Notes Mock Test - 5

Question 1 - Correct

Question: A financial services firm has traditionally operated with an on-premise data center and would like to create a disaster recovery strategy leveraging the AWS Cloud. As a Solutions Architect, you would like to ensure that a scaled-down version of a fully functional environment is always running in the AWS cloud, and in case of a disaster, the recovery time is kept to a minimum. Which disaster recovery strategy is that?

Correct Option:

- **Warm Standby**

Explanation behind Correct Option:

- **Scaled-Down Environment:** A scaled-down version of a fully functional environment is always running in the cloud.
- **Reduced Recovery Time:** Extends pilot light elements, further decreasing recovery time.
- **Always-On Services:** Some services are always running, enabling quick recovery.
- **Critical Systems Duplication:** Business-critical systems are fully duplicated on AWS and always active.

Incorrect Options:

- **Backup and Restore:**
  - **Time-Consuming:** Restoring systems from backups can be time-consuming in the event of a disaster.
  - **Storage:** Typically involves data storage on tape and off-site locations.
  - **Amazon S3:** Often used as a destination for backup data; accessible but slower recovery.
- **Pilot Light:**
  - **Minimal Environment:** Only a minimal version of the environment is always running.
  - **Analogy:** Similar to a small flame in a gas heater, which can quickly ignite a full system.
  - **Core Elements:** Maintains critical core elements, requiring rapid provisioning for full recovery.
- **Multi Site:**
  - **Active-Active Configuration:** Runs in both AWS and on-premise infrastructure simultaneously.
  - **Data Replication:** Method depends on chosen recovery point, providing continuous availability.

Conclusion / Points to Memorize:

- **Warm Standby:**
  - Scaled-down functional environment always active.
  - Quick recovery due to always-on services.
  - Suitable for business-critical systems requiring minimal downtime.
- **Backup and Restore:**
  - Involves off-site backup storage.
  - Longer recovery times.
  - Commonly uses Amazon S3 for backup data.
- **Pilot Light:**
  - Minimal environment running.
  - Rapid provisioning around critical core elements.
- **Multi Site:**
  - Active-active setup with on-premise and AWS.
    - Continuous availability with data replication.

Question 2 - Correct

Question: You have an Amazon S3 bucket that contains files in two different folders - s3://mybucket/images and s3://my-bucket/thumbnails. When an image is first uploaded and new, it is viewed several times. But after 45 days, analytics prove that image files are on average rarely requested, but the thumbnails still are. After 180 days, you would like to archive the image files and the thumbnails. Overall you would like the solution to remain highly available to prevent disasters happening against a whole Availability Zone (AZ). How can you implement an efficient cost strategy for your Amazon S3 bucket? (Select two)

Correct Options:

- **Create a Lifecycle Policy to transition objects to Amazon S3 Standard IA using a prefix after 45 days**
- **Create a Lifecycle Policy to transition all objects to Amazon S3 Glacier after 180 days**

Explanation behind Correct Options:

- **Create a Lifecycle Policy to transition objects to Amazon S3 Standard IA using a prefix after 45 days:**
  - **Standard-IA for Infrequent Access:** Suitable for data accessed less frequently but requires rapid access.

- **Cost-Effective:** Offers high durability, low cost, and high performance with minimal storage charges for 30 days.
- **Prefix Utilization:** Use a prefix to transition only the s3://my-bucket/images folder, keeping thumbnails accessible.

- **Create a Lifecycle Policy to transition all objects to Amazon S3 Glacier after 180 days:**
  - **Long-Term Archiving:** Glacier is ideal for secure, durable, and low-cost long-term data archiving.
  - **High Durability:** Ensures 99.999999999% durability with comprehensive security and compliance features.
  - **No Prefix Needed:** Applicable to all objects after 180 days, suitable for both images and thumbnails.

Incorrect Options:

- **Create a Lifecycle Policy to transition all objects to Amazon S3 Standard IA after 45 days:**
  - **Incorrect Application:** Transitioning all objects would affect thumbnails, which are still frequently accessed.
  - **Requires Prefix:** Only images should transition to Standard-IA after 45 days.
- **Create a Lifecycle Policy to transition objects to Amazon S3 Glacier using a prefix after 180 days:**
  - **Redundant Prefix:** All objects can transition to Glacier without the need for a prefix.
- **Create a Lifecycle Policy to transition objects to Amazon S3 One Zone IA using a prefix after 45 days:**
  - **Availability Concern:** One Zone-IA stores data in a single AZ, not meeting the high availability requirement.
  - **Cost vs. Durability:** Although cost-effective, One Zone-IA compromises on durability compared to Standard-IA.

Conclusion / Points to Memorize:

- **Standard-IA:**
  - For data accessed less frequently but requires rapid access.
  - High durability and low cost.
  - Use prefixes to transition specific folders.
- **Glacier:**
  - Ideal for long-term data archiving.
  - Extremely low cost and high durability.
  - Applicable to all objects after a specified period.
- **One Zone-IA:**
  - Cost-effective for infrequent access but limited to a single AZ.
    - Not suitable for high availability requirements.

Question 3 - Correct

Question: A media company uses Amazon ElastiCache Redis to enhance the performance of its Amazon RDS database layer. The company wants a robust disaster recovery strategy for its caching layer that guarantees minimal downtime as well as minimal data loss while ensuring good application performance. Which of the following solutions will you recommend to address the given use-case?

Correct Option:

- **Opt for Multi-AZ configuration with automatic failover functionality to help mitigate failure**

Explanation behind Correct Option:

- **Multi-AZ Configuration:**
  - **Data Retention:** Ensures low data-loss potential with fault tolerance for various scenarios, including hardware failures.
  - **Minimal Downtime:** Provides the fastest recovery time as it eliminates the need for manual intervention.
  - **Performance Impact:** Low impact on performance, maintaining good application performance.
  - **Cost Efficiency:** Although costs may vary, Multi-AZ is the most cost-effective option when considering the need for minimal data loss and downtime.

Incorrect Options:

- **Schedule Daily Automatic Backups:**
  - **High Data Loss Potential:** Can result in almost a day's worth of data loss, making it unsuitable for scenarios requiring minimal data loss.
- **Schedule Manual Backups Using Redis Append-Only File (AOF):**
  - **Manual Intervention Required:** Provides a measure of fault tolerance but cannot protect against hardware-related failures.
  - **Risk of Data Loss:** Data is at risk due to hardware failures, making it less reliable for robust disaster recovery.
- **Add Read-Replicas Across Multiple Availability Zones (AZs):**
  - **Scaling Read Capacity:** Primarily used to scale read traffic from the primary database.
  - **Not Fault-Tolerant:** Cannot be relied upon as a complete fault-tolerant solution, thus not suitable for ensuring minimal downtime and data loss.

Conclusion / Points to Memorize:

- **Multi-AZ Configuration:**

- Ensures fault tolerance and minimal data loss.
- Provides rapid recovery without manual procedures.
- Cost-effective considering the priority on data retention and minimal downtime.

- **Automatic Backups:**
  - Useful but can result in significant data loss.
- **Manual Backups (AOF):**
  - Provides fault tolerance but not sufficient against hardware failures.
- **Read-Replicas:**
  - Useful for scaling read capacity, not for complete disaster recovery.

Question 4 - Correct

Question: A Big Data processing company has created a distributed data processing framework that performs best if the network performance between the processing machines is high. The application has to be deployed on AWS, and the company is only looking at performance as the key measure. As a Solutions Architect, which deployment do you recommend?

Correct Option:

- **Use a Cluster placement group**

Explanation behind Correct Option:

- **Cluster Placement Group:**
  - **Low-Latency Network Performance:** Packs instances close together within a single Availability Zone (AZ), enabling low-latency node-to-node communication.
  - **High Network Throughput:** Provides a higher per-flow throughput limit of up to 10 Gbps for TCP/IP traffic.
  - **Enhanced Networking:** Recommended for applications requiring low network latency and high network throughput.
  - **High-Bisection Bandwidth:** Instances are placed in the same high-bisection bandwidth segment of the network, ideal for tightly-coupled HPC applications.

Incorrect Options:

- **Optimize the Amazon EC2 kernel using EC2 User Data:**
  - **Insufficient for Network Performance:** Kernel optimization does not address the network performance needs for the application.
- **Use Spot Instances:**
  - **Cost vs. Performance:** While cost-effective, Spot Instances may be interrupted and are not suitable for applications where performance is the key measure.
- **Use a Spread placement group:**
  - **Correlated Failures:** Designed to reduce correlated failures by placing instances on distinct racks.
  - **Low Network Performance:** Not optimized for high network performance between instances, as each instance is placed on different hardware.

Conclusion / Points to Memorize:

- **Cluster Placement Group:**
  - Provides low-latency and high network throughput.
  - Suitable for tightly-coupled applications requiring high performance.
  - Ensures instances are placed close together within a single AZ.
- **Spread Placement Group:**
  - Designed to reduce correlated failures.
  - Places instances on distinct racks with separate network and power sources.
- **Spot Instances:**
  - Cost-effective for flexible applications.
  - Not reliable for performance-critical applications due to potential interruptions.
- **Kernel Optimization:**
  - Does not significantly impact network performance.

Question 5 - Incorrect

Question: A company has migrated its application from a monolith architecture to a microservices-based architecture. The development team has updated the Amazon Route 53 simple record to point “myapp.mydomain.com” from the old Load Balancer to the new one. The users are still not redirected to the new Load Balancer. What has gone wrong in the configuration?

Correct Option:

- **The Time To Live (TTL) is still in effect**

Explanation behind Correct Option:

- **Amazon Route 53 Overview:**
  - **DNS Service:** Connects user requests to AWS infrastructure such as EC2 instances, load balancers, or S3 buckets, and can route users to infrastructure outside of AWS.
  - **DNS Health Checks:** Routes traffic to healthy endpoints and monitors application health.
  - **Traffic Management:** Supports Latency Based Routing, Geo DNS, Geoproximity, Weighted Round Robin, and DNS Failover.
- **TTL (Time to Live):**
  - **Definition:** TTL is the amount of time in seconds that DNS recursive resolvers cache information about a record.
  - **Impact:** Longer TTL reduces DNS query calls, decreases latency, and lowers costs but delays changes in records taking effect.
  - **Recommendation:** For domain changes, initially set a shorter TTL (e.g., 300 seconds) and increase it after confirming the new settings.
  - **Use-Case Issue:** The TTL for the old Load Balancer's DNS record is still in effect, causing a delay in redirecting users to the new Load Balancer.

Incorrect Options:

- **The CNAME Record is misconfigured:**
  - **Function:** Redirects DNS queries to another DNS record.
  - **Example:** Redirects queries from acme.example.com to zenith.example.com.
  - **Irrelevant:** Misconfiguration of CNAME is not the issue in this use-case.
- **The Alias Record is misconfigured:**
  - **Function:** Routes traffic to selected AWS resources or from one record to another in the hosted zone.
  - **Capability:** Can create an alias record at the zone apex, unlike a CNAME record.
  - **Irrelevant:** Misconfiguration of Alias Record is not the issue in this use-case.
- **The health checks are failing:**
  - **Simple Records:** Do not have health checks, making this option incorrect.

Conclusion / Points to Memorize:

- **TTL:**
  - Defines cache duration for DNS records.
  - Shorter TTL recommended for changes to take effect quickly.
  - Longer TTL reduces latency and cost but delays updates.
- **CNAME Records:**
  - Redirect DNS queries to another DNS record.
  - Not used at the zone apex.
- **Alias Records:**
  - Route traffic to AWS resources or other records.
  - Can be used at the zone apex.
- **Health Checks:**
  - Not applicable to simple records.

Question 6 - Correct

Question: A Pharmaceuticals company is looking for a simple solution to connect its VPCs and on-premises networks through a central hub. As a Solutions Architect, which of the following would you suggest as the solution that requires the LEAST operational overhead?

Correct Option:

- **Use AWS Transit Gateway to connect the Amazon VPCs to the on-premises networks**

Explanation behind Correct Option:

- **AWS Transit Gateway:**
  - **Centralized Hub:** Acts as a single gateway to connect multiple VPCs and on-premises networks.
  - **Simplified Management:** Only need to manage a single connection from the central gateway to each VPC or network, reducing complexity.
  - **Scalable:** Supports growing number of workloads across multiple accounts and VPCs.
  - **Traffic Routing:** Controls how traffic is routed among all connected networks, simplifying management and reducing operational costs.

Incorrect Options:

- **Use Transit VPC Solution:**
  - **Complexity:** Requires maintaining multiple VPN connections and managing EC2-based software appliances.
  - **Limitations:** Higher complexity and operational overhead compared to Transit Gateway.
- **Partially Meshed VPC Peering:**
  - **Point-to-Point:** Provides bidirectional connectivity but does not support transitive routing.
  - **Limited Connectivity:** Each VPC must have its own direct connection to on-premises networks, increasing complexity.
- **Fully Meshed VPC Peering:**
  - **Scalability Issues:** Managing fully meshed connections becomes complex as the number of VPCs increases.
  - **No Transitive Routing:** Each VPC must connect directly to on-premises networks, leading to higher operational overhead.

Conclusion / Points to Memorize:

- **AWS Transit Gateway:**
  - Centralized, scalable, and simplified connectivity.
  - Reduces complexity and operational overhead.
  - Ideal for connecting multiple VPCs and on-premises networks.
- **Transit VPC Solution:**
  - Higher complexity with multiple VPN connections.
  - Requires managing EC2-based software appliances.
- **VPC Peering:**
  - Point-to-point connectivity without transitive routing.
  - Suitable for limited number of VPCs and direct connectivity needs.
  - Higher complexity in fully meshed configurations.

Question 7 - Correct

Question: A photo hosting service publishes a collection of beautiful mountain images, every month, that aggregate over 50 gigabytes in size and downloaded all around the world. The content is currently hosted on Amazon EFS and distributed by Elastic Load Balancing (ELB) and Amazon EC2 instances. The website is experiencing high load each month and very high network costs. As a Solutions Architect, what can you recommend that won't force an application refactor and reduce network costs and Amazon EC2 load drastically?

Correct Option:

- **Create an Amazon CloudFront distribution**

Explanation behind Correct Option:

- **Amazon CloudFront:**
  - **Content Delivery Network (CDN):** Delivers data, videos, applications, and APIs globally with low latency and high transfer speeds.
  - **Points of Presence (POPs):** Edge locations ensure popular content is served quickly.
  - **Regional Edge Caches:** Improve performance for content not popular enough to stay at POPs.
  - **Caching Layer:** Effective for static files, significantly reducing network costs and EC2 load without requiring application refactor.
- **Use-Case:** Adding a CloudFront distribution as a caching layer in front of ELB would reduce network costs and EC2 load drastically by caching the static image pack.

Incorrect Options:

- **Host the Master Pack onto Amazon S3 for Faster Access:**
  - **Application Refactor Required:** Hosting on S3 would necessitate changes in the application code.
- **Upgrade the Amazon EC2 Instances:**
  - **No Network Cost Reduction:** Upgrading EC2 instances does not address network costs.
- **Enable Elastic Load Balancing (ELB) Caching:**
  - **No Caching Capability:** ELB does not provide caching capabilities, making this option invalid.

Conclusion / Points to Memorize:

- **Amazon CloudFront:**
  - CDN for global content delivery with low latency and high transfer speeds.
  - Caches content at edge locations and regional edge caches.
  - Effective for reducing network costs and EC2 load for static content.
- **S3 Hosting:**

    - Requires application refactoring.
- **EC2 Upgrade:**
    - Does not address network costs.
- **ELB Caching:**
    - ELB does not support caching.

Question 8 - Correct

Question: Amazon Route 53 is configured to route traffic to two Network Load Balancer nodes belonging to two Availability Zones (AZs): AZ-A and AZ-B. Cross-zone load balancing is disabled. AZ-A has four targets and AZ-B has six targets. Which of the below statements is true about traffic distribution to the target instances from Amazon Route 53?

Correct Option:

- **Each of the four targets in AZ-A receives 12.5% of the traffic**

Explanation behind Correct Option:

- **Load Balancer Traffic Distribution:**
    - **Cross-Zone Load Balancing Disabled:** Each load balancer node distributes traffic only across the registered targets in its respective AZ.
    - **Traffic Distribution by Route 53:** Traffic is distributed such that each load balancer node receives 50% of the traffic from clients.
    - **AZ-A Calculation:**
        - **50% Traffic to AZ-A:** AZ-A's node receives 50% of total traffic.
        - **Four Targets:** Each target in AZ-A receives 12.5% (50% / 4) of the total traffic.
    - **AZ-B Calculation:**
        - **50% Traffic to AZ-B:** AZ-B's node receives 50% of total traffic.
        - **Six Targets:** Each target in AZ-B receives 8.3% (50% / 6) of the total traffic.

Incorrect Options:

- **Each of the six targets in AZ-B receives 10% of the traffic:**
    - **Incorrect Calculation:** Each target in AZ-B actually receives 8.3% of the traffic, not 10%.
- **Each of the four targets in AZ-A receives 8% of the traffic:**
    - **Incorrect Calculation:** Each target in AZ-A actually receives 12.5% of the traffic, not 8%.
- **Each of the four targets in AZ-A receives 10% of the traffic:**
    - **Incorrect Calculation:** Each target in AZ-A actually receives 12.5% of the traffic, not 10%.

Conclusion / Points to Memorize:

- **Traffic Distribution in Load Balancers:**
    - Cross-zone load balancing disabled means each node distributes traffic within its AZ.
    - Each load balancer node receives 50% of the total traffic.
- **AZ-A and AZ-B Traffic Distribution:**
    - AZ-A with 4 targets: Each receives 12.5% of the traffic.
    - AZ-B with 6 targets: Each receives 8.3% of the traffic.

Question 9 - Correct

Question: An enterprise has decided to move its secondary workloads such as backups and archives to AWS cloud. The CTO wishes to move the data stored on physical tapes to Cloud, without changing their current tape backup workflows. The company holds petabytes of data on tapes and needs a cost-optimized solution to move this data to cloud. What is an optimal solution that meets these requirements while keeping the costs to a minimum?

Correct Option:

- **Use Tape Gateway, which can be used to move on-premises tape data onto AWS Cloud. Then, Amazon S3 archiving storage classes can be used to store data cost-effectively for years**

Explanation behind Correct Option:

- **Tape Gateway:**
    - **No Workflow Changes:** Enables the use of virtual tapes in AWS without changing existing tape backup workflows.
    - **Compatibility:** Supports all leading backup applications.
    - **Low-Latency Access:** Caches virtual tapes on-premises for low-latency data access.

- **Secure Data Transfer:** Encrypts data between the gateway and AWS.
- **Cost Optimization:** Compresses and transitions virtual tapes between Amazon S3, S3 Glacier, and S3 Glacier Deep Archive to minimize storage costs.
- **Storage Management:** Manages S3 storage, eliminating the need to manage your own S3 storage.
- **No Upfront Fees:** Only pay for what you consume, with no minimum commitments.

