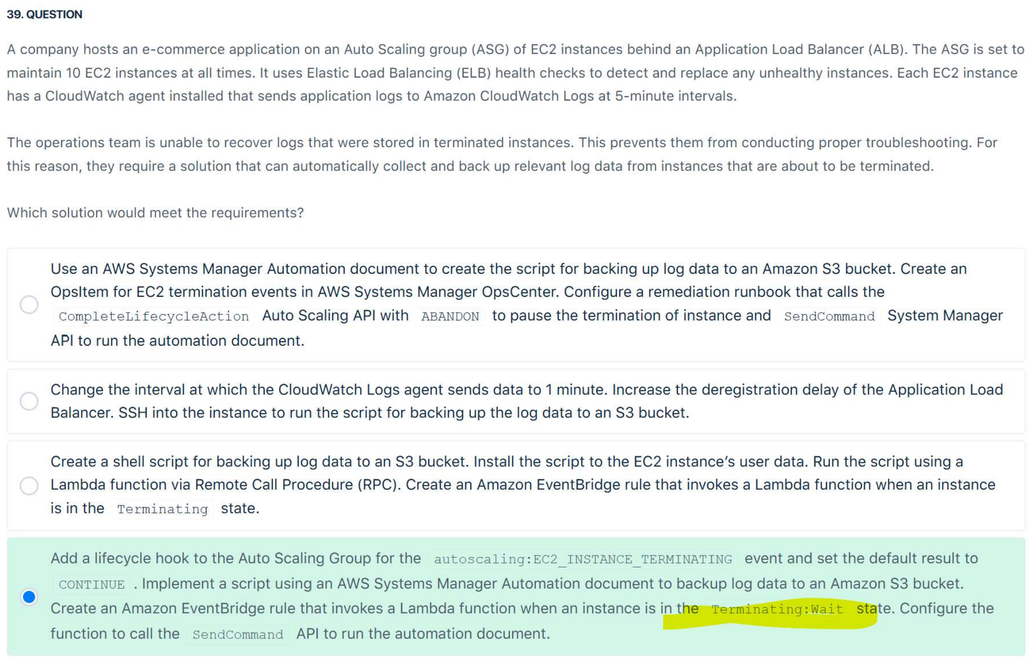
questoes revisas 3

Notebook:	我的第一个笔记本		
Created:	11/12/2025 00:12	Updated:	11/12/2025 07:26
Author:	erikachen19@gmail.com		
URL:	https://portal.tutorialsdojo.com/courses/aws-certified-solutions-architect-professional…		



39. QUESTION

A company hosts an e-commerce application on an Auto Scaling group (ASG) of EC2 instances behind an Application Load Balancer (ALB). The ASG is set to maintain 10 EC2 instances at all times. It uses Elastic Load Balancing (ELB) health checks to detect and replace any unhealthy instances. Each EC2 instance has a CloudWatch agent installed that sends application logs to Amazon CloudWatch Logs at 5-minute intervals.

The operations team is unable to recover logs that were stored in terminated instances. This prevents them from conducting proper troubleshooting. For this reason, they require a solution that can automatically collect and back up relevant log data from instances that are about to be terminated.

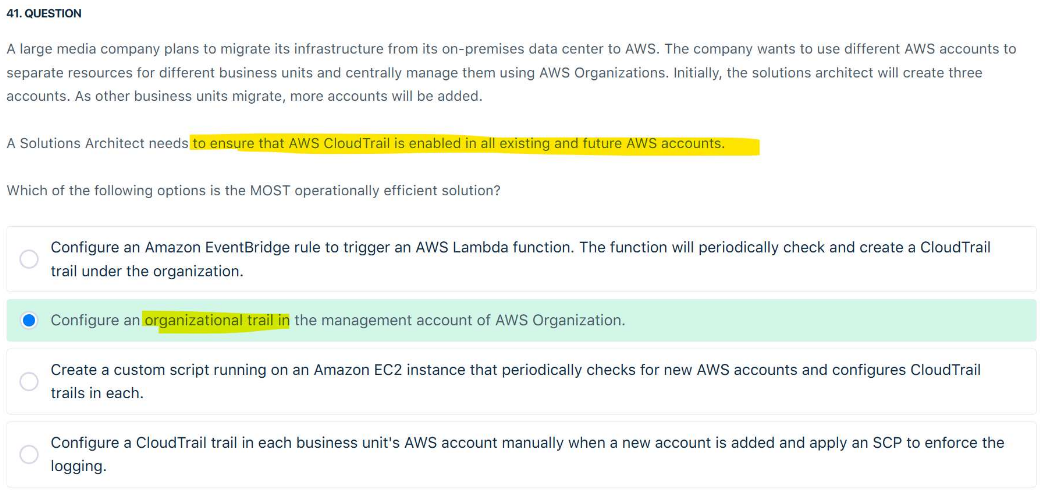
Which solution would meet the requirements?

○ Use an AWS Systems Manager Automation document to create the script for backing up log data to an Amazon S3 bucket. Create an OpsItem for EC2 termination events in AWS Systems Manager OpsCenter. Configure a remediation runbook that calls the `CompleteLifecycleAction` Auto Scaling API with `ABANDON` to pause the termination of instance and `SendCommand` System Manager API to run the automation document.

○ Change the interval at which the CloudWatch Logs agent sends data to 1 minute. Increase the deregistration delay of the Application Load Balancer. SSH into the instance to run the script for backing up the log data to an S3 bucket.

○ Create a shell script for backing up log data to an S3 bucket. Install the script to the EC2 instance's user data. Run the script using a Lambda function via Remote Call Procedure (RPC). Create an Amazon EventBridge rule that invokes a Lambda function when an instance is in the `Terminating` state.

● Add a lifecycle hook to the Auto Scaling Group for the `autoscaling:EC2_INSTANCE_TERMINATING` event and set the default result to `CONTINUE`. Implement a script using an AWS Systems Manager Automation document to backup log data to an Amazon S3 bucket. Create an Amazon EventBridge rule that invokes a Lambda function when an instance is in the `Terminating:Wait` state. Configure the function to call the `SendCommand` API to run the automation document.



41. QUESTION

A large media company plans to migrate its infrastructure from its on-premises data center to AWS. The company wants to use different AWS accounts to separate resources for different business units and centrally manage them using AWS Organizations. Initially, the solutions architect will create three accounts. As other business units migrate, more accounts will be added.

A Solutions Architect needs to ensure that AWS CloudTrail is enabled in all existing and future AWS accounts.

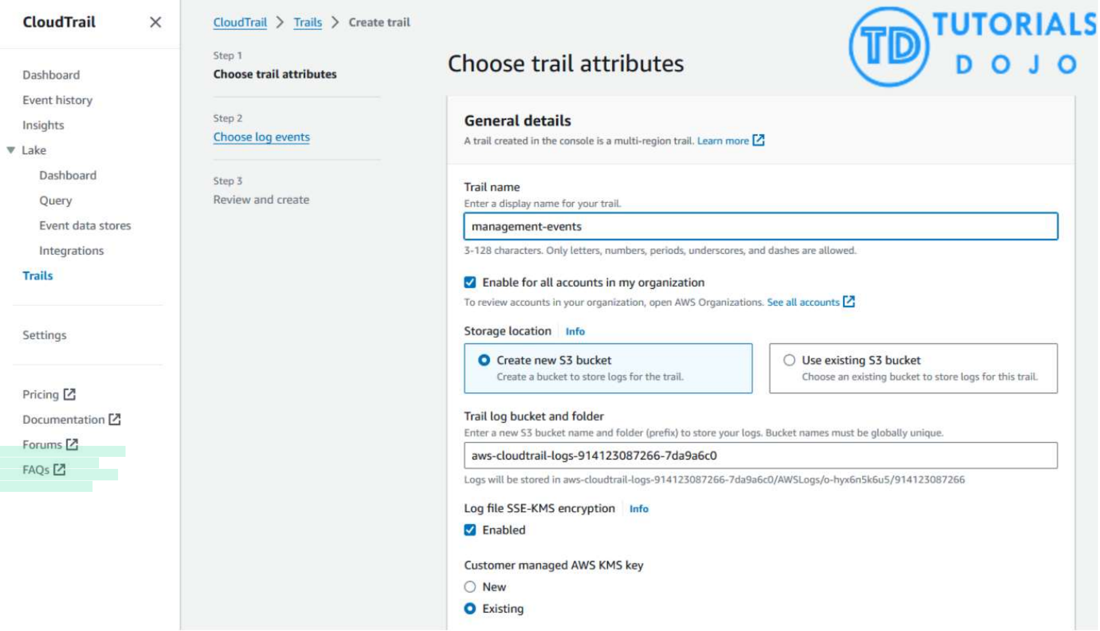
Which of the following options is the MOST operationally efficient solution?

○ Configure an Amazon EventBridge rule to trigger an AWS Lambda function. The function will periodically check and create a CloudTrail trail under the organization.

● Configure an organizational trail in the management account of AWS Organization.

○ Create a custom script running on an Amazon EC2 instance that periodically checks for new AWS accounts and configures CloudTrail trails in each.

○ Configure a CloudTrail trail in each business unit's AWS account manually when a new account is added and apply an SCP to enforce the logging.



Choose trail attributes

General details

A trail created in the console is a multi-region trail. Learn more

Trail name
Enter a display name for your trail.
management-events
3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

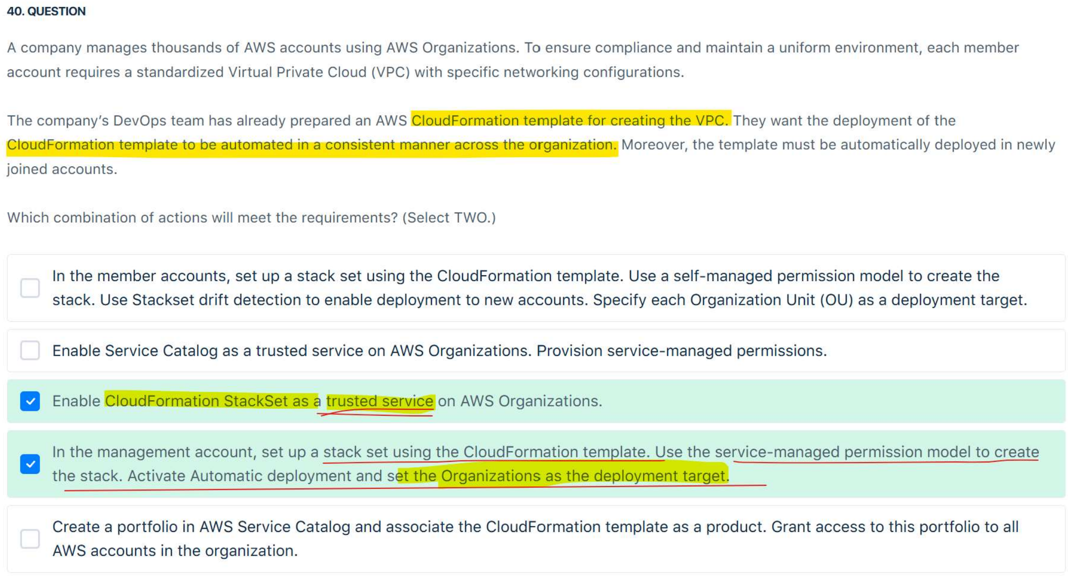
☑ Enable for all accounts in my organization
To review accounts in your organization, open AWS Organizations. See all accounts

Storage location Info
● Create new S3 bucket
Create a bucket to store logs for the trail.
○ Use existing S3 bucket
Choose an existing bucket to store logs for this trail.

Trail log bucket and folder
Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.
aws-cloudtrail-logs-914123087266-7da9a6c0
Logs will be stored in aws-cloudtrail-logs-914123087266-7da9a6c0/AWSLogs/o-hyx6n5k6u5/914123087266

Log file SSE-KMS encryption Info
☑ Enabled

Customer managed AWS KMS key
○ New
● Existing



40. QUESTION

A company manages thousands of AWS accounts using AWS Organizations. To ensure compliance and maintain a uniform environment, each member account requires a standardized Virtual Private Cloud (VPC) with specific networking configurations.

The company's DevOps team has already prepared an AWS CloudFormation template for creating the VPC. They want the deployment of the CloudFormation template to be automated in a consistent manner across the organization. Moreover, the template must be automatically deployed in newly joined accounts.

Which combination of actions will meet the requirements? (Select TWO.)

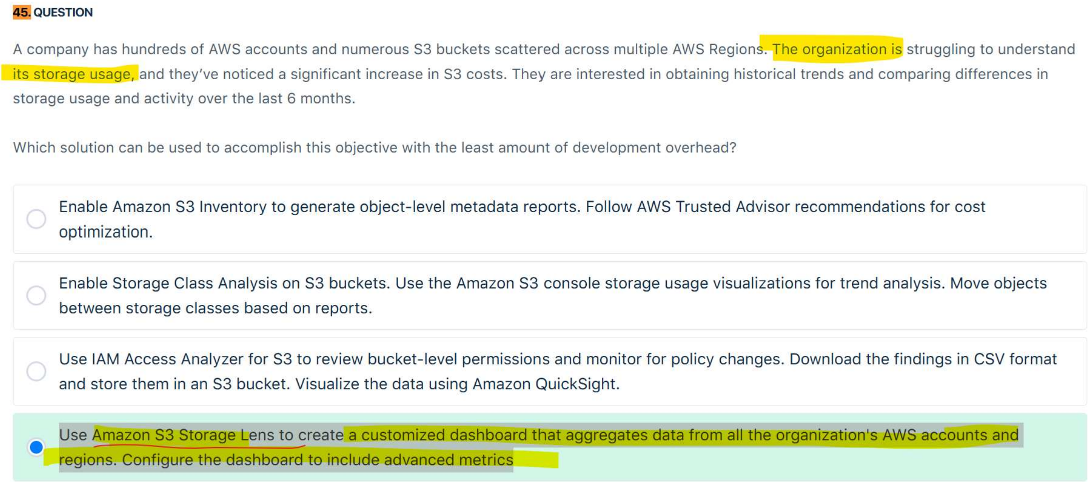
☐ In the member accounts, set up a stack set using the CloudFormation template. Use a self-managed permission model to create the stack. Use Stackset drift detection to enable deployment to new accounts. Specify each Organization Unit (OU) as a deployment target.

☐ Enable Service Catalog as a trusted service on AWS Organizations. Provision service-managed permissions.

☑ Enable CloudFormation StackSet as a trusted service on AWS Organizations.

☑ In the management account, set up a stack set using the CloudFormation template. Use the service-managed permission model to create the stack. Activate Automatic deployment and set the Organizations as the deployment target.

☐ Create a portfolio in AWS Service Catalog and associate the CloudFormation template as a product. Grant access to this portfolio to all AWS accounts in the organization.



45. QUESTION

A company has hundreds of AWS accounts and numerous S3 buckets scattered across multiple AWS Regions. The organization is struggling to understand its storage usage, and they've noticed a significant increase in S3 costs. They are interested in obtaining historical trends and comparing differences in storage usage and activity over the last 6 months.

Which solution can be used to accomplish this objective with the least amount of development overhead?

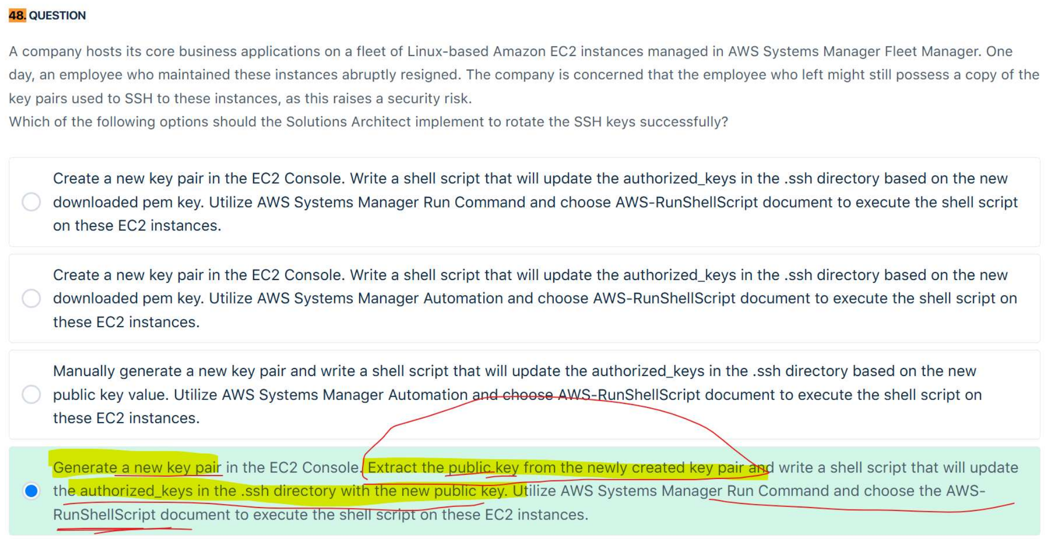
○ Enable Amazon S3 Inventory to generate object-level metadata reports. Follow AWS Trusted Advisor recommendations for cost optimization.

○ Enable Storage Class Analysis on S3 buckets. Use the Amazon S3 console storage usage visualizations for trend analysis. Move objects between storage classes based on reports.

○ Use IAM Access Analyzer for S3 to review bucket-level permissions and monitor for policy changes. Download the findings in CSV format and store them in an S3 bucket. Visualize the data using Amazon QuickSight.

● Use Amazon S3 Storage Lens to create a customized dashboard that aggregates data from all the organization's AWS accounts and regions. Configure the dashboard to include advanced metrics

Ask for access to the Migration Evaluator to begin the TCO assessment. Use the Migration Evaluator Collector to gather data from your on-premises and then import the data. Export a Migration Evaluator Quick Insights report to evaluate the Total Cost of Ownership (TCO) for migrating workloads to AWS.



48. QUESTION

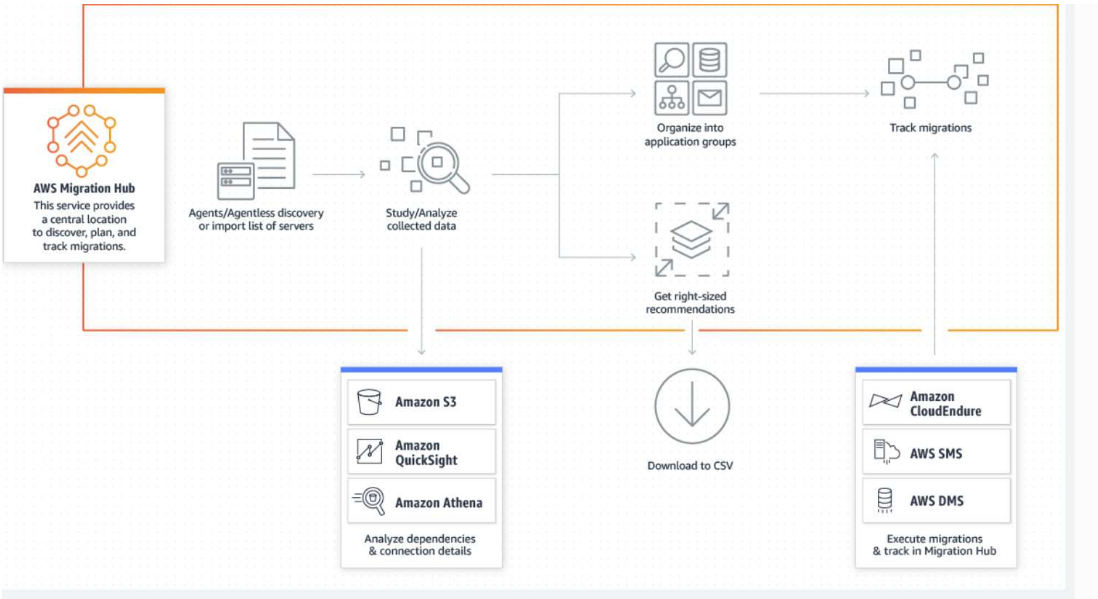
A company hosts its core business applications on a fleet of Linux-based Amazon EC2 instances managed in AWS Systems Manager Fleet Manager. One day, an employee who maintained these instances abruptly resigned. The company is concerned that the employee who left might still possess a copy of the key pairs used to SSH to these instances, as this raises a security risk.
Which of the following options should the Solutions Architect implement to rotate the SSH keys successfully?

