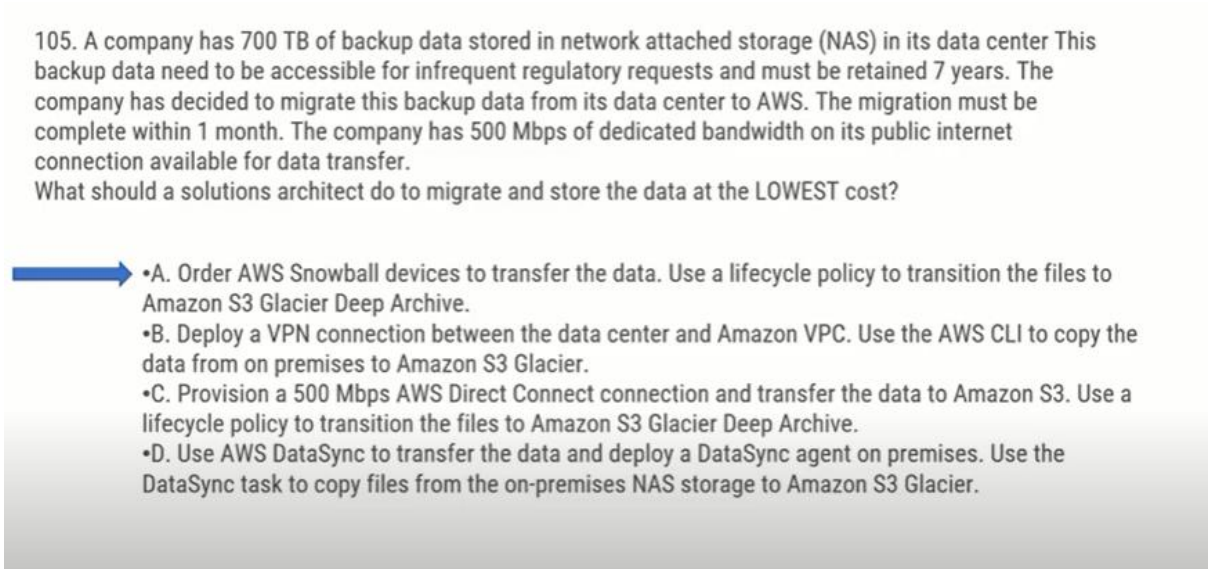
Question1: **Please advise the correct option**



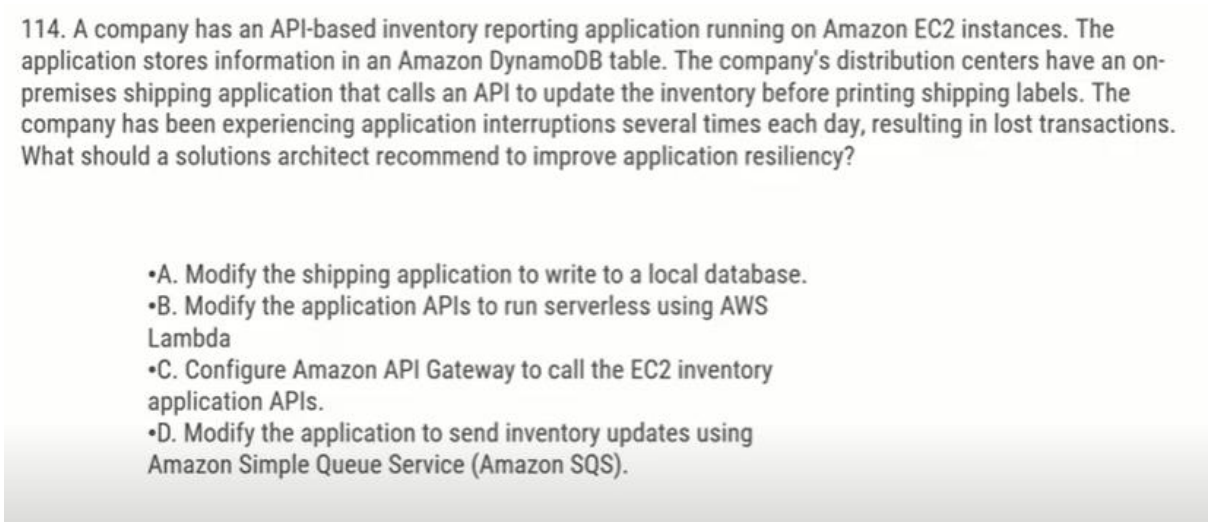
105. A company has 700 TB of backup data stored in network attached storage (NAS) in its data center This backup data need to be accessible for infrequent regulatory requests and must be retained 7 years. The company has decided to migrate this backup data from its data center to AWS. The migration must be complete within 1 month. The company has 500 Mbps of dedicated bandwidth on its public internet connection available for data transfer.
What should a solutions architect do to migrate and store the data at the LOWEST cost?

•A. Order AWS Snowball devices to transfer the data. Use a lifecycle policy to transition the files to Amazon S3 Glacier Deep Archive.
•B. Deploy a VPN connection between the data center and Amazon VPC. Use the AWS CLI to copy the data from on premises to Amazon S3 Glacier.
•C. Provision a 500 Mbps AWS Direct Connect connection and transfer the data to Amazon S3. Use a lifecycle policy to transition the files to Amazon S3 Glacier Deep Archive.
•D. Use AWS DataSync to transfer the data and deploy a DataSync agent on premises. Use the DataSync task to copy files from the on-premises NAS storage to Amazon S3 Glacier.

To me, the correct response is A. as we have a 30-day window, it is not D as it would take 141 days, 1 hours, 22 minutes, and 38 seconds to transport 700 Tb of data over the 500 Mbps network.

Since the deployment of a direct connect will take more than 30 days, C cannot be the answer.

Question 2: **Please advise the correct option**



114. A company has an API-based inventory reporting application running on Amazon EC2 instances. The application stores information in an Amazon DynamoDB table. The company's distribution centers have an on-premises shipping application that calls an API to update the inventory before printing shipping labels. The company has been experiencing application interruptions several times each day, resulting in lost transactions.
What should a solutions architect recommend to improve application resiliency?

•A. Modify the shipping application to write to a local database.
•B. Modify the application APIs to run serverless using AWS Lambda
•C. Configure Amazon API Gateway to call the EC2 inventory application APIs.
•D. Modify the application to send inventory updates using Amazon Simple Queue Service (Amazon SQS).

The person should advise:

D. Make changes to the programme so that it sends inventory updates using the Amazon Simple Queue Service. (Amazon SQS).

Without having to establish a direct connection to the DynamoDB database or EC2 instances, the shipping application can deliver inventory update messages to the queue by using SQS. The EC2

inventory application may then process the messages from the queue and update DynamoDB whenever connectivity is restored.

This ensures that no inventory updates are lost during interruptions and assists in decoupling the applications.

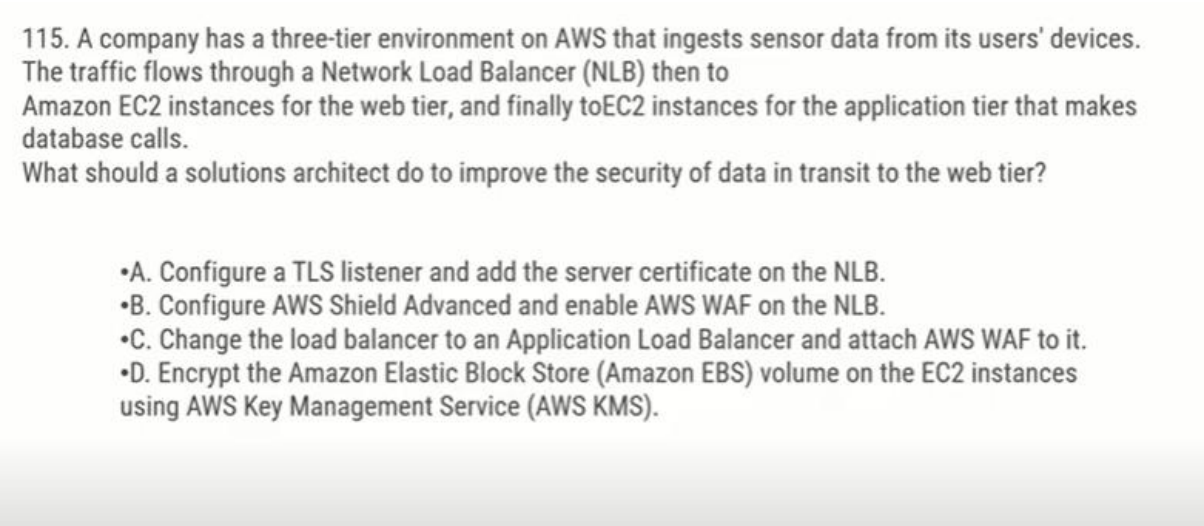
The issue of application downtime leading to lost transactions would not be satisfactorily addressed by options A, B, and C.

Therefore, the main suggestions are:

Decouple the applications using a messaging queue (SQS).

Make sure that there is no need for direct connectivity between the shipping app and the DynamoDB/EC2 instances.

Question 3: **Option A should be the correct option as NLB supports TLB**


115. A company has a three-tier environment on AWS that ingests sensor data from its users' devices. The traffic flows through a Network Load Balancer (NLB) then to
Amazon EC2 instances for the web tier, and finally toEC2 instances for the application tier that makes database calls.
What should a solutions architect do to improve the security of data in transit to the web tier?

•A. Configure a TLS listener and add the server certificate on the NLB.
•B. Configure AWS Shield Advanced and enable AWS WAF on the NLB.
•C. Change the load balancer to an Application Load Balancer and attach AWS WAF to it.
•D. Encrypt the Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instances using AWS Key Management Service (AWS KMS).

The following are the greatest options for enhancing data in transit security:

C. Switch to an application load balancer from the current load balancer. (ALB). On the ALB, enable AWS WAF.

A. Set up a TLS listener OR B. On the NLB, deploy the server certificate.

The traffic passing via the load balancers (NLB or ALB) and between the load balancers and EC2 instances will be encrypted under both of these configurations. By doing this, the sensor data is protected from eavesdropping and man-in-the-middle assaults.

Options B and D don't offer data in transit encryption.

While not encrypting traffic, AWS Shield Advanced and encrypting EBS volumes aid in other elements of security.

Additionally, the EC2 instances are protected from web application firewall (WAF) attacks by using an ALB in front of them.

Question 4: **Please advise the correct option**


119. An online shopping application accesses an Amazon RDS Multi-AZ DB instance. Database performance is slowing down the application. After upgrading to the next-generation instance type, there was no significant performance improvement.
Analysis shows approximately 700 IOPS are sustained, common queries run for long durations and memory utilization is high.
Which application change should a solutions architect recommend to resolve these issues?

•A. Migrate the RDS instance to an Amazon Redshift cluster and enable weekly garbage collection.
•B. Separate the long-running queries into a new Multi-AZ RDS database and modify the application to query whichever database is needed.
•C. Deploy a two-node Amazon ElastiCache cluster and modify the application to query the cluster first and query the database only if needed.
•D. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue for common queries and query it first and query the database only if needed.

The solutions architect ought to suggest option D in light of the aforementioned application issues:

For common queries, create an Amazon Simple Queue Service (Amazon SQS) FIFO queue, query it first, and then query the database only if necessary.

Among this strategy's major advantages are:

It lessens the volume of queries directly hitting the RDS database, lightening the strain and enhancing performance.

Response times ought to increase because the queries are periodically removed from the queue.

It serves as a caching layer, providing query results for frequent queries from memory or cache rather than the database.

The application is separated from the database, increasing resilience in the event of database outages.

