Solutions Architect Professional Questions 5

Question 1

A company managing their web application on AWS is facing challenges in ensuring efficient resource utilization across multiple Availability Zones (AZs) during peak load times. Their current setup involves Application Load Balancers, EC2 instances across three AZs, and a mix of Reserved and On-Demand Instances. The goal is to revise the architecture for quick recovery in case an AZ becomes unavailable during peak load, while also ensuring cost-effectiveness. Here are the proposed strategies:

A. Utilize both Reserved and On-Demand instances in each AZ to manage both steady-state and peak loads.

B. Set up an Auto Scaling group of Reserved instances in each AZ for peak loads, maintaining the current approach for steady-state loads.

C. Implement a mix of Spot and On-Demand instances in each AZ for both steady-state and peak loads.

D. Launch a Spot Fleet using a diversified allocation strategy, with Auto Scaling enabled in each AZ for peak loads, replacing On-Demand instances. