through an Amazon QuickSight dashboard.
- C. Create an AWS Cost and Usage Report (CUR) in each AWS Organizations member account. Allow each team to visualize the CUR through an Amazon QuickSight dashboard.
- D. Create an AWS Cost and Usage Report (CUR) by using AWS Systems Manager. Allow each team to visualize the CUR through Systems Manager OpsCenter dashboards.

**Answer:** B

#### Explanation:

<https://docs.aws.amazon.com/cur/latest/userguide/billing-cur-limits.html>

#### NEW QUESTION 28

- (Exam Topic 1)

A company wants to migrate an application to Amazon EC2 from VMware Infrastructure that runs in an on-premises data center. A solutions architect must preserve the software and configuration settings during the migration.

What should the solutions architect do to meet these requirements?

- A. Configure the AWS DataSync agent to start replicating the data store to Amazon FSx for Windows FileServer. Use the SMB share to host the VMware data store.
- B. Use VM Import/Export to move the VMs to Amazon EC2.
- C. Use the VMware vSphere client to export the application as an image in Open Virtualization Format (OVF) format. Create an Amazon S3 bucket to store the image in the destination AWS Region.
- D. Create and apply an IAM role for VM Import. Use the AWS CLI to run the EC2 import command.
- E. . Configure AWS Storage Gateway for file service to export a Common Internet File System (CIFS) share.
- F. Create a backup copy to the shared folder.
- G. Sign in to the AWS Management Console and create an AMI from the backup copy. Launch an EC2 instance that is based on the AMI.
- H. Create a managed-instance activation for a hybrid environment in AWS Systems Manager.
- I. Download and install Systems Manager Agent on the on-premises VM. Register the VM with Systems Manager to be a managed instance. Use AWS Backup to create a snapshot of the VM and create an AMI.
- J. Launch an EC2 instance that is based on the AMI.

**Answer:** D

#### Explanation:

<https://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html>

- Export an OVF Template
- Create / use an Amazon S3 bucket for storing the exported images. The bucket must be in the Region where you want to import your VMs.
- Create an IAM role named vmimport.
- You'll use AWS CLI to run the import commands. <https://aws.amazon.com/premiumsupport/knowledge-center/import-instances/>

### NEW QUESTION 31

- (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 33

- (Exam Topic 1)

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

Which solution will provide the HIGHEST availability for the database?

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

**Answer: D**

#### Explanation:

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

### NEW QUESTION 36

- (Exam Topic 1)

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

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

Which solution will meet these requirements?

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

H. Import the csvfile to an Amazon QuickSight dashboard.

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 38

- (Exam Topic 1)

An AWS partner company is building a service in AWS Organizations using its organization named org. This service requires the partner company to have access to AWS resources in a customer account, which is in a separate organization named org2. The company must establish least privilege security access using an API or command line tool to the customer account.

What is the MOST secure way to allow org1 to access resources in org2?

- A. The customer should provide the partner company with their AWS account access keys to log in and perform the required tasks.
- B. The customer should create an IAM user and assign the required permissions to the IAM user. The customer should then provide the credentials to the partner company to log in and perform the required tasks.
- C. The customer should create an IAM role and assign the required permissions to the IAM role.
- D. The partner company should then use the IAM role's Amazon Resource Name (ARN) when requesting access to perform the required tasks.
- E. The customer should create an IAM role and assign the required permissions to the IAM role.
- F. The partner company should then use the IAM role's Amazon Resource Name (ARN). Including the external ID in the IAM role's trust policy, when requesting access to perform the required tasks.

**Answer:** C

**Explanation:**

<https://docs.aws.amazon.com/IAM/latest/UserGuide/confused-deputy.html>

This is the most secure way to allow org1 to access resources in org2 because it allows for least privilege security access. The customer should create an IAM role and assign the required permissions to the IAM role. The partner company should then use the IAM role's Amazon Resource Name (ARN) and include the external ID in the IAM role's trust policy when requesting access to perform the required tasks. This ensures that the partner company can only access the resources that it needs and only from the specific customer account.

#### NEW QUESTION 40

- (Exam Topic 1)

A company developed a pilot application by using AWS Elastic Beanstalk and Java. To save costs during development, the company's development team deployed the application into a single-instance environment. Recent tests indicate that the application consumes more CPU than expected. CPU utilization is regularly greater than 85%, which causes some performance bottlenecks.