Question 6: **Please advise the correct option**

123. A media company has an application that tracks user clicks on its websites and performs analytics to provide near-real time recommendations. The application has a Heel of Amazon EC2 instances that receive data from the websites and send the data to an Amazon RDS DB instance. Another fleet of EC2 instances hosts the portion of the application that is continuously checking changes in the database and executing SQL queries to provide recommendations. Management has requested a redesign to decouple the infrastructure. The solution must ensure that data analysts are writing SQL to analyze the data only No data can the lost during the deployment.
What should a solutions architect recommend?

•A. Use Amazon Kinesis Data Streams to capture the data from the websites Kinesis Data Firehose to persist the data on Amazon S3, and Amazon Athena to query the data.
→ •B. Use Amazon Kinesis Data Streams to capture the data from the websites. Kinesis Data Analytics to query the data, and Kinesis Data Firehose to persist the data on Amazon S3.
•C. Use Amazon Simple Queue Service (Amazon SQS) to capture the data from the websites, keep the fleet of EC2 instances, and change to a bigger instance type in the Auto Scaling group configuration.
•D. Use Amazon Simple Notification Service (Amazon SNS) to receive data from the websites and proxy the messages to AWS Lambda functions that execute the queries and persist the data. Change Amazon RDS to Amazon Aurora Serverless to persist the data.

The solutions architect should suggest choice A in light of the specified requirements:

Utilize Amazon Kinesis Data Streams to download data from websites, Amazon Kinesis Data Firehose to store the data on Amazon S3, and Amazon Athena to perform queries on the data.

Among this strategy's major advantages are:

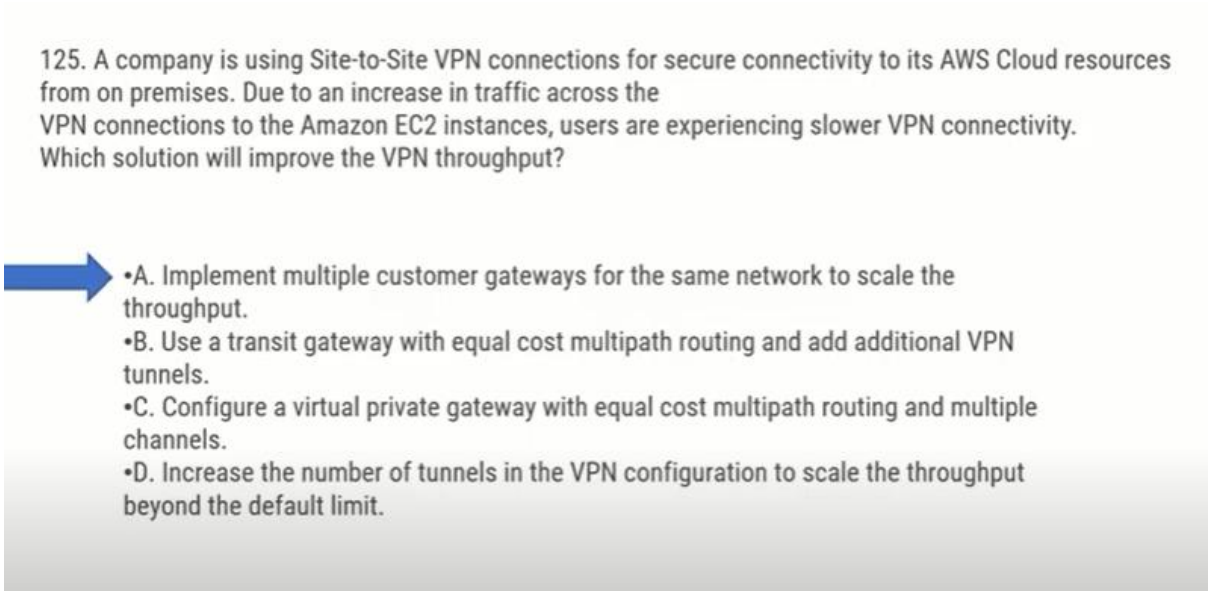
It completely decouples the parts of the infrastructure. The websites transmit data to Kinesis Data Streams, which uses Firehose to persist the data on S3. Athena looks up information on S3.

Websites, stream processors, and databases all may be scaled and managed independently because they are not directly connected.

The deployment doesn't result in any data loss. Kinesis makes sure that data is processed at least once, while Firehose keeps all records around.

Question 7: Can’t it be Option B as per below screenshot?

For Site-to-Site VPN connections on a transit gateway, you can use ECMP to get higher VPN bandwidth by aggregating multiple VPN tunnels. To use ECMP, the VPN connection must be configured for dynamic routing. ECMP is not supported on VPN connections that use static routing. For more information, see Transit gateways.



The solutions architect should advocate the following given the problems with slower VPN connectivity brought on by higher traffic:

C. Set up a virtual private gateway with multiple channels and equal cost multipath routing.

Over the built-in VPN gateway, a virtual private gateway (VGW) offers increased throughput and scalability.

One of the main advantages of employing a VGW is that:

supports equal cost multipath (ECMP) routing, which enhances bandwidth efficiency. Traffic can be forwarded via several equal-cost pathways.

enables you to set up several channels and VPN tunnels between your network and AWS. This greatly exceeds the default VPN gateway constraints in terms of aggregate bandwidth.

a transit gateway, which is made for much larger hub-and-spoke network designs, requires more setup time.

Question 8: **Orders are processed in the order they are received – should be Option B as it talks about FIFO queue. Please confirm.**

138. A company is building an ecommerce web application on AWS. The application sends information about new orders to an Amazon API Gateway REST API to process. The company wants to ensure that orders are processed in the order that they are received.
Which solution will meet these requirements?

•A. Use an API Gateway integration to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic when the application receives an order. Subscribe an AWS Lambda function to the topic to perform processing.
•B. Use an API Gateway integration to send a message to an Amazon Simple Queue Service (Amazon SQS) FIFO queue when the application receives an order. Configure the SQS FIFO queue to invoke an AWS Lambda function for processing.
•C. Use an API Gateway authorizer to block any requests while the application processes an order.
•D. Use an API Gateway integration to send a message to an Amazon Simple Queue Service (Amazon SQS) standard queue when the application receives an order. Configure the SQS standard queue to invoke an AWS Lambda function for processing.

The solution that will meet the requirement of processing orders in the order they are received is option B, which uses an API Gateway integration to send a message to an Amazon Simple Queue Service (Amazon SQS) FIFO queue when the application receives an order. Amazon SQS FIFO queues preserve the exact order in which messages are sent and received, and also ensure that messages are processed exactly once, in the order in which they are received.

Option A, which uses an API Gateway integration to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic when the application receives an order, does not guarantee the order in which messages are processed because SNS does not preserve the order of messages.

Option C, using an API Gateway authorizer to block requests while the application processes an order, does not ensure that orders are processed in the order they are received, as it only blocks requests while processing is ongoing.

Option D, using an API Gateway integration to send a message to an Amazon Simple Queue Service (Amazon SQS) standard queue when the application receives an order, does not guarantee the order in which messages are processed, as standard queues do not preserve the order of messages.

Question 9: **AWS secrets manager helps you manage, retrieve and rotate DB credentials, hence Option A looks to be the correct one. Please advise.**

139. A company has an application that runs on Amazon EC2 instances and uses an Amazon Aurora database. The EC2 instances connect to the database by using user names and passwords that are stored locally in a file. The company wants to minimize the operational overhead of credential management.
What should a solutions architect do to accomplish this goal?

•A. Use AWS Secrets Manager. Turn on automatic rotation.
•B. Use AWS Systems Manager Parameter Store. Turn on automatic rotation.
•C. Create an Amazon S3 bucket to store objects that are encrypted with an AWS Key Management Service (AWS KMS) encryption key. Migrate the credential file to the S3 bucket. Point the application to the S3 bucket.
•D. Create an encrypted Amazon Elastic Block Store (Amazon EBS) volume for each EC2 instance. Attach the new EBS volume to each EC2 instance. Migrate the credential file to the new EBS volume. Point the application to the new EBS volume.

The best solution to minimize the operational overhead of credential management is Option A: Use AWS Secrets Manager. Turn on automatic rotation. Secrets Manager is a managed service that helps you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. It also provides built-in integration with AWS Key Management Service (KMS) to help you to easily encrypt and decrypt your secrets.

Question 10: **Please advise the correct option**

144. A company hosts a data lake on AWS. The data lake consists of data in Amazon S3 and Amazon RDS for PostgreSQL. The company needs a reporting solution that provides data visualization and includes all the data sources within the data lake. Only the company's management team should have full access to all the visualizations. The rest of the company should have only limited access.
Which solution will meet these requirements?

•A. Create an analysis in Amazon QuickSight. Connect all the data sources and create new datasets. Publish dashboards to visualize the data. Share the dashboards with the appropriate IAM roles.
•B. Create an analysis in Amazon QuickSight. Connect all the data sources and create new datasets. Publish dashboards to visualize the data. Share the dashboards with the appropriate users and groups.
•C. Create an AWS Glue table and crawler for the data in Amazon S3. Create an AWS Glue extract, transform, and load (ETL) job to produce reports. Publish the reports to Amazon S3. Use S3 bucket policies to limit access to the reports.
•D. Create an AWS Glue table and crawler for the data in Amazon S3. Use Amazon Athena Federated Query to access data within Amazon RDS for PostgreSQL. Generate reports by using Amazon Athena. Publish the reports to Amazon S3. Use S3 bucket policies to limit access to the reports.

To meet the requirement of a reporting solution that provides data visualization and includes all the data sources within the data lake, with only the company's management team having full access to all the visualizations, a solutions architect should use Amazon QuickSight with appropriate IAM roles.

Option B, creating an analysis in Amazon QuickSight, connecting all the data sources and creating new datasets, publishing dashboards to visualize the data, and sharing the dashboards with the appropriate users and groups, is the preferred solution. This solution allows fine-grained access control over the dashboards by leveraging IAM roles, which can be used to restrict access to sensitive data and features in the dashboards. Only the management team needs to be granted full access to all the visualizations.

Option A is also valid, but it specifies sharing dashboards with IAM roles rather than users and groups, which may not provide fine-grained access control.

Option C, creating an AWS Glue table and crawler for the data in Amazon S3, creating an AWS Glue extract, transform, and load (ETL) job to produce reports, publishing the reports to Amazon S3, and using S3 bucket policies to limit access to the reports, does not provide visualization capabilities and is not an efficient way to generate reports.

Option D, creating an AWS Glue table and crawler for the data in Amazon S3, using Amazon Athena Federated Query to access data within Amazon RDS for PostgreSQL, generating reports by using Amazon Athena, publishing the reports to Amazon S3, and using S3 bucket policies to limit access to the reports, also does not provide visualization capabilities and may not be optimal for generating reports.

Question 11: **Please advise the correct option**

157. A development team runs monthly resource-intensive tests on its general purpose Amazon RDS for MySQL DB instance with Performance Insights enabled. The testing lasts for 48 hours once a month and is the only process that uses the database. The team wants to reduce the cost of running the tests without reducing the compute and memory attributes of the DB instance.
Which solution meets these requirements MOST cost-effectively?

- A. Stop the DB instance when tests are completed. Restart the DB instance when required.
- B. Use an Auto Scaling policy with the DB instance to automatically scale when tests are completed.
- C. Create a snapshot when tests are completed. Terminate the DB instance and restore the snapshot when required.
- D. Modify the DB instance to a low-capacity instance when tests are completed. Modify the DB instance again when required.

To reduce the cost of running monthly resource-intensive tests on a general purpose Amazon RDS for MySQL DB instance without reducing the compute and memory attributes of the DB instance, the most cost-effective solution is to stop the DB instance when tests are completed and restart it when required.

