Short Notes on individual topics + Questions:

Question 1Incorrect

A big data analytics company is using Amazon Kinesis Data Streams (KDS) to process IoT data from the field devices of an agricultural sciences company. Multiple consumer applications are using the incoming data streams and the engineers have noticed a performance lag for the data delivery speed between producers and consumers of the data streams.

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

Correct answer

Use Enhanced Fanout feature of Amazon Kinesis Data Streams

Short Notes on Amazon Kinesis Data Streams (KDS) and Amazon SQS

Amazon Kinesis Data Streams (KDS)

1. **Overview**: KDS is a scalable and durable real-time data streaming service that captures gigabytes of data per second from multiple sources like website clickstreams, IT logs, social media feeds, etc.
2. **Sharding**: Uses shards to scale, each shard providing an ingest capacity of 1MB/sec and an output capacity of 2MB/sec. Shards can be increased to handle more data.
3. **Enhanced Fan-Out**: Key feature for scenarios with multiple consumers. It allocates a dedicated 2MB/sec throughput per shard per consumer, enhancing data delivery speed. This feature auto-scales with the number of shards, ensuring parallel data retrieval without bottlenecks.
4. **Use Cases**:
   - Suitable for applications needing to process data in the same order, e.g., billing systems.
   - Ideal when multiple applications consume the same data stream independently.

Amazon Simple Queue Service (SQS)

1. **Overview**: Fully managed message queuing service that helps decouple components of a large application.
2. **Queue Types**:
   - **Standard Queues**: Offers maximum throughput, best-effort ordering, and at-least-once delivery.
   - **FIFO Queues**: Ensures messages are processed exactly once and keeps the order they are sent.
3. **Use Cases**:
   - Suitable for individual message delay needs, dynamic concurrency adjustments, and tasks requiring message-level acknowledgment.
   - Not recommended for use cases requiring high throughput data streaming like KDS.

Comparison and Selection for a Use Case

1. **Performance Issue**: For a big data analytics company experiencing lag due to multiple consumers accessing IoT data from agricultural devices, the correct choice is:
   - **Use Enhanced Fan-Out in KDS**: This feature separates the data throughput for each consumer, preventing shared throughput issues and ensuring faster data processing without altering the existing data stream setup.
2. **Why Not SQS or Kinesis Data Firehose**:
   - **SQS**: More suited for decoupling individual components of an application, not efficient for high throughput data streams consumed by multiple applications.
   - **Kinesis Data Firehose**: Designed for straightforward data loading into storage and analytics tools, without the capability for real-time consumption by multiple applications.

Question 2Incorrect

A retail company has developed a REST API which is deployed in an Auto Scaling group behind an Application Load Balancer. The REST API stores the user data in Amazon DynamoDB and any static content, such as images, are served via Amazon Simple Storage Service (Amazon S3). On analyzing the usage trends, it is found that 90% of the read requests are for commonly accessed data across all users. As a Solutions Architect, which of the following would you suggest as the MOST efficient solution to improve the application performance?

Correct answer

Enable Amazon DynamoDB Accelerator (DAX) for Amazon DynamoDB and Amazon
CloudFront for Amazon S3

Amazon DynamoDB Accelerator (DAX)

1. **Overview**: DAX is a fully managed, in-memory cache for Amazon DynamoDB that dramatically speeds up read operations by caching frequently accessed data.
2. **Performance Improvement**: Delivers up to 10 times the performance, reducing response times from milliseconds to microseconds, even under heavy load with millions of requests per second.
3. **Integration**: Seamlessly integrates with DynamoDB. Uses the DAX client SDK for existing DynamoDB API calls, requiring minimal code changes for integration.
4. **Use Cases**: Ideal for applications requiring ultra-fast read access to hot data, such as user profile information in web applications.

Amazon CloudFront

1. **Overview**: A content delivery network (CDN) that speeds up the delivery of static and dynamic content, such as images, videos, and API calls, using globally distributed servers.
2. **Efficiency**: More cost-effective than serving directly from S3, especially for geographically dispersed users.
3. **Operation**: Routes user requests to the nearest edge location to serve cached content. Retrieves content from the origin (e.g., S3 bucket) if not in cache, reducing latency and improving user experience.
4. **Use Cases**: Best for static content delivery, reducing load times for images, scripts, stylesheets, and other assets crucial for fast loading of internet applications.

Best Practices and Selection for Improving Application Performance

1. **Problem Scenario**: A retail company's REST API, heavily dependent on read operations for commonly accessed data, is experiencing performance bottlenecks.
2. **Solution**:
   - **Enable DAX for DynamoDB**: To cache common read requests, significantly speeding up data retrieval and reducing load on the database.
   - **Use Amazon CloudFront for S3**: To serve static content like images more efficiently, leveraging the CDN to reduce latency and bandwidth costs.

Incorrect Options Analysis

1. **Using ElastiCache with DynamoDB and S3**:
   - **ElastiCache Redis/Memcached for DynamoDB**: While Redis can theoretically enhance DynamoDB when custom caching layers are needed, DAX provides a direct, simpler, and more integrated solution with automatic handling.
   - **ElastiCache for S3 Content**: Neither Redis nor Memcached is suitable for caching S3 static content as they are not designed to integrate directly with S3 for content delivery purposes.

Exam Alert

- **Understand tool-specific integrations**: Knowing how DAX and CloudFront directly integrate with DynamoDB and S3 respectively is crucial, as these tools are designed to enhance performance with minimal changes to existing setups.
  - **Recognize inappropriate solutions**: ElastiCache (Redis or Memcached) is not typically used for direct integration with DynamoDB for caching or with S3 for content delivery. These use cases are better served by DAX and CloudFront, respectively.

Question 3Incorrect

An IT company has built a custom data warehousing solution for a retail organization by using Amazon Redshift. As part of the cost optimizations, the company wants to move any historical data (any data older than a year) into Amazon S3, as the daily analytical reports consume data for just the last one year. However the analysts want to retain the ability to cross-reference this historical data along with the daily reports. The company wants to develop a solution with the LEAST amount of effort and MINIMUM cost. As a solutions architect, which option would you recommend to facilitate this usecase?

Use the Amazon Redshift COPY command to load the Amazon S3 based historical data into Amazon Redshift. Once the ad-hoc queries are run for the historic data, it can be removed from Amazon Redshift

Your answer is incorrect

Correct answer

Use Amazon Redshift Spectrum to create Amazon Redshift cluster tables pointing to the underlying historical data in Amazon S3. The analytics team can then query this historical data to cross-reference with the daily reports from Redshift.

Amazon Redshift Spectrum

1. **Overview**: Redshift Spectrum allows you to use Amazon Redshift to directly query and join data that is stored in S3, extending Redshift's data warehousing capabilities to exabytes of data.
2. **Functionality**: Provides the ability to run queries on S3 data without loading or duplicating the existing data into Redshift. It uses standard SQL for querying.
3. **Efficiency**: Utilizes Redshift's massive parallel processing to execute complex queries quickly, while pushing many compute-intensive tasks down to the Redshift Spectrum layer.
4. **Cost-Effectiveness**: Since the data remains in S3 and is queried directly, there are no storage costs in Redshift for this data, only for the compute resources used during querying.
5. **Integration**: Works with existing Redshift queries. You can create external tables that point to S3 data, and these tables appear as normal Redshift tables to your SQL queries.

Scenario Application

1. **Problem Scenario**: A retail organization needs to move historical data older than a year to S3 due to cost concerns but still requires access to this data for analysis alongside current data.
2. **Solution**: Using Redshift Spectrum to query historical data stored in S3 directly. This setup allows combining historical S3 data with more recent data stored in Redshift without additional data movement or transformation, thus saving costs and effort.

Incorrect Options Analysis

1. **Amazon Athena**: While Athena is excellent for ad-hoc querying of S3 data, it would require exporting results to combine with Redshift data, complicating daily operations.
2. **Redshift COPY Command**: Loading data back and forth between S3 and Redshift for temporary queries is inefficient and costly due to the data transfer and storage overhead.
3. **AWS Glue ETL**: Similarly, using Glue for periodic ETL tasks to load data into Redshift is more resource-intensive and costly compared to querying in place with Spectrum.

Exam Alert

- **Understanding Tool Fit**: It's crucial to understand the best scenarios for using Redshift Spectrum versus other data querying methods. Redshift Spectrum is particularly effective when you need to maintain a seamless querying layer over archived data in S3 and live data in Redshift.
- **Cost and Performance Optimization**: Know how Redshift Spectrum can reduce costs by querying data where it resides (in S3), without unnecessary data loading or duplication, leveraging the scalability and power of Redshift for compute-intensive tasks.

Question 4Correct

A cyber security company is running a mission critical application using a single Spread placement group of Amazon EC2 instances. The company needs 15 Amazon EC2 instances for optimal performance.

How many Availability Zones (AZs) will the company need to deploy these Amazon EC2
instances per the given use-case?

14

7

15

Your answer is correct

3

Amazon EC2 Spread Placement Groups

1. **Overview**: Spread placement groups ensure that instances are placed on distinct physical hardware (separate racks) with dedicated network and power sources for each instance. This setup minimizes the risk of simultaneous failures affecting all instances.
2. **Limitations**: Each spread placement group can have a maximum of seven running instances per Availability Zone (AZ).
3. **Multiple AZs**: Spread placement groups can span multiple AZs within the same region, allowing for broader distribution of instances across physical locations.

Scenario Application

1. **Problem Scenario**: A cyber security company requires 15 Amazon EC2 instances to run a mission-critical application and wants to minimize the risk of correlated failures.
2. **Solution**: Utilize three Availability Zones, placing up to seven instances in each AZ but only using three in one of them, thereby deploying all 15 instances within a single spread placement group across these AZs.
3. **Purpose**: This configuration provides high availability and fault tolerance by ensuring no single point of hardware failure can impact more than a few instances.

Calculation and Configuration

1. **Instance Distribution**: Since each AZ can support a maximum of seven instances in a spread placement group, the 15 instances must be distributed as follows:
   - AZ 1: 7 instances
   - AZ 2: 7 instances
   - AZ 3: 1 instance
2. **Selection Rationale**: Choosing three AZs allows the company to fully utilize the capacity of a spread placement group while adhering to its limitations.

Exam Alert

- **Understanding Limits and Capabilities**: It's essential to know the specific limitations of different placement strategies in EC2, such as the maximum number of instances per AZ in a spread placement group, to plan infrastructure that meets both performance and reliability requirements effectively.
  - **Strategic Use of AZs**: For setups requiring more instances than a single AZ can support in a spread placement group, expanding to multiple AZs is necessary. This approach ensures better fault tolerance and availability, aligning with best practices for mission-critical applications.

Question 5Correct
A pharmaceutical company is considering moving to AWS Cloud to accelerate the research and development process. Most of the daily workflows would be centered around running batch jobs on Amazon EC2 instances with storage on Amazon Elastic Block Store (Amazon EBS) volumes. The CTO is concerned about meeting HIPAA compliance norms for sensitive data stored on Amazon EBS.
Which of the following options outline the correct capabilities of an encrypted Amazon EBS
volume? (Select three)
Data at rest inside the volume is NOT encrypted
Your selection is correct
Data at rest inside the volume is encrypted
Your selection is correct
Any snapshot created from the volume is encrypted
Data moving between the volume and the instance is NOT encrypted
Your selection is correct
Data moving between the volume and the instance is encrypted
Any snapshot created from the volume is NOT encrypted

Amazon EBS Encryption

1. **Overview**: Amazon Elastic Block Store (EBS) provides block-level storage volumes for Amazon EC2 instances. EBS encryption is a method to secure your data to meet compliance and security requirements.
2. **Data at Rest**: Data stored on an encrypted EBS volume is automatically encrypted. This includes all data, snapshots created from the volume, and any new volumes created from these snapshots.
3. **Data in Transit**: Data moving between the EC2 instance and the EBS volume is encrypted. This ensures that the data is secure not only when it is stored but also when it is being transmitted.
4. **Snapshot Encryption**: Snapshots taken from an encrypted EBS volume inherit the same encryption status, ensuring that any data captured as a snapshot remains secure.
5. **Key Management**: Encryption and decryption are managed transparently using AWS Key Management Service (AWS KMS), and involve no additional overhead for the user.

Scenario Application

1. **Problem Scenario**: A pharmaceutical company is considering migrating to AWS to utilize EC2 and EBS for research and development but needs to ensure that their data handling complies with HIPAA regulations for sensitive data.
2. **Solution**: Utilize encrypted EBS volumes to ensure that all data at rest and in transit meets HIPAA compliance standards. This encryption extends to snapshots, enhancing data security across the board.

HIPAA Compliance

- **Data Security Measures**: Encryption of EBS volumes addresses several HIPAA requirements for protecting patient information, ensuring that data is unreadable to unauthorized users.
- **Compliance Across Data Lifecycle**: From the moment data is written to an EBS volume to when it is archived in the form of snapshots, encryption maintains the confidentiality and integrity of sensitive information.

Exam Alert

Understanding EBS Encryption: Knowing the capabilities of EBS encryption is crucial for scenarios involving sensitive data to ensure compliance with legal and regulatory requirements.

Security Best Practices: It is a best practice to enable encryption for all EBS volumes and snapshots when handling sensitive or regulated data to prevent data breaches and unauthorized access.

Question 6Incorrect
A retail company uses Amazon Elastic Compute Cloud (Amazon EC2) instances, Amazon API Gateway, Amazon RDS, Elastic Load Balancer and Amazon CloudFront services. To improve the security of these services, the Risk Advisory group has suggested a feasibility check for using the Amazon GuardDuty service. Which of the following would you identify as data sources supported by Amazon GuardDuty?
Elastic Load Balancing logs, Domain Name System (DNS) logs, AWS CloudTrail events
Amazon CloudFront logs, Amazon API Gateway logs, AWS CloudTrail events
Correct answer
VPC Flow Logs, Domain Name System (DNS) logs, AWS CloudTrail events

Your answer is incorrect
VPC Flow Logs, Amazon API Gateway logs, Amazon S3 access logs
Overall explanation
Correct option:
VPC Flow Logs, Domain Name System (DNS) logs, AWS CloudTrail events

Amazon GuardDuty Overview

1. **Overview**: Amazon GuardDuty is a threat detection service that provides continuous monitoring of your AWS environment to detect malicious or unauthorized activity.
2. **Functionality**: It leverages machine learning, anomaly detection, and integrated threat intelligence to automatically identify and prioritize potential threats without requiring additional hardware or manual intervention.

Key Features of Amazon GuardDuty

1. **Data Sources**:
    - **AWS CloudTrail Events**: Monitors and analyzes API calls and other related events within AWS to detect unusual or unauthorized activities.
    - **VPC Flow Logs**: Analyzes Virtual Private Cloud (VPC) flow logs for unusual network traffic patterns or volumes that may indicate a security threat.
    - **DNS Logs**: Reviews DNS logs to detect malicious domains and other suspicious DNS activities.
2. **Integration**: Easily integrates with Amazon EventBridge, which allows for automated responses and easier management of security incidents across multiple AWS accounts.

Scenario Application

1. **Problem Scenario**: A retail company is exploring enhanced security measures for its EC2 instances, API Gateway, RDS, Elastic Load Balancer, and CloudFront services.
2. **Solution**: Implementing GuardDuty to monitor and analyze signs of potential security threats across these services using supported logs and events.

Deployment and Management

1. **Ease of Use**: GuardDuty can be activated with a few clicks in the AWS Management Console, requiring no additional software installations.
2. **Continuous Security Monitoring**: Once enabled, it continually scans the configured data sources, applying its detection algorithms to identify potential threats.

Exam Alert

- **Understanding GuardDuty's Capabilities**: It's important to know what data sources GuardDuty can analyze. Remember, it does not directly analyze logs from services like Amazon API Gateway or Amazon CloudFront.
- **Security Best Practices**: Utilizing GuardDuty can significantly enhance the security posture of an AWS environment by providing proactive threat detection and response capabilities. Always consider integrating it into your security strategy, especially for environments handling sensitive data or complex infrastructures.

Question 7Correct
A media company wants to get out of the business of owning and maintaining its own IT infrastructure. As part of this digital transformation, the media company wants to archive about 5 petabytes of data in its on-premises data center to durable long term storage.
As a solutions architect, what is your recommendation to migrate this data in the MOST cost-optimal way?Transfer the on-premises data into multiple AWS Snowball Edge Storage Optimized
devices. Copy the AWS Snowball Edge data into Amazon S3 and create a lifecycle policy to transition the data into Amazon S3 Glacier
Setup AWS Site-to-Site VPN connection between the on-premises data center and AWS Cloud. Use this connection to transfer the data into Amazon S3 Glacier
Correct option:
Transfer the on-premises data into multiple AWS Snowball Edge Storage Optimized devices. Copy the AWS Snowball Edge data into Amazon S3 and create a lifecycle policy to transition the data into Amazon S3 Glacier

AWS Snowball Edge Storage Optimized

1. **Overview**: AWS Snowball Edge Storage Optimized devices are physical devices used to securely and efficiently transfer large amounts of data into and out of AWS.
2. **Capacity**: Each device provides up to 80 TB of usable HDD storage along with 1 TB of SATA SSD storage for faster data access.
3. **Features**: Equipped with 40 vCPUs and up to 40 Gb network connectivity, these devices are well-suited for data transfer and basic processing tasks.

Amazon S3 Glacier

1. **Overview**: Amazon S3 Glacier is a secure, durable, and extremely low-cost storage service for data archiving and long-term backup.
2. **Cost-effectiveness**: Particularly cost-effective for data that is infrequently accessed and requires long retention periods.

Recommended Migration Strategy

1. **Migration Process**:
   - **Step 1**: Transfer data from on-premises data centers to AWS using AWS Snowball Edge Storage Optimized devices. This step bypasses internet bandwidth limitations and provides a secure method of data transfer.
   - **Step 2**: Once the data is uploaded to AWS via Snowball, it should first be stored in Amazon S3.
   - **Step 3**: Implement a lifecycle policy in Amazon S3 to automatically transition this data to Amazon S3 Glacier for cost-effective long-term storage.

Advantages of Using Snowball Edge for Data Migration

1. **Speed and Security**: Provides a faster, more secure alternative to online data transfer methods, especially beneficial for transferring petabytes of data.
2. **Reduced Complexity**: Simplifies the logistics of large-scale data migrations, reducing the need for expensive network upgrades or extended transfer times over the internet.

Incorrect Options Analysis

1. **Direct Transfer to Glacier via Snowball Edge**: Not supported directly. Data must be moved to S3 before transitioning to Glacier.
2. **AWS Direct Connect**: Involves significant setup time and costs, making it less suitable for a one-time, large-scale data transfer.
3. **AWS Site-to-Site VPN**: Not feasible for transferring petabytes of data due to bandwidth limitations.

Exam Alert

- **Understanding AWS Data Transfer Solutions**: It's crucial to understand the appropriate AWS services and methods for data transfer scenarios, especially when dealing with large datasets and specific compliance or cost considerations.
  - **Selecting the Right Tools**: Choose Snowball Edge for its ability to handle large data volumes efficiently and its integration with S3 and Glacier, which supports seamless data lifecycle management.

Question 8Incorrect
An e-commerce company has copied 1 petabyte of data from its on-premises data center to an Amazon S3 bucket in the us-west-1 Region using an AWS Direct Connect link. The company now wants to set up a one-time copy of the data to another Amazon S3 bucket in the us-east-1 Region. The on-premises data center does not allow the use of AWS Snowball. As a Solutions Architect, which of the following options can be used to accomplish this goal? (Select two)
Your selection is correct
Set up Amazon S3 batch replication to copy objects across Amazon S3 buckets in another Region using S3 console and then delete the replication configuration
Overall explanation
Correct options:
Copy data from the source bucket to the destination bucket using the aws S3 sync Command

Short Notes on Data Transfer Options for Amazon S3

Amazon S3 Sync Command

1. **Overview**: The aws s3 sync command is used to synchronize the contents of one S3 bucket with another. This command is ideal for copying large volumes of data across S3 buckets, even across regions.
2. **Functionality**: It compares the source and destination buckets and copies only the objects that are new or have been updated in the source bucket since the last sync. This command is efficient as it avoids redundant data transfer.
3. **Use Case**: Suitable for one-time or periodic updates between buckets, especially useful in scenarios like the one described, where a large data set needs to be replicated across regions.