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

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

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

**Answer:** C

**Explanation:**

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

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

#### NEW QUESTION 44

- (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 45**

- (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 47**

- (Exam Topic 1)

A company has a latency-sensitive trading platform that uses Amazon DynamoDB as a storage backend. The company configured the DynamoDB table to use on-demand capacity mode. A solutions architect needs to design a solution to improve the performance of the trading platform. The new solution must ensure high availability for the trading platform.

Which solution will meet these requirements with the LEAST latency?

- A. Create a two-node DynamoDB Accelerator (DAX) cluster Configure an application to read and write data by using DAX.
- B. Create a three-node DynamoDB Accelerator (DAX) cluster
- C. Configure an application to read data by using DAX and to write data directly to the DynamoDB table.
- D. Create a three-node DynamoDB Accelerator (DAX) cluster
- E. Configure an application to read data directly from the DynamoDB table and to write data by using DAX.
- F. Create a single-node DynamoDB Accelerator (DAX) cluster
- G. Configure an application to read data by using DAX and to write data directly to the DynamoDB table.

**Answer:** B

**Explanation:**

A DAX cluster can be deployed with one or two nodes for development or test workloads. One- and two-node clusters are not fault-tolerant, and we don't recommend using fewer than three nodes for production use. If a one- or two-node cluster encounters software or hardware errors, the cluster can become unavailable or lose cached data. A DAX cluster can be deployed with one or two nodes for development or test workloads. One and two-node clusters are not fault-tolerant, and we don't recommend using fewer than three nodes for production use. If a one- or two-node cluster encounters software or hardware errors, the cluster can become unavailable or lose cached data.

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DAX.concepts.cluster.html>

**NEW QUESTION 50**

- (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 SecretsManagerReadOnlyAccess 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 SecretsManagerReadOnlyAccess 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 51**

- (Exam Topic 1)

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

The development team and testing team work on business days during business hours, but the production environment operates 24 hours a day. 7 days a week.

The company wants to reduce costs AH resources are tagged with an environment tag with either development, testing, or production as the key. What should a solutions architect do to reduce costs with the LEAST operational effort?

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 53**

- (Exam Topic 1)

A company is creating a sequel for a popular online game. A large number of users from all over the world will play the game within the first week after launch.

Currently, the game consists of the following components deployed in a single AWS Region:

- Amazon S3 bucket that stores game assets
- Amazon DynamoDB table that stores player scores

A solutions architect needs to design a multi-Region solution that will reduce latency improve reliability, and require the least effort to implement

What should the solutions architect do to meet these requirements?

- A. Create an Amazon CloudFront distribution to serve assets from the S3 bucket Configure S3Cross-Region Replication Create a new DynamoDB able in a new Region Use the new table as a replica target tor DynamoDB global tables.
- B. Create an Amazon CloudFront distribution to serve assets from the S3 bucke
- C. Configure S3Same-Region Replicatio
- D. Create a new DynamoDB able m a new Regio
- E. Configure asynchronous replication between the DynamoDB tables by using AWS Database Migration Service (AWS DMS) with change data capture (CDC)
- F. Create another S3 bucket in a new Region and configure S3 Cross-Region Replication between the buckets Create an Amazon CloudFront distribution and configure origin failover with two origins accessing the S3 buckets in each Regio
- G. Configure DynamoDB global tables by enabling Amazon DynamoDB Streams, and add a replica table in a new Region.
- H. Create another S3 bucket in the same Region, and configure S3 Same-Region Replication between the buckets- Create an Amazon CloudFront distribution and configure origin failover with two origin accessing the S3 buckets Create a new DynamoDB table m a new Region Use the new table as a replica target for DynamoDB global tables.

**Answer: C**

**Explanation:**

[https://aws.amazon.com/premiumsupport/knowledge-center/dynamodb-global-table-stream-lambda/?nc1=h\\_ls](https://aws.amazon.com/premiumsupport/knowledge-center/dynamodb-global-table-stream-lambda/?nc1=h_ls)

**NEW QUESTION 55**

- (Exam Topic 1)

A company uses an on-premises data analytics platform. The system is highly available in a fully redundant configuration across 12 servers in the company's data center.

The system runs scheduled jobs, both hourly and daily, in addition to one-time requests from users. Scheduled jobs can take between 20 minutes and 2 hours to finish running and have tight SLAs. The scheduled jobs account for 65% of the system usage. User jobs typically finish running in less than 5 minutes and have no SLA. The user jobs account for 35% of system usage. During system failures, scheduled jobs must continue to meet SLAs. However, user jobs can be delayed.