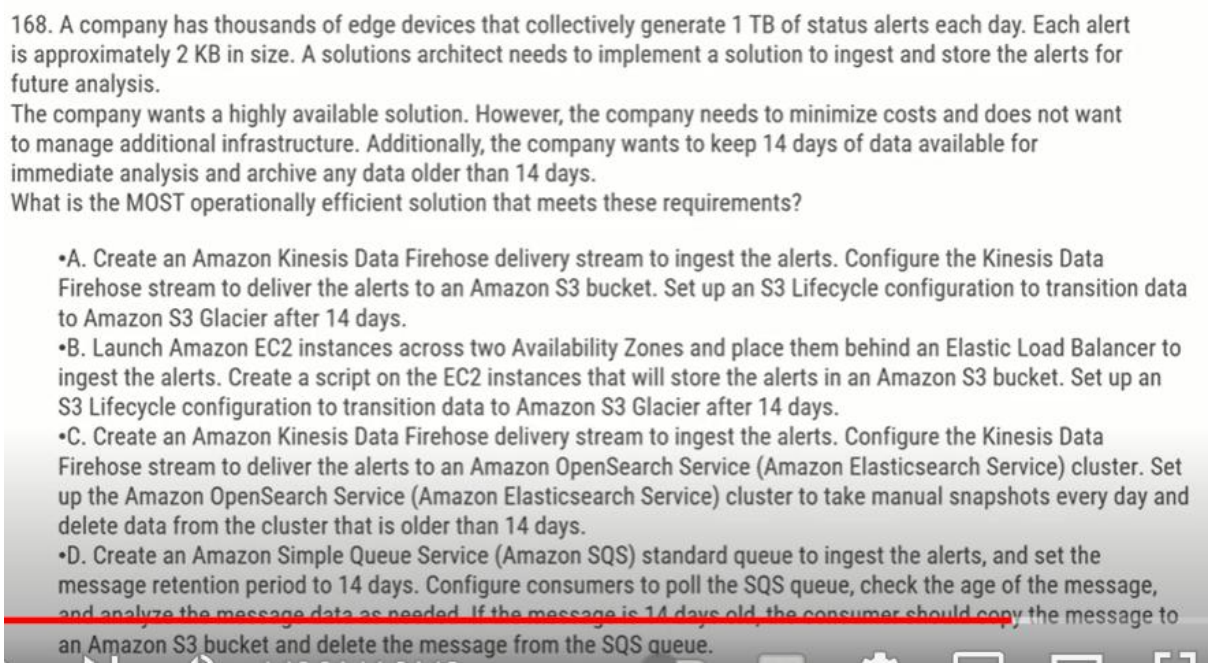
Option A, stopping the DB instance when tests are completed and restarting it when required, is the most cost-effective solution because it does not incur any ongoing costs while the DB instance is not in use. This solution also ensures that the compute and memory attributes of the DB instance remain unchanged, which is important for ensuring optimal performance during the tests.

Option B, using an Auto Scaling policy to automatically scale the DB instance when tests are completed, may not be as cost-effective as stopping the DB instance because scaling up the DB instance will increase the ongoing costs of the instance. Additionally, scaling up the DB instance may not be necessary if the tests only run once a month.

Option C, creating a snapshot when tests are completed, terminating the DB instance, and restoring the snapshot when required, may be more expensive than stopping the DB instance because creating and storing snapshots incurs additional costs. Additionally, restoring a snapshot can take longer than restarting a stopped DB instance, which may impact the testing schedule.

Option D, modifying the DB instance to a low-capacity instance when tests are completed and modifying it back when required, may not be as cost-effective as stopping the DB instance because modifying the instance incurs additional costs, and the modified instance may not provide optimal performance during the tests.

Question 12: **Please confirm the correct option**



The most operationally efficient solution that meets the requirements of ingesting and storing 1 TB of status alerts each day for future analysis, with a highly available and cost-effective solution, and keeping 14 days of data available for immediate analysis and archiving any data older than 14 days, is option A, creating an Amazon Kinesis Data Firehose delivery stream to ingest the alerts and deliver them to an Amazon S3 bucket, with S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days.

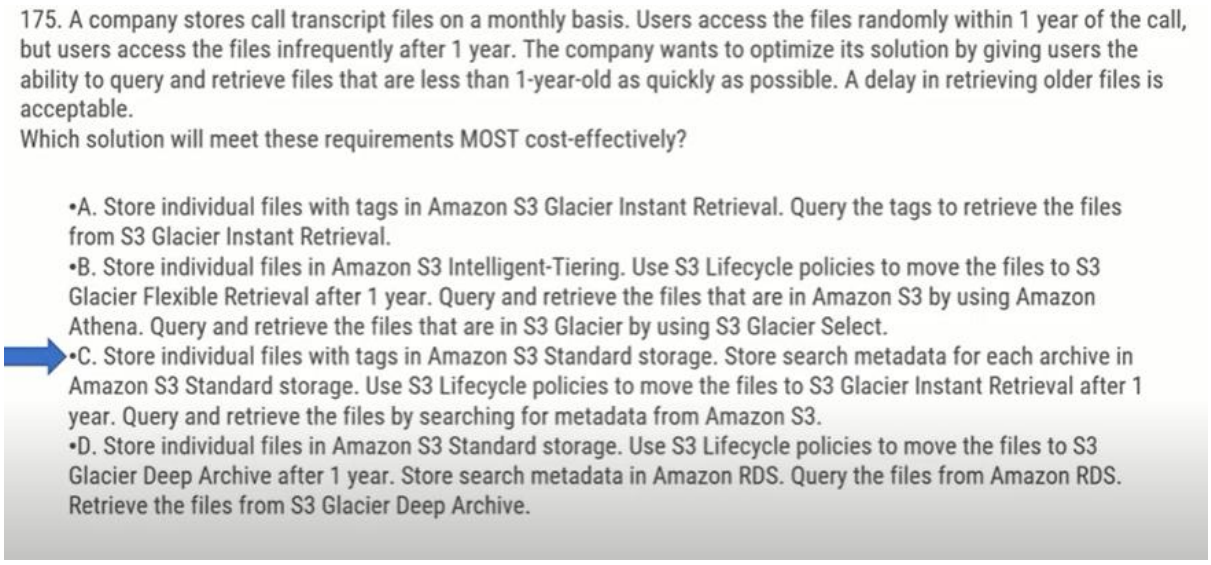
Option A is a highly available and cost-effective solution that requires minimal infrastructure management. Amazon Kinesis Data Firehose is a fully managed service that can ingest and deliver data to various destinations such as Amazon S3, Amazon Redshift, and Amazon Elasticsearch Service. In this solution, Kinesis Data Firehose is used to ingest the alerts and deliver them to an S3 bucket for storage. S3 provides a highly scalable and durable storage solution, and using an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days helps minimize costs.

Option B, launching EC2 instances to ingest the alerts and store them in an S3 bucket, is not as operationally efficient as option A because it requires managing and scaling the EC2 instances, which can be time-consuming and costly.

Option C, using Kinesis Data Firehose to ingest the alerts and deliver them to an Amazon Elasticsearch Service (Amazon ES) cluster, is not cost-effective because Amazon ES can be expensive, especially for ingesting large amounts of data. In addition, manually taking snapshots every day and deleting data older than 14 days can be time-consuming and increases operational overhead.

Option D, using Amazon SQS to ingest the alerts and copy them to an S3 bucket after 14 days, is not as operationally efficient as option A because it requires setting up consumers to poll the SQS queue, which can be complex and requires additional resources. Additionally, Amazon SQS may not be the best choice for ingesting large amounts of data.

Question 14: **Please confirm the correct option**



To meet the requirement of optimizing the solution for querying and retrieving call transcript files that are less than 1 year old as quickly as possible, while delaying the retrieval of older files, the most cost-effective solution is option B, storing individual files in Amazon S3 Intelligent-Tiering and using S3 Lifecycle policies to move the files to S3 Glacier Flexible Retrieval after 1 year.

Amazon S3 Intelligent-Tiering is designed to optimize costs by automatically moving data between two access tiers: frequent access and infrequent access, based on changing access patterns. In this solution, call transcript files can be stored in the frequent access tier, which is optimized for quick retrieval, for the first year. After one year, S3 lifecycle policies can be used to move the files to the infrequent access tier, S3 Glacier, which is optimized for long-term storage and retrieval.

To query and retrieve the files that are in S3, Amazon Athena can be used to analyze the data and retrieve specific files. For the files that are in S3 Glacier, S3 Glacier Select can be used to retrieve specific files from within a Glacier archive without having to retrieve the entire archive.

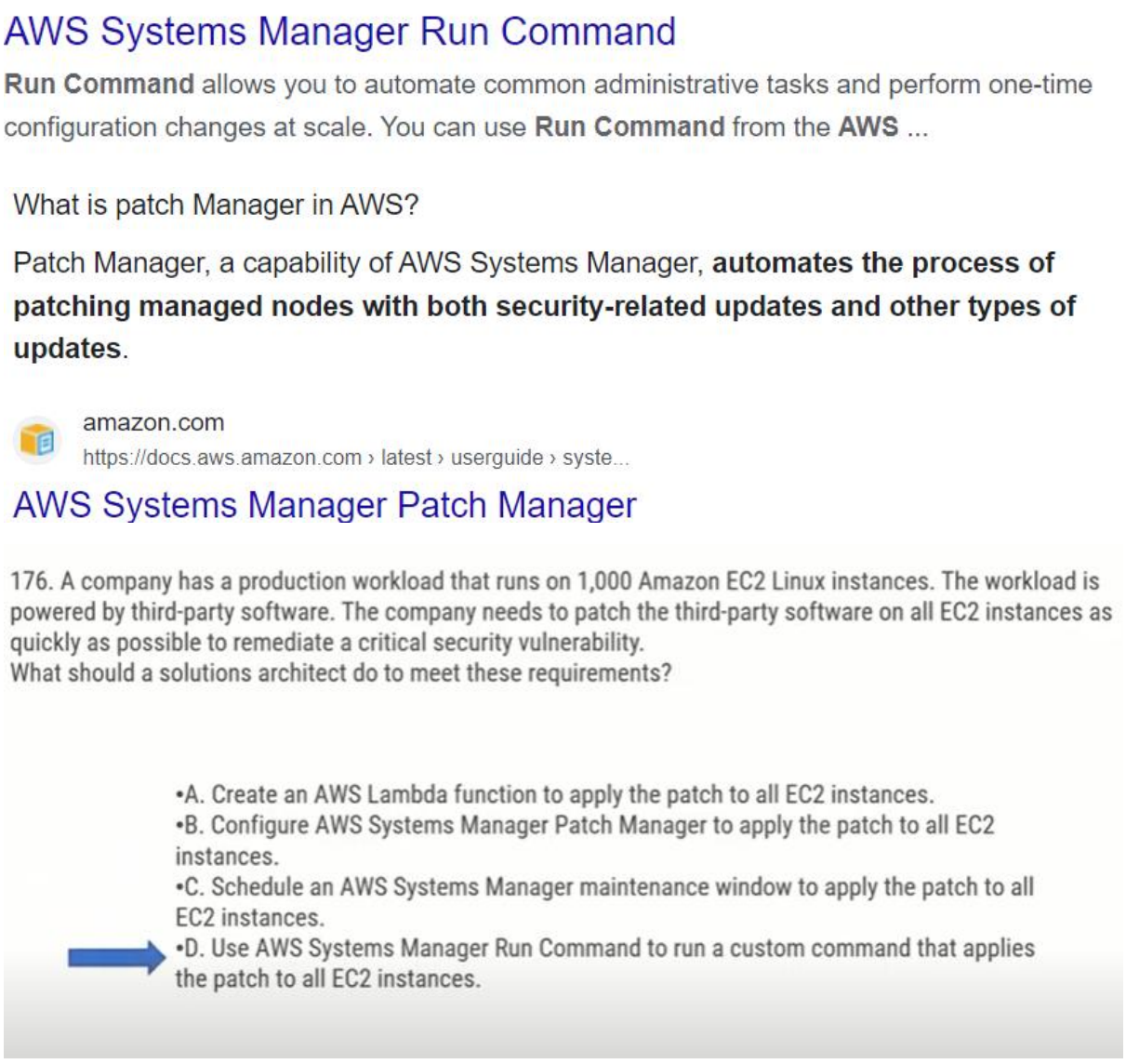
Option A, storing individual files with tags in Amazon S3 Glacier Instant Retrieval, is not the most cost-effective solution because Glacier Instant Retrieval is designed for fast, real-time access to individual files, and can be more expensive than other storage options.

