Mock Test – 4 Notes

Question 1 - Incorrect

The DevOps team at an IT company has recently migrated to AWS and they are configuring security groups for their two-tier application with public web servers and private database servers. The team wants to understand the allowed configuration options for an inbound rule for a security group.

As a solutions architect, which of the following would you identify as an INVALID option for setting up such a configuration?

Correct Option

You can use an Internet Gateway ID as the custom source for the inbound rule

Explanation

- **Security Groups:** Act as virtual firewalls that control traffic for one or more instances. You can specify one or more security groups when launching an instance or use the default security group.
- **Rules in Security Groups:** You can add rules to allow traffic to or from its associated instances. Modifications to rules are automatically applied to all instances associated with the security group.

Valid Options for Source or Destination in Security Group Rules:

- Individual IPv4 address (e.g., 203.0.113.1/32)
- Individual IPv6 address (e.g., 2001:db8:1234:1a00::123/128)
- Range of IPv4 addresses in CIDR notation (e.g., 203.0.113.0/24)
- Range of IPv6 addresses in CIDR notation (e.g., 2001:db8:1234:1a00::/64)
- Prefix list ID for AWS service (e.g., pl-1a2b3c4d)
- Another security group (e.g., current security group, different security group for the same VPC, different security group for a peer VPC in a VPC peering connection)

Therefore, **an Internet Gateway ID cannot be used as the custom source for an inbound rule**.

Incorrect Options

1. **You can use a security group as the custom source for the inbound rule**
   - **Explanation:** Valid configuration. Allows instances associated with the specified security group to access instances associated with this security group.
2. **You can use a range of IP addresses in CIDR block notation as the custom source for the inbound rule**
   - **Explanation:** Valid configuration. Allows specifying a range of IP addresses using CIDR notation.
3. **You can use an IP address as the custom source for the inbound rule**
   - **Explanation:** Valid configuration. Allows specifying an individual IP address.

Conclusion / Points to Memorize

- **Security Group Rules:** Control traffic to and from instances.
- **Allowed Sources/Destinations:**
  - Individual IPv4/IPv6 addresses
  - Range of IPv4/IPv6 addresses in CIDR notation
  - Prefix list ID for AWS service
  - Other security groups
    - **Invalid Option:** Internet Gateway ID cannot be used as a custom source for inbound rules.

Question 2 - Correct

An IT company hosts Windows-based applications on its on-premises data center. The company is looking at moving the business to the AWS Cloud. The cloud solution should offer shared storage space that multiple applications can access without a need for replication. Also, the solution should integrate with the company's self-managed Active Directory domain.

Which of the following solutions addresses these requirements with the minimal integration effort?

Correct Option

Use Amazon FSx for Windows File Server as a shared storage solution

Explanation

- **Amazon FSx for Windows File Server:** Provides fully managed, highly reliable, and scalable file storage accessible over the Server Message Block (SMB) protocol.
- **Integration with Active Directory:** Built on Windows Server, it integrates with Microsoft Active Directory (AD), providing features such as user quotas and end-user file restore.
- **Deployment Options:** Offers single-AZ and multi-AZ deployment options, fully managed backups, and encryption of data at rest and in transit.

- **Cost and Performance Optimization:** You can optimize cost and performance with SSD and HDD storage options. The service starts at $0.013 per GB-month and supports data deduplication to reduce costs.
- **Scalability:** You can increase file system storage and scale throughput capacity at any time, without upfront costs or licensing fees.

How It Works:

1. **Create an FSx for Windows File Server file system:** In minutes, create a Windows-native file system integrated with your Active Directory.
2. **Configure file shares:** Set up as many Windows file shares as needed on your file system and establish access permissions.
3. **Connect to your file shares:** Access your file shares from your application servers and end-user compute instances.
4. **Run your applications:** Use Amazon FSx file systems to share file data across application servers and end-users.

Incorrect Options

1. **Use File Gateway of AWS Storage Gateway to create a hybrid storage solution**
   - **Explanation:** AWS Storage Gateway connects on-premises software with cloud-based storage, integrating on-premises IT with AWS storage infrastructure. It uses Amazon S3 for cloud storage but is not suited as a shared storage space for multiple applications to access in parallel.
2. **Use Amazon FSx for Lustre as a shared storage solution with millisecond latencies**
   - **Explanation:** Amazon FSx for Lustre is a fully managed service providing high-performance storage for compute workloads like machine learning and HPC. It is Linux-based, not suitable for Windows-based applications.
3. **Use Amazon Elastic File System (Amazon EFS) as a shared storage solution**
   - **Explanation:** Amazon EFS provides a scalable, fully managed elastic NFS file system. It is compatible only with Linux-based AMIs for Amazon EC2 and not suitable for Windows-based applications.

Conclusion / Points to Memorize

- **Amazon FSx for Windows File Server:**
  - Fully managed, highly reliable, scalable file storage.
  - Accessible over SMB protocol, integrates with Microsoft Active Directory.
  - Offers single-AZ and multi-AZ deployment options.
  - Supports SSD and HDD storage, starting at $0.013 per GB-month.
  - Provides data deduplication to optimize costs.
  - Scalable storage and throughput capacity.
- **Other Solutions:**
  - **File Gateway:** Suited for hybrid storage, not parallel access by multiple applications.
  - **FSx for Lustre:** High-performance storage for compute workloads, Linux-based.
    - **Amazon EFS:** Scalable NFS file system, only for Linux-based applications.

Question 3 - Correct

A company recently experienced a database outage in its on-premises data center. The company now wants to migrate to a reliable database solution on AWS that minimizes data loss and stores every transaction on at least two nodes.

Which of the following solutions meets these requirements?

Correct Option

Set up an Amazon RDS MySQL DB instance with Multi-AZ functionality enabled to synchronously replicate the data

Explanation

- **Amazon RDS Multi-AZ Deployment:** When you provision an RDS Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ).
- **High Availability:** Each AZ runs on its own physically distinct, independent infrastructure, engineered to be highly reliable. This setup enhances availability during planned system maintenance and helps protect databases against instance failure and AZ disruption.
- **Automatic Failover:** In the event of a planned or unplanned outage, Amazon RDS automatically switches to a standby replica in another AZ. Failover times are typically 60–120 seconds.

How It Works:

1. **Primary Instance:** Operates in one Availability Zone.
2. **Standby Instance:** Synchronously replicates data in another Availability Zone.
3. **Failover Process:** In case of a failure, the standby instance becomes the primary, and a new standby is created.

Incorrect Options

1. **Set up an Amazon RDS MySQL DB instance and then create a read replica in another Availability Zone that synchronously replicates the data**

- **Explanation:** Read replicas in Amazon RDS are asynchronously replicated, not synchronously. They are used for read-heavy workloads to offload read traffic from the primary instance.

2. **Set up an Amazon RDS MySQL DB instance and then create a read replica in a separate AWS Region that synchronously replicates the data**
   - **Explanation:** Similar to the previous option, read replicas are asynchronously replicated and do not provide synchronous replication needed for high availability and minimal data loss.
3. **Set up an Amazon EC2 instance with a MySQL DB engine installed that triggers an AWS Lambda function to synchronously replicate the data to an Amazon RDS MySQL DB instance**
   - **Explanation:** This solution is complex and less reliable. Managing the EC2 instance and setting up Lambda for replication adds unnecessary complexity. RDS Multi-AZ provides built-in, out-of-the-box high availability.

Conclusion / Points to Memorize

- **Amazon RDS Multi-AZ:**
  - Provides high availability and durability.
  - Synchronous replication between primary and standby instances.
  - Automatic failover to standby in case of failure.
  - Suitable for minimizing data loss and ensuring every transaction is stored on at least two nodes.
- **Read Replicas:**
  - Asynchronous replication.
  - Used for offloading read traffic.
  - Not suitable for high availability or minimizing data loss.
- **Complex Solutions:**
  - Using EC2 with Lambda for replication is unnecessary when RDS Multi-AZ provides a simpler, built-in solution.

Question 4 - **Incorrect**

An AWS Organization is using Service Control Policies (SCPs) for central control over the maximum available permissions for all accounts in their organization. This allows the organization to ensure that all accounts stay within the organization's access control guidelines.

Which of the given scenarios are correct regarding the permissions described below? (Select three)

Correct Options

1. **If a user or role has an IAM permission policy that grants access to an action that is either not allowed or explicitly denied by the applicable service control policy (SCP), the user or role can't perform that action**
2. **Service control policy (SCP) affects all users and roles in the member accounts, including root user of the member accounts**
3. **Service control policy (SCP) does not affect service-linked roles**

Explanation

- **Service Control Policies (SCPs):** SCPs offer central control over the maximum available permissions for all accounts in an AWS Organization. They help ensure that all accounts adhere to the organization's access control guidelines.
- **Effect on Permissions:** SCPs can restrict AWS services, resources, and individual API actions for users and roles in each member account. These restrictions apply even to administrators of member accounts.
- **Specific Effects:**
  - **IAM Policies:** If a user or role has an IAM permission policy that grants access to an action not allowed or explicitly denied by the SCP, they cannot perform that action.
  - **Scope of SCPs:** SCPs affect all users and roles, including the root user of member accounts, but do not affect service-linked roles.

How It Works:

1. **SCPs Overview:** Central control over permissions for all accounts.
2. **Restrictions:** Can override IAM policies.
3. **Affected Entities:** All users and roles in member accounts, including root users, are affected, but service-linked roles are not.

Incorrect Options

1. **If a user or role has an IAM permission policy that grants access to an action that is either not allowed or explicitly denied by the applicable service control policy (SCP), the user or role can still perform that action**
   - **Explanation:** This is incorrect because SCPs override IAM policies, preventing the user or role from performing the action.
2. **Service control policy (SCP) affects all users and roles in the member accounts, excluding root user of the member accounts**
   - **Explanation:** This is incorrect because SCPs do affect the root user of member accounts.
3. **Service control policy (SCP) affects service-linked roles**

- **Explanation:** This is incorrect because SCPs do not affect service-linked roles.

Conclusion / Points to Memorize

- **Service Control Policies (SCPs):**
  - Central control over permissions for all accounts.
  - Can restrict AWS services, resources, and API actions.
  - Override IAM policies.
  - Apply to all users and roles, including root users.
  - Do not affect service-linked roles.
- **Important Rules:**
  - SCPs affect all users and roles in member accounts, including the root user.
  - SCPs do not affect service-linked roles.
    - Actions not allowed or explicitly denied by an SCP cannot be performed, even if granted by an IAM policy.

Question 5 - Incorrect

A media startup is looking at hosting their web application on AWS Cloud. The application will be accessed by users from different geographic regions of the world to upload and download video files that can reach a maximum size of 10 gigabytes. The startup wants the solution to be cost-effective and scalable with the lowest possible latency for a great user experience.

As a Solutions Architect, which of the following will you suggest as an optimal solution to meet the given requirements?

Correct Option

Use Amazon S3 for hosting the web application and use Amazon S3 Transfer Acceleration (Amazon S3TA) to reduce the latency that geographically dispersed users might face.

Explanation

- **Amazon S3 Transfer Acceleration (S3TA):** Speeds up content transfers to and from Amazon S3 by as much as 50-500% for long-distance transfers of larger objects. Ideal for web or mobile applications with widespread users or applications hosted far from their S3 bucket.
- **Performance Improvement:** Routes traffic through Amazon CloudFront's globally distributed Edge Locations and over AWS backbone networks, using network protocol optimizations.
- **Reducing Variability:** S3TA helps avoid variability in Internet routing and congestion by routing uploads and downloads over the AWS global network infrastructure, leveraging AWS network optimizations.

How It Works:

1. **S3 Transfer Acceleration:** Optimizes TCP protocol and adds intelligence between the client and the S3 bucket.
2. **Optimal for Large Objects:** Best for objects larger than 1GB or data sets exceeding 1GB.
3. **Routing through Edge Locations:** Utilizes CloudFront Edge Locations and AWS backbone networks for improved performance.

Incorrect Options

1. **Use Amazon S3 for hosting the web application and use Amazon CloudFront for faster distribution of content to geographically dispersed users**
   - **Explanation:** While powerful for distributing static content with low latency, CloudFront's PUT/POST commands are optimal for objects smaller than 1GB. For larger objects, S3 Transfer Acceleration is a better choice.
2. **Use Amazon EC2 with AWS Global Accelerator for faster distribution of content, while using Amazon S3 as storage service**
   - **Explanation:** AWS Global Accelerator improves user performance by up to 60% but is not designed for speeding up S3 uploads or downloads. It simplifies traffic management and improves performance for other AWS application origins.
3. **Use Amazon EC2 with Amazon ElastiCache for faster distribution of content, while Amazon S3 can be used as a storage service**
   - **Explanation:** Amazon ElastiCache is suitable for in-memory data stores and real-time use cases like caching and session stores. S3 Transfer Acceleration provides better performance for large file uploads and downloads.

Conclusion / Points to Memorize

- **Amazon S3 Transfer Acceleration:**
  - Ideal for long-distance transfers of larger objects (greater than 1GB).
  - Uses CloudFront's Edge Locations and AWS backbone networks.
  - Reduces latency and variability in Internet routing.
- **Amazon CloudFront:**
  - Best for distributing static content with low latency.
  - Optimal for objects smaller than 1GB.
- **AWS Global Accelerator:**

- Improves performance by routing traffic through AWS global network.
- Not designed for S3 uploads or downloads.

- **Amazon ElastiCache:**
  - Suitable for real-time data-intensive applications.
  - Not optimal for file transfers to and from S3.

Question 6 - Incorrect

The engineering team at a company wants to use Amazon Simple Queue Service (Amazon SQS) to decouple components of the underlying application architecture. However, the team is concerned about the VPC-bound components accessing Amazon Simple Queue Service (Amazon SQS) over the public internet.

As a solutions architect, which of the following solutions would you recommend to address this use-case?

Correct Option

Use VPC endpoint to access Amazon SQS

Explanation

- **VPC Endpoints:** Allow AWS customers to privately connect their Amazon VPC to supported AWS services like Amazon SQS without using public IPs or traversing the public internet.
- **AWS PrivateLink:** Powers VPC endpoints, enabling private connectivity and ensuring data remains within the Amazon network.
- **Benefits:**
  - **Secure and Reliable Connectivity:** No need for an internet gateway, NAT instance, VPN connection, or AWS Direct Connect.
  - **Protects Instances from Internet Traffic:** Ensures data transfer between VPC and SQS stays private.

How It Works:

1. **Configuration:** Easy to set up VPC endpoints.
2. **Private Connectivity:** Utilizes AWS PrivateLink for secure data transfer.
3. **No Public Internet Exposure:** Eliminates the need for public IPs and internet traffic.

Incorrect Options

1. **Use Internet Gateway to access Amazon SQS**
   - **Explanation:** An internet gateway allows communication between VPC instances and the internet. However, it uses the public internet, which the team wants to avoid.
2. **Use VPN connection to access Amazon SQS**
   - **Explanation:** AWS Site-to-Site VPN securely connects on-premises networks to Amazon VPC over the internet. Since the infrastructure is within AWS, VPN is unnecessary and still involves internet traffic.
3. **Use Network Address Translation (NAT) instance to access Amazon SQS**
   - **Explanation:** NAT instances enable private subnet instances to initiate outbound internet traffic while preventing inbound traffic. This solution involves internet access, which the team wants to avoid.

Conclusion / Points to Memorize

- **Amazon SQS Access:**
  - Use **VPC endpoints** for private, secure, and reliable connectivity without public internet exposure.
  - **AWS PrivateLink:** Ensures secure data transfer within the Amazon network.
- **Incorrect Solutions:**
  - **Internet Gateway:** Uses public internet, not suitable for private access needs.
  - **VPN Connection:** Meant for connecting on-premises networks, involves internet traffic.
  - **NAT Instance:** Provides internet access to private subnets, not suitable for avoiding internet exposure.

Question 7 - Incorrect

A financial services company is looking to move its on-premises IT infrastructure to AWS Cloud. The company has multiple long-term server-bound licenses across the application stack and the CTO wants to continue to utilize those licenses while moving to AWS.

As a solutions architect, which of the following would you recommend as the MOST cost-effective solution?

Correct Option

Use Amazon EC2 dedicated hosts

Explanation

- **Amazon EC2 Dedicated Hosts:** Allow launching EC2 instances on physical servers dedicated for your use. Provide additional visibility and control over how instances are placed on a physical server and enable reliable use of the same physical server over time.
- **Utilizing Existing Licenses:** Dedicated Hosts allow you to use existing server-bound software licenses, such as Windows Server, and meet corporate compliance and regulatory requirements.

How It Works:

1. **Dedicated Physical Servers:** EC2 instances run on physical servers exclusively used by your account.
2. **Control and Visibility:** Offers more control over instance placement and physical server usage.
3. **License Utilization:** Suitable for long-term server-bound software licenses.

Incorrect Options

1. **Use Amazon EC2 dedicated instances**
   - **Explanation:** Dedicated instances run on hardware dedicated to a single customer but can share hardware with other instances from the same AWS account. They do not provide the same level of control as Dedicated Hosts and cannot be used for existing server-bound software licenses.
2. **Use Amazon EC2 reserved instances (RI)**
   - **Explanation:** Reserved instances offer cost savings by committing to a specific instance configuration for 1 or 3 years. However, they do not provide the necessary control for utilizing server-bound licenses.
3. **Use Amazon EC2 on-demand instances**
   - **Explanation:** On-demand instances allow you to pay by the second for the instances you launch. They offer flexibility but do not provide the control required for using server-bound licenses and are generally more expensive for long-term use.

Additional Details on EC2 Purchasing Options:

- **On-Demand Instances:** Pay for compute capacity by the second with no long-term commitment.
- **Reserved Instances (RI):** Commitment to a specific instance type and region for 1 or 3 years, providing cost savings.

Conclusion / Points to Memorize

- **Amazon EC2 Dedicated Hosts:**
  - Suitable for using long-term server-bound software licenses.
  - Provide dedicated physical servers for exclusive use.
  - Offer control over instance placement and server usage.
- **Amazon EC2 Dedicated Instances:**
  - Run on hardware dedicated to a single customer but can share hardware within the same account.
  - Not suitable for server-bound licenses.
- **Amazon EC2 Reserved Instances (RI) and On-Demand Instances:**
  - Offer cost savings and flexibility respectively but do not support server-bound licenses.

Question 8 - **Incorrect**

An engineering lead is designing a VPC with public and private subnets. The VPC and subnets use IPv4 CIDR blocks. There is one public subnet and one private subnet in each of three Availability Zones (AZs) for high availability. An internet gateway is used to provide internet access for the public subnets. The private subnets require access to the internet to allow Amazon EC2 instances to download software updates.

Which of the following options represents the correct solution to set up internet access for the private subnets?

Correct Option

Set up three NAT gateways, one in each public subnet in each AZ. Create a custom route table for each AZ that forwards non-local traffic to the NAT gateway in its AZ

Explanation

- **NAT Gateways:** Enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating connections with those instances.
- **Public Subnet Requirement:** NAT gateways must be set up in public subnets.
- **High Availability:** Each NAT gateway is created in a specific Availability Zone and is implemented with redundancy in that zone. For high availability, a NAT gateway should be created in each AZ.

How It Works:

1. **Create NAT Gateway in Public Subnet:** Specify a public subnet and associate an Elastic IP address with the NAT gateway.
2. **Update Route Table:** Update the route table for private subnets to point internet-bound traffic to the NAT gateway.
3. **Redundancy:** Create a NAT gateway in each Availability Zone to ensure high availability and fault tolerance.

Incorrect Options

1. **Set up three NAT gateways, one in each private subnet in each AZ. Create a custom route table for each AZ that forwards non-local traffic to the NAT gateway in its AZ**
   - **Explanation:** NAT gateways need to be set up in public subnets, not private subnets.
2. **Set up three internet gateways, one in each private subnet in each AZ. Create a custom route table for each AZ that forwards non-local traffic to the internet gateway in its AZ**
   - **Explanation:** Internet gateways cannot be provisioned in private subnets. They are used to provide internet access for public subnets.
3. **Set up three egress-only internet gateways, one in each public subnet in each AZ. Create a custom route table for each AZ that forwards non-local traffic to the egress-only internet gateway in its AZ**
   - **Explanation:** Egress-only internet gateways allow outbound communication over IPv6 from instances in your VPC to the internet, preventing inbound IPv6 connections. The use-case here is for IPv4 traffic, making this option unsuitable.

Conclusion / Points to Memorize

- **NAT Gateways:**
  - Must be set up in public subnets.
  - Enable private subnet instances to connect to the internet.
  - Provide redundancy and high availability by being set up in each AZ.
  - Require Elastic IP addresses.
- **Incorrect Configurations:**
  - **NAT Gateways in Private Subnets:** Incorrect because NAT gateways must be in public subnets.
  - **Internet Gateways in Private Subnets:** Incorrect because internet gateways cannot be provisioned in private subnets.
  - **Egress-Only Internet Gateways:** Suitable for IPv6 traffic, not for IPv4 traffic as required in this use case.