A solutions architect needs to move the system to Amazon EC2 instances and adopt a consumption-based model to reduce costs with no long-term commitments. The solution must maintain high availability and must not affect the SLAs.

Which solution will meet these requirements MOST cost-effectively?

- A. Split the 12 instances across two Availability Zones in the chosen AWS Region
- B. Run two instances in each Availability Zone as On-Demand Instances with Capacity Reservation
- C. Run four instances in each Availability Zone as Spot Instances.
- D. Split the 12 instances across three Availability Zones in the chosen AWS Region
- E. In one of the Availability Zones, run all four instances as On-Demand Instances with Capacity Reservation
- F. Run the remaining instances as Spot Instances.
- G. Split the 12 instances across three Availability Zones in the chosen AWS Region
- H. Run two instances in each Availability Zone as On-Demand Instances with a Savings Plan
- I. Run two instances in each Availability Zone as Spot Instances.
- J. Split the 12 instances across three Availability Zones in the chosen AWS Region
- K. Run three instances in each Availability Zone as On-Demand Instances with Capacity Reservation
- L. Run one instance in each Availability Zone as a Spot Instance.

**Answer:** D

**Explanation:**

By splitting the 12 instances across three Availability Zones, the system can maintain high availability and availability of resources in case of a failure. Option D also uses a combination of On-Demand Instances with Capacity Reservations and Spot Instances, which allows for scheduled jobs to be run on the On-Demand instances with guaranteed capacity, while also taking advantage of the cost savings from Spot Instances for the user jobs which have lower SLA requirements.

**NEW QUESTION 59**

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

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

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

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

**Answer:** CE

**Explanation:**

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

**NEW QUESTION 63**

- (Exam Topic 1)

A company that has multiple AWS accounts is using AWS Organizations. The company's AWS accounts host VPCs, Amazon EC2 instances, and containers.

The company's compliance team has deployed a security tool in each VPC where the company has deployments. The security tools run on EC2 instances and send information to the AWS account that is dedicated for the compliance team. The company has tagged all the compliance-related resources with a key of "costCenter" and a value of "compliance".

The company wants to identify the cost of the security tools that are running on the EC2 instances so that the company can charge the compliance team's AWS account. The cost calculation must be as accurate as possible.

What should a solutions architect do to meet these requirements?

- A. In the management account of the organization, activate the costCenter user-defined tag.
- B. Configure monthly AWS Cost and Usage Reports to save to an Amazon S3 bucket in the management account.
- C. Use the tag breakdown in the report to obtain the total cost for the costCenter tagged resources.
- D. In the member accounts of the organization, activate the costCenter user-defined tag.
- E. Configure monthly AWS Cost and Usage Reports to save to an Amazon S3 bucket in the management account.
- F. Schedule a monthly AWS Lambda function to retrieve the reports and calculate the total cost for the costCenter tagged resources.
- G. In the member accounts of the organization, activate the costCenter user-defined tag.
- H. From the management account, schedule a monthly AWS Cost and Usage Report.
- I. Use the tag breakdown in the report to calculate the total cost for the costCenter tagged resources.
- J. Create a custom report in the organization view in AWS Trusted Advisor.
- K. Configure the report to generate a monthly billing summary for the costCenter tagged resources in the compliance team's AWS account.

**Answer:** A

**Explanation:**

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/custom-tags.html>

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/configurecostallocreport.html>

**NEW QUESTION 67**

- (Exam Topic 1)

A company with global offices has a single 1 Gbps AWS Direct Connect connection to a single AWS Region. The company's on-premises network uses the connection to communicate with the company's resources in the AWS Cloud. The connection has a single private virtual interface that connects to a single VPC. A solutions architect must implement a solution that adds a redundant Direct Connect connection in the same Region. The solution also must provide connectivity to other Regions through the same pair of Direct Connect connections as the company expands into other Regions. Which solution meets these requirements?

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

**Answer:** A

**Explanation:**

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

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

**NEW QUESTION 69**

- (Exam Topic 1)

A company has purchased appliances from different vendors. The appliances all have IoT sensors. The sensors send status information in the vendors' proprietary formats to a legacy application that parses the information into JSON. The parsing is simple, but each vendor has a unique format. Once daily, the application parses all the JSON records and stores the records in a relational database for analysis.

The company needs to design a new data analysis solution that can deliver faster and optimize costs. Which solution will meet these requirements?