Incorrect Options:

- **Use AWS DataSync:**
  - **File Type Limitation:** Supports only NFS and SMB file types, not suitable for tape data.
- **Use AWS Direct Connect:**
  - **High Cost:** Suitable for low-latency access with ongoing high availability bandwidth needs, not cost-effective for backup data.
- **Use AWS VPN and Amazon EFS:**
  - **Inappropriate Use:** VPN and EFS are not suitable for archiving tape data, and EFS is not designed for tape backups.

Conclusion / Points to Memorize:

- **Tape Gateway:**
  - Replaces physical tapes with virtual tapes in AWS.
  - Compatible with existing backup applications.
  - Encrypts and compresses data for secure and cost-effective storage.
  - Utilizes S3, S3 Glacier, and S3 Glacier Deep Archive for cost-efficient long-term storage.
- **AWS DataSync:**
  - Limited to NFS and SMB file types.
- **AWS Direct Connect:**
  - High cost for low-latency ongoing access needs.
- **AWS VPN and Amazon EFS:**
  - Not suitable for tape data archiving.

Question 10 - Correct

Question: A company has developed a popular photo-sharing website using a serverless pattern on the AWS Cloud using Amazon API Gateway and AWS Lambda. The backend uses an Amazon RDS PostgreSQL database. The website is experiencing high read traffic and the AWS Lambda functions are putting an increased read load on the Amazon RDS database. The architecture team is planning to increase the read throughput of the database, without changing the application's core logic. As a Solutions Architect, what do you recommend?

Correct Option:

- **Use Amazon RDS Read Replicas**

Explanation behind Correct Option:

- **Amazon RDS Read Replicas:**
  - **Enhanced Performance and Durability:** Improves read throughput by creating one or more replicas of a source DB instance.
  - **Elastic Scalability:** Allows scaling beyond the capacity of a single DB instance for read-heavy workloads.
  - **Read Traffic Distribution:** High-volume read traffic can be served from multiple copies, increasing aggregate read throughput.
  - **Promotion to Standalone DBs:** Read replicas can be promoted to standalone DB instances if needed.
  - **No Core Logic Changes:** Does not require changes to the application's core logic.

Incorrect Options:

- **Use Amazon RDS Multi-AZ feature:**
  - **Disaster Recovery:** Provides enhanced availability and durability, not specifically designed for read scalability.
  - **Synchronous Replication:** Focuses on failover capabilities rather than read performance.
- **Use Amazon ElastiCache:**
  - **In-Memory Data Store:** Suitable for caching, real-time analytics, and session stores, requiring changes to application logic.
  - **Refactoring Needed:** Would need significant changes to integrate with the current setup.
- **Use Amazon DynamoDB:**
  - **Key-Value and Document Database:** Designed for high-performance, scalable internet-scale applications.
  - **Refactoring Needed:** Would require a complete refactor of the existing application to fit the DynamoDB model.

Conclusion / Points to Memorize:

- **Amazon RDS Read Replicas:**

- Ideal for scaling read-heavy workloads.
- Increases aggregate read throughput without application changes.
- Allows promotion to standalone DB instances.

- **Amazon RDS Multi-AZ:**
  - Enhances availability and disaster recovery.
  - Not intended for read scalability.
- **Amazon ElastiCache:**
  - Provides low-latency, high-throughput caching.
  - Requires application refactoring.
- **Amazon DynamoDB:**
  - High-performance, scalable NoSQL database.
  - Requires a significant application refactor.

Question 11 - Incorrect

Question: You are working as an AWS architect for a weather tracking facility. You are asked to set up a Disaster Recovery (DR) mechanism with minimum costs. In case of failure, the facility can only bear data loss of approximately 15 minutes without jeopardizing the forecasting models. As a Solutions Architect, which DR method will you suggest?

Correct Option:

- **Pilot Light**

Explanation behind Correct Option:

- **Pilot Light:**
  - **Minimal Environment Running:** Maintains a minimal version of the environment always running in the cloud.
  - **Critical Core Elements:** Configures and runs the most critical core elements of your system in AWS.
  - **Data Syncing:** Continuously syncs mutable data like databases to prevent data loss.
  - **Quick Recovery:** Enables rapid provisioning of a full-scale production environment around the critical core during recovery.
  - **RPO/RTO:** Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are in the range of tens of minutes, making it suitable for the use case requiring minimal data loss.

Incorrect Options:

- **Backup and Restore:**
  - **Longer Recovery Time:** Typically involves RPO in hours, taking a long time to restore systems.
  - **Cheaper but Slower:** Cost-effective but not suitable for quick recovery needs due to longer restoration times.
- **Warm Standby:**
  - **Higher Cost:** A scaled-down but fully functional environment always running, which is more costly than Pilot Light.
  - **Faster Recovery:** Faster recovery times but with increased costs.
- **Multi-Site:**
  - **Active-Active Configuration:** Runs on AWS and on-site infrastructure simultaneously, which is more costly.
  - **Higher Cost:** More expensive due to the active-active setup and continuous data replication.

Conclusion / Points to Memorize:

- **Pilot Light:**
  - Minimal environment always running.
  - Suitable for minimal data loss (RPO/RTO in tens of minutes).
  - Cost-effective compared to Warm Standby and Multi-Site.
- **Backup and Restore:**
  - Longer recovery times (RPO in hours).
  - Cost-effective but slower restoration.
- **Warm Standby:**
  - Scaled-down functional environment always running.
  - Faster recovery but higher cost.
- **Multi-Site:**
  - Active-active setup with on-site and AWS infrastructure.

- Most expensive due to continuous data replication.

Question 12 – Correct

Question: A junior developer has downloaded a sample Amazon S3 bucket policy to make changes to it based on new company-wide access policies. He has requested your help in understanding this bucket policy. As a Solutions Architect, which of the following would you identify as the correct description for the given policy?

Policy:

```
{
 "Version": "2012-10-17",
 "Id": "S3PolicyId1",
 "Statement": [
  {
   "Sid": "IPAllow",
   "Effect": "Allow",
   "Principal": "*",
   "Action": "s3:*",
   "Resource": "arn:aws:s3:::examplebucket/*",
   "Condition": {
    "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
    "NotIpAddress": {"aws:SourceIp": "54.240.143.188/32"}
   }
  }
 ]
}
```

Correct Option:

- **It authorizes an entire Classless Inter-Domain Routing (CIDR) except one IP address to access the Amazon S3 bucket**

Explanation behind Correct Option:

- **Effect: Allow:** The policy grants permissions.
- **Principal: :* The policy applies to any principal (any user).
- **Action: s3:*:** The policy allows any Amazon S3 action.
- **Resource: arn:aws:s3:::examplebucket/*:** The policy applies to the examplebucket and all its contents.
- **Condition:** The conditions specify IP-based restrictions:
  - **IpAddress:** Allows access from any IP in the 54.240.143.0/24 CIDR block (54.240.143.0 - 54.240.143.255).
  - **NotIpAddress:** Denies access from the specific IP 54.240.143.188.

The policy effectively authorizes access to the examplebucket for all IP addresses within the 54.240.143.0/24 range except for 54.240.143.188.

Incorrect Options:

- **It ensures the Amazon S3 bucket is exposing an external IP within the Classless Inter-Domain Routing (CIDR) range specified, except one IP:**
  - **Misleading:** The policy does not expose an IP; it controls access based on IP addresses.
- **It authorizes an IP address and a Classless Inter-Domain Routing (CIDR) to access the S3 bucket:**
  - **Incorrect Description:** The policy specifically excludes one IP within the CIDR.
- **It ensures Amazon EC2 instances that have inherited a security group can access the bucket:**
  - **Irrelevant:** The policy does not mention EC2 instances or security groups.

Conclusion / Points to Memorize:

- **Effect: Allow:** Grants permissions.
- **Principal: :* Applies to any user.
- **Action: s3:*:** Allows any S3 action.
- **Resource:** Specifies the S3 bucket and its contents.
- **Condition (IpAddress):** Allows access from specified IP range.
  - **Condition (NotIpAddress):** Denies access from a specific IP within the allowed range.

Question 13 - Correct

Question: A company's business logic is built on several microservices that are running in the on-premises data center. They currently communicate using a message broker that supports the MQTT protocol. The company is looking at migrating these applications and the message broker to AWS Cloud without changing the application logic. Which technology allows you to get a managed message broker that supports the MQTT protocol?

Explanation behind Correct Option:

- **Amazon MQ:**
  - **Managed Message Broker:** Provides a managed service for Apache ActiveMQ.
  - **Supports Industry-Standard Protocols:** Supports protocols such as JMS, NMS, AMQP, STOMP, MQTT, and WebSocket.
  - **Easy Migration:** Ideal for migrating existing messaging applications to the cloud without changing application logic.
  - **Compatibility:** Ensures compatibility with the MQTT protocol, allowing seamless communication for microservices.

Incorrect Options:

- **Amazon Simple Queue Service (Amazon SQS):**
  - **Message Queuing Service:** Fully managed service for decoupling and scaling microservices.
  - **No MQTT Support:** Does not support the MQTT protocol.
- **Amazon Kinesis Data Streams:**
  - **Real-Time Data Streaming:** Designed for capturing and processing real-time data streams.
  - **No MQTT Support:** Not suitable for message brokering with MQTT.
- **Amazon Simple Notification Service (Amazon SNS):**
  - **Pub/Sub Messaging Service:** Enables high-throughput, push-based messaging.
  - **No MQTT Support:** Does not support MQTT, making it unsuitable for the given use case.

Conclusion / Points to Memorize:

- **Amazon MQ:**
  - Managed service for Apache ActiveMQ.
  - Supports multiple protocols including MQTT.
  - Ideal for migrating existing messaging applications without changes.
- **Amazon SQS:**
  - Message queuing service for decoupling microservices.
  - Does not support MQTT.
- **Amazon Kinesis Data Streams:**
  - Real-time data streaming service.
  - Not designed for message brokering with MQTT.
- **Amazon SNS:**
  - Pub/Sub messaging service.
  - Does not support MQTT.

Question 14 - Correct

Question: A niche social media application allows users to connect with sports athletes. As a solutions architect, you've designed the architecture of the application to be fully serverless using Amazon API Gateway and AWS Lambda. The backend uses an Amazon DynamoDB table. Some of the star athletes using the application are highly popular, and therefore Amazon DynamoDB has increased the read capacity units (RCUs). Still, the application is experiencing a hot partition problem. What can you do to improve the performance of Amazon DynamoDB and eliminate the hot partition problem without a lot of application refactoring?

Correct Option:

- **Use Amazon DynamoDB DAX**

Explanation behind Correct Option:

- **Amazon DynamoDB Accelerator (DAX):**
  - **In-Memory Caching:** Provides a fully managed, highly available, in-memory cache for DynamoDB.
  - **Performance Improvement:** Delivers up to a 10x performance boost – from milliseconds to microseconds – even at millions of requests per second.
  - **No Refactoring Needed:** Transparently integrates with existing DynamoDB tables, eliminating the need for significant application changes.
  - **Hot Key Caching:** Effectively caches "hot keys," reducing the load on specific partitions and eliminating hot partition issues.

Incorrect Options:

- **Use Amazon DynamoDB Global Tables:**
  - **Global Distribution:** Provides a multi-region, multi-master database for globally distributed applications.
  - **Not a Solution for Hot Partitions:** Does not address hot key issues; primarily focuses on global read/write performance.
- **Use Amazon DynamoDB Streams:**
  - **Change Tracking:** Captures and records changes to items in a DynamoDB table.
  - **Not for Performance:** Useful for event-driven architectures but does not address hot key issues or improve read performance.
- **Use Amazon ElastiCache:**
  - **In-Memory Data Store:** Provides high throughput and low latency in-memory caching.
  - **Requires Refactoring:** Would need significant changes to integrate with AWS Lambda and the existing architecture.

Conclusion / Points to Memorize:

- **Amazon DynamoDB DAX:**
  - In-memory caching for DynamoDB.
  - Up to 10x performance improvement.
  - No significant application refactoring required.
  - Effective for reducing hot partition issues.
- **Amazon DynamoDB Global Tables:**
  - Multi-region, multi-master replication.
  - Does not address hot partition problems.
- **Amazon DynamoDB Streams:**
  - Tracks changes to table items.
  - Not designed to resolve hot partition issues.
- **Amazon ElastiCache:**
  - High-performance in-memory caching.
  - Requires extensive application changes.

Question 15 - Incorrect

Question: A ride-sharing company wants to use an Amazon DynamoDB table for data storage. The table will not be used during the night hours whereas the read and write traffic will often be unpredictable during day hours. When traffic spikes occur they will happen very quickly. Which of the following will you recommend as the best-fit solution?

Correct Option:

- **Set up Amazon DynamoDB table in the on-demand capacity mode**

Explanation behind Correct Option:

- **Amazon DynamoDB On-Demand Capacity Mode:**
  - **Flexibility:** Automatically allocates capacity as needed, ideal for unpredictable workloads.
  - **Pay-Per-Request Pricing:** Pay only for the read and write requests you use, without capacity planning.
  - **Immediate Scaling:** Handles traffic spikes instantly without delays, making it suitable for bursty traffic patterns.
  - **Ease of Use:** No need to manage capacity settings, simplifying operations.

Incorrect Options:

- **Set up Amazon DynamoDB global table in the provisioned capacity mode:**
  - **Global Tables:** Useful for multi-region replication, not specifically for handling unpredictable load.
  - **Provisioned Capacity:** Requires capacity planning, not suitable for bursty traffic.
- **Set up Amazon DynamoDB table with a global secondary index:**
  - **Global Secondary Index (GSI):** Enhances query capabilities but does not address unpredictable traffic loads.
  - **Not Related to Capacity:** Does not manage or scale read/write capacity.
- **Set up Amazon DynamoDB table in the provisioned capacity mode with auto-scaling enabled:**
  - **Provisioned Capacity with Auto-Scaling:** Adjusts capacity based on traffic patterns but has a delay in scaling.
  - **Predictable Traffic:** Better suited for applications with predictable or gradually changing traffic patterns.

Conclusion / Points to Memorize:

- **On-Demand Capacity Mode:**
  - Instant scaling for unpredictable and bursty traffic.
  - Pay-per-request pricing model.
  - Ideal for applications with varying or unknown workloads.
- **Provisioned Capacity Mode:**
  - Requires capacity planning.
  - Suitable for predictable traffic patterns.
  - Auto-scaling can help, but has a delay.
- **Global Secondary Index:**
  - Enhances query flexibility.
  - Does not manage traffic load or capacity.
- **Global Tables:**
  - Multi-region replication for global applications.
  - Not designed for handling bursty or unpredictable traffic.

Question 16 - Incorrect

Question: A music-sharing company uses a Network Load Balancer to direct traffic to 5 Amazon EC2 instances managed by an Auto Scaling group. When a very popular song is released, the Auto Scaling Group scales to 100 instances and the company incurs high network and compute fees. The company wants a solution to reduce the costs without changing any of the application code. What do you recommend?

Correct Option:

- **Use an Amazon CloudFront distribution**

Explanation behind Correct Option:

- **Amazon CloudFront:**
  - **Content Delivery Network (CDN):** Securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds.
  - **Points of Presence (POPs):** Edge locations ensure that popular content is served quickly to viewers.
  - **Regional Edge Caches:** Bring more of your content closer to viewers, even for less popular content, improving performance.
  - **Cost Reduction:** By caching and distributing content globally, reduces the need for Auto Scaling group to scale significantly, thereby reducing compute and network costs.

Incorrect Options:

- **Leverage AWS Storage Gateway:**
  - **Hybrid Cloud Storage:** Connects on-premises applications to cloud storage with local caching.
  - **Not for End-User Distribution:** Designed for storage integration, not for distributing files to end-users.
- **Move the songs to Amazon S3:**
  - **Object Storage Service:** Provides scalable storage, but would require changes to the application code to integrate with S3.
  - **Code Changes Required:** Involves modifying the application to fetch files from S3.
- **Move the songs to Amazon S3 Glacier:**
  - **Archival Storage:** Designed for long-term storage and backup with retrieval times from minutes to hours.
  - **Not Suitable for Frequently Accessed Files:** Inappropriate for files that need to be frequently accessed due to longer retrieval times.

Conclusion / Points to Memorize:

- **Amazon CloudFront:**
  - CDN service for fast, secure, and global delivery of content.
  - Reduces load on backend servers by caching content at edge locations.
  - Minimizes compute and network costs without requiring code changes.
- **AWS Storage Gateway:**
  - Hybrid cloud storage solution, not designed for direct content distribution.
- **Amazon S3:**
  - Scalable object storage, but integrating requires code changes.
- **Amazon S3 Glacier:**
  - Archival storage for long-term, infrequently accessed data.

- Not suitable for frequently accessed content due to long retrieval times.

Question 17 - Correct

Question: You have developed a new REST API leveraging the Amazon API Gateway, AWS Lambda and Amazon Aurora database services. Most of the workload on the website is read-heavy. The data rarely changes and it is acceptable to serve users outdated data for about 24 hours. Recently, the website has been experiencing high load and the costs incurred on the Aurora database have been very high. How can you easily reduce the costs while improving performance, with minimal changes?

Correct Option:

- **Enable Amazon API Gateway Caching**

Explanation behind Correct Option:

- **Amazon API Gateway Caching:**
  - **Fully Managed Service:** Facilitates the creation, publication, maintenance, monitoring, and securing of APIs at any scale.
  - **Caching Responses:** Reduces the number of calls made to the backend endpoint and improves the latency of requests.
  - **TTL (Time-to-Live):** Caches responses for a specified TTL period (default is 300 seconds, maximum is 3600 seconds).
  - **Minimal Changes:** Enabling caching requires minimal changes to the current setup.
  - **Cost Reduction:** Decreases the load on the Aurora database, thereby reducing costs.

Incorrect Options:

- **Add Amazon Aurora Read Replicas:**
  - **High Availability and Scalability:** Useful for scaling read operations and increasing availability.
  - **Increased Cost:** Adding read replicas would significantly increase costs, not suitable for cost reduction.
- **Switch to using an Application Load Balancer:**
  - **Application Layer Load Balancing:** Routes requests based on the content of the application traffic.
  - **Not a Caching Solution:** Does not address the need for caching and cost reduction.
- **Enable AWS Lambda In Memory Caching:**
  - **No Native In-Memory Caching:** AWS Lambda does not have native in-memory caching capabilities.
  - **Incorrect Option:** This option is a distractor and does not provide a solution for the given use case.

Conclusion / Points to Memorize:

- **Amazon API Gateway Caching:**
  - Caches API responses to reduce backend load.
  - Improves latency and reduces costs.
  - Minimal configuration changes required.
- **Amazon Aurora Read Replicas:**
  - Increases read capacity and availability.
  - Significant cost increase.
- **Application Load Balancer:**
  - Routes traffic at the application layer.
  - Not a caching solution.
- **AWS Lambda In-Memory Caching:**
  - No native support for in-memory caching.
  - Not applicable for reducing costs in this scenario.

Question 18 – Correct

Question: You started a new job as a solutions architect at a company that has both AWS experts and people learning AWS. Recently, a developer misconfigured a newly created Amazon RDS database which resulted in a production outage. How can you ensure that Amazon RDS specific best practices are incorporated into a reusable infrastructure template to be used by all your AWS users?