Question 9 - I**ncorrect**

A video conferencing application is hosted on a fleet of EC2 instances which are part of an Auto Scaling group. The Auto Scaling group uses a Launch Template (LT1) with "dedicated" instance tenancy but the VPC (V1) used by the Launch Template LT1 has the instance tenancy set to default. Later the DevOps team creates a new Launch Template (LT2) with shared (default) instance tenancy but the VPC (V2) used by the Launch Template LT2 has the instance tenancy set to dedicated.

Which of the following is correct regarding the instances launched via Launch Template LT1 and Launch Template LT2?

Correct Option

The instances launched by both Launch Template LT1 and Launch Template LT2 will have dedicated instance tenancy

Explanation

- **Launch Template:** Specifies instance configuration information such as AMI ID, instance type, key pair, security groups, and other parameters for launching EC2 instances.
- **Instance Tenancy Control:** Controlled by the tenancy attribute of the VPC if the Launch Template Tenancy is set to shared (default). If the Launch Template Tenancy is set to dedicated, the instances will have dedicated tenancy regardless of the VPC tenancy setting.
- **Tenancy Scenarios:**
  - **Launch Template Tenancy (default) + VPC Tenancy (dedicated):** Instances will have dedicated tenancy.
  - **Launch Template Tenancy (dedicated) + VPC Tenancy (default):** Instances will have dedicated tenancy.

How It Works:

1. **Launch Template LT1:** Set to dedicated instance tenancy.
2. **VPC V1:** Set to default instance tenancy.
   - **Result:** Instances launched by LT1 will have dedicated tenancy.
3. **Launch Template LT2:** Set to shared (default) instance tenancy.
4. **VPC V2:** Set to dedicated instance tenancy.
   - **Result:** Instances launched by LT2 will have dedicated tenancy.

Incorrect Options

1. **The instances launched by Launch Template LT1 will have dedicated instance tenancy while the instances launched by the Launch Template LT2 will have shared (default) instance tenancy**
   - **Explanation:** If either the Launch Template Tenancy or the VPC Tenancy is set to dedicated, the instances will have dedicated tenancy. This option is incorrect.

2. **The instances launched by both Launch Template LT1 and Launch Template LT2 will have default instance tenancy**
    - **Explanation:** Since the VPC Tenancy for V2 is set to dedicated, instances launched by LT2 will have dedicated tenancy. This option is incorrect.
3. **The instances launched by Launch Template LT1 will have default instance tenancy while the instances launched by the Launch Template LT2 will have dedicated instance tenancy**
    - **Explanation:** Since the Launch Template Tenancy for LT1 is set to dedicated, instances launched by LT1 will have dedicated tenancy. This option is incorrect.

Additional Details on EC2 Tenancy Options:

- **Shared (default):** Multiple AWS accounts may share the same physical hardware.
- **Dedicated Instances:** Instances run on single-tenant hardware, physically isolated from instances in other accounts.
- **Dedicated Hosts:** Instances run on physical servers dedicated to your use, suitable for BYOL (Bring Your Own License) requirements.

Conclusion / Points to Memorize

- **Instance Tenancy Control:**
    - If either the Launch Template Tenancy or the VPC Tenancy is set to dedicated, the instances will have dedicated tenancy.
    - Default tenancy allows sharing hardware with other AWS accounts.
- **Correct Tenancy Scenarios:**
    - **LT1 (dedicated) + V1 (default):** Dedicated tenancy.
    - **LT2 (default) + V2 (dedicated):** Dedicated tenancy.
- **Incorrect Configurations:**
    - Assuming default tenancy when either LT or VPC is set to dedicated is incorrect.

Question 10 - Incorrect

A retail organization is moving some of its on-premises data to AWS Cloud. The DevOps team at the organization has set up an AWS Managed IPSec VPN Connection between their remote on-premises network and their Amazon VPC over the internet.

Which of the following represents the correct configuration for the IPSec VPN Connection?

Correct Option

Create a virtual private gateway (VGW) on the AWS side of the VPN and a Customer Gateway on the on-premises side of the VPN

Explanation

- **Virtual Private Gateway (VGW):** The endpoint on the AWS VPC side of your VPN connection. It serves as a connection point for the IPSec VPN.
- **Customer Gateway (CGW):** An AWS resource that provides information to AWS about the customer's gateway device. The customer gateway device is the physical device or software application on the customer side of the VPN connection.
- **AWS Site-to-Site VPN:** A secure connection between your on-premises equipment and your VPCs over the internet.

How It Works:

1. **Virtual Private Gateway (VGW):** Created on the AWS side of the VPN.
2. **Customer Gateway (CGW):** Created on the on-premises side of the VPN.
3. **VPN Connection:** Establishes a secure, encrypted connection between the VGW and CGW.

Incorrect Options

1. **Create a virtual private gateway (VGW) on the on-premises side of the VPN and a Customer Gateway on the AWS side of the VPN**
    - **Explanation:** The VGW should be on the AWS side and the CGW on the on-premises side, making this option incorrect.
2. **Create a Customer Gateway on both the AWS side of the VPN as well as the on-premises side of the VPN**
    - **Explanation:** Only the on-premises side requires a CGW. The AWS side needs a VGW, making this option incorrect.
3. **Create a virtual private gateway (VGW) on both the AWS side of the VPN as well as the on-premises side of the VPN**
    - **Explanation:** The VGW is only required on the AWS side, and a CGW is required on the on-premises side, making this option incorrect.

Additional Details:

- **VPN Tunnel:** An encrypted link for data transfer between the customer network and AWS.
- **IPSec VPN:** Provides secure communication over the internet using encryption.

Conclusion / Points to Memorize

- **Correct Configuration for AWS Managed IPSec VPN:**
    - **VGW on AWS Side:** Acts as the endpoint for the VPN connection.
    - **CGW on On-Premises Side:** Provides information to AWS about the customer's gateway device.
- **Incorrect Configurations:**

- VGW or CGW should not be set up on both sides; each has a specific role.
- Ensure the correct assignment of VGW and CGW according to their respective roles.

Question 11 - Correct

A company has a hybrid cloud structure for its on-premises data center and AWS Cloud infrastructure. The company wants to build a web log archival solution such that only the most frequently accessed logs are available as cached data locally while backing up all logs on Amazon S3.

As a solutions architect, which of the following solutions would you recommend for this use-case?

Correct Option

Use AWS Volume Gateway - Cached Volume - to store the most frequently accessed logs locally for low-latency access while storing the full volume with all logs in its Amazon S3 service bucket

Explanation

- **AWS Storage Gateway:** A hybrid cloud storage service providing on-premises access to virtually unlimited cloud storage.
- **Volume Gateway - Cached Volume:** Stores the full volume in Amazon S3 while retaining the most frequently accessed data locally for low-latency access.
- **Use-Case Fit:** Perfect for scenarios where frequently accessed logs need low-latency access, while all logs are backed up in Amazon S3.

How It Works:

1. **Volume Gateway - Cached Volume:** Stores recently accessed data locally.
2. **Full Backup in Amazon S3:** Ensures that all logs are stored securely and can be retrieved when needed.
3. **Low-Latency Access:** Provides quick access to frequently accessed logs.

Incorrect Options

1. **Use AWS Direct Connect to store the most frequently accessed logs locally for low-latency access while storing the full backup of logs in an Amazon S3 bucket**
   - **Explanation:** AWS Direct Connect establishes a dedicated network connection between your network and AWS locations. It cannot be used to store logs locally for low-latency access.
2. **Use AWS Volume Gateway - Stored Volume - to store the most frequently accessed logs locally for low-latency access while storing the full volume with all logs in its Amazon S3 service bucket**
   - **Explanation:** Stored Volumes keep the entire data volume locally for fast read access and maintain an asynchronous copy in Amazon S3. This does not fit the use-case where only frequently accessed logs should be cached locally.
3. **Use AWS Snowball Edge Storage Optimized device to store the most frequently accessed logs locally for low-latency access while storing the full backup of logs in an Amazon S3 bucket**
   - **Explanation:** Snowball Edge Storage Optimized devices are used for securely and quickly transferring large amounts of data to AWS. They are not suitable for storing frequently accessed logs locally for low-latency access.

Additional Details:

- **AWS Volume Gateway - Cached Volume:**
  - **Local Cache:** Stores frequently accessed data for low-latency access.
  - **Full Backup:** Stores the entire volume in Amazon S3.

Conclusion / Points to Memorize

- **AWS Volume Gateway - Cached Volume:**
  - Ideal for scenarios requiring low-latency access to frequently accessed data.
  - Stores the full data volume in Amazon S3.
- **Incorrect Configurations:**
  - **AWS Direct Connect:** Not suitable for storing data locally for low-latency access.
  - **AWS Volume Gateway - Stored Volume:** Keeps the entire volume locally, not just frequently accessed logs.
  - **AWS Snowball Edge:** Used for large data transfers, not for local low-latency access to frequently accessed logs.

Question 12 - Incorrect

A company has hired you as an AWS Certified Solutions Architect – Associate to help with redesigning a real-time data processor. The company wants to build custom applications that process and analyze the streaming data for its specialized needs.

Which solution will you recommend to address this use-case?

Correct Option

Use Amazon Kinesis Data Streams to process the data streams as well as decouple the producers and consumers for the real-time data processor

Explanation

- **Amazon Kinesis Data Streams:** Useful for rapidly moving data off data producers and then continuously processing the data. It allows for transforming data before emitting it to a data store, running real-time metrics and analytics, or deriving more complex data streams for further processing.
- **Capabilities:** Can continuously capture gigabytes of data per second from hundreds of thousands of sources like website clickstreams, database event streams, financial transactions, social media feeds, IT logs, and location-tracking events.

How It Works:

1. **Data Capture:** Ingests and stores data streams for processing.
2. **Data Processing:** Build custom, real-time applications using Kinesis Data Analytics, Spark on EMR, Amazon EC2, AWS Lambda, etc.
3. **Output:** Analyze streaming data using favorite BI tools.

Incorrect Options

1. **Use Amazon Simple Notification Service (Amazon SNS) to process the data streams as well as decouple the producers and consumers for the real-time data processor**
   - **Explanation:** SNS is a pub/sub messaging service that enables decoupling microservices, distributed systems, and serverless applications. It is not designed for processing and analyzing streaming data for custom applications.
2. **Use Amazon Simple Queue Service (Amazon SQS) to process the data streams as well as decouple the producers and consumers for the real-time data processor**
   - **Explanation:** SQS offers a secure, durable, and available hosted queue for integrating and decoupling distributed software systems and components. It is not suitable for real-time data processing and analysis as described in the use case.
3. **Use Amazon Kinesis Data Firehose to process the data streams as well as decouple the producers and consumers for the real-time data processor**
   - **Explanation:** Kinesis Data Firehose is the easiest way to load streaming data into data stores and analytics tools like Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk. It cannot be used to process and analyze streaming data in custom applications.

Additional Details:

- **Kinesis Data Streams:**
  - Enables real-time data processing and analysis.
  - Decouples producers and consumers for data streams.
- **Kinesis Data Firehose:**
  - Loads streaming data into data stores and analytics tools.
  - Suitable for capturing, transforming, and loading data into specified destinations.

Conclusion / Points to Memorize

- **Amazon Kinesis Data Streams:**
  - Ideal for processing and analyzing streaming data in custom applications.
  - Decouples producers and consumers for real-time data processing.
- **Incorrect Configurations:**
  - **Amazon SNS:** Not designed for real-time data processing and analysis.
  - **Amazon SQS:** Suitable for decoupling distributed systems, not real-time data analysis.
  - **Amazon Kinesis Data Firehose:** Suitable for loading data into data stores, not for custom data processing and analysis.

Question 13 - Correct

The DevOps team at a multinational company is helping its subsidiaries standardize Amazon EC2 instances by using the same Amazon Machine Image (AMI). Some of these subsidiaries are in the same AWS region but use different AWS accounts, whereas others are in different AWS regions but use the same AWS account as the parent company. The DevOps team has hired you as a solutions architect for this project.

Which of the following would you identify as CORRECT regarding the capabilities of an Amazon Machine Image (AMI)? (Select three)

Correct Options

1. **You can copy an Amazon Machine Image (AMI) across AWS Regions**
2. **You can share an Amazon Machine Image (AMI) with another AWS account**
3. **Copying an Amazon Machine Image (AMI) backed by an encrypted snapshot cannot result in an unencrypted target snapshot**

Explanation

- **Amazon Machine Image (AMI):** Provides the information required to launch an instance, including Amazon EBS snapshots, launch permissions, and block device mappings.
- **Copying AMIs:**

- **Across Regions:** AMIs can be copied within or across AWS regions using the AWS Management Console, CLI, SDKs, or EC2 API.
- **Encrypted Snapshots:** An encrypted snapshot cannot be copied to yield an unencrypted target snapshot.
- **Shared AMIs:** AMIs can be shared with other AWS accounts.

How It Works:

1. **Copying Across Regions:** Use the CopyImage action to copy AMIs across regions.
2. **Encryption Rules:** While you can copy an unencrypted snapshot to yield an encrypted snapshot, you cannot do the reverse.
3. **Sharing with Other Accounts:** AMIs can be shared, and permissions need to be set for the associated storage.

Incorrect Options

1. **You cannot share an Amazon Machine Image (AMI) with another AWS account**
   - **Explanation:** AMIs can indeed be shared with other AWS accounts, provided appropriate permissions are granted.
2. **Copying an Amazon Machine Image (AMI) backed by an encrypted snapshot results in an unencrypted target snapshot**
   - **Explanation:** An encrypted snapshot cannot be copied to yield an unencrypted target snapshot.
3. **You cannot copy an Amazon Machine Image (AMI) across AWS Regions**
   - **Explanation:** AMIs can be copied across AWS regions using the CopyImage action.

Additional Details:

- **Copying AMIs:**
  - Supports encrypted-to-encrypted and unencrypted-to-encrypted scenarios.
  - Does not support encrypted-to-unencrypted copying.

Conclusion / Points to Memorize

- **Amazon Machine Image (AMI):**
  - Provides necessary information to launch instances.
  - Includes EBS snapshots, launch permissions, and block device mappings.
- **Capabilities:**
  - **Copying Across Regions:** Supported using the CopyImage action.
  - **Sharing with Accounts:** Supported with appropriate permissions.
  - **Encryption Rules:** Encrypted snapshots cannot be copied to yield unencrypted snapshots.

Question 14 - Correct

A DevOps engineer at an IT company just upgraded an Amazon EC2 instance type from t2.nano (0.5G of RAM, 1 vCPU) to u-12tb1.metal (12.3 TB of RAM, 448 vCPUs). How would you categorize this upgrade?

Correct Option

This is a scale up example of vertical scalability

Explanation

- **Vertical Scalability (Scale Up):** Involves increasing the size of the instance (e.g., upgrading from a smaller instance type like t2.nano to a larger instance type like u-12tb1.metal). It is commonly used for non-distributed systems, such as databases.
- **Horizontal Scalability (Scale Out):** Involves increasing the number of instances/systems for the application (e.g., adding more instances to handle increased load).

How It Works:

1. **Scale Up:** Upgrading to a larger instance type (more RAM, vCPUs).
2. **Scale Down:** Downgrading to a smaller instance type.
3. **Vertical vs. Horizontal:**
   - Vertical (Scale Up/Down): Changing instance size.
   - Horizontal (Scale Out/In): Changing instance count.

Incorrect Options

1. **This is a scale up example of horizontal scalability**
   - **Explanation:** Scale up is associated with vertical scalability, not horizontal scalability.
2. **This is a scale out example of vertical scalability**
   - **Explanation:** Scale out is associated with horizontal scalability, not vertical scalability.
3. **This is an example of high availability**

- **Explanation:** High availability involves running applications across multiple data centers (Availability Zones) to survive data center loss, not scaling up instances.

Additional Details:

- **Vertical Scaling:** Limited by hardware limits.
- **Horizontal Scaling:** Can be more flexible and handle distributed workloads.

Conclusion / Points to Memorize

- **Vertical Scaling (Scale Up/Down):** Changing the instance size.
- **Horizontal Scaling (Scale Out/In):** Changing the number of instances.
- **High Availability:** Running applications across multiple Availability Zones for resilience.

Question 15 - Correct

A retail company has its flagship application running on a fleet of Amazon EC2 instances behind Elastic Load Balancing (ELB). The engineering team has been seeing recurrent issues wherein the in-flight requests from the ELB to the Amazon EC2 instances are getting dropped when an instance becomes unhealthy.

Which of the following features can be used to address this issue?

Correct Option

Connection Draining

Explanation

- **Connection Draining:** Ensures that the ELB stops sending requests to instances that are de-registering or unhealthy while keeping existing connections open, allowing in-flight requests to complete. The timeout can be set between 1 and 3,600 seconds.

How It Works:

1. **Connection Draining:** Stops sending new requests to unhealthy instances but allows existing connections to complete.
2. **Timeout Configuration:** Set between 1 and 3,600 seconds (default is 300 seconds).

Incorrect Options

1. **Cross Zone load balancing**
   - **Explanation:** Distributes requests across all registered targets in all enabled Availability Zones. Does not handle in-flight requests to unhealthy instances.
2. **Sticky Sessions**
   - **Explanation:** Binds a user's session to a specific instance, ensuring all requests during the session go to the same instance. Does not handle in-flight requests to unhealthy instances.
3. **Idle Timeout**
   - **Explanation:** Maintains connections between the client and the load balancer. Closes connections if no data is sent/received within the idle timeout period. Does not handle in-flight requests to unhealthy instances.

Additional Details:

- **Connection Draining:** Vital for graceful handling of de-registering or unhealthy instances.

Conclusion / Points to Memorize

- **Connection Draining:** Ensures in-flight requests to unhealthy or de-registering instances are completed.
- **Cross Zone Load Balancing:** Distributes requests across all registered targets in all enabled Availability Zones.
- **Sticky Sessions:** Binds a user's session to a specific instance.
- **Idle Timeout:** Closes connections if no data is sent/received within the specified timeout period.

Question 16 - Correct

A financial services company is migrating their messaging queues from self-managed message-oriented middleware systems to Amazon Simple Queue Service (Amazon SQS). The development team at the company wants to minimize the costs of using Amazon SQS.

As a solutions architect, which of the following options would you recommend for the given use-case?

Correct Option

Use SQS long polling to retrieve messages from your Amazon SQS queues

Explanation

- **Amazon Simple Queue Service (Amazon SQS):** A fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications.

- **Long Polling:** Delays the response to a ReceiveMessage request until a message arrives in the queue or the long polling timeout is reached. Reduces the number of empty receives and hence reduces cost.

How It Works:

1. **Long Polling:**
   - Waits until at least one message is available in the queue before sending a response.
   - Reduces the number of empty responses, minimizing costs.
   - The maximum long polling wait time is 20 seconds.
2. **Short Polling:**

- Sends a response immediately, even if no messages are available, which can increase costs due to empty receives.

Incorrect Options

1. **Use SQS short polling to retrieve messages from your Amazon SQS queues**
   - **Explanation:** Short polling sends a response immediately, even if no messages are available. This can increase costs due to a higher number of empty receives.
2. **Use SQS visibility timeout to retrieve messages from your Amazon SQS queues**
   - **Explanation:** Visibility timeout prevents other consumers from receiving and processing a given message for a specified period. It does not help in retrieving messages and is not related to minimizing costs.
3. **Use SQS message timer to retrieve messages from your Amazon SQS queues**
   - **Explanation:** Message timers set an initial invisibility period for a message added to a queue. This feature is used to delay message visibility, not for retrieving messages and minimizing costs.

Additional Details:

- **Visibility Timeout:** Default is 30 seconds, with a maximum of 12 hours.
- **Message Timer:** Allows delaying message visibility for up to 15 minutes.

Conclusion / Points to Memorize

- **SQS Long Polling:** Reduces the number of empty receives, lowering costs. Delays response until a message is available or timeout is reached.
- **SQS Short Polling:** Sends immediate responses, which can lead to higher costs due to empty receives.
- **Visibility Timeout:** Prevents other consumers from processing a message for a specified period, not related to retrieval or cost reduction.
- **Message Timer:** Delays visibility of a message, not related to retrieval or cost reduction.

Question 17 - Incorrect

A healthcare company has deployed its web application on Amazon Elastic Container Service (Amazon ECS) container instances running behind an Application Load Balancer. The website slows down when the traffic spikes and the website availability is also reduced. The development team has configured Amazon CloudWatch alarms to receive notifications whenever there is an availability constraint so the team can scale out resources. The company wants an automated solution to respond to such events.

Which of the following addresses the given use case?

Correct Option

Configure AWS Auto Scaling to scale out the Amazon ECS cluster when the ECS service's CPU utilization rises above a threshold

Explanation

- **Amazon ECS Auto Scaling:** Automatically adjusts the desired count of your service's tasks in response to changes in demand.
- **ECS Service Metric:** The appropriate metric to track for scaling an ECS service is its CPU utilization.
- **Scaling Policy:** Use a target tracking scaling policy to scale your service automatically based on the service's CPU utilization.

How It Works:

1. **Configure ECS Service Metric:**
   - **ECSServiceAverageCPUUtilization:** Tracks the average CPU utilization of the service.
2. **Target Value:** Set the target CPU utilization percentage (e.g., 75%).
3. **Scale-Out Cooldown Period:** Define the cooldown period after a scale-out activity.
4. **Scale-In Cooldown Period:** Define the cooldown period after a scale-in activity.

Incorrect Options

1. **Configure AWS Auto Scaling to scale out the Amazon ECS cluster when the Application Load Balancer's CPU utilization rises above a threshold**
   - **Explanation:** The metric to track for scaling ECS services should be the ECS service's CPU utilization, not the Application Load Balancer's CPU utilization.

2. **Configure AWS Auto Scaling to scale out the Amazon ECS cluster when the Application Load Balancer's target group's CPU utilization rises above a threshold**
    - **Explanation:** Similar to the first option, this does not track the ECS service's CPU utilization, which is the correct metric.
3. **Configure AWS Auto Scaling to scale out the Amazon ECS cluster when the CloudWatch alarm's CPU utilization rises above a threshold**
    - **Explanation:** CloudWatch alarms notify based on thresholds but do not directly manage scaling policies. The ECS service's CPU utilization should be tracked for scaling.

Additional Details:

- **Target Tracking Scaling Policy:** Automatically adjusts the number of tasks based on CPU utilization.
- **Cooldown Periods:** Prevent excessive scaling activities by defining time intervals.

Conclusion / Points to Memorize

- **ECS Service Auto Scaling:**
    - Track **ECSServiceAverageCPUUtilization** for scaling.
    - Set target values for CPU utilization.
    - Configure scale-out and scale-in cooldown periods.
- **Incorrect Metrics:**
    - Application Load Balancer's CPU utilization is not relevant for ECS scaling.
- CloudWatch alarms notify but do not manage scaling directly.

Question 18 - Incorrect

An IT company is looking to move its on-premises infrastructure to AWS Cloud. The company has a portfolio of applications with a few of them using server-bound licenses that are valid for the next year. To utilize the licenses, the CTO wants to use dedicated hosts for a one-year term and then migrate the given instances to default tenancy thereafter.

As a solutions architect, which of the following options would you identify as CORRECT for changing the tenancy of an instance after you have launched it? (Select two)

Correct Options

1. **You can change the tenancy of an instance from dedicated to host.**
2. **You can change the tenancy of an instance from host to dedicated.**

Explanation

- **Tenancy Attribute:** Each Amazon EC2 instance launched into a VPC has a tenancy attribute which can be set to different values (default, dedicated, or host).
- **Dedicated Instances:** Run in a virtual private cloud (VPC) on hardware dedicated to a single customer. Can share hardware with other instances from the same AWS account that are not dedicated instances.
- **Dedicated Host:** A physical server dedicated to your use, providing visibility and control over how instances are placed on the server.

How It Works:

1. **Changing Tenancy:**
    - **From Dedicated to Host:** You can change the tenancy of an instance from dedicated to host after launch.
- **From Host to Dedicated:** You can change the tenancy of an instance from host to dedicated after launch.

Incorrect Options

1. **You can change the tenancy of an instance from default to dedicated**
    - **Explanation:** You cannot change the tenancy of an instance from default to dedicated after launch.
2. **You can change the tenancy of an instance from dedicated to default**
    - **Explanation:** You cannot change the tenancy of an instance from dedicated to default after launch.
3. **You can change the tenancy of an instance from default to host**
    - **Explanation:** You cannot change the tenancy of an instance from default to host after launch.

Additional Details:

- **Default Tenancy:** Instances run on shared hardware by default.
- **Tenancy Changes:** Only changes between dedicated and host are allowed after instance launch.

Conclusion / Points to Memorize

- **Instance Tenancy:**
    - Default: Shared hardware.

    - Dedicated: Hardware dedicated to a single customer.
    - Host: Physical server dedicated to your use.
- **Allowed Changes Post-Launch:**
    - From **dedicated to host**.
    - From **host to dedicated**.
- **Not Allowed Post-Launch:**
    - From **default to dedicated**.
    - From **dedicated to default**.
- From **default to host**.

Question 19 - Incorrect

A company has set up AWS Organizations to manage several departments running their own AWS accounts. The departments operate from different countries and are spread across various AWS Regions. The company wants to set up a consistent resource provisioning process across departments so that each resource follows pre-defined configurations such as using a specific type of Amazon EC2 instances, specific IAM roles for AWS Lambda functions, etc.

As a solutions architect, which of the following options would you recommend for this use-case?

Correct Option

Use AWS CloudFormation StackSets to deploy the same template across AWS accounts and regions

Explanation

- **AWS CloudFormation StackSets:** Extend the functionality of stacks by enabling you to create, update, or delete stacks across multiple accounts and regions with a single operation. A StackSet allows you to create stacks in AWS accounts across regions by using a single AWS CloudFormation template.

How It Works:

1. **StackSets:**
    - Define and manage an AWS CloudFormation template.
    - Use the template to provision stacks into selected target accounts across specified regions.
- Utilize an administrator account within an AWS Organization for managing the StackSets.

Incorrect Options

1. **Use AWS CloudFormation stacks to deploy the same template across AWS accounts and regions**
    - **Explanation:** AWS CloudFormation stacks are sets of AWS resources managed as a single unit when AWS CloudFormation instantiates a template. Stacks cannot be used to deploy the same template across multiple accounts and regions.
2. **Use AWS CloudFormation templates to deploy the same template across AWS accounts and regions**
    - **Explanation:** AWS CloudFormation templates are JSON or YAML-format files that describe all the AWS resources needed to run an application. Templates act as blueprints for stacks but cannot deploy the same template across multiple accounts and regions directly.
3. **Use AWS Resource Access Manager (AWS RAM) to deploy the same template across AWS accounts and regions**
    - **Explanation:** AWS Resource Access Manager (AWS RAM) is used to share AWS resources securely with any AWS account or within an AWS Organization. AWS RAM does not facilitate deploying the same template across multiple accounts and regions.

Additional Details:

- **StackSets:** Enable centralized management of infrastructure and consistent resource provisioning across multiple AWS accounts and regions.
- **CloudFormation Templates:** Define resources but require StackSets for multi-account and multi-region deployment.
- **AWS RAM:** Used for sharing resources, not for deploying templates.

Conclusion / Points to Memorize

- **AWS CloudFormation StackSets:**
    - Extend CloudFormation stacks functionality for multi-account and multi-region deployments.
    - Managed using an administrator account within an AWS Organization.
    - Ensure consistent resource provisioning and compliance with predefined configurations.
- **AWS CloudFormation Templates:** Serve as blueprints but require StackSets for deployment across multiple accounts and regions.
- **AWS RAM:** Shares resources but does not deploy templates.

Question 20 - Correct

The database backend for a retail company's website is hosted on Amazon RDS for MySQL having a primary instance and three read replicas to support read scalability. The company has mandated that the read replicas should lag no more than 1 second behind the primary instance to provide the best possible

user experience. The read replicas are falling further behind during periods of peak traffic spikes, resulting in a bad user experience as the searches produce inconsistent results.

You have been hired as an AWS Certified Solutions Architect - Associate to reduce the replication lag as much as possible with minimal changes to the application code or the effort required to manage the underlying resources

Which of the following will you recommend?

Correct Option

Set up database migration from Amazon RDS MySQL to Amazon Aurora MySQL. Swap out the MySQL read replicas with Aurora Replicas. Configure Aurora Auto Scaling

Explanation

- **Amazon Aurora MySQL:** Offers a distributed, fault-tolerant, and self-healing storage system that auto-scales up to 128 TiB per database instance.
- **Replication Lag:** Aurora Replicas share the same data volume as the primary instance in the same AWS Region, resulting in virtually no replication lag. The replica lag times are in the 10s of milliseconds, compared to the seconds of lag in MySQL read replicas.
- **Aurora Auto Scaling:** Automatically adjusts the number of Aurora Replicas based on traffic, ensuring optimal performance.

How It Works:

1. **Migration to Aurora:**
   - **Aurora MySQL:** Migrate the database from RDS MySQL to Amazon Aurora MySQL.
   - **Aurora Replicas:** Use Aurora Replicas instead of MySQL read replicas.
2. **Configure Aurora Auto Scaling:**

- Automatically manage the number of read replicas based on the load.

Incorrect Options

1. **Host the MySQL primary database on a memory-optimized Amazon EC2 instance. Spin up additional compute-optimized Amazon EC2 instances to host the read replicas**
   - **Explanation:** Managing MySQL on EC2 instances results in significant overhead for managing the infrastructure, such as OS patching and database maintenance.
2. **Set up an Amazon ElastiCache for Redis cluster in front of the MySQL database. Update the website to check the cache before querying the read replicas**
   - **Explanation:** Introducing a caching layer would require significant changes to the application code to check the cache before querying the database.
3. **Set up database migration from Amazon RDS MySQL to Amazon DynamoDB. Provision a large number of read capacity units (RCUs) to support the required throughput and enable Auto-Scaling**
   - **Explanation:** Migrating to a NoSQL database like DynamoDB would require extensive changes to the application code to adapt to the new database queries and schema.

Additional Details:

- **Amazon Aurora:**
  - Supports up to 15 replicas with asynchronous replication in milliseconds.
  - Low performance impact on the primary instance.
  - Automated failover and high availability.
- **MySQL Replicas:**
  - Supports up to 5 replicas with asynchronous replication in seconds.
  - Higher performance impact on the primary instance.

Conclusion / Points to Memorize

- **Amazon Aurora MySQL:**
  - Virtually no replication lag with asynchronous replication in milliseconds.
  - Automated scaling and management of read replicas.
  - High availability and fault tolerance.
- **Incorrect Alternatives:**
  - Managing MySQL on EC2 instances increases overhead.
  - Caching requires significant application code changes.
- Migrating to DynamoDB involves extensive application modifications.

Question 21 - Correct

A developer has configured inbound traffic for the relevant ports in both the Security Group of the Amazon EC2 instance as well as the Network Access Control List (Network ACL) of the subnet for the Amazon EC2 instance. The developer is, however, unable to connect to the service running on the Amazon EC2 instance.

As a solutions architect, how will you fix this issue?

Correct Option

Security Groups are stateful, so allowing inbound traffic to the necessary ports enables the connection. Network ACLs are stateless, so you must allow both inbound and outbound traffic.

Explanation

- **Security Groups:**
  - Stateful, meaning that if you allow an incoming request to a port, the response is automatically allowed back out.
  - Ensuring inbound rules are set up correctly will permit the connection.
- **Network ACLs:**
  - Stateless, meaning that both inbound and outbound rules must be explicitly allowed.
  - You must allow outbound traffic from ephemeral ports (1024-65535) to enable return traffic from the service.
  - Ensure that both inbound and outbound traffic is allowed in the Network ACL for the necessary ports.

How It Works:

1. **Security Groups:** Allow inbound traffic to the necessary ports (stateful, automatic outbound response).
2. **Network ACLs:** Allow both inbound and outbound traffic for the necessary ports (stateless, requires explicit rules).

Incorrect Options

1. **IAM Role defined in the Security Group is different from the IAM Role that is given access in the Network ACLs**
   - **Explanation:** IAM roles are not relevant to configuring Security Groups or Network ACLs, making this a distractor.
2. **Rules associated with Network ACLs should never be modified from command line. An attempt to modify rules from command line blocks the rule and results in an erratic behavior**
   - **Explanation:** This option is incorrect and misleading. AWS does support modifying rules of Network ACLs from the command line tool.
3. **Network ACLs are stateful, so allowing inbound traffic to the necessary ports enables the connection. Security Groups are stateless, so you must allow both inbound and outbound traffic**
   - **Explanation:** This is incorrect as Security Groups are stateful and Network ACLs are stateless, contradicting the correct explanation provided.

Additional Details:

- **Stateful Security Groups:** Automatically allow return traffic for inbound requests.
- **Stateless Network ACLs:** Require explicit rules for both inbound and outbound traffic.

Conclusion / Points to Memorize

- **Security Groups:**
  - Stateful, requiring only inbound rules to be set for allowing connections.
- **Network ACLs:**
  - Stateless, requiring both inbound and outbound rules to be set for allowing connections.
- **Common Pitfalls:**
- Ensure both security group and network ACL rules are properly configured to avoid connection issues.

Question 22 - Correct

The application maintenance team at a company has noticed that the production application is very slow when the business reports are run on the Amazon RDS database. These reports fetch a large amount of data and have complex queries with multiple joins, spanning across multiple business-critical core tables. CPU, memory, and storage metrics are around 50% of the total capacity.

Can you recommend an improved and cost-effective way of generating the business reports while keeping the production application unaffected?

Correct Option

Create a read replica and connect the report generation tool/application to it.

Explanation

Amazon RDS Read Replicas provide enhanced performance and durability for Amazon RDS database (DB) instances. They make it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. You can create one or more replicas of a given source DB instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances.

Common Reasons for Deploying a Read Replica:

1. **Scaling beyond compute or I/O capacity:** Excess read traffic can be directed to one or more read replicas.
2. **Serving read traffic during source DB unavailability:** You can direct read traffic to your read replica(s) if the source DB instance is unavailable.
3. **Business reporting or data warehousing scenarios:** Running business reporting queries against a read replica rather than your primary production DB instance.
4. **Disaster recovery:** A read replica can be used for disaster recovery of the source DB instance, either in the same AWS Region or in another Region.

Comparison: Read Replicas with Multi-AZ and Multi-Region Amazon RDS Deployments

- **Multi-AZ deployments:** Provide enhanced availability and durability but do not allow reading from the standby database.
- **Multi-Region deployments:** Useful for disaster recovery and local performance but also do not allow reading from the standby database.
- **Read replicas:** Ideal for read scalability and can be used within an Availability Zone, Cross-AZ, or Cross-Region.

Incorrect Options

1. **Increase the size of Amazon RDS instance:**
   - **Explanation:** This will not help as CPU, memory, and storage are already running at only 50% of the total capacity.
2. **Migrate from General Purpose SSD to magnetic storage to enhance IOPS:**
   - **Explanation:** Amazon RDS supports magnetic storage for backward compatibility only. AWS recommends General Purpose SSD or Provisioned IOPS for any storage needs.
3. **Configure the Amazon RDS instance to be Multi-AZ DB instance, and connect the report generation tool to the DB instance in a different AZ:**
   - **Explanation:** Amazon RDS Multi-AZ deployments provide enhanced availability and durability for RDS database (DB) instances. However, you cannot read from the standby database, making this option incorrect for the given scenario.

Key Takeaways:

- **Read Replicas:** Best solution for read-heavy workloads and business reporting scenarios.
- **Multi-AZ Deployments:** Enhance availability but do not support reading from standby instances.
- **Storage Choices:** Prefer General Purpose SSD or Provisioned IOPS over magnetic storage for better performance.

Question 23 - Incorrect

An e-commerce company has deployed its application on several Amazon EC2 instances that are configured in a private subnet using IPv4. These Amazon EC2 instances read and write a huge volume of data to and from Amazon S3 in the same AWS region. The company has set up subnet routing to direct all the internet-bound traffic through a Network Address Translation gateway (NAT gateway). The company wants to build the most cost-optimal solution without impacting the application's ability to communicate with Amazon S3 or the internet.

As an AWS Certified Solutions Architect Associate, which of the following would you recommend?

Correct Option

Set up a VPC gateway endpoint for Amazon S3. Attach an endpoint policy to the endpoint. Update the route table to direct the S3-bound traffic to the VPC endpoint.

Explanation

Gateway endpoints provide reliable connectivity to Amazon S3 without requiring an internet gateway or a NAT device for your VPC. After you create the gateway endpoint, you can add it as a target in your route table for traffic destined from your VPC to Amazon S3. There is no additional charge for using gateway endpoints.

The VPC endpoint policy for the gateway endpoint controls access to Amazon S3 from the VPC through the endpoint. The default policy allows full access.

How to Configure a Gateway Endpoint

1. **Create a Gateway Endpoint:**
   - When you create a gateway endpoint, you select the VPC route tables for the subnets that you enable.
- The following route is automatically added to each route table that you select:

  Destination: prefix_list_id

  Target: gateway_endpoint_id

2. **Update Route Tables:**
   - Ensure that each subnet route table has a route that sends traffic destined for the service to the gateway endpoint using the prefix list for the service.

Benefits of Using Gateway Endpoints

- **Cost-effective:** No data transfer costs for ingress or egress traffic within the same AWS region.
- **Enhanced Security:** The data transfer remains within the AWS network and does not traverse the public internet.

Key Points to Memorize

- **Gateway Endpoints:** Used for services like Amazon S3 and DynamoDB.
- **Statefulness:**
  - **Security Groups:** Stateful; allow both inbound and outbound traffic.
  - **Network ACLs:** Stateless; need explicit rules for both inbound and outbound traffic.
- **Private Subnets:** Must use NAT gateways or gateway endpoints for internet-bound traffic.

Incorrect Options and Explanations

1. **Set up a Gateway Load Balancer (GWLB) endpoint for Amazon S3:**
   - Gateway Load Balancers are used for private connectivity between VPCs and are not designed for accessing Amazon S3.
2. **Provision an internet gateway and update the route table:**
   - Adding a route to the internet gateway in the route table associated with the private subnet would make the subnet public, which is not desired.
3. **Set up an egress-only internet gateway:**
   - Egress-only internet gateways are designed for IPv6 traffic. The given scenario involves IPv4 traffic.

Conclusion

Using a VPC gateway endpoint for Amazon S3 is the most cost-effective and efficient solution for enabling Amazon EC2 instances in a private subnet to communicate with Amazon S3 without using the public internet. This approach ensures secure and reliable connectivity while minimizing costs.

Question 24 - Correct

A media company has its corporate headquarters in Los Angeles with an on-premises data center using an AWS Direct Connect connection to the AWS VPC. The branch offices in San Francisco and Miami use AWS Site-to-Site VPN connections to connect to the AWS VPC. The company is looking for a solution to have the branch offices send and receive data with each other as well as with their corporate headquarters.

As a solutions architect, which of the following AWS services would you recommend addressing this use-case?

Correct Option

AWS VPN CloudHub

Explanation

Use AWS Site-to-Site VPN CloudHub for Secure Communication:

1. **Enable Secure Communication:**
   - AWS VPN CloudHub allows multiple remote sites to securely communicate with each other, not just with the VPC.
2. **Hub-and-Spoke Model:**
   - Operates on a hub-and-spoke model for primary or backup connectivity between remote offices.
   - Suitable for multiple branch offices with existing internet connections.
3. **Direct Connect Integration:**
   - Corporate headquarters can use AWS Direct Connect for VPC connection.
   - Branch offices use Site-to-Site VPN connections to the VPC.
   - Enables secure data exchange between branch offices and headquarters.
4. **Cost-Effective:**
   - Potentially low-cost solution for primary or backup connectivity.

How to Configure AWS VPN CloudHub

1. **Create Virtual Private Gateway:** Attach it to your VPC.
2. **Set Up Site-to-Site VPN Connections:** For each branch office.
3. **Configure Route Tables:** To direct traffic from the branch offices to the virtual private gateway.
4. **Enable VPN CloudHub:** Configure the customer gateway to enable communication between the branch offices.

Benefits of Using AWS VPN CloudHub

- **Scalable:** Easily add new branch offices to the hub.
- **Cost-effective:** Uses existing internet connections.
- **Simple Configuration:** Works with existing VPN connections.

Key Points to Memorize

- **VPN CloudHub:** Ideal for connecting multiple branch offices in a hub-and-spoke model.
- **Compatibility:** Works with both AWS Direct Connect and Site-to-Site VPN.
- **Statefulness:**

- **Security Groups:** Stateful; allow both inbound and outbound traffic.
- **Network ACLs:** Stateless; need explicit rules for both inbound and outbound traffic.

Incorrect Options and Explanations

1. **VPC Endpoint:**
   - A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. This option cannot be used to send and receive data between the remote branch offices of the company.
2. **VPC Peering connection:**
   - A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. VPC peering facilitates a connection between two VPCs within the AWS network, but it cannot be used to send and receive data between the remote branch offices of the company.
3. **Software VPN:**
   - Amazon VPC offers the flexibility to fully manage both sides of your Amazon VPC connectivity by creating a VPN connection between your remote network and a software VPN appliance running in your Amazon VPC network. Since Software VPN just handles connectivity between the remote network and Amazon VPC, it cannot be used to send and receive data between the remote branch offices of the company.

Conclusion

Using AWS VPN CloudHub is the optimal solution for enabling secure communication between multiple branch offices and the corporate headquarters using existing Site-to-Site VPN and AWS Direct Connect connections. This approach ensures a cost-effective and scalable hub-and-spoke model for inter-office communication.

Question 25

An e-commerce company is using Elastic Load Balancing (ELB) for its fleet of Amazon EC2 instances spread across two Availability Zones (AZs), with one instance as a target in Availability Zone A and four instances as targets in Availability Zone B. The company is doing benchmarking for server performance when cross-zone load balancing is enabled compared to the case when cross-zone load balancing is disabled.

As a solutions architect, which of the following traffic distribution outcomes would you identify as correct?

- **Correct Option:**

With cross-zone load balancing enabled, one instance in Availability Zone A receives 20% traffic and four instances in Availability Zone B receive 20% traffic each. With cross-zone load balancing disabled, one instance in Availability Zone A receives 50% traffic and four instances in Availability Zone B receive 12.5% traffic each.

