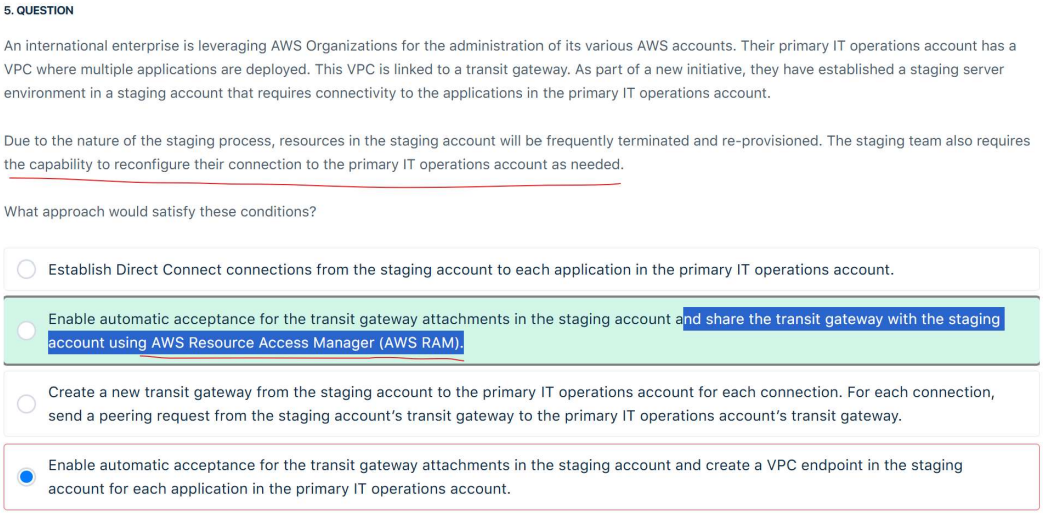
questoes erradas 2

Notebook:	solutions profissional_ef8e1c0f-5d3c-42ab-ab04-9217e53e12cd		
Created:	10/12/2025 09:06	**Updated:**	11/12/2025 00:12
Author:	erikachen19@gmail.com		
URL:	https://portal.tutorialsdojo.com/courses/aws-certified-solutions-architect-professional...		



Hence, the correct answer is: **Enable automatic acceptance for the transit gateway attachments in the staging account and share the transit gateway with the staging account using AWS Resource Access Manager (AWS RAM).** By enabling automatic acceptance for the transit gateway attachments, the staging account can easily connect to the primary IT operations account. This approach allows for easy reconfiguration of connections as needed, which is a requirement in the question. Furthermore, **by sharing the transit gateway with the staging account using AWS RAM, the staging account can access the resources in the primary IT operations account, providing the necessary connectivity for the staging process.**

Enable automatic acceptance for the transit gateway attachments in the staging account and create a VPC endpoint in the staging account for each application in the primary IT operations account is incorrect because while this option does involve enabling automatic acceptance for the transit gateway attachments, creating a VPC endpoint in the staging account for each application in the primary IT operations account is not the most efficient or flexible solution. It would require a significant amount of configuration and wouldn't easily allow for reconfiguration of connections.

7. QUESTION

A digital marketing firm is planning to integrate its local servers with AWS for better scalability. The firm has chosen a 200 Mbps AWS Direct Connect connection for this integration. The proposed setup includes a transit gateway and a Direct Connect gateway to ensure smooth communication between several VPCs and the local servers.

The firm needs to make sure that its local servers can interact with the AWS VPC resources through a transit virtual interface (VIF) using the Direct Connect connection.

Which two actions should the firm take to achieve these requirements? (Select TWO.)

- [ ] Advertise the allowed prefixes to a range that is the same or wider than the VPC CIDR block on the Direct Connect gateway.
- [x] Advertise the allowed prefixes list on the Direct Connect gateway for the transit gateway association.
- [ ] Configure the Direct Connect connection by setting the MACsec encryption mode parameter to `must_encrypt` .
- [ ] Upgrade the AWS Direct Connect connection from 200 Mbps to 500 Mbps.
- [x] Use the same Connection Key Name (CKN) and Connectivity Association Key (CAK) for all AWS Direct Connect connections.

Advertise the allowed prefixes to a range that **is the same or wider than the VPC CIDR block o**n the Direct Connect gateway.
将允许的前缀通告到与 Direct Connect 网关上的 VPC CIDR 块相同或更宽的范围。
Provisioning the allowed prefixes list on the Direct Connect gateway is a necessary step. This list is used to route on-premises traffic to or from a Direct Connect gateway to the transit gateway, even when the VPCs attached to the transit gateway do not have assigned CIDRs. This setup ensures that the local servers can interact with the AWS VPC resources through the transit VIF.

11. QUESTION

A company hosts a web application service in the AWS eu-east-1 region. The application serves weather maps to users. The maps are updated every 1 hour and are stored in an Amazon S3 bucket along with static web content. The web application is behind an Amazon CloudFront distribution. The company has expanded and now provides the same service to North American users. Reports indicate that the viewing experience for weather maps is slow at times in this region.

Which combination of actions can provide the LEAST latency between the users and the application? (Select TWO.)

- [x] Configure S3 cross-region replication from the eu-east-1 bucket to a new bucket in the us-east-1 region.
- [ ] Create a new AWS Global Accelerator endpoint for the eu-west-1 S3 bucket. Configure additional endpoint groups in the us-east-1 S3 bucket for TCP port 443.
- [ ] Create a Lambda@Edge function that modifies requests from North American users to use the S3 Transfer Acceleration endpoint of the S3 bucket in the us-east-1 region.
- [ ] Create a Lambda@Edge that modifies requests from North American users to retrieve files from a new us-east-1 S3 bucket.
- [x] Create a new AWS Global Accelerator endpoint for the us-east-1 bucket and add it as an origin for the CloudFront distribution. Use Lambda@Edge to modify North American requests to use this new origin.

– Create a Lambda@Edge that modifies requests from North American users to retrieve files from a new us-east-1 S3 bucket. By having the data replicated in a geographically closer region (us-east-1), the data retrieval time is significantly decreased for users in that region.
The option that says: **Create a new AWS Global Accelerator endpoint for the us-east-1 bucket and add it as an origin for the CloudFront distribution. Use Lambda@Edge to modify North American requests to use this new origin** is incorrect. While AWS Global Accelerator can improve performance for some use cases, it typically front-ends applications or load balancers. Simply creating a Global Accelerator endpoint for a new S3 bucket does not address the crucial need to replicate or store the updated objects in a bucket closer to the users.

AWS **Global Accelerator (GA)** é um serviço de **rede global** da AWS que melhora a **disponibilidade**, a **resiliência** e principalmente a **latência** de aplicações **com endpoints regionais** — mas *não* funciona como acelerador para S3 diretamente.

Aqui vai a explicação clara e objetiva:

☑ Para que serve o AWS Global Accelerator

GA fornece **endereços IP Anycast globais** que distribuem automaticamente o tráfego para o endpoint AWS **mais saudável e mais próximo** do usuário.

Ele melhora:

- ◇ **Latência** (entra na rede AWS mais perto do usuário)
- ◇ **Failover rápido** entre regiões
- ◇ **Roteamento inteligente** via rede global da AWS

🚀 Quando usar Global Accelerator

Use GA quando os **endpoints finais** forem um destes:

✓ Aceitos como endpoints GA

- **Application Load Balancer (ALB)**
- **Network Load Balancer (NLB)**
- **EC2 instances com Elastic IP**
- **Elastic IPs diretamente**
- **AWS Global Accelerator custom routing para gaming / UDP / VoIP**

Esses endpoints recebem tráfego TCP/UDP.

❌ Quando NÃO usar Global Accelerator

GA **não** acelera:

- ❌ **Amazon S3 buckets**

- ❌ **CloudFront distributions**
- ❌ **Static websites in S3**
- ❌ **APIs diretamente no API Gateway sem integração com ALB**
- ❌ **Requests HTTP estáticos como imagens, JS, HTML via S3**

👉 Para S3 e conteúdo estático, o serviço correto de baixa latência é **CloudFront**.

CloudFront = CDN

Global Accelerator = IP global + roteamento otimizado para ALB/NLB/EC2

Serviço	Usar quando	Exemplo típico
CloudFront	reduzir latência de conteúdo estático global	imagens, vídeos, HTML no S3
Global Accelerator	reduzir latência e failover p/ aplicações TCP/UDP	APIs atrás de ALB/NLB, apps multi-region

☑ Exemplo prático

Você tem uma **API global** rodando em duas regiões:

- **us-east-1** → ALB + ECS
- **eu-west-1** → ALB + ECS

Usuários do mundo inteiro acessam a mesma API.