Correct Option:

- **Use AWS CloudFormation to manage Amazon RDS databases**

Explanation behind Correct Option:

- **AWS CloudFormation:**
  - **Infrastructure as Code:** Provides a common language to model and provision AWS and third-party application resources.

- **Reusable Templates:** Allows creating reusable infrastructure templates that incorporate best practices.
- **Consistency and Standardization:** Ensures consistent and standardized configuration across all AWS environments.
- **Automated Provisioning:** Facilitates automated and secure provisioning of resources.
- **Single Source of Truth:** Maintains a single source of truth for AWS resources, reducing the risk of misconfiguration.

Incorrect Options:

- **Store your recommendations in a custom AWS Trusted Advisor rule:**
  - **Recommendation Tool:** Provides real-time guidance and recommendations.
  - **Not a Template Solution:** Does not create reusable infrastructure templates.
- **Create an AWS Lambda function which sends emails when it finds misconfigured Amazon RDS databases:**
  - **Reactive Measure:** Sends alerts when misconfigurations are found.
  - **Not Proactive:** Does not prevent misconfigurations or create reusable templates.
- **Attach an IAM policy to interns preventing them from creating an Amazon RDS database:**
  - **Access Control:** Restricts access to specific users.
  - **Not a Comprehensive Solution:** Does not address the need for reusable infrastructure templates for all users.

Conclusion / Points to Memorize:

- **AWS CloudFormation:**
  - Facilitates infrastructure as code.
  - Allows creation of reusable, best practice-compliant templates.
  - Ensures consistency and standardization.
- **AWS Trusted Advisor:**
  - Provides recommendations but does not create reusable templates.
- **AWS Lambda for Misconfiguration Alerts:**
  - Reactive measure, not proactive.
  - Not suitable for template creation.
- **IAM Policy for Access Control:**
  - Limits access but does not ensure best practices or reusable templates.

Question 19 - Correct

Question: A retail company uses AWS Cloud to manage its technology infrastructure. The company has deployed its consumer-focused web application on Amazon EC2-based web servers and uses Amazon RDS PostgreSQL database as the data store. The PostgreSQL database is set up in a private subnet that allows inbound traffic from selected Amazon EC2 instances. The database also uses AWS Key Management Service (AWS KMS) for encrypting data at rest. Which of the following steps would you recommend to facilitate end-to-end security for the data-in-transit while accessing the database?

Correct Option:

- **Configure Amazon RDS to use SSL for data in transit**

Explanation behind Correct Option:

- **SSL/TLS Encryption:**
  - **Secure Connections:** Use Secure Socket Layer (SSL) or Transport Layer Security (TLS) connections to encrypt data in transit.
  - **Automatic Certificate Provisioning:** Amazon RDS creates an SSL certificate and installs it on the DB instance during provisioning.
  - **PostgreSQL Integration:** You can encrypt a PostgreSQL connection between applications and the PostgreSQL DB instances using SSL.
  - **Enforce SSL Connections:** Option to force all connections to use SSL, ensuring end-to-end encryption.

Incorrect Options:

- **Use IAM authentication to access the database instead of the database user's access credentials:**
  - **IAM Authentication:** Allows using AWS Identity and Access Management (IAM) for database authentication without passwords.
  - **Limited Scope:** Does not provide encryption for data in transit, only improves authentication security.
- **Create a new security group that blocks SSH from the selected Amazon EC2 instances into the database:**
  - **Misleading Option:** Amazon RDS instances do not support SSH access, so this is not relevant for securing data in transit.
- **Create a new network access control list (network ACL) that blocks SSH from the entire Amazon EC2 subnet into the database:**
  - **Misleading Option:** Similarly, blocking SSH access via network ACLs is not relevant for RDS instances and does not address data in transit encryption.

Conclusion / Points to Memorize:

- **Amazon RDS SSL/TLS:**

- Encrypts data in transit between applications and the database.
- Automatically provisions and installs SSL certificates.
- Essential for end-to-end security.

- **IAM Authentication:**
  - Enhances user authentication without passwords.
  - Does not encrypt data in transit.
- **Security Groups and Network ACLs:**
  - SSH blocking irrelevant for Amazon RDS.
  - Not related to data encryption in transit.

Question 20 - Correct

Question: A social media company wants the capability to dynamically alter the size of a geographic area from which traffic is routed to a specific server resource. Which feature of Amazon Route 53 can help achieve this functionality?

Correct Option:

- **Geoproximity routing**

Explanation behind Correct Option:

- **Geoproximity Routing:**
  - **Traffic Based on Geographic Location:** Routes traffic to resources based on the geographic location of users and resources.
  - **Bias Adjustment:** Allows for expanding or shrinking the size of the geographic region from which traffic is routed by specifying a bias value.
  - **Positive Bias:** Expands the region (specify an integer from 1 to 99).
  - **Negative Bias:** Shrinks the region (specify a value from -1 to -99).
  - **Dynamic Adjustments:** Enables dynamic alterations to the size of the geographic area for traffic routing.

Incorrect Options:

- **Geolocation Routing:**
  - **Fixed Geographic Routing:** Routes traffic based on the fixed geographic location of users, without the ability to dynamically alter the size of the geographic area.
  - **Use Cases:** Localizing content, restricting content distribution, balancing load predictably.
- **Latency-based Routing:**
  - **Performance Improvement:** Routes traffic to the AWS Region that provides the lowest latency for the user.
  - **Latency Records:** Uses latency records to determine the best region for serving requests.
- **Weighted Routing:**
  - **Traffic Distribution:** Allows distributing traffic across multiple resources by assigning weights.
  - **Use Cases:** Load balancing, testing new versions of software.

Conclusion / Points to Memorize:

- **Geoproximity Routing:**
  - Dynamically adjust the size of geographic areas for routing traffic.
  - Use bias values to expand or shrink regions.
- **Geolocation Routing:**
  - Fixed routing based on user location.
  - Useful for localizing and restricting content.
- **Latency-based Routing:**
  - Improves performance by selecting the region with the lowest latency.
- **Weighted Routing:**
  - Distributes traffic based on assigned weights.
  - Useful for load balancing and software testing.

Question 21 - Correct

An e-commerce company tracks user clicks on its flagship website and performs analytics to provide near-real-time product recommendations. An Amazon EC2 instance receives data from the website and sends the data to an Amazon Aurora Database instance. Another Amazon EC2 instance continuously checks

the changes in the database and executes SQL queries to provide recommendations. Now, the company wants a redesign to decouple and scale the infrastructure. The solution must ensure that data can be analyzed in real-time without any data loss even when the company sees huge traffic spikes.

What would you recommend as an AWS Certified Solutions Architect - Associate?

Overall explanation

Correct option:

Leverage Amazon Kinesis Data Streams to capture the data from the website and feed it into Amazon Kinesis Data Analytics which can query the data in real time. Lastly, the analyzed feed is output into Amazon Kinesis Data Firehose to persist the data on Amazon S3

- Amazon Kinesis Data Streams is designed to capture streaming data and process it in real time. It manages the infrastructure, storage, networking, and configuration needed for data streams.
- Amazon Kinesis Data Analytics processes and analyzes the data in real time. It takes care of running streaming applications continuously and scales automatically based on the volume and throughput of incoming data.
- Amazon Kinesis Data Firehose is used to reliably capture, transform, and deliver streaming data to data lakes, data stores, and analytics services like Amazon S3.
- This combination allows for real-time analysis without data loss, even during traffic spikes, and helps decouple and scale the infrastructure effectively.

Incorrect options:

- **Leverage Amazon Kinesis Data Streams to capture the data from the website and feed it into Amazon QuickSight which can query the data in real time. Lastly, the analyzed feed is output into Kinesis Data Firehose to persist the data on Amazon S3** - Amazon QuickSight cannot use Amazon Kinesis Data Streams as a source and cannot perform real-time streaming data analysis.
- **Leverage Amazon Kinesis Data Streams to capture the data from the website and feed it into Amazon Kinesis Data Firehose to persist the data on Amazon S3. Lastly, use Amazon Athena to analyze the data in real time** - Amazon Athena is not designed for real-time analysis; it is used for interactive querying of data in Amazon S3 using standard SQL.
- **Leverage Amazon SQS to capture the data from the website. Configure a fleet of Amazon EC2 instances under an Auto scaling group to process messages from the Amazon SQS queue and trigger the scaling policy based on the number of pending messages in the queue. Perform real-time analytics using a third-party library on the Amazon EC2 instances** - Although this decouples the architecture, it is not the best fit for real-time analytics. Amazon Kinesis services are better suited for this purpose.

Conclusion / Points to Memorize

- **Amazon Kinesis Data Streams** is used to capture real-time data from various sources.
- **Amazon Kinesis Data Analytics** allows for real-time querying and analysis of streaming data.
- **Amazon Kinesis Data Firehose** delivers streaming data to data lakes, data stores, and analytics services.
    - This setup is ideal for handling unpredictable traffic spikes and ensuring real-time data analysis with minimal changes to the application infrastructure.

Question 22 - Correct

You are working for a software as a service (SaaS) company as a solutions architect and help design solutions for the company's customers. One of the customers is a bank and has a requirement to whitelist a public IP when the bank is accessing external services across the internet.

Which architectural choice do you recommend to maintain high availability, support scaling-up to 10 instances and comply with the bank's requirements?

Correct option:

Use a Network Load Balancer with an Auto Scaling Group

Explanation behind correct option:

1. **Low Latency and High Throughput**: Network Load Balancer (NLB) is suited for low latency and high throughput workloads, capable of handling millions of requests per second.
2. **Layer 4 Operation**: Operates at the connection level (Layer 4), routing connections based on IP protocol data.
3. **Fixed IP Address**: Exposes a fixed IP to the public web, which is crucial for the bank's requirement to whitelist a public IP.
4. **Scalability**: Supports scaling of backend instances using an Auto Scaling Group (ASG) while maintaining a single fixed public IP.

Incorrect options:

1. **Classic Load Balancer with an Auto Scaling Group**
    - **Basic Load Balancing**: Provides basic load balancing at both the request and connection level.
    - **Private IPs**: Uses private IP addresses for forwarding requests, not suitable for the requirement of a fixed public IP.
2. **Application Load Balancer with an Auto Scaling Group**
    - **Layer 7 Operation**: Operates at the request level (Layer 7), ideal for HTTP/HTTPS traffic and advanced request routing.

- **DNS Exposure**: Exposes a fixed DNS (URL) rather than an IP address, not fitting the requirement for a fixed public IP.

3. **Auto Scaling Group with Dynamic Elastic IPs attachment**
   - **Incorrect Feature**: ASG does not support dynamic Elastic IPs attachment, included as a distractor.

Conclusion / Points to Memorize:

1. **NLB for Fixed Public IP**: Use Network Load Balancer when a fixed public IP is needed for whitelisting.
2. **Layer 4 vs. Layer 7**: Understand the difference between Network Load Balancer (Layer 4) and Application Load Balancer (Layer 7) operations.
3. **Scaling and High Availability**: NLB combined with Auto Scaling Group ensures high availability and scalability.
4. **Private vs. Public IPs**: Classic and Application Load Balancers use private IPs for internal traffic, whereas NLB provides a public IP.
5. **Feature Awareness**: Be aware of features and limitations of ASG and load balancers to avoid choosing incorrect options.

Question 23 - Correct

For security purposes, a development team has decided to deploy the Amazon EC2 instances in a private subnet. The team plans to use VPC endpoints so that the instances can access some AWS services securely. The members of the team would like to know about the two AWS services that support Gateway Endpoints.

As a solutions architect, which of the following services would you suggest for this requirement? (Select two)

Correct options:

- **Amazon S3**
- **Amazon DynamoDB**

Explanation behind correct options:

1. **VPC Endpoints**: Enables private connection to supported AWS services without an internet gateway, NAT device, VPN connection, or AWS Direct Connect.
2. **Types of VPC Endpoints**:
   - **Interface Endpoints**: Elastic Network Interface with a private IP address.
   - **Gateway Endpoints**: Gateway specified as a target for a route in your route table.
3. **Supported Services for Gateway Endpoints**:
   - **Amazon S3**
   - **Amazon DynamoDB**

Incorrect options:

1. **Amazon Simple Queue Service (Amazon SQS)**
   - Uses **Interface Endpoints**, not Gateway Endpoints.
2. **Amazon Simple Notification Service (Amazon SNS)**
   - Uses **Interface Endpoints**, not Gateway Endpoints.
3. **Amazon Kinesis**
   - Uses **Interface Endpoints**, not Gateway Endpoints.

Conclusion / Points to Memorize:

1. **Gateway Endpoints**: Only **Amazon S3** and **Amazon DynamoDB** support Gateway Endpoints.
2. **Interface Endpoints**: All other AWS services use Interface Endpoints.
3. **Private Connection**: VPC Endpoints allow secure connections to AWS services without requiring public IP addresses or internet gateways.
4. **Route Table Configuration**: Gateway Endpoints need to be specified as a target in the route table for traffic destined to the supported AWS service.

Question 24 - Correct

A company has noticed that its Amazon EBS Elastic Volume (io1) accounts for 90% of the cost and the remaining 10% cost can be attributed to the Amazon EC2 instance. The Amazon CloudWatch metrics report that both the Amazon EC2 instance and the Amazon EBS volume are under-utilized. The Amazon CloudWatch metrics also show that the Amazon EBS volume has occasional I/O bursts. The entire infrastructure is managed by AWS CloudFormation.

As a Solutions Architect, what do you propose to reduce the costs?

Correct option:

- Convert the Amazon EC2 instance EBS volume to gp2

Explanation behind correct option:

1. **Amazon EBS Volume Types**:
   - **io1 (Provisioned IOPS SSD)**: Designed for I/O-intensive workloads, particularly databases. Provides consistent IOPS rate.

- **gp2 (General Purpose SSD)**: Cost-effective, ideal for a broad range of workloads. Can burst to 3,000 IOPS and scales linearly with volume size.

2. **Cost-Effectiveness**:
   - **gp2 Volumes**: Offer cost-effective storage with single-digit millisecond latencies and burst capabilities, making them suitable for workloads with occasional I/O bursts. More cost-effective than io1.

Incorrect options:

1. **Keep the Amazon EBS volume to io1 and reduce the IOPS**:
   - Reducing IOPS might interfere with the required burst performance, making it an unreliable option.
2. **Change the Amazon EC2 instance type to something much smaller**:
   - Since 90% of the cost is from the EBS volume, changing the EC2 instance type (which accounts for only 10% of the cost) will not significantly reduce overall costs.
3. **Don't use AWS CloudFormation template**:
   - AWS CloudFormation is a free service. Costs are incurred based on the resources created, not by using the CloudFormation service itself.

Conclusion / Points to Memorize:

1. **Amazon EBS Volume Types**:
   - **io1 (Provisioned IOPS SSD)**: High cost, consistent IOPS.
   - **gp2 (General Purpose SSD)**: Cost-effective, burst capability.
2. **Cost Reduction Strategy**:
   - Convert under-utilized io1 volumes to gp2 to reduce costs without compromising on occasional burst performance.
3. **AWS CloudFormation**:
   - AWS CloudFormation itself is free. Costs are from the resources it creates.
4. **Key Metrics**:
   - Monitor Amazon CloudWatch metrics to identify under-utilized resources and optimize costs accordingly.

Question 25 - Incorrect

A developer in your company has set up a classic 2 tier architecture consisting of an Application Load Balancer and an Auto Scaling group (ASG) managing a fleet of Amazon EC2 instances. The Application Load Balancer is deployed in a subnet of size 10.0.1.0/24 and the Auto Scaling group is deployed in a subnet of size 10.0.4.0/22. As a solutions architect, you would like to adhere to the security pillar of the well-architected framework. How do you configure the security group of the Amazon EC2 instances to only allow traffic coming from the Application Load Balancer?

Correct option:

- Add a rule to authorize the security group of the Application Load Balancer

Explanation behind correct option:

1. **Auto Scaling Group (ASG)**:
   - ASG manages a collection of Amazon EC2 instances for automatic scaling and management.
   - Core functionality includes health check replacements and scaling policies.
2. **Security Groups**:
   - Act as virtual firewalls controlling traffic for one or more instances.
   - Rules can allow traffic to or from instances.
   - New rules automatically apply to all associated instances.
   - Characteristics:
     - Default: Allow all outbound traffic.
     - Rules are permissive (can't deny access).
     - Stateful.
3. **Application Load Balancer (ALB)**:
   - Operates at layer 7 (request level).
   - Routes traffic to targets (EC2 instances, containers, IP addresses, Lambda functions) based on request content.
   - Provides advanced routing for HTTP and HTTPS traffic, suitable for modern applications.
4. **Correct Configuration**:
   - Adding a rule to authorize the security group of the Application Load Balancer ensures that only traffic from the ALB reaches the EC2 instances in the ASG.
   - This adheres to the security principle of least privilege.

Incorrect options:

1. **Add a rule to authorize the CIDR 10.0.4.0/22**:
   - Broadly authorizes traffic from the entire subnet, not just the ALB, potentially exposing instances to unwanted traffic.
2. **Add a rule to authorize the security group of the Auto Scaling group**:
   - Incorrectly targets the ASG itself rather than the ALB, not addressing the source of incoming traffic.
3. **Add a rule to authorize the CIDR 10.0.1.0/24**:
   - Similar to the first incorrect option, it allows traffic from the entire subnet, not specifically from the ALB.

Conclusion / Points to Memorize:

1. **Security Group Rules**:
   - Use security groups to control traffic, not broad CIDR ranges.
   - Ensure rules allow specific, required traffic only.
2. **Load Balancers and Security**:
   - Authorize traffic from the security group of the load balancer to enhance security.
3. **Well-Architected Framework Security Pillar**:
   - Adhere to the principle of least privilege.
   - Use specific, narrowly-scoped rules to control access.
4. **Auto Scaling and Load Balancing**:
   - Understand the roles of ASGs and ALBs in scaling and routing traffic.
   - Configure security groups to support these roles securely.

Question 26 - Incorrect

A CRM web application was written as a monolith in PHP and is facing scaling issues because of performance bottlenecks. The CTO wants to re-engineer towards microservices architecture and expose their application from the same load balancer, linked to different target groups with different URLs: checkout.mycorp.com, www.mycorp.com, yourcorp.com/profile and yourcorp.com/search. The CTO would like to expose all these URLs as HTTPS endpoints for security purposes. As a solutions architect, which of the following would you recommend as a solution that requires MINIMAL configuration effort?

Correct option:

- Use Secure Sockets Layer certificate (SSL certificate) with SNI

Explanation behind correct option:

1. **Secure Sockets Layer (SSL) Certificate with SNI**:
   - **SNI (Server Name Indication)** allows hosting multiple TLS secured applications behind a single load balancer.
   - Multiple certificates can be bound to the same secure listener on the load balancer.
   - ALB (Application Load Balancer) automatically selects the optimal TLS certificate for each client.
   - This method supports different domain names efficiently.
   - SNI support enables the use of more than one certificate with the same ALB.
   - Benefits:
     - Handles different domains with the same load balancer.
     - Avoids limitations of wildcard and SAN certificates.
     - Eliminates the need to reauthenticate and reprovision certificates when adding new domains.

Incorrect options:

1. **Use a wildcard Secure Sockets Layer certificate (SSL certificate)**:
   - Wildcard certificates only work for related subdomains matching a simple pattern.
   - Not suitable for different domain names such as checkout.mycorp.com and yourcorp.com/profile.
2. **Use an HTTP to HTTPS redirect**:
   - This approach does not provide multiple secure endpoints for different URLs.
   - Only redirects HTTP requests to HTTPS, does not address the requirement for different secure endpoints.
3. **Change the Elastic Load Balancing (ELB) SSL Security Policy**:
   - Changing the SSL Security Policy does not provide multiple secure endpoints.
   - Only adjusts the security protocols and ciphers used, not suitable for managing multiple domain certificates.

Conclusion / Points to Memorize:

1. **Server Name Indication (SNI)**:

- Essential for hosting multiple TLS-secured applications with different domain names behind a single load balancer.
- Allows binding multiple certificates to a single secure listener.

2. **Certificate Management**:
   - Understand the limitations of wildcard and SAN certificates.
   - SNI provides flexibility and scalability in handling multiple domains.
3. **Load Balancer Configuration**:
   - ALB can automatically choose the best certificate when using SNI.
   - Simplifies certificate management and scaling for microservices architectures.
4. **Security**:
   - Ensures secure endpoints for all URLs without extensive configuration.
   - Adheres to best practices for managing SSL/TLS certificates in a dynamic environment.

Question 27 - Correct

A company has grown from a small startup to an enterprise employing over 1000 people. As the team size has grown, the company has recently observed some strange behavior, with Amazon S3 buckets settings being changed regularly. How can you figure out what's happening without restricting the rights of the users?

Correct option:

- Use AWS CloudTrail to analyze API calls

Explanation behind correct option:

1. **Use AWS CloudTrail to analyze API calls**:
   - **AWS CloudTrail** provides governance, compliance, operational auditing, and risk auditing.
   - Logs, continuously monitors, and retains account activity related to actions across AWS infrastructure.
   - Provides event history of AWS account activity, including actions taken through:
     - AWS Management Console
     - AWS SDKs
     - Command-line tools
     - Other AWS services
   - Recommended for logging bucket and object-level actions for Amazon S3 resources.
   - Enables detailed tracking of API calls to understand who is changing S3 bucket settings and when.

Incorrect options:

1. **Implement an IAM policy to forbid users to change Amazon S3 bucket settings**:
   - Restricting user permissions through IAM policies would be disruptive.
   - Users would notice and potentially be hindered in their work.
2. **Use Amazon S3 access logs to analyze user access using Athena**:
   - Amazon S3 server access logging provides records for requests made to a bucket.
   - Useful for security and access audits, learning about customer base, and understanding billing.
   - AWS recommends using AWS CloudTrail for logging bucket and object-level actions for more comprehensive tracking.
3. **Implement a bucket policy requiring AWS Multi-Factor Authentication (AWS MFA) for all operations**:
   - MFA provides an extra level of security but is not suitable for analyzing current activity.
   - Changing the bucket policy to require MFA would be noticed by users and could disrupt their workflow.

Conclusion / Points to Memorize:

1. **AWS CloudTrail**:
   - Best tool for detailed analysis of API calls and actions across AWS services.
   - Provides comprehensive logging and monitoring capabilities.
2. **Event History and API Call Analysis**:
   - CloudTrail logs provide detailed information about actions taken by users, roles, and AWS services.
   - Essential for understanding changes to resources like S3 bucket settings.
3. **Non-Disruptive Monitoring**:
   - CloudTrail allows monitoring and analysis without changing user permissions or policies.
   - Ensures continuous operation and security without impacting user activities.

4. **Complementary Tools**:
    - While IAM policies, S3 access logs, and MFA are useful for security and access control, CloudTrail is the primary tool for auditing and analyzing API activities.

Question 28 - Incorrect

A company has recently created a new department to handle their services workload. An IT team has been asked to create a custom VPC to isolate the resources created in this new department. They have set up the public subnet and internet gateway (IGW). However, they are not able to ping the Amazon EC2 instances with elastic IP address (EIP) launched in the newly created VPC. As a Solutions Architect, the team has requested your help. How will you troubleshoot this scenario? (Select two)

Correct options:

- Check if the route table is configured with internet gateway
- Check if the security groups allow ping from the source

Explanation behind correct options:

1. **Check if the route table is configured with internet gateway**:
    - **Internet Gateway (IGW)**: A horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet.
    - **Route Table Configuration**:
        - Attach an internet gateway to your VPC.
        - Add a route to your subnet's route table that directs internet-bound traffic to the internet gateway.
        - Ensure instances have a globally unique IP address.
        - Verify network access control lists (ACLs) and security group rules allow relevant traffic.
2. **Check if the security groups allow ping from the source**:
    - **Security Group**: Acts as a virtual firewall controlling traffic for one or more instances.
    - **Security Group Rules**:
        - Allow traffic to or from its associated instances.
        - By default, security groups allow all outbound traffic.
        - Rules are always permissive and stateful.
    - Ensure the security group allows the ICMP protocol for ping requests.

Incorrect options:

1. **Disable Source / Destination check on the Amazon EC2 instance**:
    - **Source/Destination Check**: Controls whether source/destination checking is enabled on the instance.
    - Disabling is relevant for instances handling network traffic not specifically destined for the instance (e.g., NAT, routing, firewall).
    - Not relevant to the scenario of enabling ping.
2. **Create a secondary internet gateway to attach with public subnet and move the current internet gateway to private and write route tables**:
    - No concept of a secondary IGW.
    - Incorrect and misleading option.
3. **Contact AWS support to map your VPC with subnet**:
    - AWS support cannot map VPCs with subnets.
    - Not a viable troubleshooting step.

Conclusion / Points to Memorize:

1. **Internet Gateway (IGW) and Route Table Configuration**:
    - Attach IGW to VPC and configure route tables to direct traffic to IGW.
2. **Security Groups**:
    - Ensure security groups allow the necessary traffic, including ICMP for ping requests.
3. **Network Access Control**:
    - Verify network ACLs and security group rules.
4. **Common Misconceptions**:
    - No secondary IGWs.
    - AWS support does not map VPCs with subnets.
    - Source/Destination check is not relevant for enabling ping.

Question 29 - Correct

As a solutions architect, you have created a solution that utilizes an Application Load Balancer with stickiness and an Auto Scaling Group (ASG). The Auto Scaling Group spans across 2 Availability Zones (AZs). AZ-A has 3 Amazon EC2 instances and AZ-B has 4 Amazon EC2 instances. The Auto Scaling Group is about to go into a scale-in event due to the triggering of an Amazon CloudWatch alarm.

What will happen under the default Auto Scaling Group configuration?

Correct option:

- The instance with the oldest launch template or launch configuration will be terminated in AZ-B

Explanation behind correct options:

1. **Amazon EC2 Auto Scaling**:
   - Ensures you have the correct number of Amazon EC2 instances to handle the load for your application.
   - Auto Scaling groups can specify minimum and maximum number of instances.
   - Scaling out adds instances, scaling in removes instances.
2. **Default Termination Policy**:
   - Designed to ensure instances span Availability Zones (AZs) evenly for high availability.
   - Steps for termination:
     1. **Determine AZ with the most instances**:
        - Identify AZ with the most instances and at least one instance not protected from scale-in.
     2. **Align remaining instances to allocation strategy**:
        - Ensure remaining instances match the allocation strategy for the terminating instance (On-Demand or Spot).
     3. **Identify oldest launch template or configuration**:
        - For launch templates, identify instances using the oldest template.
        - For launch configurations, identify instances using the oldest configuration.
     4. **Select instance closest to the next billing hour**:
        - If multiple unprotected instances exist, choose the one closest to the next billing hour to maximize usage.

Incorrect options:

1. **A random instance in the AZ-A will be terminated**:
   - Does not follow the policy of balancing instances across AZs.
2. **An instance in the AZ-A will be created**:
   - Incorrect, as the question pertains to a scale-in event, not scaling out.
3. **A random instance will be terminated in AZ-B**:
   - Termination is based on the oldest launch template or configuration, not random selection.

Conclusion / Points to Memorize:

1. **Auto Scaling Group (ASG)**:
   - Manages scaling events to maintain desired instance count.
   - Ensures high availability by distributing instances across AZs.
2. **Default Termination Policy**:
   - Balances instances across AZs.
   - Terminates instances with the oldest launch template or configuration first.
   - Considers billing hour to maximize instance usage.
3. **Scaling Events**:
   - **Scaling out**: Adding instances.
   - **Scaling in**: Removing instances based on the termination policy.
4. **Application Load Balancer (ALB)**:
   - Distributes traffic across instances.
   - Stickiness ensures session persistence.

Question 30:

A healthcare company is evaluating storage options on Amazon S3 to meet regulatory guidelines. The data should be stored in such a way on Amazon S3 that it cannot be deleted until the regulatory time period has expired.

Correct Option:

- **Use Amazon S3 Object Lock**

Explanation Behind Correct Option:

1. **Amazon S3 Object Lock:**
   - Allows you to store objects using a Write Once, Read Many (WORM) model.
   - Helps prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely.
   - Meets regulatory requirements for compliance by ensuring data cannot be altered or deleted during the specified retention period.
   - Offers two ways to manage object retention:
     - **Retention Period:** Specifies a fixed period during which an object remains locked.
     - **Legal Hold:** Provides the same protection as a retention period but without an expiration date.
   - Object Lock works only in versioned buckets and applies to individual object versions.

Incorrect Options:

1. **Use Amazon S3 Glacier Vault Lock:**
   - Glacier Vault Lock is used for Amazon S3 Glacier, not Amazon S3.
   - Suitable for long-term archiving but not applicable for real-time data compliance needs in Amazon S3.
2. **Activate AWS Multi-Factor Authentication (AWS MFA) delete on the Amazon S3 bucket:**
   - MFA delete provides an extra security layer requiring MFA for delete operations.
   - Can be disabled by users with root access, hence not foolproof for regulatory compliance.
3. **Use Amazon S3 cross-region replication (S3 CRR):**
   - Replicates objects across Amazon S3 buckets automatically.
   - Does not prevent deletion of objects if replication is disabled.
   - Suitable for data redundancy but not for compliance to prevent deletion.

Conclusion / Points to Memorize:

1. **S3 Object Lock:**
   - WORM model ensures data cannot be deleted or modified.
   - Retention Period and Legal Hold for regulatory compliance.
2. **Glacier Vault Lock:**
   - For long-term archiving in S3 Glacier, not suitable for real-time S3 compliance.
3. **MFA Delete:**
   - Adds a security layer, not absolute for regulatory needs.
4. **S3 Cross-Region Replication:**
   - Useful for redundancy, not for preventing deletions under compliance needs.

Question 31 - Incorrect:

Your company runs a web portal to match developers to clients who need their help. As a solutions architect, you've designed the architecture of the website to be fully serverless with Amazon API Gateway and AWS Lambda. The backend uses Amazon DynamoDB table. You would like to automatically congratulate your developers on important milestones, such as - their first paid contract. All the contracts are stored in Amazon DynamoDB. Which Amazon DynamoDB feature can you use to implement this functionality such that there is LEAST delay in sending automatic notifications?

Correct Option:

- **Amazon DynamoDB Streams + AWS Lambda**

Explanation Behind Correct Option:

1. **Amazon DynamoDB Streams + AWS Lambda:**
   - **Amazon DynamoDB Streams:** Provides an ordered flow of information about changes to items in a DynamoDB table.
   - Captures information about every modification to data items (creates, updates, deletes).
   - Writes a stream record with primary key attributes of the modified items.
   - **AWS Lambda:** Can be triggered by DynamoDB Streams to execute code in response to the changes.
   - Minimal delay in triggering Lambda functions for real-time processing.
   - Ideal for sending notifications based on data changes without additional setup or delay.

Incorrect Options:

1. **Amazon DynamoDB DAX + Amazon API Gateway:**

- **DynamoDB Accelerator (DAX):** In-memory cache for DynamoDB, improving read performance.
- **Amazon API Gateway:** Deploys APIs at scale.
- Not suited for real-time change notifications; DAX is for read performance enhancement.

2. **Amazon Simple Queue Service (SQS) + AWS Lambda:**
   - **Amazon SQS:** Fully managed message queuing service.
   - Requires additional logic to send messages to SQS from DynamoDB.
   - Adds complexity and delay compared to direct use of DynamoDB Streams.
3. **Amazon EventBridge events + AWS Lambda:**
   - **EventBridge:** Event bus for integrating AWS services.
   - Does not support DynamoDB as a direct target for events.
   - Not applicable for directly triggering notifications based on DynamoDB changes.

Conclusion / Points to Memorize:

1. **Amazon DynamoDB Streams + AWS Lambda:**
   - Best for real-time processing and notifications based on changes in DynamoDB.
   - Direct integration ensures minimal delay.
2. **Amazon DynamoDB DAX:**
   - Enhances read performance, not suitable for change notifications.
3. **Amazon Simple Queue Service (SQS):**
   - Useful for decoupling and scaling but requires additional logic for notifications.
4. **Amazon EventBridge:**
   - Event bus not directly compatible with DynamoDB for the given use case.

Question 32 - Correct:

A systems administrator is creating IAM policies and attaching them to IAM identities. After creating the necessary identity-based policies, the administrator is now creating resource-based policies. Which is the only resource-based policy that the IAM service supports?

Correct Option:

- **Trust policy**

Explanation Behind Correct Option:

1. **Trust policy:**
   - Defines which principal entities (accounts, users, roles, and federated users) can assume the role.
   - An IAM role is both an identity and a resource that supports resource-based policies.
   - Requires both a trust policy and an identity-based policy to be attached to an IAM role.
   - IAM service supports trust policies as resource-based policies, specifically for IAM roles.

Incorrect Options:

1. **Access control list (ACL):**
   - ACLs control which principals in another account can access a resource.
   - Cannot be used to control access for a principal within the same account.
   - Used in services like Amazon S3, AWS WAF, and Amazon VPC.
2. **Permissions boundary:**
   - Advanced feature for using a managed policy to set the maximum permissions for an IAM entity.
   - Applies to IAM users or roles.
   - Defines the maximum actions allowed, but is not considered a resource-based policy.
3. **AWS Organizations Service Control Policies (SCP):**
   - Applied to any or all accounts within an AWS organization.
   - Limits permissions for entities in member accounts.
   - Acts as a guardrail for maximum permissions but is not a resource-based policy for individual resources.

Conclusion / Points to Memorize:

1. **Trust Policy:**
   - Only resource-based policy supported by IAM.
   - Defines which principals can assume an IAM role.

- Essential for configuring roles within IAM.

2. **Access Control List (ACL):**
   - Used for cross-account resource access control.
   - Applicable to services like Amazon S3, AWS WAF, and Amazon VPC.
3. **Permissions Boundary:**
   - Sets maximum permissions for IAM users or roles.
   - Works in conjunction with identity-based policies.
4. **AWS Organizations Service Control Policies (SCP):**
   - Limits permissions for accounts within an AWS organization.
   - Acts at the organization or organizational unit (OU) level.

Question 33 - Correct:

The engineering team at a leading e-commerce company is anticipating a surge in the traffic because of a flash sale planned for the weekend. You have estimated the web traffic to be 10x. The content of your website is highly dynamic and changes very often. As a Solutions Architect, which of the following options would you recommend to make sure your infrastructure scales for that day?

Correct Option:

- **Use an Auto Scaling Group**

Explanation Behind Correct Option:

1. **Auto Scaling Group (ASG):**
   - **Automatic Scaling:** ASG manages a collection of Amazon EC2 instances as a logical group for automatic scaling and management.
   - **Desired Capacity:** You can set the desired number of instances, and ASG will automatically adjust to meet demand.
   - **Health Checks:** Performs periodic health checks and replaces unhealthy instances.
   - **Scaling Policies:** Supports both manual and automatic scaling based on demand.
   - **Dynamic Content:** Suitable for highly dynamic websites that need to scale rapidly in response to traffic surges.

Incorrect Options:

1. **Use an Amazon CloudFront distribution in front of your website:**
   - **Content Delivery Network (CDN):** CloudFront improves performance by caching content at edge locations worldwide.
   - **Caching Issue:** Not suitable for highly dynamic content as it caches files, which could lead to outdated content being served.
2. **Deploy the website on Amazon S3:**
   - **Static Content Hosting:** S3 is designed for hosting static websites with static content.
   - **Dynamic Content Limitation:** Cannot host dynamic applications, making it unsuitable for the given scenario.
3. **Use an Amazon Route 53 Multi Value record:**
   - **DNS Service:** Route 53 is a DNS web service that provides routing policies like Multi Value answer routing.
   - **Scaling Limitation:** Does not assist in scaling the actual infrastructure or handling dynamic content.

Conclusion / Points to Memorize:

1. **Auto Scaling Group (ASG):**
   - Ideal for managing dynamic scaling needs.
   - Automatically adjusts the number of EC2 instances based on traffic demands.
   - Ensures high availability by performing health checks and replacing unhealthy instances.
2. **Amazon CloudFront:**
   - Best for static content delivery and improving performance via edge caching.
   - Not suitable for highly dynamic content due to caching.
3. **Amazon S3:**
   - Suitable for static website hosting.
   - Cannot host dynamic content or handle application scaling.
4. **Amazon Route 53:**
   - Used for DNS management and routing policies.
   - Does not provide infrastructure scaling capabilities.

Question 34 - Correct:

A company runs a popular dating website on the AWS Cloud. As a Solutions Architect, you've designed the architecture of the website to follow a serverless pattern on the AWS Cloud using Amazon API Gateway and AWS Lambda. The backend uses an Amazon RDS PostgreSQL database. Currently, the application uses a username and password combination to connect the AWS Lambda function to the Amazon RDS database. You would like to improve the security at the authentication level by leveraging short-lived credentials. What will you choose? (Select two)

Correct Options:

- **Use IAM authentication from AWS Lambda to Amazon RDS PostgreSQL**
- **Attach an AWS Identity and Access Management (IAM) role to AWS Lambda**

Explanation Behind Correct Options:

1. **Use IAM authentication from AWS Lambda to Amazon RDS PostgreSQL:**
   - **IAM Database Authentication:** Allows authentication to your database instance using AWS IAM. Works with MySQL and PostgreSQL.
   - **Authentication Token:** Uses tokens generated using AWS Signature Version 4, which are valid for 15 minutes, eliminating the need for passwords.
   - **Centralized Management:** Enables central management of database access using IAM.
   - **Encryption:** Ensures network traffic to and from the database is encrypted using SSL.
2. **Attach an AWS Identity and Access Management (IAM) role to AWS Lambda:**
   - **IAM Role Attachment:** Allows the Lambda function to assume a role with the necessary permissions to access the RDS database.
   - **Enhanced Security:** IAM roles provide secure, short-lived credentials for accessing AWS resources, improving overall security.

Incorrect Options:

1. **Embed a credential rotation logic in the AWS Lambda, retrieving them from SSM:**
   - **SSM Parameter Store:** While SSM provides secure storage for configuration data and secrets, embedding rotation logic in Lambda is overly complex and not the most efficient solution for this scenario.
2. **Restrict the Amazon RDS database security group to the AWS Lambda's security group:**
   - **Security Group Restriction:** Improves security but does not address the need for short-lived credentials at the authentication level.
3. **Deploy AWS Lambda in a VPC:**
   - **Lambda in VPC:** Enhances network security by controlling Lambda's access to VPC resources but does not change the authentication mechanism.

Conclusion / Points to Memorize:

1. **IAM Database Authentication:**
   - Use IAM to manage database access with authentication tokens instead of passwords.
   - Tokens are short-lived and generated using AWS Signature Version 4.
   - Provides centralized access management and SSL encryption.
2. **IAM Roles for Lambda:**
   - Attach IAM roles to Lambda functions to provide secure, short-lived access credentials.
   - Improves security by eliminating the need to hard-code credentials.
3. **Security Group Restrictions and VPC Deployment:**
   - Improve network security but do not address authentication mechanism changes.
   - Important for overall security architecture but not specifically for authentication improvements.

Question 35 - Correct:

An Elastic Load Balancer has marked all the Amazon EC2 instances in the target group as unhealthy. Surprisingly, when a developer enters the IP address of the Amazon EC2 instances in the web browser, he can access the website. What could be the reason the instances are being marked as unhealthy? (Select two)

Correct Options:

- **The security group of the Amazon EC2 instance does not allow for traffic from the security group of the Application Load Balancer**
- **The route for the health check is misconfigured**

Explanation Behind Correct Options:

1. **The security group of the Amazon EC2 instance does not allow for traffic from the security group of the Application Load Balancer:**
   - **Security Group Configuration:** The security groups associated with the EC2 instances must allow traffic from the security group associated with the Application Load Balancer (ALB).
   - **Health Check Communication:** ALB sends health check requests to its registered targets. If the security group of the EC2 instances blocks traffic from the ALB's security group, the health checks will fail, marking the instances as unhealthy.
2. **The route for the health check is misconfigured:**

- **Health Check Route:** ALB requires a specific route for health checks to determine the health of instances. Misconfiguration in the health check path can result in ALB marking instances as unhealthy.
- **Health Check Settings:** Ensure the health check settings in the ALB target group are correctly configured to match the expected route on the EC2 instances.

Incorrect Options:

1. **The Amazon Elastic Block Store (Amazon EBS) volumes have been improperly mounted:**
   - **EBS Volume Mounting:** If the developer can access the website via IP address, it indicates that the EBS volumes are properly mounted and functional. Thus, this is not the reason for health check failures.
2. **Your web-app has a runtime that is not supported by the Application Load Balancer:**
   - **Web App Runtime:** ALB operates at Layer 7 (HTTP/HTTPS) and is independent of the web application's runtime environment. Therefore, the web app runtime does not affect the ALB's ability to mark instances as healthy or unhealthy.
3. **You need to attach elastic IP address (EIP) to the Amazon EC2 instances:**
   - **Elastic IPs:** EIPs are not required for instances behind an ALB. ALB can route traffic to EC2 instances using private IPs. Hence, attaching EIPs is irrelevant in this context.

Conclusion / Points to Memorize:

1. **Security Group Configuration:**
   - Ensure EC2 instance security groups allow traffic from the ALB's security group, particularly for health check ports.
   - Verify inbound rules to allow communication on required ports (e.g., HTTP, HTTPS).
2. **Health Check Configuration:**
   - Confirm the correct health check path is configured in the ALB target group settings.
   - Ensure the health check path on the EC2 instances is accessible and responds correctly.
3. **General ALB Configuration:**
   - ALB operates at Layer 7, handling HTTP/HTTPS traffic independently of the web application's runtime environment.
   - EIPs are not necessary for EC2 instances behind an ALB.

Question 36 - Correct:

An IT company has a large number of clients opting to build their application programming interface (API) using Docker containers. To facilitate the hosting of these containers, the company is looking at various orchestration services available with AWS. As a Solutions Architect, which of the following solutions will you suggest? (Select two)

Correct Options:

- **Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate for serverless orchestration of the containerized services**
- **Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate for serverless orchestration of the containerized services**

Explanation Behind Correct Options:

1. **Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate for serverless orchestration of the containerized services:**
   - **Amazon EKS:** Fully managed Kubernetes service to run Kubernetes on AWS without needing to install and operate your own Kubernetes control plane or nodes.
   - **AWS Fargate:** Serverless compute engine for containers that works with both Amazon ECS and Amazon EKS. It allows you to run containers without having to manage the underlying infrastructure.
   - **Benefits:** Combines Kubernetes with serverless to provide a highly scalable, efficient, and cost-effective solution for managing containerized applications.
2. **Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate for serverless orchestration of the containerized services:**
   - **Amazon ECS:** Fully managed container orchestration service. You can deploy, manage, and scale containerized applications.
   - **AWS Fargate:** Provides a serverless infrastructure to run containers. It eliminates the need to manage server instances.
   - **Benefits:** Simplifies running containerized workloads by removing the need to manage infrastructure and allows focus on application development.

Incorrect Options:

1. **Use Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 for serverless orchestration of the containerized services:**
   - **Amazon EC2:** Requires managing and provisioning instances, which contradicts the serverless requirement.
   - **Reason:** While ECS can run on EC2, it is not considered a serverless solution because you still need to manage the underlying EC2 instances.
2. **Use Amazon EMR for serverless orchestration of the containerized services:**
   - **Amazon EMR:** Service for processing vast amounts of data using Hadoop framework on EC2 and S3.

- **Reason:** EMR is designed for big data processing and is not suitable for orchestrating Docker containers.

3. **Use Amazon SageMaker for serverless orchestration of the containerized services:**
   - **Amazon SageMaker:** Service for building, training, and deploying machine learning models.
   - **Reason:** SageMaker is not a container orchestration service and is not suitable for managing Docker containerized applications.

Conclusion / Points to Memorize:

1. **Amazon ECS and EKS with AWS Fargate:**
   - Ideal for serverless orchestration of Docker containers.
   - Fargate eliminates the need to manage the underlying infrastructure, offering a true serverless experience.
2. **Amazon ECS with EC2:**
   - Not serverless; requires managing EC2 instances.
3. **Amazon EMR and SageMaker:**
   - Not suitable for Docker container orchestration.
   - EMR is for big data processing; SageMaker is for machine learning.

Question 37 - Correct:

The engineering team at an e-commerce company has been tasked with migrating to a serverless architecture. The team wants to focus on the key points of consideration when using AWS Lambda as a backbone for this architecture. As a Solutions Architect, which of the following options would you identify as correct for the given requirement? (Select three)

Correct Options:

- **By default, AWS Lambda functions always operate from an AWS-owned VPC and hence have access to any public internet address or public AWS APIs. Once an AWS Lambda function is VPC-enabled, it will need a route through a Network Address Translation gateway (NAT gateway) in a public subnet to access public resources**
- **Since AWS Lambda functions can scale extremely quickly, it's a good idea to deploy an Amazon CloudWatch Alarm that notifies your team when function metrics such as ConcurrentExecutions or Invocations exceeds the expected threshold**
- **If you intend to reuse code in more than one AWS Lambda function, you should consider creating an AWS Lambda Layer for the reusable code**

Explanation Behind Correct Options:

1. **By default, AWS Lambda functions always operate from an AWS-owned VPC and hence have access to any public internet address or public AWS APIs. Once an AWS Lambda function is VPC-enabled, it will need a route through a Network Address Translation gateway (NAT gateway) in a public subnet to access public resources:**
   - **AWS Lambda:** Operates from an AWS-owned VPC by default, which allows access to public internet addresses and public AWS APIs.
   - **VPC-Enabled Lambda:** When a Lambda function is configured to run within a VPC, it requires a NAT gateway to access the internet or other public resources.
   - **Reason:** This ensures secure and controlled access to private resources within a VPC.
2. **Since AWS Lambda functions can scale extremely quickly, it's a good idea to deploy an Amazon CloudWatch Alarm that notifies your team when function metrics such as ConcurrentExecutions or Invocations exceeds the expected threshold:**
   - **AWS Lambda Scaling:** Can scale up rapidly based on the demand.
   - **CloudWatch Alarms:** Useful to monitor function metrics like ConcurrentExecutions or Invocations to manage and respond to scaling events.
   - **Reason:** Helps in proactive monitoring and management to avoid unexpected costs and performance issues.
3. **If you intend to reuse code in more than one AWS Lambda function, you should consider creating an AWS Lambda Layer for the reusable code:**
   - **AWS Lambda Layers:** A feature that allows you to include additional code and content (like libraries or dependencies) that can be used across multiple Lambda functions.
   - **Benefits:** Reduces redundancy, keeps deployment packages smaller, and simplifies updates.
   - **Reason:** Promotes code reuse and efficient management of dependencies.

Incorrect Options:

1. **AWS Lambda allocates compute power in proportion to the memory you allocate to your function. AWS, thus recommends to over provision your function time out settings for the proper performance of AWS Lambda functions:**
   - **Memory Allocation:** AWS Lambda allocates compute power based on the memory allocated.
   - **Reason Incorrect:** AWS recommends understanding the performance requirements and setting appropriate timeouts, not over-provisioning function timeout settings, as this can lead to unnecessary costs.

2. **The bigger your deployment package, the slower your AWS Lambda function will cold-start. Hence, AWS suggests packaging dependencies as a separate package from the actual AWS Lambda package:**
   - **Deployment Package:** Larger packages can affect cold start times.
   - **Reason Incorrect:** AWS suggests using Lambda Layers to manage dependencies and keep the deployment package smaller, not creating separate packages.
3. **Serverless architecture and containers complement each other but you cannot package and deploy AWS Lambda functions as container images:**
   - **Containers and Lambda:** AWS Lambda now supports packaging and deploying functions as container images.
   - **Reason Incorrect:** The statement is outdated and incorrect, as Lambda functions can be packaged as container images.

Conclusion / Points to Memorize:

1. **AWS Lambda VPC Integration:**
   - Default operation from an AWS-owned VPC.
   - Requires NAT gateway for internet access when VPC-enabled.
2. **AWS Lambda Monitoring and Scaling:**
   - Use CloudWatch Alarms for critical function metrics.
   - Monitor for spikes in concurrency and invocations.
3. **AWS Lambda Code Management:**
   - Use Lambda Layers for reusable code.
   - Keep deployment packages small for efficient performance.

Question 38 - Correct

The engineering team at a social media company has recently migrated to AWS Cloud from its on-premises data center. The team is evaluating Amazon CloudFront to be used as a CDN for its flagship application. The team has hired you as an AWS Certified Solutions Architect – Associate to advise on Amazon CloudFront capabilities on routing, security, and high availability.

Which of the following would you identify as correct regarding Amazon CloudFront?(Select three)

Correct Options

1. **Amazon CloudFront can route to multiple origins based on the content type**
2. **Use an origin group with primary and secondary origins to configure Amazon CloudFront for high-availability and failover**
3. **Use field level encryption in Amazon CloudFront to protect sensitive data for specific content**

Explanation Behind Correct Options

1. **Amazon CloudFront can route to multiple origins based on the content type**
   - Amazon CloudFront can be configured to serve different types of requests from multiple origins within a single web distribution. This is useful for websites serving static content from Amazon S3 and dynamic content from a load balancer.
   - **Key Point:** Supports routing based on content type.
2. **Use an origin group with primary and secondary origins to configure Amazon CloudFront for high-availability and failover**
   - You can set up CloudFront with origin failover by creating an origin group with two origins: primary and secondary. If the primary origin fails, CloudFront will automatically switch to the secondary origin.
   - **Key Point:** Ensures high availability and automatic failover.
3. **Use field level encryption in Amazon CloudFront to protect sensitive data for specific content**
   - Field-level encryption allows encryption of sensitive information provided by users at the edge. This ensures that only applications with the necessary credentials can decrypt and access the data.
   - **Key Point:** Provides additional security for sensitive data.

Incorrect Options

1. **Use AWS Key Management Service (AWS KMS) encryption in Amazon CloudFront to protect sensitive data for specific content**
   - **Reason:** AWS KMS is not used for protecting sensitive data in CloudFront. Field-level encryption should be used instead.
2. **Use geo restriction to configure Amazon CloudFront for high-availability and failover**
   - **Reason:** Geo restriction is used to block access from specific geographic locations, not for configuring high availability or failover.
3. **Amazon CloudFront can route to multiple origins based on the price class**
   - **Reason:** CloudFront price classes determine the geographic regions where content is served from, but routing to multiple origins is based on content type, not price class.

Conclusion / Points to Memorize

- **Routing Capabilities:** CloudFront can route requests to different origins based on content type.
- **High Availability:** Use origin groups with primary and secondary origins to ensure high availability and automatic failover.
- **Security:** Use field-level encryption to protect sensitive data at the edge.
- **Geo Restriction:** Useful for blocking access based on geographic location, but not for high availability.
    - **Price Classes:** Determine the geographic regions for serving content, not for routing based on origins.

Question 39 - Incorrect

A mobile gaming company is experiencing heavy read traffic to its Amazon Relational Database Service (Amazon RDS) database that retrieves player's scores and stats. The company is using an Amazon RDS database instance type that is not cost-effective for their budget. The company would like to implement a strategy to deal with the high volume of read traffic, reduce latency, and also downsize the instance size to cut costs.

Which of the following solutions do you recommend?

Correct Option

- **Setup Amazon ElastiCache in front of Amazon RDS**

Explanation Behind Correct Option

- **Setup Amazon ElastiCache in front of Amazon RDS**
    - Amazon ElastiCache is a caching service that can significantly improve the performance of read-heavy applications by reducing the load on the database.
    - It provides a high-performance, low-latency middle tier for applications, which can handle high request rates.
    - **Key Points:**
        - Reduces latency by caching frequent read requests.
        - Helps in downsizing the RDS instance as it offloads the read traffic.
        - Minimally invasive and cost-effective solution for scaling applications.

Incorrect Options

1. **Setup Amazon RDS Read Replicas**
    - Adding read replicas would distribute the read load but also increase overall costs due to additional RDS instances.
    - It does not provide the latency benefits that a caching solution like ElastiCache offers.
    - **Reason:** Increases database costs without significantly reducing latency.
2. **Move to Amazon Redshift**
    - Amazon Redshift is a data warehousing solution optimized for large datasets and complex queries, not suitable for the operational database requirements of a gaming application.
    - It is not cost-effective for smaller, real-time read operations compared to RDS.
    - **Reason:** Not designed for operational workloads and may not be cost-effective.
3. **Switch application code to AWS Lambda for better performance**
    - AWS Lambda is a serverless compute service, useful for running code in response to events, but does not directly address the high read traffic to the database.
    - Data still needs to be read from RDS, so a caching solution is more appropriate.
    - **Reason:** Does not solve the read traffic issue on the database.

Conclusion / Points to Memorize

- **Caching Solutions:** Use Amazon ElastiCache to reduce read latency and offload traffic from RDS.
- **Cost Efficiency:** ElastiCache helps in downsizing RDS instances, making the solution cost-effective.
- **Read Replicas vs Caching:** Read replicas distribute the load but do not reduce latency as effectively as caching.
- **Service Suitability:** Understand the appropriate use cases for services like Amazon Redshift (data warehousing) and AWS Lambda (event-driven compute) to avoid misapplication.
    - **Application Performance:** Caching frequently accessed data significantly improves application performance and scalability.

Question 40 - Correct

The engineering team at a global e-commerce company is currently reviewing their disaster recovery strategy. The team has outlined that they need to be able to quickly recover their application stack with a Recovery Time Objective (RTO) of 5 minutes in all of the AWS Regions that the application runs. The application stack currently takes over 45 minutes to install on a Linux system.

As a Solutions Architect, which of the following options would you recommend as the disaster recovery strategy?

Correct Option

- **Create an Amazon Machine Image (AMI) after installing the software and copy the AMI across all Regions. Use this Region-specific AMI to run the recovery process in the respective Regions**

Explanation Behind Correct Option

- **Create an Amazon Machine Image (AMI) after installing the software and copy the AMI across all Regions. Use this Region-specific AMI to run the recovery process in the respective Regions**
  - **AMI**: An Amazon Machine Image (AMI) provides the information required to launch an instance. It includes the software configuration (OS, application server, applications) for your instance.
  - **Cross-Region Copying**: AMIs are Region-specific and need to be copied across Regions for disaster recovery purposes.
  - **Benefits**:
    - **Consistency**: Ensures that instances in different Regions are launched from the same AMI.
    - **Scalability**: Facilitates building global applications efficiently.
    - **Performance**: Enhances performance by distributing applications across multiple Regions.
    - **High Availability**: Increases availability by deploying applications across AWS Regions.

Incorrect Options

1. **Store the installation files in Amazon S3 for quicker retrieval**
   - **Reason**: While S3 can store installation files, the installation process still needs to be executed on the EC2 instance, which takes the same amount of time (45 minutes). It does not meet the RTO of 5 minutes.
2. **Use Amazon EC2 user data to speed up the installation process**
   - **Reason**: User data scripts run at instance launch and would still take 45 minutes to install the application. This does not meet the RTO requirement.
3. **Create an Amazon Machine Image (AMI) after installing the software and use this AMI to run the recovery process in other Regions**
   - **Reason**: AMIs need to be copied across Regions as they are Region-specific. Simply creating an AMI in one Region and not copying it to other Regions will not work for cross-Region recovery.

Conclusion / Points to Memorize

- **AMI Creation**: Create an AMI after installing the software to capture the entire application stack.
- **Cross-Region Copy**: Ensure the AMI is copied across all intended Regions for disaster recovery readiness.
- **RTO Compliance**: Using AMIs ensures quick instance launches, meeting tight RTO requirements.
- **High Availability and Performance**: Distribute applications across multiple Regions for enhanced availability and performance.
  - **Consistency**: Use consistent AMIs across Regions for uniform application deployment and recovery.

Question 41: Correct

A company has built a serverless application using Amazon API Gateway and AWS Lambda. The backend is leveraging an Amazon Aurora MySQL database. The web application was initially launched in the Americas and the company would now like to expand it to Europe, where a read-only version will be available to improve latency. You plan on deploying the Amazon API Gateway and AWS Lambda using AWS CloudFormation, but would like to have a read-only copy of your data in Europe as well.As a Solutions Architect, what do you recommend?

Correct Option

- **Use Amazon Aurora Read Replicas**

Explanation Behind Correct Option

- **Use Amazon Aurora Read Replicas**
  - **Amazon Aurora Read Replicas**: Aurora Replicas are independent endpoints in an Aurora DB cluster, used for scaling read operations. Up to 15 Aurora Replicas can be distributed across Availability Zones (AZs) within an AWS Region.
  - **Cross-Region Replication**: Aurora Read Replicas can be created in different AWS Regions, allowing for global deployment. This setup provides a read-only copy of the data in the target Region, improving latency for read operations.
  - **High Performance and Availability**: Aurora features a distributed, fault-tolerant, self-healing storage system that auto-scales up to 64TB per database instance, ensuring high performance and availability.

Incorrect Options

1. **Use Amazon Aurora Multi-AZ**
   - **Reason**: Multi-AZ deployments provide high availability and failover support within a single AWS Region by storing copies of the data in multiple Availability Zones. However, Multi-AZ is not designed for cross-Region read scalability and would not provide a read-only copy in Europe.
2. **Use Amazon DynamoDB Streams**

- **Reason**: DynamoDB Streams capture a time-ordered sequence of item-level modifications in a DynamoDB table and store the information for up to 24 hours. This service is not related to Amazon Aurora and does not support creating read-only copies of an Aurora database.

3. **Create an AWS Lambda function to periodically back up and restore the Amazon Aurora database in another region**
   - **Reason**: While AWS Lambda can be used to create backups, this method is not optimized for read scalability and latency improvements. Aurora Read Replicas are a more efficient and effective solution for this use case.

Conclusion / Points to Memorize

- **Aurora Read Replicas**: Best for scaling read operations and providing read-only copies of data across Regions.
- **Multi-AZ**: Primarily for high availability and failover within a single Region, not for cross-Region read scalability.
- **DynamoDB Streams**: Used for capturing changes in DynamoDB tables, not applicable for Aurora databases.
- **Lambda Backups**: Not optimal for read scalability and latency improvements when Aurora Read Replicas are available.
  - **Cross-Region Replication**: Essential for providing low-latency read access in different Regions, achievable with Aurora Read Replicas.

Question 42 - Correct

An e-commerce company has copied 1 petabyte of data from its on-premises data center to an Amazon S3 bucket in the us-west-1 Region using an AWS Direct Connect link. The company now wants to set up a one-time copy of the data to another Amazon S3 bucket in the us-east-1 Region. The on-premises data center does not allow the use of AWS Snowball.

As a Solutions Architect, which of the following options can be used to accomplish this goal? (Select two)

Correct Options

- **Copy data from the source bucket to the destination bucket using the aws S3 sync command**
- **Set up Amazon S3 batch replication to copy objects across Amazon S3 buckets in another Region using S3 console and then delete the replication configuration**

Explanation Behind Correct Options

- **Copy data from the source bucket to the destination bucket using the aws S3 sync command**
  - **aws S3 sync**: This command uses the CopyObject APIs to copy objects between Amazon S3 buckets. It synchronizes the source and target buckets, copying only the missing or different objects. This method is efficient and ensures that only necessary data is transferred, reducing redundancy.
  - **Usage**: aws s3 sync s3://source-bucket s3://target-bucket
- **Set up Amazon S3 batch replication to copy objects across Amazon S3 buckets in another Region using S3 console and then delete the replication configuration**
  - **Batch Replication**: This method allows you to replicate objects that existed before a replication configuration was in place. It uses a Batch Operations job to copy objects to the target bucket.
  - **Process**: Configure batch replication, execute the batch replication job, and then delete the replication configuration once the one-time copy is complete.

Incorrect Options

1. **Use AWS Snowball Edge device to copy the data from one Region to another Region**
   - **Reason**: AWS Snowball Edge is used for transferring data from on-premises locations to AWS or between AWS regions in scenarios where internet connections are not feasible. However, the problem explicitly states that the on-premises data center does not allow the use of AWS Snowball.
2. **Copy data from the source Amazon S3 bucket to a target Amazon S3 bucket using the S3 console**
   - **Reason**: The AWS S3 console is not suitable for copying large amounts of data, such as 1 petabyte, due to limitations in handling such large-scale operations efficiently.
3. **Set up Amazon S3 Transfer Acceleration (Amazon S3TA) to copy objects across Amazon S3 buckets in different Regions using S3 console**
   - **Reason**: S3 Transfer Acceleration is designed to speed up uploads to S3 from clients over long distances but is not used for copying objects between S3 buckets in different regions.

Conclusion / Points to Memorize

- **aws S3 sync**: Efficient for copying large datasets between S3 buckets, using the command line.
- **Amazon S3 Batch Replication**: Ideal for one-time replication of existing objects across regions using a Batch Operations job.
- **S3 Console**: Not suitable for handling very large data transfers directly between buckets.
- **S3 Transfer Acceleration**: Designed for speeding up uploads to S3, not for inter-bucket transfers.
  - **AWS Snowball**: Not applicable when on-premises restrictions are present and typically used for initial large data migrations.

Question 43: Correct

What does this AWS CloudFormation snippet do? (Select three)

```
SecurityGroupIngress:
- IpProtocol: tcp
  FromPort: 80
  ToPort: 80
  CidrIp: 0.0.0.0/0
- IpProtocol: tcp
  FromPort: 22
  ToPort: 22
  CidrIp: 192.168.1.1/32
```

Correct Options

- **It allows any IP to pass through on the HTTP port**
- **It configures a security group's inbound rules**
- **It lets traffic flow from one IP on port 22**

Explanation Behind Correct Options

- **It allows any IP to pass through on the HTTP port**
  - **Details**: The rule with FromPort: 80 and ToPort: 80 allows inbound traffic on port 80 (HTTP) from any IP address (CidrIp: 0.0.0.0/0).
- **It configures a security group's inbound rules**
  - **Details**: The SecurityGroupIngress keyword indicates that these are inbound rules for a security group. Security groups act as virtual firewalls for your instances to control incoming and outgoing traffic.
- **It lets traffic flow from one IP on port 22**
  - **Details**: The rule with FromPort: 22 and ToPort: 22 allows inbound traffic on port 22 (SSH) from a specific IP address (CidrIp: 192.168.1.1/32).

Incorrect Options

1. **It configures the inbound rules of a network access control list (network ACL)**
   - **Reason**: The snippet configures security group rules, not network ACL rules. Security groups and network ACLs are different components in AWS.
2. **It only allows the IP 0.0.0.0 to reach HTTP**
   - **Reason**: 0.0.0.0/0 means any IP address can access HTTP, not just the IP 0.0.0.0.
3. **It prevents traffic from reaching on HTTP unless from the IP 192.168.1.1**
   - **Reason**: The rule with FromPort: 80 and ToPort: 80 allows HTTP traffic from any IP address, not just 192.168.1.1.
4. **It configures a security group's outbound rules**
   - **Reason**: The snippet configures inbound rules (SecurityGroupIngress), not outbound rules.

Conclusion / Points to Memorize

- **Security Group Ingress Rules**: Used for defining inbound traffic rules.
- **0.0.0.0/0**: Represents all IP addresses, allowing traffic from anywhere.
- **CIDR Notation**: /32 indicates a single IP address.
- **Security Group vs. Network ACL**: Security groups are stateful and used for instance-level security, while network ACLs are stateless and used for subnet-level security.
  - **Inbound and Outbound Rules**: Ingress rules are for inbound traffic, while egress rules are for outbound traffic.

Question 44 - Correct

An IT company runs a high-performance computing (HPC) workload on AWS. The workload requires high network throughput and low-latency network performance along with tightly coupled node-to-node communications. The Amazon EC2 instances are properly sized for compute and storage capacity and are launched using default options. Which of the following solutions can be used to improve the performance of the workload?

Correct Options

- **Select a cluster placement group while launching Amazon EC2 instances**

Explanation Behind Correct Options

- **Select a cluster placement group while launching Amazon EC2 instances**

- **Details**: A cluster placement group is a logical grouping of instances within a single Availability Zone (AZ). Instances in the same cluster placement group enjoy a higher per-flow throughput limit for TCP/IP traffic and are placed in the same high-bisection bandwidth segment of the network. This setup enables workloads to achieve the low-latency network performance necessary for tightly coupled node-to-node communication typical of HPC applications.

Incorrect Options

1. **Select the appropriate capacity reservation while launching Amazon EC2 instances**
   - **Reason**: Capacity Reservations ensure you have access to Amazon EC2 capacity when needed, but they do not improve the network performance of the instances.
2. **Select dedicated instance tenancy while launching Amazon EC2 instances**
   - **Reason**: Dedicated Instances are physically isolated from instances that belong to other AWS accounts, which is useful for compliance, but they do not inherently improve network performance.
3. **Select an Elastic Inference accelerator while launching Amazon EC2 instances**
   - **Reason**: Elastic Inference accelerators are used to accelerate deep learning inference workloads and require AWS PrivateLink VPC Endpoints, making them unsuitable for improving network performance for HPC workloads.

Conclusion / Points to Memorize

- **Cluster Placement Groups**: Used to achieve high network throughput and low-latency performance for HPC applications by placing instances close together within the same Availability Zone.
- **Capacity Reservations**: Ensure access to EC2 capacity but do not affect network performance.
- **Dedicated Instances**: Provide physical isolation for compliance but do not enhance network performance.
  - **Elastic Inference Accelerators**: Used for accelerating deep learning workloads and not suitable for general network performance improvement.

Question 45 - Correct

A ride-sharing company wants to improve the ride-tracking system that stores GPS coordinates for all rides. The engineering team at the company is looking for a NoSQL database that has single-digit millisecond latency, can scale horizontally, and is serverless, so that they can perform high-frequency lookups reliably. Which database do you recommend for their requirements?

Correct Option:

- **Amazon DynamoDB:**
  - **Key-Value and Document Database:** Delivers single-digit millisecond performance at any scale.
  - **Fully Managed:** Multi-region, multi-master, durable NoSQL database with built-in security, backup and restore.
  - **In-Memory Caching:** For internet-scale applications.
  - **Scalability:** Can handle more than 10 trillion requests per day and support peaks of more than 20 million requests per second.
  - **Serverless:** No need to manage servers.
  - **Low Latency:** Single-digit millisecond latency.
  - **Horizontal Scaling:** Scales horizontally.

Incorrect Options:

- **Amazon ElastiCache:**
  - **Purpose:** Allows seamless setup, running, and scaling of popular open-source compatible in-memory data stores, compatible with Redis or Memcached.
  - **Use Cases:** Caching, session stores, gaming, geospatial services, real-time analytics, and queuing.
  - **Primary Use Case:** Caching service, not suitable as the main database.
- **Amazon Relational Database Service (Amazon RDS):**
  - **Function:** Makes it easy to set up, operate, and scale a relational database in the cloud.
  - **Features:** Cost-efficient and resizable capacity, automates time-consuming tasks such as hardware provisioning, database setup, patching, and backups.
  - **Limitation:** Relational databases cannot provide the millisecond latency and NoSQL features needed for the given use case.

Conclusion / Points to Memorize:

1. **Amazon DynamoDB:**
   - Key-value and document database.
   - Single-digit millisecond latency.
   - Scales horizontally and is serverless.

- Suitable for high-frequency lookups.

2. **Amazon ElastiCache:**
   - In-memory data store.
   - Primarily for caching, session stores, and real-time analytics.
   - Not suitable as the main database.
3. **Amazon RDS:**
   - Relational database service.
   - Cannot provide the millisecond latency required.
   - Not suitable for NoSQL use cases.

Question 46 - Correct

A Big Data analytics company writes data and log files in Amazon S3 buckets. The company now wants to stream the existing data files as well as any ongoing file updates from Amazon S3 to Amazon Kinesis Data Streams. As a Solutions Architect, which of the following would you suggest as the fastest possible way of building a solution for this requirement?

Correct option:

- Leverage AWS Database Migration Service (AWS DMS) as a bridge between Amazon S3 and Amazon Kinesis Data Streams

Explanation behind correct option:

1. **AWS DMS**:
   - Enables seamless migration of data from supported sources to relational databases, data warehouses, streaming platforms, and other data stores in AWS.
   - Supports specifying Amazon S3 as the source and streaming services like Kinesis and Amazon MSK as the target.
   - Facilitates migration of full and change data capture (CDC) files without complex configuration or code development.
   - Allows the configuration of an AWS DMS replication instance to scale up or down depending on the workload.
   - Several consumers, such as AWS Lambda, Amazon Kinesis Data Firehose, Amazon Kinesis Data Analytics, and the Kinesis Consumer Library (KCL), can consume the data concurrently for real-time analytics.
   - AWS DMS supports the architecture needed for streaming data from Amazon S3 to Kinesis Data Streams.

Incorrect options with brief explanation:

1. **Configure Amazon EventBridge events for the bucket actions on Amazon S3. An AWS Lambda function can then be triggered from the Amazon EventBridge event that will send the necessary data to Amazon Kinesis Data Streams**:
   - Requires enabling AWS CloudTrail trail to use object-level actions as a trigger.
   - Involves significant custom development to write the data into Amazon Kinesis Data Streams, making it a less optimal solution.
2. **Leverage Amazon S3 event notification to trigger an AWS Lambda function for the file create event. The AWS Lambda function will then send the necessary data to Amazon Kinesis Data Streams**:
   - Requires significant custom development to write the data into Amazon Kinesis Data Streams, making it less efficient and quick compared to AWS DMS.
3. **Amazon S3 bucket actions can be directly configured to write data into Amazon Simple Notification Service (Amazon SNS). Amazon SNS can then be used to send the updates to Amazon Kinesis Data Streams**:
   - Amazon S3 cannot directly write data into Amazon SNS; it can send event notifications to SNS.
   - Amazon SNS cannot directly send messages to Amazon Kinesis Data Streams, making this approach incorrect.

Conclusion / Points to Memorize:

1. **AWS DMS** is highly suitable for seamless data migration and streaming without extensive custom development.
2. **AWS DMS** supports specifying Amazon S3 as the source and streaming services like Kinesis as the target.
3. AWS DMS enables concurrent real-time data consumption by multiple services like AWS Lambda and Amazon Kinesis Data Analytics.
4. Solutions involving custom development (e.g., using AWS Lambda with EventBridge or S3 event notifications) are less optimal for quick implementation.

Question 47 - Correct

As a Solutions Architect, you are tasked to design a distributed application that will run on various Amazon EC2 instances. This application needs to have the highest performance local disk to cache data. Also, data is copied through an Amazon EC2 to EC2 replication mechanism. It is acceptable if the instance loses its data when stopped or terminated. Which storage solution do you recommend?

Correct option:

- Instance Store

Explanation behind correct option:

1. **Instance Store:**
   - Provides temporary block-level storage for EC2 instances.
   - Storage is located on disks physically attached to the host computer.
   - Ideal for temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content.
   - Suitable for data replicated across a fleet of instances, such as a load-balanced pool of web servers.
   - Volumes are included as part of the instance's usage cost.
   - Some instance types use NVMe or SATA-based SSDs to deliver high random I/O performance.
   - Offers very low latency storage.
   - Data is lost when the instance is stopped or terminated, which is acceptable in this case.

Incorrect options with brief explanation:

1. **Amazon Elastic Block Store (EBS):**
   - High-performance block storage for use with EC2 instances.
   - Provides persistent storage that survives instance termination or reboots.
   - Performance is good but not as high as Instance Store.
2. **Amazon Simple Storage Service (Amazon S3):**
   - Object storage service offering scalability, data availability, security, and performance.
   - Not designed to be mounted as a local disk.
   - Suitable for storing large amounts of data but not for high-performance local disk caching.
3. **Amazon Elastic File System (Amazon EFS):**
   - Scalable, fully managed elastic NFS file system.
   - Suitable for use with AWS Cloud services and on-premises resources.
   - Provides persistent storage that grows and shrinks automatically.
   - Performance is not as high as Instance Store for local disk caching needs.

Conclusion / Points to Memorize:

1. **Instance Store** is the best option for highest performance local disk caching with temporary storage needs.
2. **Amazon EBS** offers persistent storage with good performance, but not as high as Instance Store.
3. **Amazon S3** and **Amazon EFS** are not suitable for high-performance local disk caching.
4. **Instance Store** data is lost upon instance termination, which is acceptable in this scenario.
5. **Instance Store** uses NVMe or SATA-based SSDs for high random I/O performance.

Question 48 - Correct

A company wants to grant access to an Amazon S3 bucket to users in its own AWS account as well as to users in another AWS account. Which of the following options can be used to meet this requirement?

Correct option:

Use a bucket policy to grant permission to users in its account as well as to users in another account

Explanation behind correct options:

1. A bucket policy is a type of resource-based policy that can be used to grant permissions to the principal specified in the policy.
2. Principals can be in the same account as the resource or in other accounts.
3. For cross-account permissions to other AWS accounts or users in another account, you must use a bucket policy.

Incorrect options:

1. **Use either a bucket policy or a user policy to grant permission to users in its account as well as to users in another account**
   - User policies are for managing permissions for users in their own AWS account and NOT for users in other AWS accounts.
   - This option is incorrect because it suggests user policies can be used for cross-account permissions, which is not true.
2. **Use a user policy to grant permission to users in its account as well as to users in another account**
   - Same as above, user policies cannot grant permissions to users in other AWS accounts.
3. **Use permissions boundary to grant permission to users in its account as well as to users in another account**

- Permissions boundaries define the maximum permissions that the identity-based policies can grant to an entity but do not grant permissions themselves.
- This option is incorrect because it does not apply permissions but rather limits them.

Conclusion / points to memorize:

1. Use bucket policies for cross-account permissions in Amazon S3.
2. User policies cannot be used for granting permissions to users in other AWS accounts.
3. Permissions boundaries only limit permissions and do not grant them.

Question 49 - Correct

As part of the on-premises data center migration to AWS Cloud, a company is looking at using multiple AWS Snow Family devices to move their on-premises data. Which AWS Snow Family service offers the feature of storage clustering?

Correct option:

AWS Snowball Edge Compute Optimized

Explanation behind correct options:

1. AWS Snowball Edge Compute Optimized provides 52 vCPUs, 42 terabytes of usable block or object storage, and an optional GPU for use cases such as advanced machine learning and full-motion video analysis in disconnected environments.
2. It supports storage clustering, which allows multiple devices to be connected and managed as a single large storage pool.
3. AWS Snowball Edge devices (both Storage Optimized and Compute Optimized) can be used for data collection, machine learning, processing, and storage in environments with intermittent connectivity.
4. These devices can also be rack-mounted and clustered together to build larger, temporary installations.

Incorrect options and brief explanation:

1. **AWS Snowcone** - AWS Snowcone is a smaller, portable, and rugged device ideal for data collection, processing, and transfer but does not support storage clustering.
2. **AWS Snowmobile** - AWS Snowmobile is a large-scale data transfer service for multi-petabyte or exabyte-scale data migrations but does not support storage clustering.
3. **AWS Snowmobile Storage Compute** - This option is a distractor and does not exist as an AWS service.

Conclusion / Points to memorize:

1. **AWS Snowball Edge Compute Optimized** and **AWS Snowball Edge Storage Optimized** are the AWS Snow Family devices that support storage clustering.
2. **AWS Snowcone** and **AWS Snowmobile** do not support storage clustering.
3. AWS Snowball Edge devices are suitable for environments with intermittent connectivity and can be used for local storage, machine learning, and processing tasks.
4. Always verify the specific capabilities and features of AWS Snow Family devices to ensure they meet your requirements for data migration and edge computing.

Question 50 - Incorrect

You are working as a Solutions Architect for a photo processing company that has a proprietary algorithm to compress an image without any loss in quality. Because of the efficiency of the algorithm, your clients are willing to wait for a response that carries their compressed images back. You also want to process these jobs asynchronously and scale quickly, to cater to the high demand. Additionally, you also want the job to be retried in case of failures.

Which combination of choices do you recommend to minimize cost and comply with the requirements? (Select two)

Correct options:

- Amazon EC2 Spot Instances
- Amazon Simple Queue Service (Amazon SQS)

Explanation behind correct options:

1. **Amazon EC2 Spot Instances:**
   - Spot Instances are unused Amazon EC2 instances available at a lower cost than On-Demand instances.
   - They are ideal for applications with flexible start and end times, which can handle interruptions.
   - Significantly lower costs make them suitable for high-demand, cost-sensitive applications.
   - Suitable for the unpredictable nature of job volumes in this scenario.
2. **Amazon Simple Queue Service (Amazon SQS):**
   - Fully managed message queuing service that decouples and scales microservices, distributed systems, and serverless applications.

- Offers Standard and FIFO queues for different ordering and delivery guarantees.
- Enables asynchronous processing and built-in retries, which are essential for handling image compression jobs.
- Scales seamlessly to accommodate high demand.

Incorrect options and brief explanation:

1. **Amazon Simple Notification Service (Amazon SNS):**
   - SNS is a pub/sub messaging service suitable for push-based, many-to-many messaging.
   - Not appropriate for queuing and retry mechanisms needed for the job processing scenario.
2. **Amazon EC2 Reserved Instances (RIs):**
   - RIs provide cost savings with a commitment to consistent instance configuration for 1 or 3 years.
   - Not suitable for irregular, high-demand jobs with flexible schedules.
3. **Amazon EC2 On-Demand Instances:**
   - On-Demand Instances provide flexibility without long-term commitments but are costlier than Spot Instances.
   - Suitable for short-term, irregular workloads but not as cost-effective for this use case.

Conclusion / Points to memorize:

1. **Use Spot Instances for cost-effective, flexible, and high-demand compute needs** with tolerable interruptions.
2. **Utilize SQS for asynchronous processing and retry mechanisms** to handle job queuing effectively.
3. **SNS is for push-based notifications, not queuing.**
4. **RIs require long-term commitments and are not suitable for flexible or unpredictable workloads.**
5. **On-Demand Instances offer flexibility but at a higher cost compared to Spot Instances.**

Question 51 - Incorrect

A startup's cloud infrastructure consists of a few Amazon EC2 instances, Amazon RDS instances, and Amazon S3 storage. A year into their business operations, the startup is incurring costs that seem too high for their business requirements.

Which of the following options represents a valid cost-optimization solution?

Correct option:

- Use AWS Cost Explorer Resource Optimization to get a report of Amazon EC2 instances that are either idle or have low utilization and use AWS Compute Optimizer to look at instance type recommendations

Explanation behind correct option:

1. **AWS Cost Explorer Resource Optimization:**
   - Identifies under-utilized Amazon EC2 instances.
   - Helps in downsizing instances within the same instance family.
   - Provides potential impact on AWS bill, considering Reserved Instances and Savings Plans.
2. **AWS Compute Optimizer:**
   - Recommends optimal AWS Compute resources for reducing costs and improving performance.
   - Analyzes historical utilization metrics using machine learning.
   - Suggests optimal Amazon EC2 instance types based on utilization data, including for EC2 Auto Scaling groups.

Incorrect options and brief explanation:

1. **Use Amazon S3 Storage class analysis to get recommendations for transitions of objects to Amazon S3 Glacier storage classes to reduce storage costs. You can also automate moving these objects into lower-cost storage tier using Lifecycle Policies:**
   - Amazon S3 Storage Class Analysis does not provide recommendations for transitions to ONEZONE_IA or S3 Glacier storage classes.
   - Primarily used for analyzing storage access patterns for transitioning data to STANDARD_IA.
2. **Use AWS Trusted Advisor checks on Amazon EC2 Reserved Instances to automatically renew reserved instances (RI). AWS Trusted advisor also suggests Amazon RDS idle database instances:**
   - AWS Trusted Advisor checks for expiring RIs but does not automatically renew them.
   - RIs do not renew automatically; post-expiration, instances are charged On-Demand rates.
3. **Use AWS Compute Optimizer recommendations to help you choose the optimal Amazon EC2 purchasing options and help reserve your instance capacities at reduced costs:**
   - AWS Compute Optimizer does not recommend instance purchasing options.
   - Focuses on recommending optimal compute resources based on utilization data.

Conclusion / Points to memorize:

1. **Use AWS Cost Explorer for identifying under-utilized EC2 instances** and potential cost savings from downsizing.
2. **AWS Compute Optimizer helps recommend optimal instance types** based on utilization data to reduce costs and improve performance.
3. **Amazon S3 Storage Class Analysis is limited to analyzing storage access patterns** and recommending transitions mainly to STANDARD_IA, not Glacier.
4. **AWS Trusted Advisor provides checks on RI expirations** but does not automatically renew them.
5. **Compute Optimizer focuses on resource optimization, not purchasing options.**

Question 52 - Incorrect

Your company is deploying a website running on AWS Elastic Beanstalk. The website takes over 45 minutes for the installation and contains both static as well as dynamic files that must be generated during the installation process.

As a Solutions Architect, you would like to bring the time to create a new instance in your AWS Elastic Beanstalk deployment to be less than 2 minutes. Which of the following options should be combined to build a solution for this requirement? (Select two)

Correct options:

- Create a Golden Amazon Machine Image (AMI) with the static installation components already setup
- Use Amazon EC2 user data to customize the dynamic installation parts at boot time

Explanation behind correct options:

1. **Create a Golden Amazon Machine Image (AMI) with the static installation components already setup:**
   - A Golden AMI is standardized with pre-configured software, security patches, and other essential components.
   - It helps in reducing the setup time by having the static components pre-installed.
2. **Use Amazon EC2 user data to customize the dynamic installation parts at boot time:**
   - User data scripts allow customization and execution of dynamic configurations at instance launch.
   - This method ensures the dynamic parts are configured quickly during the boot process.

Incorrect options and brief explanation:

1. **Store the installation files in Amazon S3 so they can be quickly retrieved:**
   - S3 can store files, but it cannot execute or run installation processes.
   - Retrieving files from S3 does not speed up the actual installation process that takes 45 minutes.
2. **Use Amazon EC2 user data to install the application at boot time:**
   - User data is not efficient for lengthy installations that take over 45 minutes.
   - This option would still result in long instance creation times.
3. **Use AWS Elastic Beanstalk deployment caching feature:**
   - This is a made-up option and does not exist in AWS Elastic Beanstalk.

Conclusion / Points to memorize:

1. **Golden AMIs are effective for pre-configuring static components**, reducing setup times for new instances.
2. **User data scripts are ideal for customizing dynamic configurations quickly at instance boot time**.
3. **AWS Elastic Beanstalk simplifies application deployment but understanding its limitations and proper configurations** (like custom AMIs and user data) can significantly enhance performance.
4. **Amazon S3 is primarily for storage and not for running installations or executing scripts**.
5. **AWS has no "deployment caching feature" in Elastic Beanstalk; ensure to differentiate real features from distractors**.

Question 53 - Incorrect

An e-commerce company wants to migrate its on-premises application to AWS. The application consists of application servers and a Microsoft SQL Server database. The solution should result in the maximum possible availability for the database layer while minimizing operational and management overhead.

As a solutions architect, which of the following would you recommend to meet the given requirements?

Correct options:

- Migrate the data to Amazon RDS for SQL Server database in a Multi-AZ deployment

Explanation behind correct options:

1. **Migrate the data to Amazon RDS for SQL Server database in a Multi-AZ deployment:**
   - **High Availability and Fault Tolerance:** Amazon RDS supports Multi-AZ deployments for Microsoft SQL Server using SQL Server Database Mirroring (DBM) or Always On Availability Groups (AGs).
   - **Automatic Failover:** In the event of a planned maintenance or unplanned disruption, Amazon RDS automatically fails over to a standby instance, ensuring minimal downtime.

- **Minimized Management Overhead:** Amazon RDS handles routine database tasks like patching and backups, reducing operational overhead.
- **Single Endpoint:** The primary and standby instances use the same endpoint, making failovers transparent to applications.

Incorrect options and brief explanation:

1. **Migrate the data to Amazon EC2 instance hosted SQL Server database. Deploy the Amazon EC2 instances in a Multi-AZ configuration:**
   - **Operational Overhead:** Managing SQL Server on EC2 involves significant overhead for OS and database patching, backups, and failover management.
   - **Complex Management:** This option is less preferable due to the increased complexity and manual management required.
2. **Migrate the data to Amazon RDS for SQL Server database in a cross-region read-replica configuration:**
   - **Read Scalability, Not Availability:** Read replicas are used to offload read traffic and improve read scalability, not to increase database availability.
   - **Incorrect Use Case:** This configuration does not provide high availability or fault tolerance for the primary database instance.
3. **Migrate the data to Amazon RDS for SQL Server database in a cross-region Multi-AZ deployment:**
   - **No Such Feature:** Amazon RDS Multi-AZ deployments provide high availability within a single region. There is no support for cross-region Multi-AZ deployments.
   - **Invalid Option:** This option is not technically feasible with current AWS capabilities.

Conclusion / Points to memorize:

1. **Amazon RDS Multi-AZ Deployment:** Provides high availability, automatic failover, and minimizes management overhead for database instances within a single region.
2. **Amazon RDS for SQL Server:** Supports high availability using SQL Server Database Mirroring (DBM) or Always On Availability Groups (AGs).
3. **Read Replicas:** Enhance read scalability but do not improve the availability of the primary database instance.
4. **Cross-Region Multi-AZ:** Not supported by Amazon RDS; high availability solutions are region-specific.
5. **EC2-hosted Databases:** Involve significant management overhead compared to managed services like Amazon RDS.

Question 54 - Correct

The development team at a social media company wants to handle some complicated queries such as "What are the number of likes on the videos that have been posted by friends of a user A?".

Correct Option: Amazon Neptune

Explanation Behind Correct Option:

- **Amazon Neptune**:
  - **Purpose-Built Graph Database**: Optimized for storing billions of relationships and querying the graph with milliseconds latency.
  - **Use Cases**: Recommendation engines, fraud detection, knowledge graphs, drug discovery, and network security.
  - **Key Features**:
    - **High Availability**: Read replicas, point-in-time recovery, continuous backup to Amazon S3, and replication across Availability Zones.
    - **Security**: Supports HTTPS encrypted client connections and encryption at rest.
    - **Fully Managed**: No need for database management tasks like hardware provisioning, software patching, setup, configuration, or backups.
  - **Performance**: Quickly processes large sets of user profiles and interactions, enabling highly interactive graph queries with high throughput.
  - **Social Networking**: Ideal for applications involving user interactions and relationships, such as social feeds that prioritize updates from friends.

Incorrect Options:

- **Amazon OpenSearch Service**:
  - **Primary Use**: Interactive log analytics, real-time application monitoring, and website search.
  - **Not Suitable**: It's not optimized for handling highly connected datasets and complex relationship queries as required in social networking use cases.
- **Amazon Redshift**:
  - **Primary Use**: Cloud-based data warehousing for large scale data set storage and analysis.
  - **Not Suitable**: The use case is not about data warehousing but about handling highly connected datasets.
- **Amazon Aurora**:
  - **Primary Use**: Relational database service that combines the performance and availability of traditional enterprise databases with simplicity and cost-effectiveness.
  - **Not Suitable**: Aurora is not an in-memory database and is not optimized for graph queries and highly connected datasets.

Conclusion / Points to Memorize:

1. **Graph Databases**: Use Amazon Neptune for applications requiring processing of highly connected datasets and complex relationship queries.
2. **High Throughput and Low Latency**: Neptune is optimized for graph queries with milliseconds latency, ideal for social networking applications.

3. **Use Cases for Neptune**: Includes social networking, recommendation engines, and other scenarios involving complex user interactions.
4. **Alternative Services**: Understand that OpenSearch, Redshift, and Aurora have different primary uses and are not optimized for graph-based queries.

Question 55 - Correct

A small rental company had 5 employees, all working under the same AWS cloud account. These employees deployed their applications built for various functions- including billing, operations, finance, etc. Each of these employees has been operating in their own VPC. Now, there is a need to connect these VPCs so that the applications can communicate with each other. Which of the following is the MOST cost-effective solution for this use-case?

Correct Option: Use a VPC peering connection

Explanation Behind Correct Option:

- **VPC Peering Connection**:
  - **Definition**: A networking connection between two VPCs that enables routing traffic using private IPv4 or IPv6 addresses.
  - **Functionality**: Instances in either VPC can communicate as if they are within the same network.
  - **Flexibility**: Can be created between your own VPCs or with a VPC in another AWS account.
  - **Inter-Region**: VPCs can be in different regions, known as inter-region VPC peering.
  - **Cost-Effectiveness**: The most cost-effective way to connect multiple VPCs within the same account.
  - **Limitation**: Not transitive; each VPC pair needs a separate peering connection.

Incorrect Options:

- **Use an Internet Gateway**:
  - **Purpose**: Allows communication between instances in your VPC and the internet.
  - **Limitation**: Not designed for connecting VPCs; used for internet connectivity.
- **Use an AWS Direct Connect Connection**:
  - **Purpose**: Establishes a dedicated network connection from your premises to AWS.
  - **Limitation**: Overkill for connecting VPCs within the same account and not cost-effective.
- **Use a Network Address Translation (NAT) Gateway**:
  - **Purpose**: Enables instances in a private subnet to connect to the internet or other AWS services, while preventing the internet from initiating connections with those instances.
  - **Limitation**: Not used for VPC-to-VPC connection; incurs additional costs.

Conclusion / Points to Memorize:

1. **VPC Peering**: The most cost-effective solution for connecting multiple VPCs within the same AWS account.
2. **Internet Gateway**: Designed for internet connectivity, not VPC-to-VPC communication.
3. **Direct Connect**: Used for dedicated network connections from premises to AWS; overkill for VPC peering.
4. **NAT Gateway**: Enables internet connectivity for private subnets; not suitable for VPC peering.

Question 56 - Correct

A development team has configured Elastic Load Balancing for host-based routing. The idea is to support multiple subdomains and different top-level domains. The rule *.example.com matches which of the following?

Correct Option: test.example.com

Explanation Behind Correct Option:

- **Host-Based Routing**:
  - **Definition**: Routing requests based on the hostname in the host header.
  - **Purpose**: Supports multiple subdomains and different top-level domains using a single load balancer.
  - **Hostname Characteristics**:
    - Not case-sensitive.
    - Can be up to 128 characters in length.
    - Allowed characters include: A–Z, a–z, 0–9, -, ., *, ?.
    - Must include at least one “.” character.
    - Only alphabetical characters are allowed after the final “.” character.
  - **Wildcard Matching**: The rule *.example.com matches any subdomain of example.com but not example.com itself.
    - **Example**: test.example.com matches the rule, while example.com does not.

Incorrect Options:

- **example.com**:
  - **Reason**: The rule *.example.com requires at least one character before the ".", so example.com does not match.
- **example.test.com**:
  - **Reason**: The rule *.example.com matches subdomains of example.com, not higher-level domains or different domains.
- **EXAMPLE.COM**:
  - **Reason**: Hostnames are not case-sensitive, but the wildcard rule requires a subdomain before example.com.

Conclusion / Points to Memorize:

1. **Wildcard Rules**: The rule *.example.com matches any subdomain of example.com, not example.com itself.
2. **Hostname Characteristics**: Hostnames can include A–Z, a–z, 0–9, -, ., *, ?, and must contain at least one "." character.
3. **Host-Based Routing**: Used to support multiple subdomains and different top-level domains with a single load balancer.
4. **Case-Insensitivity**: Hostnames are not case-sensitive.

Question 57 - correct

An Internet of Things (IoT) company would like to have a streaming system that performs real-time analytics on the ingested IoT data. Once the analytics is done, the company would like to send notifications back to the mobile applications of the IoT device owners. As a solutions architect, which of the following AWS technologies would you recommend to send these notifications to the mobile applications?

Correct Option: Amazon Kinesis with Amazon Simple Notification Service (Amazon SNS)

Explanation Behind Correct Option:

- **Amazon Kinesis**:
  - **Purpose**: Collects, processes, and analyzes real-time, streaming data.
  - **Use Cases**: Ingests real-time data such as video, audio, application logs, website clickstreams, and IoT telemetry data for machine learning, analytics, and other applications.
  - **Advantage**: Processes and analyzes data as it arrives, enabling instant responses.
- **Amazon Simple Notification Service (Amazon SNS)**:
  - **Purpose**: A highly available, durable, secure, fully managed pub/sub messaging service.
  - **Features**: Provides topics for high-throughput, push-based, many-to-many messaging.
  - **Use Case**: Ideal for sending notifications to mobile applications.
- **Combination**:
  - **Kinesis**: Handles real-time data streaming from IoT devices.
  - **SNS**: Sends notifications to mobile applications after analytics are performed.

Incorrect Options:

- **Amazon Simple Queue Service (Amazon SQS) with Amazon SNS**:
  - **SQS**: A fully managed message queuing service to decouple and scale microservices, distributed systems, and serverless applications.
  - **Reason Incorrect**: SQS is not suitable for real-time streaming of data; queues are meant for decoupling and scaling, not for real-time processing.
- **Amazon Kinesis with Amazon Simple Email Service (Amazon SES)**:
  - **SES**: A cloud-based email sending service for marketing, notification, and transactional emails.
  - **Reason Incorrect**: SES is an email service, not a notification service for mobile applications.
- **Amazon Kinesis with Amazon SQS**:
  - **Reason Incorrect**: SQS is a queuing service and does not provide notification capabilities. SQS needs to be paired with SNS for sending notifications.

Conclusion / Points to Memorize:

1. **Amazon Kinesis**: Used for real-time data streaming and analytics.
2. **Amazon SNS**: Used for sending notifications to mobile applications.
3. **Optimal Combination**: Use Amazon Kinesis for streaming data and Amazon SNS for sending notifications.
4. **Incorrect Uses**:
   - **SQS**: Not suitable for real-time streaming; used for decoupling and scaling.
   - **SES**: Email service, not a notification service.
- **SQS with Kinesis**: SQS alone cannot send notifications.

Question 58 – Correct

A digital media company needs to manage uploads of around 1 terabyte each from an application being used by a partner company. As a Solutions Architect, how will you handle the upload of these files to Amazon S3?

Correct Option: Use multi-part upload feature of Amazon S3

Explanation Behind Correct Option:

- **Multi-part Upload**:
  - **Purpose**: Allows uploading a single object as a set of parts.
  - **Benefits**:
    - Parts can be uploaded independently and in any order.
    - If any part fails during upload, only that part needs to be retransmitted.
    - Enhances upload speed by enabling parallel uploads.
    - Increases resiliency to network errors.
  - **Usage Recommendations**:
    - For large objects over a stable, high-bandwidth network.
    - For objects over spotty networks to avoid upload restarts.
    - Mandatory for files larger than 5 GB.
    - Consider for files larger than 100 MB for improved upload efficiency.

Incorrect Options:

- **Amazon S3 Versioning**:
  - **Purpose**: Keeps multiple variants of an object in the same bucket.
  - **Benefits**:
    - Preserves, retrieves, and restores object versions.
    - Recovers from unintended user actions and application failures.
  - **Reason Incorrect**: Does not assist with the process of large file uploads; it's for version control.
- **AWS Direct Connect to Provide Extra Bandwidth**:
  - **Purpose**: Establishes a dedicated network connection from premises to AWS.
  - **Benefits**:
    - Provides private connectivity to AWS.
    - Reduces network costs and increases bandwidth throughput.
  - **Reason Incorrect**: Setting up AWS Direct Connect is time-consuming (at least a month) and not practical for immediate file uploads.
- **AWS Snowball**:
  - **Purpose**: Used for transferring large-scale data to AWS securely and quickly.
  - **Benefits**:
    - Offers up to 80 TB of storage.
    - Suitable for large data transfer and pre-processing use cases.
  - **Reason Incorrect**: Best for large-scale data migrations rather than regular large file uploads to Amazon S3.