- **Explanation behind Correct Option:**
  1. **Cross-Zone Load Balancing Enabled:**
     - Each load balancer node distributes traffic evenly across all registered targets in all enabled Availability Zones.
     - Traffic distribution is equal across all instances regardless of the AZ they are in.
     - Therefore, if there are 5 instances (1 in AZ A and 4 in AZ B), each instance receives 20% of the traffic.
  2. **Cross-Zone Load Balancing Disabled:**
     - Each load balancer node distributes traffic only to targets in its respective Availability Zone.
     - Traffic is distributed proportionally to the number of instances in each AZ.
     - Therefore, if there are 5 instances (1 in AZ A and 4 in AZ B), the single instance in AZ A receives 50% of the traffic, and each of the 4 instances in AZ B receives 12.5% of the traffic.
- **Incorrect Options and Explanations:**
  1. **Option:** With cross-zone load balancing enabled, one instance in Availability Zone A receives 50% traffic and four instances in Availability Zone B receive 12.5% traffic each. With cross-zone load balancing disabled, one instance in Availability Zone A receives 20% traffic and four instances in Availability Zone B receive 20% traffic each.
     - **Explanation:** This contradicts the even distribution nature of cross-zone load balancing, which distributes traffic equally across all instances.
  2. **Option:** With cross-zone load balancing enabled, one instance in Availability Zone A receives no traffic and four instances in Availability Zone B receive 25% traffic each. With cross-zone load balancing disabled, one instance in Availability Zone A receives 50% traffic and four instances in Availability Zone B receive 12.5% traffic each.
     - **Explanation:** This is incorrect because cross-zone load balancing ensures that traffic is evenly distributed, not skipping any instances.

3. **Option:** With cross-zone load balancing enabled, one instance in Availability Zone A receives 20% traffic and four instances in Availability Zone B receive 20% traffic each. With cross-zone load balancing disabled, one instance in Availability Zone A receives no traffic and four instances in Availability Zone B receive 25% traffic each.
    - **Explanation:** This is incorrect because with cross-zone load balancing disabled, each instance in AZ A would still receive a proportional amount of traffic, not zero traffic.

- **Conclusion / Points to Memorize:**
    1. **Cross-Zone Load Balancing Enabled:**
        - Traffic is evenly distributed across all instances in all AZs.
    2. **Cross-Zone Load Balancing Disabled:**
        - Traffic is distributed proportionally based on the number of instances in each AZ.
        - Instances in an AZ with fewer instances receive more traffic per instance compared to those in an AZ with more instances.
    3. **Traffic Distribution:**
- Understand that cross-zone load balancing aims to balance the load evenly, while without it, traffic is divided within the same AZ only.

Question 26

An IT company is using Amazon Simple Queue Service (Amazon SQS) queues for decoupling the various components of application architecture. As the consuming components need additional time to process Amazon Simple Queue Service (Amazon SQS) messages, the company wants to postpone the delivery of new messages to the queue for a few seconds.

As a solutions architect, which of the following solutions would you suggest to the company?

- **Correct Option:**

Use delay queues to postpone the delivery of new messages to the queue for a few seconds.

- **Explanation behind Correct Option:**
    1. **Amazon SQS**:
        - Fully managed message queuing service to decouple and scale microservices, distributed systems, and serverless applications.
    2. **Delay Queues**:
        - Let you postpone the delivery of new messages to a queue for several seconds.
        - Useful when consumer applications need additional time to process messages.
        - Messages remain invisible to consumers for the duration of the delay period.
        - The delay period can range from 0 seconds to 15 minutes.
    3. **Implementation**:
        - Configure delay seconds on the queue to set the postponement period.
- **Incorrect Options and Explanations:**
    1. **Use Amazon SQS FIFO queues to postpone the delivery of new messages to the queue for a few seconds**:
        - **Explanation**: FIFO queues guarantee that messages are processed exactly once, in the exact order that they are sent. They do not inherently delay message delivery.
    2. **Use dead-letter queues to postpone the delivery of new messages to the queue for a few seconds**:
        - **Explanation**: Dead-letter queues are used for capturing messages that can't be processed successfully by the consumer. They are not intended for postponing message delivery.
    3. **Use visibility timeout to postpone the delivery of new messages to the queue for a few seconds**:
        - **Explanation**: Visibility timeout is a period during which Amazon SQS prevents other consumers from receiving and processing a given message that is already being processed. It does not delay the delivery of new messages to the queue.
- **Conclusion / Points to Memorize:**
    1. **Delay Queues**:
        - Use for postponing the delivery of new messages for a specified period.
        - Configurable from 0 seconds to 15 minutes.
    2. **FIFO Queues**:
        - Ensure messages are processed in the order they are sent, not for delaying messages.
    3. **Dead-Letter Queues**:
        - Capture unprocessable messages for debugging, not for delaying messages.
    4. **Visibility Timeout**:

- Prevents reprocessing of a message while it is being handled, does not delay new message delivery.

Question 27

A financial services company has recently migrated from on-premises infrastructure to AWS Cloud. The DevOps team wants to implement a solution that allows all resource configurations to be reviewed and make sure that they meet compliance guidelines. Also, the solution should be able to offer the capability to look into the resource configuration history across the application stack.

As a solutions architect, which of the following solutions would you recommend to the team?

- **Correct Option:**

Use AWS Config to review resource configurations to meet compliance guidelines and maintain a history of resource configuration changes.

- **Explanation behind Correct Option:**
    1. **AWS Config**:
        - Enables assessment, auditing, and evaluation of AWS resource configurations.
        - Allows review of changes in configurations and relationships between AWS resources.
        - Provides detailed resource configuration histories.
        - Helps determine overall compliance against specified internal guidelines.
        - Example Question: "What did my AWS resource look like at a specific point in time?"
    2. **Compliance**:
        - Helps ensure that resource configurations meet compliance guidelines.
    3. **Configuration History**:
        - Maintains a comprehensive history of resource configuration changes.
- **Incorrect Options and Explanations:**
    1. **Use Amazon CloudWatch to review resource configurations to meet compliance guidelines and maintain a history of resource configuration changes**:
        - **Explanation**: Amazon CloudWatch is designed for monitoring applications, responding to system-wide performance changes, optimizing resource utilization, and getting a unified view of operational health. It does not maintain a history of resource configuration changes.
    2. **Use AWS CloudTrail to review resource configurations to meet compliance guidelines and maintain a history of resource configuration changes**:
        - **Explanation**: AWS CloudTrail logs account activity related to actions across AWS infrastructure, providing an event history of AWS account activity. It focuses on tracking API calls and does not maintain a detailed history of resource configuration changes.
    3. **Use AWS Systems Manager to review resource configurations to meet compliance guidelines and maintain a history of resource configuration changes**:
        - **Explanation**: AWS Systems Manager groups resources for monitoring and troubleshooting and allows actions on groups of resources. It does not provide a history of resource configuration changes.
- **Conclusion / Points to Memorize:**
    1. **AWS Config**:
        - Use for auditing, assessing, and evaluating resource configurations.
        - Provides detailed histories of resource configurations.
        - Ensures compliance with internal guidelines.
    2. **Amazon CloudWatch**:
        - Monitors resource performance, events, and alerts.
    3. **AWS CloudTrail**:
        - Logs account-specific activity and provides an event history.
    4. **AWS Systems Manager**:
- Manages and groups resources for operational tasks.

Question 28

A health care application processes the real-time health data of the patients into an analytics workflow. With a sharp increase in the number of users, the system has become slow and sometimes even unresponsive as it does not have a retry mechanism. The startup is looking at a scalable solution that has minimal implementation overhead.

Which of the following would you recommend as a scalable alternative to the current solution?

- **Correct Option:**

Use Amazon Kinesis Data Streams to ingest the data, process it using AWS Lambda or run analytics using Amazon Kinesis Data Analytics.

- **Explanation behind Correct Option:**
  1. **Amazon Kinesis Data Streams (KDS)**:
     - Massively scalable and durable real-time data streaming service.
     - Supports retry mechanisms for data processing.
     - Can capture gigabytes of data per second from various sources (e.g., website clickstreams, database event streams, IT logs).
     - Data is available in milliseconds for real-time analytics (e.g., dashboards, anomaly detection, dynamic pricing).
     - Scales from megabytes to terabytes per hour and from thousands to millions of PUT records per second.
     - Dynamically adjusts throughput based on input data volume.
  2. **Processing and Analytics**:
     - Data can be processed using AWS Lambda.
     - Run analytics using Amazon Kinesis Data Analytics.
- **Incorrect Options and Explanations:**
  1. **Use Amazon Simple Notification Service (Amazon SNS) for data ingestion and configure AWS Lambda to trigger logic for downstream processing**:
     - **Explanation**: Amazon SNS is a fully managed messaging service suitable for A2A and A2P communication. It is a push mechanism and does not support robust retry mechanisms required for real-time data streaming.
  2. **Use Amazon Simple Queue Service (Amazon SQS) for data ingestion and configure AWS Lambda to trigger logic for downstream processing**:
     - **Explanation**: Amazon SQS is a messaging service that helps in decoupling systems and reducing architectural complexity. However, it is not specifically designed for streaming real-time data, making it less suitable than Kinesis Data Streams for this use case.
  3. **Use Amazon API Gateway with the existing REST-based interface to create a high-performing architecture**:
     - **Explanation**: Amazon API Gateway is designed for creating and maintaining APIs. It is not suitable for handling real-time streaming data.
- **Conclusion / Points to Memorize:**
  1. **Amazon Kinesis Data Streams**:
     - Ideal for real-time data ingestion and processing.
     - Scalable and supports retry mechanisms.
     - Suitable for real-time analytics and dynamic data processing.
  2. **Amazon SNS**:
     - Used for push-based messaging (A2A and A2P communication).
     - Not suitable for real-time data streaming.
  3. **Amazon SQS**:
     - Suitable for decoupling systems and managing message queues.
     - Not specifically designed for real-time data streaming.
  4. **Amazon API Gateway**:
     - Used for creating and managing APIs.
- Not suitable for handling real-time streaming data.

Question 29

The engineering team at an e-commerce company wants to migrate from Amazon Simple Queue Service (Amazon SQS) Standard queues to FIFO (First-In-First-Out) queues with batching.

As a solutions architect, which of the following steps would you have in the migration checklist? (Select three)

Correct Options:

1. **Delete the existing standard queue and recreate it as a FIFO (First-In-First-Out) queue**
2. **Make sure that the name of the FIFO (First-In-First-Out) queue ends with the .fifo suffix**
3. **Make sure that the throughput for the target FIFO (First-In-First-Out) queue does not exceed 3,000 messages per second**

Explanation behind Correct Options:

1. **Delete the existing standard queue and recreate it as a FIFO (First-In-First-Out) queue:**
   - You cannot convert an existing standard queue into a FIFO queue.
   - To migrate, you need to delete the standard queue and create a new FIFO queue.
2. **Make sure that the name of the FIFO (First-In-First-Out) queue ends with the .fifo suffix:**

- FIFO queue names must end with the .fifo suffix.
- This suffix counts towards the 80-character queue name limit.

3. **Make sure that the throughput for the target FIFO (First-In-First-Out) queue does not exceed 3,000 messages per second:**
   - By default, FIFO queues support up to 3,000 messages per second with batching.
   - Without batching, the limit is 300 messages per second.

Incorrect Options and Explanations:

1. **Make sure that the name of the FIFO (First-In-First-Out) queue is the same as the standard queue:**
   - Incorrect because the name of a FIFO queue must end with the .fifo suffix, which would make it different from the standard queue name.
2. **Convert the existing standard queue into a FIFO (First-In-First-Out) queue:**
   - Incorrect because you cannot directly convert a standard queue into a FIFO queue. You must delete the standard queue and create a new FIFO queue.
3. **Make sure that the throughput for the target FIFO (First-In-First-Out) queue does not exceed 300 messages per second:**
   - Incorrect because, with batching, the FIFO queue can support up to 3,000 messages per second.

Conclusion / Points to Memorize:

1. **FIFO Queue Naming:**
   - The name of a FIFO queue must end with the .fifo suffix.
   - This suffix counts towards the 80-character limit.
2. **Migration Steps:**
   - You cannot convert a standard queue to a FIFO queue directly.
   - Delete the standard queue and create a new FIFO queue.
3. **Throughput Limits:**
   - FIFO queues support up to 3,000 messages per second with batching.
   - Without batching, the limit is 300 messages per second.
4. **Understand Amazon SQS Types:**
   - Standard queues offer maximum throughput, best-effort ordering, and at-least-once delivery.

- FIFO queues ensure messages are processed exactly once, in the exact order they are sent.

Question 30

A startup has created a new web application for users to complete a risk assessment survey for COVID-19 symptoms via a self-administered questionnaire. The startup has purchased the domain covid19survey.com using Amazon Route 53. The web development team would like to create Amazon Route 53 record so that all traffic for covid19survey.com is routed to www.covid19survey.com.

As a solutions architect, which of the following is the MOST cost-effective solution that you would recommend to the web development team?

Correct Option:

- **Create an alias record for covid19survey.com that routes traffic to www.covid19survey.com**

Explanation behind Correct Option:

1. **Alias Records:**
   - Alias records are Amazon Route 53–specific extensions to DNS functionality.
   - They allow routing traffic to selected AWS resources, such as Amazon CloudFront distributions and Amazon S3 buckets.
   - You can create an alias record at the top node of a DNS namespace (zone apex), which is not possible with CNAME records.
   - Alias records are cost-effective as Route 53 does not charge for alias queries to AWS resources.
2. **Zone Apex:**
   - For the domain covid19survey.com, the zone apex is covid19survey.com.
   - A CNAME record cannot be created for the zone apex, but an alias record can be created to route traffic to www.covid19survey.com.

Incorrect Options and Explanations:

1. **Create a CNAME record for covid19survey.com that routes traffic to www.covid19survey.com:**
   - You cannot create a CNAME record for the top node of the DNS namespace (zone apex), making this option incorrect.
2. **Create an MX record for covid19survey.com that routes traffic to www.covid19survey.com:**
   - An MX record specifies the names of mail servers and their priority order.
   - It is used for mail delivery, not for routing web traffic, making this option incorrect.
3. **Create an NS record for covid19survey.com that routes traffic to www.covid19survey.com:**

- An NS record identifies the name servers for the hosted zone.
- It is used for delegating a DNS zone to use the given authoritative name servers, not for routing traffic, making this option incorrect.

Conclusion / Points to Memorize:

1. **Use Alias Records for Zone Apex:**
   - Alias records can be created at the top node of a DNS namespace (zone apex) and are ideal for routing traffic to AWS resources.
   - They are cost-effective as Route 53 does not charge for alias queries to AWS resources.
2. **Limitations of CNAME Records:**
   - CNAME records cannot be created for the zone apex. They can only be used for subdomains.
   - Example: You cannot use a CNAME record for covid19survey.com, but you can use it for www.covid19survey.com.
3. **Purpose of MX and NS Records:**
   - MX records are used for specifying mail servers.
   - NS records are used for delegating a DNS zone to authoritative name servers.
4. **Routing Traffic with Alias Records:**

- Use alias records to route traffic from the main domain (zone apex) to a subdomain or other AWS resources efficiently and cost-effectively.

Question 31

A financial services company wants to move the Windows file server clusters out of their datacenters. They are looking for cloud file storage offerings that provide full Windows compatibility. Can you identify the AWS storage services that provide highly reliable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol compatible with Windows systems? (Select two)

Correct Options:

- **Amazon FSx for Windows File Server**
- **File Gateway Configuration of AWS Storage Gateway**

Explanation behind Correct Options:

1. **Amazon FSx for Windows File Server:**
   - Fully managed and highly reliable file storage.
   - Accessible over the industry-standard SMB protocol.
   - Built on Windows Server, providing features such as user quotas, end-user file restore, and Microsoft Active Directory (AD) integration.
2. **File Gateway Configuration of AWS Storage Gateway:**
   - File Gateway enables storing and retrieving objects in Amazon S3 using file protocols like NFS and SMB.
   - Provides seamless integration with on-premises applications and AWS storage.

Incorrect Options and Explanations:

1. **Amazon Simple Storage Service (Amazon S3):**
   - S3 is an object storage service with a REST web services interface.
   - It does not support the SMB protocol, making it incompatible with Windows file server requirements.
2. **Amazon Elastic Block Store (Amazon EBS):**
   - EBS is a block-level storage service for use with Amazon EC2.
   - It provides low-latency access to data from a single EC2 instance.
   - EBS does not support the SMB protocol.
3. **Amazon Elastic File System (Amazon EFS):**
   - EFS is a file storage service for use with Amazon EC2.
   - Provides a file system interface and access semantics for multiple EC2 instances.
   - Uses the NFS protocol, not SMB, making it unsuitable for Windows compatibility.

Conclusion / Points to Memorize:

1. **SMB Protocol for Windows Compatibility:**
   - For Windows compatibility and SMB protocol support, consider **Amazon FSx for Windows File Server** and **File Gateway Configuration of AWS Storage Gateway**.
2. **Understanding Service Protocols:**
   - **Amazon FSx for Windows File Server**: Fully managed file storage, SMB protocol, Windows Server features.
   - **File Gateway (AWS Storage Gateway)**: Accesses Amazon S3 using NFS and SMB protocols.
3. **Identify Service Use-Cases:**

    - **Amazon S3**: Object storage with REST interface.
    - **Amazon EBS**: Block storage for EC2, does not support SMB.
- **Amazon EFS**: File storage with NFS protocol, not suitable for SMB requirements.

Question 32

An e-commerce company runs its web application on Amazon EC2 instances in an Auto Scaling group and it's configured to handle consumer orders in an Amazon Simple Queue Service (Amazon SQS) queue for downstream processing. The DevOps team has observed that the performance of the application goes down in case of a sudden spike in orders received.

Correct Option:

- **Use a target tracking scaling policy based on a custom Amazon SQS queue metric**

Explanation behind Correct Option:

1. **Target Tracking Scaling Policy:**
    - **Dynamic Scaling:** Adjusts to the demand curve of the application more effectively.
    - **Custom Metric:** Utilizes a custom Amazon SQS metric, like ApproximateNumberOfMessagesVisible.
    - **Backlog per Instance Metric:** Divides the ApproximateNumberOfMessages queue attribute by the number of instances in the InService state for the Auto Scaling group to set a target value for the acceptable backlog per instance.
    - **Example Calculation:** If ApproximateNumberOfMessages is 1500 and fleet capacity is 10, with an average processing time of 0.1 seconds and longest acceptable latency of 10 seconds, the target backlog per instance is 100. If the current backlog per instance is 150, the fleet scales out by five instances to maintain proportion to the target value.

Incorrect Options and Explanations:

1. **Simple Scaling Policy:**
    - **Cooldown Period:** After a scaling activity starts, it must wait for the activity or health check replacement to complete and cooldown period to expire before responding to additional alarms, which delays response to sudden spikes.
2. **Step Scaling Policy:**
    - **Step Adjustments:** Increases or decreases current capacity based on the size of the alarm breach. This is less efficient compared to target tracking, which calculates the exact number of instances required.
3. **Scheduled Scaling Policy:**
    - **Predictable Traffic Patterns:** Sets scaling actions based on predictable traffic patterns, which cannot address sudden spikes in orders.

Conclusion / Points to Memorize:

1. **Target Tracking Scaling Policy:**
    - **Best for Dynamic Scaling:** Adjusts dynamically to demand curves.
    - **Custom Metrics:** Utilizes custom metrics like ApproximateNumberOfMessagesVisible.
    - **Backlog per Instance:** Calculates backlog per instance for precise scaling.
2. **Other Scaling Policies:**
    - **Simple Scaling:** Limited by cooldown period.
    - **Step Scaling:** Uses step adjustments, less precise than target tracking.
- **Scheduled Scaling:** Best for predictable traffic patterns, not sudden spikes.

Question 33

A retail company has connected its on-premises data center to the AWS Cloud via AWS Direct Connect. The company wants to be able to resolve Domain Name System (DNS) queries for any resources in the on-premises network from the AWS VPC and also resolve any DNS queries for resources in the AWS VPC from the on-premises network. As a solutions architect, which of the following solutions can be combined to address the given use case? (Select two)

Correct Options:

1. Create an inbound endpoint on Amazon Route 53 Resolver and then DNS resolvers on the on-premises network can forward DNS queries to Amazon Route 53 Resolver via this endpoint
2. Create an outbound endpoint on Amazon Route 53 Resolver and then Amazon Route 53 Resolver can conditionally forward queries to resolvers on the on-premises network via this endpoint

Explanation behind correct options:

1. **Create an inbound endpoint on Amazon Route 53 Resolver and then DNS resolvers on the on-premises network can forward DNS queries to Amazon Route 53 Resolver via this endpoint:**

- Inbound endpoints allow DNS queries from on-premises systems to resolve AWS VPC resources.
- This setup enables DNS resolvers on the on-premises network to forward queries to Route 53 Resolver.

2. **Create an outbound endpoint on Amazon Route 53 Resolver and then Amazon Route 53 Resolver can conditionally forward queries to resolvers on the on-premises network via this endpoint:**
   - Outbound endpoints allow Route 53 Resolver to forward DNS queries to on-premises DNS servers.
   - This setup enables DNS queries for on-premises resources to be resolved from AWS VPC.