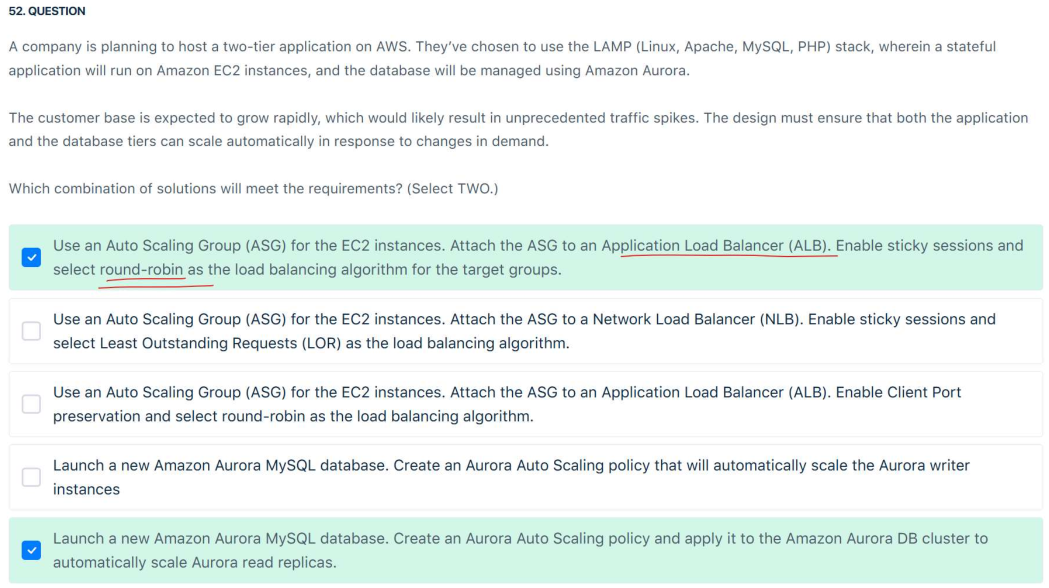
○ Create a new key pair in the EC2 Console. Write a shell script that will update the authorized_keys in the .ssh directory based on the new downloaded pem key. Utilize AWS Systems Manager Run Command and choose AWS-RunShellScript document to execute the shell script on these EC2 instances.

○ Create a new key pair in the EC2 Console. Write a shell script that will update the authorized_keys in the .ssh directory based on the new downloaded pem key. Utilize AWS Systems Manager Automation and choose AWS-RunShellScript document to execute the shell script on these EC2 instances.

○ Manually generate a new key pair and write a shell script that will update the authorized_keys in the .ssh directory based on the new public key value. Utilize AWS Systems Manager Automation and choose AWS-RunShellScript document to execute the shell script on these EC2 instances.

● Generate a new key pair in the EC2 Console. Extract the public key from the newly created key pair and write a shell script that will update the authorized_keys in the .ssh directory with the new public key. Utilize AWS Systems Manager Run Command and choose the AWS-RunShellScript document to execute the shell script on these EC2 instances.


AWS Migration Hub
This service provides a central location to discover, plan, and track migrations.
Agents/Agentless discovery or import list of servers
Study/Analyze collected data
Organize into application groups
Get right-sized recommendations
Track migrations
Amazon S3
Amazon QuickSight
Amazon Athena
Analyze dependencies & connection details
Download to CSV
Amazon CloudEndure
AWS SMS
AWS DMS
Execute migrations & track in Migration Hub



52. QUESTION

A company is planning to host a two-tier application on AWS. They've chosen to use the LAMP (Linux, Apache, MySQL, PHP) stack, wherein a stateful application will run on Amazon EC2 instances, and the database will be managed using Amazon Aurora.

The customer base is expected to grow rapidly, which would likely result in unprecedented traffic spikes. The design must ensure that both the application and the database tiers can scale automatically in response to changes in demand.

Which combination of solutions will meet the requirements? (Select TWO.)

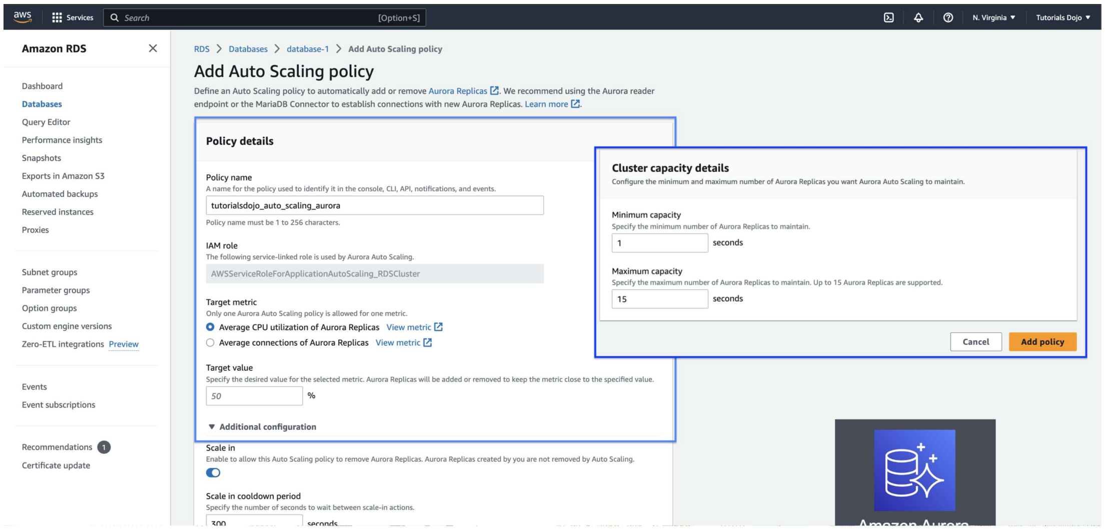
☑ Use an Auto Scaling Group (ASG) for the EC2 instances. Attach the ASG to an Application Load Balancer (ALB). Enable sticky sessions and select round-robin as the load balancing algorithm for the target groups.

□ Use an Auto Scaling Group (ASG) for the EC2 instances. Attach the ASG to a Network Load Balancer (NLB). Enable sticky sessions and select Least Outstanding Requests (LOR) as the load balancing algorithm.

□ Use an Auto Scaling Group (ASG) for the EC2 instances. Attach the ASG to an Application Load Balancer (ALB). Enable Client Port preservation and select round-robin as the load balancing algorithm.

□ Launch a new Amazon Aurora MySQL database. Create an Aurora Auto Scaling policy that will automatically scale the Aurora writer instances

☑ Launch a new Amazon Aurora MySQL database. Create an Aurora Auto Scaling policy and apply it to the Amazon Aurora DB cluster to automatically scale Aurora read replicas.



Add Auto Scaling policy

Define an Auto Scaling policy to automatically add or remove Aurora Replicas. We recommend using the Aurora reader endpoint or the MariaDB Connector to establish connections with new Aurora Replicas. Learn more.

Policy details

Policy name
A name for the policy used to identify it in the console, CLI, API, notifications, and events.
tutorialsdojo_auto_scaling_aurora
Policy name must be 1 to 256 characters.

IAM role
The following service-linked role is used by Aurora Auto Scaling.
AWSServiceRoleForApplicationAutoScaling_RDSCluster

Target metric
Only one Aurora Auto Scaling policy is allowed for one metric.
● Average CPU utilization of Aurora Replicas View metric
○ Average connections of Aurora Replicas View metric

Target value
Specify the desired value for the selected metric. Aurora Replicas will be added or removed to keep the metric close to the specified value.
50 %

▼ Additional configuration

Scale in
Enable to allow this Auto Scaling policy to remove Aurora Replicas. Aurora Replicas created by you are not removed by Auto Scaling.

Scale in cooldown period
Specify the number of seconds to wait between scale-in actions.
300 seconds

Cluster capacity details
Configure the minimum and maximum number of Aurora Replicas you want Aurora Auto Scaling to maintain.

Minimum capacity
Specify the minimum number of Aurora Replicas to maintain.
1 seconds

Maximum capacity
Specify the maximum number of Aurora Replicas to maintain. Up to 15 Aurora Replicas are supported.
15 seconds

53. QUESTION

A company is managing a hybrid environment comprising on-premises servers and Amazon EC2 instances. Their servers are a mix of Linux and Windows systems. The company utilizes AWS Security Hub as its cloud security posture management (CSPM) service to automate security best practice checks, aggregate alerts, and enables automated remediation.