Option C, storing individual files with tags in Amazon S3 Standard storage and storing search metadata for each archive in S3 Standard storage as well, and using S3 Lifecycle policies to move the files to S3 Glacier Instant Retrieval after 1 year, can be more expensive than the S3 Intelligent-Tiering solution in option B, and requires additional management of search metadata.

Option D, storing individual files in Amazon S3 Standard storage, using S3 Lifecycle policies to move the files to S3 Glacier Deep Archive after 1 year, and storing search metadata in Amazon RDS, is not the most cost-effective solution because Glacier Deep Archive is designed for long-term storage and

retrieval, and can be more expensive than other storage options. Additionally, storing search metadata in Amazon RDS can also increase costs.

Question 15: **Option B should be the correct answer as AWS System Manager Patch Manager is responsible for applying security related patches. Please confirm the correct option.**



To quickly patch the third-party software on all 1,000 Amazon EC2 Linux instances to remediate a critical security vulnerability, the most appropriate solution is option C, scheduling an AWS Systems Manager maintenance window to apply the patch to all EC2 instances.

AWS Systems Manager provides a range of tools and services for managing EC2 instances, including Patch Manager, Run Command, and maintenance windows. In this case, scheduling a maintenance window allows the patch to be applied to all instances within a specified time frame, ensuring that the patch is applied in a timely and consistent manner across all instances.

Option A, creating an AWS Lambda function to apply the patch to all EC2 instances, is not the most appropriate solution because it requires additional configuration and management of the Lambda function, which can be time-consuming.

Option B, configuring AWS Systems Manager Patch Manager to apply the patch to all EC2 instances, is a valid solution, but it may not be the most appropriate solution for quickly patching all 1,000 instances, as Patch Manager can take some time to apply patches to a large number of instances.

Option D, using AWS Systems Manager Run Command to run a custom command that applies the patch to all EC2 instances, is also a valid solution, but it may not be the most appropriate solution for quickly patching all 1,000 instances, as it can be time-consuming to configure the custom command and execute it on all instances.

Therefore, scheduling a maintenance window is the most appropriate and efficient solution for quickly patching all 1,000 Amazon EC2 Linux instances to remediate a critical security vulnerability.

Question 16: **Please confirm the correct option.**

Option A: should be the correct option

Option B: not a good option as VPN connection is available over internet and the question asks about highly available connection which is possible through Direct Connect

Option C: not a good option as provision another direct connect would incur costs

Option D: not sure about this option

192. A solutions architect is designing a new hybrid architecture to extend a company's on-premises infrastructure to AWS. The company requires a highly available connection with consistent low latency to an AWS Region. The company needs to minimize costs and is willing to accept slower traffic if the primary connection fails.
What should the solutions architect do to meet these requirements?

- A. Provision an AWS Direct Connect connection to a Region. Provision a VPN connection as a backup if the primary Direct Connect connection fails.
- B. Provision a VPN tunnel connection to a Region for private connectivity. Provision a second VPN tunnel for private connectivity and as a backup if the primary VPN connection fails.
- C. Provision an AWS Direct Connect connection to a Region. Provision a second Direct Connect connection to the same Region as a backup if the primary Direct Connect connection fails.
- D. Provision an AWS Direct Connect connection to a Region. Use the Direct Connect failover attribute from the AWS CLI to automatically create a backup connection if the primary Direct Connect connection fails.

To extend a company's on-premises infrastructure to AWS with a highly available connection with consistent low latency to an AWS Region, while minimizing costs and accepting slower traffic if the primary connection fails, the most appropriate solution is option A, provisioning an AWS Direct Connect connection to a Region and provisioning a VPN connection as a backup if the primary Direct Connect connection fails.

AWS Direct Connect is a dedicated network connection from on-premises to AWS that provides consistent low latency and high bandwidth. In this case, a Direct Connect connection can provide the primary connection to the AWS Region. If the primary Direct Connect connection fails, a VPN connection can be used as a backup connection to maintain connectivity. This solution is cost-effective and provides a high level of availability while still meeting the company's cost requirements.

Option B, provisioning two VPN tunnel connections for private connectivity, is not the most appropriate solution for a highly available and low-latency connection, as VPN connections can be prone to latency and reliability issues.

Option C, provisioning two Direct Connect connections to the same Region, is a valid solution but can be more expensive than using a VPN connection as a backup.

Option D, using the Direct Connect failover attribute from the AWS CLI to automatically create a backup connection if the primary Direct Connect connection fails, is a valid solution, but it may not be the most appropriate solution for minimizing costs, as it still requires provisioning a backup Direct Connect connection.

Question 17: **Please confirm the correct option**

199. A company wants to move a multi-tiered application from on premises to the AWS Cloud to improve the application's performance. The application consists of application tiers that communicate with each other by way of RESTful services. Transactions are dropped when one tier becomes overloaded. A solutions architect must design a solution that resolves these issues and modernizes the application.
Which solution meets these requirements and is the MOST operationally efficient?

- A. Use Amazon API Gateway and direct transactions to the AWS Lambda functions as the application layer. Use Amazon Simple Queue Service (Amazon SQS) as the communication layer between application services.
- B. Use Amazon CloudWatch metrics to analyze the application performance history to determine the servers' peak utilization during the performance failures. Increase the size of the application server's Amazon EC2 instances to meet the peak requirements.
- C. Use Amazon Simple Notification Service (Amazon SNS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SNS queue length and scale up and down as required.
- D. Use Amazon Simple Queue Service (Amazon SQS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SQS queue length and scale up when communication failures are detected.

To move a multi-tiered application from on-premises to the AWS Cloud, improve application performance, and modernize the application, the most operationally efficient solution that meets the requirements of resolving dropped transactions and modernizing the application is option A, using Amazon API Gateway and AWS Lambda for the application layer and Amazon Simple Queue Service (Amazon SQS) for the communication layer.

Amazon API Gateway is a fully managed service that allows developers to create, publish, and monitor APIs at any scale. AWS Lambda is a serverless compute service that runs code in response to events and automatically scales to meet demand. By using these services together, the application layer can be modernized and easily scaled to meet demand.

Using Amazon SQS as the communication layer between application services helps to decouple the application tiers and provides fault tolerance. When one tier becomes overloaded, messages can be queued in Amazon SQS until the tier is ready to process them. This helps to prevent dropped transactions and ensures that transactions are processed efficiently.

Option B, using Amazon CloudWatch metrics to analyze application performance history and increase the size of EC2 instances to meet peak requirements, is not as operationally efficient as option A because it requires manual intervention and may not be able to handle sudden spikes in traffic.

Option C, using Amazon SNS to handle messaging between application servers running on EC2 in an Auto Scaling group, may not be the most appropriate solution for handling RESTful services, which typically require a request-response model.

Option D, using Amazon SQS to handle messaging between application servers running on EC2 in an Auto Scaling group and scaling up when communication failures are detected, may not be the most efficient solution for handling RESTful services, which typically require a request-response model, and may not be able to handle sudden spikes in traffic.

Question 18: Since the question asks for supply the material rapidly regardless of origin of the request, should be AWS Global Accelerator (i.e Option B) Please confirm.

22) A significant media corporation uses AWS to host a web application. The corporation intends to begin caching secret media files in order to provide dependable access to them to consumers worldwide. Amazon S3 buckets are used to store the material. The organization must supply material rapidly, regardless of the origin of the requests.

Which solution will satisfy these criteria?

- A. Use AWS DataSync to connect the S3 buckets to the web application.
- B. Deploy AWS Global Accelerator to connect the S3 buckets to the web application.
- C. Deploy Amazon CloudFront to connect the S3 buckets to CloudFront edge servers.
- D. Use Amazon Simple Queue Service (Amazon SQS) to connect the S3 buckets to the web application.

To cache confidential media files and deliver them quickly to users around the world, regardless of where the requests originate, the most appropriate solution is option C, deploying Amazon CloudFront to connect the S3 buckets to CloudFront edge servers.

Amazon CloudFront is a content delivery network service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds. By deploying CloudFront and configuring it to use S3 as the origin, the media files can be cached at edge locations around the world, reducing latency and improving performance. CloudFront also provides security features such as HTTPS encryption and field-level encryption, which can be used to protect confidential media files.

Option A, using AWS DataSync to connect the S3 buckets to the web application, is not the most appropriate solution for caching and delivering media files, as DataSync is primarily used for transferring large amounts of data between on-premises storage and AWS storage services.

Option B, deploying AWS Global Accelerator to connect the S3 buckets to the web application, is not the most appropriate solution for caching and delivering media files, as Global Accelerator is designed to improve the availability and performance of applications running in one or more AWS Regions, not to cache and deliver media files.

Option D, using Amazon Simple Queue Service (Amazon SQS) to connect the S3 buckets to the web application, is not the most appropriate solution for caching and delivering media files, as SQS is a messaging queue service that is primarily used to decouple and scale microservices, not to cache and deliver media files.

Question 19: **Please advise the correct option**

31) A business has two virtual private clouds (VPCs) labeled Management and Production. The Management VPC connects to a single device in the data center using VPNs via a customer gateway. The Production VPC is connected to AWS through two AWS Direct Connect connections via a virtual private gateway. Both the Management and Production VPCs communicate with one another through a single VPC peering connection.

What should a solutions architect do to minimize the architecture's single point of failure?

- A. Add a set of VPNs between the Management and Production VPCs.
- B. Add a second virtual private gateway and attach it to the Management VPC.
- C. Add a second set of VPNs to the Management VPC from a second customer gateway device.
- D. Add a second VPC peering connection between the Management VPC and the Production VPC.

To mitigate any single point of failure in the architecture involving the Management and Production VPCs, the most appropriate solution is option D, adding a second VPC peering connection between the Management VPC and the Production VPC.

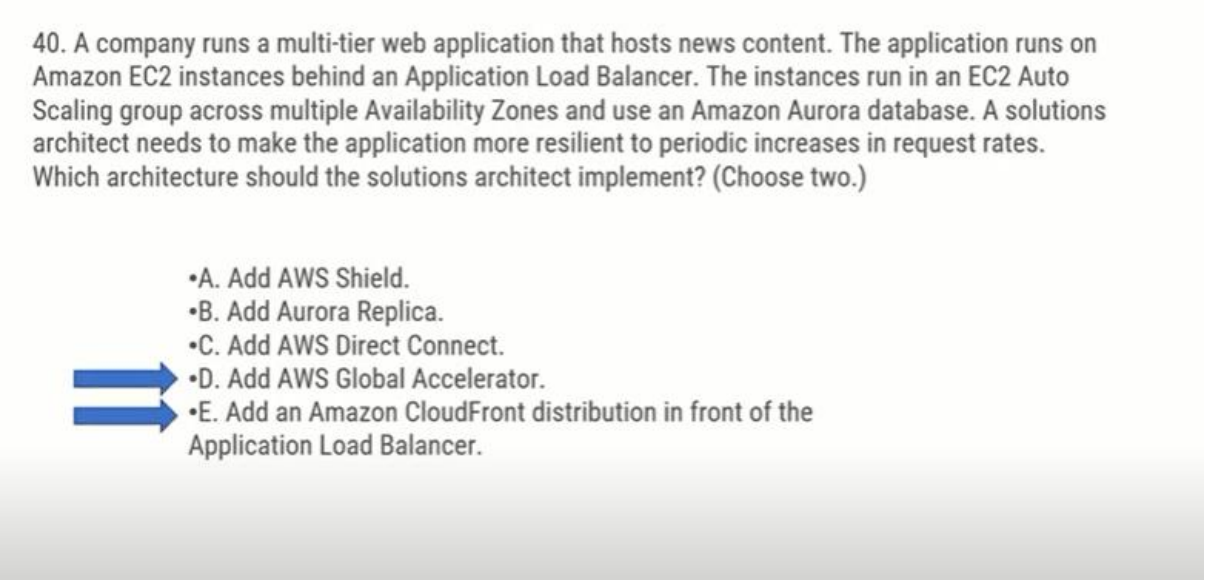
Currently, the Management and Production VPCs are connected through a single VPC peering connection, which can be a single point of failure. By adding a second VPC peering connection, the architecture is made more resilient to failure. This will also provide additional bandwidth and redundancy for communication between the applications in the two VPCs.