- A. Connect the IoT sensors to AWS IoT Cor
- B. Set a rule to invoke an AWS Lambda function to parse the information and save a .csv file to Amazon S3. Use AWS Glue to catalog the file
- C. Use Amazon Athena and Amazon QuickSight for analysis.
- D. Migrate the application server to AWS Fargate, which will receive the information from IoT sensors and parse the information into a relational forma
- E. Save the parsed information to Amazon Redshift for analysis.
- F. Create an AWS Transfer for SFTP serve
- G. Update the IoT sensor code to send the information as a .csv file through SFTP to the serve
- H. Use AWS Glue to catalog the file
- I. Use Amazon Athena for analysis.
- J. Use AWS Snowball Edge to collect data from the IoT sensors directly to perform local analysis.Periodically collect the data into Amazon Redshift to perform global analysis.

**Answer:** A

**Explanation:**

➤ Connect the IoT sensors to AWS IoT Core. Set a rule to invoke an AWS Lambda function to parse the information and save a .csv file to Amazon S3. Use AWS Glue to catalog the files. Use Amazon Athena and Amazon QuickSight for analysis. This solution meets the requirement of faster analysis and cost optimization by using AWS IoT Core to collect data from the IoT sensors in real-time and then using AWS Glue and Amazon Athena for efficient data analysis. This solution involves connecting the IoT sensors to the AWS IoT Core, setting a rule to invoke an AWS Lambda function to parse the information, and saving a .csv file to Amazon S3. AWS Glue can be used to catalog the files and Amazon Athena and Amazon QuickSight can be used for analysis. This solution will enable faster and more cost-effective data analysis.

This solution is in line with the official Amazon Textbook and Resources for the AWS Certified Solutions Architect - Professional certification. In particular, the book states that: "AWS IoT Core can be used to ingest and process the data, AWS Lambda can be used to process and transform the data, and Amazon S3 can be used to store the data. AWS Glue can be used to catalog and access the data, Amazon Athena can be used to query the data, and Amazon QuickSight can be used to visualize the data." (Source: [https://d1.awsstatic.com/training-and-certification/docs-sa-pro/AWS\\_Certified\\_Solutions\\_Architect\\_Professiona](https://d1.awsstatic.com/training-and-certification/docs-sa-pro/AWS_Certified_Solutions_Architect_Professiona))

**NEW QUESTION 72**

- (Exam Topic 1)

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

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

While the company is working on the problem, the solutions architect needs to provide a custom error page instead of the standard ALB error page to visitors.

Which combination of steps will meet this requirement with the LEAST amount of operational overhead? (Choose two.)

- A. Create an Amazon S3 bucke
- B. Configure the S3 bucket to host a static webpag
- C. Upload the custom error pages to Amazon S3.
- D. Create an Amazon CloudWatch alarm to invoke an AWS Lambda function if the ALB health check response Target.FailedHealthChecks is greater than 0. Configure the Lambda function to modify the forwarding rule at the ALB to point to a publicly accessible web server.
- E. Modify the existing Amazon Route 53 records by adding health check
- F. Configure a fallback target if the health check fail

- G. Modify DNS records to point to a publicly accessible webpage.
- H. Create an Amazon CloudWatch alarm to invoke an AWS Lambda function if the ALB health check response `Elb.InternalError` is greater than 0. Configure the Lambda function to modify the forwarding rule at the ALB to point to a public accessible web server.
- I. Add a custom error response by configuring a CloudFront custom error pag
- J. Modify DNS records to point to a publicly accessible web page.

**Answer:** CE

**Explanation:**

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

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

**NEW QUESTION 76**

- (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 81**

- (Exam Topic 1)

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

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

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

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

**Answer:** AD

**Explanation:**

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

provisioning a Gateway Load Balancer for each Availability Zone, the traffic is redirected to the security tool in the event of any failures or outages. This ensures that the security tool is always available to inspect the traffic, even in the event of a failure.

#### NEW QUESTION 82

- (Exam Topic 1)

A video streaming company recently launched a mobile app for video sharing. The app uploads various files to an Amazon S3 bucket in the us-east-1 Region. The files range in size from 1 GB to 10 GB.

Users who access the app from Australia have experienced uploads that take long periods of time. Sometimes the files fail to completely upload for these users. A solutions architect must improve the app's performance for these uploads.

Which solutions will meet these requirements? (Select TWO.)