Problemas:

- Latência alta para quem está longe da região primária
- Failover entre regiões é lento
- DNS (Route 53) leva segundos para trocar o endpoint

Solução:

Usar **AWS Global Accelerator**:

- Ele cria **dois IPs globais Anycast**
- Usuários entram na **rede da AWS no ponto mais próximo** (Brasil, EUA, Europa, etc.)
- GA direciona automaticamente para o **ALB da região mais próxima e saudável**

Resultado:

- ◇ **Menor latência mundial**
- ◇ **Failover quase instantâneo** entre regiões
- ◇ **Mesmos IPs fixos**, mesmo que você troque ou mova endpoints

---

🎯 Em uma frase:

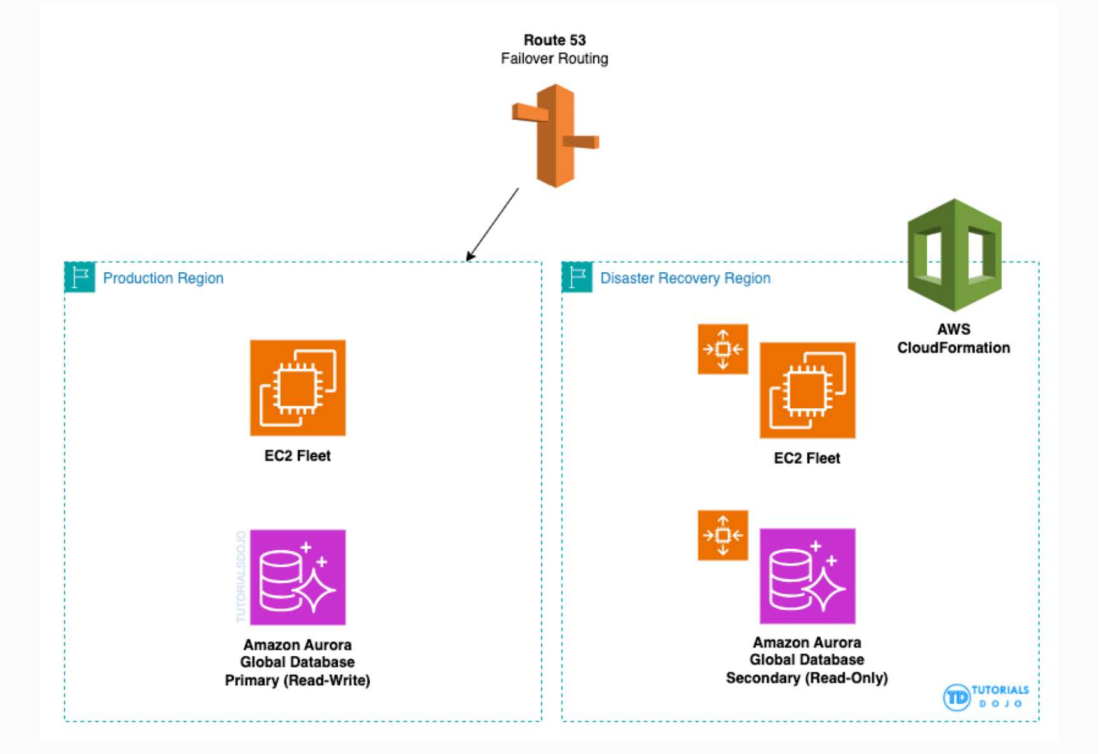
API multi-região + ALB é o cenário clássico para usar Global Accelerator.

13. QUESTION

A financial company is migrating its banking application to the cloud. The application will be deployed on medium-sized Amazon EC2 instances with an Amazon Aurora for PostgreSQL database. The company aims to increase the resiliency of the application by creating a disaster recovery plan to failover across different AWS regions. As part of compliance, the recovery point objective (RPO) should be under one minute, while the recovery time objective (RTO) should be a maximum of 15 minutes only.

What solution will fulfill these requirements MOST cost-effectively?

- Build the infrastructure using AWS CloudFormation templates to allow provisioning the resources in a DR region in the event of a disaster. Create an Amazon Aurora global database with the primary instance in the production region and a secondary (read-only) instance in the DR region. Configure Elastic Disaster Recovery to continuously replicate the EC2 instances from the production region to the DR region, and setup an auto-scaling group in the DR region. Use Amazon Route 53 failover routing policy to direct traffic to DR in case of a disaster.
- **Set up a scaled-down replica of the infrastructure in another AWS region. Keep the replica in a warm state by keeping at least one EC2 instance running and an Amazon Aurora for PostgreSQL instance active. Enable data replication from the primary database to the secondary database.**
- Deploy an identical infrastructure in multiple regions and keep the regions actively serving traffic. Use global load balancers to distribute requests between regions.
- Periodically take snapshots of the Amazon EC2 instances and Amazon Aurora for PostgreSQL database to serve as backups. In the event of a disaster, restore the system by launching EC2 instances from the snapshots and restoring the Amazon Aurora database from the database backup.



The option that says: **Set up a scaled-down replica of the infrastructure in another AWS region. Keep the replica in a warm state by keeping at least one EC2 instance running and an Amazon Aurora for PostgreSQL instance active. Enable data replication from the primary database to the secondary database** is incorrect. Although this approach can achieve the specified objectives of recovery time and recovery point, there is no automatic failover in place and can add to the recovery time of the infrastructure in the DR region.

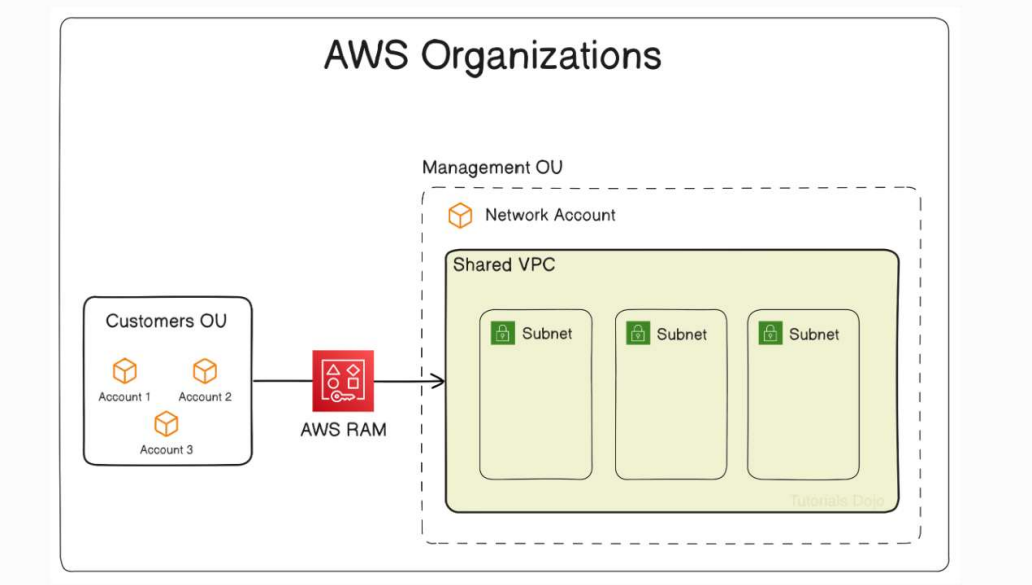
15. QUESTION

A company uses AWS Organizations to manage hundreds of AWS accounts. The company plans to designate a central network account where a shared VPC will be created. Accounts under the Customers Organization Unit (OU) are allowed to create resources on the shared VPC, but they should not be able to manage it.

The AWS Security Hub has also been configured to provide the company with a comprehensive view of their security state in AWS and to help them verify their AWS workloads against security industry standards and best practices. There's also a Security Hub administrator account that has already been designated in AWS Organizations to view data from its member accounts.

Which combination of steps would meet the company's objectives? (Select TWO.)

- [ ] Configure the management account to enable AWS Resource Access Manager (RAM) resource sharing with AWS Organizations.
- [x] Use AWS Resource Access Manager (RAM) to create a resource share in the management account. Include all subnets of the shared VPC and set the Customers OU as the principal.
- [ ] Configure a managed prefix list in the central network account, specifying the IP ranges that align with the desired network configuration. Use AWS Resource Access Manager (RAM) to share this prefix list with the Customers OU.
- [x] Create a service control policy (SCP) within AWS Organizations and attach it to the Customers OU. This SCP should contain statements for denying management actions to a VPC.
- [ ] Create a separate VPC within each individual account in the Customers OU. Set up a Resource Access Manager (RAM) resource share for a Transit Gateway in the management account and share it with the Customers OU. Establish VPC peering connections between all VPCs.