Option A, adding a set of VPNs between the Management and Production VPCs, is not the most appropriate solution because VPNs are already being used to connect the Management VPC to the data center, and adding more VPNs would add complexity to the architecture.

Option B, adding a second virtual private gateway and attaching it to the Management VPC, is not the most appropriate solution because it would not provide redundancy for the VPC peering connection between the Management and Production VPCs.

Option C, adding a second set of VPNs to the Management VPC from a second customer gateway device, is not the most appropriate solution because it would not provide redundancy for the VPC peering connection between the Management and Production VPCs, and would also add complexity to the architecture.

Question 20: **How can AWS Global Accelerator can make the application more resilient? I think instead of Option D should be B. Please confirm.**



To make the multi-tier web application more resilient to periodic increases in request rates, the solutions architect should implement the following two architectures:

B. Add an Aurora Replica: Adding an Aurora Replica will provide additional read capacity to the database and improve the application's overall performance. This will help the application to handle an increased number of requests and reduce the chances of a database becoming a bottleneck.

E. Add an Amazon CloudFront distribution in front of the Application Load Balancer: Adding a CloudFront distribution in front of the ALB will improve the application's performance and reduce the load on the ALB and EC2 instances. CloudFront will cache frequently accessed content and serve it from edge locations close to the users, reducing latency and improving the overall user experience. The ALB can then focus on handling the remaining requests that are not served by CloudFront, improving its resiliency.

AWS Shield (option A) protects applications against DDoS attacks and is useful for keeping applications available during an attack. However, it is not directly related to improving the application's resiliency to periodic increases in request rates.

AWS Direct Connect (option C) is a dedicated network connection from on-premises to AWS and does not directly improve the application's resiliency to periodic increases in request rates.

AWS Global Accelerator (option D) is designed to improve the availability and performance of applications running in one or more AWS Regions. While it can help distribute traffic across multiple endpoints, it is not directly related to improving the application's resiliency to periodic increases in request rates.

Question 21: **Please confirm the correct option**

79. A company runs an application in a branch office within a small data closet with no virtualized compute resources. The application data is stored on an NFS volume. Compliance standards require a daily offsite backup of the NFS volume.
Which solution meets these requirements?

- A. Install an AWS Storage Gateway file gateway on premises to replicate the data to Amazon S3.
- B. Install an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3.
- C. Install an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3.
- D. Install an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3.

To comply with the daily offsite backup requirement of the NFS volume in the branch office, the most appropriate solution is option A, installing an AWS Storage Gateway file gateway on premises to replicate the data to Amazon S3.

The AWS Storage Gateway file gateway is a virtual machine that runs in a branch office or data center as a hardware appliance or software appliance. It provides seamless integration between on-premises applications and AWS storage services, and supports industry-standard file and volume protocols.

By installing an AWS Storage Gateway file gateway on premises, the application data on the NFS volume can be backed up to Amazon S3 using the gateway's built-in backup functionality. This provides a secure and reliable way to store and manage backups offsite, while also complying with compliance standards.

Option B, installing an AWS Storage Gateway file gateway hardware appliance on premises, is not the most appropriate solution because it requires additional hardware and may not be cost-effective for a small data closet.

Option C, installing an AWS Storage Gateway volume gateway with stored volumes on premises, is not the most appropriate solution because it is designed for block storage rather than file storage, and may not be the most suitable option for backing up an NFS volume.

Option D, installing an AWS Storage Gateway volume gateway with cached volumes on premises, is not the most appropriate solution because it is designed for block storage rather than file storage, and may not be the most suitable option for backing up an NFS volume.

Question 22:

111. A company is managing health records on-premises. The company must keep these records indefinitely, disable any modifications to the records once they are stored, and granularly audit access at all levels. The chief technology officer (CTO) is concerned because there are already millions of records not being used by any application, and the current infrastructure is running out of space. The CTO has requested a solutions architect design a solution to move existing data and support future records. Which services can the solutions architect recommend to meet these requirements?

- A. Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with data events.
- B. Use AWS Storage Gateway to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events.
- C. Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events.
- D. Use AWS Storage Gateway to move existing data to AWS. Use Amazon Elastic Block Store (Amazon EBS) to store existing and new data. Enable Amazon S3 object lock and enable Amazon S3 server access logging.

To meet the requirements of storing health records indefinitely, disabling modifications to the records once they are stored, granularly auditing access at all levels, and moving existing data while also supporting future records, the most appropriate solution is option C, using AWS DataSync to move existing data to AWS, using Amazon S3 to store existing and new data, enabling Amazon S3 object lock, and enabling AWS CloudTrail with management events.

AWS DataSync is a fully managed service that makes it simple and fast to move large amounts of data online between on-premises storage and Amazon S3, Amazon Elastic File System (Amazon EFS), or Amazon FSx for Windows File Server. By using DataSync, the company can efficiently move existing data to AWS.

Amazon S3 is a highly scalable and durable object storage service that is ideal for storing health records. By enabling Amazon S3 object lock, the company can ensure that the records are tamper-proof and cannot be modified once stored. This is important for maintaining the integrity and security of the records.

Enabling AWS CloudTrail with management events can be used to monitor and audit access to Amazon S3 buckets and objects. This enables granular auditing of access at all levels, ensuring that the company can comply with any regulatory or compliance requirements.

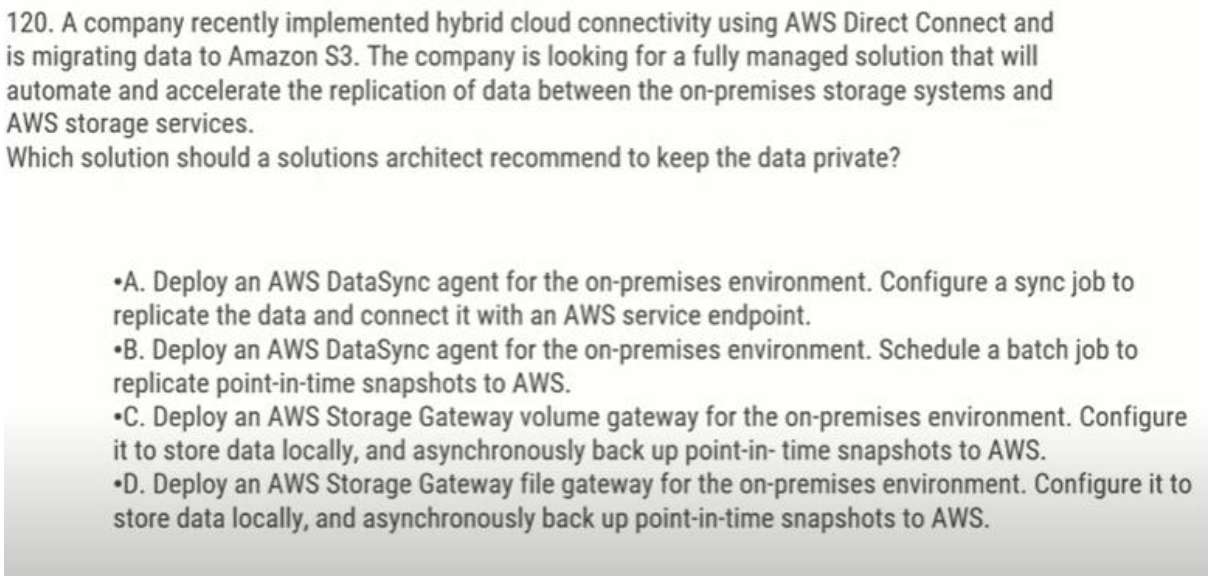
Option A, using AWS DataSync to move existing data to AWS, using Amazon S3 to store existing and new data, enabling Amazon S3 object lock, and enabling AWS CloudTrail with data events, is not the most appropriate solution because data events in AWS CloudTrail do not provide detailed information about management-level activity, such as changes to bucket policies or object-level permissions.

Option B, using AWS Storage Gateway to move existing data to AWS, using Amazon S3 to store existing and new data, enabling Amazon S3 object lock, and enabling AWS CloudTrail with management events, is not the most appropriate solution because AWS Storage Gateway is designed for hybrid cloud use cases and may not be the most efficient way to move large amounts of data to AWS.

Option D, using AWS Storage Gateway to move existing data to AWS, using Amazon Elastic Block Store (Amazon EBS) to store existing and new data, enabling Amazon S3 object lock, and enabling Amazon S3 server access logging, is not the most appropriate solution because Amazon EBS is

designed for block storage rather than object storage, and may not be the most suitable option for storing health records.

Question 23:


120. A company recently implemented hybrid cloud connectivity using AWS Direct Connect and is migrating data to Amazon S3. The company is looking for a fully managed solution that will automate and accelerate the replication of data between the on-premises storage systems and AWS storage services.
Which solution should a solutions architect recommend to keep the data private?

•A. Deploy an AWS DataSync agent for the on-premises environment. Configure a sync job to replicate the data and connect it with an AWS service endpoint.
•B. Deploy an AWS DataSync agent for the on-premises environment. Schedule a batch job to replicate point-in-time snapshots to AWS.
•C. Deploy an AWS Storage Gateway volume gateway for the on-premises environment. Configure it to store data locally, and asynchronously back up point-in- time snapshots to AWS.
•D. Deploy an AWS Storage Gateway file gateway for the on-premises environment. Configure it to store data locally, and asynchronously back up point-in-time snapshots to AWS.

To keep the data private while automating and accelerating the replication of data between the on-premises storage systems and AWS storage services, the most appropriate solution is option A, deploying an AWS DataSync agent for the on-premises environment, configuring a sync job to replicate the data, and connecting it with an AWS service endpoint.

AWS DataSync is a fully managed data transfer service that makes it easy to automate and accelerate moving data between on-premises storage systems and AWS storage services. DataSync uses a simple web interface or API to configure, launch, and monitor data transfer workflows. By connecting to an AWS service endpoint, DataSync can help keep the data private and secure during transfer.

Option B, scheduling a batch job to replicate point-in-time snapshots to AWS, is not the most appropriate solution because it is not fully automated and may be subject to delays and errors.

Option C, deploying an AWS Storage Gateway volume gateway for the on-premises environment, and configuring it to store data locally and asynchronously back up point-in-time snapshots to AWS, is not the most appropriate solution because it is designed for block storage rather than object storage, which is used by Amazon S3.

Option D, deploying an AWS Storage Gateway file gateway for the on-premises environment, and configuring it to store data locally and asynchronously back up point-in-time snapshots to AWS, is not the most appropriate solution because it may not be the most efficient way to transfer large amounts of data to Amazon S3, and it is not designed to be fully automated.

Question 24:

We can use AWS Datasync for data transfer between on-premise and AWS but as there is 20TB data that needs to be transferred, SNOWBALL (Option A) is a good option here. Is this correct?

Also, how much data can we transfer using AWS Datasync? Is there any limit to it?