Amazon S3 Batch Replication

1. **Overview**: S3 Batch Replication is a feature that enables the replication of existing objects within an S3 bucket to another bucket, which can be in the same or a different region.
2. **Batch Operations**: This process involves creating a Batch Operations job that can handle the replication of objects that existed before the replication configuration was set up.
3. **Replication Configuration**: It's typically used for one-time or infrequent replication tasks. Once replication needs are met, the configuration can be deleted to prevent further unintended replications.

Incorrect Options and Clarifications

1. **AWS Snowball Edge**: Not suitable for region-to-region data transfers within AWS. Snowball is primarily for transferring data into and out of AWS from on-premises locations.
2. **S3 Console for Large Data Volumes**: The S3 management console is not practical for copying very large data sets like 1 petabyte due to interface limitations and potential for errors. It's better suited for smaller, more manageable data volumes.

3. **Amazon S3 Transfer Acceleration (S3TA)**: Designed to speed up the transfer of files to S3 over long distances by routing traffic through Amazon CloudFront's network. It does not facilitate copying data between S3 buckets across regions.

Exam Alert

- **Choosing the Right Tool for the Job**: Understanding the capabilities and limitations of each S3 data handling tool is crucial. For large-scale data transfers across regions, aws s3 sync and S3 Batch Replication are appropriate, whereas tools like S3TA and the S3 console have specific use cases.

• **Efficiency and Cost Considerations**: For large data volumes, always consider the efficiency of the transfer method in terms of both time and cost. Methods that reduce redundant data transfer and leverage existing AWS infrastructure efficiently are preferable.

Question 9Correct
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?
Use Auto Scaling group to provide a low latency way to distribute live sports results
Use Elastic Load Balancing (ELB) to provide a low latency way to distribute live sports results
Use Amazon CloudFront to provide a low latency way to distribute live sports results
Your answer is correct
Use AWS Global Accelerator to provide a low latency way to distribute live sports results

AWS Global Accelerator Overview

1. **Overview**: AWS Global Accelerator is a service designed to optimize the path of internet traffic from end users to applications hosted in AWS, improving performance and availability.
2. **Functionality**: Provides fixed entry points to your applications through static IP addresses associated with the accelerator, routing traffic to the nearest optimal endpoint based on health and geographic proximity.

Key Features of AWS Global Accelerator

1. **Traffic Routing**: Dynamically routes user traffic to the nearest healthy endpoint, reducing latency and improving the overall user experience.
2. **Protocol Support**: Unlike many AWS services that focus primarily on HTTP/S, Global Accelerator supports both TCP and UDP traffic, making it ideal for a variety of applications, including those that require constant and fast data exchange like live sports results.
3. **Health Checks**: Regularly checks the health of the application endpoints and reroutes traffic to healthy endpoints in case of any issues, ensuring high availability.

Scenario Application

1. **Problem Scenario**: A media company needs a low-latency solution to distribute live sports results, which are delivered via a proprietary application using UDP protocol.
2. **Solution**: Implementing AWS Global Accelerator to handle the traffic will ensure that data packets are directed efficiently through AWS's vast global network, optimizing the path for the lowest latency possible.

Benefits Over Other Solutions

1. **Comparison with ELB and Auto Scaling**: Elastic Load Balancing and Auto Scaling are great for distributing and scaling traffic within AWS environments but do not inherently reduce latency of traffic entering AWS from various global points.
2. **Comparison with Amazon CloudFront**: While CloudFront is effective for cacheable content like images and videos, it is primarily geared towards HTTP/S traffic. Global Accelerator is more suited for real-time, non-cacheable UDP traffic like live sports data.

Exam Alert

- **Understanding Different AWS Services**: Knowing when to use AWS Global Accelerator versus other services like Amazon CloudFront or Elastic Load Balancing is crucial. Global Accelerator is particularly beneficial for applications requiring minimized latency with non-HTTP traffic across global locations.

• **Service Selection for Specific Needs**: Choose Global Accelerator for applications that benefit from steady, low-latency connections and support for protocols beyond HTTP/S, such as UDP needed for live broadcasts or interactive real-time applications

Question 10Incorrect
The engineering team at an e-commerce company has been tasked with migrating to a serverless architecture. The team wants to focus on the key points of consideration when using AWS Lambda as a backbone for this architecture. As a Solutions Architect, which of the following options would you identify as correct for the given requirement? (Select three)
The bigger your deployment package, the slower your AWS Lambda function will cold-start. Hence, AWS suggests packaging dependencies as a separate package from the actual AWS Lambda package
Correct selection
By default, AWS Lambda functions always operate from an AWS-owned VPC and hence have access to any public internet address or public AWS APIs. Once an AWS Lambda function is VPC-enabled, it will need a route through a Network Address Translation gateway (NAT gateway) in a public subnet to access public resources
Correct options:

By default, AWS Lambda functions always operate from an AWS-owned VPC and hence have access to any public internet address or public AWS APIs. Once an AWS Lambda function is VPC-enabled, it will need a route through a Network Address Translation gateway (NAT gateway) in a public subnet to access public resources

Short Notes on AWS Lambda VPC Integration and Best Practices

AWS Lambda VPC Integration

1. **Overview**: AWS Lambda functions typically operate within an AWS-managed VPC but can be configured to access resources within a customer's VPC.
2. **Functionality**: By enabling VPC access for a Lambda function, it can interact with resources that are isolated within a private subnet of a customer VPC, such as an Amazon RDS instance or an internal microservices endpoint.

Key Considerations for VPC-Enabled Lambda Functions

1. **Network Configuration**: When Lambda functions are configured to access resources within a VPC, network setup must include proper routing. For Lambda functions to access the internet (and public AWS services), a NAT Gateway in a public subnet is necessary.
2. **Performance Implications**: Configuring Lambda with VPC access may add some initial latency (cold start time), particularly if the networking setup is complex or improperly configured.

Correct Options for Lambda Function Best Practices

1. **Monitoring with CloudWatch Alarms**: Given the scalability of AWS Lambda, it's crucial to monitor function metrics like ConcurrentExecutions or Invocations to manage unexpected spikes and understand the application behavior under different loads.
2. **Reusable Code with Lambda Layers**: For code that needs to be shared across multiple Lambda functions, using Lambda Layers is highly recommended. This allows for cleaner management of shared dependencies and can reduce the size of the deployment package.
3. **Deployment Package Management**: Although not explicitly correct in this instance, generally keeping the deployment package size minimal is suggested for reducing cold start times. This typically involves efficient dependency management and possibly using Lambda Layers to separate the core logic from larger dependencies.

Incorrect Options and Clarifications

1. **Over Provisioning Timeouts**: Over provisioning function timeout settings can lead to higher costs and is not a recommended practice. It's better to understand the function's performance characteristics and set timeouts based on actual needs rather than arbitrary higher limits.
2. **Serverless and Containers**: Modern AWS services do allow Lambda functions to be packaged and deployed as container images, which gives users flexibility in how they manage their serverless applications and integrate them with container-based workflows.

Exam Alert

- **Understanding Lambda and VPC**: When preparing for AWS certifications or designing architectures, it's crucial to understand when and how to enable VPC integration for Lambda functions.
- **Best Practices for Performance and Cost Management**: Employ best practices like monitoring with CloudWatch, using Lambda Layers for code reusability, and proper timeout settings to optimize both performance and cost.
- **Modern Capabilities of Lambda**: Be aware of the latest capabilities of AWS Lambda, including its support for container image deployments, which can be crucial for certain application requirements and integration scenarios.

Question 11Incorrect
Your company is deploying a website running on AWS Elastic Beanstalk. The website takes over 45 minutes for the installation and contains both static as well as dynamic files that must be generated during the installation process. As a Solutions Architect, you would like to bring the time to create a new instance in your AWS Elastic Beanstalk deployment to be less than 2 minutes. Which of the following options should be combined to build a solution for this requirement? (Select two)
Use AWS Elastic Beanstalk deployment caching feature Store the installation files in Amazon S3 so they can be quickly retrieved Your selection is correct Create a Golden Amazon Machine Image (AMI) with the static installation components already setup Your selection is incorrect Use Amazon EC2 user data to install the application at boot time
Correct selection
Use Amazon EC2 user data to customize the dynamic installation parts at boot time Overall explanation
Correct options:
AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS.

Overview of AWS Elastic Beanstalk

1. **Functionality**: AWS Elastic Beanstalk is a service for deploying and scaling web applications using a variety of programming languages and servers. It manages deployment details such as capacity provisioning, load balancing, auto-scaling, and application health monitoring.
2. **Control and Accessibility**: While Elastic Beanstalk manages many aspects of the application deployment, developers still maintain full control over the AWS resources used by the application and can access these resources as needed.

Recommended Solutions for Reducing Instance Creation Time

1. **Create a Golden Amazon Machine Image (AMI)**:
   - **Purpose**: Using a Golden AMI allows you to pre-install all static components of your application, which can significantly reduce the time required to provision new instances.
   - **Benefits**: By having a standard configuration that includes security patches, software installations, and performance monitoring agents, you ensure that new instances start with a consistent baseline, minimizing the need for additional configuration and setup.
2. **Use Amazon EC2 User Data for Dynamic Installation Parts**:
   - **Purpose**: EC2 user data scripts are executed when an instance is launched for the first time. These scripts are ideal for customizing dynamic aspects of the installation that cannot be pre-configured in a Golden AMI.
   - **Benefits**: Allows for the dynamic configuration of instances based on current conditions or specific deployment requirements without increasing the base provisioning time of new instances.

Incorrect Options and Explanations

1. **Store Installation Files in Amazon S3**: While S3 is useful for storing application source code and logs, it is not suitable for directly handling installations or generating dynamic content due to its nature as a static storage service.
2. **Install Application at Boot Time Using User Data**: This method is impractical for applications like the one described, which take significant time to install. Using user data for lengthy installation processes could lead to slow startup times and decreased responsiveness during scaling events.
3. **Elastic Beanstalk Deployment Caching**: This is a fictitious feature and does not exist within the AWS Elastic Beanstalk service offerings.

Exam Alert

- **Understanding Deployment Optimization**: When preparing for AWS certifications or designing architectures, it's crucial to understand how to optimize deployments for performance and scalability. This involves selecting the right strategies for instance provisioning and configuration.
- **Selecting Appropriate AWS Tools**: Knowing when to use tools like Golden AMIs and EC2 user data scripts can significantly impact the efficiency and performance of AWS deployments, particularly in managed environments like Elastic Beanstalk

Question 12Correct

A leading social media analytics company is contemplating moving its dockerized application stack into AWS Cloud. The company is not sure about the pricing for using Amazon Elastic Container Service (Amazon ECS) with the EC2 launch type compared to the

Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type. Which of the following is correct regarding the pricing for these two services?

Both Amazon ECS with EC2 launch type and Amazon ECS with Fargate launch type are charged based on Amazon EC2 instances and Amazon EBS Elastic Volumes used

Both Amazon ECS with EC2 launch type and Amazon ECS with Fargate launch type are charged based on vCPU and memory resources that the containerized application requests

Both Amazon ECS with EC2 launch type and Amazon ECS with Fargate launch type are just charged based on Elastic Container Service used per hour

Your answer is correct

Amazon ECS with EC2 launch type is charged based on EC2 instances and EBS volumes used. Amazon ECS with Fargate launch type is charged based on vCPU and memory resources that the containerized application requests

Correct option:

Amazon ECS with EC2 launch type is charged based on EC2 instances and EBS volumes used. Amazon ECS with Fargate launch type is charged based on vCPU and memory resources that the containerized application requests

Short Notes on Pricing for Amazon ECS with EC2 and Fargate Launch Types

Amazon ECS Overview

1. **Functionality**: Amazon Elastic Container Service (ECS) is a fully managed container orchestration service that supports Docker containers and allows you to easily run and scale containerized applications on AWS.

Pricing Models for ECS Launch Types

1. **ECS with EC2 Launch Type**:
   - **Pricing**: Costs are based on the AWS resources that you consume, including the EC2 instances and optionally, EBS volumes you use to run and store your applications. This means you are responsible for managing the underlying server instances and the scaling of the containers.
   - **Use Case**: Suitable for scenarios where you need control over the instance types and configurations used by your containers.
2. **ECS with Fargate Launch Type**:
   - **Pricing**: Charged based on the amount of compute (vCPU) and memory resources that your containerized applications use. With Fargate, pricing is clear and straightforward as you pay only for the resources allocated to your containers without needing to manage the underlying server instances.
   - **Use Case**: Ideal for users who want a serverless experience, focusing solely on application development without the overhead of managing servers or clusters.

Key Differences in Pricing Approach

- **EC2 Launch Type**: The cost depends on the choice of EC2 instances and EBS volumes. This model gives more flexibility and potential cost savings if managed efficiently but requires more administrative oversight.
- **Fargate Launch Type**: Simplifies deployment by charging for compute and memory resources used by the container, abstracting away the server and cluster management. This can be more cost-effective for predictable workloads but potentially more expensive for sporadic or small-scale deployments.

Exam Alert

- **Understanding ECS Pricing**: Knowing the distinct pricing models for ECS's two launch types is crucial for planning and managing costs in containerized environments.
- **Selecting the Right Launch Type**: For exams and practical implementations, assess whether the control and potential cost optimization of EC2 launch type outweigh the simplicity and predictability of costs with the Fargate launch type

Question 13Correct
A Big Data processing company has created a distributed data processing framework that performs best if the network performance between the processing machines is high. The application has to be deployed on AWS, and the company is only looking at performance as the key measure. As a Solutions Architect, which deployment do you recommend?
Optimize the Amazon EC2 kernel using EC2 User Data
Use Spot Instances
Use a Spread placement group
Your answer is correct
Use a Cluster placement group

Recommended AWS EC2 Placement Strategy for High-Performance Data Processing

Understanding AWS EC2 Placement Groups

1. **Cluster Placement Group**:
   - **Definition**: A cluster placement group is a logical grouping of instances within a single Availability Zone (AZ). This configuration ensures that instances are physically located close to each other, reducing the network latency and increasing the network throughput.
   - **Use Case**: Ideal for high-performance computing (HPC) applications, big data processing frameworks, and other applications where low network latency and high network throughput are critical.
2. **Partition Placement Group**:
   - **Definition**: This type of placement group spreads instances across logical partitions, ensuring that groups of instances in one partition do not share underlying hardware with instances in other partitions.
   - **Use Case**: Suitable for large distributed and replicated workloads, such as Hadoop, Cassandra, and Kafka. This strategy helps to limit the impact of hardware failures to one partition.
3. **Spread Placement Group**:
   - **Definition**: Ensures that instances are placed on distinct physical hardware, with each instance on a separate rack with its own network and power source.
   - **Use Case**: Best for applications where the independent failure of any single instance must be minimized. Useful for smaller sets of critical instances.

Recommendation for High-Performance Data Processing

For a Big Data processing company focused on performance:

- **Recommended Placement**: **Cluster Placement Group**
- **Rationale**: Maximizes network performance by enhancing per-flow throughput limits up to 10 Gbps for TCP/IP traffic and ensures instances are placed in the same high-bisection bandwidth segment of the network. This is crucial for distributed data processing applications that require frequent, high-speed networking between nodes to process large datasets efficiently.

Incorrect Options Explained

1. **Use Spot Instances**:
   - **Issue**: While cost-effective, Spot Instances do not guarantee constant availability and could be interrupted, which is detrimental to performance-focused applications that require consistent computational power.
2. **Optimize the Amazon EC2 kernel using EC2 User Data**:
   - **Issue**: Kernel optimizations can improve performance to an extent but do not address the fundamental need for enhanced network throughput and low latency provided by physical proximity in a cluster placement group.
3. **Use a Spread Placement Group**:

- **Issue**: Focuses on reducing correlated failures rather than enhancing network performance, which is less relevant to the performance requirements of high-throughput data processing applications.

Conclusion

For applications where network performance and low latency are paramount, such as in distributed data processing frameworks, utilizing a cluster placement group in Amazon EC2 is the most effective strategy. This setup supports the high-speed, low-latency interconnects needed for intensive data processing tasks, aligning with the company's goal of enhancing performance in the AWS cloud.

Question 14Incorrect
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? Create a virtual private gateway (VGW) on both the AWS side of the VPN as well as the on-premises side of the VPN
Correct answer
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
Create a Customer Gateway on both the AWS side of the VPN as well as the onpremises side of the VPN
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

Correct Configuration for AWS Managed IPSec VPN Connection

Overview of AWS IPSec VPN Components

1. **Virtual Private Gateway (VGW)**:
   - **Location**: AWS side of the VPN connection.
   - **Purpose**: Serves as the VPN concentrator on the AWS side of the Site-to-Site VPN connection.
   - **Functionality**: Interfaces with the customer gateway to establish VPN tunnels for securely routing traffic between the customer's on-premises network and Amazon VPC.
2. **Customer Gateway (CGW)**:
   - **Location**: On-premises side of the VPN connection.
   - **Purpose**: Provides AWS with necessary information about the external endpoint of the on-premises networking environment where the VPN connection is established.
   - **Functionality**: Can be a physical device or software application that supports IPSec VPN connections.

Correct Configuration for IPSec VPN

- **Virtual Private Gateway (VGW) on the AWS Side**: Acts as the gateway for all traffic entering AWS from the on-premises network.
- **Customer Gateway (CGW) on the On-premises Side**: Acts as the gateway for all traffic entering the on-premises network from AWS.

How the Components Interact

- The VPN connection consists of two VPN tunnels for redundancy. Traffic between AWS and the customer's on-premises network is securely transferred over these tunnels.
- The VPN tunnels are encrypted and pass over the public internet, making IPSec VPN a secure method to extend on-premises networks into the cloud.

Visual Explanation Based on the Attached Diagram

The attached diagram accurately represents the AWS Managed IPSec VPN architecture:

- **AWS Side**: Shows a Virtual Private Gateway connected to Amazon VPC across multiple Availability Zones, ensuring high availability and fault tolerance.
- **On-premises Side**: Connected to a Customer Gateway, which interfaces with the organization's local network.

Common Misconceptions Corrected

- **Incorrect**: Creating a VGW or CGW on both ends. VGW is always on the AWS side, and CGW is always on the on-premises side.
- **Incorrect**: Misplacement of VGW and CGW roles.

Importance in Architecture Design

- Understanding the proper setup of VPN components is crucial for securely extending on-premises networks into the cloud without exposing internal network resources directly to the public internet.
- This setup allows for the secure migration of data, application connectivity, and hybrid cloud configurations, crucial for organizations looking to leverage cloud resources alongside existing on-premises infrastructure.

This configuration ensures that all traffic between AWS and the on-premises network remains secure and efficient, adhering to best practices for network security and performance.

Question 15Incorrect

A weather forecast agency collects key weather metrics across multiple cities in the US and sends this data in the form of key-value pairs to AWS Cloud at a one-minute frequency. As a solutions architect, which of the following AWS services would you use to build a solution for processing and then reliably storing this data with high availability? (Select two)

Amazon Redshift

Amazon ElastiCache

Your selection is incorrect

Amazon RDS

Your selection is correct

AWS Lambda

Correct selection

Amazon DynamoDB

Overall explanation

Correct options:

Recommended AWS Services for Weather Data Processing and Storage

Overview of Suitable AWS Services for the Task

1. **AWS Lambda**:
   - **Functionality**: AWS Lambda allows running code in response to events without the need for managing servers. It is ideal for executing code that processes or transforms incoming data.
   - **Use Case**: Can be triggered each minute to process incoming key-value pairs from the weather data, perform necessary computations or transformations, and then store the processed data.
2. **Amazon DynamoDB**:
   - **Functionality**: DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability.
   - **Use Case**: Perfect for storing key-value pair data. It offers single-digit millisecond latency to access data, which is ideal for applications requiring high-performance data retrieval.