The option that says: **Create a service control policy (SCP) within AWS Organizations and attach it to the Customers OU. This SCP should contain statements for denying management actions to a VPC** is incorrect. SCPs are used to set fine-grained permissions for AWS Organizations and can indeed deny specific actions. However, in the context of a shared VPC using AWS RAM**, it's AWS RAM that manages the permissions**, and the shared accounts do not have management permissions for the VPC by default. Therefore, denying VPC management actions via an SCP would be unnecessary in this scenario.

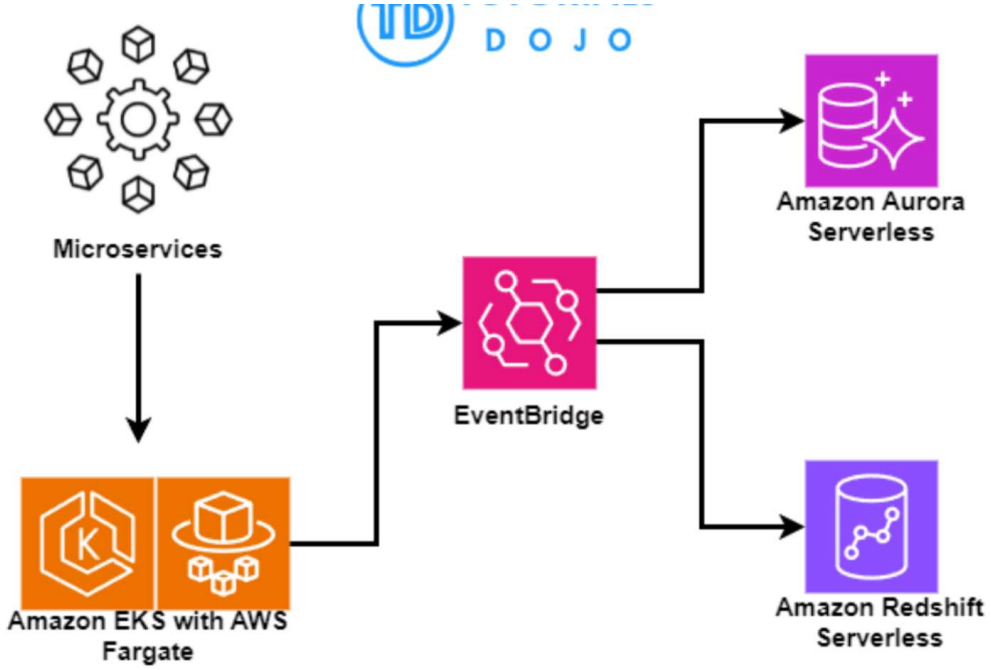
18. QUESTION

An organization operates web and mobile platforms for online sales, inventory management, order processing, and shipping logistics. The platforms are running on Amazon EC2 instances across multiple regions. The organization's databases include a MySQL database for the e-commerce site and a PostgreSQL database for analytics, both managed on EC2 instances.

A solutions architect requires a solution to transition the organization's architecture to an event-driven, serverless architecture to improve efficiency and data processing speeds, enable real-time analytics, and streamline application data flows. The company also plans to launch a multi-cloud configuration that runs additional clusters on other cloud service providers to further improve the site's performance.

Which of the following options would most efficiently meet these requirements?

- Migrate app components to microservices with Amazon EKS using AWS Fargate. Change e-commerce MySQL to Amazon Aurora MySQL and analytics DB to Amazon Redshift. Use Amazon Kinesis for real-time data streaming.
- Use Amazon ECS with Fargate to repackage applications as microservices. Migrate e-commerce and analytics databases to Aurora Serverless MySQL and Redshift Serverless. Manage data flow between services using Amazon EventBridge.
- Create Auto Scaling groups for each platform component with specific EC2 instance numbers. Migrate e-commerce MySQL and analytics PostgreSQL databases to Amazon Aurora PostgreSQL. Use Amazon SNS to route incoming data to the right EC2 instances and databases.
- Migrate to microservices with Amazon EKS and Fargate. Use Aurora Serverless MySQL for e-commerce and Redshift Serverless for analytics. Use Amazon EventBridge to streamline and manage data flows.



The option that says: **Use Amazon ECS with Fargate to repackage applications as microservices. Migrate e-commerce and analytics databases to Aurora Serverless MySQL and Redshift Serverless. Manage data flow between services using Amazon EventBridge** is incorrect. Although this option also suggests using Aurora Serverless, Amazon EventBridge, and Redshift Serverless, the container service being used is **Amazon ECS, which typically does not support multi-cloud deployments,** unlike EKS. While ECS with Fargate allows for container orchestration and management, it doesn't fully address the requirement of explicit multi-cloud integration. In contrast, Amazon EKS (Elastic Kubernetes Service) with Fargate offers a more suitable platform for multi-cloud configuration with cost-effective serverless computing.

23. QUESTION

A global energy firm aggregates sensor readings from its offshore wind turbines and stores the data in an Amazon S3 data lake governed by AWS Lake Formation. The research department runs analytics on Amazon EC2 instances in two private subnets within a VPC. The EC2 instances already have an IAM role with permission to access the S3 bucket.

Corporate security mandates that only specific, approved networks be used when retrieving turbine data. The research team must be able to continue to access the data lake without exposing it to public internet traffic.

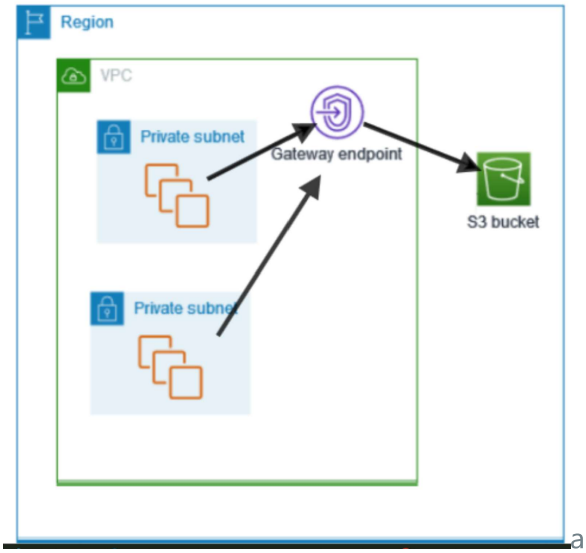
What combination of actions will meet these requirements? (Select THREE.)

- [ ] Modify the S3 bucket policy to include a condition that allows `s3:GetObject` only if the `s3:DataAccessPointAccount` matches the research team's AWS account.
- [x] Update the S3 bucket policy to include a condition that allows `s3:GetObject` only if the `s3:DataAccessPointArn` matches the correct S3 access point.
- [x] Create a NAT Gateway and modify the VPC's route table to direct traffic from the private subnets to the NAT Gateway.
- [x] Encrypt the data lake objects using AWS Key Management Service (AWS KMS) and reassign the key to the research team's IAM role
- [ ] Set up an S3 access point in the research team's AWS account and reference its Amazon Resource Name (ARN) when retrieving objects.
- [ ] Configure a Gateway VPC endpoint for Amazon S3 within the research team's VPC.

他问如何acessar 数据不暴露public 看题看题 **Gateway VPC Endpoint + S3 Access Points**+bucket policy

S3 Access Points are unique network endpoints for Amazon S3 buckets that make data access management easier for shared datasets. Each access point is linked to a single S3 bucket and has its own access policy. This allows you to create custom access policies tailored to different applications or user groups that access the same bucket. Access points also include network origin control and Block Public Access settings, making them beneficial for managing access in complex scenarios, such as multi-tenant applications or data lakes.

Gateway VPC Endpoint s are specifically designed for Amazon S3 and DynamoDB. They enable resources within a Virtual Private Cloud (VPC) to communicate with S3 or DynamoDB without going through the public internet. Gateway endpoints use prefix lists in the VPC route table to direct traffic to the target service. This setup provides a secure and cost-effective way to access S3 or DynamoDB from within a VPC. Unlike interface endpoints, gateway endpoints do not require elastic network interfaces and do not utilize AWS PrivateLink technology.