134. A company must migrate 20 TB of data from a data center to the AWS Cloud within 30 days. The company's network bandwidth is limited to 15 Mbps and cannot exceed 70% utilization. What should a solutions architect do to meet these requirements?

- A. Use AWS Snowball.
- B. Use AWS DataSync.
- C. Use a secure VPN connection.
- D. Use Amazon S3 Transfer Acceleration.

To migrate 20 TB of data from a data center to the AWS Cloud within 30 days, given a limited network bandwidth of 15 Mbps and a 70% utilization cap, the most appropriate solution is option A, using AWS Snowball.

AWS Snowball is a petabyte-scale data transport solution that uses secure appliances to transfer large amounts of data into and out of AWS. By using Snowball, the company can avoid the limitations of its network bandwidth and ensure fast, secure, and reliable data transfer.

With Snowball, the company can request a physical device that will be shipped to the data center, and then copy the data onto the device. The device is then shipped back to AWS and the data is imported into an Amazon S3 bucket. This approach is faster and more efficient than transferring the data over the network, especially when the network bandwidth is limited.

Option B, using AWS DataSync, may not be the most appropriate solution because it relies on network connectivity and may be impacted by the limited network bandwidth and utilization cap.

Option C, using a secure VPN connection, may not be the most appropriate solution because it relies on the limited network bandwidth and may not be able to transfer the data within the required timeframe.

Option D, using Amazon S3 Transfer Acceleration, may not be the most appropriate solution because it is designed to improve data transfer over the public internet, rather than a limited network bandwidth with a utilization cap.

Question 25:

137. A company has an on-premises data center that is running out of storage capacity. The company wants to migrate its storage infrastructure to AWS while minimizing bandwidth costs. The solution must allow for immediate retrieval of data at no additional cost.
How can these requirements be met?

•A. Deploy Amazon S3 Glacier Vault and enable expedited retrieval. Enable provisioned retrieval capacity for the workload.
•B. Deploy AWS Storage Gateway using cached volumes. Use Storage Gateway to store data in Amazon S3 while retaining copies of frequently accessed data subsets locally.
•C. Deploy AWS Storage Gateway using stored volumes to store data locally. Use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3.
•D. Deploy AWS Direct Connect to connect with the on-premises data center. Configure AWS Storage Gateway to store data locally. Use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3.

To migrate the storage infrastructure to AWS while minimizing bandwidth costs, and allow for immediate retrieval of data at no additional cost, the most appropriate solution is option B, deploying AWS Storage Gateway using cached volumes, and using it to store data in Amazon S3 while retaining copies of frequently accessed data subsets locally.

AWS Storage Gateway is a hybrid cloud storage service that enables on-premises applications to use AWS cloud storage. By deploying Storage Gateway using cached volumes, the company can store frequently accessed data subsets locally and store the rest of the data in Amazon S3. This will minimize bandwidth costs by reducing the amount of data that needs to be transferred to and from the data center.

By using Storage Gateway, the company can also enable immediate retrieval of data at no additional cost. This is because frequently accessed data subsets are stored locally, and can be accessed quickly by on-premises applications. When data is not found in the local cache, it is retrieved from Amazon S3.

Option A, deploying Amazon S3 Glacier Vault and enabling expedited retrieval, may not be the most appropriate solution because it is designed for long-term archival storage and may not provide immediate retrieval of data, especially for frequently accessed data subsets. Additionally, the provisioned retrieval capacity may add additional costs.

Option C, deploying AWS Storage Gateway using stored volumes to store data locally, and using it to asynchronously back up point-in-time snapshots of the data to Amazon S3, may not be the most appropriate solution because it is designed for block storage rather than object storage, which is used by Amazon S3.

Option D, deploying AWS Direct Connect to connect with the on-premises data center, configuring AWS Storage Gateway to store data locally, and using it to asynchronously back up point-in-time snapshots of the data to Amazon S3, may not be the most appropriate solution because it may not minimize bandwidth costs, especially for frequently accessed data subsets.

Question 26:

Why can’t we setup a peering connection between 2 VPCs?

145. An application running on an Amazon EC2 instance in VPC-A needs to access files in another EC2 instance in VPC-B. Both are in separate AWS accounts. The network administrator needs to design a solution to configure secure access to EC2 instance in VPC-B from VPC-A. The connectivity should not have a single point of failure or bandwidth concerns.
Which solution will meet these requirements?

- A. Set up a VPC peering connection between VPC-A and VPC-B.
- B. Set up VPC gateway endpoints for the EC2 instance running in VPC-B.
- C. Attach a virtual private gateway to VPC-B and set up routing from VPC-A.
- D. Create a private virtual interface (VIF) for the EC2 instance running in VPC-B and add appropriate routes from VPC-A.

To enable secure access to the EC2 instance in VPC-B from VPC-A, across AWS accounts, without a single point of failure or bandwidth concerns, the most appropriate solution is option D, creating a private virtual interface (VIF) for the EC2 instance running in VPC-B and adding appropriate routes from VPC-B.

A private VIF provides dedicated, private connectivity from an on-premises data center, office, or colocation environment to Amazon VPC. By creating a private VIF for the EC2 instance running in VPC-B, and adding appropriate routes from VPC-B to the VIF, the EC2 instance in VPC-A will be able to access the files in the EC2 instance in VPC-B securely and efficiently.

Option A, setting up a VPC peering connection between VPC-A and VPC-B, is not the most appropriate solution because it is used to connect VPCs within the same AWS account, and does not work across AWS accounts.

Option B, setting up VPC gateway endpoints for the EC2 instance running in VPC-B, is not the most appropriate solution because it is used to connect to AWS services over a private connection, and does not work for EC2 instances running in another VPC.

Option C, attaching a virtual private gateway to VPC-B and enabling routing from VPC-A, is not the most appropriate solution because it is used to connect to an on-premises data center, office, or colocation environment, and does not work across AWS accounts.

Question:

156. A company is using Amazon EC2 to run its big data analytics workloads. These variable workloads run each night, and it is critical they finish by the start of business the following day. A solutions architect has been tasked with designing the MOST cost-effective solution.
Which solution will accomplish this?

- A. Spot Fleet
- B. Spot Instances
- C. Reserved Instances
- D. On-Demand Instances

To design the most cost-effective solution for running big data analytics workloads that need to finish by the start of business the following day, and are run only at night, the most appropriate solution is option B, using Spot Instances.

Amazon EC2 Spot Instances provide spare Amazon EC2 computing capacity at a discounted price compared to On-Demand instances. Spot Instances allow you to request unused EC2 instances, and you pay the Spot price for the instances. The Spot price fluctuates based on supply and demand and is often much lower than the On-Demand price.

By using Spot Instances, the company can take advantage of the discounted pricing to run the big data analytics workloads at a lower cost. Additionally, since the workloads are running only at night, the company can use Spot Instances at a higher risk level, which can provide even greater cost savings.

Option A, using Spot Fleet, is not the most appropriate solution because it is used to launch a single request that includes multiple Spot Instance types and across multiple Availability Zones.

Option C, using Reserved Instances, is not the most appropriate solution because Reserved Instances require a long-term commitment for a fixed amount of usage and may not be the most cost-effective solution for variable workloads.

Option D, using On-Demand Instances, is not the most cost-effective solution because On-Demand Instances have the highest hourly rates compared to other EC2 pricing options.

Question:

173. A company wants to migrate a workload to AWS. The chief information security officer requires that all data be encrypted at rest when stored in the cloud. The company wants complete control of encryption key lifecycle management.
The company must be able to immediately remove the key material and audit key usage independently of AWS CloudTrail. The chosen services should integrate with other storage services that will be used on AWS.
Which services satisfies these security requirements?

- A. AWS CloudHSM with the CloudHSM client
- B. AWS Key Management Service (AWS KMS) with AWS CloudHSM
- C. AWS Key Management Service (AWS KMS) with an external key material origin
- D. AWS Key Management Service (AWS KMS) with AWS managed customer master keys (CMKs)

To meet the security requirements of encrypting all data at rest when stored in the cloud, having complete control of encryption key lifecycle management, being able to immediately remove the key material, auditing key usage independently of AWS CloudTrail, and integrating with other storage services on AWS, the most appropriate solution is option C, using AWS Key Management Service (AWS KMS) with an external key material origin.

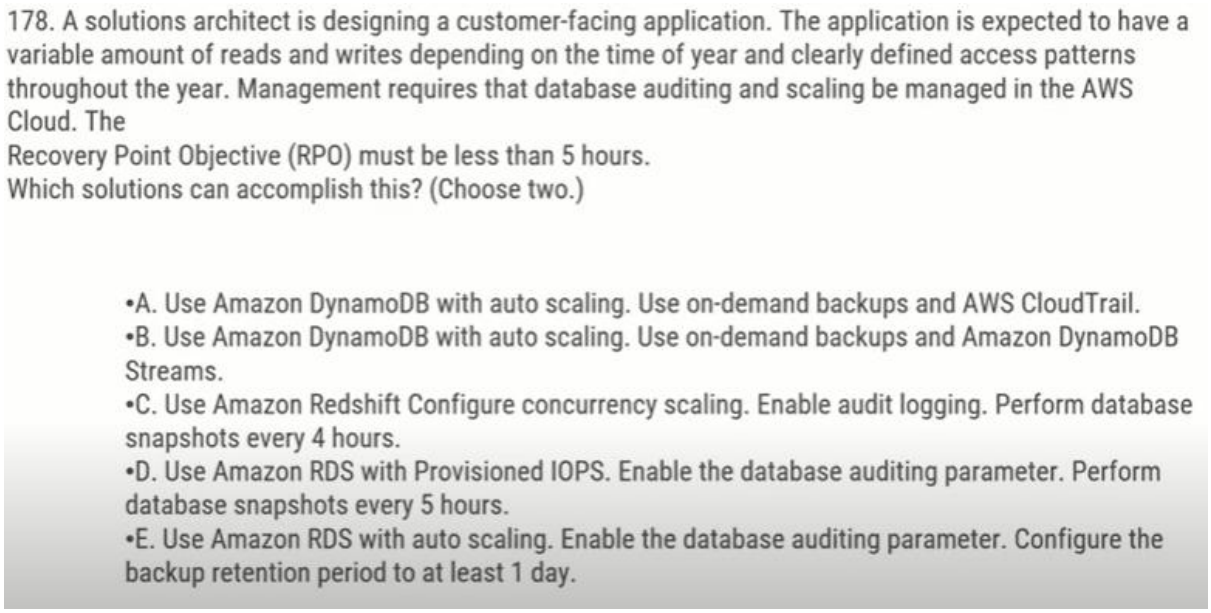
AWS KMS is a fully managed service that makes it easy to create and control the encryption keys used to encrypt data. By using an external key material origin, the company can have complete control over the key lifecycle management, including generating, storing, and managing keys on-premises, and importing them into AWS KMS. This provides the company with greater control over the encryption keys and enables them to meet their security requirements.

Option A, using AWS CloudHSM with the CloudHSM client, may not be the most appropriate solution because it may be more complex to manage and may not integrate as easily with other AWS storage services.

Option B, using AWS Key Management Service (AWS KMS) with AWS CloudHSM, may not be the most appropriate solution because it may add additional complexity and cost to the solution, and may not be necessary to meet the security requirements.

Option D, using AWS Key Management Service (AWS KMS) with AWS managed customer master keys (CMKs), may not be the most appropriate solution because it does not provide complete control over the key lifecycle and may not meet the requirement to audit key usage independently of AWS CloudTrail.

Question:


178. A solutions architect is designing a customer-facing application. The application is expected to have a variable amount of reads and writes depending on the time of year and clearly defined access patterns throughout the year. Management requires that database auditing and scaling be managed in the AWS Cloud. The
Recovery Point Objective (RPO) must be less than 5 hours.
Which solutions can accomplish this? (Choose two.)