Why These Services are Suitable

- **AWS Lambda and DynamoDB Integration**: Lambda functions can seamlessly integrate with DynamoDB to process incoming data and store it efficiently. This setup leverages Lambda's ability to handle code execution triggered by event sources like Amazon Kinesis or direct HTTP calls and uses DynamoDB to handle high-throughput, low-latency data storage.
- **Scalability and Availability**: Both services are designed to scale automatically. DynamoDB, being a fully managed service, handles the demands of replicating data across multiple availability zones, thus ensuring high availability and data durability.

Incorrect Options Explained

1. **Amazon Redshift**:
   - **Issue**: While Redshift is a powerful data warehousing solution, it is not optimized for handling high-velocity, real-time data ingestion of key-value pairs. It is better suited for analytical queries on large static datasets rather than real-time processing or storage.
2. **Amazon ElastiCache**:
   - **Issue**: ElastiCache is primarily used to enhance the performance of existing databases through caching. While it excels in speed for cacheable items, it is not intended for long-term data storage or as a primary database for transactional data.
3. **Amazon RDS**:
   - **Issue**: RDS is designed for structured data and relational databases. It operates on tables and rows and is not optimized for the key-value pair data model, which is typical in IoT and real-time data scenarios.

Conclusion

For a solution architect tasked with designing a system to process and store weather data from multiple cities using key-value pairs, AWS Lambda and Amazon DynamoDB provide a robust, scalable, and cost-effective combination. This solution efficiently addresses the needs for real-time data processing and durable, low-latency storage, leveraging the strengths of both serverless computing and NoSQL database technologies.

Question 16Incorrect

A company manages a multi-tier social media application that runs on Amazon Elastic Compute Cloud (Amazon EC2) instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones (AZs) and use an Amazon Aurora database. As an AWS Certified Solutions Architect – Associate, you have been tasked to make the application more resilient to periodic spikes in request rates. Which of the following solutions would you recommend for the given use-case? (Select two)

Correct selection

Use Amazon CloudFront distribution in front of the Application Load Balancer

Correct options:

You can use Amazon Aurora replicas and Amazon CloudFront distribution to make the application more resilient to spikes in request rates.

Recommendations to Enhance Resilience for a Social Media Application on AWS

Background

A multi-tier social media application experiences periodic spikes in request rates, which challenges its current architecture set up with Amazon EC2 instances behind an Application Load Balancer, utilizing an Amazon EC2 Auto Scaling group across multiple Availability Zones, and an Amazon Aurora database.

Recommended Solutions

1. **Use Amazon Aurora Replica**:
   - **Purpose**: Amazon Aurora Replicas are used primarily to increase the read capacity of your database. This is particularly useful during spikes in traffic when many read requests can be served by the replicas, thereby reducing the load on the primary database.
   - **High Availability**: Aurora Replicas also contribute to high availability. In the event the primary instance fails, Aurora automatically promotes a replica to be the new primary, ensuring minimal disruption.
   - **Scaling**: Allows scaling beyond the capacity constraints of a single DB instance by having up to 15 Aurora Replicas spread across different Availability Zones within a region.
2. **Use Amazon CloudFront Distribution**:
   - **Purpose**: Amazon CloudFront is a content delivery network (CDN) that can cache static content at edge locations closer to the users, significantly reducing the load on the origin servers during traffic spikes.
   - **Low Latency and High Transfer Speeds**: By serving content from locations geographically closer to users, CloudFront reduces latency and improves the speed of content delivery.
   - **Origin Failover**: CloudFront's origin failover capability can automatically route traffic to a secondary origin if the primary origin becomes unavailable, enhancing the application's resilience.

Explanation of Incorrect Options

1. **Use AWS Shield**:
   - **Issue**: AWS Shield provides DDoS protection but does not inherently handle or improve application resilience to regular traffic spikes; it's more about security rather than traffic management.
2. **Use AWS Global Accelerator**:
   - **Issue**: While AWS Global Accelerator improves application availability and performance by routing user traffic through AWS's global network infrastructure, it is not the best fit solely for handling traffic spikes in a typical HTTP/S web application scenario like social media platforms, where CloudFront's content caching capabilities are more directly beneficial.
3. **Use AWS Direct Connect**:
   - **Issue**: AWS Direct Connect establishes a private network connection from a business's premises to AWS and is not designed to handle internet traffic spikes. It's more about data transfer consistency and reducing internet-based transfer costs, not managing or scaling for internet traffic spikes.

Conclusion

For managing periodic spikes in request rates for a social media application, leveraging Amazon Aurora Replicas can offload read requests from the primary database instance, while Amazon CloudFront can serve content faster and reduce load on the servers during peak times. These solutions enhance the application's responsiveness and availability without additional complexity or significant changes to the existing infrastructure setup.

Question 17Correct
A company has noticed that its application performance has deteriorated after a new Auto Scaling group was deployed a few days back. Upon investigation, the team found out that the Launch Configuration selected for the Auto Scaling group is using the incorrect instance type that is not optimized to handle the application workflow. As a solutions architect, what would you recommend to provide a long term resolution for this issue?
No need to modify the launch configuration.
Just modify the Auto Scaling group to use more number of existing instance types. More instances may offset the loss of
performance
No need to modify the launch configuration. Just modify the Auto Scaling group to use the correct instance type
Correct option:
Create a new launch configuration to use the correct instance type. Modify the Auto Scaling group to use this new launch configuration. Delete the old launch configuration as it is no longer needed

Recommended Solution for Correcting Instance Type in AWS Auto Scaling Group

Overview of the Issue

A company has deployed a new Auto Scaling group that uses an inappropriate instance type, leading to deteriorated application performance. This is a critical issue as the instance type does not match the requirements needed to optimally run the application's workflow.

Correct Approach to Resolve the Issue

1. **Create a New Launch Configuration**:
    - **Action**: Since launch configurations cannot be modified once created, the solution is to create a new launch configuration that specifies the correct instance type suited for the application's demands.
    - **Details**: Include necessary configurations such as the appropriate Amazon Machine Image (AMI), instance type, key pair, security groups, and a block device mapping that aligns with the application needs.
2. **Update the Auto Scaling Group**:
    - **Action**: Modify the existing Auto Scaling group to utilize the newly created launch configuration.
    - **Purpose**: This ensures that any new instances launched by the Auto Scaling group will use the correct instance type, thereby potentially restoring and enhancing the application's performance.
3. **Delete the Old Launch Configuration**:
    - **Action**: Once the Auto Scaling group is successfully updated to use the new launch configuration, the old, incorrect launch configuration should be deleted to prevent future confusion and maintain organizational clarity.

Explanation of Incorrect Options

1. **Modify the Existing Launch Configuration**:
    - **Issue**: It is not possible to modify a launch configuration after it is created. This option is technically unfeasible.
2. **Adjusting Instance Count Only**:
    - **Issue**: Simply increasing the number of instances of the incorrect type does not address the fundamental issue of the instance type mismatch. While this might provide a temporary relief in performance degradation, it does not serve as a long-term solution.
3. **Directly Modifying Instance Type in Auto Scaling Group**:
    - **Issue**: The instance type of an Auto Scaling group is dictated by its associated launch configuration. Direct modifications to instance types within the Auto Scaling group settings are not possible without updating or changing the launch configuration first.

Conclusion

For a long-term resolution, creating a new launch configuration with the correct instance type and updating the Auto Scaling group to use this configuration is the most effective and straightforward approach. This ensures that the infrastructure is aligned with the application requirements and can scale appropriately without incurring unnecessary costs or performance issues

Question 18Incorrect
An Electronic Design Automation (EDA) application produces massive volumes of data that can be divided into two categories. The 'hot data' needs to be both processed and stored quickly in a parallel and distributed fashion. The 'cold data' needs to be kept for reference with quick access for reads and updates at a low cost. Which of the following AWS services is BEST suited to accelerate the aforementioned chip design process?
Amazon FSx for Windows File Server
Correct answer
Amazon FSx for Lustre
AWS Glue
Your answer is incorrect
Amazon EMR

Optimal AWS Service for EDA Application Data Processing

Overview of the Requirement

An Electronic Design Automation (EDA) application produces a substantial volume of data categorized into 'hot' and 'cold' data. The application demands both rapid processing and storage for 'hot data' and cost-effective, accessible storage for 'cold data.'

Recommended AWS Service: Amazon FSx for Lustre

1. **Purpose and Functionality**:
    - **Amazon FSx for Lustre** is specifically designed for high-performance computing (HPC) environments where speed of access to data directly impacts performance.
    - It is well-suited for applications such as machine learning, video processing, financial modeling, and, pertinent to this case, EDA applications.
2. **Benefits for 'Hot Data'**:
    - **High-Performance Storage**: FSx for Lustre provides fast, scalable, and parallel file storage. It is capable of handling the large and intense workloads typical in EDA applications, ensuring that storage performance keeps pace with compute speed.
    - **Parallel and Distributed Processing**: Supports processing workflows where multiple compute instances need to access and process data simultaneously without bottlenecks.
3. **Integration with Amazon S3 for 'Cold Data'**:

- **Seamless S3 Integration**: While FSx for Lustre handles 'hot data' with high I/O requirements, it can also integrate with Amazon S3 for 'cold data' storage. This allows data that is less frequently accessed but still needs to be available for quick reads and updates to be stored cost-effectively in S3.
- **Data Management**: FSx for Lustre allows for data to be automatically moved to S3 once it is no longer needed in high-speed storage, balancing cost and performance efficiently.

Incorrect Options Analysis

1. **Amazon FSx for Windows File Server**:
   - **Not Suitable for EDA**: This service is optimized for enterprise applications requiring Windows compatibility and SMB protocol access, not for high-performance computing tasks that are characteristic of EDA workloads.
2. **Amazon EMR**:
   - **Big Data Processing, Not High-Speed Storage**: Primarily used for processing vast amounts of data using big data frameworks like Apache Hadoop and Spark. While powerful for data processing, it does not provide the same level of storage performance as FSx for Lustre for use cases needing intensive read/write speeds.
3. **AWS Glue**:

- **ETL Service, Not for Real-Time Processing**: AWS Glue is a managed ETL service designed for batch processing and data transformation tasks, not for real-time, high-performance data access and processing required by EDA applications

Question 19Incorrect
The development team at a social media company wants to handle some complicated queries such as "What are the number of likes on the videos that have been posted by friends of a user A?".As a solutions architect, which of the following AWS database services would you suggest as the BEST fit to handle such use cases?
Amazon Redshift
Amazon Aurora
Correct answer
Amazon Neptune

Recommended AWS Database Service for Complex Social Media Queries

Overview of the Requirement

A social media company requires handling complex queries, such as retrieving the number of likes on videos posted by friends of a specific user. This involves navigating and processing highly connected data, typical of social networks where entities (such as users, friends, posts, likes) are interconnected.

Recommended AWS Service: Amazon Neptune

1. **Amazon Neptune Overview**:
   - **Purpose**: Amazon Neptune is a fully managed graph database service designed specifically to handle highly connected data sets efficiently.
   - **Functionality**: Neptune supports graph queries that make it exceptionally suitable for social networking applications, enabling features such as friend recommendations, social feed generations, and complex relationship traversals.
2. **Advantages of Using Neptune for Social Media Queries**:
   - **Graph Database Features**: Neptune enables highly interactive graph queries which are crucial for navigating and extracting relationships and connections within data, such as finding friends of friends or aggregating likes from a user's social circle.
   - **Performance**: Offers high throughput and low latency in querying large sets of user data and their interactions, crucial for real-time social media functionalities.
   - **Integration and Scalability**: Easily integrates with other AWS services and scales to accommodate growing data from social network interactions.
3. **Use Case Implementation**:
   - **Handling 'Hot Data'**: For data that needs to be processed and stored quickly (hot data), Neptune's fast processing capabilities ensure timely updates to the user's feed and other interactive features.
   - **Managing 'Cold Data'**: Although primarily for hot data, Neptune can also handle less active data (cold data) which needs to be stored cost-effectively yet remain quickly accessible for occasional reads and updates, leveraging Amazon S3 for cost-effective storage.

Incorrect Options Analysis

1. **Amazon Redshift**:
   - **Issue**: While powerful for data warehousing and analytics, Redshift is not optimized for the type of real-time, highly connected query operations required in this social media scenario.
2. **Amazon Aurora**:

- **Issue**: As a relational database, Aurora offers high performance and availability but lacks the native graph processing capabilities needed for efficiently managing complex and interconnected social media data.

3. **Amazon OpenSearch Service**:
   - **Issue**: Primarily used for search and log analytics, OpenSearch does not provide the graph database functionalities necessary for complex relational queries typical in social networking contexts.

Conclusion

Amazon Neptune is the best-suited AWS service for the described social media application due to its ability to efficiently process and manage highly connected datasets. This capability is essential for supporting the dynamic and interactive nature of social media platforms where user engagement hinges on the real-time processing of complex data relationships.

Question 20Correct
A financial services company recently launched an initiative to improve the security of its AWS resources and it had enabled AWS Shield Advanced across multiple AWS accounts owned by the company. Upon analysis, the company has found that the costs incurred are much higher than expected. Which of the following would you attribute as the underlying reason for the unexpectedly high costs for AWS Shield Advanced service?
Your answer is correct
Consolidated billing has not been enabled. All the AWS accounts should fall under a single consolidated billing for the monthly fee to be charged only once AWS Shield Advanced is being used for custom servers, that are not part of AWS Cloud, thereby resulting in increased costs Savings Plans has not been enabled for the AWS Shield Advanced service across all the AWS accounts AWS Shield Advanced also covers AWS Shield Standard plan, thereby resulting in
increased costs

Understanding High Costs of AWS Shield Advanced for a Financial Services Company

Context

A financial services company has implemented AWS Shield Advanced across multiple AWS accounts to enhance security. However, the costs associated with AWS Shield Advanced have been unexpectedly high.

Primary Reason for High Costs: Lack of Consolidated Billing

1. **Consolidated Billing**:
   - **Description**: Consolidated billing in AWS allows the organization to combine billing and payments for multiple AWS accounts into a single bill. This approach can significantly simplify the financial management of AWS resources across several accounts.
   - **Impact on Costs**: For services like AWS Shield Advanced, which include a fixed monthly fee, consolidated billing ensures that this fee is charged only once per organization, rather than being charged separately for each AWS account.
2. **How Consolidated Billing Works with AWS Shield Advanced**:
   - If AWS Shield Advanced is activated on multiple accounts without consolidated billing, each account is billed separately for the Shield Advanced subscription.
   - When consolidated billing is enabled, despite multiple accounts using Shield Advanced, the monthly fee is incurred only once, leading to significant cost savings.

Incorrect Assumptions and Their Clarifications

1. **AWS Shield Advanced Usage for Non-AWS Servers**:
   - **Clarification**: Although AWS Shield Advanced can offer protection for certain non-AWS resources, the main cost implications come from how billing is structured across AWS accounts, not from the types of resources being protected.
2. **Inclusion of AWS Shield Standard**:
   - **Clarification**: AWS Shield Standard is provided at no extra cost to all AWS customers and does not contribute additional costs when AWS Shield Advanced is used. AWS Shield Advanced is a separate, higher-tier service providing additional protection features.
3. **Lack of Savings Plans for AWS Shield Advanced**:
   - **Clarification**: Savings Plans apply to services like Amazon EC2, AWS Lambda, and AWS Fargate, which are compute services. AWS Shield Advanced, being a security and protection service, does not fit into the Savings Plans model, hence not applicable.

Recommendation

To address the unexpectedly high costs of AWS Shield Advanced:

- **Implement Consolidated Billing**: Ensure that all AWS accounts under the company's control are grouped under a single consolidated billing account. This approach will ensure the monthly fee for AWS Shield Advanced is charged only once for the entire organization rather than per account.
- **Review Account Structure**: Conduct a thorough review of the account structure and billing setup to ensure that all accounts are appropriately linked under the consolidated billing framework.

Conclusion

The primary step to mitigate the high costs associated with AWS Shield Advanced for the financial services company is to enable consolidated billing. This adjustment will ensure that the company benefits from aggregated billing advantages, significantly reducing the overall cost of utilizing AWS Shield Advanced across multiple accounts.

Question 21Correct
The infrastructure team at a company maintains 5 different VPCs (let's call these VPCs A, B, C, D, E) for resource isolation. Due to the changed organizational structure, the team wants to interconnect all VPCs together. To facilitate this, the team has set up VPC peering connection between VPC A and all other VPCs in a hub and spoke model with VPC A at the center. However, the team has still failed to establish connectivity between all VPCs. As a solutions architect, which of the following would you recommend as the MOST resource-efficient and scalable solution?
Use an internet gateway to interconnect the VPCs
Use a VPC endpoint to interconnect the VPCs
Establish VPC peering connections between all VPCs
Your answer is correct
Use AWS transit gateway to interconnect the VPCs

Recommended Solution for Interconnecting Multiple VPCs

Problem Context

A company has 5 different VPCs (A, B, C, D, E) set up in a hub-and-spoke model with VPC A at the center, aiming to establish interconnectivity among all. Despite peering VPC A with the others, connectivity between VPCs other than A (e.g., B to C, D to E) has not been established due to the limitations of VPC peering.

Optimal Solution: Use AWS Transit Gateway

1. **AWS Transit Gateway Overview**:
   - **Functionality**: Acts as a network transit hub that simplifies the network architecture by connecting VPCs and on-premises networks through a central hub. This reduces complexity and operational overhead compared to managing multiple VPC peering connections.
   - **Benefits**:
     - **Simplified Connectivity**: Allows all connected VPCs to communicate with each other, overcoming the transitive peering limitation.
     - **Scalable and Efficient**: Manages centralized routing using a transit gateway route table, which can scale more efficiently as more VPCs or connections are added.
2. **Implementation Considerations**:
   - **Central Control**: Transit gateways provide a single gateway to manage routing and security more effectively across multiple VPCs.
   - **Cost Efficiency**: Reduces the cost and complexity of having to establish and manage multiple peering connections or redundant networking hardware.

Analysis of Incorrect Options

1. **Use an Internet Gateway**:
   - **Misapplication**: Internet gateways provide a route for Internet traffic to and from VPCs but are not suitable for interconnecting multiple VPCs internally.
2. **Use a VPC Endpoint**:
   - **Limitation**: VPC endpoints facilitate private connections between VPCs and AWS services using PrivateLink, but do not provide connectivity between VPCs themselves.
3. **Establish VPC Peering Connections Between All VPCs**:
   - **Non-transitive Nature**: Direct VPC peering is non-transitive, meaning each pair of VPCs requires an individual connection, which becomes complex and cumbersome with an increasing number of VPCs.

Conclusion

To effectively interconnect multiple VPCs within a company, leveraging AWS Transit Gateway is the most resource-efficient and scalable solution. This approach simplifies network management, reduces potential points of failure, and can adapt to future expansions in network infrastructure.

Question 22Correct
A cybersecurity company uses a fleet of Amazon EC2 instances to run a proprietary application. The infrastructure maintenance group at the company wants to be notified via an email whenever the CPU utilization for any of the Amazon EC2 instances breaches a certain threshold. Which of the following services would you use for building a solution with the LEAST amount of development effort? (Select two)
Your selection is correct
Amazon Simple Notification Service (Amazon SNS) AWS Lambda

Optimal Services for EC2 Instance Monitoring and Notification

Problem Context

A cybersecurity company requires a system to monitor CPU utilization of their Amazon EC2 instances and to be notified via email when CPU usage exceeds a predefined threshold.

Recommended AWS Services

1. **Amazon CloudWatch**:
   - **Purpose**: Provides monitoring and operational data for AWS resources and applications running on AWS infrastructure.
   - **Functionality**: You can set alarms in CloudWatch to monitor metrics such as CPU utilization. When a specified threshold is breached, an action can be triggered.
2. **Amazon Simple Notification Service (Amazon SNS)**:
   - **Purpose**: Offers a managed solution for sending notifications.
   - **Functionality**: Integrates with CloudWatch alarms to send notifications through various channels, including email, when an alarm state change occurs.