- A. Enable S3 Transfer Acceleration on the S3 bucket. Configure the app to use the Transfer Acceleration endpoint for uploads.
- B. Configure an S3 bucket in each Region to receive the upload.
- C. Use S3 Cross-Region Replication to copy the files to the distribution S3 bucket.
- D. Set up Amazon Route 53 with latency-based routing to route the uploads to the nearest S3 bucket Region.
- E. Configure the app to break the video files into chunks. Use a multipart upload to transfer files to Amazon S3.
- F. Modify the app to add random prefixes to the files before uploading.

**Answer:** AD

#### Explanation:

<https://aws.amazon.com/premiumsupport/knowledge-center/s3-upload-large-files/>

Enabling S3 Transfer Acceleration on the S3 bucket and configuring the app to use the Transfer Acceleration endpoint for uploads will improve the app's performance for these uploads by leveraging Amazon CloudFront's globally distributed edge locations to accelerate the uploads. Breaking the video files into chunks and using a multipart upload to transfer files to Amazon S3 will also improve the app's performance by allowing parts of the file to be uploaded in parallel, reducing the overall upload time.

#### NEW QUESTION 87

- (Exam Topic 1)

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

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

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 91

- (Exam Topic 1)

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

A solutions architect must implement a redirect service that accepts HTTP and HTTPS requests.

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

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

**Answer:** CEF

#### Explanation:

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

#### NEW QUESTION 96

- (Exam Topic 1)

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

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

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

**Answer:** ACF

**Explanation:**

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

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

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

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

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

These recommendations are in line with the official Amazon Textbook and Resources for the AWS Certified Solutions Architect - Professional certification. In particular, the book states that "You can use cost allocation tags to group your costs by application, team, or other categories" (Source:

[https://d1.awsstatic.com/training-and-certification/docs-sa-pro/AWS\\_Certified\\_Solutions\\_Architect\\_Professiona](https://d1.awsstatic.com/training-and-certification/docs-sa-pro/AWS_Certified_Solutions_Architect_Professiona) Additionally, the book states that "Cost Explorer enables you to view the costs of your AWS resources over the last 12 months and to create forecasts for the next 12 months" (Source:

[https://d1.awsstatic.com/training-and-certification/docs-sa-pro/AWS\\_Certified\\_Solutions\\_Architect\\_Professiona](https://d1.awsstatic.com/training-and-certification/docs-sa-pro/AWS_Certified_Solutions_Architect_Professiona)

**NEW QUESTION 97**

- (Exam Topic 1)

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

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

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

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

**Answer:** BD

**Explanation:**

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

**NEW QUESTION 100**

- (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 101**

- (Exam Topic 1)

A company runs a serverless application in a single AWS Region. The application accesses external URLs and extracts metadata from those sites. The company uses an Amazon Simple Notification Service (Amazon SNS) topic to publish URLs to an Amazon Simple Queue Service (Amazon SQS) queue. An AWS Lambda function uses the queue as an event source and processes the URLs from the queue. Results are saved to an Amazon S3 bucket.

The company wants to process each URL in other Regions to compare possible differences in site localization. URLs must be published from the existing Region. Results must be written to the existing S3 bucket in the current Region.

Which combination of changes will produce multi-Region deployment that meets these requirements? (Select TWO.)

- A. Deploy the SQS queue with the Lambda function to other Regions.
- B. Subscribe the SNS topic in each Region to the SQS queue.
- C. Subscribe the SQS queue in each Region to the SNS topics in each Region.
- D. Configure the SQS queue to publish URLs to SNS topics in each Region.

E. Deploy the SNS topic and the Lambda function to other Regions.

**Answer:** AC

**Explanation:**

<https://docs.aws.amazon.com/sns/latest/dg/sns-cross-region-delivery.html>

#### NEW QUESTION 106

- (Exam Topic 1)

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

Which solution will meet this requirement?

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 111

- (Exam Topic 1)

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

Which solution will meet these requirements with the LEAST effort?

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

**Answer:** C

**Explanation:**

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

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

Reference:

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

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

#### NEW QUESTION 116

- (Exam Topic 1)

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

What should the solutions architect do to meet these requirements?

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

**Answer:** C

**Explanation:**

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

CloudFormation StackSets allows creating, updating, and deleting stacks across multiple accounts and regions in an organization. This solution allows creating a

single CloudFormation template that can be deployed across multiple accounts and regions, and also allows for the management of access and permissions for the different accounts through the use of IAM roles and policies in the management account.

#### NEW QUESTION 118

- (Exam Topic 1)

A delivery company needs to migrate its third-party route planning application to AWS. The third party supplies a supported Docker image from a public registry. The image can run in as many containers as required to generate the route map.