Separate teams handle the environment, each using different tools for patching. The company wants to simplify this process and requires a consolidated view of patch statuses across all servers.

Which combination of actions will meet the requirements? (Select TWO.)

☑ Generate patch compliance reports using AWS System Manager Patch Manager.

□ Create a custom AWS Config rule for detecting non-compliant patches across servers. Set up an AWS Config remediation rule using AWS Systems Manager Automation documents to apply patches. Configure AWS Config to send patch compliance reports to an Amazon S3 bucket.

☑ Register all servers as managed nodes in AWS System Manager. Use AWS System Manager Patch Manager for handling patch operations.

□ Generate patch compliance reports using Amazon Inspector. Use Amazon Athena for aggregating and viewing patch compliance reports.

□ Create an AWS Systems Manager Automation document for running patching jobs. Use Amazon EventBridge to schedule these jobs and configure the AWS Systems Manager OpsCenter to generate patch compliance reports.

61. QUESTION

A company hosts an SFTP server in an Amazon EC2 instance with an Elastic IP address inside a VPC. The SFTP server acts as a central repository for uploading inventory data of its partners. The partner companies connect to the server via the Elastic IP address and use SSH for authentication. The security group of the EC2 instance is restricted to allow only the IP addresses of the partner companies. The solutions architect has been tasked to improve the current solution, increase the availability of the server, and minimize the management complexity of the infrastructure. The company wants minimal disruption for its partners and it should retain the current process on how the partners connect to the SFTP server.

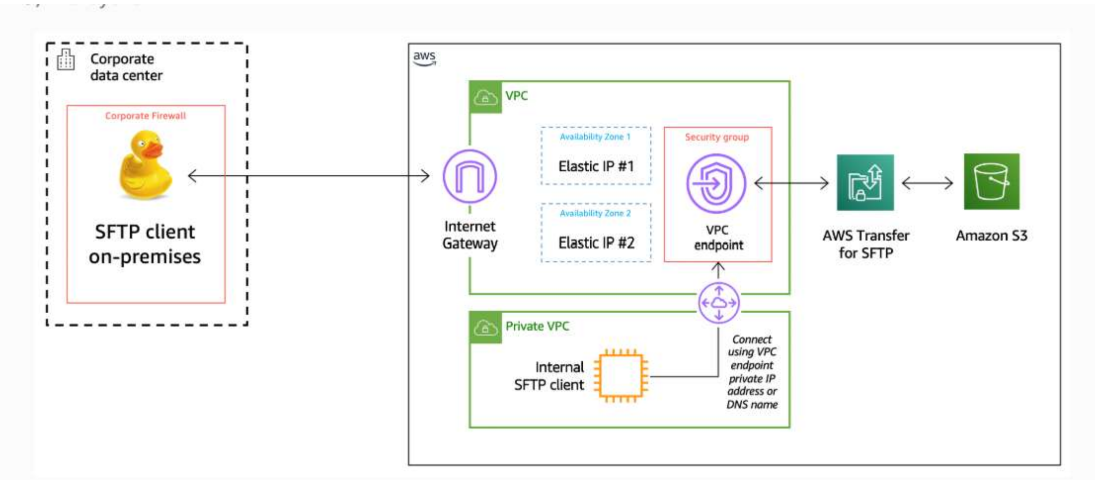
Which of the following implementations will meet the company requirements?

● Create a new Amazon S3 bucket to host the files for the SFTP server. Create an AWS Transfer Family server inside the VPC with an internet-facing endpoint. Disassociate the Elastic IP address from the EC2 instance and associate it to the new endpoint. Create a security group for the endpoint to allow only the IP addresses of the partner companies. Set the S3 bucket as the destination for the AWS Transfer Family server and copy all the SFTP server files to the S3 bucket.

○ Create an AWS Fargate task definition to run the SFTP server. Create a new Amazon Elastic File System (EFS) volume and add it as a mount point in the task definition. Sync all the SFTP server files to the EFS volume. Create a Fargate service using the task definition and place it behind a Network Load Balancer (NLB). Disassociate the Elastic IP address from the EC2 instance and associate it to the NLB. Create a security group for the Fargate service to allow only the IP addresses of the partner companies.

○ Create an Auto Scaling group of Amazon EC2 instances that run the SFTP server and place it behind a Network Load Balancer. Create a multi-attach Amazon EBS volume to be mounted on all the EC2 instances in the cluster. Sync all the SFTP server files to the multi-attach volume. Disassociate the Elastic IP address from the EC2 instance and associate it to the NLB. Create a security group for the Auto Scaling group to allow only the IP addresses of the partner companies.

○ Create a new Amazon S3 bucket to host the files for the SFTP server. Create an AWS Transfer Family SFTP-enabled server with a publicly accessible endpoint. Disassociate the Elastic IP address from the EC2 instance and associate it to the new endpoint. Set the S3 bucket as the destination for the AWS Transfer Family server and copy all the SFTP server files to the S3 bucket.



62. QUESTION

A company is developing a serverless application that is deployed on AWS Lambda. The application consists of several Lambda functions that resize, watermark, and process images. The metadata generated from the functions is written in an Amazon DynamoDB table. The company deployed an Amazon Neptune DB cluster in three private subnets inside a VPC. A new feature was developed that requires the Lambda functions to access the Neptune DB cluster.

Which of the following options are possible solutions to allow the Lambda functions to access both the DynamoDB table and Neptune DB cluster? (Select TWO.)

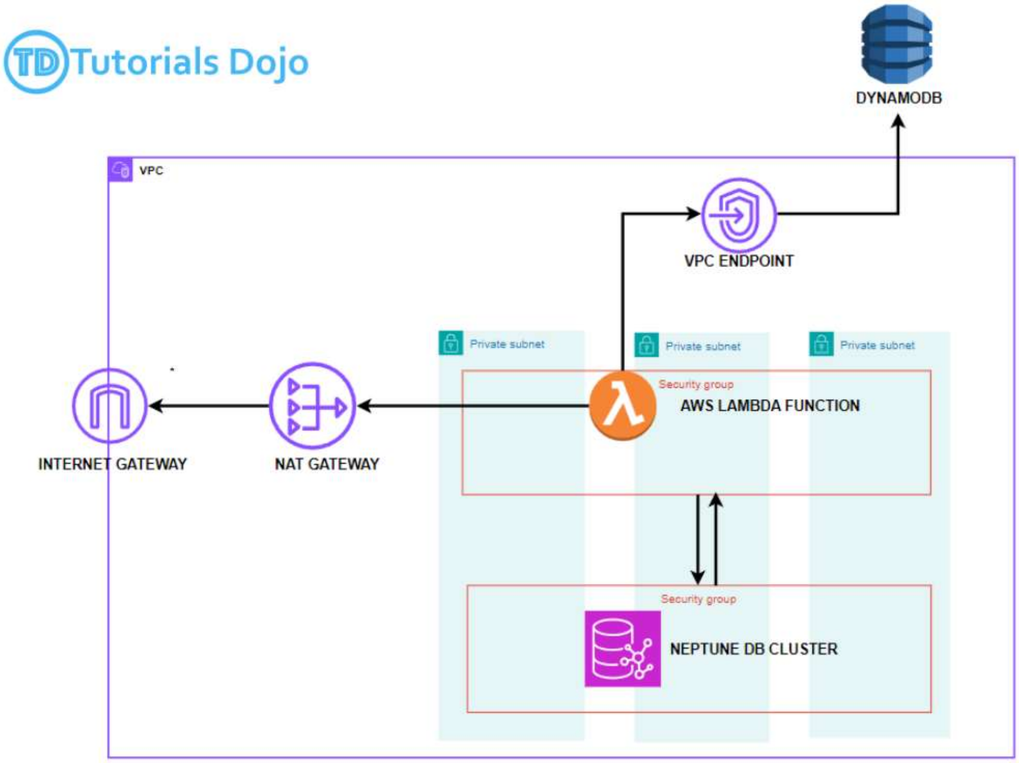
☐ Deploy the AWS Lambda functions into three new public subnets in the same VPC. Update the Amazon Neptune DB security group to allow connections from the Lambda security group. Route internet traffic to the Internet Gateway.

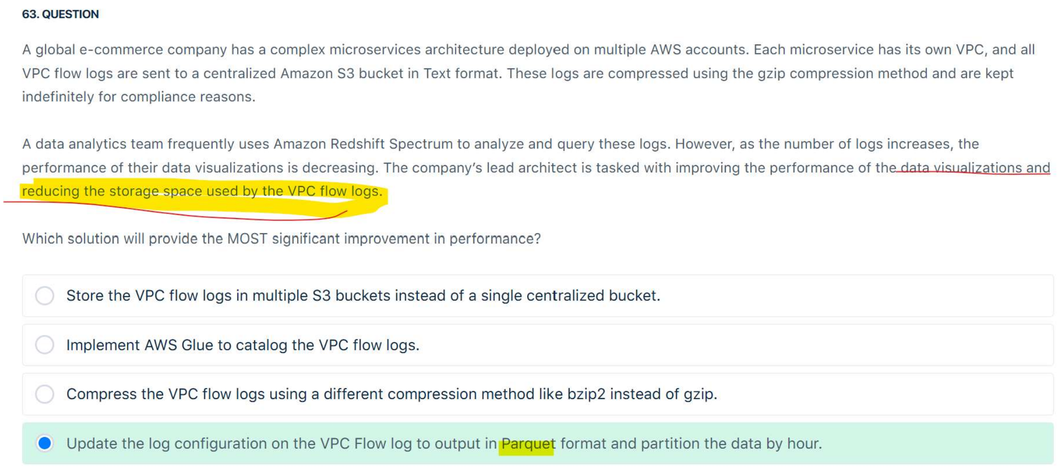
☑ Deploy the AWS Lambda functions into three new private subnets in the same VPC. Update the Neptune DB security group to allow connections from the Lambda security group. Route the internet traffic of the Lambda functions through a NAT gateway.