Solution Architecture

- **CloudWatch Alarm**: Set up a CloudWatch alarm for CPU utilization on the EC2 instances. Specify the threshold that, when breached, triggers the alarm.
- **SNS Topic**: Create an SNS topic to handle the notifications.
- **Email Subscription**: Subscribe the necessary email addresses to the SNS topic. When CloudWatch triggers an alarm, it publishes a message to the SNS topic, which then sends an email notification to the subscribed addresses.

Steps to Implement

1. **Configure CloudWatch Alarm**:
   - Navigate to the CloudWatch console.
   - Create a new alarm and select the CPU utilization metric associated with the desired EC2 instances.
   - Define the threshold for the alarm (e.g., CPU utilization above 80% for 5 consecutive minutes).
2. **Set Up SNS Topic**:
   - Go to the SNS dashboard.
   - Create a new topic for EC2 CPU utilization alerts.
   - Add email subscriptions by entering the email addresses that should receive alerts.
3. **Link CloudWatch Alarm to SNS Topic**:
   - In the CloudWatch alarm configuration, set the action to publish to the SNS topic when the alarm state is “ALARM.”

Incorrect Options and Clarifications

1. **AWS Lambda**:
   - **Clarification**: While Lambda is powerful for running backend processes in response to events, it is not directly used for monitoring or sending notifications without integrating with other services like CloudWatch and SNS.
2. **Amazon Simple Queue Service (Amazon SQS)**:
   - **Clarification**: SQS is ideal for decoupling application components via message queuing and not suitable for direct monitoring or alert notifications.
3. **AWS Step Functions**:
   - **Clarification**: Used for coordinating multi-step workflows and is not a direct tool for monitoring or notifications.

Conclusion

The combination of **Amazon CloudWatch** and **Amazon Simple Notification Service (SNS)** offers the most straightforward and effective solution for monitoring EC2 CPU utilization and sending notifications with minimal development effort. This approach leverages AWS’s robust monitoring tools and notification service to ensure real-time, reliable alerting for resource management

Question 23Incorrect
A medium-sized business has a taxi dispatch application deployed on an Amazon EC2 instance. Because of an unknown bug, the application causes the instance to freeze regularly. Then, the instance has to be manually restarted via the AWS management console.
Which of the following is the MOST cost-optimal and resource-efficient way to implement an automated solution until a permanent fix is delivered by the development team? Setup an Amazon CloudWatch alarm to monitor the health status of the instance. In case of an Instance Health Check failure, Amazon CloudWatch Alarm can publish to an Amazon Simple Notification Service (Amazon SNS) event which can then trigger an AWS lambda function. The AWS lambda function can use Amazon EC2 API to reboot the instance Use Amazon EventBridge events to trigger an AWS Lambda function to reboot the instance status every 5 minutes
Correct answer
Setup an Amazon CloudWatch alarm to monitor the health status of the instance. In case of an Instance Health Check failure, an EC2 Reboot CloudWatch Alarm Action can be used to reboot the instance

Automated Reboot Solution for EC2 Instance Freezing Issue

Problem Context

A medium-sized business is experiencing regular freezing of an EC2 instance due to an application bug, requiring manual restarts. An automated solution is sought to handle this issue until a permanent software fix is implemented.

Recommended Solution: CloudWatch Alarm with EC2 Reboot Action

1. **Amazon CloudWatch**:
   - **Purpose**: Monitors AWS resources and applications, providing data and actionable insights.
   - **Functionality**: Allows setting up alarms based on specific metrics or health statuses that can trigger automated actions like stopping, terminating, rebooting, or recovering EC2 instances.
2. **EC2 Reboot Alarm Action**:
   - **Operation**: Configures a CloudWatch alarm that monitors the EC2 instance for any health check failures. If such a failure is detected, the alarm triggers an automatic reboot of the instance without manual intervention.
   - **Advantages**: This method is directly integrated into AWS management tools, making it a simple and cost-effective solution for automatically managing instance availability issues.

Steps to Implement

1. **Configure CloudWatch Alarm**:
   - Navigate to the CloudWatch console.
   - Create a new alarm based on the EC2 Instance Health Check.
   - Set the metric for the alarm (e.g., Status Check Failed (Any)).
   - Configure the threshold that indicates when the alarm should be triggered.
2. **Set Alarm Action**:
   - Choose the reboot action for the alarm. This ensures that the instance is automatically rebooted if the health check fails.

Incorrect Options and Why They Are Inefficient

1. **Using AWS Lambda via CloudWatch and SNS**:
   - **Inefficiency**: Involves multiple services (CloudWatch, SNS, Lambda) which complicates the architecture unnecessarily for a task that can be handled directly by CloudWatch.
   - **Cost**: Although Lambda is cost-effective at low invocation levels, maintaining a Lambda function for this purpose might introduce slight overheads in terms of performance and management.
2. **Using Amazon EventBridge with AWS Lambda**:
   - **Reboot Every 5 Minutes**: Automatically rebooting the instance every 5 minutes is excessive and can lead to service disruption and potential data loss or inconsistency.
   - **Check and Reboot on Failure**: While this is a more targeted approach than indiscriminate reboots, it still involves unnecessary complexity when a direct CloudWatch alarm action can suffice.

Conclusion

The most resource-efficient and straightforward approach to automatically managing the freezing issue on an EC2 instance is to set up a CloudWatch alarm that directly triggers an EC2 reboot upon health check failures. This method leverages built-in AWS capabilities, minimizes the moving parts, and avoids unnecessary computational overhead, thus providing a reliable and cost-effective solution until the application bug is fixed

Question 24Incorrect
A healthcare company uses its on-premises infrastructure to run legacy applications that require specialized customizations to the underlying Oracle database as well as its host operating system (OS). The company also wants to improve the availability of the Oracle database layer. The company has hired you as an AWS Certified Solutions Architect – Associate to build a solution on AWS that meets these requirements while minimizing the underlying infrastructure maintenance effort. Which of the following options represents the best solution for this use case? Deploy the Oracle database layer on multiple Amazon EC2 instances spread across two Availability Zones (AZs). This deployment configuration guarantees high availability and also allows the Database Administrator (DBA) to access and customize the database environment and the underlying operating system
Correct answer
Leverage multi-AZ configuration of Amazon RDS Custom for Oracle that allows the Database Administrator (DBA) to access and customize the database environment and the underlying operating system Leverage cross AZ read-replica configuration of Amazon RDS for Oracle that allows the Database Administrator (DBA) to access and customize the database environment and the underlying operating system

Solution Recommendation for a Healthcare Company with Oracle Database Requirements

Scenario Overview

A healthcare company seeks to migrate its legacy Oracle database, which requires specific customizations at both the database and operating system levels, to AWS while enhancing availability and minimizing infrastructure maintenance.

Recommended AWS Solution: Amazon RDS Custom for Oracle

1. **Amazon RDS Custom for Oracle**:
   - **Customization Capability**: Unlike standard RDS offerings, RDS Custom for Oracle allows database administrators (DBAs) to access and customize the database server and operating system. This includes applying special patches and modifying database software settings, which are essential for supporting legacy applications that have specific requirements.
   - **Features**:
     - Supports advanced database configurations and third-party application integrations.
     - Provides the ability to manage the underlying operating system and database environment directly.
2. **Multi-AZ Configuration**:
   - **High Availability**: Deploying in a multi-AZ configuration ensures that the database service remains highly available, with automatic failover to a secondary instance in a different Availability Zone in the event of a failure.
   - **Data Durability and Reliability**: Multi-AZ deployments significantly enhance data durability and availability, crucial for healthcare applications requiring near-constant database access.

Implementation Approach

- **Set Up RDS Custom for Oracle**: Configure the Oracle database on Amazon RDS Custom with the necessary custom settings and patches. Ensure that all configurations align with the legacy application's requirements.
- **Enable Multi-AZ Deployment**: During the setup, enable Multi-AZ deployment to ensure high availability. This configuration automatically replicates the database to a secondary instance in a different Availability Zone without manual intervention.
- **Monitoring and Maintenance**: Utilize AWS tools like Amazon CloudWatch for monitoring the database performance and setting up alerts for operational metrics that could indicate potential issues.

Incorrect Options and Rationale

- **Amazon RDS for Oracle without Customization**: Standard RDS for Oracle does not provide the necessary access for OS-level and deeper database customizations needed for legacy applications.
- **Deploying on EC2 Instances**: While deploying Oracle on EC2 allows full control over the database and OS, it significantly increases the maintenance burden related to patching, scaling, and securing the instances and does not fulfill the requirement for minimal infrastructure effort.
- **Cross-AZ Read-Replica Configuration**: This option, while providing some level of high availability, does not offer the customization capabilities required for the Oracle database in legacy application scenarios.

Conclusion

For the healthcare company's needs, **Amazon RDS Custom for Oracle in a Multi-AZ configuration** is the optimal choice. This setup not only meets the customization requirements but also provides a highly available, scalable, and maintenance-minimized environment, aligning with the company's goals to improve operational efficiency on the cloud.

Question 25Incorrect
A company has grown from a small startup to an enterprise employing over 1000 people. As the team size has grown, the company has recently observed some strange behavior, with Amazon S3 buckets settings being changed regularly. How can you figure out what's happening without restricting the rights of the users? Implement an IAM policy to forbid users to change Amazon S3 bucket settings
Correct answer
Use AWS CloudTrail to analyze API calls Implement a bucket policy requiring AWS Multi-Factor Authentication (AWS MFA) for all operations

Analyzing Strange Behavior in Amazon S3 Bucket Settings

Scenario Overview

A rapidly growing enterprise has noticed unauthorized changes to its Amazon S3 bucket settings. The company needs a solution to monitor and identify the source of these changes without impacting user permissions.

Recommended AWS Solution: AWS CloudTrail

1. **AWS CloudTrail**:
   - **Activity Monitoring**: AWS CloudTrail is designed for governance, compliance, operational auditing, and risk auditing. It logs all API calls made on your AWS resources, making it the ideal service to monitor and audit changes to Amazon S3 buckets.
   - **API Call Logging**: CloudTrail will capture all API calls that modify the S3 bucket settings, including who made the call, from which IP address, and when it occurred. This allows for precise tracing of changes.
   - **Integration**: CloudTrail can integrate with other AWS services like Amazon S3 and AWS Lambda for deeper analysis and real-time alerting.
2. **Configuration Steps**:
   - **Enable CloudTrail**: If not already enabled, set up AWS CloudTrail in the AWS Management Console. Ensure it's configured to log Read and Write API calls for S3 buckets.

  - **Create a Trail**: Set up a trail that specifically logs activities related to S3 buckets. Ensure the trail configuration captures every API activity for comprehensive monitoring.
  - **Log Storage and Analysis**: Ensure that the CloudTrail logs are stored in a secure S3 bucket. Optionally, configure integration with Amazon Athena or AWS Lambda for advanced analysis or real-time alerting on specific API call patterns indicative of unauthorized access.

Additional Tools for Enhanced Monitoring:

- **Amazon S3 Access Logs**: For a more detailed analysis of data access patterns, enable S3 access logging. These logs can be analyzed using Amazon Athena to provide insights into access patterns and potential security lapses.
- **AWS Lambda and Amazon SNS**: Set up AWS Lambda functions triggered by CloudTrail log updates to analyze suspicious activities and send alerts using Amazon SNS. This provides real-time notifications to administrators when critical changes are detected.

Incorrect Options and Rationale

- **Implement an IAM Policy to Forbid Changes**: This approach is restrictive and might disrupt legitimate user operations. It is also a reactive measure that does not provide insights into activities.
- **Amazon S3 Access Logs with Athena**: While useful for access pattern analysis, S3 access logs do not capture the identity of the API caller or the exact API call used, which is critical in identifying the source of unauthorized changes.
- **Implement MFA for All Operations**: This approach enhances security but does not address the need to audit and analyze changes to understand the root cause of the issue.

Conclusion

Utilizing **AWS CloudTrail** is the most effective and least intrusive method to monitor and audit changes to Amazon S3 bucket settings in the described scenario. It provides comprehensive logging and integration capabilities, which are essential for maintaining security and compliance in a growing enterprise environment.

Question 26Correct
A healthcare startup needs to enforce compliance and regulatory guidelines for objects stored in Amazon S3. One of the key requirements is to provide adequate protection against accidental deletion of objects. As a solutions architect, what are your recommendations to address these guidelines? (Select two) ?
Your selection is correct
Enable versioning on the Amazon S3 bucket

Enhancing Object Protection in Amazon S3

Scenario Overview

A healthcare startup needs to ensure that their Amazon S3 objects are protected against accidental deletion, complying with regulatory guidelines.

Recommendations for S3 Object Protection

1. **Enable Versioning on the Amazon S3 Bucket**:
   - **Purpose**: Versioning is crucial as it maintains multiple versions of an object within the same bucket. This feature allows any overwritten or deleted object to be recoverable by keeping its previous versions.
   - **Configuration**: Activate versioning on the S3 bucket through the Amazon S3 console. This setting allows each object version to be preserved even after deletion or modification, where a delete marker is added instead of actual data removal.
2. **Enable Multi-Factor Authentication (MFA) Delete on the Amazon S3 Bucket**:
   - **Security Enhancement**: MFA delete adds an additional layer of security by requiring two factors of authentication before an object can be permanently deleted.
   - **Setup**: This can be configured via the S3 console under the bucket's versioning settings. It requires the use of an MFA device when deleting an object, preventing accidental or malicious deletions.

Additional Details

- **Versioning Details**:
  - When enabled, every object modification results in a new version, while the original is preserved.
  - Deleting an object doesn't remove it but adds a delete marker, making the object appear deleted until the marker is removed.
- **MFA Delete Capabilities**:
  - It ensures that deletions require not just the usual permissions but also a code from a registered MFA device, significantly reducing the risk of accidental data loss.

Incorrect Options and Their Limitations

- **Event Trigger on Deletion**: While monitoring deletions is useful, it does not prevent the deletion of objects. It only informs stakeholders after the fact, which does not comply with the proactive security measures required.

- **Managerial Approval Process**: This manual process is not enforceable through Amazon S3's technical controls and depends heavily on organizational policies, which can be bypassed or not followed strictly.
- **Additional Confirmation for Deletions in S3 Console**: Amazon S3 does not provide an option to configure additional confirmations for deletions directly through the console. This would have to be managed through client-side controls or scripts, which are not supported directly by AWS.

Conclusion

For the healthcare startup, enabling versioning and MFA delete on Amazon S3 buckets are the most direct and effective solutions to ensure compliance with regulatory guidelines and protect against accidental object deletions. These features provide robust safeguards that align with the need for high security and data integrity in the healthcare industry

Question 27Incorrect
A pharma company is working on developing a vaccine for the COVID-19 virus. The researchers at the company want to process the reference healthcare data in a highly available as well as HIPAA compliant in-memory database that supports caching results of
SQL queries. As a solutions architect, which of the following AWS services would you recommend for this task?
Amazon DocumentDB
Amazon DynamoDB
Correct answer
Amazon ElastiCache for Redis/Memcached
Your answer is incorrect
Amazon DynamoDB Accelerator (DAX)

Question 27: A pharma company is working on developing a vaccine for the COVID-19 virus. The researchers at the company want to process the reference healthcare data in a highly available as well as HIPAA compliant in-memory database that supports caching results of SQL queries.

Correct Answer:

Amazon ElastiCache for Redis/Memcached

Overall Explanation:

Amazon ElastiCache for Redis is a blazing fast in-memory data store that provides sub-millisecond latency to power internet-scale real-time applications. It is a great choice for real-time transactional and analytical processing use cases such as caching, chat/messaging, gaming leaderboards, geospatial, machine learning, media streaming, queues, real-time analytics, and session store. ElastiCache for Redis supports replication, high availability, and cluster sharding right out of the box.

Amazon ElastiCache for Memcached is a Memcached-compatible in-memory key-value store service that can be used as a cache or a data store. It is a great choice for implementing an in-memory cache to decrease access latency, increase throughput, and ease the load off your relational or NoSQL database. Session stores are easy to create with Amazon ElastiCache for Memcached.

Both Amazon ElastiCache for Redis and Amazon ElastiCache for Memcached are HIPAA Eligible, making them suitable for healthcare applications. Therefore, this is the correct option.

Incorrect Options:

- **Amazon DynamoDB Accelerator (DAX):** While it is a caching service that enables fast in-memory performance for demanding applications, DAX does not support SQL query caching.
- **Amazon DynamoDB:** This is a key-value and document database that is not an in-memory database.
- **Amazon DocumentDB:** This service supports MongoDB workloads and is not an in-memory database, thus not suitable for the described use case.

Question 28Correct
An Elastic Load Balancer has marked all the Amazon EC2 instances in the target group as unhealthy. Surprisingly, when a developer enters the IP address of the Amazon EC2 instances in the web browser, he can access the website. What could be the reason the instances are being marked as unhealthy? (Select two)
Your selection is correct
The route for the health check is misconfigured You need to attach elastic IP address (EIP) to the Amazon EC2 instances

Question 28:

An Elastic Load Balancer has marked all the Amazon EC2 instances in the target group as unhealthy. Surprisingly, when a developer enters the IP address of the Amazon EC2 instances in the web browser, he can access the website.

Correct Answer:

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

Overall Explanation:

An Application Load Balancer (ALB) periodically sends requests to its registered targets to test their status. These tests are called health checks. Each load balancer node routes requests only to the healthy targets in the enabled Availability Zones (AZs) for the load balancer. If a target group contains only unhealthy registered targets, the load balancer nodes route requests across its unhealthy targets.

To ensure proper functionality, you must verify that the security groups associated with the load balancer allow traffic on the new port in both directions. It is also crucial that the health check routes are correctly configured to ensure the ALB can successfully verify the health of the EC2 instances.

Application Load Balancer Configuration for Security Groups and Health Check Routes:

This involves setting up the security groups to permit traffic between the ALB and the EC2 instances on both the listener and health check ports. Correct configuration ensures the ALB can communicate with the EC2 instances to perform health checks.

Incorrect options:

- The Amazon Elastic Block Store (Amazon EBS) volumes have been improperly mounted - This is incorrect because accessing the website via the IP address indicates the EBS volumes are functioning correctly.
- Your web-app has a runtime that is not supported by the Application Load Balancer - This is incorrect as ALB issues are not related to the runtime of the web application.
- You need to attach elastic IP address (EIP) to the Amazon EC2 instances - This is unnecessary for ALB functionality and is therefore a distractor.

This explanation clarifies how security groups and health check configurations impact the functionality of an Application Load Balancer in AWS environments.

Question 29Incorrect

An e-commerce application uses an Amazon Aurora Multi-AZ deployment for its database. While analyzing the performance metrics, the engineering team has found that the database reads are causing high input/output (I/O) and adding latency to the write requests against the database. As an AWS Certified Solutions Architect Associate, what would you recommend to separate the read requests from the write requests?

Correct answer

Set up a read replica and modify the application to use the appropriate endpoint Activate read-through caching on the Amazon Aurora database

To address the performance issues encountered with the e-commerce application using an Amazon Aurora Multi-AZ deployment, the correct recommendation is to utilize Aurora Replicas to separate read operations from write operations. This approach leverages Aurora's capacity for handling high read loads without impacting the write performance of the primary instance.

Here's a breakdown of how to implement this:

1. **Set Up Aurora Replicas**: Create Aurora Replicas in different Availability Zones to enhance the database's fault tolerance and read capacity. These replicas will handle read-only queries, thus offloading such operations from the primary database instance which handles all write operations.
2. **Use the Appropriate Endpoint**: Modify the application's database configuration to route read queries to the reader endpoint. Aurora provides a reader endpoint that automatically load-balances read requests across all available Aurora Replicas. By using the reader endpoint, the application can distribute its read load effectively, thereby minimizing the I/O and latency impacts on the primary instance which processes the write requests.

By configuring the application to connect to the reader endpoint for read operations and the cluster endpoint for write operations, you can significantly improve the overall efficiency and responsiveness of your database operations in a high-load environment.