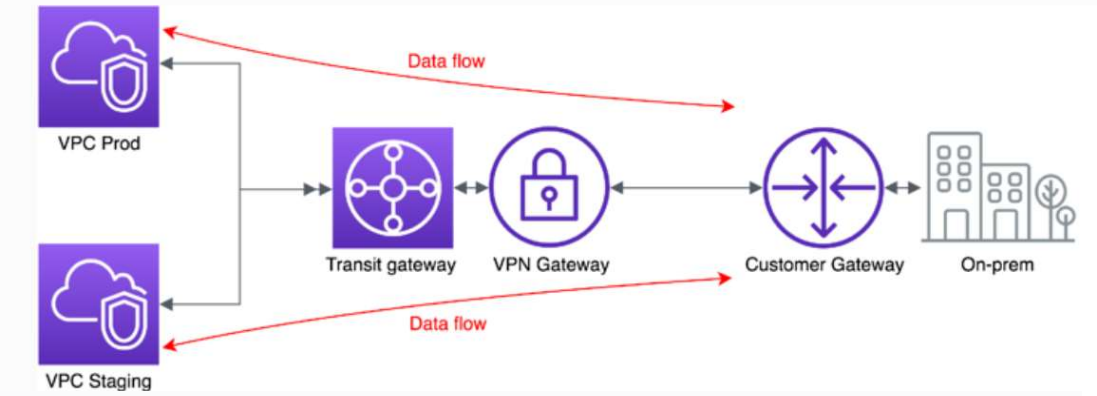
and set up an S3 access point

28. QUESTION

A company uses Amazon EC2 instances to host development and production workloads in the us-east-1 region. The instances are spread across multiple AWS accounts under the AWS Organization of the main company account. Every VPC on the us-east-1 region hosts either a development or production workload. All EC2 instances under the organization that have the same environment must be able to communicate with each other, while EC2 instances in different environments must not be able to communicate with each other. To accomplish this requirement, the company created a common network account and used the AWS Transit Gateway service. A transit gateway is created in the us-east-1 region and with the help of AWS Resource Access Manager, it is shared with the entire AWS Organization. Each VPC is then attached to the transit gateway to allow communication between the EC2 instances. However, this also allowed communication between the production and development EC2 instances.

Which of the following implementation would ensure that the development traffic is isolated from the production traffic?

- (●) Create a network tag for each VPC attachment and assign a value of development or production depending on the environment of that VPC. Configure the AWS Transit Gateway route table to allow production tagged attachments to communicate with other production tagged attachments. Set up the same configuration for development tagged attachments.
- ( ) Configure the attached security groups of the production Amazon EC2 instances to block traffic from the development EC2 instances. Configure the attached security groups of the development EC2 instances to block traffic from the production EC2 instances.
- ( ) Delete each account's route propagation and association to the default route table of the AWS Transit Gateway. Create two separate transit gateway route tables for development and production environments. Attach each VPC to their respective route tables and enable route propagation for each attachment.
- ( ) Create an env tag for each VPC attachment and assign a value of development or production depending on the environment of that VPC. Create policies to restrict traffic between the development and production VPCs based on the tag by using the AWS Transit Gateway Network Manager.



Therefore, the correct answer is: **Delete each account's route propagation and association to the default route table of the AWS Transit Gateway. Create two separate transit gateway route tables for development and production environments. Attach each VPC to their respective route tables and enable route propagation for each attachment.** This enables you to segment your network. With this method, you can associate development VPCs with one route table and production VPCs with a different route table.

The option that says: **Create an env tag for each VPC attachment and assign a value of development or production depending on the environment of that VPC. Create policies to restrict traffic between the development and production VPCs based on the tag by using the AWS Transit Gateway Network Manager** is incorrect. AWS Transit Gateway Network Manager is used to monitor network activity into a single dashboard. It is not used for creating network policies.

AWS Transit Gateway Network Manager é um serviço que oferece visibilidade centralizada, monitoramento e gestão global de redes que usam AWS Transit Gateway. Ele ajuda a acompanhar conexões entre VPCs, redes on-premises e regiões AWS — tudo em um painel único.

32. QUESTION

A forecasting agency is struggling to meet the Service Level Agreement (SLA) of its online platform. To avoid penalties and maintain credibility, they aim to develop a recovery plan that assures a Recovery Time Objective (RTO) of no more than 30 minutes.

Their platform runs on an Auto Scaling Group (ASG) connected to an Application Load Balancer (ALB). Data is stored in an Amazon RDS PostgreSQL database. An identical environment exists in a secondary region where the ASG's capacity limits are set to zero. A read replica of the RDS database is deployed in this backup region as well. A Route 53 alias record is configured to route domain traffic to the ALB.

The agency cannot afford an active-active failover and is opting for a more cost-effective way of switching over to the backup region.

Which strategy would meet these requirements?

- Update the routing policy of the alias record to Weight with a value of 100. Create a new alias record for the application's domain with a Weight routing policy initialized to 0. Adjust the Auto Scaling Group (ASG) in the secondary Region to match the capacity limits of the ASG in the primary Region. Create a Lambda function for weight adjustment and read replica promotion. Set up a Route 53 health check that sends an Amazon SNS notification to the Lambda function.
- Add a failover policy in the alias record to redirect traffic to the Application Load Balancer in the secondary Region. Create a Lambda function that updates the ASG's capacity limits and promotes the read replica to primary in the secondary Region. Monitor the application status with a Route 53 health check that uses Amazon SNS to invoke the Lambda function when the application becomes unhealthy.
- (selected) Set up an Amazon CloudWatch alarm that tracks the `HTTPCode_Target_5XX_Count` metric of the ALB in the primary Region. Create a secondary Route 53 record with identical values as the primary record. Adjust the Auto Scaling Group (ASG) in the secondary Region to match the capacity limits of the ASG in the primary Region. Create a Route 53 health check that sends an Amazon SNS notification to a Lambda function that will promote the read replica to the primary.
- Create a Lambda function that updates the ASG's capacity limits and promotes the read replica to primary in the secondary Region. Set up a CloudWatch alarm that triggers the function when the `HTTPCode_ELB_502_Count` ALB metric becomes greater than or equal to 1.

The option that says: **Set up an Amazon CloudWatch alarm that tracks the `HTTPCode_Target_5XX_Count` metric of the ALB in the primary Region. Create a secondary Route 53 record with the same name, the same type, and the same routing policy as the primary record. Adjust the Auto Scaling Group (ASG) in the secondary Region to match the capacity limits of the ASG in the primary Region. Create a Route 53 health check that sends an Amazon SNS notification to a Lambda function that will promote the read replica to primary** is incorrect. **This option actually suggests an active-active setup**, **X** where both environments are running simultaneously. In this setup, Route 53's health checks would monitor both environments and if one becomes unhealthy, Route 53 will route traffic only to the healthy environment. This setup costs a lot more since two environments are running at the same time. The scenario specifically mentioned that the agency cannot afford an active-active failover and is opting for a more cost-effective way of switching over to the backup region.

36. QUESTION

A company has a suite of services hosted on its on-premises data center. These services run on a network of virtualized Ubuntu and Windows servers. To benefit from AWS' scaling capabilities, the company decides to migrate its entire system to AWS.

Their migration strategy aims to precisely understand their actual usage and deeply analyze application components and their dependencies within its on-premises workload. The company also wants to right-size its EC2 instances to avoid unnecessary expenses for underutilized resources.

Which set of actions will meet the requirements?

- Install the AWS Application Discovery Agent on both the physical servers and Virtual machines to gather performance and usage information. Use AWS Migration Hub to discover and group servers into applications before initiating the migration. Generate Amazon EC2 instance recommendations using AWS Migration Hub.
- (selected) Install the AWS Application Discovery Agent on both the physical servers and Virtual machines to gather performance and usage information. Use AWS Migration Hub to discover and group servers into applications before initiating the migration. Follow the EC2 size recommendations of AWS Compute Optimizer.
- Install the Amazon Inspector Agent on both the physical servers and Virtual machines to assess and scan running applications. Use AWS Migration Hub to discover and group servers into applications before initiating the migration. Follow the EC2 size recommendations of AWS Compute Optimizer.
- Install the AWS Systems Manager Agent on both the physical servers and Virtual machines to perform an application-level assessment. Utilize AWS Systems Manager Application Manager to logically separate servers into different applications. Input server size data into the AWS Pricing calculator and adhere to its recommendations.

The option that says: **Install the AWS Application Discovery Agent on both the**

physical servers and Virtual machines to gather performance and usage information. Use AWS Migration Hub to discover and group servers into applications before initiating the migration. Follow the EC2 size recommendations of AWS Compute Optimizer is incorrect. AWS Compute Optimizer provides recommendations for optimal AWS resource utilization based on historical usage data IN AWS. In this case, the company has not yet migrated to AWS, so there's no historical usage data for the Compute Optimizer to base its recommendations on.

59. QUESTION

An organization uses AWS Organizations to manage its IT resources across multiple member accounts. The organization deploys virtual appliances as part of its centralized networking strategy. The appliances are critical for the company's network security and must scale dynamically to meet fluctuating traffic demands. The virtual appliances operate in a centralized networking account connected through a transit gateway to various member account VPCs.

Recently, a misconfigured script accidentally terminated all instances of the virtual appliances, causing operational downtime. In response, the organization revised the startup scripts for the appliances to enhance resilience and scalability.