Conclusion / Points to Memorize:

1. **Multi-part Upload**:
   - Best for large file uploads to Amazon S3.
   - Handles files larger than 5 GB (mandatory) and 100 MB (recommended).
   - Allows parallel and independent part uploads, increasing efficiency and resilience.
2. **Amazon S3 Versioning**:
   - Used for version control, not for improving upload efficiency.
3. **AWS Direct Connect**:
   - Provides dedicated network connections.
   - Not suitable for immediate upload needs due to setup time.
4. **AWS Snowball**:
   - Ideal for bulk data transfers, not regular uploads.
- Physical device requiring shipment and setup, not instant.

Question 59 – Incorrect

A CRM company has a software as a service (SaaS) application that feeds updates to other in-house and third-party applications. The SaaS application and the in-house applications are being migrated to use AWS services for this inter-application communication. As a Solutions Architect, which of the following would you suggest to asynchronously decouple the architecture?

Correct Option: Use Amazon EventBridge to decouple the system architecture

Explanation Behind Correct Option:

- **Amazon EventBridge**:
  - **Purpose**: Event bus service to build event-driven applications by integrating with SaaS applications and AWS services.
  - **Benefits**:
    - Direct integration with third-party SaaS partners.
    - Automatic ingestion of events from over 90 AWS services.
    - Allows creation of rules using JSON-based structure for events.
    - Supports over 15 AWS services as targets, including AWS Lambda, Amazon SQS, Amazon SNS, and Amazon Kinesis Streams and Firehose.
  - **Use Case Fit**: Ideal for integrating with third-party SaaS services and for decoupling system architectures asynchronously.

Incorrect Options:

- **Amazon Simple Notification Service (Amazon SNS)**:
  - **Purpose**: Highly available, durable, secure, fully managed pub/sub messaging service.
  - **Reason Incorrect**: Does not support direct integration with third-party SaaS services.
- **Amazon Simple Queue Service (Amazon SQS)**:
  - **Purpose**: Message queuing service for decoupling and scaling microservices, distributed systems, and serverless applications.
  - **Reason Incorrect**: Lacks direct integration with third-party SaaS services.
- **Elastic Load Balancing (ELB)**:
  - **Purpose**: Distributes incoming application or network traffic across multiple targets.
  - **Reason Incorrect**: Offers synchronous decoupling, which is not suitable for the asynchronous decoupling required in the use case.

Conclusion / Points to Memorize:

1. **Amazon EventBridge**:
   - Best for decoupling system architecture when integrating with third-party SaaS services.
   - Supports direct integration with over 90 AWS services and third-party applications.
   - Allows creation of rules using JSON-based structure for events and supports various AWS services as targets.
2. **Amazon SNS**:
   - Suitable for pub/sub messaging within AWS ecosystem.
   - Not ideal for third-party SaaS service integration.
3. **Amazon SQS**:
   - Good for decoupling applications and message queuing.
   - Not suitable for direct integration with third-party SaaS services.
4. **Elastic Load Balancing (ELB)**:
   - Provides synchronous decoupling by distributing traffic.
   - Not suitable for asynchronous decoupling required for the use case.

Question 60 – Incorrect

A company uses Application Load Balancers in multiple AWS Regions. The Application Load Balancers receive inconsistent traffic that varies throughout the year. The engineering team at the company needs to allow the IP addresses of the Application Load Balancers in the on-premises firewall to enable connectivity. Which of the following represents the MOST scalable solution with minimal configuration changes?

Correct Option: Set up AWS Global Accelerator. Register the Application Load Balancers in different Regions to the AWS Global Accelerator. Configure the on-premises firewall's rule to allow static IP addresses associated with the AWS Global Accelerator

Explanation Behind Correct Option:

- **AWS Global Accelerator**:
  - **Purpose**: Networking service that improves availability and performance of applications.
  - **Benefits**:
    - Provides static IP addresses for a fixed entry point to applications.
    - Eliminates the complexity of managing specific IP addresses for different AWS Regions and Availability Zones.

    - IP addresses are anycast from AWS edge locations for optimal performance.
    - Simplifies firewall configuration to allow static IP addresses associated with the Global Accelerator.
  - **Use Case Fit**: Ideal for managing IP addresses across multiple regions with minimal configuration changes.

Incorrect Options:

- **Migrate all Application Load Balancers in different Regions to the Network Load Balancers**:
  - **Reason Incorrect**: Requires changes to the on-premises firewall's configuration rules for each Network Load Balancer, which is not optimal.
- **Set up a Network Load Balancer in one Region**:
  - **Reason Incorrect**: Network Load Balancer is region-bound, making it impossible to manage multiple regions with a single NLB. Multiple NLBs would be needed, complicating firewall configuration.
- **Develop an AWS Lambda script to get the IP addresses of the Application Load Balancers in different Regions**:
  - **Reason Incorrect**: Requires ongoing changes to the firewall's configuration as IP addresses of Application Load Balancers change, making it less optimal than using static IPs provided by AWS Global Accelerator.

Conclusion / Points to Memorize:

1. **AWS Global Accelerator**:
   - Provides static IP addresses that are anycast from AWS edge locations.
   - Simplifies firewall configuration by allowing static IP addresses.
   - Ideal for managing IP addresses across multiple regions.
2. **Network Load Balancers**:
   - Region-bound and requires multiple NLBs for cross-region traffic management.
   - Not optimal for minimizing firewall configuration changes.
3. **AWS Lambda Script for IP Management**:
   - Requires ongoing updates to firewall rules.
- Less optimal compared to static IPs provided by AWS Global Accelerator.

Question 61 – Incorrect

As an e-sport tournament hosting company, you have servers that need to scale and be highly available. Therefore you have deployed an Elastic Load Balancing (ELB) with an Auto Scaling group (ASG) across 3 Availability Zones (AZs). When e-sport tournaments are running, the servers need to scale quickly. And when tournaments are done, the servers can be idle. As a general rule, you would like to be highly available, have the capacity to scale and optimize your costs. What do you recommend? (Select two)

Correct Options:

1. **Set the minimum capacity to 2**
2. **Use Reserved Instances (RIs) for the minimum capacity**

Explanation Behind Correct Options:

1. **Set the Minimum Capacity to 2**:
   - **Auto Scaling Group (ASG)**:
     - **Functionality**: Manages and scales Amazon EC2 instances.
     - **Minimum Capacity**: Setting the minimum capacity to 2 ensures high availability. The ASG will distribute these instances across two different Availability Zones (AZs), ensuring fault tolerance.
     - **Scaling**: As demand increases, ASG will add instances in the third AZ, and reduce them back to 2 when demand decreases.
   - **High Availability**: Ensures at least two instances are always running, maintaining application availability even if one AZ fails.
2. **Use Reserved Instances (RIs) for the Minimum Capacity**:
   - **Cost Savings**: RIs provide significant savings compared to On-Demand Instances.
   - **Billing Discount**: RIs apply a billing discount to On-Demand Instances that match specific attributes.
   - **Guaranteed Capacity**: Minimum capacity will always be maintained, making RIs a cost-effective choice.
   - **Resilience**: In case of an AZ outage, ASG will provision replacement instances in another AZ, maintaining the minimum capacity of 2.

Incorrect Options:

1. **Set the Minimum Capacity to 1**:
   - **Reason Incorrect**: Not failure-proof; only one instance will be maintained, which will be in a single AZ. This does not ensure high availability.
2. **Set the Minimum Capacity to 3**:

- **Reason Incorrect**: Not cost-effective; maintaining three instances consistently is unnecessary when two instances in different AZs are sufficient for high availability.

3. **Use Dedicated Hosts for the Minimum Capacity**:
   - **Reason Incorrect**: Dedicated hosts are suitable for specific use cases requiring existing software licenses or dedicated physical hosts, which are not relevant here.

Conclusion / Points to Memorize:

1. **Auto Scaling Group (ASG)**:
   - Use to manage and scale EC2 instances.
   - Set minimum capacity to 2 for high availability across multiple AZs.
2. **Reserved Instances (RIs)**:
   - Provide cost savings over On-Demand Instances.
   - Ideal for instances that are always running, such as the minimum capacity in an ASG.
3. **Avoid Setting Minimum Capacity to 1**:
   - Does not ensure high availability or fault tolerance.
4. **Avoid Setting Minimum Capacity to 3**:
   - Unnecessarily increases costs without additional benefits for availability.
5. **Avoid Using Dedicated Hosts**:

- Only relevant for specific licensing or physical host requirements not applicable in this scenario.

Question 62 – Incorrect

A leading e-commerce company runs its IT infrastructure on AWS Cloud. The company has a batch job running at 7AM daily on an Amazon RDS database. It processes shipping orders for the past day, and usually gets around 2000 records that need to be processed sequentially in a batch job via a shell script. The processing of each record takes about 3 seconds. What platform do you recommend to run this batch job?

Correct Option: Amazon Elastic Compute Cloud (Amazon EC2)

Explanation Behind Correct Option:

- **Amazon Elastic Compute Cloud (Amazon EC2)**:
  - **Secure, Resizable Compute Capacity**: EC2 provides flexible compute capacity in the cloud.
  - **Control**: Complete control over computing resources.
  - **Customization**: Can run customized scripts and accommodate batch processing workloads.
  - **AWS Batch**: Can be used to plan, schedule, and execute batch computing workloads on EC2 Instances.
  - **Fit for the Use-Case**: Able to handle long-running jobs and sequential processing of records without time limitations.

Incorrect Options:

1. **AWS Glue**:
   - **Purpose**: Fully managed ETL (Extract, Transform, Load) service.
   - **Limitation**: Meant for batch ETL data processing, not for running custom shell scripts.
   - **Fit**: Not suitable for the requirement to process records using a custom shell script.
2. **Amazon Kinesis Data Streams**:
   - **Purpose**: Real-time data streaming service.
   - **Use Cases**: Captures gigabytes of data per second from various sources for real-time processing.
   - **Limitation**: Designed for real-time data processing, not for batch processing of records.
   - **Fit**: Not suitable for the given use-case of batch job processing.
3. **AWS Lambda**:
   - **Purpose**: Run code without provisioning or managing servers.
   - **Limitations**: Functions can run up to 15 minutes per execution.
   - **Fit**: Total runtime for the use-case is 100 minutes (2000 records * 3 seconds per record = 6000 seconds = 100 minutes). Lambda would timeout after 15 minutes, making it unsuitable.

Conclusion / Points to Memorize:

1. **Amazon EC2**:
   - Best for long-running batch jobs.
   - Allows running custom scripts.

- Suitable for tasks requiring significant compute resources and flexibility.

2. **AWS Glue**:
   - Used for ETL tasks.
   - Not suitable for running custom shell scripts.
3. **Amazon Kinesis Data Streams**:
   - Ideal for real-time data streaming.
   - Not suitable for batch processing tasks.
4. **AWS Lambda**:
   - Good for short-duration tasks.
   - Maximum execution time of 15 minutes.
- Not suitable for tasks requiring longer processing times.

Question 63 – Correct

The engineering team at a company is running batch workloads on AWS Cloud. The team has embedded Amazon RDS database connection strings within each web server hosting the flagship application. After failing a security audit, the team is looking at a different approach to store the database secrets securely and automatically rotate the database credentials. Which of the following solutions would you recommend to meet this requirement?

Correct Option: AWS Secrets Manager

Explanation Behind Correct Option:

- **AWS Secrets Manager**:
  - **Secure Storage**: Enables secure storage and retrieval of database credentials, API keys, and other secrets.
  - **Automatic Rotation**: Supports automatic rotation of secrets with built-in integration for Amazon RDS, Amazon Redshift, and Amazon DocumentDB.
  - **API Access**: Users and applications retrieve secrets through Secrets Manager APIs, eliminating the need to hardcode sensitive information.
  - **Compliance**: Helps meet security and compliance requirements by securely rotating secrets without the need for code deployments.
  - **Integration**: Integrates with other AWS services to help audit and secure secrets.

Incorrect Options:

1. **AWS Systems Manager Parameter Store**:
   - **Purpose**: Provides secure, hierarchical storage for configuration data management and secrets management.
   - **Limitation**: Does not support automatic rotation of database credentials.
   - **Fit**: Not suitable for the requirement of automatic rotation of database credentials.
2. **AWS Systems Manager**:
   - **Purpose**: Provides visibility and control over AWS infrastructure, allowing automation of operational tasks.
   - **Limitation**: Cannot be used to store secrets securely or automatically rotate database credentials.
   - **Fit**: Not relevant for secrets management.
3. **AWS Key Management Service (KMS)**:
   - **Purpose**: Manages cryptographic keys and controls their use across AWS services.
   - **Limitation**: Cannot store secrets securely or automatically rotate database credentials.
   - **Fit**: Primarily used for encryption key management.

Conclusion / Points to Memorize:

1. **AWS Secrets Manager**:
   - Best for securely storing and automatically rotating database credentials, API keys, and other secrets.
   - Provides built-in integration for automatic rotation with Amazon RDS, Redshift, and DocumentDB.
   - Ensures compliance and enhances security by avoiding hardcoding of sensitive information.
2. **AWS Systems Manager Parameter Store**:
   - Suitable for storing configuration data and secrets, but does not support automatic rotation.
3. **AWS Systems Manager**:
   - Used for operational visibility and control, not for secrets management.
4. **AWS Key Management Service (KMS)**:
- Manages cryptographic keys for encryption, not for storing or rotating secrets.

Question 64 – Incorrect

A retail company is using AWS Site-to-Site VPN connections for secure connectivity to its AWS cloud resources from its on-premises data center. Due to a surge in traffic across the VPN connections to the AWS cloud, users are experiencing slower VPN connectivity. Which of the following options will maximize the VPN throughput?

Correct Option: Create an AWS Transit Gateway with equal cost multipath routing and add additional VPN tunnels

Explanation Behind Correct Option:

- **Create an AWS Transit Gateway with Equal Cost Multipath Routing (ECMP) and Add Additional VPN Tunnels**:
  - **AWS Transit Gateway**: Simplifies the connectivity between multiple VPCs and connects to any VPC attached to the Transit Gateway with a single VPN connection.
  - **ECMP Routing**: Scales IPsec VPN throughput by supporting multiple VPN tunnels.
  - **Scalability**: Establishing multiple VPN tunnels to an ECMP-enabled Transit Gateway can scale beyond the default maximum limit of 1.25 Gbps.
  - **Dynamic Routing**: Must enable dynamic routing on the Transit Gateway to take advantage of ECMP.

Incorrect Options:

1. **Use Transfer Acceleration for the VPN Connection to Maximize the Throughput**:
   - **Purpose**: Optimizes transfer speeds from clients to Amazon S3 buckets using Amazon CloudFront.
   - **Limitation**: Not relevant to AWS VPN connections and does not maximize VPN throughput.
   - **Fit**: Added as a distractor, not suitable for VPN connections.
2. **Use AWS Global Accelerator for the VPN Connection to Maximize the Throughput**:
   - **Purpose**: Improves the performance of user traffic using the AWS global network.
   - **Limitation**: Optimizes network paths but does not maximize VPN throughput.
   - **Fit**: Not the best fit for maximizing VPN throughput.
3. **Create a Virtual Private Gateway with Equal Cost Multipath Routing and Multiple Channels**:
   - **Purpose**: A virtual private gateway is the VPN endpoint on the Amazon side of Site-to-Site VPN connection.
   - **Limitation**: Does not support ECMP routing.
   - **Fit**: Incorrect for maximizing VPN throughput.

Conclusion / Points to Memorize:

1. **AWS Transit Gateway with ECMP**:
   - Ideal for scaling VPN throughput with support for multiple VPN tunnels.
   - Requires enabling dynamic routing to utilize ECMP.
2. **Transfer Acceleration**:
   - Not relevant for VPN connections, designed for optimizing S3 bucket transfers.
3. **AWS Global Accelerator**:
   - Improves network performance but not specifically designed for maximizing VPN throughput.
4. **Virtual Private Gateway**:

- Suitable for single VPC connections but does not support ECMP routing.

Question 65 - Correct

A company wants to adopt a hybrid cloud infrastructure where it uses some AWS services such as Amazon S3 alongside its on-premises data center. The company wants a dedicated private connection between the on-premise data center and AWS. In case of failures though, the company needs to guarantee uptime and is willing to use the public internet for an encrypted connection.

What do you recommend? (Select two)

Correct Options

- **Use AWS Direct Connect connection as a primary connection**
- **Use AWS Site-to-Site VPN as a backup connection**

Explanation Behind Correct Options

- **AWS Direct Connect connection as a primary connection**
  - **High Performance and Security**: AWS Direct Connect provides a dedicated, private network connection between your network and AWS. It avoids the internet, ensuring high performance and security.
  - **Reliable and Consistent**: It uses industry-standard 802.1q VLANs, which provide a consistent network experience compared to internet-based connections.

    - **Partitioning Capability**: This dedicated connection can be partitioned into multiple virtual interfaces, allowing access to both public resources (like Amazon S3) and private resources (like Amazon VPC) while maintaining network separation.
- **AWS Site-to-Site VPN as a backup connection**
    - **Secure and Encrypted**: AWS Site-to-Site VPN provides secure connectivity between your on-premises network and AWS VPC using IPSec to establish encrypted network connectivity over the internet.
    - **Cost-Effective Backup**: In case the Direct Connect link fails, the VPN serves as a cost-effective backup solution, leveraging the public internet but ensuring data security through encryption.
    - **Quick Setup**: VPN connections can be set up quickly and are suitable for immediate needs with low to modest bandwidth requirements.

Incorrect Options

- **Use Egress Only Internet Gateway as a backup connection**
    - **Purpose Mismatch**: Egress-Only Internet Gateway is designed for outbound IPv6 communication from instances in your VPC to the internet. It cannot be used for connecting on-premises data centers to AWS Cloud.
- **Use AWS Site-to-Site VPN as a primary connection**
    - **Not Optimal for Primary Connection**: While VPN provides secure connectivity, it relies on the public internet, which can introduce variability and is not ideal for a primary connection where high performance and reliability are critical.
- **Use AWS Direct Connect connection as a backup connection**
    - **Cost Inefficiency**: Using Direct Connect as a backup is costly and redundant. It's more logical and cost-effective to use a Site-to-Site VPN for failover scenarios since it only comes into play during primary connection failures.

Conclusion / Points to Memorize

1. **Primary Connection**: Use AWS Direct Connect for a high-performance, reliable, and secure primary connection.
2. **Backup Connection**: Use AWS Site-to-Site VPN as a cost-effective and secure backup solution.
3. **Avoid Overengineering**: Avoid using costly solutions like Direct Connect as a backup when a VPN can provide sufficient redundancy.
4. **Understand the Use Case**: Ensure that the chosen solution matches the specific requirements and constraints, like the need for encrypted connections over the public internet during failovers.