Question 30Correct

A Big Data analytics company wants to set up an AWS cloud architecture that throttles requests in case of sudden traffic spikes. The company is looking for AWS services that can be used for buffering or throttling to handle such traffic variations. Which of the following services can be used to support this requirement? Amazon Simple Queue Service (Amazon SQS), Amazon Simple Notification Service (Amazon SNS) and AWS Lambda Amazon Gateway Endpoints, Amazon Simple Queue Service (Amazon SQS) and Amazon Kinesis

Your answer is correct

Amazon API Gateway, Amazon Simple Queue Service (Amazon SQS) and Amazon Kinesis Elastic Load Balancer, Amazon Simple Queue Service (Amazon SQS), AWS Lambda

To handle sudden traffic spikes efficiently by buffering or throttling requests, using the combination of Amazon API Gateway, Amazon Simple Queue Service (Amazon SQS), and Amazon Kinesis is highly effective. Here's how each service contributes to managing traffic variations:

1. **Amazon API Gateway**: This service provides throttling at multiple levels including global and per-method throttling on individual API calls. By setting up throttling rules, API Gateway can limit the number of requests a user can submit over a period of time, which helps to prevent your backend systems from being overwhelmed by too many requests.

2. **Amazon Simple Queue Service (Amazon SQS)**: SQS acts as a buffer between your application components and the end user, absorbing any inconsistencies in traffic flow. It helps manage and scale automatically based on the volume of requests, ensuring no data loss during spikes and maintaining the smooth operation of your services.
3. **Amazon Kinesis**: This service is ideal for real-time data streaming and big data ingestion. Kinesis can handle large streams of data records that are generated continuously by thousands of data sources. This capability allows it to buffer and process large amounts of incoming data in real time, which is crucial for analytics workloads during traffic spikes.

Together, these AWS services provide a robust infrastructure to manage, buffer, and throttle requests effectively, ensuring that the Big Data analytics company can handle sudden increases in data traffic without service disruption or degradation. This setup is essential for maintaining service reliability and responsiveness under varying load conditions.

Question 31Incorrect
The engineering team at an e-commerce company is working on cost optimizations forAmazon Elastic Compute Cloud (Amazon EC2) instances. The team wants to manage the workload using a mix of on-demand and spot instances across multiple instance types. They would like to create an Auto Scaling group with a mix of these instances. Which of the following options would allow the engineering team to provision the instances for this use-case?
Correct answer
You can only use a launch template to provision capacity across multiple instance types using both On-Demand Instances and Spot Instances to achieve the desired scale, performance, and cost You can neither use a launch configuration nor a launch template to provision capacity across multiple instance types using both On-Demand Instances and Spot Instances to achieve the desired scale, performance, and cost You can use a launch configuration or a launch template to provision capacity across multiple instance types using both On-Demand Instances and Spot Instances to achieve the desired scale, performance, and cost

To efficiently manage the workload on Amazon EC2 instances with a mix of on-demand and spot instances across multiple instance types, the best practice is to use a launch template. Here’s a detailed explanation of why this is the recommended approach:

1. **Launch Templates**: A launch template in AWS provides the capability to specify a wide range of parameters that are used to launch EC2 instances. This includes the Amazon Machine Image (AMI) ID, instance type, key pair, security groups, and other essential configurations. The advantage of using a launch template over a launch configuration is its versatility and the ability to manage multiple versions. This is crucial when dealing with a mix of different instance types and purchase options (like on-demand and spot instances).
2. **Advantages of Launch Templates**:
   - **Flexibility**: Launch templates support specifying both on-demand and spot options in the same template, which allows for more dynamic and cost-effective scaling strategies.
   - **Version Control**: They allow you to create different versions of launch templates, making it easier to iterate and update instance specifications without disrupting existing setups.
   - **Simplification**: Using launch templates simplifies the management of instance specifications and scaling policies in Auto Scaling groups.

With the launch template, the engineering team can set instance market options to target the desired balance between on-demand and spot instances. This method ensures that the Auto Scaling group can provision the capacity as needed, depending on availability and cost criteria set by the team.

Thus, using a launch template is the only method that allows for provisioning capacity across multiple instance types using both on-demand and spot instances to achieve the desired scale, performance, and cost. This approach is not only cost-effective but also enhances the flexibility of the cloud infrastructure, aligning with best practices for scaling and cost management in AWS environments.

Question 32Incorrect
A startup's cloud infrastructure consists of a few Amazon EC2 instances, Amazon RDS instances and Amazon S3 storage. A year into their business operations, the startup is incurring costs that seem too high for their business requirements. Which of the following options represents a valid cost-optimization solution? Use AWS Compute Optimizer recommendations to help you choose the optimal Amazon EC2 purchasing options and help reserve your instance capacities at reduced costs
Correct answer
Use AWS Cost Explorer Resource Optimization to get a report of Amazon EC2 instances that are either idle or have low utilization and use AWS Compute Optimizer to look at instance type recommendations Use AWS Trusted Advisor checks on Amazon EC2 Reserved Instances to automatically renew reserved instances (RI). AWS Trusted advisor also suggests Amazon RDS idle database instances

To address high costs for a startup using Amazon EC2, Amazon RDS, and Amazon S3, focusing on resource optimization and cost management is crucial. Here’s how you can effectively reduce costs:

1. **AWS Cost Explorer Resource Optimization**:
   - **Functionality**: AWS Cost Explorer provides a detailed report of your resource usage and associated costs. It specifically identifies underutilized Amazon EC2 instances that may be downsized or terminated to save costs.

  - **Usage**: Utilize the Resource Optimization feature to get a detailed report on instances that are either idle or have low utilization. This helps in identifying where you can reduce the instance size or terminate unnecessary instances, thereby optimizing costs without impacting performance.

2. **AWS Compute Optimizer**:
   - **Functionality**: AWS Compute Optimizer uses machine learning to analyze historical utilization metrics to provide recommendations for the optimal Amazon EC2 instance types. This can include suggestions for resizing or changing instances within auto-scaling groups to align more closely with actual usage patterns.
   - **Usage**: Implement recommendations from AWS Compute Optimizer to adjust your EC2 instance types and sizes based on actual need. This can lead to significant savings, especially if the current instances are over-provisioned.

Correct Cost Optimization Strategy:

- **Combining the Insights**: Start by using AWS Cost Explorer to identify and address under-utilized resources. Follow up with AWS Compute Optimizer to ensure that the remaining resources are optimally configured. This two-pronged approach ensures that you're not only reducing the number of resources but also enhancing the efficiency of what remains.
- **Monitoring and Continuous Optimization**: Regularly review the insights from these tools to keep your AWS environment optimized as your usage patterns and AWS pricing models evolve.

Why Other Options Are Less Suitable:

- **S3 Storage Class Analysis**: While useful for optimizing S3 costs, it doesn't address costs related to EC2 and RDS, which are often significant contributors to overall AWS expenses.
- **Trusted Advisor for Reserved Instances**: While helpful, this doesn't provide the proactive resource utilization insights needed for immediate cost reduction. It also does not automate the renewal of Reserved Instances, which requires manual intervention.

By prioritizing these approaches, the startup can significantly reduce operational costs while maintaining or even enhancing application performance. This strategy not only provides immediate cost benefits but also sets up the infrastructure for scalable and efficient growth.

Question 33Correct
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?
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
Use Amazon Macie to monitor any malicious activity on data stored in Amazon S3. Use Amazon GuardDuty to identify any sensitive data stored on Amazon S3 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
Your answer is correct
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

For **Question 33**, here's the breakdown based on the provided images and text:

Question:

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.

Recommendations:

- **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** is a threat detection service that continuously monitors for malicious or unauthorized behavior to protect your AWS accounts, workloads, and data stored in Amazon S3. It utilizes machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats.
- **Amazon Macie** is a data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in Amazon S3. Macie is particularly adept at recognizing sensitive data such as personally identifiable information (PII).

Correct Configuration:

You should configure Amazon GuardDuty to monitor and detect malicious activities and potential threats in S3. Concurrently, Amazon Macie should be used to analyze S3 buckets for sensitive data, ensuring compliance and enhancing data protection strategies. This dual-service approach leverages the strengths of each service in accordance with their specific capabilities, as illustrated in the attached images.

By using both Amazon GuardDuty for threat detection and Amazon Macie for sensitive data identification, the company can achieve a robust security posture that addresses both aspects of security and compliance. This approach is confirmed as the correct and effective method according to AWS best practices and the functionalities of each service as detailed in the descriptions provided in the images.

Question 34Incorrect
A mobile gaming company is experiencing heavy read traffic to its Amazon Relational Database Service (Amazon RDS) database that retrieves player's scores and stats. The company is using an Amazon RDS database instance type that is not cost-effective for their budget. The company would like to implement a strategy to deal with the high volume of read traffic, reduce latency, and also downsize the instance size to cut costs. Which of the following solutions do you recommend? Move to Amazon Redshift Switch application code to AWS Lambda for better performance
Correct answer
Setup Amazon ElastiCache in front of Amazon RDS
Your answer is incorrect
Setup Amazon RDS Read Replicas

For **Question 34**, the details provided along with the user requirements suggest the following breakdown:

Question:

A mobile gaming company is experiencing heavy read traffic to its Amazon Relational Database Service (Amazon RDS) that retrieves player's scores and stats. They are looking for a solution to manage high read traffic, reduce latency, and cut costs by potentially downsizing the instance size.

Recommendations:

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

Explanation:

- **Amazon ElastiCache** serves as an excellent high-performance caching layer for Amazon RDS. By caching frequently accessed data, it reduces the load on the RDS database, thereby minimizing the need for a larger, more expensive database instance. This setup can handle high volumes of read traffic effectively, improving performance and reducing latency.
- Caching is particularly effective for gaming applications where player scores and stats are frequently queried but not as frequently updated. This can dramatically improve read performance and reduce the load on the underlying database.

Why Other Options Are Incorrect:

- **Setup Amazon RDS Read Replicas**: While this could distribute the load of read operations, it does not necessarily reduce costs since each read replica incurs additional charges. It's more beneficial when read traffic is so high that a single database (even with caching) cannot handle the load, or when there is a need to serve reads from different geographical locations.
- **Move to Amazon Redshift**: This option is not cost-effective for scenarios primarily involving heavy read traffic of operational data rather than complex querying of large datasets typical in data warehousing scenarios.
- **Switch application code to AWS Lambda**: While AWS Lambda can enhance performance by processing data with serverless computing, it does not address the core issue of reducing load and latency directly at the database level. Lambda would still need to fetch data from RDS, which wouldn't alleviate the read load issue.

Using **Amazon ElastiCache** to cache frequently accessed data such as player scores and stats directly addresses the company's needs for high performance, reduced latency, and potentially lower costs by allowing for a smaller RDS instance due to reduced load. This approach is the most suitable given the use-case of high read volume and the need for cost efficiency.

Question 35Incorrect
A retail company uses AWS Cloud to manage its technology infrastructure. The company has deployed its consumer-focused web application on Amazon EC2-based web servers and uses Amazon RDS PostgreSQL database as the data store. The PostgreSQL database is set up in a private subnet that allows inbound traffic from selected Amazon EC2 instances. The database also uses AWS Key Management Service (AWS KMS) for encrypting data at rest. Which of the following steps would you recommend to facilitate secure access to the database?
Correct answer
Configure Amazon RDS to use SSL for data in transit Use IAM authentication to access the database instead of the database user's access Credentials Create a new security group that blocks SSH from the selected Amazon EC2 instances into the database

For **Question 35**, the scenario described involves a retail company utilizing AWS Cloud, including Amazon EC2 web servers and an Amazon RDS PostgreSQL database with AWS Key Management Service (AWS KMS) for encryption at rest. The primary concern is ensuring secure access to the database, especially regarding data in transit.

Recommendations:

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

Explanation:

- **SSL/TLS Configuration for Amazon RDS PostgreSQL**: Enabling SSL/TLS for the Amazon RDS PostgreSQL database ensures that data transmitted between the database and the EC2 instances is encrypted, protecting it from interception or tampering during transit. Amazon RDS automatically manages the SSL certificate installation when the DB instance is provisioned. This not only secures the data in transit but also complies with many security standards and regulations that mandate encryption for sensitive data transmission.

Why Other Options Are Incorrect:

- **Use IAM Authentication**: While IAM authentication offers a secure way to authenticate to the database without using database credentials (relying on AWS IAM roles and policies instead), it primarily enhances access control rather than the security of data in transit. It's an authentication improvement but doesn't address the encryption of data as it moves between the server and the database.
- **Blocking SSH Access (via Security Group or Network ACL)**: These options are distractors because they refer to blocking SSH (Secure Shell) access. However, SSH is not a method used for accessing Amazon RDS instances for database operations; RDS does not support SSH access. These controls would not apply to the database access scenario described.

The correct action is to configure SSL/TLS for the RDS instance to encrypt data in transit, ensuring that any data exchanged between the EC2 instances and the RDS database remains secure. This is directly aligned with best practices for protecting data in transit and is supported by AWS configuration options for RDS.

Question 36Correct
You have been hired as a Solutions Architect to advise a company on the various authentication/authorization mechanisms that AWS offers to authorize an API call within the Amazon API Gateway. The company would prefer a solution that offers built-in user management. Which of the following solutions would you suggest as the best fit for the given use-case? Use AWS Lambda authorizer for Amazon API Gateway
Your answer is correct
Use Amazon Cognito User Pools
Use Amazon Cognito Identity Pools
Use AWS_IAM authorization

For **Question 36**, the scenario involves recommending an AWS service for authenticating API calls within Amazon API Gateway, with a preference for a solution that offers built-in user management. Here's the recommendation and explanation:

Recommendation:

- **Use Amazon Cognito User Pools**

Explanation:

- **Amazon Cognito User Pools** provide a comprehensive solution for user management, authentication, and access control. It supports direct sign-up and sign-in capabilities, as well as integration with third-party identity providers like Google, Facebook, and Amazon through OpenID Connect (OIDC) and SAML.

Why This Option:

- Amazon Cognito User Pools can handle user directory management, authentication, and security features like multi-factor authentication (MFA) and compromised credentials protection.
- User pools can be directly integrated with Amazon API Gateway to create an authorizer that uses OAuth tokens or identity tokens, enabling secure and straightforward access control for APIs.

Diagram Analysis:

The provided diagram illustrates a common architecture using Amazon Cognito along with other AWS services like API Gateway and AWS Lambda. The flow shows how Cognito interacts with external identity providers and facilitates user login, generating tokens that are then used to authorize API calls through API Gateway.

Incorrect Options:

- **AWS Lambda Authorizer**: Suitable for custom authentication logic but does not provide built-in user management. It is more flexible but requires more setup and is used primarily when integrating with external identity providers not supported natively by Amazon Cognito.
- **AWS_IAM Authorization**: Mainly used for service-to-service permissions within AWS environments, not for consumer-facing applications where user management is required.
- **Amazon Cognito Identity Pools**: These are used to provide AWS credentials to authenticated users to allow access to AWS services, not for managing API authentication directly.

In this context, **Amazon Cognito User Pools** is clearly the best option given its built-in user management, ease of integration with Amazon API Gateway, and support for secure user authentication and authorization. This fits perfectly with the company's requirement for a built-in user management system that securely handles API authentication.

Question 37Correct
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 costeffective solution?
Your answer is correct

Use Amazon EC2 dedicated hosts
Use Amazon EC2 reserved instances (RI)
Use Amazon EC2 on-demand instances
Use Amazon EC2 dedicated instances

For **Question 37**, the scenario involves a financial services company planning to migrate its IT infrastructure to AWS Cloud and wanting to leverage its existing server-bound software licenses. The task is to find the most cost-effective AWS solution that supports using these licenses.

Recommendation:

- **Use Amazon EC2 Dedicated Hosts**

Explanation:

- **Amazon EC2 Dedicated Hosts** provide physical servers fully dedicated for your use. This option is especially beneficial when you have server-bound licenses (such as for Microsoft Windows Server or specific database software), which often have restrictions that do not allow them to be moved between different servers or shared environments.

Why This Option:

- Dedicated Hosts allow you to utilize existing software licenses compliantly, often leading to significant cost savings as opposed to purchasing new licenses in the cloud.
- They provide control over instance placement, enabling you to meet compliance and regulatory requirements that might not be possible with other types of instances.

Incorrect Options:

- **Amazon EC2 Dedicated Instances**: These instances run on hardware dedicated to a single customer within a VPC but may share the hardware with other non-dedicated instances from the same account. They do not adequately address the need to apply server-bound licenses which are tied specifically to hardware.
- **Amazon EC2 On-Demand Instances**: While offering flexibility, they don't support the use of server-bound licenses, which are typically tied to specific hardware for compliance reasons.
- **Amazon EC2 Reserved Instances (RI)**: Although they offer a cost reduction for long-term commitments, they are similar to on-demand instances in terms of licensing flexibility and do not specifically support physical server dedication which is required for server-bound licenses.

In summary, **Amazon EC2 Dedicated Hosts** are the optimal choice for the company's requirement to continue utilizing its existing server-bound licenses while ensuring compliance and reducing potential licensing costs during the transition to AWS Cloud.

Question 38Incorrect
A financial services firm uses a high-frequency trading system and wants to write the log files into Amazon S3. The system will also read these log files in parallel on a near real-time basis. The engineering team wants to address any data discrepancies that might arise when the trading system overwrites an existing log file and then tries to read that specific log file. Which of the following options BEST describes the capabilities of Amazon S3 relevant to this scenario?
Correct answer
A process replaces an existing object and immediately tries to read it. Amazon S3 always returns the latest version of the object A process replaces an existing object and immediately tries to read it. Until the change is fully propagated, Amazon S3 might return the new data

For **Question 38**, the situation involves a high-frequency trading system utilizing Amazon S3 for storing and reading log files, with potential concerns about reading data immediately after it's written, particularly in cases of overwriting existing log files.

Correct Option and Explanation:

- **A process replaces an existing object and immediately tries to read it. Amazon S3 always returns the latest version of the object.**

Why This Option:

- Amazon S3 provides **strong read-after-write consistency** for all PUTS of new objects and overwrites of existing objects (PUTS and DELETES), which means that as soon as a write is completed, any subsequent retrieves (reads) will see the latest version of the object.
- This capability is crucial for applications like high-frequency trading systems, where immediate and accurate data retrieval following log updates is essential for maintaining data integrity and system accuracy.

Detailed Capabilities of Amazon S3:

- **Strong Consistency**: Amazon S3 offers strong consistency automatically for all applications without any additional cost, ensuring that the system reads the latest version of the data immediately after it is written.
- This applies to both writing new data and overwriting existing data, which addresses the engineering team's concerns about data discrepancies during concurrent writes and reads on log files.

Incorrect Options:

- **A process replaces an existing object and immediately tries to read it. Until the change is fully propagated, Amazon S3 might return the previous data**: This was historically true but is no longer accurate since Amazon S3 announced strong read-after-write consistency in December 2020.

- **A process replaces an existing object and immediately tries to read it. Until the change is fully propagated, Amazon S3 might return the new data**: Incorrect as the new data is immediately available upon write completion.
- **A process replaces an existing object and immediately tries to read it. Until the change is fully propagated, Amazon S3 does not return any data**: Also incorrect because Amazon S3 does not have a delay where no data is returned; the new data is available right after the write is confirmed.

In summary, the correct recommendation is that with strong read-after-write consistency, Amazon S3 ensures that any operations to overwrite existing objects are immediately visible to subsequent read operations, making it ideal for scenarios where rapid and reliable data access is critical post-update.