A solutions architect must find a solution to efficiently scale the virtual appliances horizontally, ensure secure and private connection across accounts, and minimize manual configuration.

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

- [ ] Set up an Auto Scaling group using a launch template with the updated script as user data to automate the configuration of virtual appliances, linking to a target group with instance-based targets.
- [x] Configure VPC peering between the centralized networking account and member accounts to streamline network traffic routing.
- [x] Deploy a Gateway Load Balancer in the centralized networking account and configure it with an endpoint service using AWS PrivateLink.
- [ ] Use an Application Load Balancer to distribute traffic to the virtual appliances based on demand.
- [ ] Implement AWS Direct Connect to establish a dedicated network connection between the centralized networking account and member account VPCs.

To provide scalability of virtual appliances while maintaining consistent security policies across different accounts, a solutions architect should use a **combination of Gateway Load Balancer, AWS PrivateLink, and Auto Scaling group**. The Gateway Load Balancer would distribute traffic to the virtual appliances, allowing them to **scale horizontally behind t**he load balancer as traffic increases. Using **AWS PrivateLink, the virtual appliances would be accessible to other accounts in a private** and secure manner without exposing them publicly. Configuring an **Auto Scaling group with the updated startup script would enable automatic scaling of the virtual appliance instances**, 使用启动模板和更新后的脚本作为用户数据设置自动扩展组，以自动配置虚拟设备，并链接到具有基于实例的目标的目标组。linking to a target group associated with the Gateway Load Balancer. Together, these steps would eliminate manual work and provide scalability of the appliances, along with secure and private connections across accounts.

64. QUESTION

A retail company is using Amazon OpenSearch Service to analyze its sales and inventory data. Every week, new data from an Amazon S3 Standard bucket is indexed and loaded into a 20-data node Amazon OpenSearch cluster. Read-only queries are performed on this data to monitor recent trends. After 1 week, it's occasionally accessed for identifying long-term patterns. After three months, the index containing the older data is deleted from the system. However, due to audit requirements, the company needs to keep a complete copy of all processed data.

The company is looking for strategies to reduce storage costs without abandoning Amazon OpenSearch. A slower query response time on infrequently accessed data is acceptable as long as it can be retrieved on demand.

Which solution fits the requirements while being the MOST cost-effective?

- Downsize the OpenSearch cluster by reducing the number of its data nodes. Add UltraWarm nodes to compensate for the read capacity. Create an Index State Management (ISM) policy that moves data to cold storage after 1 week. Use an S3 lifecycle policy to transition data older than 3 months to the S3 Glacier Deep archive.
- Downsize the OpenSearch cluster by reducing the number of its data nodes. Add UltraWarm nodes to compensate for the read capacity. Create an Index State Management (ISM) policy that moves data to cold storage after 1 week. Use an S3 lifecycle policy to transition data older than 3 months to the S3 Infrequently Access tier.
- Upsize the OpenSearch cluster by adding UltraWarm nodes to improve read performance. Use an S3 lifecycle policy to delete data older than 3 months.
- **Reconfigure the OpenSearch cluster by replacing all data nodes with a mix of UltraWarm nodes and cold storage nodes. Use the UltraWarm node for indexing and the cold storage for reading. Create an Index State Management (ISM) policy that moves data to cold storage after 1 week. Use an S3 lifecycle policy to transition data older than 3 months to the S3 Glacier Deep archive.**

Reconfigure the OpenSearch cluster by replacing all data nodes with a mix of UltraWarm nodes and cold storage nodes. Use the UltraWarm node for indexing and the cold storage for reading. Create an Index State Management (ISM) policy that moves data to cold storage after 1 week. Use an S3 lifecycle policy to transition data older than 3 months to the S3 Glacier Deep archive is incorrect. This approach is not valid because UltraWarm nodes are designed to work on read-only data.

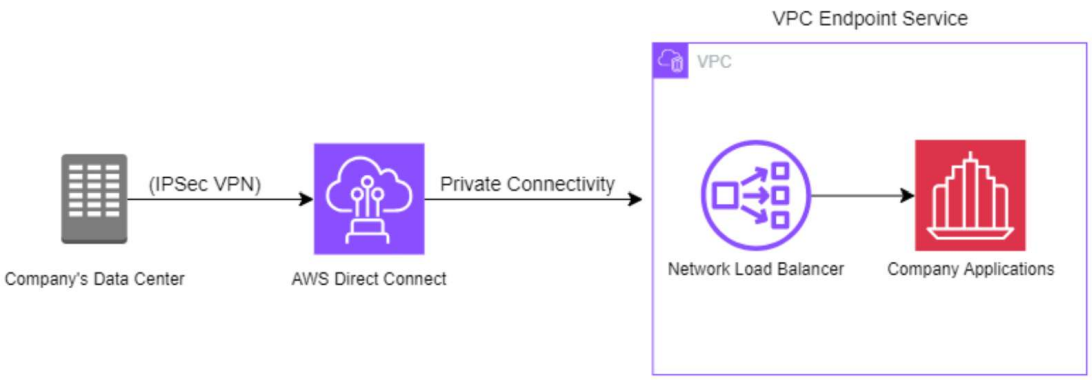
66. QUESTION

An e-commerce company operates its core infrastructure within a private data center. This infrastructure is linked to AWS through a combination of AWS Direct Connect and a secure IPSec VPN, ensuring that sensitive customer data remains off the public internet. As part of its strategic growth, the company aims to extend its proprietary services to other e-commerce businesses hosted on AWS.

Which networking solution aligns with the company's requirements?

- **Set up a NAT Gateway in a VPC for the company's applications and secure it with network access control and security group rules.**
- Establish a VPC Endpoint Service for the company's applications and associate it with a Network Load Balancer that manages TCP traffic. Maintain a secure connection between the company's data center and AWS using Direct Connect.
- Use AWS Direct Connect to link the company's data center to a VPC in AWS. Within the VPC, set up security group rules to manage access to the company's applications.
- Set up a VPC Endpoint Service for the company's applications and link it with an Application Load Balancer that handles HTTP or HTTPS traffic. Maintain a secure connection between the company's data center and AWS using Direct Connect.

A **VPC Endpoint Service** allows the **company's applications to be accessed securely within the AWS network. This is a crucial component in the solution as it enables the company's services to be exposed to other businesses on AWS without exposing the data to the public internet.** This is particularly important given the sensitive nature of the data handled by the company.
The Network Load Balancer operates at the fourth layer of the Open Systems Interconnection (OSI) model and can handle millions of requests per second. By efficiently managing TCP traffic, the Network Load Balancer ensures high availability and fault tolerance of the applications. This is critical for maintaining a high-quality user experience, especially as the company expands its services to other businesses on AWS.



68. QUESTION

An IT company provides on-demand video training materials to its employees. High-resolution MP4 format videos are created monthly to increase the topics covered in the video library. Most employees that will view the videos are working remotely from different countries. The video application installed on the employee laptops requires the videos to be in HTTP Live Streaming (HLS) format. The management asked the solutions architect to design a cost-effective solution that will transcode the training videos into the proper format.

Which of the following architectures meet the above requirements while maintaining high availability and good quality video transmission?

- Create a queue in AWS Elemental MediaConvert to transcode the high-resolution MP4 videos into the HLS format. Store the transcoded videos on an Amazon S3 bucket. Configure Lifecycle Management on the bucket to move the original videos to Amazon S3 Glacier Instant Retrieval. Create an Amazon CloudFront distribution and set the S3 bucket as the origin to serve the transcoded videos.
- Create a pipeline in AWS CodePipeline with stages that transcode the high-resolution MP4 videos into the HLS format and send the transcoded videos to an Amazon S3 bucket. Configure Lifecycle Management on the bucket to move the original videos to Amazon S3 Glacier Instant Retrieval. Then, set up an endpoint in AWS Wavelength and configure it to serve the transcoded videos from the S3 bucket.
- **Create a pipeline on Amazon Elastic Transcoder to transcode the high-resolution MP4 videos into the HLS format. Host the transcoded videos on large EBS volumes attached to Amazon EC2 instances. Configure automated EBS snapshots to back up the video files every few days. Create an Amazon CloudFront distribution and set the EC2 instances as the origin to serve the transcoded videos.**
- Create a Jenkins pipeline to transcode the high-resolution MP4 videos. Use an SQS queue to distribute the transcoding job to a set of Amazon EC2 instances in an Auto Scaling group that scales based on the length of the queue. Store the transcoded videos on EBS volumes and configure automated snapshots to back up the files every few days. Create an Amazon CloudFront distribution and set the EC2 instances as the origin to serve the transcoded videos.