☐ Keep the Lambda functions outside the VPC. Configure the Neptune DB security group to allow inbound access from the AWS Lambda IP range.

☑ Deploy the AWS Lambda functions into three new private subnets in the same VPC. Update the Neptune DB security group to allow connections from the Lambda security group. Create a DynamoDB VPC endpoint and update the route table for routing DynamoDB requests.

☐ Keep the AWS Lambda functions outside the VPC. Create a VPC endpoint for the Amazon Neptune service. Update the Lambda functions to use this endpoint to send requests to the Neptune DB cluster.





63. QUESTION

A global e-commerce company has a complex microservices architecture deployed on multiple AWS accounts. Each microservice has its own VPC, and all VPC flow logs are sent to a centralized Amazon S3 bucket in Text format. These logs are compressed using the gzip compression method and are kept indefinitely for compliance reasons.

A data analytics team frequently uses Amazon Redshift Spectrum to analyze and query these logs. However, as the number of logs increases, the performance of their data visualizations is decreasing. The company's lead architect is tasked with improving the performance of the data visualizations and reducing the storage space used by the VPC flow logs.

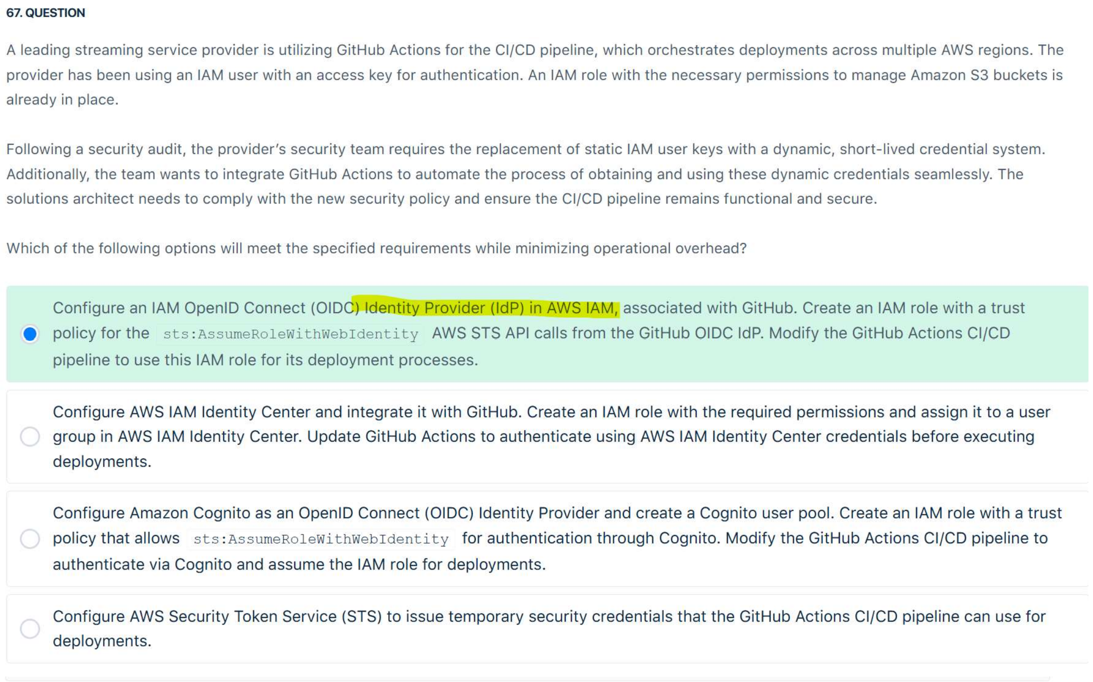
Which solution will provide the MOST significant improvement in performance?

○ Store the VPC flow logs in multiple S3 buckets instead of a single centralized bucket.

○ Implement AWS Glue to catalog the VPC flow logs.

○ Compress the VPC flow logs using a different compression method like bzip2 instead of gzip.

● Update the log configuration on the VPC Flow log to output in Parquet format and partition the data by hour.



67. QUESTION

A leading streaming service provider is utilizing GitHub Actions for the CI/CD pipeline, which orchestrates deployments across multiple AWS regions. The provider has been using an IAM user with an access key for authentication. An IAM role with the necessary permissions to manage Amazon S3 buckets is already in place.

Following a security audit, the provider's security team requires the replacement of static IAM user keys with a dynamic, short-lived credential system. Additionally, the team wants to integrate GitHub Actions to automate the process of obtaining and using these dynamic credentials seamlessly. The solutions architect needs to comply with the new security policy and ensure the CI/CD pipeline remains functional and secure.

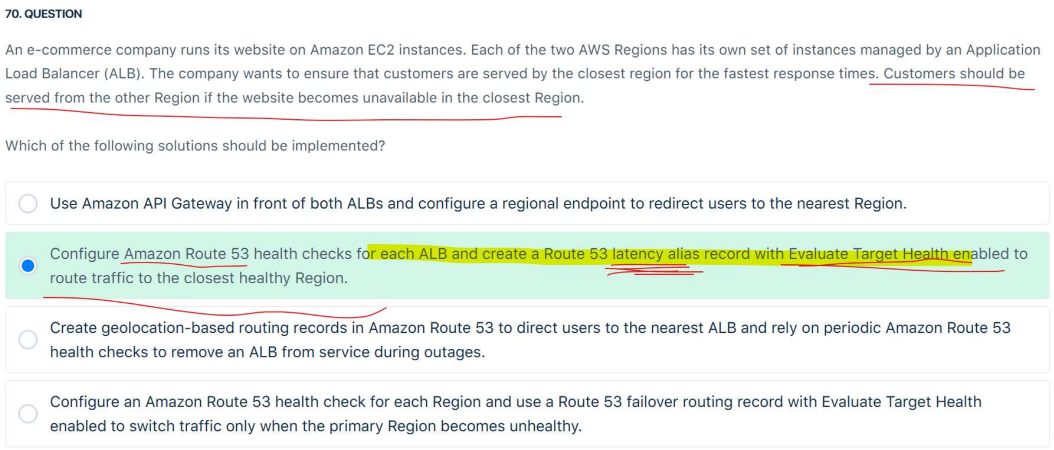
Which of the following options will meet the specified requirements while minimizing operational overhead?

● Configure an IAM OpenID Connect (OIDC) Identity Provider (IdP) in AWS IAM, associated with GitHub. Create an IAM role with a trust policy for the `sts:AssumeRoleWithWebIdentity` AWS STS API calls from the GitHub OIDC IdP. Modify the GitHub Actions CI/CD pipeline to use this IAM role for its deployment processes.

○ Configure AWS IAM Identity Center and integrate it with GitHub. Create an IAM role with the required permissions and assign it to a user group in AWS IAM Identity Center. Update GitHub Actions to authenticate using AWS IAM Identity Center credentials before executing deployments.

○ Configure Amazon Cognito as an OpenID Connect (OIDC) Identity Provider and create a Cognito user pool. Create an IAM role with a trust policy that allows `sts:AssumeRoleWithWebIdentity` for authentication through Cognito. Modify the GitHub Actions CI/CD pipeline to authenticate via Cognito and assume the IAM role for deployments.

○ Configure AWS Security Token Service (STS) to issue temporary security credentials that the GitHub Actions CI/CD pipeline can use for deployments.



70. QUESTION

An e-commerce company runs its website on Amazon EC2 instances. Each of the two AWS Regions has its own set of instances managed by an Application Load Balancer (ALB). The company wants to ensure that customers are served by the closest region for the fastest response times. Customers should be served from the other Region if the website becomes unavailable in the closest Region.

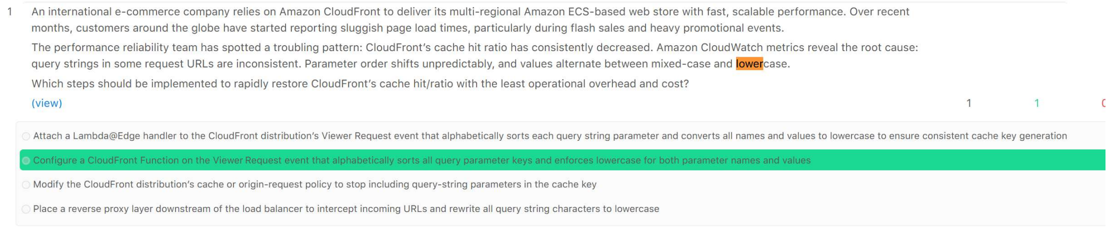
Which of the following solutions should be implemented?

○ Use Amazon API Gateway in front of both ALBs and configure a regional endpoint to redirect users to the nearest Region.

● Configure Amazon Route 53 health checks for each ALB and create a Route 53 latency alias record with Evaluate Target Health enabled to route traffic to the closest healthy Region.

○ Create geolocation-based routing records in Amazon Route 53 to direct users to the nearest ALB and rely on periodic Amazon Route 53 health checks to remove an ALB from service during outages.

○ Configure an Amazon Route 53 health check for each Region and use a Route 53 failover routing record with Evaluate Target Health enabled to switch traffic only when the primary Region becomes unhealthy.



1 An international e-commerce company relies on Amazon CloudFront to deliver its multi-regional Amazon ECS-based web store with fast, scalable performance. Over recent months, customers around the globe have started reporting sluggish page load times, particularly during flash sales and heavy promotional events.

The performance reliability team has spotted a troubling pattern: CloudFront's cache hit ratio has consistently decreased. Amazon CloudWatch metrics reveal the root cause: query strings in some request URLs are inconsistent. Parameter order shifts unpredictably, and values alternate between mixed-case and lowercase.