Incorrect options with brief explanations:

1. **Create a universal endpoint on Amazon Route 53 Resolver and then Amazon Route 53 Resolver can receive and forward queries to resolvers on the on-premises network via this endpoint:**
   - There is no such thing as a universal endpoint in Amazon Route 53 Resolver. This option is a distractor.
2. **Create an outbound endpoint on Amazon Route 53 Resolver and then DNS resolvers on the on-premises network can forward DNS queries to Amazon Route 53 Resolver via this endpoint:**
   - DNS resolvers on the on-premises network should forward DNS queries to Amazon Route 53 Resolver via an inbound endpoint, not an outbound endpoint.
3. **Create an inbound endpoint on Amazon Route 53 Resolver and then Amazon Route 53 Resolver can conditionally forward queries to resolvers on the on-premises network via this endpoint:**
   - Amazon Route 53 Resolver can conditionally forward queries to resolvers on the on-premises network via an outbound endpoint, not an inbound endpoint.

Conclusion / Points to memorize:

1. **Inbound Endpoints:**
   - Use inbound endpoints for DNS queries from on-premises to AWS VPC.
   - They allow DNS resolvers on the on-premises network to forward DNS queries to Route 53 Resolver in AWS.
2. **Outbound Endpoints:**
   - Use outbound endpoints for DNS queries from AWS VPC to on-premises.
   - They enable Route 53 Resolver in AWS to forward DNS queries to on-premises DNS servers.
3. **No Universal Endpoints:**
   - Be aware that there is no concept of a universal endpoint in Amazon Route 53 Resolver.
4. **Conditional Forwarding:**
   - Use Resolver rules to specify domain names for forwarding queries to specific DNS servers.
5. **Remember the directionality:**
   - Inbound endpoints for on-premises to AWS.
- Outbound endpoints for AWS to on-premises.

Question 34

Which of the following AWS services provides a highly available and fault-tolerant solution to capture the clickstream events from the source and then provide a concurrent feed of the data stream to the downstream applications?

Correct Option:

2. Amazon Kinesis Data Streams

Explanation behind correct options:

1. **Amazon Kinesis Data Streams (KDS):**
   - KDS is a massively scalable and durable real-time data streaming service.
   - It can continuously capture gigabytes of data per second from hundreds of thousands of sources such as website clickstreams, database event streams, financial transactions, social media feeds, IT logs, and location-tracking events.
   - The data collected is available in milliseconds, enabling real-time analytics use cases such as real-time dashboards, real-time anomaly detection, dynamic pricing, and more.
   - KDS provides ordering of records and the ability to read and/or replay records in the same order to multiple Amazon Kinesis Applications.
   - The Amazon Kinesis Client Library (KCL) delivers all records for a given partition key to the same record processor, making it easier to build multiple applications reading from the same Amazon Kinesis data stream (e.g., to perform counting, aggregation, and filtering).
   - KDS is recommended when multiple applications need to consume the same stream concurrently, such as one application updating a real-time dashboard and another archiving data to Amazon Redshift.

- **Source:** AWS Kinesis Data Streams FAQ

Incorrect options with brief explanations:

1. **Amazon Kinesis Data Firehose:**
   - It is designed to load streaming data into data stores and analytics tools like Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk.
   - It can capture, transform, and load streaming data, enabling near real-time analytics with existing BI tools and dashboards.
   - Firehose is a fully managed service that automatically scales to match throughput and requires no ongoing administration.
   - It is not designed for concurrent consumption by multiple applications.
2. **Amazon Kinesis Data Analytics:**
   - It is used to analyze streaming data in real-time using SQL queries or Java applications.
   - It enables building sophisticated streaming applications to organize, transform, aggregate, and analyze data at any scale.
   - While it is powerful for analytics, it is not designed for capturing and providing a concurrent feed to multiple downstream applications.
3. **Amazon Simple Queue Service (Amazon SQS):**
   - SQS is a fully managed message queuing service that enables decoupling and scaling microservices, distributed systems, and serverless applications.
   - SQS offers standard queues with maximum throughput and best-effort ordering and FIFO queues for exactly-once processing in order.
   - SQS does not support concurrent consumption of the same message by multiple consumers at the same time.

Conclusion / Points to memorize:

1. **Amazon Kinesis Data Streams (KDS):**
   - Ideal for real-time data streaming and concurrent consumption by multiple applications.
   - Supports ordering of records and replaying data for multiple applications.
2. **Amazon Kinesis Data Firehose:**
   - Used to load streaming data into data stores for near real-time analytics.
   - Not designed for concurrent consumption by multiple applications.
3. **Amazon Kinesis Data Analytics:**
   - Used for real-time data analytics with SQL queries or Java applications.
   - Not suitable for capturing and providing concurrent feeds to multiple applications.
4. **Amazon Simple Queue Service (SQS):**
   - Used for decoupling and scaling systems with message queuing.
- Does not support concurrent consumption of the same message by multiple consumers.

Question 35

The engineering team at a company is moving the static content from the company's logistics website hosted on Amazon EC2 instances to an Amazon S3 bucket. The team wants to use an Amazon CloudFront distribution to deliver the static content. The security group used by the Amazon EC2 instances allows the website to be accessed by a limited set of IP ranges from the company's suppliers. Post-migration to Amazon CloudFront, access to the static content should only be allowed from the aforementioned IP addresses. Which options would you combine to build a solution to meet these requirements? (Select two)

Correct Options:

2. Create an AWS WAF ACL and use an IP match condition to allow traffic only from those IPs that are allowed in the Amazon EC2 security group. Associate this new AWS WAF ACL with the Amazon CloudFront distribution.

3. Configure an origin access identity (OAI) and associate it with the Amazon CloudFront distribution. Set up the permissions in the Amazon S3 bucket policy so that only the OAI can read the objects.

Explanation behind correct options:

1. **Create an AWS WAF ACL and use an IP match condition to allow traffic only from those IPs that are allowed in the Amazon EC2 security group. Associate this new AWS WAF ACL with the Amazon CloudFront distribution:**
   - AWS WAF allows you to create rules that block or allow traffic based on specified conditions, such as IP addresses.
   - By using an IP match condition, you can ensure that only requests from the specified IP addresses are allowed.
   - Associating this WAF ACL with the CloudFront distribution ensures that the traffic is filtered before it reaches the S3 bucket.
2. **Configure an origin access identity (OAI) and associate it with the Amazon CloudFront distribution. Set up the permissions in the Amazon S3 bucket policy so that only the OAI can read the objects:**
   - OAI is used to restrict access to the S3 bucket content so that it can only be accessed through the CloudFront distribution.
   - This setup ensures that the S3 bucket is not publicly accessible and can only be accessed by CloudFront, which then applies the WAF ACL rules.

Incorrect options with brief explanations:

1. **Create an AWS Web Application Firewall (AWS WAF) ACL and use an IP match condition to allow traffic only from those IPs that are allowed in the Amazon EC2 security group. Associate this new AWS WAF ACL with the Amazon S3 bucket policy:**
   - AWS WAF cannot be directly associated with an S3 bucket policy. WAF is used with CloudFront, API Gateway, or ALB.
2. **Create a new security group that allows traffic from the same IPs as specified in the current Amazon EC2 security group. Associate this new security group with the Amazon CloudFront distribution:**
   - Security groups are used with VPC resources like EC2 instances and cannot be associated with a CloudFront distribution, which uses edge locations.
3. **Create a new NACL that allows traffic from the same IPs as specified in the current Amazon EC2 security group. Associate this new NACL with the Amazon CloudFront distribution:**
   - Network ACLs (NACLs) are associated with subnets within a VPC and cannot be used with CloudFront, which is a global service using edge locations.

Conclusion / Points to memorize:

1. **AWS WAF with CloudFront:**
   - Use AWS WAF ACLs to control access based on IP addresses.
   - Associate WAF ACLs with CloudFront distributions to filter traffic.
2. **Origin Access Identity (OAI):**
   - OAI restricts access to S3 bucket content to be accessible only through CloudFront.
   - Set up S3 bucket policies to allow access only to OAI.
3. **CloudFront Compatibility:**
   - Security groups and NACLs cannot be used with CloudFront.
   - WAF can be used with CloudFront to provide IP-based access control.
4. **Configuration Best Practices:**
   - Always use OAI to restrict direct access to S3 buckets when using CloudFront.
- Use WAF for IP-based access control and other web application firewall functionalities.

Question 36

A biotechnology company has multiple High Performance Computing (HPC) workflows that quickly and accurately process and analyze genomes for hereditary diseases. The company is looking to migrate these workflows from their on-premises infrastructure to AWS Cloud. As a solutions architect, which of the following networking components would you recommend on the Amazon EC2 instances running these HPC workflows?

Correct Option:

2. Elastic Fabric Adapter (EFA)

Explanation behind correct option:

1. **Elastic Fabric Adapter (EFA):**
   - EFA is designed to accelerate High Performance Computing (HPC) and machine learning applications.
   - It enhances the performance of inter-instance communication, which is crucial for scaling HPC and machine learning applications.
   - EFA provides all the functionalities of Elastic Network Adapter (ENA) devices, plus an OS bypass hardware interface allowing user-space applications to communicate directly with the hardware-provided reliable transport functionality.
   - This direct communication bypasses the instance kernel, significantly improving performance for HPC workflows.

Incorrect options with brief explanations:

1. **Elastic Network Adapter (ENA):**
   - ENA supports enhanced networking via single root I/O virtualization (SR-IOV) for high-performance networking capabilities.
   - While ENA provides higher bandwidth, higher packet per second (PPS) performance, and lower latencies, it lacks the OS bypass functionality provided by EFA, which is crucial for HPC applications.
2. **Elastic IP Address (EIP):**
   - An EIP is a static IPv4 address associated with your AWS account.
   - It is used for public IP address allocation and does not contribute to HPC networking performance.
3. **Elastic Network Interface (ENI):**
   - ENI is a logical networking component representing a virtual network card in a VPC.
   - It is the simplest networking component and does not provide the enhanced capabilities needed for HPC workflows.

Conclusion / Points to memorize:

1. **Elastic Fabric Adapter (EFA):**

- Designed specifically for HPC and machine learning applications.
- Enhances inter-instance communication performance.
- Provides OS bypass hardware interface for direct communication with hardware.

2. **Elastic Network Adapter (ENA):**
   - Supports enhanced networking but lacks the direct communication capabilities of EFA.
3. **Elastic IP Address (EIP):**
   - Used for static public IP address allocation, not relevant for HPC networking performance.
4. **Elastic Network Interface (ENI):**
   - Basic virtual network card, insufficient for HPC workflows.
5. **Use EFA for HPC Workflows:**

- Always opt for EFA when dealing with high-performance computing requirements on AWS for its enhanced capabilities and direct communication features.

Question 37

A company has its application servers in the public subnet that connect to the Amazon RDS instances in the private subnet. For regular maintenance, the Amazon RDS instances need patch fixes that need to be downloaded from the internet. Considering the company uses only IPv4 addressing and is looking for a fully managed service, which of the following would you suggest as an optimal solution?

Correct Option:

4. Configure a Network Address Translation gateway (NAT gateway) in the public subnet of the VPC

Explanation behind correct option:

1. **Configure a Network Address Translation gateway (NAT gateway) in the public subnet of the VPC:**
   - A NAT gateway allows instances in a private subnet to connect to the internet or other AWS services while preventing inbound connections from the internet.
   - NAT gateway is a fully managed service, which means AWS handles its maintenance and management.
   - You must specify the public subnet in which the NAT gateway resides and associate an Elastic IP address with it.
   - After creation, update the route table for private subnets to point internet-bound traffic to the NAT gateway.

Incorrect options with brief explanations:

1. **Configure an Egress-only internet gateway for the resources in the private subnet of the VPC:**
   - An egress-only internet gateway supports IPv6 traffic only. Since the company uses IPv4, this option is not applicable.
2. **Configure a Network Address Translation instance (NAT instance) in the public subnet of the VPC:**
   - A NAT instance allows private subnet instances to access the internet but requires manual management, unlike the fully managed NAT gateway.
   - Managing a NAT instance involves maintaining high availability, scaling, and patching, which is not optimal compared to the NAT gateway.
3. **Configure the Internet Gateway of the VPC to be accessible to the private subnet resources by changing the route tables:**
   - Directly connecting private subnet instances to the internet gateway is not feasible without a NAT instance or NAT gateway, as it would expose private instances to inbound internet traffic.

Conclusion / Points to memorize:

1. **NAT Gateway:**
   - Use for enabling private subnet instances to access the internet while blocking inbound traffic.
   - Fully managed service, no maintenance required.
   - Requires an Elastic IP and must be placed in a public subnet.
   - Update private subnet route tables to direct internet-bound traffic to the NAT gateway.
2. **Egress-only Internet Gateway:**
   - Supports only IPv6 traffic.
   - Not suitable for IPv4-only environments.
3. **NAT Instance:**
   - Requires manual management (scaling, availability, patching).
   - Used for similar purposes as NAT gateway but less optimal due to management overhead.
4. **Internet Gateway:**
   - Provides a connection to the internet.

- Cannot be directly used with private subnets without NAT configurations.

Question 38

A media company wants a low-latency way to distribute live sports results which are delivered via a proprietary application using UDP protocol. As a solutions architect, which of the following solutions would you recommend such that it offers the BEST performance for this use case?

Correct Option:

1. Use AWS Global Accelerator to provide a low latency way to distribute live sports results

Explanation behind correct option:

1. **Use AWS Global Accelerator to provide a low latency way to distribute live sports results:**
   - AWS Global Accelerator is a networking service that helps improve the availability and performance of applications with global users.
   - It provides static IP addresses as fixed entry points to your applications, simplifying management.
   - It routes user traffic to the optimal endpoint based on performance, reacting instantly to changes in application health, user location, and policies.
   - AWS Global Accelerator is ideal for non-HTTP use cases such as gaming (UDP), IoT (MQTT), or Voice over IP, which matches the given use case.

Incorrect options with brief explanations:

2. **Use Elastic Load Balancing (ELB) to provide a low latency way to distribute live sports results:**
   - ELB distributes incoming application traffic across multiple targets like EC2 instances, containers, IP addresses, and Lambda functions.
   - It handles traffic load but does not specifically reduce latency for incoming traffic.
   - ELB is not designed for optimizing performance for UDP traffic.
3. **Use Amazon CloudFront to provide a low latency way to distribute live sports results:**
   - Amazon CloudFront is a content delivery network (CDN) that delivers data, videos, applications, and APIs with low latency and high transfer speeds.
   - It supports HTTP/RTMP protocols but is not designed for UDP traffic.
   - CloudFront is more suitable for cacheable content rather than real-time streaming via UDP.
4. **Use Auto Scaling group to provide a low latency way to distribute live sports results:**
   - Auto Scaling groups ensure the correct number of EC2 instances are available to handle the load.
   - They help with scalability but do not address the issue of reducing latency for traffic distribution.

Conclusion / Points to memorize:

1. **AWS Global Accelerator:**
   - Ideal for improving availability and performance of applications globally.
   - Provides static IP addresses and routes traffic based on optimal performance.
   - Suitable for non-HTTP use cases (e.g., gaming, IoT, VoIP) including UDP traffic.
   - Reacts to changes in application health and user location instantly.
2. **Elastic Load Balancer (ELB):**
   - Distributes application traffic but does not specifically reduce latency.
   - Not optimized for UDP traffic.
3. **Amazon CloudFront:**
   - CDN optimized for HTTP/RTMP protocols and cacheable content.
   - Not designed for real-time UDP traffic distribution.
4. **Auto Scaling Group:**
   - Ensures the right number of instances but does not reduce traffic latency.
- Focuses on scalability rather than performance optimization.

Question 39

An IT training company hosted its website on Amazon S3 a couple of years ago. Due to COVID-19 related travel restrictions, the training website has suddenly gained traction. With an almost 300% increase in the requests served per day, the company's AWS costs have sky-rocketed for just the Amazon S3 outbound data costs. As a Solutions Architect, can you suggest an alternate method to reduce costs while keeping the latency low?

Correct Option:

3. Configure Amazon CloudFront to distribute the data hosted on Amazon S3 cost-effectively

Explanation behind correct option:

1. **Configure Amazon CloudFront to distribute the data hosted on Amazon S3 cost-effectively:**
   - **Performance Improvement:** Amazon CloudFront is a content delivery network (CDN) that delivers content with low latency by caching it in a worldwide network of edge locations.

- **Cost Efficiency:** Delivering data through CloudFront is often more cost-effective than directly from S3 because CloudFront caches content closer to users, reducing the amount of data transfer from S3.
- **Security:** CloudFront adds an additional layer of security to your content delivery.
- **Usage:** When a user requests content, CloudFront serves it from the nearest edge location. If the content is not cached, CloudFront retrieves it from S3, caches it, and then serves it, reducing subsequent retrieval costs from S3.
- **No Data Transfer Fees:** There is no data transfer fee from Amazon S3 to CloudFront.

Incorrect options with brief explanations:

2. **To reduce Amazon S3 cost, the data can be saved on an Amazon EBS volume connected to an Amazon EC2 instance that can host the application:**
   - **Limited Accessibility:** Amazon EBS volumes are accessible only through EC2 instances and are region-specific.
   - **Cost:** While EBS is relatively cheap, it is not as cost-effective as S3 for large-scale data storage and delivery.
   - **Management Overhead:** Requires managing and maintaining EC2 instances.
3. **Use Amazon EFS service, as it provides a shared, scalable, fully managed elastic NFS file system for storing AWS Cloud or on-premises data:**
   - **Higher Cost:** Amazon EFS is more expensive than Amazon S3.
   - **Not Suitable for Cost Reduction:** EFS is designed for different use cases and does not align with the goal of reducing costs for web content delivery.
4. **Configure Amazon S3 Batch Operations to read data in bulk at one go, to reduce the number of calls made to Amazon S3 buckets:**
   - **Irrelevant Use Case:** Amazon S3 Batch Operations is designed for large-scale batch operations on S3 objects and not for reducing content delivery costs.
   - **Misleading:** This option does not address the issue of reducing outbound data transfer costs.

Conclusion / Points to memorize:

1. **Amazon CloudFront:**
   - Ideal for reducing data transfer costs from S3.
   - Provides low latency and high transfer speeds by caching content in edge locations.
   - No data transfer fees from S3 to CloudFront.
   - Enhances performance and adds a layer of security.
2. **Amazon EBS and EFS:**
   - EBS is region-specific and tied to EC2 instances, not ideal for reducing web content delivery costs.
   - EFS is more expensive and not suitable for reducing costs in this scenario.
3. **Amazon S3 Batch Operations:**
   - Designed for batch operations on S3 objects.

- Not related to cost reduction for data transfer or content delivery.

Question 40

A legacy application is built using a tightly-coupled monolithic architecture. Due to a sharp increase in the number of users, the application performance has degraded. The company now wants to decouple the architecture and adopt AWS microservices architecture. Some of these microservices need to handle fast-running processes whereas other microservices need to handle slower processes. Which of these options would you identify as the right way of connecting these microservices?

Explanation behind correct option:

1. **Configure Amazon Simple Queue Service (Amazon SQS) queue to decouple microservices running faster processes from the microservices running slower ones:**
   - **Decoupling:** SQS decouples application components so that they run and fail independently, enhancing the overall fault tolerance of the system.
   - **Message Storage and Replay:** SQS stores messages and allows them to be replayed, which is critical for ensuring that slower processes can catch up without losing messages.
   - **Scalability:** SQS handles any volume of data and any level of throughput without message loss, making it ideal for scaling microservices.
   - **Redundancy:** Multiple copies of each message are stored across multiple availability zones, ensuring high availability.
   - **Use Case Fit:** Perfectly fits the requirement of handling fast and slow processes by providing reliable message queuing.

Incorrect options with brief explanations:

2. **Use Amazon Simple Notification Service (Amazon SNS) to decouple microservices running faster processes from the microservices running slower ones:**
   - **Pub-Sub Model:** SNS uses a “publish-subscribe” model with push notifications, which is less suitable for ensuring that messages are processed at the comfort of slower microservices.

- **No Message Storage:** SNS does not store messages, assuming that subscribers are always available to receive notifications. This does not fit the requirement of decoupling processes with varying speeds.

3. **Configure Amazon Kinesis Data Streams to decouple microservices running faster processes from the microservices running slower ones:**
   - **Real-Time Streaming:** Kinesis is designed for real-time, high-volume data streaming and follows a pub-sub model.
   - **Not Suitable:** Although Kinesis can handle high throughput, it is not designed for the decoupling of processes with different processing speeds and does not store messages like SQS.
4. **Add Amazon EventBridge to decouple the complex architecture:**
   - **Event-Based Service:** EventBridge is excellent for integrating AWS services with non-AWS SaaS applications and for immediate event processing.
   - **Tightly Coupled:** It requires downstream applications to process events as they arrive, which does not support the requirement for decoupling fast and slow processes effectively.