69. QUESTION

A media organization operates a content delivery system that experiences peak loads whenever new content is released. The release dates and times for the content are pre-set and automatically triggered. The system is hosted on an Amazon ECS (Elastic Container Service) cluster, consisting of Amazon EC2 On-Demand Instances within an ASG (Auto Scaling Group) that uses a predictive scaling policy. The Amazon ECS cluster frequently retrieves data from an Amazon S3 bucket located in the same AWS Region. All traffic routes through a NAT gateway.

The organization aims to reduce platform costs, all while ensuring that availability is not compromised.

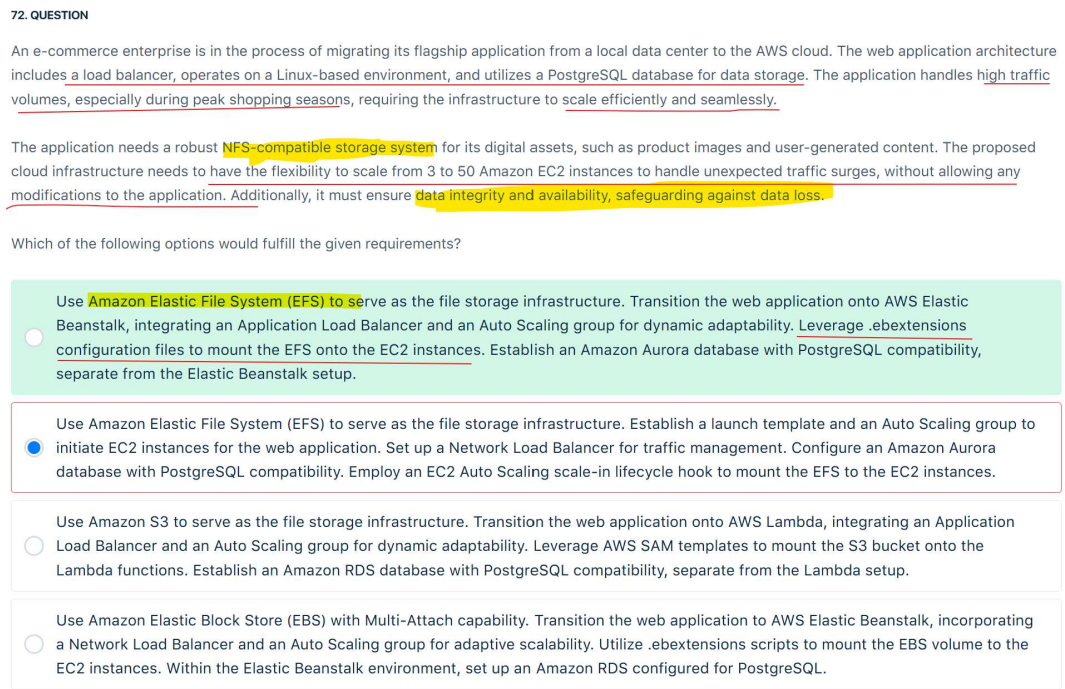
What combination of steps can be taken to achieve this goal? (Select TWO.)

- [x] Enable S3 Intelligent-Tiering to move objects to cheaper storage tiers automatically.
- [ ] Create a new ECS capacity provider using an Auto Scaling Group of Spot Instances, and adjust the strategy to distribute weight evenly.
- [ ] Replace the NAT gateway with a Gateway VPC Endpoint for Amazon S3.
- [x] Switch from the predictive scaling policy to a scheduled scaling policy.
- [ ] Replace the NAT gateway with a NAT instance hosted on an Amazon EC2 On-Demand Capacity Reservation.

1. **Manual Scaling**: You can manually adjust the desired capacity of your Auto Scaling group. This method is useful when you need to make immediate changes to your group's capacity.

2. **Scheduled Scaling**: This method allows you to set up scheduled actions to scale your group at specific times. It's ideal for predictable load changes that occur at fixed times.
3. **Dynamic Scaling**: This approach automatically adjusts capacity in response to changing demand. There are three types of dynamic scaling policies: a. Target Tracking Scaling: Adjusts capacity to maintain a specific metric at a target value. b. Step Scaling: Uses step adjustments to scale based on the size of the alarm breach. c. Simple Scaling: Adjusts capacity based on a single scaling adjustment.
4. **Predictive Scaling**: This method uses **machine learning to forecast future traffic and automatically provisions** the right number of EC2 instances in advance. It's useful for handling cyclical traffic patterns.

Gateway VPC Endpoints are specifically designed for A**mazon S3** and DynamoDB. They enable resources within a Virtual Private Cloud (VPC) to communicate with S3 or DynamoDB **without going through the public internet**. Gateway endpoints **use prefix lists** in the VPC route table to direct traffic to the target service. This setup provides a secure and cost-effective way to access S3 or DynamoDB from within a VPC.
The media organization frequently retrieves data from an Amazon S3 bucket. Their current setup involves a NAT gateway, which can lead to significant data transfer costs. By replacing the NAT gateway with a Gateway VPC Endpoint for Amazon S3, the organization can keep data traffic within the AWS network, thereby reducing data transfer costs and improving performance. This change maintains availability while aligning with the goal of cost reduction.



72. QUESTION

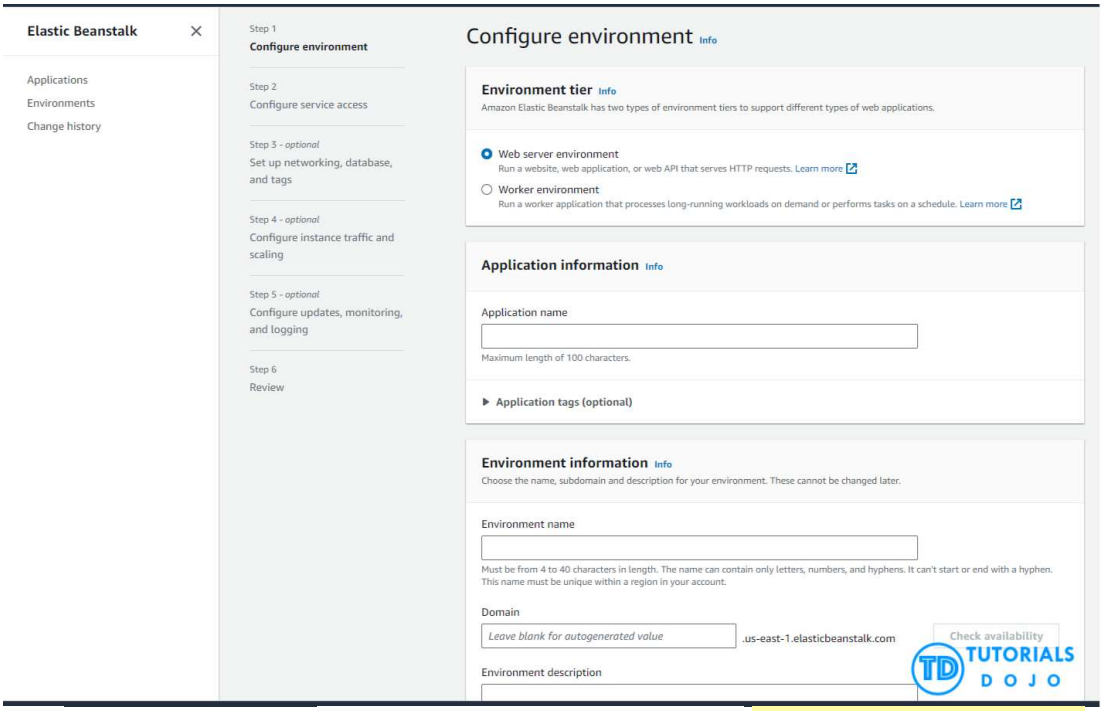
An e-commerce enterprise is in the process of migrating its flagship application from a local data center to the AWS cloud. The web application architecture includes a load balancer, operates on a Linux-based environment, and utilizes a PostgreSQL database for data storage. The application handles high traffic volumes, especially during peak shopping seasons, requiring the infrastructure to scale efficiently and seamlessly.

The application needs a robust NFS-compatible storage system for its digital assets, such as product images and user-generated content. The proposed cloud infrastructure needs to have the flexibility to scale from 3 to 50 Amazon EC2 instances to handle unexpected traffic surges, without allowing any modifications to the application. Additionally, it must ensure data integrity and availability, safeguarding against data loss.

Which of the following options would fulfill the given requirements?