Which steps should be implemented to rapidly restore CloudFront's cache hit/ratio with the least operational overhead and cost?

(view) 1 1

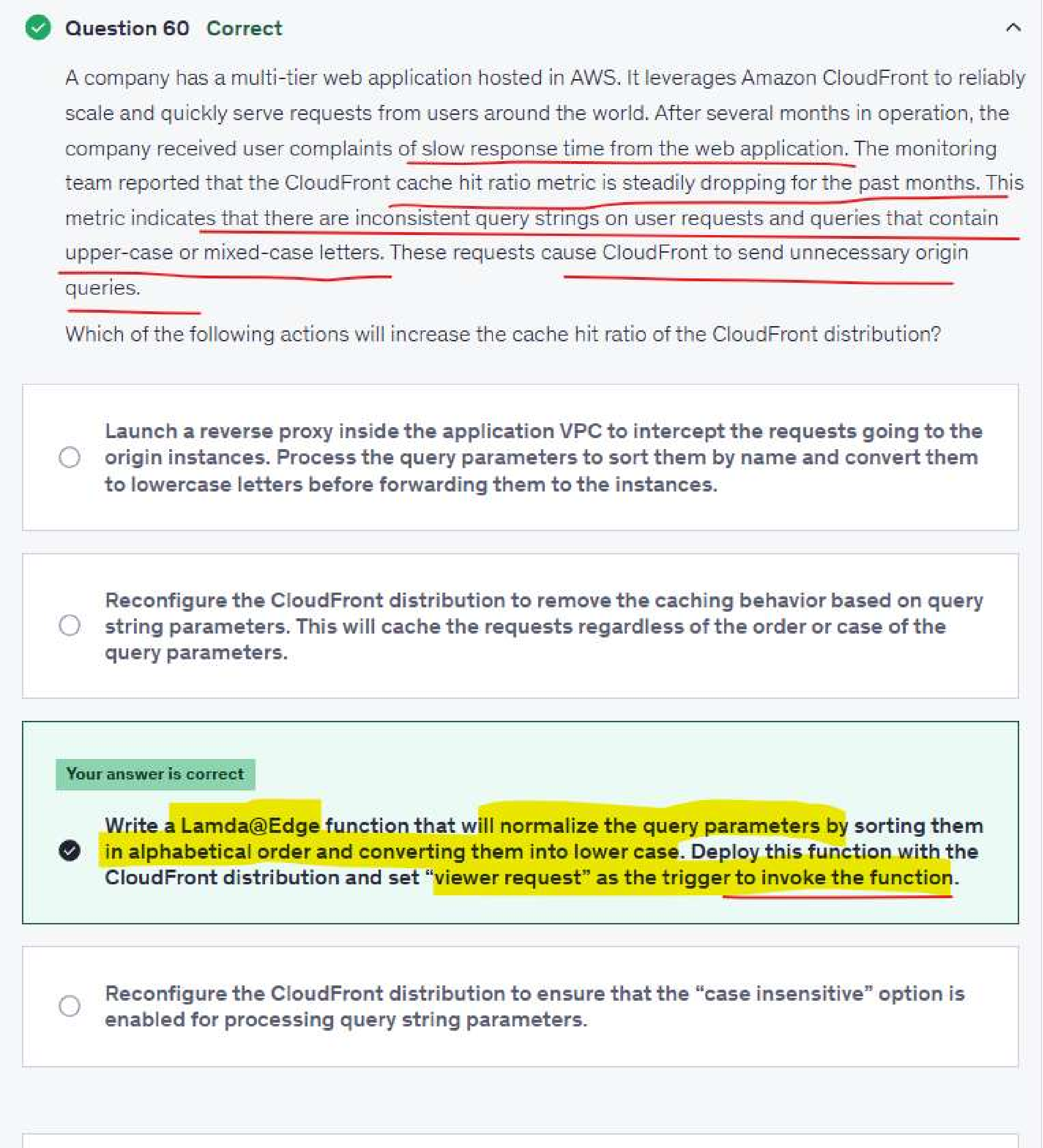
○ Attach a Lambda@Edge handler to the CloudFront distribution's Viewer Request event that alphabetically sorts each query string parameter and converts all names and values to lowercase to ensure consistent cache key generation

○ Configure a CloudFront Function on the Viewer Request event that alphabetically sorts all query parameter keys and enforces lowercase for both parameter names and values

○ Modify the CloudFront distribution's cache or origin-request policy to stop including query-string parameters in the cache key

○ Place a reverse proxy layer downstream of the load balancer to intercept incoming URLs and rewrite all query string characters to lowercase

atual
antigo



Question 60 Correct

A company has a multi-tier web application hosted in AWS. It leverages Amazon CloudFront to reliably scale and quickly serve requests from users around the world. After several months in operation, the company received user complaints of slow response time from the web application. The monitoring team reported that the CloudFront cache hit ratio metric is steadily dropping for the past months. This metric indicates that there are inconsistent query strings on user requests and queries that contain upper-case or mixed-case letters. These requests cause CloudFront to send unnecessary origin queries.

Which of the following actions will increase the cache hit ratio of the CloudFront distribution?

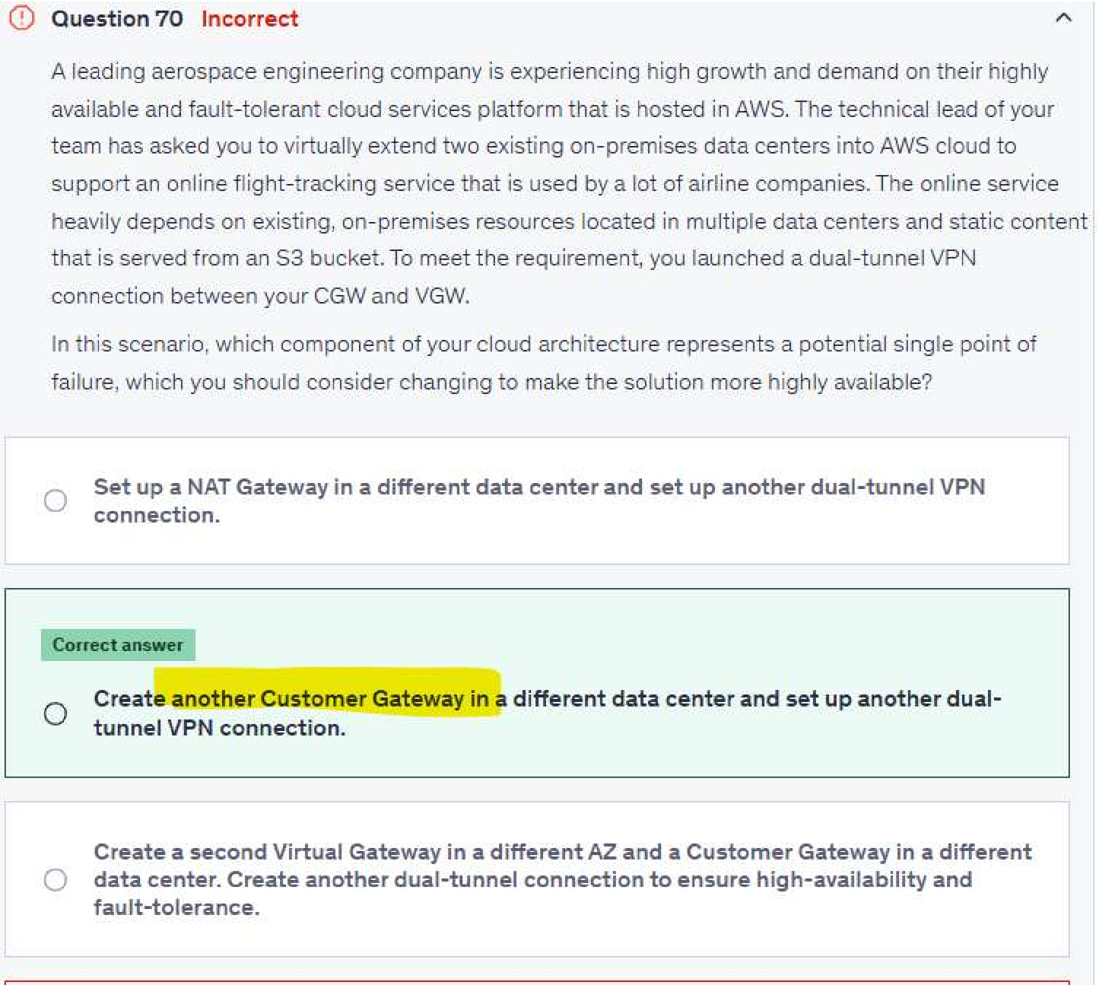
○ Launch a reverse proxy inside the application VPC to intercept the requests going to the origin instances. Process the query parameters to sort them by name and convert them to lowercase letters before forwarding them to the instances.

○ Reconfigure the CloudFront distribution to remove the caching behavior based on query string parameters. This will cache the requests regardless of the order or case of the query parameters.

Your answer is correct

● Write a Lamda@Edge function that will normalize the query parameters by sorting them in alphabetical order and converting them into lower case. Deploy this function with the CloudFront distribution and set "viewer request" as the trigger to invoke the function.

○ Reconfigure the CloudFront distribution to ensure that the "case insensitive" option is enabled for processing query string parameters.



Question 70 Incorrect

A leading aerospace engineering company is experiencing high growth and demand on their highly available and fault-tolerant cloud services platform that is hosted in AWS. The technical lead of your team has asked you to virtually extend two existing on-premises data centers into AWS cloud to support an online flight-tracking service that is used by a lot of airline companies. The online service heavily depends on existing, on-premises resources located in multiple data centers and static content that is served from an S3 bucket. To meet the requirement, you launched a dual-tunnel VPN connection between your CGW and VGW.