Conclusion / Points to Memorize:

1. **Amazon SQS:**
   - Ideal for decoupling microservices with different processing speeds.
   - Provides reliable message storage and replay capabilities.
   - Ensures high availability and fault tolerance with redundant message storage.
2. **Amazon SNS:**
   - Best for scenarios requiring a pub-sub model with immediate push notifications.
   - Not suitable for storing messages and handling varied processing speeds.
3. **Amazon Kinesis:**
   - Designed for real-time data streaming and high throughput.
   - Not suitable for decoupling processes with different processing speeds.
4. **Amazon EventBridge:**
   - Ideal for integrating AWS and non-AWS services with immediate event processing.

- Not suitable for scenarios requiring decoupling of processes with varied speeds.

Question 41

A social media startup uses AWS Cloud to manage its IT infrastructure. The engineering team at the startup wants to perform weekly database rollovers for a MySQL database server using a serverless cron job that typically takes about 5 minutes to execute the database rollover script written in Python. The database rollover will archive the past week's data from the production database to keep the database small while still keeping its data accessible. As a solutions architect, which of the following would you recommend as the MOST cost-efficient and reliable solution?

Correct Option:

1. Schedule a weekly Amazon EventBridge event cron expression to invoke an AWS Lambda function that runs the database rollover job

Explanation behind correct option:

1. **Schedule a weekly Amazon EventBridge event cron expression to invoke an AWS Lambda function that runs the database rollover job:**
   - **Cost-Efficiency:** AWS Lambda charges only for the compute time consumed, making it a cost-effective solution.
   - **Serverless:** No need to manage servers, aligning with the requirement for a serverless cron job.
   - **Reliability:** EventBridge can reliably trigger the Lambda function on a specified schedule using cron expressions.
   - **Simplicity:** AWS Lambda integrates easily with EventBridge for scheduling, providing a straightforward implementation for running the Python script weekly.

Incorrect options with brief explanations:

2. **Provision an Amazon EC2 spot instance to run the database rollover script to be run via an OS-based weekly cron expression:**
   - **No Guarantee:** Spot instances do not guarantee availability at specific times as they run based on capacity availability.
   - **Management Overhead:** Requires managing the EC2 instance and ensuring it is up and running when needed.
   - **Not Serverless:** The requirement specifies a serverless solution, which this option does not fulfill.
3. **Provision an Amazon EC2 scheduled reserved instance to run the database rollover script to be run via an OS-based weekly cron expression:**
   - **Cost:** Scheduled Reserved Instances are less cost-effective compared to AWS Lambda for periodic tasks.
   - **Management Overhead:** Similar to spot instances, requires managing the EC2 instance.
   - **Not Serverless:** Again, this does not meet the requirement for a serverless solution.
4. **Create a time-based schedule option within an AWS Glue job to invoke itself every week and run the database rollover script:**
   - **Misfit for Use Case:** AWS Glue is designed for ETL tasks and data transformation, not for running custom scripts like database rollovers.

- **Cost:** AWS Glue is generally more expensive than Lambda for short, periodic tasks.
- **Not Ideal:** AWS Lambda is a better fit for running lightweight scripts periodically.

Conclusion / Points to Memorize:

1. **AWS Lambda + EventBridge:**
   - Ideal for serverless cron jobs.
   - Cost-effective as you pay only for the compute time used.
   - Reliable scheduling with EventBridge.
   - Simplifies infrastructure management by eliminating the need for server provisioning.
2. **AWS Glue:**
   - Best suited for ETL tasks, not for running arbitrary scripts periodically.
   - Typically more costly for short-duration tasks compared to Lambda.
3. **Amazon EC2 Spot Instances:**
   - Cost-effective but lacks guaranteed availability.
   - Requires managing the instances, contrary to the serverless requirement.
4. **Amazon EC2 Scheduled Reserved Instances:**
   - Scheduled usage but higher cost compared to Lambda.

- Not a serverless solution and requires managing EC2 instances.

Question 42

A data analytics company manages an application that stores user data in an Amazon DynamoDB table. The development team has observed that once in a while, the application writes corrupted data in the Amazon DynamoDB table. As soon as the issue is detected, the team needs to remove the corrupted data at the earliest. What do you recommend?

Correct Option:

4. Use Amazon DynamoDB point in time recovery to restore the table to the state just before corrupted data was written

Explanation behind correct option:

1. **Use Amazon DynamoDB point in time recovery to restore the table to the state just before corrupted data was written:**
   - **Point-in-Time Recovery (PITR):** Allows you to back up your DynamoDB table data continuously with per-second granularity.
   - **Restoration:** You can restore your table to any second within the preceding 35 days.
   - **Accidental Writes and Deletes:** Helps protect against accidental writes and deletes, making it suitable for quickly removing corrupted data.

Incorrect options with brief explanations:

2. **Use Amazon DynamoDB on-demand backup to restore the table to the state just before corrupted data was written:**
   - **Manual Backup:** On-demand backups are created manually and not automatically.
   - **Not Suitable:** On-demand backup cannot be created preemptively to handle sporadic data corruption issues, making it unsuitable for immediate restoration.
3. **Configure the Amazon DynamoDB table as a global table and point the application to use the table from another AWS region that has no corrupted data:**
   - **Global Tables:** Designed for multi-region replication and high availability, not for handling data corruption.
   - **Replication:** Changes are replicated across all regions, so corrupted data would be propagated, making this option ineffective.
4. **Use Amazon DynamoDB Streams to restore the table to the state just before corrupted data was written:**
   - **Streams Functionality:** Captures item-level changes and stores them in a log for up to 24 hours.
   - **Complexity:** Requires significant custom coding to rebuild table data to the desired state, which is not ideal for immediate restoration.

Conclusion / Points to Memorize:

1. **Amazon DynamoDB Point-in-Time Recovery (PITR):**
   - Automatically backs up table data continuously.
   - Allows restoration to any second within the last 35 days.
   - Ideal for protecting against accidental writes and deletes.
   - Suitable for quickly removing corrupted data.
2. **Amazon DynamoDB On-Demand Backup:**
   - Requires manual creation of backups.
   - Not suitable for handling sporadic data corruption issues.

3. **Amazon DynamoDB Global Tables:**
    - Designed for multi-region replication and high availability.
    - Not suitable for preventing data corruption propagation.
4. **Amazon DynamoDB Streams:**
    - Captures item-level changes for up to 24 hours.

- Requires custom coding for rebuilding data, making it less suitable for immediate restoration.

Question 43

A media streaming company is looking to migrate its on-premises infrastructure into the AWS Cloud. The engineering team is looking for a fully managed NoSQL persistent data store with in-memory caching to maintain low latency that is critical for real-time scenarios such as video streaming and interactive content. The team expects the number of concurrent users to touch up to a million so the database should be able to scale elastically. As a solutions architect, which of the following AWS services would you recommend for this use-case?

Correct Option:

3. Amazon DynamoDB

Explanation behind correct option:

1. **Amazon DynamoDB:**
    - **Performance:** Delivers single-digit millisecond performance at any scale.
    - **Fully Managed:** Multi-region, multi-master, durable database with built-in security, backup and restore.
    - **Scalability:** Designed to handle up to a million concurrent users, scaling elastically.
    - **In-Memory Caching:** Uses DynamoDB Accelerator (DAX) for fast in-memory performance, reducing read latency significantly, which is crucial for real-time video streaming and interactive content.

Incorrect options with brief explanations:

2. **Amazon DocumentDB:**
    - **Document Database:** Supports MongoDB workloads and is designed for JSON data.
    - **No In-Memory Caching:** Lacks built-in in-memory caching necessary for low-latency real-time applications, making it less suitable for this use case.
3. **Amazon ElastiCache:**
    - **Caching Layer:** Provides high throughput and low latency in-memory data stores like Redis and Memcached.
    - **Not a Database:** Used as a caching layer to improve performance of existing databases, not as a fully managed NoSQL persistent data store.
4. **Amazon RDS:**
    - **Relational Database:** Supports relational database engines like MySQL, PostgreSQL, Oracle, and SQL Server.
    - **Not NoSQL:** Does not meet the requirement for a NoSQL database and lacks the in-memory caching integration provided by DynamoDB and DAX.

Conclusion / Points to Memorize:

1. **Amazon DynamoDB:**
    - Best for high-performance NoSQL needs with in-memory caching (DAX).
    - Handles up to millions of concurrent users with single-digit millisecond latency.
    - Fully managed, multi-region, and scalable solution.
2. **Amazon DocumentDB:**
    - Suitable for MongoDB workloads.
    - Lacks built-in in-memory caching for real-time low-latency applications.
3. **Amazon ElastiCache:**
    - Used for caching to boost database performance.
    - Not a fully managed NoSQL database solution.
4. **Amazon RDS:**
    - Relational database service.

- Not suitable for NoSQL requirements and lacks native in-memory caching support for real-time scenarios.

Question 44

A company has a license-based, expensive, legacy commercial database solution deployed at its on-premises data center. The company wants to migrate this database to a more efficient, open-source, and cost-effective option on AWS Cloud. The CTO at the company wants a solution that can handle complex

database configurations such as secondary indexes, foreign keys, and stored procedures. As a solutions architect, which of the following AWS services should be combined to handle this use-case? (Select two)

Correct Options:

4. AWS Database Migration Service (AWS DMS)

5. AWS Schema Conversion Tool (AWS SCT)

Explanation behind correct options:

1. **AWS Schema Conversion Tool (AWS SCT):**
   - **Functionality:** Converts the source database schema and code to match that of the target database.
   - **Usage:** Essential for heterogeneous migrations where the source and target database engines are different (e.g., Oracle to Amazon Aurora, Oracle to PostgreSQL).
   - **Benefit:** Handles complex database configurations such as secondary indexes, foreign keys, and stored procedures.
2. **AWS Database Migration Service (AWS DMS):**
   - **Functionality:** Migrates databases to AWS quickly and securely while keeping the source database fully operational.
   - **Usage:** Used after schema conversion to migrate data from the source database to the target database.
   - **Benefit:** Supports both homogeneous and heterogeneous migrations, handling data type conversions automatically during migration.

Incorrect options with brief explanations:

1. **AWS Snowball Edge:**
   - **Functionality:** Designed for secure and fast data transfer to AWS, not for database migrations.
   - **Usage:** Best suited for large-scale data transfer and pre-processing use cases, not for handling database schema and data migrations.
2. **AWS Glue:**
   - **Functionality:** Fully managed extract, transform, and load (ETL) service for data preparation and loading for analytics.
   - **Usage:** Not designed for database migrations but for batch ETL data processing.
3. **Basic Schema Copy:**
   - **Functionality:** Copies the basic schema to the target instance but does not handle secondary indexes, foreign keys, or stored procedures.
   - **Usage:** Useful for test migrations but not suitable for complex schema migrations required for production databases.

Conclusion / Points to Memorize:

1. **AWS Schema Conversion Tool (AWS SCT):**
   - Converts source schema and code to match the target database.
   - Handles complex database configurations (secondary indexes, foreign keys, stored procedures).
2. **AWS Database Migration Service (AWS DMS):**
   - Migrates data securely with minimal downtime.
   - Supports homogeneous and heterogeneous migrations.
   - Essential for actual data migration after schema conversion.
3. **AWS Snowball Edge and AWS Glue:**
   - Not suitable for database migrations; Snowball Edge is for data transfer and Glue for ETL processing.
4. **Basic Schema Copy:**

- Only for quick, simple schema copy, not suitable for complex production migrations.

Question 45

An e-commerce company uses Microsoft Active Directory to provide users and groups with access to resources on the on-premises infrastructure. The company has extended its IT infrastructure to AWS in the form of a hybrid cloud. The engineering team at the company wants to run directory-aware workloads on AWS for a SQL Server-based application. The team also wants to configure a trust relationship to enable single sign-on (SSO) for its users to access resources in either domain. As a solutions architect, which of the following AWS services would you recommend for this use-case?

Correct Option:

2. AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD)

Explanation behind correct options:

1. **AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD):**
   - **Functionality:** Powered by an actual Microsoft Windows Server Active Directory (AD), managed by AWS.
   - **Usage:** Enables running directory-aware workloads in the AWS Cloud, such as SQL Server-based applications.

- **Benefit:** Allows configuration of a trust relationship between AWS Managed Microsoft AD in the AWS Cloud and existing on-premises Microsoft Active Directory. This setup provides users and groups with access to resources in either domain using single sign-on (SSO).

Incorrect options with brief explanations:

1. **Active Directory Connector:**
   - **Functionality:** Connects existing on-premises Active Directory to AWS.
   - **Limitation:** Only allows on-premises users to log in to AWS applications and services with their Active Directory credentials. It does not support running directory-aware workloads on AWS or establishing trust relationships.
2. **Simple Active Directory (Simple AD):**
   - **Functionality:** Provides a subset of the features offered by AWS Managed Microsoft AD, powered by a Samba 4 Active Directory Compatible Server.
   - **Limitation:** Does not support trust relationships with other domains, making it unsuitable for the given use case.
3. **Amazon Cloud Directory:**
   - **Functionality:** A cloud-native directory that can store application-specific objects with multiple relationships and schemas.
   - **Limitation:** Not suitable for establishing trust relationships with on-premises infrastructure. It is designed for storing hierarchical data and not for running directory-aware workloads.

Conclusion / Points to Memorize:

1. **AWS Managed Microsoft AD:**
   - Ideal for running directory-aware workloads on AWS.
   - Supports trust relationships with on-premises Active Directory.
   - Suitable for environments with more than 5,000 users.
2. **AD Connector:**
   - Used for allowing on-premises users to log in to AWS applications with their Active Directory credentials.
   - Does not support directory-aware workloads or trust relationships.
3. **Simple AD:**
   - Least expensive option for environments with 5,000 or fewer users.
   - Does not support advanced Microsoft AD features such as trust relationships.
4. **Amazon Cloud Directory:**
   - Designed for storing hierarchical data.
- Not suitable for running directory-aware workloads or establishing trust relationships.

Question 46

A leading news aggregation company offers hundreds of digital products and services for customers ranging from law firms to banks to consumers. The company bills its clients based on per unit of clickstream data provided to the clients. As the company operates in a regulated industry, it needs to have the same ordered clickstream data available for auditing within a window of 7 days. As a solutions architect, which of the following AWS services provides the ability to run the billing process and auditing process on the given clickstream data in the same order?

Correct Option:

3. Amazon Kinesis Data Streams

Explanation behind correct options:

- **Amazon Kinesis Data Streams:**
  - **Functionality:** Massively scalable and durable real-time data streaming service.
  - **Capability:** Continuously captures gigabytes of data per second from numerous sources like website clickstreams, database event streams, financial transactions, social media feeds, IT logs, and location-tracking events.
  - **Feature:** Enables real-time processing of streaming big data, providing ordering of records and the ability to read and/or replay records in the same order to multiple Amazon Kinesis Applications.
  - **Use Case:** Suitable when the ability to consume records in the same order a few hours later is required, such as having a billing application and an audit application that runs a few hours behind the billing application. KDS stores data for up to 365 days, making it easy to run the audit application up to 7 days behind the billing application.

Incorrect options with brief explanations:

1. **Amazon Kinesis Data Firehose:**
   - **Functionality:** Easiest way to load streaming data into data stores and analytics tools.

- **Limitation:** Designed to capture, transform, and load streaming data into data stores like Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk. It does not provide the ability to consume data in the same order a few hours later, making it unsuitable for the given use case.

2. **Amazon Kinesis Data Analytics:**
   - **Functionality:** Easiest way to analyze streaming data in real-time.
   - **Limitation:** Used to build SQL queries and sophisticated Java applications for common processing functions to organize, transform, aggregate, and analyze data. It is not designed for ensuring ordered consumption of data for auditing purposes.
3. **Amazon Simple Queue Service (SQS):**
   - **Functionality:** Fully managed message queuing service.
   - **Limitation:** Offers Standard and FIFO queues. While FIFO queues guarantee ordered processing, SQS cannot ensure that the same message will be consumed by multiple consumers in the same order a few hours later, making it unsuitable for the given use case.

Conclusion / Points to Memorize:

1. **Amazon Kinesis Data Streams (KDS):**
   - Best for real-time data streaming and processing.
   - Provides ordered records and the ability to replay records.
   - Suitable for applications requiring the same ordered data for multiple consumers, such as billing and auditing processes.
2. **Amazon Kinesis Data Firehose:**
   - Used for loading streaming data into data stores and analytics tools.
   - Not suitable for scenarios requiring ordered consumption of data.
3. **Amazon Kinesis Data Analytics:**
   - Used for analyzing streaming data in real-time with SQL queries and Java applications.
   - Not designed for ordered consumption and replay of data.
4. **Amazon Simple Queue Service (SQS):**
   - Message queuing service for decoupling microservices.

- Does not support ordered consumption of data for multiple consumers over a period of time.

Question 47

A small business has been running its IT systems on the on-premises infrastructure but the business now plans to migrate to AWS Cloud for operational efficiencies. As a Solutions Architect, can you suggest a cost-effective serverless solution for its flagship application that has both static and dynamic content?

Correct Option:

4. Host the static content on Amazon S3 and use AWS Lambda with Amazon DynamoDB for the serverless web application that handles dynamic content. Amazon CloudFront will sit in front of AWS Lambda for distribution across diverse regions

Explanation behind correct options:

- **Host the static content on Amazon S3 and use AWS Lambda with Amazon DynamoDB for the serverless web application that handles dynamic content. Amazon CloudFront will sit in front of AWS Lambda for distribution across diverse regions:**
  - **Static Content Hosting:** Amazon S3 is ideal for hosting static content such as HTML, CSS, JavaScript, and images. It provides high durability, availability, and low cost.
  - **Serverless Dynamic Content Handling:** AWS Lambda allows running code without provisioning or managing servers. When combined with Amazon DynamoDB, it provides a scalable, high-performance, serverless database solution for dynamic content.
  - **Global Distribution:** Amazon CloudFront, a content delivery network (CDN), caches the content at edge locations to reduce latency and improve the user experience by delivering content closer to users geographically.
  - **Cost-effective:** This solution leverages serverless components (AWS Lambda and DynamoDB), which scale automatically with demand and reduce operational overhead.

Incorrect options with brief explanations:

1. **Host both the static and dynamic content of the web application on Amazon S3 and use Amazon CloudFront for distribution across diverse regions/countries:**
   - **Limitation:** Amazon S3 is not suitable for hosting dynamic content. While it can serve static files efficiently, it lacks the capability to handle server-side processing required for dynamic content.
2. **Host the static content on Amazon S3 and use Amazon EC2 with Amazon RDS for generating the dynamic content. Amazon CloudFront can be configured in front of Amazon EC2 instance, to make global distribution easy:**

- **Limitation:** Amazon EC2 is not a serverless service; it requires management of instances, which adds operational overhead and may not be as cost-effective as serverless options like AWS Lambda.

3. **Host both the static and dynamic content of the web application on Amazon EC2 with Amazon RDS as database. Amazon CloudFront should be configured to distribute the content across geographically disperse regions:**
   - **Limitation:** This solution involves higher costs and more operational overhead compared to serverless architectures. Amazon EC2 and RDS need to be managed and scaled manually.

Conclusion / Points to Memorize:

1. **Serverless Architecture:**
   - **Static Content:** Use Amazon S3 for storing and serving static content.
   - **Dynamic Content:** Use AWS Lambda for serverless compute and Amazon DynamoDB for a serverless NoSQL database.
   - **Global Distribution:** Use Amazon CloudFront to cache content at edge locations, reducing latency.
2. **Cost-effective and Scalable:**
   - **AWS Lambda and DynamoDB:** Automatically scale with demand, reducing the need for manual intervention and management.
   - **Amazon S3:** Cost-effective storage solution for static content.
3. **Avoid EC2 for Serverless Solutions:**
   - **Operational Overhead:** Amazon EC2 requires instance management and is not serverless.
   - **Higher Costs:** EC2 and RDS combined can lead to higher operational costs compared to serverless alternatives.
4. **Use Cases:**
   - **AWS Lambda:** Ideal for dynamic, event-driven applications.
   - **Amazon DynamoDB:** Suitable for high-performance, scalable NoSQL databases.
   - **Amazon S3:** Best for static content hosting.

- **Amazon CloudFront:** Essential for low-latency content delivery across different geographic locations.

Question 48

A leading online gaming company is migrating its flagship application to AWS Cloud for delivering its online games to users across the world. The company would like to use a Network Load Balancer (NLB) to handle millions of requests per second. The engineering team has provisioned multiple instances in a public subnet and specified these instance IDs as the targets for the NLB. As a solutions architect, can you help the engineering team understand the correct routing mechanism for these target instances?

Correct Option:

2. Traffic is routed to instances using the primary private IP address specified in the primary network interface for the instance

Explanation behind correct options:

- **Traffic is routed to instances using the primary private IP address specified in the primary network interface for the instance:**
  - A Network Load Balancer (NLB) functions at the fourth layer of the OSI model (Transport layer) and can handle millions of requests per second.
  - When you specify targets using an instance ID, traffic is routed to instances using the primary private IP address specified in the primary network interface for the instance.
  - The load balancer rewrites the destination IP address from the data packet before forwarding it to the target instance.