- Use Amazon Elastic File System (EFS) to serve as the file storage infrastructure. Transition the web application onto AWS Elastic Beanstalk, integrating an Application Load Balancer and an Auto Scaling group for dynamic adaptability. Leverage .ebextensions configuration files to mount the EFS onto the EC2 instances. Establish an Amazon Aurora database with PostgreSQL compatibility, separate from the Elastic Beanstalk setup.
- (selected) Use Amazon Elastic File System (EFS) to serve as the file storage infrastructure. Establish a launch template and an Auto Scaling group to initiate EC2 instances for the web application. Set up a Network Load Balancer for traffic management. Configure an Amazon Aurora database with PostgreSQL compatibility. Employ an EC2 Auto Scaling scale-in lifecycle hook to mount the EFS to the EC2 instances.
- Use Amazon S3 to serve as the file storage infrastructure. Transition the web application onto AWS Lambda, integrating an Application Load Balancer and an Auto Scaling group for dynamic adaptability. Leverage AWS SAM templates to mount the S3 bucket onto the Lambda functions. Establish an Amazon RDS database with PostgreSQL compatibility, separate from the Lambda setup.
- Use Amazon Elastic Block Store (EBS) with Multi-Attach capability. Transition the web application to AWS Elastic Beanstalk, incorporating a Network Load Balancer and an Auto Scaling group for adaptive scalability. Utilize .ebextensions scripts to mount the EBS volume to the EC2 instances. Within the Elastic Beanstalk environment, set up an Amazon RDS configured for PostgreSQL.

AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS. This service would allow the e-commerce enterprise to easily migrate their web application to the cloud.



The `.ebextensions` **configuration files** are used to **customize the software that runs on the EC2 instances** of your Elastic Beanstalk environment. You can use `.ebextensions` configuration files to mount the EFS onto the EC2 instances.

The option that says: **Use Amazon Elastic File System (EFS) to serve as the file storage infrastructure. Establish a launch template and an Auto Scaling group to initiate EC2 instances for the web application. Set up a Network Load Balancer for traffic management. Configure an Amazon Aurora database with PostgreSQL compatibility. Employ an EC2 Auto Scaling scale-in lifecycle hook to mount the EFS to the EC2 instances** is incorrect because lifecycle hooks are not designed for mounting file systems, which is necessary for the application's operation.

Launch Template é um **modelo reutilizável** que define *como* suas instâncias EC2 devem ser criadas automaticamente.

Ele guarda a c**onfiguração padrão que o Auto Scaling Group ou você mesmo vão usar para lançar novas EC2.**

O **RDS Data API** é uma **API HTTP** que permite executar consultas SQL em **Aurora Serverless v1/v2 sem precisar de conexão JDBC/ODBC**.

RDS Data API = Execute SQL via HTTP, sem conexões, com IAM.

Você chama a API via HTTP (SDK, Lambda, apps serverless), e ela executa o SQL no banco.

✓ Integração com IAM

Não precisa senhas no código.

Permissões controladas pelo IAM ("quem pode rodar SQL").

✓ Retorna JSON

Resultados vêm estruturados em JSON, simples de tratar.

✓ Perfeito para workloads event-driven

Lambda → Data API → Aurora Serverless

```
rds = boto3.client('rds-data')


response = rds.execute_statement(
    resourceArn=DB_ARN,
    secretArn=SECRET_ARN,
    sql="SELECT * FROM weather",
    database="weatherdb"
)
```

Deploy a Windows Amazon EC2 instance and install the Migration Evaluator agentless collector on the EC2 instance to collect the data from the on-premises servers via SNMP. Use the Migration Evaluator to generate the comprehensive Total Cost of Ownership (TCO) analysis for the proposed migration.

▧ 1. AWS DataSync
Purpose: Move large amounts of data fast, automatic, recurring, high-performance.
✓ Use DataSync when you need:
Migration of TBs/PBs
Incremental sync (only changed files)
Scheduled/automated transfers
VPC/private network transfers
Validated, checksum-protected transfer
Copying on-prem → AWS, AWS → AWS, AWS → on-prem
🔧 Typical sources/destinations:
On-prem NFS/SMB file servers
S3
EFS
FSx (Windows/ONTAP/OpenZFS/Lustre)
S3 cross-region
💧 Keywords:
Fast, automated, large-scale, NFS/SMB, scheduled, high throughput, verification.

Amazon AppStream 2.0 aplicacao desktop
AWS AppSync é um serviço gerenciado da AWS para criar APIs GraphQL(custom schema) e WebSocket em tempo real, com segurança, caching e sincronização de dados integrada.

Conectar on-premise → VPC Endpoint

Com Direct Connect + PrivateLink você pode expor um serviço da VPC para on-premise sem abrir na internet. jdbc
ensuring that sensitive customer data remains off the public internet
Establish a VPC Endpoint Service for the company's applications and associate it with a Network Load Balancer that manages TCP traffic. Maintain a secure connection between the company's data center and AWS using Direct Connect.

Deploy AWS Application Discovery Agent on the on-premises Hyper-V servers to collect server data.
Run predefined Amazon Athena queries on the data hosted in Amazon S3.
Enable Data exploration in AWS Migration Hub.
✓ Exporta automaticamente para:
AWS Migration Hub
Amazon S3 (CSV/JSON)
AWS Athena
QuickSight
...para análises detalhadas.

Use **AWS Transfer for SFTP service** instead to serve as the SFTP server. Update the Amazon Route 53 record to point the sftp.tutorialsdojo.com URL to the server endpoint hostname. fully managed, highly scalable solution for hosting SFTP services in AWS.
AWS Transfer Family supports transferring data over the following protocols:
-Secure Shell (SSH) File Transfer Protocol (SFTP) (AWS Transfer for SFTP)
-File Transfer Protocol Secure (FTPS) (AWS Transfer for FTPS)
-File Transfer Protocol (FTP) (AWS Transfer for FTP)

▨ 3. AWS Transfer Family

Purpose: Replace legacy FTP/SFTP/FTPS servers with a managed solution.

✓ Use Transfer Family when:
You need partners, suppliers, vendors to upload/download files

External systems use SFTP/FTP/FTPS
You need a file server endpoint that drops files into S3 or EFS
🔧 Example:
Partner uploads file via SFTP → Transfer Family → File lands in S3 → Lambda/Glue processes it.

RDS Read Replica is primarily used to improve the scalability of the database. NOT highly available 24/7 nor fault-tolerant in the event of an AZ outage.

O que é o AWS Trusted Advisor?

O AWS Trusted Advisor é um serviço que analisa automaticamente sua conta AWS e fornece recomendações de melhores práticas em 5 áreas:
Cost Optimization (redução de custos)
Performance
Security
Fault Tolerance (alta disponibilidade)
Service Limits / Quotas
Ele funciona como um consultor automático, te dizendo onde você está gastando demais, onde há risco, onde está inseguro, etc.

EC2Rescue tool

unreachable due to network misconfigurations, RDP issues, firewall settings, and many others to meet the compliance requirements.

##

Because **ALB does not support Least Outstanding Requests (LOR).**
Only NLB supports LOR, and ALB uses round-robin for HTTP/HTTPS unless you use advanced weighting rules.

🟢 1. Round-robin routing (RR)

É o algoritmo mais simples.

✓ Como funciona:

O load balancer envia requisições em ordem sequencial, distribuindo igualmente.

Ele não considera:

carga do servidor

número de requisições ativas

capacidade dos targets

🧠 Exemplo:
Requisição 1 → EC2 A
Requisição 2 → EC2 B
Requisição 3 → EC2 C
Requisição 4 → EC2 A
Requisição 5 → EC2 B

✓ Bom para:

servidores iguais

workloads leves

latência previsível

❌ Problema:

Se uma instância ficar lenta, ela vai continuar recebendo requisições pelo mesmo ritmo — causando fila e lentidão para os usuários.

🟢 2. Least Outstanding Requests (LOR) -> NLB

Este algoritmo distribui requisições para o servidor menos ocupado.

✓ Como funciona:

O load balancer monitora quantas requisições cada target está processando.

Ele envia a nova requisição para o target com menos requisições pendentes (outstanding requests).

🧠 Exemplo:
EC2 A está com 10 requisições ativas
EC2 B está com 2 requisições ativas
EC2 C está com 5 requisições ativas

→ Nova requisição vai para EC2 B (que está menos ocupado)

✓ Benefícios:

Distribuição mais inteligente

Evita sobrecarregar instâncias lentas

Adapta ao desempenho real dos servidores

Ideal para workloads variáveis

Use AWS Lambda functions to store a hash of each PII data on an Amazon Managed Blockchain network. Store the PII data off-chain in an Amazon DynamoDB table.