In this scenario, which component of your cloud architecture represents a potential single point of failure, which you should consider changing to make the solution more highly available?

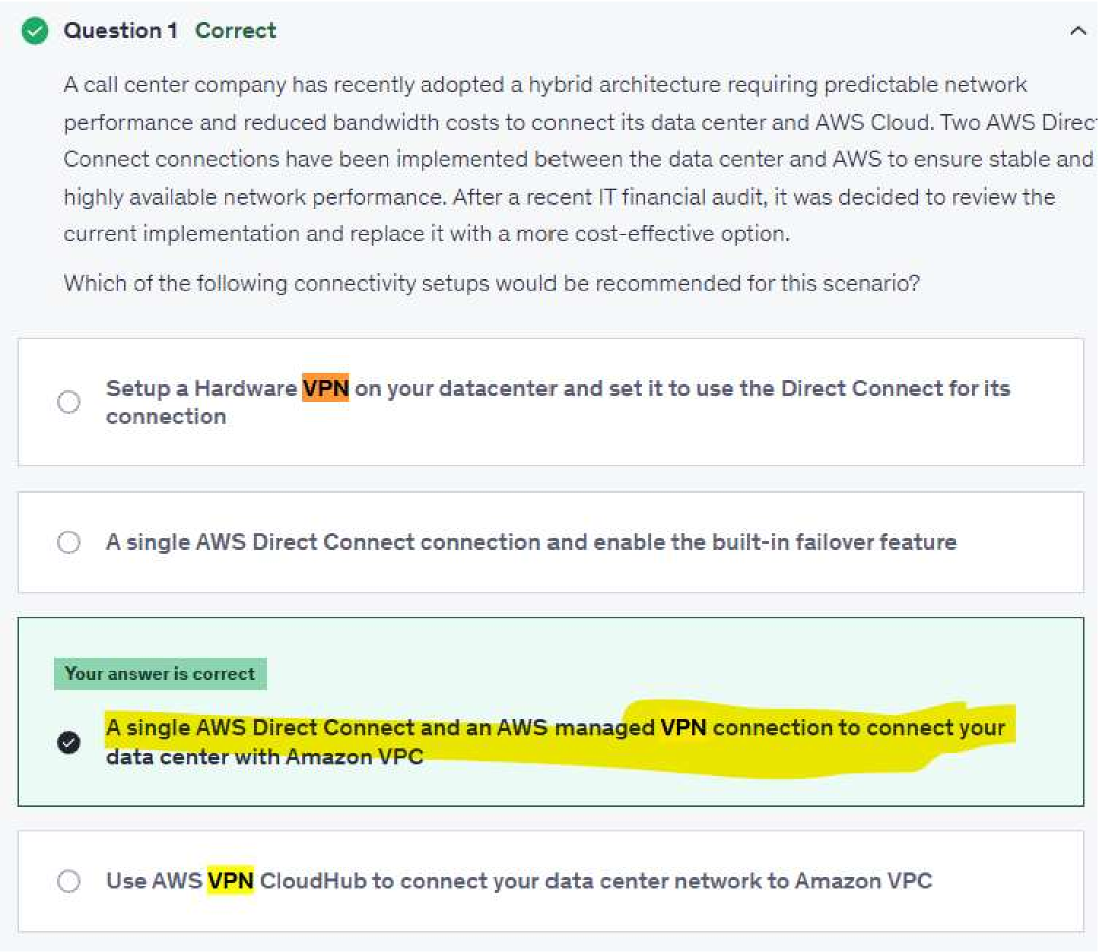
○ Set up a NAT Gateway in a different data center and set up another dual-tunnel VPN connection.

Correct answer

○ Create another Customer Gateway in a different data center and set up another dual-tunnel VPN connection.

○ Create a second Virtual Gateway in a different AZ and a Customer Gateway in a different data center. Create another dual-tunnel connection to ensure high-availability and fault-tolerance.

one VGW attached to a VPC at a given time



Question 1 Correct

A call center company has recently adopted a hybrid architecture requiring predictable network performance and reduced bandwidth costs to connect its data center and AWS Cloud. Two AWS Direc Connect connections have been implemented between the data center and AWS to ensure stable and highly available network performance. After a recent IT financial audit, it was decided to review the current implementation and replace it with a more cost-effective option.

Which of the following connectivity setups would be recommended for this scenario?

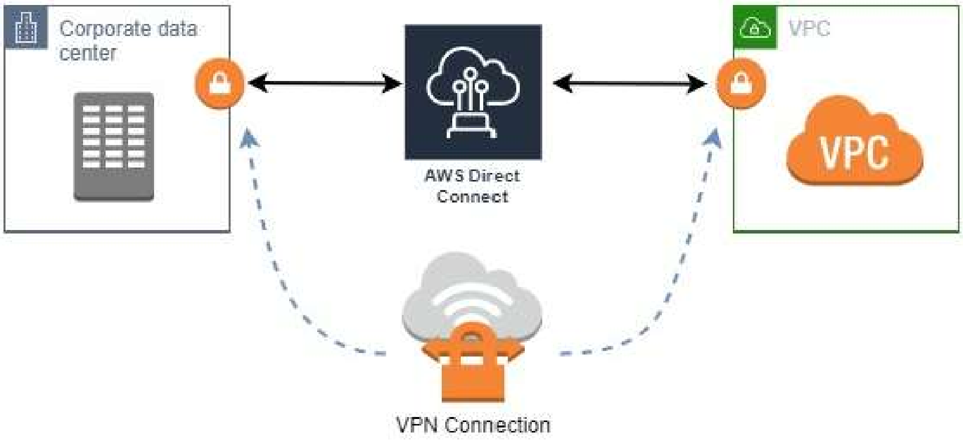
○ Setup a Hardware VPN on your datacenter and set it to use the Direct Connect for its connection

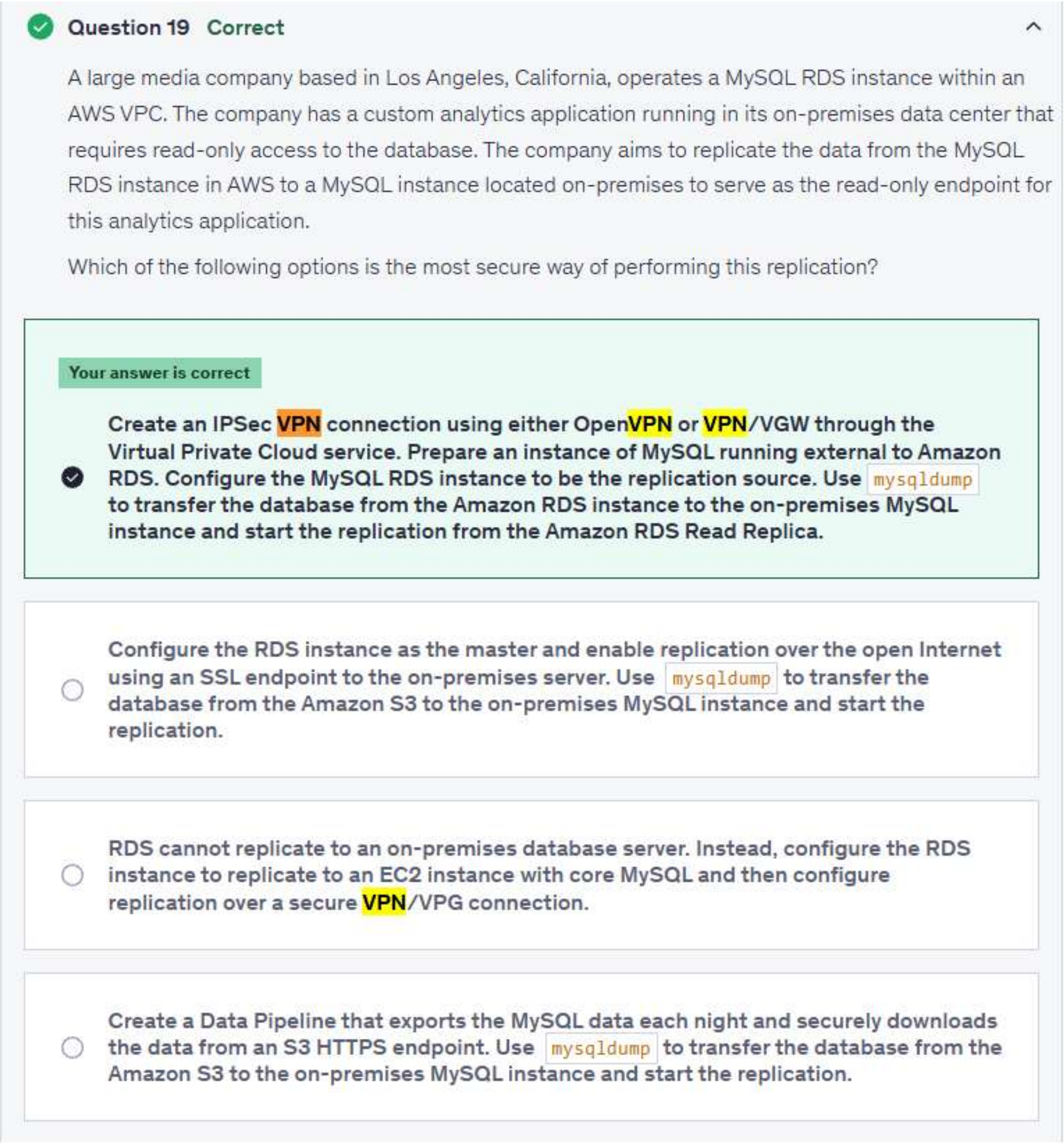
○ A single AWS Direct Connect connection and enable the built-in failover feature

Your answer is correct

● A single AWS Direct Connect and an AWS managed VPN connection to connect your data center with Amazon VPC

○ Use AWS VPN CloudHub to connect your data center network to Amazon VPC





Question 19 **Correct**

A large media company based in Los Angeles, California, operates a MySQL RDS instance within an AWS VPC. The company has a custom analytics application running in its on-premises data center that requires read-only access to the database. The company aims to replicate the data from the MySQL RDS instance in AWS to a MySQL instance located on-premises to serve as the read-only endpoint for this analytics application.