Incorrect options with brief explanations:

1. **Traffic is routed to instances using the primary public IP address specified in the primary network interface for the instance:**
   - **Limitation:** Public IP addresses are not used for routing traffic to instances when specifying targets using instance IDs. NLB uses the private IP address for routing.
2. **Traffic is routed to instances using the primary elastic IP address specified in the primary network interface for the instance:**
   - **Limitation:** Elastic IP addresses are not used for routing traffic to instances when specifying targets using instance IDs. NLB uses the private IP address for routing.
3. **Traffic is routed to instances using the instance ID specified in the primary network interface for the instance:**
   - **Limitation:** Instance ID itself is not used for routing traffic. It is used to identify the target, but the actual routing is done using the primary private IP address.

Conclusion / Points to Memorize:

1. **Network Load Balancer (NLB) Basics:**
   - Operates at layer 4 (Transport layer) of the OSI model.
   - Can handle millions of requests per second.

- Designed for applications requiring extreme performance and low latency.

2. **Routing Mechanism:**
   - **Instance ID Targets:** Traffic is routed to instances using the primary private IP address.
   - **IP Address Targets:** Can route traffic using any private IP address from one or more network interfaces.
3. **Private IP Address Usage:**
   - When targets are specified using instance IDs, the NLB uses the primary private IP address for routing.
   - Public or elastic IP addresses are not used for routing in this case.
4. **Load Balancer Rewrite:**
   - NLB rewrites the destination IP address from the data packet before forwarding it to the target instance, ensuring proper routing within the VPC.
5. **Practical Application:**
   - Ensure instances in the target group are specified correctly using their instance IDs.

- Confirm that the primary network interface has the correct private IP address for routing.

Question 49

A financial services company wants to identify any sensitive data stored on its Amazon S3 buckets. The company also wants to monitor and protect all data stored on Amazon S3 against any malicious activity.

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

Correct Option:

Use Amazon GuardDuty to monitor any malicious activity on data stored in Amazon S3. Use Amazon Macie to identify any sensitive data stored on Amazon S3.

Explanation:

- **Amazon GuardDuty:**
  - **Functionality:** Provides threat detection by continuously monitoring for malicious activity and unauthorized behavior.
  - **Data Sources:** Analyzes AWS CloudTrail Events, Amazon VPC Flow Logs, and DNS Logs.
  - **Threat Intelligence:** Uses known malicious IP addresses, anomaly detection, and machine learning to identify threats accurately.
  - **Purpose:** Monitors and protects AWS accounts, workloads, and data stored in Amazon S3.
  - **How it works:** It enables continuous monitoring and protection by analyzing meta-data and integrated threat intelligence.
- **Amazon Macie:**
  - **Functionality:** A fully managed data security and data privacy service that uses machine learning and pattern matching.
  - **Sensitive Data Detection:** Automatically detects sensitive data types, including PII such as names, addresses, and credit card numbers.
  - **Visibility:** Provides constant visibility into the security and privacy of data stored in Amazon S3.
  - **Purpose:** Identifies and protects sensitive data on Amazon S3.
  - **How it works:** Analyzes buckets for sensitive data, integrates findings with workflows, and recommends actions.

Incorrect Options:

1. **Use Amazon Macie to monitor any malicious activity on data stored in Amazon S3.**
   - **Reason:** Amazon Macie is designed to discover and protect sensitive data, not to monitor malicious activity.
2. **Use Amazon GuardDuty to identify any sensitive data stored on Amazon S3.**
   - **Reason:** Amazon GuardDuty is for threat detection and monitoring malicious activities, not for identifying sensitive data.
3. **Use Amazon Macie to monitor any malicious activity on data stored in Amazon S3 as well as to identify any sensitive data stored on Amazon S3.**
   - **Reason:** Amazon Macie specializes in identifying sensitive data, not in monitoring for malicious activities.
4. **Use Amazon GuardDuty to monitor any malicious activity on data stored in Amazon S3 as well as to identify any sensitive data stored on Amazon S3.**
   - **Reason:** Amazon GuardDuty focuses on threat detection and does not identify sensitive data.

Conclusion / Points to Memorize:

- **Amazon GuardDuty** is used for threat detection, monitoring malicious activities, and unauthorized behavior on AWS accounts, workloads, and data stored in Amazon S3.
- **Amazon Macie** is used to discover, classify, and protect sensitive data on Amazon S3 using machine learning and pattern matching.
- Always use **Amazon GuardDuty** for monitoring and protecting against malicious activity.
- Always use **Amazon Macie** for identifying and protecting sensitive data.

Question 50

A global manufacturing company with facilities in the US, Europe, and Asia is designing a new distributed application to optimize its procurement workflow. The orders booked in one AWS Region should be visible to all AWS Regions in a second or less. The database should be able to facilitate failover with a short Recovery Time Objective (RTO). The uptime of the application is critical to ensure that the manufacturing processes are not impacted.

As a solutions architect, which of the following will you recommend as the MOST cost-effective solution?

Correct Option:

Provision Amazon Aurora Global Database

Explanation:

- **Amazon Aurora Global Database:**
  - **Failover Capabilities:** Provides more comprehensive failover capabilities than a default Aurora DB cluster.
  - **Recovery Time Objective (RTO):** The time it takes a system to return to a working state after a disaster. For Aurora global database, RTO can be in the order of minutes.
  - **Recovery Point Objective (RPO):** The amount of data that can be lost (measured in time). For Aurora global database, RPO is typically measured in seconds.
  - **Failover Approaches:**
    - **Managed Planned Failover:** Intended for controlled environments like DR testing scenarios, operational maintenance, and other planned operational procedures. Ensures no data loss (RPO is 0).
    - **Unplanned Failover ("Detach and Promote"):** Used to recover from an unplanned outage by performing a cross-Region failover to one of the secondaries. The RTO depends on how quickly tasks are performed. RPO is typically measured in seconds, depending on Aurora storage replication lag.

Disaster Recovery in Aurora Global Databases:

- Allows planning and recovery from disasters quickly.
- RTO and RPO values are typically in minutes and seconds, respectively.

Incorrect Options:

1. **Provision Amazon RDS for MySQL with a cross-Region read replica**
   - **Reason:** RDS Read Replicas need to be manually promoted to a standalone database instance, resulting in high RTO.
2. **Provision Amazon RDS for PostgreSQL with a cross-Region read replica**
   - **Reason:** Similar to MySQL, RDS Read Replicas require manual promotion, leading to high RTO.
3. **Provision Amazon DynamoDB global tables**
   - **Reason:** While DynamoDB global tables offer cross-region active-active capabilities with high performance, they lack the SQL-based database flexibility needed for this use case. Also, they are a much costlier solution compared to Aurora Global Database.

Conclusion / Points to Memorize:

- **Amazon Aurora Global Database**:
  - Best suited for applications needing cross-Region reads with low latency updates and quick failover.
  - Provides RTO in minutes and RPO in seconds.
  - Supports both managed planned failover (with zero data loss) and unplanned failover.
- **Amazon RDS Read Replicas**:
  - Requires manual promotion for failover.
  - Not suitable for applications needing low RTO.
- **Amazon DynamoDB Global Tables**:
  - Offers high performance and cross-region active-active capabilities.
  - More costly and less flexible for SQL-based applications.
- Does not have a concept of failover as it operates in an active-active configuration.

Question 51

The development team at a retail company wants to optimize the cost of Amazon EC2 instances. The team wants to move certain nightly batch jobs to spot instances. The team has hired you as a solutions architect to provide the initial guidance.

Which of the following would you identify as CORRECT regarding the capabilities of spot instances? (Select three)

Correct Options:

- **When you cancel an active spot request, it does not terminate the associated instance**

- **If a spot request is persistent, then it is opened again after your Spot Instance is interrupted**
- **Spot Fleets can maintain target capacity by launching replacement instances after Spot Instances in the fleet are terminated**

Explanation:

1. **When you cancel an active spot request, it does not terminate the associated instance**
   - **Reason:** If your Spot Instance request is active and has an associated running Spot Instance, or your Spot Instance request is disabled and has an associated stopped Spot Instance, canceling the request does not terminate the instance. You must terminate the running Spot Instance manually.
2. **If a spot request is persistent, then it is opened again after your Spot Instance is interrupted**
   - **Reason:** A Spot Instance request can be either one-time or persistent. If the spot request is persistent, the request is reopened after your Spot Instance is interrupted. This ensures that the request continues to be available for potential fulfillment even after interruptions.
3. **Spot Fleets can maintain target capacity by launching replacement instances after Spot Instances in the fleet are terminated**
   - **Reason:** A Spot Fleet is a set of Spot Instances and optionally On-Demand Instances launched based on specified criteria. Spot Fleets are designed to maintain target capacity by launching replacement instances after Spot Instances in the fleet are terminated, ensuring consistent availability.

Incorrect Options:

1. **When you cancel an active spot request, it terminates the associated instance as well**
   - **Reason:** Canceling the request does not automatically terminate the instance; termination must be done manually.
2. **If a spot request is persistent, then it is opened again after you stop the Spot Instance**
   - **Reason:** If the request is persistent and you stop your Spot Instance, the request is reopened only after you start your Spot Instance again, not immediately upon stopping.
3. **Spot Fleets cannot maintain target capacity by launching replacement instances after Spot Instances in the fleet are terminated**
   - **Reason:** This is incorrect because Spot Fleets are explicitly designed to maintain target capacity by launching replacement instances after Spot Instances in the fleet are terminated.

Conclusion / Points to Memorize:

- **Persistent Spot Requests:** Persistent spot requests reopen after Spot Instances are interrupted, ensuring continuous availability.
- **Canceling Spot Requests:** Canceling an active spot request does not terminate the associated instance; termination must be done manually.
- **Spot Fleets:** Spot Fleets maintain target capacity by launching replacement instances after Spot Instances are terminated, ensuring reliability and availability for your applications.

Question 52

An IT consultant is helping a small business revamp their technology infrastructure on the AWS Cloud. The business has two AWS accounts and all resources are provisioned in the us-west-2 region. The IT consultant is trying to launch an Amazon EC2 instance in each of the two AWS accounts such that the instances are in the same Availability Zone (AZ) of the us-west-2 region. Even after selecting the same default subnet (us-west-2a) while launching the instances in each of the AWS accounts, the IT consultant notices that the Availability Zones (AZs) are still different.

As a solutions architect, which of the following would you suggest resolving this issue?

Correct Option:

Use Availability Zone (AZ) ID to uniquely identify the Availability Zones across the two AWS Accounts

Explanation:

1. **Use Availability Zone (AZ) ID to uniquely identify the Availability Zones across the two AWS Accounts**
   - **Reason:** An Availability Zone is represented by a region code followed by a letter identifier; for example, us-east-1a. To ensure that resources are distributed across the Availability Zones for a region, AWS maps Availability Zones to names for each AWS account. For example, the Availability Zone us-west-2a for one AWS account might not be the same location as us-west-2a for another AWS account.
   - To coordinate Availability Zones across accounts, you must use the AZ ID, which is a unique and consistent identifier for an Availability Zone. For example, usw2-az2 is an AZ ID for the us-west-2 region and it has the same location in every AWS account.
   - You can view the AZ IDs by going to the service health section of the Amazon EC2 Dashboard via your AWS Management Console.

Incorrect Options:

1. **Use the default VPC to uniquely identify the Availability Zones across the two AWS Accounts**
   - **Reason:** A virtual private cloud (VPC) is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS Cloud. Since a VPC spans an AWS region, it cannot be used to uniquely identify an Availability Zone. Therefore, this option is incorrect.
2. **Use the default subnet to uniquely identify the Availability Zones across the two AWS Accounts**

- **Reason:** A subnet is a range of IP addresses in your VPC. A subnet spans an Availability Zone of an AWS region. The default subnet representing the Availability Zone us-west-2a for one AWS account might not be the same location as us-west-2a for another AWS account. Therefore, this option is incorrect.

3. **Reach out to AWS Support for creating the Amazon EC2 instances in the same Availability Zone (AZ) across the two AWS accounts**
   - **Reason:** Since the AZ ID is a unique and consistent identifier for an Availability Zone, there is no need to contact AWS Support. Therefore, this option is incorrect.

Conclusion / Points to Memorize:

- **Availability Zones (AZs):** AWS maps Availability Zones to names for each AWS account. To coordinate AZs across accounts, use the AZ ID, which is a unique and consistent identifier for an Availability Zone.
- **Viewing AZ IDs:** You can view the AZ IDs by going to the service health section of the Amazon EC2 Dashboard via your AWS Management Console.
- **Default VPC/Subnet:** VPCs and subnets are not suitable for uniquely identifying Availability Zones across different AWS accounts.

Question 53

An online gaming application has a large chunk of its traffic coming from users who download static assets such as historic leaderboard reports and the game tactics for various games. The current infrastructure and design are unable to cope up with the traffic and application freezes on most of the pages.

Which of the following is a cost-optimal solution that does not need provisioning of infrastructure?

Correct Option:

Use Amazon CloudFront with Amazon S3 as the storage solution for the static assets

Explanation:

1. **Simplified Management:**
   - Amazon S3 buckets automatically scale storage space, eliminating the need for planning and managing specific storage.
   - No need for server management or patching; S3 handles static content.
2. **Cost-Effective Content Delivery:**
   - CloudFront delivers content globally using a network of Edge Locations.
   - More cost-effective than direct S3 delivery due to caching closer to users.
3. **Improved Performance:**
   - Edge caching reduces load on S3 and improves response times.
   - No data transfer fees from S3 to CloudFront; only pay for delivered content.

Incorrect Options:

1. **Configure AWS Lambda with an Amazon RDS database to provide a serverless architecture**
   - **Reason:** Amazon RDS is not suitable for this scenario because it involves managing a database system, which introduces unnecessary overhead. The use-case can be effectively addressed with Amazon S3 for storing static content.
2. **Use Amazon CloudFront with Amazon DynamoDB for greater speed and low latency access to static assets**
   - **Reason:** Amazon DynamoDB is designed for key-value and document databases that deliver single-digit millisecond performance. However, it is an overkill and a costly solution for serving static assets, which can be efficiently handled by Amazon S3.
3. **Use AWS Lambda with Amazon ElastiCache and Amazon RDS for serving static assets at high speed and low latency**
   - **Reason:** As discussed, Amazon RDS introduces unnecessary overhead for managing static assets. Amazon S3 is a more appropriate and cost-effective solution for this requirement.

Conclusion / Points to Memorize:

- **Amazon CloudFront + S3:** Ideal for serving static assets with high speed and low latency without the need for provisioning infrastructure. It reduces the load on S3 buckets and ensures fast response times for users by caching content in Edge Locations.
- **Avoid Overhead:** Using services like Amazon RDS or DynamoDB for static content can introduce unnecessary complexity and cost.
- **Serverless Benefits:** Amazon S3 and CloudFront provide a serverless approach, eliminating the need for managing or patching servers.

Question 54

A retail company uses AWS Cloud to manage its IT infrastructure. The company has set up AWS Organizations to manage several departments running their AWS accounts and using resources such as Amazon EC2 instances and Amazon RDS databases. The company wants to provide shared and centrally-managed VPCs to all departments using applications that need a high degree of interconnectivity.

As a solutions architect, which of the following options would you choose to facilitate this use-case?

Correct Option:

Use VPC sharing to share one or more subnets with other AWS accounts belonging to the same parent organization from AWS Organizations

Explanation:

1. **Use VPC sharing to share one or more subnets with other AWS accounts belonging to the same parent organization from AWS Organizations**
   - **Reason:** VPC sharing (part of AWS Resource Access Manager) allows multiple AWS accounts to create their application resources such as Amazon EC2 instances, Amazon RDS databases, Amazon Redshift clusters, and AWS Lambda functions, into shared and centrally-managed Amazon Virtual Private Clouds (VPCs). The account that owns the VPC (owner) shares one or more subnets with other accounts (participants) that belong to the same organization from AWS Organizations. After a subnet is shared, the participants can view, create, modify, and delete their application resources in the subnets shared with them. Participants cannot view, modify, or delete resources that belong to other participants or the VPC owner.
   - This approach leverages the implicit routing within a VPC for applications requiring a high degree of interconnectivity and within the same trust boundaries. This reduces the number of VPCs to manage while maintaining separate accounts for billing and access control.

Incorrect Options:

1. **Use VPC sharing to share a VPC with other AWS accounts belonging to the same parent organization from AWS Organizations**
   - **Reason:** VPC sharing allows the sharing of subnets, not the entire VPC itself. Therefore, the VPC owner shares one or more subnets with other accounts, not the whole VPC. This option is incorrect as it suggests sharing the VPC, which is not possible.
2. **Use VPC peering to share a VPC with other AWS accounts belonging to the same parent organization from AWS Organizations**
   - **Reason:** VPC peering is a networking connection between two VPCs that allows traffic routing between them using private IP addresses. However, VPC peering does not facilitate centrally managed VPCs or shared subnets for centralized management. It merely allows communication between VPCs.
3. **Use VPC peering to share one or more subnets with other AWS accounts belonging to the same parent organization from AWS Organizations**
   - **Reason:** Similar to the previous option, VPC peering allows routing traffic between VPCs but does not facilitate shared subnets or centrally managed VPCs. Furthermore, an AWS owner account cannot share the VPC or subnets directly with another AWS account using VPC peering.

Conclusion / Points to Memorize:

- **VPC Sharing:** Best solution for centrally managed and shared VPCs where subnets can be shared across multiple AWS accounts within the same AWS Organization.
- **VPC Peering:** Allows communication between VPCs but does not provide centralized management or shared subnets.
- **AWS Resource Access Manager (RAM):** Utilized for VPC sharing to manage resources across multiple AWS accounts efficiently.
- **Subnets vs. VPC:** In VPC sharing, subnets are shared, not the entire VPC.

Question 55

The DevOps team at an IT company has created a custom VPC (V1) and attached an Internet Gateway (I1) to the VPC. The team has also created a subnet (S1) in this custom VPC and added a route to this subnet's route table (R1) that directs internet-bound traffic to the Internet Gateway. Now the team launches an Amazon EC2 instance (E1) in the subnet S1 and assigns a public IPv4 address to this instance. Next, the team also launches a Network Address Translation (NAT) instance (N1) in the subnet S1.

Under the given infrastructure setup, which of the following entities is doing the Network Address Translation for the Amazon EC2 instance E1?

Correct Answer:

Internet Gateway (I1)

Explanation:

1. **Internet Gateway (I1):**
   - **Purpose:** An Internet Gateway allows communication between your VPC and the internet.
   - **NAT Function:** It performs Network Address Translation (NAT) for instances with public IPv4 addresses.
   - **Supporting IPv4 and IPv6:** It supports both IPv4 and IPv6 traffic.
   - **Key Roles:**
     1. Provides a target for internet-routable traffic in the VPC route tables.
     2. Performs NAT for instances with public IP addresses, enabling them to communicate with the internet.
   - **Steps to Enable Internet Access:**
     1. Attach an Internet Gateway to your VPC.
     2. Add a route to the subnet's route table that directs internet-bound traffic to the Internet Gateway.
     3. Ensure instances have a globally unique IP address (public IPv4 address, Elastic IP address, or IPv6 address).
     4. Configure network access control lists and security group rules to allow relevant traffic.

Source: AWS Internet Gateway Documentation

2. **Incorrect Options:**
    - **Network Address Translation (NAT) instance (N1):**
        - **Purpose:** Enables instances in a private subnet to initiate outbound IPv4 traffic to the internet while preventing inbound traffic from the internet.
        - **Incorrect Usage:** E1 is in a public subnet and has a public IP address, so the NAT instance is not responsible for its NAT.
    - **Subnet (S1):**
        - **Definition:** A range of IP addresses in your VPC.
        - **Role:** It organizes instances within the VPC but does not perform NAT.
    - **Route Table (R1):**
        - **Definition:** Contains rules (routes) used to determine where network traffic is directed.
        - **Role:** Directs traffic but does not perform NAT.

Conclusion / Points to Memorize:

- **Internet Gateway (IGW):**
    - Performs NAT for instances with public IP addresses.
    - Enables communication between VPC and the internet.
    - Must be attached to the VPC and correctly referenced in the route table for public subnets.
- **NAT Instance:**
    - Used for private subnets to allow outbound internet traffic.
    - Not needed for instances in public subnets with public IP addresses.
- **Subnet and Route Table:**
- Organize and direct traffic within the VPC but do not perform NAT.

Question 56

A gaming company uses Application Load Balancers in front of Amazon EC2 instances for different services and microservices. The architecture has now become complex with too many Application Load Balancers in multiple AWS Regions. Security updates, firewall configurations, and traffic routing logic have become complex with too many IP addresses and configurations.

The company is looking at an easy and effective way to bring down the number of IP addresses allowed by the firewall and easily manage the entire network infrastructure.

Which of these options represents an appropriate solution for this requirement?

Correct Answer:

Launch AWS Global Accelerator and create endpoints for all the Regions. Register the Application Load Balancers of each Region to the corresponding endpoints.