The company has divided the delivery area into sections with supply hubs so that delivery drivers travel the shortest distance possible from the hubs to the customers. To reduce the time necessary to generate route maps, each section uses its own set of Docker containers with a custom configuration that processes orders only in the section's area.

The company needs the ability to allocate resources cost-effectively based on the number of running containers.

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

- A. Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster on Amazon EC2. Use the Amazon EKS CLI to launch the planning application in pods by using the `-tags` option to assign a custom tag to the pod.
- B. Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster on AWS Fargate
- C. Use the Amazon EKS CLI to launch the planning applicatio
- D. Use the AWS CLI `tag-resource` API call to assign a custom tag to the pod.
- E. Create an Amazon Elastic Container Service (Amazon ECS) cluster on Amazon EC2. Use the AWS CLI with `run-tasks` set to `true` to launch the planning application by using the `-tags` option to assign a custom tag to the task.
- F. Create an Amazon Elastic Container Service (Amazon ECS) cluster on AWS Fargate
- G. Use the AWS CLI `run-task` command and set `enableECSTags` to `true` to launch the planning applicatio
- H. Use the `--tags` option to assign a custom tag to the task.

**Answer:** D

#### Explanation:

Amazon Elastic Container Service (ECS) on AWS Fargate is a fully managed service that allows you to run containers without having to manage the underlying infrastructure. When you launch tasks on Fargate,

resources are automatically allocated based on the number of tasks running, which reduces the operational overhead.

Using ECS on Fargate allows you to assign custom tags to tasks using the `--tags` option in the `run-task` command, as described in the documentation:

<https://docs.aws.amazon.com/cli/latest/reference/ecs/run-task.html> You can also set `enableECSTags` to `true`, which allows the service to automatically add the cluster name and service name as tags.

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/task-placement-constraints.html#tag-based-sch>

#### NEW QUESTION 123

- (Exam Topic 1)

An adventure company has launched a new feature on its mobile app. Users can use the feature to upload their hiking and raftering photos and videos anytime. The photos and videos are stored in Amazon S3 Standard storage in an S3 bucket and are served through Amazon CloudFront.

The company needs to optimize the cost of the storage. A solutions architect discovers that most of the uploaded photos and videos are accessed infrequently after 30 days. However, some of the uploaded photos and videos are accessed frequently after 30 days. The solutions architect needs to implement a solution that maintains millisecond retrieval availability of the photos and videos at the lowest possible cost.

Which solution will meet these requirements?

- A. Configure S3 Intelligent-Tiering on the S3 bucket.
- B. Configure an S3 Lifecycle policy to transition image objects and video objects from S3 Standard to S3 Glacier Deep Archive after 30 days.
- C. Replace Amazon S3 with an Amazon Elastic File System (Amazon EFS) file system that is mounted on Amazon EC2 instances.
- D. Add a Cache-Control: max-age header to the S3 image objects and S3 video object
- E. Set the header to 30 days.

**Answer:** A

#### Explanation:

Amazon S3 Intelligent-Tiering is a storage class that automatically moves objects between two access tiers based on changing access patterns. Objects that are accessed frequently are stored in the frequent access tier and objects that are accessed infrequently are stored in the infrequent access tier. This allows for cost optimization without requiring manual intervention. This makes it an ideal solution for the scenario described, as it can automatically move objects that are infrequently accessed after 30 days to a lower-cost storage tier while still maintaining millisecond retrieval availability.

#### NEW QUESTION 127

- (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 132

- (Exam Topic 1)

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

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

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

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

**Answer:** A

#### Explanation:

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

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

### NEW QUESTION 135

- (Exam Topic 1)

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

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

Which solution will meet these requirements?

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

**Answer:** C

#### Explanation:

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

### NEW QUESTION 139

- (Exam Topic 1)

A health insurance company stores personally identifiable information (PII) in an Amazon S3 bucket. The company uses server-side encryption with S3 managed encryption keys (SSE-S3) to encrypt the objects. According to a new requirement, all current and future objects in the S3 bucket must be encrypted by keys that the company's security team manages. The S3 bucket does not have versioning enabled. Which solution will meet these requirements?