•A. Use Amazon DynamoDB with auto scaling. Use on-demand backups and AWS CloudTrail.
•B. Use Amazon DynamoDB with auto scaling. Use on-demand backups and Amazon DynamoDB Streams.
•C. Use Amazon Redshift Configure concurrency scaling. Enable audit logging. Perform database snapshots every 4 hours.
•D. Use Amazon RDS with Provisioned IOPS. Enable the database auditing parameter. Perform database snapshots every 5 hours.
•E. Use Amazon RDS with auto scaling. Enable the database auditing parameter. Configure the backup retention period to at least 1 day.

To design a customer-facing application with variable reads and writes, clearly defined access patterns, database auditing, and scaling managed in the AWS Cloud, with a Recovery Point Objective (RPO) of less than 5 hours, the most appropriate solutions are options A and B:

A. Use Amazon DynamoDB with auto scaling. Use on-demand backups and AWS CloudTrail.

B. Use Amazon DynamoDB with auto scaling. Use on-demand backups and Amazon DynamoDB Streams.

Amazon DynamoDB is a fully managed NoSQL database service that can support variable and clearly defined access patterns, with the ability to scale both up and down to meet changing workloads.

Option A is appropriate, using on-demand backups and AWS CloudTrail to manage auditing, as well as auto scaling to automatically adjust capacity in response to changes in application traffic. This solution provides the necessary RPO of less than 5 hours.

Option B is also appropriate, using on-demand backups and Amazon DynamoDB Streams to manage auditing, as well as auto scaling to automatically adjust capacity in response to changes in application traffic. Amazon DynamoDB Streams provides a time-ordered sequence of item-level modifications, which can be used to replicate data across multiple DynamoDB tables in near real-time.

Option C, using Amazon Redshift with concurrency scaling and enabling audit logging, and performing database snapshots every 4 hours, may not be the most appropriate solution because Redshift is a data warehousing solution that is optimized for OLAP queries, and not OLTP workloads.

Option D, using Amazon RDS with Provisioned IOPS, enabling the database auditing parameter, and performing database snapshots every 5 hours, may not be the most appropriate solution because it may not provide the necessary scalability and flexibility for variable and clearly defined access patterns.

Option E, using Amazon RDS with auto scaling, enabling the database auditing parameter, and configuring the backup retention period to at least 1 day, may not be the most appropriate solution because it may not provide the necessary RPO of less than 5 hours.

Question:

Option A is not correct as there is no way to directly transfer data from Storage gateway to S3 Glacier

Option C: looks to be the correct one.

194. A company is using a tape backup solution to store its key application data offsite. The daily data volume is around 50 TB. The company needs to retain the backups for 7 years for regulatory purposes. The backups are rarely accessed, and a week's notice is typically given if a backup needs to be restored.
The company is now considering a cloud-based option to reduce the storage costs and operational burden of managing tapes. The company also wants to make sure that the transition from tape backups to the cloud minimizes disruptions.
Which storage solution is MOST cost-effective?

- A. Use Amazon Storage Gateway to back up to Amazon Glacier Deep Archive.
- B. Use AWS Snowball Edge to directly integrate the backups with Amazon S3 Glacier.
- C. Copy the backup data to Amazon S3 and create a lifecycle policy to move the data to Amazon S3 Glacier.
- D. Use Amazon Storage Gateway to back up to Amazon S3 and create a lifecycle policy to move the backup to Amazon S3 Glacier.

Question: should be option D. please confirm

201. A company runs a web service on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across two Availability Zones. The company needs a minimum of four instances at all times to meet the required service level agreement (SLA) while keeping costs low.
If an Availability Zone fails, how can the company remain compliant with the SLA?

- A. Add a target tracking scaling policy with a short cooldown period.
- B. Change the Auto Scaling group launch configuration to use a larger instance type.
- C. Change the Auto Scaling group to use six servers across three Availability Zones.
- D. Change the Auto Scaling group to use eight servers across two Availability Zones.

To reduce storage costs and operational burden of managing tapes, and minimize disruptions during the transition from tape backups to the cloud, while retaining the backups for 7 years for regulatory purposes, the most cost-effective solution is option C, copying the backup data to Amazon S3 and creating a lifecycle policy to move the data to Amazon S3 Glacier.

Amazon S3 is a highly durable and scalable object storage service that provides a cost-effective solution for storing backup data. By copying the backup data to Amazon S3, the company can take advantage of the durability and scalability of the service, while also reducing storage costs. The company can then create a lifecycle policy to automatically move the data to Amazon S3 Glacier, which provides a low-cost, long-term storage option for rarely accessed data.

Option A, using Amazon Storage Gateway to back up to Amazon Glacier Deep Archive, may not be the most cost-effective solution because Deep Archive is designed for data that is accessed once or twice a year and requires a 12-hour retrieval time.

Option B, using AWS Snowball Edge to directly integrate the backups with Amazon S3 Glacier, may not be the most cost-effective solution because it requires additional hardware to be shipped to the data center, and may add additional complexity to the solution.

Option D, using Amazon Storage Gateway to back up to Amazon S3 and creating a lifecycle policy to move the backup to Amazon S3 Glacier, may not be the most cost-effective solution because it adds an additional layer of storage (S3) that may not be necessary, and could increase storage costs.

Question:

203. A company is designing a web application using AWS that processes insurance quotes. Users will request quotes from the application. Quotes must be separated by quote type must be responded to within 24 hours, and must not be lost. The solution should be simple to set up and maintain.
Which solution meets these requirements?

•A. Create multiple Amazon Kinesis data streams based on the quote type. Configure the web application to send messages to the proper data stream. Configure each backend group of application servers to pool messages from its own data stream using the Kinesis Client Library (KCL).
•B. Create multiple Amazon Simple Notification Service (Amazon SNS) topics and register Amazon SQS queues to their own SNS topic based on the quote type. Configure the web application to publish messages to the SNS topic queue. Configure each backend application server to work its own SQS queue.
•C. Create a single Amazon Simple Notification Service (Amazon SNS) topic and subscribe the Amazon SQS queues to the SNS topic. Configure SNS message filtering to publish messages to the proper SQS queue based on the quote type. Configure each backend application server to work its own SQS queue.
•D. Create multiple Amazon Kinesis Data Firehose delivery streams based on the quote type to deliver data streams to an Amazon Elasticsearch Service (Amazon ES) cluster. Configure the web application to send messages to the proper delivery stream. Configure each backend group of application servers to search for the messages from Amazon ES and process them accordingly.

To process insurance quotes from a web application and separate quotes by quote type, and respond to them within 24 hours without losing any quotes, the most appropriate solution is option B, creating multiple Amazon Simple Notification Service (Amazon SNS) topics and registering Amazon SQS queues to their own SNS topic based on the quote type, and configuring each backend application server to work its own SQS queue.

Amazon SNS is a fully managed pub/sub messaging service that enables you to send messages to multiple subscribers or endpoints. By creating multiple SNS topics and registering Amazon SQS queues to their own SNS topic based on the quote type, the web application can publish messages to the appropriate SNS topic queue, and each backend application server can work its own SQS queue to process the messages.

This solution is simple to set up and maintain and ensures that quotes are not lost, while also enabling the application to respond to quotes within the required 24 hours.

Option A, creating multiple Amazon Kinesis data streams, may not be the most appropriate solution because it may add additional complexity to the solution, and may not be necessary for the requirements stated.

Option C, creating a single Amazon SNS topic and subscribing Amazon SQS queues to the SNS topic, configured with SNS message filtering to publish messages to the proper SQS queue based on the quote type, may not be the most appropriate solution because it may increase the complexity of the solution with message filtering.

Option D, creating multiple Amazon Kinesis Data Firehose delivery streams based on the quote type to deliver data streams to an Amazon Elasticsearch Service (Amazon ES) cluster, may not be the most appropriate solution because it may add additional complexity to the solution, and may not be necessary for the requirements stated.

Question: **C & E should be the correct options.. Please confirm**

212. A company is hosting multiple websites for several lines of business under its registered parent domain. Users accessing these websites will be routed to appropriate backend Amazon EC2 instances based on the subdomain. The websites host static webpages, images, and server-side scripts like PHP and JavaScript.
Some of the websites experience peak access during the first two hours of business with constant usage throughout the rest of the day. A solutions architect needs to design a solution that will automatically adjust capacity to these traffic patterns while keeping costs low.
Which combination of AWS services or features will meet these requirements? (Choose two.)

To automatically adjust capacity to traffic patterns while keeping costs low for hosting multiple websites under a registered parent domain, the most appropriate solutions are options C and D:

C. Application Load Balancer

D. Amazon EC2 Auto Scaling

An Application Load Balancer can route traffic based on the subdomain to the appropriate backend EC2 instances hosting the websites. Amazon EC2 Auto Scaling can be used to automatically adjust the capacity of the backend instances based on traffic patterns. By doing so, the company can ensure that the websites are responsive during peak access hours while keeping the costs low during less busy times.

Option A, AWS Batch, is not the most appropriate solution because it is used for batch computing workloads, and may not be necessary for hosting websites.

Option B, Network Load Balancer, may not be the most appropriate solution because it is designed for high performance, low latency traffic and may not be necessary for hosting websites.

Option E, Amazon S3 website hosting, may not be the most appropriate solution because it is designed for hosting static websites, and may not be suitable for hosting dynamic websites with server-side scripts like PHP and JavaScript.

Question: **EC2 metadata tells abt hostname, security group etc.. doesn't tell about swap space data. So Option B seems to be not the correct one. It looks like D is correct one. Please confirm.**

228. A company operates a website on Amazon EC2 Linux instances. Some of the instances are failing. Troubleshooting points to insufficient swap space on the failed instances. The operations team lead needs a solution to monitor this.
What should a solutions architect recommend?

•A. Configure an Amazon CloudWatch SwapUsage metric dimension. Monitor the SwapUsage dimension in the EC2 metrics in CloudWatch.
→ •B. Use EC2 metadata to collect information, then publish it to Amazon CloudWatch custom metrics. Monitor SwapUsage metrics in CloudWatch.
•C. Install an Amazon CloudWatch agent on the instances. Run an appropriate script on a set schedule. Monitor SwapUtilization metrics in CloudWatch.
•D. Enable detailed monitoring in the EC2 console. Create an Amazon CloudWatch SwapUtilization custom metric. Monitor SwapUtilization metrics in CloudWatch.

To monitor the swap space usage on Amazon EC2 Linux instances and troubleshoot instances that fail due to insufficient swap space, the most appropriate solution is option C, installing an Amazon CloudWatch agent on the instances and running an appropriate script on a set schedule to monitor SwapUtilization metrics in CloudWatch.

The Amazon CloudWatch agent can be installed on the instances to collect system-level metrics and logs, including SwapUtilization, which can be used to monitor swap space usage. The agent can run an appropriate script on a set schedule to monitor and report on the swap space usage, which can be viewed in CloudWatch.

Option A, configuring an Amazon CloudWatch SwapUsage metric dimension, may not be the most appropriate solution because it is not a default metric dimension and may require additional configuration.

Option B, using EC2 metadata to collect information and publish it to Amazon CloudWatch custom metrics, may not be the most appropriate solution because it may require additional scripting and may not provide the necessary level of detail.

Option D, enabling detailed monitoring in the EC2 console and creating an Amazon CloudWatch SwapUtilization custom metric, may not be the most appropriate solution because it may not provide the necessary level of detail and may require additional configuration.

Question: correct option should be A rather than B . please confirm.

242. A solutions architect is designing the storage architecture for a new web application used for storing and viewing engineering drawings. All application components will be deployed on the AWS infrastructure. The application design must support caching to minimize the amount of time that users wait for the engineering drawings to load. The application must be able to store petabytes of data. Which combination of storage and caching should the solutions architect use?