Question 39Correct
A social photo-sharing web application is hosted on Amazon Elastic Compute Cloud (Amazon EC2) instances behind an Elastic Load Balancer. The app gives the users the ability to upload their photos and also shows a leaderboard on the homepage of the app. The uploaded photos are stored in Amazon Simple Storage Service (Amazon S3) and the leaderboard data is maintained in Amazon DynamoDB. The Amazon EC2 instances need to access both Amazon S3 and Amazon DynamoDB for these features. As a solutions architect, which of the following solutions would you recommend as the MOST secure option?
Save the AWS credentials (access key Id and secret access token) in a configuration file within the application code on the Amazon EC2 instances. Amazon EC2 instances can use these credentials to access Amazon S3 and Amazon DynamoDB
Your answer is correct
Attach the appropriate IAM role to the Amazon EC2 instance profile so that the instance can access Amazon S3 and Amazon DynamoDB Configure AWS CLI on the Amazon EC2 instances using a valid IAM user's credentials. The application code can then invoke shell scripts to access Amazon S3 and Amazon DynamoDB via AWS CLI Encrypt the AWS credentials via a custom encryption library and save it in a secret directory on the Amazon EC2 instances. The application code can then safely decrypt the AWS credentials to make the API calls to Amazon S3 and Amazon DynamoDB

For **Question 39**, you're tasked with identifying the most secure way for Amazon EC2 instances hosting a social photo-sharing application to access resources such as Amazon S3 for photo storage and Amazon DynamoDB for maintaining leaderboard data.

Correct Option and Explanation:

- **Attach the appropriate IAM role to the Amazon EC2 instance profile so that the instance can access Amazon S3 and Amazon DynamoDB.**

Why This Option:

- **IAM roles** provide a secure way to grant permissions to entities that you trust. By associating an IAM role with an EC2 instance, the applications running on that instance can securely make API calls to AWS services like S3 and DynamoDB without needing to manage static AWS credentials.
- IAM roles provide temporary credentials that are automatically rotated and are securely delivered to the instance. They minimize the risk of credential leakage and simplify the credential management process.

Additional Insights:

- **Using IAM roles** with EC2 instances eliminates the need to embed or programmatically manage AWS credentials within your application, thereby enhancing security and reducing the overhead associated with credentials management and rotation.

Incorrect Options:

- **Save the AWS credentials (access key Id and secret access token) in a configuration file within the application code on the Amazon EC2 instances.** This method risks exposing sensitive credentials if the instance is compromised.
- **Configure AWS CLI on the Amazon EC2 instances using a valid IAM user's credentials.** This option involves managing long-term credentials on the instance, which can be risky and goes against the security best practices of using temporary credentials wherever possible.
- **Encrypt the AWS credentials via a custom encryption library and save it in a secret directory on the Amazon EC2 instances.** While encryption adds a layer of security, managing and decrypting these credentials still poses risks and complicates credential management unnecessarily.

In summary, leveraging IAM roles for EC2 instances to access AWS services like S3 and DynamoDB provides a secure, scalable, and manageable approach to access management without exposing AWS credentials. This method is fully integrated with AWS services and does not require additional implementation overhead.

Question 40Correct
A Big Data analytics company writes data and log files in Amazon S3 buckets. The company now wants to stream the existing data files as well as any ongoing file updates from Amazon S3 to Amazon Kinesis Data Streams. As a Solutions Architect, which of the following would you suggest as the fastest possible way of building a solution for this requirement?
Amazon S3 bucket actions can be directly configured to write data into Amazon Simple Notification Service (Amazon SNS). Amazon SNS can then be used to send the updates to Amazon Kinesis Data Streams Configure Amazon EventBridge events for the bucket actions on Amazon S3. An AWS Lambda function can then be triggered from the Amazon EventBridge event that will send the necessary data to Amazon Kinesis Data Streams Leverage Amazon S3 event notification to trigger an AWS Lambda function for the file create event. The AWS Lambda function will then send the necessary data to Amazon Kinesis Data Streams Your answer is correct Leverage AWS Database Migration Service (AWS DMS) as a bridge between Amazon S3 and Amazon Kinesis Data Streams

For **Question 40**, the solution involves integrating AWS services to efficiently manage the data flow from Amazon S3 to Amazon Kinesis Data Streams for a Big Data analytics company. The goal is to establish a real-time analytics system capable of handling both historical and ongoing data feeds from Amazon S3.

Recommended Solution:

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

Why This Solution:

- **AWS Database Migration Service (AWS DMS)** can be effectively used to migrate data from an Amazon S3 bucket directly into Amazon Kinesis Data Streams. This approach is beneficial for setting up real-time data streaming architectures with minimal coding and maintenance effort.
- **AWS DMS** supports continuous data replication and can handle large volumes of data transfer between Amazon S3 and Kinesis. It simplifies the process by managing the data flow seamlessly and offers scaling capabilities to handle varying loads.
- Using AWS DMS ensures that the data migration is efficient and minimizes the risk of data loss or delays, making it ideal for the high-speed requirements of a high-frequency trading system.

Incorrect Options and Explanation:

- **Configure Amazon EventBridge events for the bucket actions on Amazon S3. An AWS Lambda function can then be triggered from the Amazon EventBridge event that will send the necessary data to Amazon Kinesis Data Streams** - This setup requires additional custom development and is not as straightforward as using AWS DMS.
- **Leverage Amazon S3 event notification to trigger an AWS Lambda function for the file create event. The AWS Lambda function will then send the necessary data to Amazon Kinesis Data Streams** - While feasible, this approach requires significant custom coding and ongoing maintenance to manage data flows effectively.
- **Amazon S3 bucket actions can be directly configured to write data into Amazon Simple Notification Service (Amazon SNS). Amazon SNS can then be used to send the updates to Amazon Kinesis Data Streams** - This option incorrectly describes the capabilities of Amazon S3 and Amazon SNS as S3 cannot directly write data into SNS, and SNS is not directly integrated with Kinesis Data Streams for streaming solutions.

The provided diagram illustrates how various AWS services, including AWS DMS, can be integrated to create a robust architecture for real-time data processing and analytics, enhancing the ability to handle data-intensive tasks without extensive system reconfiguration or development effort.

Question 41Incorrect
An IT company provides Amazon Simple Storage Service (Amazon S3) bucket access to specific users within the same account for completing project specific work. With changing business requirements, cross-account S3 access requests are also growing every month. The company is looking for a solution that can offer user level as well as account-level access permissions for the data stored in Amazon S3 buckets. As a Solutions Architect, which of the following would you suggest as the MOST optimized way of controlling access for this use-case? Use Access Control Lists (ACLs) Your answer is incorrect Use Identity and Access Management (IAM) policies Use Security Groups
Correct answer
Use Amazon S3 Bucket Policies

For **Question 41**, you are addressing how to manage cross-account access to Amazon S3 buckets effectively.

Recommended Solution:

- **Use Amazon S3 Bucket Policies**

Why This Solution:

- **Amazon S3 Bucket Policies** allow you to create comprehensive, flexible policies that can control access based on a variety of conditions such as the AWS account, IP address, SSL use, and more. This makes it ideal for both user-level and account-level permissions management.
- S3 Bucket Policies can be applied directly to the bucket, providing centralized management of permissions and enabling scenarios where specific access needs to be granted to users from other AWS accounts, making it perfect for cross-account access scenarios.

Explanation of Bucket Policies:

- Bucket policies provide a powerful way to manage access permissions centrally for all objects within a bucket. They are attached directly to the S3 bucket and can specify permissions that apply either across the entire bucket or only to a subset of objects within it.
- These policies support various condition keys to tailor permissions according to the request context, such as the time of the request, the requester's IP, whether the connection is over SSL, and more.

Incorrect Options and Why:

- **Use Identity and Access Management (IAM) policies**: While IAM policies are effective for managing permissions within your own AWS account, they are not as streamlined as bucket policies for managing cross-account access.
- **Use Access Control Lists (ACLs)**: ACLs offer a more granular level of access control but are less flexible and comprehensive compared to bucket policies. They do not offer the same level of detailed condition-based control and are generally considered less manageable for complex scenarios.
- **Use Security Groups**: Security groups are not applicable to Amazon S3 as they are designed to control access to Amazon EC2 instances, not S3 buckets.

By implementing S3 bucket policies, the company can efficiently manage permissions across both users within the same account and users from other AWS accounts, aligning with changing business requirements and maintaining a secure and organized access strategy.

Question 42Correct
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?
VPC Endpoint
Software VPN
Your answer is correct
AWS VPN CloudHub
VPC Peering connection

For **Question 42**, you are addressing how to enable secure communication between multiple branch offices and a corporate headquarters using a combination of AWS Direct Connect and AWS Site-to-Site VPN connections.

Recommended Solution:

- **AWS VPN CloudHub**

Why This Solution:

- **AWS VPN CloudHub** enables secure communication between multiple AWS Site-to-Site VPN connections. It allows remote sites to communicate with each other and with the corporate headquarters.
- The VPN CloudHub operates on a simple hub-and-spoke model, which is suitable for scenarios where multiple branch offices need to communicate with each other and with a central location (the corporate headquarters).
- In this use case, the corporate headquarters is connected to the AWS VPC using AWS Direct Connect, and the branch offices are connected using AWS Site-to-Site VPN. AWS VPN CloudHub can integrate these connections seamlessly, enabling data exchange among all locations.

Diagram Explanation:

- **Virtual Private Gateway**: The central hub that connects the VPC to multiple customer gateways.
- **Customer Gateway**: Represents the branch offices and corporate headquarters that connect to the VPC via VPN or Direct Connect.

Incorrect Options and Why:

- **VPC Endpoint**: VPC endpoints are used to connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink. They are not designed for enabling communication between multiple remote locations.
- **VPC Peering Connection**: VPC peering is used to route traffic between two VPCs using private IP addresses. It does not facilitate communication between remote branch offices and on-premises data centers connected via VPN or Direct Connect.
- **Software VPN**: While a software VPN can manage connectivity between a remote network and a VPC, it does not facilitate direct communication between multiple branch offices and the corporate headquarters.

By implementing **AWS VPN CloudHub**, the media company can ensure efficient and secure communication between its corporate headquarters and branch offices, leveraging their existing Direct Connect and Site-to-Site VPN connections.

Question 43Incorrect
A financial services company has deployed its flagship application on Amazon EC2 instances. Since the application handles sensitive customer data, the security team at the company wants to ensure that any third-party Secure Sockets Layer certificate (SSL certificate) SSL/Transport Layer Security (TLS) certificates configured on Amazon EC2 instances via the AWS Certificate Manager (ACM) are renewed before their expiry date. The company has hired you as an AWS Certified Solutions Architect Associate to build a solution that notifies the security team 30 days before the certificate expiration. The solution should require the least amount of scripting and maintenance effort. What will you recommend?
Correct answer
Leverage AWS Config managed rule to check if any third-party SSL/TLS certificates imported into ACM are marked for expiration within 30 days. Configure the rule to trigger an Amazon SNS notification to the security team if any certificate expires within 30 days

Leverage AWS Config managed rule to check if any third-party SSL/TLS certificates imported into ACM are marked for expiration within 30 days. Configure the rule to trigger an Amazon SNS notification to the security team if any certificate expires within 30 days

Explanation:

- **AWS Config**: Provides a detailed view of resource configurations in your AWS account and can monitor compliance with pre-defined rules.
- **ACM Certificates**: ACM automatically renews its own certificates, but not third-party ones.
- **Managed Rule**: Use AWS Config's managed rule to check for upcoming certificate expirations and trigger notifications via Amazon SNS.

Incorrect Options:

1. **CloudWatch Metric for Imported Certificates**: Requires more configuration effort compared to using AWS Config managed rule.
2. **Config Rule for ACM Certificates**: ACM automatically renews its own certificates; no need to monitor them.

3. **CloudWatch Metric for ACM Certificates**: Same reason as above, ACM handles its own renewals.

Question 44Incorrect
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 answer
Use VPC sharing to share one or more subnets with other AWS accounts belonging to the same parent organization from AWS Organizations

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

Explanation:

- **VPC Sharing**: Allows multiple AWS accounts to use resources like EC2 and RDS within shared subnets.
- **Centrally-Managed VPCs**: The owner account shares subnets with other accounts in the same AWS Organization, enabling centralized VPC management and high interconnectivity.
- **Participants**: Can create, modify, and delete resources in shared subnets but cannot interfere with resources of other participants or the VPC owner.

Incorrect Options:

1. **VPC Sharing to Share a VPC**: VPC sharing involves sharing subnets, not the entire VPC.
2. **VPC Peering to Share a VPC or Subnets**: VPC peering connects two VPCs for traffic routing but does not support centrally managed VPCs or sharing specific subnets.

Question 45Correct
An Internet of Things (IoT) company would like to have a streaming system that performs real-time analytics on the ingested IoT data. Once the analytics is done, the company would like to send notifications back to the mobile applications of the IoT device owners. As a solutions architect, which of the following AWS technologies would you recommend to send these notifications to the mobile applications?
Amazon Kinesis with Amazon Simple Email Service (Amazon SES) Amazon Kinesis with Amazon Simple Queue Service (Amazon SQS) Amazon Simple Queue Service (Amazon SQS) with Amazon Simple Notification Service (Amazon SNS)
Your answer is correct
Amazon Kinesis with Amazon Simple Notification Service (Amazon SNS)
Amazon Kinesis with Amazon Simple Notification Service (Amazon SNS)

Explanation:

- **Amazon Kinesis**: Ideal for real-time data collection, processing, and analysis from IoT devices.
- **Amazon SNS**: Perfect for sending notifications to mobile applications due to its push-based, many-to-many messaging service.

Combining **Amazon Kinesis** for real-time analytics and **Amazon SNS** for notifications ensures a streamlined process from data ingestion to user notification.

Incorrect Options:

1. **Amazon SQS with Amazon SNS**: SQS is great for message queuing but not for real-time streaming.
2. **Amazon Kinesis with Amazon SES**: SES is for sending emails, not real-time notifications.
3. **Amazon Kinesis with Amazon SQS**: SQS is not suitable for sending notifications, it requires SNS for that functionality.

Question 46Incorrect
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 selection
NAT instance can be used as a bastion server
Your selection is incorrect
NAT gateway supports port forwarding
Correct selection
Security Groups can be associated with a NAT instance
Explanation

Correct options:

- **NAT instance can be used as a bastion server**: NAT instances can be used as bastion servers because they are EC2 instances that you can SSH into.

- **Security Groups can be associated with a NAT instance**: Security groups can be associated with NAT instances to control the inbound and outbound traffic.
- **NAT instance supports port forwarding**: NAT instances can be configured to support port forwarding.

Incorrect options:

- **Security Groups can be associated with a NAT gateway**: NAT gateways cannot have security groups associated with them. Security groups can only be associated with instances.
- **NAT gateway can be used as a bastion server**: NAT gateways cannot be used as bastion servers. They are managed services and do not provide SSH access.
- **NAT gateway supports port forwarding**: NAT gateways do not support port forwarding. They are meant to provide outbound internet access for instances in a private subnet.

Summary of the differences between NAT instances and NAT gateways:

- **Security Groups**: Associated with NAT instances but not with NAT gateways.
- **Port Forwarding**: Supported by NAT instances, not by NAT gateways.
    - **Bastion Server**: NAT instances can be used as bastion servers; NAT gateways cannot.

Question 47Correct
An IT company wants to review its security best-practices after an incident was reported where a new developer on the team was assigned full access to Amazon DynamoDB. The developer accidentally deleted a couple of tables from the production environment while building out a new feature. Which is the MOST effective way to address this issue so that such incidents do not recur? Only root user should have full database access in the organization Your answer is correct Use permissions boundary to control the maximum permissions employees can grant to the IAM principals The CTO should review the permissions for each new developer's IAM user so that Such incidents don't recur Remove full database access for all IAM users in the organization

Explanation

Correct option:

- **Use permissions boundary to control the maximum permissions employees can grant to the IAM principals**: A permissions boundary helps define the maximum permissions that employees can grant to the IAM principals (users and roles) they create and manage. The effective permissions are the intersection of the permissions boundary and the permissions policy, ensuring that the new principal cannot exceed the defined boundary.

Incorrect options:

- **Remove full database access for all IAM users in the organization**: Not practical, as certain users require full access for database administration.
- **The CTO should review the permissions for each new developer's IAM user**: This process should be automated, not manually reviewed by the CTO.
- **Only root user should have full database access in the organization**: The root user should not be used for daily administrative tasks as a best practice.

Visual Representation:

- The diagram illustrates how the permissions boundary restricts the maximum permissions an IAM policy can grant, ensuring the new principal's permissions do not exceed the boundary.

Question 48Correct
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)
Your selection is correct
AWS Database Migration Service (AWS DMS)
AWS Snowball Edge
AWS Glue
Basic Schema Copy
Your selection is correct
AWS Schema Conversion Tool (AWS SCT)

Explanation

Correct options:

- **AWS Schema Conversion Tool (AWS SCT)**: AWS SCT helps convert your commercial database schema to open-source schemas in a cost-effective manner. It handles complex database configurations such as secondary indexes, foreign keys, and stored procedures.
- **AWS Database Migration Service (AWS DMS)**: AWS DMS enables quick and secure migration of databases to AWS with minimal downtime. It supports heterogeneous migrations (different database platforms) and works well with AWS SCT for schema conversion before data migration.

Migration Steps:

1. Use AWS SCT to convert the source schema and code to match the target database.
2. Use AWS DMS to migrate data from the source database to the target database.

Incorrect options:

- **AWS Snowball Edge**: Used for transferring large amounts of data to AWS, not for database migrations.
- **AWS Glue**: Designed for ETL operations, not for database migrations.
- **Basic Schema Copy**: Useful for test migrations, but cannot handle secondary indexes, foreign keys, or stored procedures.

Visual Representation:

- The diagram shows the two-step process using AWS SCT and AWS DMS for migrating from Oracle or MySQL databases to Amazon Aurora, handling schema conversion and data migration.

Question 49Incorrect
A news network uses Amazon Simple Storage Service (Amazon S3) to aggregate the raw video footage from its reporting teams across the US. The news network has recently expanded into new geographies in Europe and Asia. The technical teams at the overseas branch offices have reported huge delays in uploading large video files to the destination Amazon S3 bucket. Which of the following are the MOST cost-effective options to improve the file upload speed into Amazon S3 (Select two)
Correct selection
Use multipart uploads for faster file uploads into the destination Amazon S3 bucket Create multiple AWS Direct Connect connections between the AWS Cloud and branch offices in Europe and Asia. Use the direct connect connections for faster file uploads into Amazon S3
Your selection is correct
Use Amazon S3 Transfer Acceleration (Amazon S3TA) to enable faster file uploads into the destination S3 bucket
Your selection is incorrect
Use AWS Global Accelerator for faster file uploads into the destination Amazon S3 Bucket Create multiple AWS Site-to-Site VPN connections between the AWS Cloud and branch offices in Europe and Asia. Use these VPN connections for faster file uploads into Amazon S3

Explanation

Correct options:

- **Use Amazon S3 Transfer Acceleration (Amazon S3TA)**: This service speeds up file uploads by leveraging Amazon CloudFront's globally distributed edge locations. Data arrives at the edge location and is routed to Amazon S3 over an optimized network path, reducing latency and increasing upload speeds.
- **Use multipart uploads**: This method splits a single large object into smaller parts, which can be uploaded independently and in parallel. This improves throughput and allows retransmission of any failed part without affecting the rest, enhancing upload efficiency.

Diagram Explanation:

- The first image explains how S3 Transfer Acceleration works using edge locations to accelerate uploads.
- The second image illustrates how multipart uploads work, with independent parts being uploaded in parallel for improved speed and reliability.

Incorrect options:

- **AWS Direct Connect**: Although it provides a dedicated network connection, it is not cost-effective and has long provisioning times, making it impractical for this use case.
- **AWS Site-to-Site VPN**: Suitable for secure connections but does not improve file upload speeds to S3.
- **AWS Global Accelerator**: Enhances the performance and availability of applications but does not directly improve file upload speeds to S3.