- A. In the S3 bucket properties, change the default encryption to SSE-S3 with a customer managed key.
- B. Use the AWS CLI to re-upload all objects in the S3 bucket.
- C. Set an S3 bucket policy to deny unencrypted PutObject requests.
- D. In the S3 bucket properties, change the default encryption to server-side encryption with AWS KMS managed encryption keys (SSE-KMS). Set an S3 bucket policy to deny unencrypted PutObject request.
- E. Use the AWS CLI to re-upload all objects in the S3 bucket.
- F. In the S3 bucket properties, change the default encryption to server-side encryption with AWS KMS managed encryption keys (SSE-KMS). Set an S3 bucket policy to automatically encrypt objects on GetObject and PutObject requests.
- G. In the S3 bucket properties, change the default encryption to AES-256 with a customer managed key. Attach a policy to deny unencrypted PutObject requests to any entities that access the S3 bucket.
- H. Use the AWS CLI to re-upload all objects in the S3 bucket.

**Answer:** D

#### Explanation:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/ServerSideEncryptionCustomerKeys.html> Clearly says we need following header for SSE-C: x-amz-server-side-encryption-customer-algorithm. Use this header to specify the encryption algorithm. The header value must be AES256.

#### NEW QUESTION 141

- (Exam Topic 1)

A company wants to use AWS to create a business continuity solution in case the company's main on-premises application fails. The application runs on physical servers that also run other applications. The on-premises application that the company is planning to migrate uses a MySQL database as a data store. All the company's on-premises applications use operating systems that are compatible with Amazon EC2.

Which solution will achieve the company's goal with the LEAST operational overhead?

- A. Install the AWS Replication Agent on the source servers, including the MySQL server
- B. Set up replication for all server
- C. Launch test instances for regular drill
- D. Cut over to the test instances to fail over the workload in the case of a failure event.
- E. Install the AWS Replication Agent on the source servers, including the MySQL server
- F. Initialize AWS Elastic Disaster Recovery in the target AWS Region
- G. Define the launch setting
- H. Frequently perform failover and fallback from the most recent point in time.
- I. Create AWS Database Migration Service (AWS DMS) replication servers and a target Amazon Aurora MySQL DB cluster to host the databases
- J. Create a DMS replication task to copy the existing data to the target DB cluster
- K. Create a local AWS Schema Conversion Tool (AWS SCT) change data capture (CDC) task to keep the data synchronized
- L. Install the rest of the software on EC2 instances by starting with a compatible base AMI.
- M. Deploy an AWS Storage Gateway Volume Gateway on-premise
- N. Mount volumes on all on-premises server
- O. Install the application and the MySQL database on the new volume
- P. Take regular snapshot
- Q. Install all the software on EC2 instances by starting with a compatible base AMI
- R. Launch a Volume Gateway on an EC2 instance
- S. Restore the volumes from the latest snapshot
- T. Mount the new volumes on the EC2 instances in the case of a failure event.

**Answer: B**

#### Explanation:

<https://docs.aws.amazon.com/drs/latest/userguide/what-is-drs.html> <https://docs.aws.amazon.com/drs/latest/userguide/recovery-workflow-gs.html>

#### NEW QUESTION 146

- (Exam Topic 1)

A company is running an application in the AWS Cloud. Recent application metrics show inconsistent response times and a significant increase in error rates. Calls to third-party services are causing the delays. Currently, the application calls third-party services synchronously by directly invoking an AWS Lambda function.

A solutions architect needs to decouple the third-party service calls and ensure that all the calls are eventually completed.

Which solution will meet these requirements?

- A. Use an Amazon Simple Queue Service (Amazon SQS) queue to store events and invoke the Lambda function.
- B. Use an AWS Step Functions state machine to pass events to the Lambda function.
- C. Use an Amazon EventBridge rule to pass events to the Lambda function.
- D. Use an Amazon Simple Notification Service (Amazon SNS) topic to store events and invoke the Lambda function.

**Answer: A**

#### Explanation:

Using an SQS queue to store events and invoke the Lambda function will decouple the third-party service calls and ensure that all the calls are eventually completed. SQS allows you to store messages in a queue and process them asynchronously, which eliminates the need for the application to wait for a response from the third-party service. The messages will be stored in the SQS queue until they are processed by the Lambda function, even if the Lambda function is currently unavailable or busy. This will ensure that all the calls are eventually completed, even if there are delays or errors.

AWS Step Functions state machines can also be used to pass events to the Lambda function, but it would require additional management and configuration to set up the state machine, which would increase operational overhead.

Amazon EventBridge rule can also be used to pass events to the Lambda function, but it would not provide the same level of decoupling and reliability as SQS.