Which of the following options is the most secure way of performing this replication?

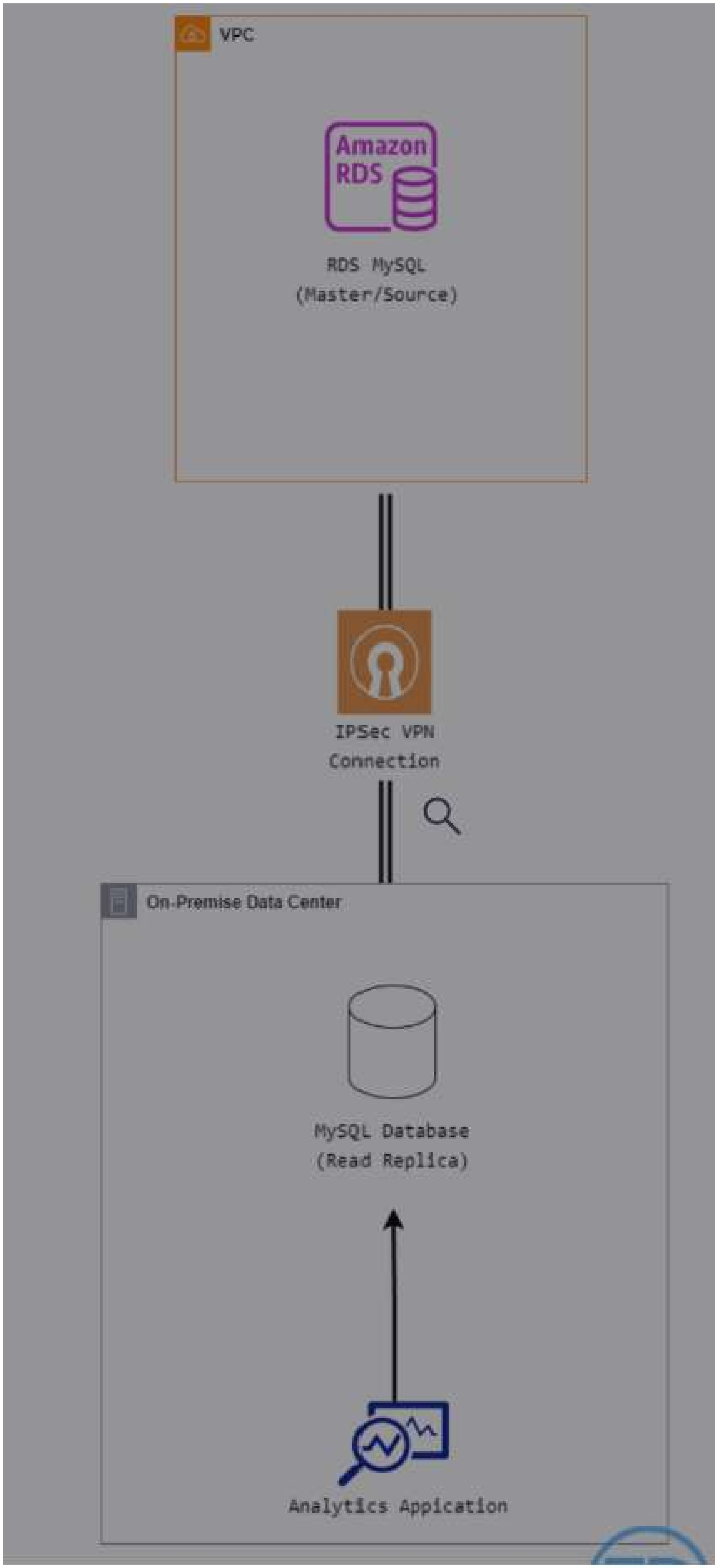
Your answer is correct

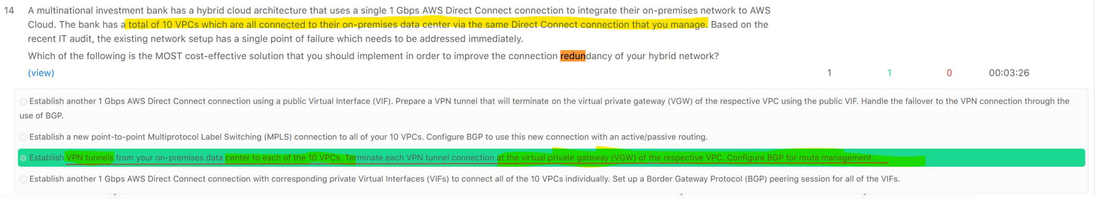
● **Create an IPSec VPN connection using either OpenVPN or VPN/VGW through the Virtual Private Cloud service. Prepare an instance of MySQL running external to Amazon RDS. Configure the MySQL RDS instance to be the replication source. Use `mysqldump` to transfer the database from the Amazon RDS instance to the on-premises MySQL instance and start the replication from the Amazon RDS Read Replica.**

○ **Configure the RDS instance as the master and enable replication over the open Internet using an SSL endpoint to the on-premises server. Use `mysqldump` to transfer the database from the Amazon S3 to the on-premises MySQL instance and start the replication.**

○ **RDS cannot replicate to an on-premises database server. Instead, configure the RDS instance to replicate to an EC2 instance with core MySQL and then configure replication over a secure VPN/VPG connection.**

○ **Create a Data Pipeline that exports the MySQL data each night and securely downloads the data from an S3 HTTPS endpoint. Use `mysqldump` to transfer the database from the Amazon S3 to the on-premises MySQL instance and start the replication.**


VPC
Amazon RDS
RDS MySQL
(Master/Source)
IPSec VPN
Connection
On-Premise Data Center
MySQL Database
(Read Replica)
Analytics Appication



14 A multinational investment bank has a hybrid cloud architecture that uses a single 1 Gbps AWS Direct Connect connection to integrate their on-premises network to AWS Cloud. The bank has a total of 10 VPCs which are all connected to their on-premises data center via the same Direct Connect connection that you manage. Based on the recent IT audit, the existing network setup has a single point of failure which needs to be addressed immediately.

Which of the following is the MOST cost-effective solution that you should implement in order to improve the connection redundancy of your hybrid network?

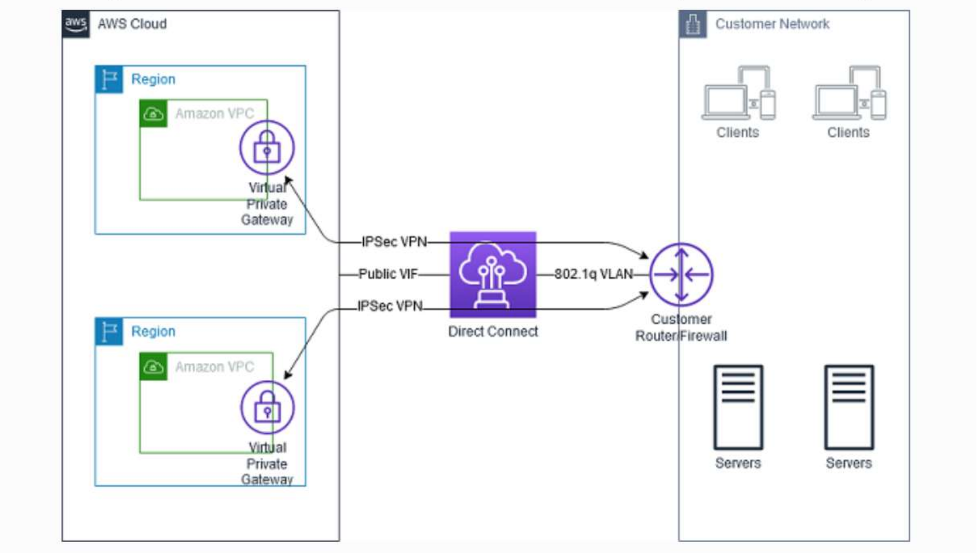
(view) 1 1 0 00:03:26

○ Establish another 1 Gbps AWS Direct Connect connection using a public Virtual Interface (VIF). Prepare a VPN tunnel that will terminate on the virtual private gateway (VGW) of the respective VPC using the public VIF. Handle the failover to the VPN connection through the use of BGP.

○ Establish a new point-to-point Multiprotocol Label Switching (MPLS) connection to all of your 10 VPCs. Configure BGP to use this new connection with an active/passive routing.

○ Establish VPN tunnels from your on-premises data center to each of the 10 VPCs. Terminate each VPN tunnel connection at the virtual private gateway (VGW) of the respective VPC. Configure BGP for route management.

○ Establish another 1 Gbps AWS Direct Connect connection with corresponding private Virtual Interfaces (VIFs) to connect all of the 10 VPCs individually. Set up a Border Gateway Protocol (BGP) peering session for all of the VIFs.


AWS Cloud
Region
Amazon VPC
Virtual Private Gateway
Region
Amazon VPC
Virtual Private Gateway
IPSec VPN
Public VIF
IPSec VPN
Direct Connect
802.1q VLAN
Customer Router/Firewall
Customer Network
Clients
Clients
Servers
Servers