Question 50Correct
A retail company maintains an AWS Direct Connect connection to AWS and has recently migrated its data warehouse to AWS. The data analysts at the company query the data warehouse using a visualization tool. The average size of a query returned by the data warehouse is 60 megabytes and the query responses returned by the data warehouse are not cached in the visualization tool. Each webpage returned by the visualization tool is approximately 600 kilobytes.
Which of the following options offers the LOWEST data transfer egress cost for the company? Deploy the visualization tool in the same AWS region as the data warehouse. Access the visualization tool over the internet at a location in the same region
Your answer is correct
Deploy the visualization tool in the same AWS region as the data warehouse. Access the visualization tool over a Direct Connect connection at a location in the same region Deploy the visualization tool on-premises. Query the data warehouse over the Internet at a location in the same AWS region Deploy the visualization tool on-premises. Query the data warehouse directly over an AWS Direct Connect connection at a location in the same AWS region

Explanation

Correct option:

- **Deploy the visualization tool in the same AWS region as the data warehouse. Access the visualization tool over a Direct Connect connection at a location in the same region**:

By placing the visualization tool in the same region as the data warehouse and accessing it via Direct Connect, the data transfer out (DTO) charges are minimized. Only the 600 kilobytes for each webpage are counted as DTO, rather than the 60 megabytes of query data. This approach leverages the lower cost and efficiency of Direct Connect for minimal data transfer charges.

Diagram Explanation:

- The image explains AWS Direct Connect pricing, emphasizing that data transfer out (DTO) charges apply for traffic sent through Direct Connect to outside AWS destinations. By deploying the visualization tool within the same AWS region and using Direct Connect, DTO charges are significantly reduced compared to internet-based data transfer.

Incorrect options:

- **Deploy the visualization tool in the same AWS region as the data warehouse. Access the visualization tool over the internet at a location in the same region**:

Data transfer pricing over the internet is higher than using AWS Direct Connect.

- **Deploy the visualization tool on-premises. Query the data warehouse directly over an AWS Direct Connect connection at a location in the same AWS region**:

This incurs higher DTO charges due to the 60 MB of query response data being transferred over Direct Connect.

- **Deploy the visualization tool on-premises. Query the data warehouse over the internet at a location in the same AWS region**:

Similar to the previous point, this also incurs higher DTO charges and has higher data transfer pricing over the internet.

Question 51Correct
An IT company has an Access Control Management (ACM) application that uses Amazon RDS for MySQL but is running into performance issues despite using Read Replicas. The company has hired you as a solutions architect to address these performance-related challenges without moving away from the underlying relational database schema. The company has branch offices across the world, and it needs the solution to work on a global scale. Which of the following will you recommend as the MOST cost-effective and high performance solution?
Spin up a Amazon Redshift cluster in each AWS region. Migrate the existing data into Redshift clusters Use Amazon DynamoDB Global Tables to provide fast, local, read and write performance in each region Spin up Amazon EC2 instances in each AWS region, install MySQL databases and migrate the existing data into these new databases
Your answer is correct
Use Amazon Aurora Global Database to enable fast local reads with low latency in each region

Explanation

Correct Option:

- **Amazon Aurora Global Database:**
  - **Technology Involved:** Aurora Global Database allows a single Amazon Aurora database to span multiple AWS regions. It replicates your data with no impact on database performance, enables fast local reads with low latency in each region, and provides disaster recovery from region-wide outages.
  - **Relevant Use Cases:** Ideal for applications that require globally distributed access with high performance, low latency, and strong consistency. Suitable for read-heavy applications needing quick failover capabilities.

Incorrect Options:

- **Amazon DynamoDB Global Tables:**
  - **Technology Involved:** DynamoDB Global Tables provide a fully managed, multi-region, multi-master database that delivers fast, local read and write performance.
  - **Relevant Use Cases:** Best for NoSQL databases that need global scalability and low-latency access. Not suitable for applications that need to maintain a relational database schema, as it is a NoSQL solution.
- **Amazon Redshift Clusters:**
  - **Technology Involved:** Redshift is a fully-managed data warehouse designed for large-scale data set storage and analysis.
  - **Relevant Use Cases:** Suitable for analytical and reporting workloads, not for transactional relational database operations.
- **Amazon EC2 with MySQL:**
  - **Technology Involved:** Manually setting up MySQL databases on EC2 instances across multiple regions.

• **Relevant Use Cases:** Requires significant manual management and is not ideal for applications needing high availability and low maintenance. Not a scalable or efficient solution for global applications needing high performance and low latency.

Question 52Correct
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)

Your selection is correct
Make sure that the throughput for the target FIFO (First-In-First-Out) queue does not exceed 3,000 messages per second Make sure that the name of the FIFO (First-In-First-Out) queue is the same as the standard queue Your selection is correct Delete the existing standard queue and recreate it as a FIFO (First-In-First-Out) queue
Your selection is correct
Make sure that the name of the FIFO (First-In-First-Out) queue ends with the .fifoSuffix Convert the existing standard queue into a FIFO (First-In-First-Out) queue Make sure that the throughput for the target FIFO (First-In-First-Out) queue does not exceed 300 messages per second

Explanation

Correct Options:

1. **Delete the existing standard queue and recreate it as a FIFO (First-In-First-Out) queue:**
   - **Technology Involved:** Amazon SQS (Simple Queue Service)
   - **Relevant Use Cases:** You cannot directly convert a standard queue to a FIFO queue. The standard queue needs to be deleted and recreated as a FIFO queue to ensure the correct ordering and exactly-once processing features.
2. **Make sure that the name of the FIFO (First-In-First-Out) queue ends with the .fifo suffix:**
   - **Technology Involved:** Amazon SQS
   - **Relevant Use Cases:** FIFO queue names must end with the .fifo suffix to distinguish them from standard queues and ensure the correct configuration for FIFO processing.
3. **Make sure that the throughput for the target FIFO (First-In-First-Out) queue does not exceed 3,000 messages per second:**
   - **Technology Involved:** Amazon SQS
   - **Relevant Use Cases:** FIFO queues support up to 3,000 messages per second with batching. This ensures the application can handle the required throughput within the limits of FIFO queues.

Incorrect Options:

1. **Convert the existing standard queue into a FIFO (First-In-First-Out) queue:**
   - **Technology Involved:** Amazon SQS
   - **Relevant Use Cases:** Direct conversion from standard to FIFO is not supported. You must delete and recreate the queue as FIFO.
2. **Make sure that the name of the FIFO (First-In-First-Out) queue is the same as the standard queue:**
   - **Technology Involved:** Amazon SQS
   - **Relevant Use Cases:** The FIFO queue must have a name ending with .fifo, which may differ from the original standard queue name.
3. **Make sure that the throughput for the target FIFO (First-In-First-Out) queue does not exceed 300 messages per second:**
   - **Technology Involved:** Amazon SQS

- **Relevant Use Cases:** This limit applies without batching. With batching, the limit is 3,000 messages per second, making the 300 messages per second limit incorrect when batching is enabled.

Question 53Correct
A development team has deployed a microservice to the Amazon Elastic Container Service (Amazon ECS). The application layer is in a Docker container that provides both static and dynamic content through an Application Load Balancer. With increasing load, the Amazon ECS cluster is experiencing higher network usage. The development team has looked into the network usage and found that 90% of it is due to distributing static content of the application. As a Solutions Architect, what do you recommend to improve the application's network usage and decrease costs? Distribute the static content through Amazon EFS
Your answer is correct
Distribute the static content through Amazon S3
Distribute the dynamic content through Amazon S3
Distribute the dynamic content through Amazon EFS
Explanation

Correct Option:

- **Distribute the static content through Amazon S3:**
  - **Technology Involved:** Amazon S3
  - **Relevant Use Cases:** Amazon S3 is an ideal solution for hosting static content like HTML, CSS, JavaScript, and media files. By distributing static content through Amazon S3, you can offload the network usage from the Amazon ECS instances, reducing network costs and improving performance. Amazon S3 provides a scalable and cost-effective solution for serving static assets with high availability and low latency.

Incorrect Options:

- **Distribute the dynamic content through Amazon S3:**
  - **Technology Involved:** Amazon S3

    - **Relevant Use Cases:** Amazon S3 does not support server-side scripting and is not suitable for dynamic content that requires server-side processing. Dynamic content needs to be processed by server-side technologies such as PHP, JSP, or ASP.NET, which Amazon S3 cannot handle.
- **Distribute the static content through Amazon EFS:**
    - **Technology Involved:** Amazon EFS
    - **Relevant Use Cases:** Amazon EFS is a fully managed elastic file system that provides shared file storage for use with AWS Cloud services and on-premises resources. However, using Amazon EFS for static content would not reduce network usage effectively since the static content would still be distributed by the Amazon ECS instances. This does not address the issue of offloading network traffic.
- **Distribute the dynamic content through Amazon EFS:**
    - **Technology Involved:** Amazon EFS

• **Relevant Use Cases:** While Amazon EFS can be used for shared file storage, it does not optimize the distribution of dynamic content. Dynamic content typically involves server-side processing, which requires a compute environment like Amazon ECS or AWS Lambda. Using Amazon EFS would not provide any specific advantages for handling dynamic content and would not reduce network usage or costs effectively.

Question 54Correct
A developer needs to implement an AWS Lambda function in AWS account A that accesses an Amazon Simple Storage Service (Amazon S3) bucket in AWS account B. As a Solutions Architect, which of the following will you recommend to meet this requirement?
Your answer is correct
Create an IAM role for the AWS Lambda function that grants access to the Amazon S3 bucket. Set the IAM role as the AWS Lambda function's execution role. Make sure that the bucket policy also grants access to the AWS Lambda function's execution role Create an IAM role for the AWS Lambda function that grants access to the Amazon S3 bucket. Set the IAM role as the Lambda function's execution role and that would give the AWS Lambda function cross-account access to the Amazon S3 bucket AWS Lambda cannot access resources across AWS accounts. Use Identity federation to work around this limitation of Lambda The Amazon S3 bucket owner should make the bucket public so that it can be accessed by the AWS Lambda function in the other AWS account

Correct Option:

- **Create an IAM role for the AWS Lambda function that grants access to the Amazon S3 bucket. Set the IAM role as the AWS Lambda function's execution role. Make sure that the bucket policy also grants access to the AWS Lambda function's execution role:**
    - **Technology Involved:** AWS Lambda, Amazon S3, IAM Roles, Bucket Policies
    - **Relevant Use Cases:** This approach ensures that the Lambda function in account A has the necessary permissions to access the S3 bucket in account B. You need to create an IAM role with the required permissions and set it as the execution role for the Lambda function. Additionally, you must update the bucket policy in account B to allow access from the Lambda function's execution role. This setup allows cross-account access securely and efficiently.

Incorrect Options:

- **AWS Lambda cannot access resources across AWS accounts. Use Identity federation to work around this limitation of Lambda:**
    - **Technology Involved:** AWS Lambda, Identity Federation
    - **Explanation:** This statement is incorrect. AWS Lambda can access resources across accounts using the appropriate IAM roles and policies, making identity federation unnecessary for this scenario.
- **Create an IAM role for the AWS Lambda function that grants access to the Amazon S3 bucket. Set the IAM role as the Lambda function's execution role and that would give the AWS Lambda function cross-account access to the Amazon S3 bucket:**
    - **Technology Involved:** AWS Lambda, IAM Roles
    - **Explanation:** While creating an IAM role for the Lambda function and setting it as the execution role is part of the solution, this option misses the crucial step of updating the S3 bucket policy in account B to allow access from the Lambda function's execution role in account A. Both steps are necessary for cross-account access.
- **The Amazon S3 bucket owner should make the bucket public so that it can be accessed by the AWS Lambda function in the other AWS account:**
    - **Technology Involved:** Amazon S3

• **Explanation:** Making the S3 bucket public is a security risk and not recommended for this use case. It exposes the bucket to anyone on the internet, not just the Lambda function in the other account. Proper permissions should be configured using IAM roles and bucket policies to ensure secure access.

Question 55Correct
For security purposes, a development team has decided to deploy the Amazon EC2 instances in a private subnet. The team plans to use VPC endpoints so that the instances can access some AWS services securely. The members of the team would like to know about the two AWS services that support Gateway Endpoints. As a solutions architect, which of the following services would you suggest for this requirement? (Select two)
Your selection is correct
Amazon S3

Amazon Simple Notification Service (Amazon SNS)
Your selection is correct
Amazon DynamoDB
Amazon Kinesis
Amazon Simple Queue Service (Amazon SQS)

Explanation

Correct Options:

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

Technology Involved: VPC Endpoints, Gateway Endpoints, Amazon S3, Amazon DynamoDB

Relevant Use Cases:

- **Amazon S3:** VPC endpoints allow instances in a VPC to securely access Amazon S3 without needing a public IP address or traversing the internet. A gateway endpoint is specified in the route table and routes traffic destined to S3.
- **Amazon DynamoDB:** Similar to Amazon S3, VPC endpoints allow secure access to DynamoDB within a VPC using a gateway endpoint. This setup enhances security and performance by keeping the traffic within the AWS network.

Incorrect Options:

- **Amazon Simple Queue Service (Amazon SQS)**
- **Amazon Simple Notification Service (Amazon SNS)**
- **Amazon Kinesis**

Technology Involved: VPC Endpoints, Interface Endpoints, Amazon SQS, Amazon SNS, Amazon Kinesis

Explanation: These services (Amazon SQS, Amazon SNS, and Amazon Kinesis) use interface endpoints instead of gateway endpoints. Interface endpoints are Elastic Network Interfaces (ENIs) with private IP addresses that serve as entry points for traffic destined for supported services. Therefore, they do not meet the requirement for services that support gateway endpoints.

Conclusion:

For securely accessing services like Amazon S3 and Amazon DynamoDB from instances in a private subnet using VPC endpoints, you should use gateway endpoints. Other services typically utilize interface endpoints for secure access within a VPC.

Question 56Incorrect
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?
Your answer is incorrect
Use AWS EMR to replicate the data from the databases into Amazon Redshift
Use AWS Glue to replicate the data from the databases into Amazon Redshift
Correct answer
Use AWS Database Migration Service (AWS DMS) to replicate the data from the databases into Amazon Redshift Use Amazon Kinesis Data Streams to replicate the data from the databases into Amazon Redshift

Explanation

Correct Option:

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

Technology Involved: AWS Database Migration Service (AWS DMS), Amazon Redshift

Relevant Use Cases:

- **AWS DMS:** AWS Database Migration Service helps you migrate databases to AWS quickly and securely. It minimizes downtime to applications by keeping the source database fully operational during migration. It supports continuous data replication, which is ideal for consolidating multiple databases into a single data warehouse. AWS DMS is capable of migrating data from various sources to Amazon Redshift, leveraging Amazon S3 for intermediate storage before loading data into Redshift.
- **Amazon Redshift:** Amazon Redshift is a fully managed, petabyte-scale data warehouse service in the cloud. It is designed for large-scale data storage and analytics, making it suitable for business analytics that require petabyte-scale data consolidation and processing.

Incorrect Options:

- **Use AWS Glue to replicate the data from the databases into Amazon Redshift:** AWS Glue is a fully managed ETL (extract, transform, load) service for preparing and loading data for analytics. However, it is typically used for batch processing rather than continuous replication. Using AWS Glue would involve significant development efforts to create custom migration scripts, making it less efficient for this use case.
- **Use AWS EMR to replicate the data from the databases into Amazon Redshift:** Amazon EMR (Elastic MapReduce) is used for big data processing with tools like Apache Spark and Hadoop. While powerful for large-scale data processing, EMR requires considerable infrastructure management and development effort to set up and maintain clusters, as well as to write custom jobs for data migration.
- **Use Amazon Kinesis Data Streams to replicate the data from the databases into Amazon Redshift:** Amazon Kinesis Data Streams is a real-time data streaming service. It is designed to capture and process continuous data streams from various sources. However, setting up Kinesis for database replication to Redshift involves complex shard management and does not directly address the need for consolidating relational databases into a data warehouse.

Conclusion

Using AWS Database Migration Service (AWS DMS) to replicate the data from the databases into Amazon Redshift is the most resource-efficient solution requiring the least amount of development time. AWS DMS simplifies the process by continuously replicating data with minimal downtime and handling the data transfer to Amazon Redshift in a managed way.

Question 57Correct
A company wants to store business-critical data on Amazon Elastic Block Store (Amazon EBS) volumes which provide persistent storage independent of Amazon EC2 instances. During a test run, the development team found that on terminating an Amazon EC2 instance, the attached Amazon EBS volume was also lost, which was contrary to their assumptions.
As a solutions architect, could you explain this issue?
On termination of an Amazon EC2 instance, all the attached Amazon EBS volumes are always terminated The Amazon EBS volumes were not backed up on Amazon EFS file system storage, resulting in the loss of volume The Amazon EBS volumes were not backed up on Amazon S3 storage, resulting in the loss of volume
Your answer is correct
The Amazon EBS volume was configured as the root volume of Amazon EC2 instance. On termination of the instance, the default behavior is to also terminate the attached root volume
Explanation

Correct Option:

- **The Amazon EBS volume was configured as the root volume of Amazon EC2 instance. On termination of the instance, the default behavior is to also terminate the attached root volume**

Technology Involved: Amazon Elastic Block Store (Amazon EBS)

Relevant Use Cases:

- **Amazon EBS:** Amazon Elastic Block Store (EBS) is designed to provide persistent block storage for Amazon EC2 instances. EBS volumes are independent of the lifecycle of the EC2 instances to which they are attached, allowing them to persist beyond the life of the instance itself. However, this persistence depends on the configuration of the volume.

Scenario Explanation:

- When an Amazon EC2 instance is launched, it typically includes a root device volume that contains the boot image. This root volume is essential for the instance's operation. By default, if the root volume is an EBS volume, it is configured to be deleted upon the termination of the instance. This default behavior ensures that the boot volume is cleaned up when the instance is no longer needed.
- Non-root EBS volumes, however, are not deleted by default when an instance terminates. They remain available for reattachment to other instances or for other uses.
- If the requirement is to retain the root volume after the instance is terminated, the "Delete on Termination" attribute can be modified to ensure that the root volume persists beyond the instance's termination.

Incorrect Options:

- **The Amazon EBS volumes were not backed up on Amazon S3 storage, resulting in the loss of volume**
- **The Amazon EBS volumes were not backed up on Amazon EFS file system storage, resulting in the loss of volume**

These options are distractors because EBS volumes do not need to be backed up on Amazon S3 or Amazon EFS to persist beyond the life of an instance. Persistence of the EBS volume is managed by its configuration, not by backing up to other storage services.

- **On termination of an Amazon EC2 instance, all the attached Amazon EBS volumes are always terminated**

This statement is incorrect because only the root EBS volume is deleted by default upon instance termination. Other attached EBS volumes (non-root) are not automatically deleted and will remain available for future use.

Question 58Incorrect
A retail company wants to rollout and test a blue-green deployment for its global application in the next 48 hours. Most of the customers use mobile phones which are prone to Domain Name System (DNS) caching. The company has only two days left for the annual Thanksgiving sale to commence.

As a Solutions Architect, which of the following options would you recommend to test the deployment on as many users as possible in the given time frame?
Correct answer
Use AWS Global Accelerator to distribute a portion of traffic to a particular Deployment Use AWS CodeDeploy deployment options to choose the right deployment Use Elastic Load Balancing (ELB) to distribute traffic across deployments Your answer is incorrectUse Amazon Route 53 weighted routing to spread traffic across different Deployments

Explanation

Correct Option:

- **Use AWS Global Accelerator to distribute a portion of traffic to a particular deployment**

Technology Involved: AWS Global Accelerator

Relevant Use Cases:

- **Blue/Green Deployment:** This deployment strategy involves running two identical environments, one being the current version (blue) and the other being the new version (green). Traffic is gradually shifted from blue to green, allowing for testing and minimizing downtime and rollback risks.
- **AWS Global Accelerator:** This service provides a static IP address that serves as a fixed entry point to your application endpoints, improving availability and performance by using the AWS global network. It allows you to control traffic flow using endpoint weights and traffic dials, which are effective within seconds and are not affected by DNS caching issues.

Scenario Explanation:

- **AWS Global Accelerator:** This service is ideal for blue/green deployments, especially in scenarios where quick and controlled traffic transition is crucial. Unlike DNS-based routing, AWS Global Accelerator is not prone to DNS caching, which can delay the transition. It uses static anycast IP addresses, ensuring immediate changes in traffic distribution when needed.
- **DNS Caching Issue:** DNS caching can cause delays in traffic transition, as some client devices and internet resolvers cache DNS answers for long periods. This makes DNS-based solutions like Route 53 less effective for rapid deployment scenarios.