Explanation:

1. **AWS Global Accelerator:**
    - **Global Network Infrastructure:** Sends user's traffic through Amazon Web Service's global network infrastructure, improving performance by up to 60%.
    - **Global Static IPs:** Provides two global static customer-facing IPs to simplify traffic management.
    - **Backend Management:** Allows adding or removing AWS application origins (e.g., Network Load Balancers, Application Load Balancers, EIPs, Amazon EC2 Instances) without user-facing changes.
    - **Automatic Routing:** Mitigates endpoint failure by automatically re-routing traffic to the nearest healthy available endpoint.
2. **Incorrect Options:**
    - **Network Load Balancer with Elastic IP:** While this setup is possible, it becomes equally cumbersome to manage due to the high number of load balancers.
    - **Elastic IPs for Application Load Balancers:** Application Load Balancers cannot be assigned Elastic IP addresses.
    - **Elastic IP to Auto Scaling Group:** Elastic IP cannot be assigned to an Auto Scaling Group directly since ASG manages a collection of Amazon EC2 instances, not a single entity.

Conclusion / Points to Memorize:

- **AWS Global Accelerator:**
    - Simplifies traffic management with global static IPs.
    - Improves performance by routing traffic through AWS's global network.

    - Automatically re-routes traffic to healthy endpoints.
    - Suitable for reducing IP management complexity in multi-region applications.
- **Network Load Balancer and Elastic IP:**
    - Possible but not optimal for managing a large number of load balancers.
- **Elastic IPs for Application Load Balancers:**
    - Not supported.
- **Elastic IP for Auto Scaling Group:**
- Not applicable directly to ASGs.

Question 57

A leading bank has moved its IT infrastructure to AWS Cloud and they have been using Amazon EC2 Auto Scaling for their web servers. This has helped them deal with traffic spikes effectively. But, their MySQL relational database has now become a bottleneck and they urgently need a fully managed auto scaling solution for their relational database to address any unpredictable changes in the traffic.

Can you identify the AWS service that is best suited for this use-case?

Correct Answer:

Amazon Aurora Serverless

Explanation:

1. **Amazon Aurora Serverless:**
    - **On-Demand Auto Scaling:** Automatically starts up, shuts down, and scales capacity based on application needs.
    - **Fully Managed:** No need to manage database instances.
    - **Cost-Effective:** Pay per second for the database capacity you use when the database is active.
    - **Ideal for Unpredictable Workloads:** Suitable for infrequent, intermittent, or unpredictable workloads.
    - **Simple Migration:** Easily migrate between standard and serverless configurations with a few clicks in the Amazon RDS Management Console.
2. **Incorrect Options:**
    - **Amazon DynamoDB:**
        - **NoSQL Database:** Key-value and document database, not suitable for relational database needs.
        - **High Performance:** Handles more than 10 trillion requests per day, but it's not a MySQL-compatible solution.
    - **Amazon ElastiCache:**
        - **In-Memory Data Store:** Used for caching to boost database performance.
        - **Not a Database:** Not suitable as a primary MySQL database solution.
    - **Amazon Aurora:**
        - **MySQL-Compatible Relational Database:** Built for the cloud with high performance and availability.
        - **Not Fully Auto Scaling:** Aurora itself is not a complete auto-scaling solution like Aurora Serverless.

Conclusion / Points to Memorize:

- **Amazon Aurora Serverless:**
    - Auto-scaling based on application needs.
    - Fully managed, no need to manage instances.
    - Cost-effective, pay per second when active.
    - Suitable for unpredictable workloads.
- **Amazon DynamoDB:**
    - NoSQL, not suitable for relational needs.
- **Amazon ElastiCache:**
    - In-memory cache, not a primary database.
- **Amazon Aurora:**
- High performance but not fully auto-scaling.

Question 58

A big data analytics company is working on a real-time vehicle tracking solution. The data processing workflow involves both I/O intensive and throughput intensive database workloads. The development team needs to store this real-time data in a NoSQL database hosted on an Amazon EC2 instance and needs

to support up to 25,000 IOPS per volume. As a solutions architect, which of the following Amazon Elastic Block Store (Amazon EBS) volume types would you recommend for this use-case?

Correct Answer:

Provisioned IOPS SSD (io1)

Explanation:

1. **Provisioned IOPS SSD (io1):**
   - **Designed for High Performance:** Specifically designed for I/O intensive and throughput-intensive workloads.
   - **High IOPS Support:** Capable of delivering up to 50 IOPS/GB, with a maximum of 64,000 IOPS.
   - **Consistent Performance:** Provides up to 1,000 MB/s of throughput per volume, making it suitable for critical database applications.
   - **Meets Requirement:** Can handle up to 25,000 IOPS per volume, which fits the company's needs.
2. **Incorrect Options:**
   - **General Purpose SSD (gp2):**
     - **Max IOPS:** Supports up to 16,000 IOPS/Volume.
     - **Usage:** Suitable for a broad range of transactional workloads but not sufficient for 25,000 IOPS requirement.
   - **Cold HDD (sc1):**
     - **Max IOPS:** Supports up to 250 IOPS/Volume.
     - **Usage:** Ideal for less frequently accessed, cold datasets.
     - **Not Suitable:** Insufficient IOPS for real-time vehicle tracking.
   - **Throughput Optimized HDD (st1):**
     - **Max IOPS:** Supports up to 500 IOPS/Volume.
     - **Usage:** Ideal for frequently accessed, throughput-intensive workloads like MapReduce, Kafka.
     - **Not Suitable:** Insufficient IOPS for the given requirement.

Points to Remember:

- **Provisioned IOPS SSD (io1):**
  - High performance for I/O intensive workloads.
  - Supports up to 64,000 IOPS, fitting high IOPS needs.
- **General Purpose SSD (gp2):**
  - Broad transactional workloads.
  - Max 16,000 IOPS.
- **Cold HDD (sc1):**
  - Low IOPS, cold datasets.
  - Max 250 IOPS.
- **Throughput Optimized HDD (st1):**
  - Throughput-intensive workloads.
- Max 500 IOPS.

Question 59

A global pharmaceutical company wants to move most of the on-premises data into Amazon S3, Amazon Elastic File System (Amazon EFS), and Amazon FSx for Windows File Server easily, quickly, and cost-effectively. As a solutions architect, which of the following solutions would you recommend as the BEST fit to automate and accelerate online data transfers to these AWS storage services?

Correct Answer:

Use AWS DataSync to automate and accelerate online data transfers to the given AWS storage services.

Explanation:

1. **Correct Option: Use AWS DataSync to automate and accelerate online data transfers to the given AWS storage services.**
   - **Automated Transfers:** AWS DataSync automates and accelerates copying large amounts of data to and from AWS storage services.
   - **Performance:** DataSync can transfer data up to 10 times faster than command-line tools.
   - **Seamless Integration:** Natively integrated with Amazon S3, Amazon EFS, Amazon FSx for Windows File Server, Amazon CloudWatch, and AWS CloudTrail.
   - **Scalability:** Uses a purpose-built network protocol and scale-out architecture, with a single agent capable of saturating a 10 Gbps network link.
   - **Reliability:** Includes retry mechanisms, network resiliency, built-in task scheduling, and monitoring via DataSync API and Console.

2. **Incorrect Options:**
   - **Use AWS Snowball Edge Storage Optimized device to automate and accelerate online data transfers to the given AWS storage services:**
     - **Offline Transfers:** Suitable for offline data transfers, not for automated online transfers.
     - **Use Case:** Best for bandwidth-constrained or remote environments.
   - **Use File Gateway to automate and accelerate online data transfers to the given AWS storage services:**
     - **Limited Scope:** Primarily connects on-premises applications to Amazon S3 with local caching.
     - **Compatibility:** Does not support migration into Amazon EFS and Amazon FSx for Windows File Server.
   - **Use AWS Transfer Family to automate and accelerate online data transfers to the given AWS storage services:**
     - **Limited Services:** Supports file transfers directly into and out of Amazon S3 and Amazon EFS.
     - **Compatibility:** Cannot support migration into Amazon FSx for Windows File Server.

Points to Remember:

- **AWS DataSync:**
  - Automates and accelerates data transfer.
  - Supports S3, EFS, and FSx for Windows File Server.
  - Fast and reliable, suitable for large datasets.
- **AWS Snowball Edge:**
  - Suitable for offline, large-scale data transfers.
  - Best for remote or disconnected environments.
- **File Gateway:**
  - Connects on-premises applications to S3.
  - Limited to SMB/NFS access to S3.
- **AWS Transfer Family:**
  - Manages file transfers to S3 and EFS.
  - Limited scope, does not support FSx for Windows File Server.

Conclusion:

For automated and accelerated online data transfers to Amazon S3, Amazon EFS, and Amazon FSx for Windows File Server, **AWS DataSync** is the best fit.

Question 60

A startup has recently moved their monolithic web application to AWS Cloud. The application runs on a single Amazon EC2 instance. Currently, the user base is small and the startup does not want to spend effort on elaborate disaster recovery strategies or Auto Scaling Group. The application can afford a maximum downtime of 10 minutes. In case of a failure, which of these options would you suggest as a cost-effective and automatic recovery procedure for the instance?

Correct Answer:

Configure an Amazon CloudWatch alarm that triggers the recovery of the Amazon EC2 instance, in case the instance fails. The instance, however, should only be configured with an Amazon EBS volume.

Explanation:

1. **Correct Option: Configure an Amazon CloudWatch alarm that triggers the recovery of the Amazon EC2 instance, in case the instance fails. The instance, however, should only be configured with an Amazon EBS volume.**
   - **Automatic Recovery:** Amazon CloudWatch alarm actions can automatically recover instances that fail due to system status check failures.
   - **Instance Configuration:** Only instances configured with Amazon EBS volumes can be automatically recovered. Instance store volumes are not supported.
   - **Recovery Characteristics:** Recovered instances retain the same instance ID, private IP addresses, Elastic IP addresses, and instance metadata.
   - **Reliability:** The recovery process attempts up to three times per day.
2. **Incorrect Options:**
   - **Configure Amazon EventBridge events that can trigger the recovery of the Amazon EC2 instance, in case the instance or the application fails:**
     - **Limitation:** Amazon EventBridge cannot directly trigger the recovery of EC2 instances.
   - **Configure an Amazon CloudWatch alarm that triggers the recovery of the Amazon EC2 instance, in case the instance fails. The instance can be configured with Amazon Elastic Block Store (Amazon EBS) or with instance store volumes:**
     - **Limitation:** The recovery action is only supported for instances with Amazon EBS volumes, not instance store volumes.
   - **Configure AWS Trusted Advisor to monitor the health check of Amazon EC2 instance and provide a remedial action in case an unhealthy flag is detected:**

- **Limitation:** AWS Trusted Advisor does not directly support health checks of EC2 instances or their recovery.
- **Support:** This option requires AWS Business or Enterprise Support and uses EventBridge for status changes, not direct recovery.

Points to Remember:

- **Amazon CloudWatch Alarms:**
  - Automate recovery for EC2 instances with EBS volumes.
  - Monitors system status check failures, not instance status check failures.
  - Attempts recovery up to three times per day.
- **Amazon EventBridge:**
  - Cannot directly trigger instance recovery.
  - Useful for other event-driven tasks.
- **AWS Trusted Advisor:**
  - Provides insights but not direct recovery actions.
  - Requires Business or Enterprise Support for event-based notifications.

Conclusion:

For a cost-effective and automatic recovery procedure for an EC2 instance, configuring an Amazon CloudWatch alarm to trigger recovery for instances with Amazon EBS volumes is the best fit.

Question 61:

The engineering team at a social media company wants to use Amazon CloudWatch alarms to automatically recover Amazon EC2 instances if they become impaired. The team has hired you as a solutions architect to provide subject matter expertise. As a solutions architect, which of the following statements would you identify as CORRECT regarding this automatic recovery process? (Select two)

Correct Selections:

1. **If your instance has a public IPv4 address, it retains the public IPv4 address after recovery.**
2. **A recovered instance is identical to the original instance, including the instance ID, private IP addresses, Elastic IP addresses, and all instance metadata.**

Explanation:

1. **Correct Option: If your instance has a public IPv4 address, it retains the public IPv4 address after recovery.**
   - **Public IPv4 Address Retention:** During the recovery process, the instance retains its public IPv4 address.
   - **Recovery Characteristics:** This ensures that the recovered instance is accessible using the same public IP as before the failure.
2. **Correct Option: A recovered instance is identical to the original instance, including the instance ID, private IP addresses, Elastic IP addresses, and all instance metadata.**
   - **Instance Characteristics:** After recovery, the instance maintains the same instance ID, private IP addresses, Elastic IP addresses, and metadata.
   - **Consistency:** This ensures that the instance's identity and network configuration remain consistent post-recovery.
3. **Incorrect Options:**
   - **During instance recovery, the instance is migrated during an instance reboot, and any data that is in-memory is retained.**
     - **Data Loss:** During the recovery process, any data in-memory is lost, not retained.
   - **Terminated Amazon EC2 instances can be recovered if they are configured at the launch of instance.**
     - **Irrecoverable Termination:** Terminated instances cannot be recovered.
   - **If your instance has a public IPv4 address, it does not retain the public IPv4 address after recovery.**
     - **Retention Mismatch:** Public IPv4 addresses are retained during the recovery process.

Points to Remember:

- **Amazon CloudWatch Alarms:**
  - Can automatically recover impaired EC2 instances.
  - Recovery maintains the instance's ID, private IP, Elastic IP, and metadata.
  - Does not recover terminated instances.
  - Public IPv4 addresses are retained post-recovery.
  - Data in-memory is lost during the recovery process.

Conclusion:

For automatic recovery of EC2 instances using Amazon CloudWatch alarms, the instance retains its public IPv4 address and all metadata post-recovery, ensuring minimal disruption and consistency in network configurations.

Question 62 - Incorrect

A company wants to improve its gaming application by adding a leaderboard that uses a complex proprietary algorithm based on the participating user's performance metrics to identify the top users on a real-time basis. The technical requirements mandate high elasticity, low latency, and real-time processing to deliver customizable user data for the community of users. The leaderboard would be accessed by millions of users simultaneously.

Which of the following options support the case for using Amazon ElastiCache to meet the given requirements? (Select two)

- **Use Amazon ElastiCache to improve latency and throughput for write-heavy application workloads**

Overall explanation

Correct options:

1. **Use Amazon ElastiCache to improve latency and throughput for read-heavy application workloads**
   - Amazon ElastiCache can significantly enhance latency and throughput for read-heavy workloads by storing frequently accessed data in memory, leading to faster data retrieval.
2. **Use Amazon ElastiCache to improve the performance of compute-intensive workloads**
   - ElastiCache supports Redis, which can handle advanced data structures and compute-intensive tasks efficiently, such as real-time leaderboards for gaming applications.

Incorrect options:

1. **Use Amazon ElastiCache to improve latency and throughput for write-heavy application workloads**
   - Caching is not suitable for write-heavy workloads as the cache may quickly become stale.
2. **Use Amazon ElastiCache to improve the performance of Extract-Transform-Load (ETL) workloads**
   - ETL workloads involve heavy data processing and transformations, which are better suited for AWS Glue or Amazon EMR.
3. **Use Amazon ElastiCache to run highly complex JOIN queries**
   - Complex JOIN queries are better handled by relational databases like Amazon RDS or Amazon Aurora, not by in-memory caches like ElastiCache.

Question 63

The DevOps team at an IT company is provisioning a two-tier application in a VPC with a public subnet and a private subnet. The team wants to use either a Network Address Translation (NAT) instance or a Network Address Translation (NAT) gateway in the public subnet to enable instances in the private subnet to initiate outbound IPv4 traffic to the internet but needs some technical assistance in terms of the configuration options available for the Network Address Translation (NAT) instance and the Network Address Translation (NAT) gateway.

As a solutions architect, which of the following options would you identify as CORRECT? (Select three)

Correct options:

1. **NAT instance can be used as a bastion server**
2. **Security Groups can be associated with a NAT instance**
3. **NAT instance supports port forwarding**

Explanation:

- **NAT instance can be used as a bastion server:**
  - A NAT instance can be configured to act as a bastion server.
- **Security Groups can be associated with a NAT instance:**
  - NAT instances can be associated with security groups to control inbound and outbound traffic.
- **NAT instance supports port forwarding:**
  - NAT instances can be manually configured to support port forwarding.

Incorrect options:

- **NAT gateway supports port forwarding:**
  - NAT gateways do not support port forwarding. This is a feature available with NAT instances, not gateways.
- **Security Groups can be associated with a NAT gateway:**
  - NAT gateways cannot have security groups associated directly with them. Security groups can be associated with resources behind the NAT gateway.
- **NAT gateway can be used as a bastion server:**
  - NAT gateways cannot be used as bastion servers. This functionality is supported by NAT instances.

Conclusion / Points to Memorize:

- **NAT Instances:**

- Can be used as a bastion server.
- Can have security groups associated with them.
- Support port forwarding.
- Require manual management and configuration.

- **NAT Gateways:**
  - Do not support port forwarding.
  - Cannot be associated with security groups directly.
  - Cannot be used as bastion servers.
  - Are managed services and require less maintenance compared to NAT instances.

Question 64

Your application is hosted by a provider on yourapp.provider.com. You would like to have your users access your application using www.your-domain.com, which you own and manage under Amazon Route 53. Which Amazon Route 53 record should you create?

Correct option:

- **Create a CNAME record**

Explanation:

1. **Create a CNAME record:**
   - **Purpose:** Maps DNS queries for the name of the current record to another domain or subdomain.
   - **Example:** You can create a CNAME record for www.your-domain.com that points to yourapp.provider.com.
   - **Limitation:** Cannot be created for the top node of a DNS namespace (zone apex).

Incorrect options:

1. **Create an A record:**
   - **Purpose:** Points a domain or subdomain to an IP address.
   - **Reason Incorrect:** Cannot be used to map one domain name to another.
2. **Create a PTR record:**
   - **Purpose:** Resolves an IP address to a fully-qualified domain name (FQDN), also known as Reverse DNS records.
   - **Reason Incorrect:** Cannot be used to map one domain name to another.
3. **Create an Alias Record:**
   - **Purpose:** Routes traffic to selected AWS resources (e.g., Amazon CloudFront distributions, Amazon S3 buckets).
   - **Reason Incorrect:** Cannot be used to map one domain name to another, especially for third-party websites which are not under AWS control.

Conclusion / Points to Memorize:

- **CNAME Records:**
  - Used to map one domain name to another.
  - Cannot be created for the zone apex.
- **A Records:**
  - Used to point domains or subdomains to IP addresses.
  - Not suitable for mapping domain names.
- **PTR Records:**
  - Used for Reverse DNS lookups.
  - Not suitable for mapping domain names.
- **Alias Records:**
  - Used for routing traffic to AWS resources.
  - Not suitable for third-party domain mapping.

Question 65

The business analytics team at a company has been running ad-hoc queries on Oracle and PostgreSQL services on Amazon RDS to prepare daily reports for senior management. To facilitate the business analytics reporting, the engineering team now wants to continuously replicate this data and consolidate these databases into a petabyte-scale data warehouse by streaming data to Amazon Redshift. As a solutions architect, which of the following would you recommend as the MOST resource-efficient solution that requires the LEAST amount of development time without the need to manage the underlying infrastructure?

Correct option:

- **Use AWS Database Migration Service (AWS DMS) to replicate the data from the databases into Amazon Redshift**

Explanation:

1. **Use AWS Database Migration Service (AWS DMS) to replicate the data from the databases into Amazon Redshift:**
   - **Functionality:** AWS DMS helps you migrate databases to AWS quickly and securely while the source database remains fully operational.
   - **Advantages:**
     - Minimizes downtime during migration.
     - Supports continuous data replication with high availability.
     - Consolidates databases into a petabyte-scale data warehouse like Amazon Redshift.
     - No need to manage the underlying infrastructure.
   - **Process:** During migration, data is first moved to an Amazon S3 bucket and then transferred to Amazon Redshift tables.
   - **Requirement:** The Amazon Redshift cluster must be in the same AWS account and region as the replication instance.

Incorrect options:

1. **Use AWS Glue to replicate the data from the databases into Amazon Redshift:**
   - **Functionality:** AWS Glue is a fully managed ETL (Extract, Transform, Load) service.
   - **Disadvantages:**
     - Requires significant development efforts to write custom migration scripts.
     - Primarily designed for batch ETL data processing, not continuous replication.
2. **Use Amazon EMR to replicate the data from the databases into Amazon Redshift:**
   - **Functionality:** Amazon EMR is a big data platform for processing large amounts of data using open-source tools.
   - **Disadvantages:**
     - Involves significant infrastructure management to set up and maintain the EMR cluster.
     - Requires major development effort to write custom migration jobs.
3. **Use Amazon Kinesis Data Streams to replicate the data from the databases into Amazon Redshift:**
   - **Functionality:** Amazon Kinesis Data Streams is a real-time data streaming service.
   - **Disadvantages:**
     - Requires manual provisioning of an appropriate number of shards to handle the data stream.
     - Not ideal for continuous database replication for this use-case.

Conclusion / Points to Memorize:

- **AWS DMS:**
  - Best for quick, secure database migration with minimal downtime.
  - Supports continuous data replication to Amazon Redshift.
  - Automates data transfer, reducing development and management efforts.
- **AWS Glue:**
  - Suitable for ETL jobs but requires significant custom development for migration.
- **Amazon EMR:**
  - Ideal for big data processing but involves high infrastructure management and custom development.
- **Amazon Kinesis Data Streams:**
  - Effective for real-time data streaming but requires manual shard management and is not optimal for continuous database replication.