- A. Amazon S3 with Amazon CloudFront
- B. Amazon S3 Glacier with Amazon ElastiCache
- C. Amazon Elastic Block Store (Amazon EBS) volumes with Amazon CloudFront
- D. AWS Storage Gateway with Amazon ElastiCache

To support caching and minimize the amount of time that users wait for engineering drawings to load, while also being able to store petabytes of data, the most appropriate solution is option A, using Amazon S3 with Amazon CloudFront.

Amazon S3 is a highly scalable and durable object storage service that can store petabytes of data. Amazon CloudFront is a content delivery network (CDN) that can cache the engineering drawings and reduce the latency of accessing the files from anywhere in the world. By using Amazon S3 with Amazon CloudFront, the application can scale to meet the storage requirements and provide fast access to the engineering drawings.

Option B, using Amazon S3 Glacier with Amazon ElastiCache, may not be the most appropriate solution because Amazon S3 Glacier is an archival storage service that is designed for long-term storage and retrieval of data, and may not be suitable for frequently accessed data. Amazon ElastiCache is an in-memory data store that can improve application performance, but may not be necessary for caching static files like engineering drawings.

Option C, using Amazon Elastic Block Store (Amazon EBS) volumes with Amazon CloudFront, may not be the most appropriate solution because Amazon EBS volumes are block storage devices that are designed for storing data that is accessed frequently by a single EC2 instance, and may not be suitable for storing petabytes of data.

Option D, using AWS Storage Gateway with Amazon ElastiCache, may not be the most appropriate solution because AWS Storage Gateway is a hybrid storage service that enables on-premises applications to use AWS storage services, and may not be necessary for a web application that is deployed entirely on AWS infrastructure.

Question:

255. A company with facilities in North America, Europe, and Asia is designing new distributed application to optimize its global supply chain and manufacturing process. The orders booked on one continent should be visible to all Regions in a second or less. The database should be able to support failover with a short
Recovery Time Objective (RTO). The uptime of the application is important to ensure that manufacturing is not impacted.
What should a solutions architect recommend?

- A. Use Amazon DynamoDB global tables.
- B. Use Amazon Aurora Global Database.
- C. Use Amazon RDS for MySQL with a cross-Region read replica.
- D. Use Amazon RDS for PostgreSQL with a cross-Region read replica.

To optimize the global supply chain and manufacturing process, and ensure that orders booked on one continent are visible to all regions in a second or less, while also supporting failover with a short Recovery Time Objective (RTO), the most appropriate solution is option B, using Amazon Aurora Global Database.

Amazon Aurora Global Database is a MySQL and PostgreSQL-compatible relational database service that allows you to create a single database that spans multiple AWS regions. This enables you to provide low-latency access to the database from any region, ensuring that orders booked on one continent are visible to all regions in a second or less. It also provides automatic failover with a short RTO, ensuring that the uptime of the application is maintained.

Option A, using Amazon DynamoDB global tables, may not be the most appropriate solution because DynamoDB is a NoSQL database service that may not be suitable for relational data and may require additional application development effort.

Option C, using Amazon RDS for MySQL with a cross-Region read replica, may not be the most appropriate solution because it may not provide the necessary low-latency access to the database from any region.

Option D, using Amazon RDS for PostgreSQL with a cross-Region read replica, may not be the most appropriate solution because it may not provide the necessary low-latency access to the database from any region.

Question:

267. A company uses Application Load Balancers (ALBs) in different AWS Regions. The ALBs receive inconsistent traffic that can spike and drop throughout the year.
The company's networking team needs to allow the IP addresses of the ALBs in the on-premises firewall to enable connectivity.
Which solution is the MOST scalable with minimal configuration changes?

•A. Write an AWS Lambda script to get the IP addresses of the ALBs in different Regions. Update the on-premises firewall's rule to allow the IP addresses of the ALBs.
•B. Migrate all ALBs in different Regions to the Network Load Balancer (NLBs). Update the on-premises firewall's rule to allow the Elastic IP addresses of all the NLBs.
•C. Launch AWS Global Accelerator. Register the ALBs in different Regions to the accelerator. Update the on-premises firewall's rule to allow static IP addresses associated with the accelerator.
•D. Launch a Network Load Balancer (NLB) in one Region. Register the private IP addresses of the ALBs in different Regions with the NLB. Update the on- premises firewall's rule to allow the Elastic IP address attached to the NLB.

To allow the IP addresses of Application Load Balancers (ALBs) in different AWS Regions in the on-premises firewall for a company, while ensuring scalability with minimal configuration changes, the most appropriate solution is option C, launching AWS Global Accelerator, registering the ALBs in different Regions to the accelerator, and updating the on-premises firewall's rule to allow static IP addresses associated with the accelerator.

AWS Global Accelerator is a service that can improve the availability and performance of applications by routing traffic to optimal endpoints based on health, geography, and routing policies that you configure. By registering the ALBs in different Regions with Global Accelerator, the on-premises firewall can be updated to allow static IP addresses associated with the accelerator, which remains the same even if the underlying resources change.

Option A, writing an AWS Lambda script to get the IP addresses of the ALBs in different Regions, may not be the most appropriate solution because it requires additional scripting and may not be scalable.

Option B, migrating all ALBs in different Regions to the Network Load Balancer (NLBs), may not be the most appropriate solution because it may require significant changes to the current infrastructure and may not be necessary for the requirements stated.

Option D, launching a Network Load Balancer (NLB) in one Region and registering the private IP addresses of the ALBs in different Regions with the NLB, may not be the most appropriate solution because it may require additional configuration changes and may not be necessary for the requirements stated.

Question:

282. A company is building a media sharing application and decides to use Amazon S3 for storage. When a media file is uploaded, the company starts a multi-step process to create thumbnails, identify objects in the images, transcode videos into standard formats and resolutions, and extract and store the metadata to an Amazon DynamoDB table. The metadata is used for searching and navigation.
The amount of traffic is variable. The solution must be able to scale to handle spikes in load without unnecessary expenses.
What should a solutions architect recommend to support this workload?

- •A. Build the processing into the website or mobile app used to upload the content to Amazon S3. Save the required data to the DynamoDB table when the objects are uploaded.
- •B. Trigger AWS Step Functions when an object is stored in the S3 bucket. Have the Step Functions perform the steps needed to process the object and then write the metadata to the DynamoDB table.
- •C. Trigger an AWS Lambda function when an object is stored in the S3 bucket. Have the Lambda function start AWS Batch to perform the steps to process the object. Place the object data in the DynamoDB table when complete.
- •D. Trigger an AWS Lambda function to store an initial entry in the DynamoDB table when an object is uploaded to Amazon S3. Use a program running on an Amazon EC2 instance in an Auto Scaling group to poll the index for unprocessed items, and use the program to perform the processing.

To support the multi-step process of creating thumbnails, identifying objects in images, transcoding videos, and extracting metadata from media files uploaded to Amazon S3, and to scale the solution to handle spikes in load without unnecessary expenses, the most appropriate solution is option B, triggering AWS Step Functions when an object is stored in the S3 bucket, having the Step Functions perform the processing steps, and then writing the metadata to the DynamoDB table.

AWS Step Functions is a fully managed service that allows you to coordinate multiple AWS services, including AWS Lambda, to build and run multi-step workflows. By triggering Step Functions when an object is stored in the S3 bucket, the processing steps can be performed in a scalable and cost-effective manner, and the metadata can be written to the DynamoDB table for searching and navigation.

Option A, building the processing into the website or mobile app used to upload the content to Amazon S3, may not be the most appropriate solution because it may require additional development effort and may not be scalable.

Option C, triggering an AWS Lambda function to start AWS Batch to perform the steps to process the object and place the object data in the DynamoDB table when complete, may not be the most appropriate solution because it may add additional complexity to the solution and may not be necessary for the requirements stated.

Option D, triggering an AWS Lambda function to store an initial entry in the DynamoDB table when an object is uploaded to Amazon S3, and using a program running on an Amazon EC2 instance in an Auto Scaling group to poll the index for unprocessed items and perform the processing, may not be the most appropriate solution because it may add additional complexity to the solution and may not be as scalable and cost-effective as using Step Functions.

Question: **How can CloudFront increases the availability? It can reduce the latency and not the option to make the application highly available. Please confirm**

296. A company hosts its static website content from an Amazon S3 bucket in the us-east-1 Region. Content is made available through an Amazon CloudFront origin pointing to that bucket. Cross-Region replication is set to create a second copy of the bucket in the ap-southeast-1 Region. Management wants a solution that provides greater availability for the website.
Which combination of actions should a solutions architect take to increase availability? (Choose two.)

- A. Add both buckets to the CloudFront origin.
- B. Configure failover routing in Amazon Route 53.
- C. Create a record in Amazon Route 53 pointing to the replica bucket.
- D. Create an additional CloudFront origin pointing to the ap-southeast-1 bucket.
- E. Set up a CloudFront origin group with the us-east-1 bucket as the primary and the ap-southeast-1 bucket as the secondary.

To increase availability for a static website content hosted in an Amazon S3 bucket, with cross-Region replication to create a second copy of the bucket in another Region, the most appropriate solutions are options B and E:

B. Configure failover routing in Amazon Route 53.

E. Set up a CloudFront origin group with the us-east-1 bucket as the primary and the ap-southeast-1 bucket as the secondary.

Option B, configuring failover routing in Amazon Route 53, can be used to route traffic to the secondary bucket in the ap-southeast-1 Region in case the primary bucket in the us-east-1 Region is unavailable.

Option E, setting up a CloudFront origin group with the us-east-1 bucket as the primary and the ap-southeast-1 bucket as the secondary, can provide greater availability by allowing CloudFront to automatically switch to the secondary bucket in the ap-southeast-1 Region in case the primary bucket in the us-east-1 Region is unavailable.

Option A, adding both buckets to the CloudFront origin, may not be the most appropriate solution because it may not provide failover capability.

Option C, creating a record in Amazon Route 53 pointing to the replica bucket, may not be the most appropriate solution because it may not provide the necessary failover capability.

Option D, creating an additional CloudFront origin pointing to the ap-southeast-1 bucket, may not be the most appropriate solution because it may require additional configuration changes and may not provide the necessary failover capability.

Question:

295. A company has a live chat application running on its on-premises servers that use WebSockets. The company wants to migrate the application to AWS.
Application traffic is inconsistent, and the company expects there to be more traffic with sharp spikes in the future.
The company wants a highly scalable solution with no server maintenance nor advanced capacity planning.
Which solution meets these requirements?

- A. Use Amazon API Gateway and AWS Lambda with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for provisioned capacity.
- B. Use Amazon API Gateway and AWS Lambda with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for on-demand capacity.
- C. Run Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for on-demand capacity.
- D. Run Amazon EC2 instances behind a Network Load Balancer in an Auto Scaling group with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for provisioned capacity.

To migrate a live chat application running on on-premises servers that use WebSockets to AWS, with a highly scalable solution that requires no server maintenance nor advanced capacity planning, the most appropriate solution is option B, using Amazon API Gateway and AWS Lambda with an Amazon DynamoDB table as the data store, configured for on-demand capacity.

Amazon API Gateway and AWS Lambda can be used to build a highly scalable and cost-effective WebSocket API to handle the live chat application traffic. By using on-demand capacity for the Amazon DynamoDB table, the application can scale automatically to meet the incoming traffic without requiring any capacity planning or maintenance.

Option A, using Amazon API Gateway and AWS Lambda with an Amazon DynamoDB table as the data store, configured for provisioned capacity, may not be the most appropriate solution because it may require capacity planning and may not be as cost-effective as using on-demand capacity.

Option C, running Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group with an Amazon DynamoDB table as the data store, configured for on-demand capacity, may not be the most appropriate solution because it requires server maintenance and capacity planning.

Option D, running Amazon EC2 instances behind a Network Load Balancer in an Auto Scaling group with an Amazon DynamoDB table as the data store, configured for provisioned capacity, may not be the most appropriate solution because it requires server maintenance and capacity planning.