Incorrect Options:

- **Use Amazon Route 53 weighted routing to spread traffic across different deployments**
  - **DNS Caching:** Route 53's weighted routing allows traffic distribution based on assigned weights, but it relies on DNS. DNS caching can delay the propagation of changes, making it unsuitable for scenarios requiring immediate traffic transition.
- **Use Elastic Load Balancing (ELB) to distribute traffic across deployments**
  - **Scope Limitation:** ELB can distribute traffic within a single region. For a global application requiring a multi-region solution, ELB is not suitable.
- **Use AWS CodeDeploy deployment options to choose the right deployment**
  - **Traffic Distribution:** AWS CodeDeploy focuses on deploying application content and managing deployment strategies, including blue/green deployments. However, it does not handle traffic distribution across instances or regions, which is essential for this scenario.

Using AWS Global Accelerator ensures that traffic can be shifted quickly and effectively between different environments, overcoming the limitations of DNS caching and providing a robust solution for global application deployments.

Question 59Correct
An organization wants to delegate access to a set of users from the development environment so that they can access some resources in the production environment which is managed under another AWS account. As a solutions architect, which of the following steps would you recommend?
Your answer is correct
Create a new IAM role with the required permissions to access the resources in the production environment. The users can then assume this IAM role while accessing the resources from the production environment Both IAM roles and IAM users can be used interchangeably for cross-account access It is not possible to access cross-account resources Create new IAM user credentials for the production environment and share these credentials with the set of users from the development environment

Explanation

Correct Option:

- **Create a new IAM role with the required permissions to access the resources in the production environment. The users can then assume this IAM role while accessing the resources from the production environment.**

Technology Involved: AWS Identity and Access Management (IAM)

Relevant Use Cases:

- **Cross-Account Access:** IAM roles are designed to grant permissions to access resources across AWS accounts. By creating an IAM role in the production account with the necessary permissions and allowing users from the development account to assume that role, secure and controlled access can be provided without sharing long-term credentials.

- **Temporary Security Credentials:** When users assume an IAM role, they receive temporary security credentials, which enhance security by reducing the risk associated with long-term credentials.

Scenario Explanation:

- **IAM Roles for Cross-Account Access:** IAM roles enable you to grant access to resources in one AWS account (production) to users or services in another AWS account (development). This approach is secure and manageable as it leverages temporary credentials and the principle of least privilege.
- **Role Assumption:** Users in the development account can assume the IAM role in the production account, which provides them with the necessary permissions to access specific resources. This method avoids the need to create and distribute new IAM user credentials.

Incorrect Options:

- **Create new IAM user credentials for the production environment and share these credentials with the set of users from the development environment**
  - **Security Risks:** Sharing IAM user credentials is not a best practice as it increases security risks and makes credential management more difficult. IAM roles are a more secure and scalable solution.
- **It is not possible to access cross-account resources**
  - **Incorrect Statement:** AWS supports cross-account access through IAM roles. This allows for secure and controlled resource sharing between different AWS accounts.
- **Both IAM roles and IAM users can be used interchangeably for cross-account access**
  - **Roles vs. Users:** IAM roles and IAM users are distinct entities with different purposes. IAM roles are designed for cross-account access and providing temporary permissions, while IAM users are intended for long-term access within a single account. They are not interchangeable for cross-account access.

Using IAM roles for cross-account access provides a secure and efficient way to manage permissions, ensuring that access is granted appropriately without the need for sharing long-term credentials. This approach aligns with AWS best practices for security and resource management.

Question 60Incorrect
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 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 answer
Traffic is routed to instances using the primary private IP address specified in the primary network interface for the instance
Traffic is routed to instances using the instance ID specified in the primary network interface for the instance Traffic is routed to instances using the primary public IP address specified in thprimary network interface for the instance Your answer is incorrect Traffic is routed to instances using the primary elastic IP address specified in the primary network interface for the instance

Explanation

Correct Option:

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

Technology Involved: Network Load Balancer (NLB) on AWS

Relevant Use Cases:

- **High-Performance Load Balancing:** NLBs are designed to handle millions of requests per second, making them suitable for applications with high traffic demands, such as online gaming platforms.
- **Layer 4 Load Balancing:** NLB operates at the transport layer (Layer 4) of the OSI model, focusing on managing TCP/UDP connections and routing traffic based on IP addresses and ports.

Scenario Explanation:

- **Instance ID Target Specification:** When you specify instances as targets using their instance IDs, the NLB routes traffic to these instances based on their primary private IP addresses. The load balancer rewrites the destination IP address to the instance’s private IP before forwarding the request.
- **Private IP Address:** Using the primary private IP address ensures that traffic remains within the AWS network, which enhances security and performance by avoiding public internet routing.

Incorrect Options:

- **Traffic is routed to instances using the primary public IP address specified in the primary network interface for the instance**
  - **Public IP Address:** Public IP addresses are not used for routing traffic by NLB when instances are specified by their instance IDs. Public IPs are primarily for external access and do not serve the purpose of internal AWS network traffic routing.
- **Traffic is routed to instances using the primary elastic IP address specified in the primary network interface for the instance**

- **Elastic IP Address:** Elastic IPs are static public IP addresses associated with instances or network interfaces for external access. They are not utilized for routing internal traffic within the AWS network when using instance IDs as targets.

- **Traffic is routed to instances using the instance ID specified in the primary network interface for the instance**
  - **Instance ID:** While the instance ID is used to identify targets in the configuration, the actual routing to instances is based on their primary private IP addresses. The instance ID itself is not used for the routing mechanism.

Using the primary private IP address for routing traffic ensures efficient and secure handling of requests within the AWS network, leveraging the internal IP addressing scheme. This approach aligns with AWS best practices for internal traffic management and load balancing.

Question 61Incorrect
A media agency stores its re-creatable assets on Amazon Simple Storage Service (Amazon S3) buckets. The assets are accessed by a large number of users for the first few days and the frequency of access falls down drastically after a week. Although the assets would be accessed occasionally after the first week, but they must continue to be immediately accessible when required. The cost of maintaining all the assets on Amazon S3 storage is turning out to be very expensive and the agency is looking at reducing costs as much as possible. As an AWS Certified Solutions Architect – Associate, can you suggest a way to lower the storage costs while fulfilling the business requirements? Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 7 days Your answer is incorrect Configure a lifecycle policy to transition the objects to Amazon S3 Standard- Infrequent Access (S3 Standard-IA) after 30 days Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 7 days Correct answer Configure a lifecycle policy to transition the objects to Amazon S3 One Zone- Infrequent Access (S3 One Zone-IA) after 30 days

Explanation

Correct Option:

- **Create a new IAM role with the required permissions to access the resources in the production environment. The users can then assume this IAM role while accessing the resources from the production environment.**

Technology Involved: AWS Identity and Access Management (IAM)

Relevant Use Cases:

- **Cross-Account Access:** IAM roles are designed to grant permissions to access resources across AWS accounts. By creating an IAM role in the production account with the necessary permissions and allowing users from the development account to assume that role, secure and controlled access can be provided without sharing long-term credentials.
- **Temporary Security Credentials:** When users assume an IAM role, they receive temporary security credentials, which enhance security by reducing the risk associated with long-term credentials.

Scenario Explanation:

- **IAM Roles for Cross-Account Access:** IAM roles enable you to grant access to resources in one AWS account (production) to users or services in another AWS account (development). This approach is secure and manageable as it leverages temporary credentials and the principle of least privilege.
- **Role Assumption:** Users in the development account can assume the IAM role in the production account, which provides them with the necessary permissions to access specific resources. This method avoids the need to create and distribute new IAM user credentials.

Incorrect Options:

- **Create new IAM user credentials for the production environment and share these credentials with the set of users from the development environment**
  - **Security Risks:** Sharing IAM user credentials is not a best practice as it increases security risks and makes credential management more difficult. IAM roles are a more secure and scalable solution.
- **It is not possible to access cross-account resources**
  - **Incorrect Statement:** AWS supports cross-account access through IAM roles. This allows for secure and controlled resource sharing between different AWS accounts.
- **Both IAM roles and IAM users can be used interchangeably for cross-account access**
  - **Roles vs. Users:** IAM roles and IAM users are distinct entities with different purposes. IAM roles are designed for cross-account access and providing temporary permissions, while IAM users are intended for long-term access within a single account. They are not interchangeable for cross-account access.

Using IAM roles for cross-account access provides a secure and efficient way to manage permissions, ensuring that access is granted appropriately without the need for sharing long-term credentials. This approach aligns with AWS best practices for security and resource management.

Question 62Incorrect
A media company has created an AWS Direct Connect connection for migrating its flagship application to the AWS Cloud. The on-premises application writes hundreds of video files into a mounted NFS file system daily. Post migration, the company will host the application on an Amazon EC2 instance with a mounted Amazon Elastic File System (Amazon EFS) file system. Before the migration cutover, the company must build a process that will

replicate the newly created on-premises video files to the Amazon EFS file system. Which of the following represents the MOST operationally efficient way to meet this requirement?
Correct answer
Configure an AWS DataSync agent on the on-premises server that has access to the NFS file system. Transfer data over the AWS Direct Connect connection to an AWS PrivateLink interface VPC endpoint for Amazon EFS by using a private VIF. Set up an AWS Data Sync scheduled task to send the video files to the Amazon EFS file systemevery 24 hours
Your answer is incorrect
Configure an AWS DataSync agent on the on-premises server that has access to the NFS file system. Transfer data over the AWS Direct Connect connection to an Amazon S3 bucket by using public VIF. Set up an AWS Lambda function to process event notifications from Amazon S3 and copy the video files from Amazon S3 to the Amazon EFS file system Configure an AWS DataSync agent on the on-premises server that has access to the NFS file system. Transfer data over the AWS Direct Connect connection to an Amazon S3 bucket by using a VPC gateway endpoint for Amazon S3. Set up an AWS Lambda function to process event notifications from Amazon S3 and copy the video files from Amazon S3 to the Amazon EFS file system Configure an AWS DataSync agent on the on-premises server that has access to the NFS file system. Transfer data over the AWS Direct Connect connection to an AWS VPC peering endpoint for Amazon EFS by using a private VIF. Set up an AWS DataSync scheduled task to send the video files to the Amazon EFS file system every 24 hours

Correct answer:

Configure an AWS DataSync agent on the on-premises server that has access to the NFS file system. Transfer data over the AWS Direct Connect connection to an AWS PrivateLink interface VPC endpoint for Amazon EFS by using a private VIF. Set up an AWS DataSync scheduled task to send the video files to the Amazon EFS file system every 24 hours.

Overall Explanation:

Correct Option:

- **AWS DataSync with AWS PrivateLink:**
  - AWS DataSync simplifies, automates, and accelerates copying large amounts of data between on-premises storage systems and AWS storage services.
  - You can use AWS DataSync to migrate data located on-premises to Amazon S3, Amazon EFS, and other AWS storage services.
  - By configuring an AWS DataSync agent on the on-premises server and using AWS Direct Connect with a private VIF to transfer data to an AWS PrivateLink interface VPC endpoint for Amazon EFS, you can efficiently and securely transfer the data. This setup ensures that the data is transferred over a private network, improving security and efficiency.
  - Scheduling tasks in AWS DataSync to run every 24 hours ensures that the data is regularly synced without manual intervention.

Incorrect Options:

- **AWS DataSync with VPC Peering Endpoint:**
  - VPC peering is a networking connection between two VPCs that enables routing traffic between them privately. It cannot be used to transfer data over Direct Connect from on-premises systems to AWS.
- **AWS DataSync with Public VIF to Amazon S3:**
  - While this is theoretically possible, it is not operationally efficient. It involves an additional step of sending data to Amazon S3 and then using an AWS Lambda function to move data to Amazon EFS, increasing complexity.
- **AWS DataSync with VPC Gateway Endpoint for Amazon S3:**
  - VPC gateway endpoints are used to access Amazon S3 from a VPC, but they cannot be used to transfer data over Direct Connect from on-premises systems to Amazon S3.

Technology Involved and Relevant Use Cases:

- **AWS DataSync:** Used for online data transfer to simplify, automate, and accelerate data copying between on-premises and AWS storage services.
- **AWS PrivateLink:** Provides secure and private connectivity between VPCs and AWS services, bypassing the public internet.
- **AWS Direct Connect:** Offers a dedicated network connection from on-premises to AWS, providing consistent and reliable performance.
- **Amazon EFS:** A scalable, elastic file system for use with AWS Cloud services and on-premises resources.

By leveraging these technologies, the company can ensure efficient, secure, and automated data transfer from their on-premises NFS file system to Amazon EFS on AWS.

Question 63Incorrect
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? 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 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 Correct answer Use Amazon Kinesis Data Streams to process the data streams as well as decouple the producers and consumers for the real-time data processor Your answer is incorrect Use Amazon Kinesis Data Firehose to process the data streams as well as decouple the producers and consumers for the real-time data processor

Correct Option:

- **Amazon Kinesis Data Streams**

Amazon Kinesis Data Streams is designed to enable you to build custom, real-time applications that process or analyze streaming data for specialized needs. It is highly scalable and can handle a large amount of data from numerous sources such as website clickstreams, database event streams, financial transactions, social media feeds, IT logs, and location-tracking events. Kinesis Data Streams also allow for the separation of data producers and consumers, providing the necessary decoupling for effective real-time data processing.

Incorrect Options:

- **Amazon Simple Notification Service (Amazon SNS)**: SNS is a fully managed pub/sub messaging service that decouples microservices, distributed systems, and serverless applications. It is not designed to handle real-time data processing needs as required in this use case.
- **Amazon Simple Queue Service (Amazon SQS)**: SQS is used to decouple the components of a cloud application. While it can handle the decoupling of producers and consumers, it is not suitable for real-time data stream processing.
- **Amazon Kinesis Data Firehose**: Kinesis Data Firehose is used for loading streaming data into data lakes, data stores, and analytics services. It can capture, transform, and load streaming data into services like Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk. However, it does not support custom real-time processing and analysis as required.

Technology Involved and Relevant Use Cases:

- **Amazon Kinesis Data Streams**:
  - **Use Cases**: Real-time applications requiring high data throughput and low-latency processing. Ideal for monitoring, analytics, log and event data processing.
  - **Features**: Custom application development, real-time analytics, high scalability.
- **Amazon Simple Notification Service (Amazon SNS)**:
  - **Use Cases**: Messaging between distributed systems, sending notifications.
  - **Features**: Pub/Sub messaging, decoupling of microservices.
- **Amazon Simple Queue Service (Amazon SQS)**:
  - **Use Cases**: Decoupling of system components, message queuing.
  - **Features**: Secure, durable message queue service.
- **Amazon Kinesis Data Firehose**:
  - **Use Cases**: Data ingestion and loading into data stores and analytics services.
  - **Features**: Stream capture, transformation, and loading into services like S3, Redshift, Elasticsearch, and Splunk.

These distinctions make Amazon Kinesis Data Streams the optimal solution for building custom real-time data processing applications as per the requirements described.

Question 64Incorrect
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 addressthis use-case? Use Network Address Translation (NAT) instance to access Amazon SQS Your answer is incorrect Use Internet Gateway to access Amazon SQS Use VPN connection to access Amazon SQS Correct answerUse VPC endpoint to access Amazon SQS

Overall Explanation

Correct Option:

- **Use VPC endpoint to access Amazon SQS**

Amazon VPC endpoints allow you to connect your VPC to AWS services such as Amazon SQS without requiring an Internet gateway, NAT instance, VPN connection, or AWS Direct Connect connection. This connection is facilitated through AWS PrivateLink, which offers secure and scalable technology to connect VPCs privately to supported AWS services. With VPC endpoints, all communication between your VPC and Amazon SQS occurs within the AWS network, eliminating exposure to the public internet and enhancing security.

Incorrect Options:

- **Use Internet Gateway to access Amazon SQS**: An Internet Gateway allows communication between instances in your VPC and the internet. However, using an Internet Gateway would expose the data to the public internet, which the engineering team wants to avoid.
- **Use VPN connection to access Amazon SQS**: A VPN connection securely connects your on-premises network or branch office to your Amazon VPC. Since the scenario involves AWS resources within the AWS Cloud, a VPN connection is unnecessary and adds complexity.
- **Use Network Address Translation (NAT) instance to access Amazon SQS**: NAT instances allow instances in a private subnet to access the internet while preventing inbound traffic initiated from the internet. Using a NAT instance involves public internet usage, which does not meet the requirement of avoiding the public internet to access Amazon SQS.

Technology Involved and Relevant Use Cases:

- **Amazon VPC Endpoint**:
  - **Use Cases**: Securely access AWS services from a VPC without using public IPs or traversing the internet. Ideal for scenarios where enhanced security and private connectivity are required.
  - **Features**: Private connectivity, enhanced security, easy configuration, reliable connection within AWS network.
- **Internet Gateway**:
  - **Use Cases**: Enabling internet access to and from instances in a VPC. Not suitable for scenarios where internet exposure needs to be avoided.
  - **Features**: Horizontal scalability, high availability, allows communication between VPC instances and the internet.
- **VPN Connection**:
  - **Use Cases**: Securely connect on-premises networks to AWS VPCs. Adds unnecessary complexity for intra-AWS cloud connections.
  - **Features**: Encrypted connectivity, secure connection over the internet, suitable for connecting on-premises environments to AWS.
- **NAT Instance**:
  - **Use Cases**: Allow instances in private subnets to access the internet without exposing them to inbound internet traffic. Not suitable when avoiding public internet usage for accessing AWS services.
  - **Features**: Outbound internet access for private subnet instances, prevents inbound internet-initiated traffic, requires management of NAT instance.

These distinctions make VPC endpoints the optimal solution for securely accessing Amazon SQS without using the public internet, as per the requirements described.

Question 65Incorrect
An engineering team wants to examine the feasibility of the user data feature of Amazon EC2 for an upcoming project.
Which of the following are true about the Amazon EC2 user data configuration? (Select two)
Correct selection
By default, scripts entered as user data are executed with root user privileges
Correct selection
By default, user data runs only during the boot cycle when you first launch an Instance When an instance is running, you can update user data by using root user credentials Your selection is incorrect By default, scripts entered as user data do not have root user privileges for executing Your selection is incorrect By default, user data is executed every time an Amazon EC2 instance is re-started

Overall Explanation

Correct Options:

- **By default, scripts entered as user data are executed with root user privileges**

When you launch an EC2 instance with user data, the scripts provided in the user data are executed as the root user. This means they run with root privileges, and you don't need to use the sudo command within the script. Any files created by the script will be owned by root, and you should modify file permissions within the script if non-root users need access.

- **By default, user data runs only during the boot cycle when you first launch an instance**

User data scripts and cloud-init directives are designed to run only once during the instance's initial boot cycle by default. This allows for initial setup and configuration of the instance. However, you can configure the instance to run these scripts again on every reboot if needed.

Incorrect Options:

- **By default, user data is executed every time an Amazon EC2 instance is re-started**

This statement is incorrect because, by default, user data scripts are not re-executed when an instance is restarted. They run only once during the initial boot cycle unless you explicitly configure them to run on every restart.

- **When an instance is running, you can update user data by using root user credentials**

While you can view the user data of a running instance, you cannot change or update it while the instance is running. User data is set during the instance launch and remains unchanged thereafter.

- **By default, scripts entered as user data do not have root user privileges for executing**

This is incorrect. Scripts entered as user data are executed with root user privileges by default, meaning they run with the highest level of access on the instance.

Technology Involved and Relevant Use Cases:

- **Amazon EC2 User Data**:
  - **Use Cases**: Automating instance setup, running initialization scripts, installing software, and performing configuration tasks during the first boot.

- **Features**: Executes with root privileges, runs only during the first boot by default, can be configured to run on every boot, and supports both shell scripts and cloud-init directives.

These explanations clarify why the correct options are valid and why the incorrect options do not meet the stated conditions.