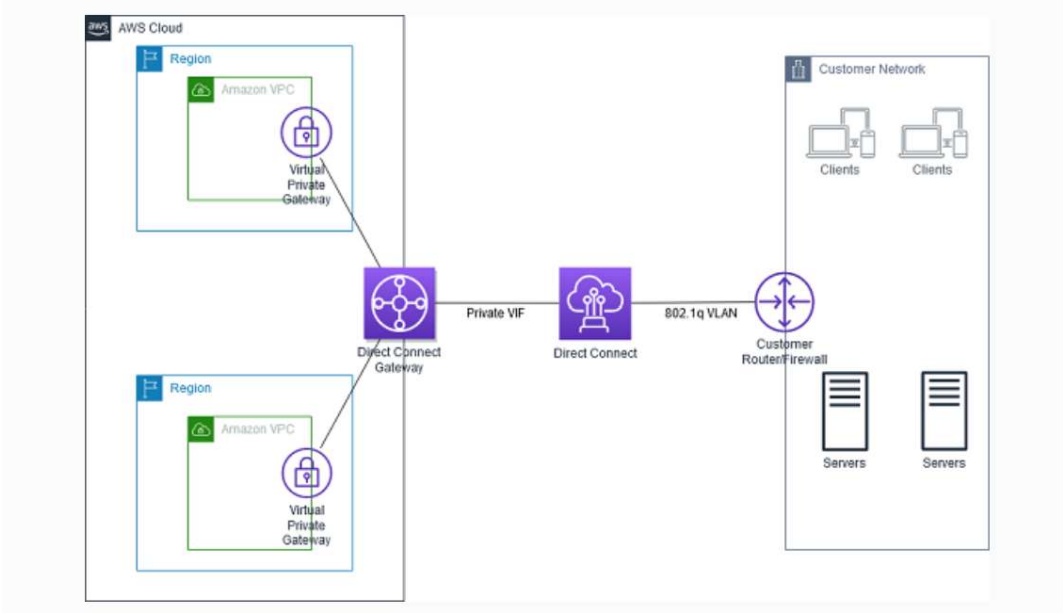
DynamoDB with a Target Utilization of 100% auto scaling target utilization values between 20 and 90 percent for your read and write capacity, not 100%.

24. QUESTION

A company has an on-premises data center and uses a single 1 Gbps AWS Direct Connect connection to connect to its cloud resources in the us-east-1 region. The AWS Direct Connect connection uses a single private virtual interface to establish a connection to the VPC in us-east-1. The company has plans to expand and create a new VPC in the us-west-1 region. The solutions architect must design a solution that will add redundancy to the current AWS Direct Connect connection and use the same network to provide connectivity to the new VPC in the new region.

Which of the following should the solutions architect implement to meet the requirements?

- Remove the current private virtual interface. Request to provision a second AWS Direct Connect connection for redundancy. Create a new private virtual interface for each Direct Connect connection. Create a transit gateway for each region's VPC. Connect both private VIFs to the transit gateways.
- Retain the current private virtual interface. Request to provision a second AWS Direct Connect connection for redundancy. Create a new public virtual interface for the second connection. Connect the us-west-1 VPC to the new public virtual interface.
- Retain the current private virtual interface. Request to provision a second AWS Direct Connect connection for redundancy. Create a new private virtual interface for the second connection. Create virtual private gateways on each VPC and associate both of them to the two private VIFs.
- **Remove the current private virtual interface. Request to provision a second AWS Direct Connect connection. Create a Direct Connect gateway. Create a new private virtual interface for each connection and associate them both to the Direct Connect gateway. Create a virtual private gateway for each region's VPC and connect them to the Direct Connect gateway.**



Use AWS Direct Connect gateway to connect your VPCs. You associate an AWS Direct Connect gateway with either of the following gateways:

-A transit gateway when you have multiple VPCs in the same Region

-A virtual private gateway

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**. In the diagram, each VPC has a virtual private gateway that connects to the Direct Connect gateway using a virtual private gateway association. The Direct Connect gateway uses a private virtual interface for the connection to the AWS Direct Connect location. There is an AWS Direct Connect connection from the location to the customer data center.

26. QUESTION

A company has developed an Optical Character Recognition (OCR) application that allows users to upload PDF files to an Amazon S3 bucket. The user-facing website is hosted on S3, and its content is distributed by Amazon CloudFront. When a user initiates an OCR job, the application makes a call to a REST API in Amazon API Gateway (Regional), which in turn invokes an AWS Lambda function asynchronously to start the OCR process. The OCR output's S3 path is then stored in an Amazon DynamoDB table

Currently, the application stack is deployed in the `us-east-1` AWS region. The company wants to expand its user base to include users from Asia and the Middle East and aims to improve latency for these users.

Which combination of steps is the most cost-effective approach that would meet this requirement? (Select TWO.)

- [ ] Migrate the DynamoDB table to Amazon Aurora Serverless and use an Amazon RDS Proxy in front of the Lambda function.
- [ ] Deploy additional Lambda functions and S3 buckets in Asia and Middle East regions. Set up cross-region S3 replication. Configure Route 53 Geolocation Routing to direct users to the closest regional resources.
- [x] Enable S3 Transfer Acceleration on the S3 bucket and update the application code to use the Transfer Acceleration endpoint.
- [x] Switch the existing Amazon API Gateway from a Regional endpoint to an Edge-Optimized endpoint.
- [ ] Upload the PDF files to an Amazon EBS-backed Amazon EC2 instance in the `us-east-1` region. Create an AWS Global Accelerator for the EC2 instance. Switch the existing Amazon API Gateway from a Regional endpoint to an Edge-Optimized endpoint.

S3 Transfer Acceleration é um recurso do Amazon S3 que acelera uploads e downloads de objetos em longas distâncias usando a rede global de edge locations da AWS (Amazon CloudFront).

38. QUESTION

A company is developing a containerized web application using the .NET Core framework which is packaged as a Docker container. This application will serve public traffic and the management wants to deploy it in AWS. The application requires a highly-available Microsoft SQL Server as its database backend. As a security best practice, the SQL Server connection string should not be saved inside the container to avoid exposing the database password.

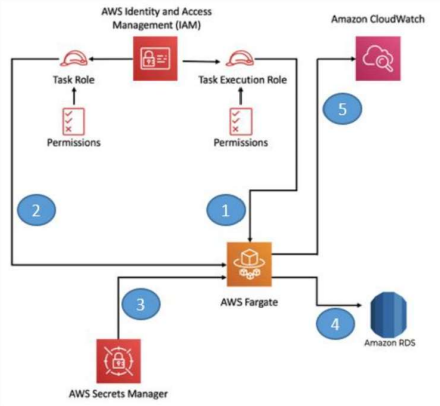
Which of the following options should the Solutions Architect implement to deploy the application in AWS while satisfying the company requirements?

- Deploy the SQL Server on Amazon RDS with Multi-AZ enabled. Create a secret in AWS Secrets Manager to store the database credentials. Create an Amazon EKS Distro cluster with Service Auto Scaling for the application tasks which are placed behind an Application Load Balancer with multiple Availability Zones. Create an IAM role associated with the EKS service that allows fetching of secrets from Secrets Manager. Specify the ARN of the database secret in the environment variable section of the application's pod definition. Create an empty non-persistent volume attachment in the pod definition. This allows EKS to write the database credentials to the non-persistent volume when starting the containers.

- Deploy the SQL Server in an Auto Scaling group of Amazon EC2 instances. Create an encrypted parameter in AWS SSM Parameter Store to store the database credentials. Create a Fargate cluster with Service Auto Scaling for the application tasks which are placed behind an Application Load Balancer with multiple Availability Zones. Create an ECS task execution role associated with the application service that allows fetching of parameters from SSM Parameter Store. Specify the ARN of the database parameter in the environment variable section of the application's task definition. This allows Fargate to inject the database credentials as an environment variable when starting the containers.

- Deploy the SQL Server in an AWS Fargate cluster with Service Auto Scaling. Create an encrypted parameter in AWS SSM Parameter Store to store the database credentials. Create another Fargate Service Auto Scaling for the application tasks which are placed behind an Application Load Balancer. Create an ECS task execution role associated with the application service that allows fetching of parameters from SSM Parameter Store. Specify the ARN of the database parameter in the environment variable section of the application's task definition. This allows Fargate to inject the database credentials as an environment variable when starting the containers.

- Deploy the SQL Server on Amazon RDS with Multi-AZ enabled. Create a secret in AWS Secrets Manager to store the database credentials. Create a Fargate cluster with Service Auto Scaling for the application tasks which are placed behind an Application Load Balancer with multiple Availability Zones. Create an ECS task execution role associated with the Fargate service that allows fetching of secrets from Secrets Manager. Specify the ARN of the database secret in the environment variable section of the application's task definition. This allows Fargate to inject the database credentials as an environment variable when starting the containers.



When you inject a secret as an environment variable, you can specify the full contents of a secret, a specific JSON key within a secret, or a specific version of a secret to inject. This helps you control the sensitive data exposed to your container.