Using Amazon Simple Notification Service (Amazon SNS) topic to store events and invoke the Lambda function, is similar to SQS, but SNS is a publish-subscribe messaging service and SQS is a queue service. SNS is used for sending messages to multiple recipients, SQS is used for sending messages to a single recipient, so SQS is more appropriate for this use case.

References:

- > [AWS SQS](#)
- > [AWS Step Functions](#)
- > [AWS EventBridge](#)
- > [AWS SNS](#)

#### NEW QUESTION 147

- (Exam Topic 1)

A solutions architect is auditing the security setup of an AWS Lambda function for a company. The Lambda function retrieves the latest changes from an Amazon Aurora database. The Lambda function and the database run in the same VPC. Lambda environment variables are providing the database credentials to the Lambda function.

The Lambda function aggregates data and makes the data available in an Amazon S3 bucket that is configured for server-side encryption with AWS KMS managed encryption keys (SSE-KMS). The data must not travel across the internet. If any database credentials become compromised, the company needs a solution that minimizes the impact of the compromise.

What should the solutions architect recommend to meet these requirements?

- A. Enable IAM database authentication on the Aurora DB cluster
- B. Change the IAM role for the Lambda function to allow the function to access the database by using IAM database authentication
- C. Deploy a gateway VPC endpoint for Amazon S3 in the VPC.
- D. Enable IAM database authentication on the Aurora DB cluster

- E. Change the IAM role for the Lambda function to allow the function to access the database by using IAM database authenticatio
- F. Enforce HTTPS on the connection to Amazon S3 during data transfers.
- G. Save the database credentials in AWS Systems Manager Parameter Stor
- H. Set up password rotation on the credentials in Parameter Stor
- I. Change the IAM role for the Lambda function to allow the function to access Parameter Stor
- J. Modify the Lambda function to retrieve the credentials from Parameter Stor
- K. Deploy a gateway VPC endpoint for Amazon S3 in the VPC.
- L. Save the database credentials in AWS Secrets Manage
- M. Set up password rotation on the credentials in Secrets Manage
- N. Change the IAM role for the Lambda function to allow the function to access Secrets Manage
- O. Modify the Lambda function to retrieve the credentials Om Secrets Manage
- P. Enforce HTTPS on the connection to Amazon S3 during data transfers.

**Answer:** A

**Explanation:**

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/UsingWithRDS.IAMDBAuth.html>

**NEW QUESTION 148**

- (Exam Topic 1)

A start up company hosts a fleet of Amazon EC2 instances in private subnets using the latest Amazon Linux 2 AMI. The company's engineers rely heavily on SSH access to the instances for troubleshooting.

The company's existing architecture includes the following:

- A VPC with private and public subnets, and a NAT gateway
- Site-to-Site VPN for connectivity with the on-premises environment
- EC2 security groups with direct SSH access from the on-premises environment

The company needs to increase security controls around SSH access and provide auditing of commands executed by the engineers.

Which strategy should a solutions architect use?

- A. Install and configure EC2 Instance Connect on the fleet of EC2 instance
- B. Remove all security group rules attached to EC2 instances that allow inbound TCP on port 22. Advise the engineers to remotely access the instances by using the EC2 Instance Connect CLI.
- C. Update the EC2 security groups to only allow inbound TCP on port 22 to the IP addresses of the engineer's device
- D. Install the Amazon CloudWatch agent on all EC2 instances and send operating system audit logs to CloudWatch Logs.
- E. Update the EC2 security groups to only allow inbound TCP on port 22 to the IP addresses of the engineer's device
- F. Enable AWS Config for EC2 security group resource change
- G. Enable AWS Firewall Manager and apply a security group policy that automatically remediates changes to rules.
- H. Create an IAM role with the AmazonSSMManagedInstanceCore managed policy attache
- I. Attach the IAM role to all the EC2 instance
- J. Remove all security group rules attached to the EC2 instances that allow inbound TCP on port 22. Have the engineers install the AWS Systems Manager Session Manager plugin for their devices and remotely access the instances by using the start-session API call from Systems Manager.

**Answer:** D

**Explanation:**

Allows client machines to be able to connect to Session Manager using the AWS CLI instead of going through the AWS EC2 or AWS Server Manager console.

<https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager-working-with-install-plugin.ht> [https://docs.aws.amazon.com/systems-](https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager-working-with-install-plugin.ht)

**NEW QUESTION 151**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SAP-C02 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SAP-C02 Product From:

<https://www.2passeasy.com/dumps/SAP-C02/>

## Money Back Guarantee

### **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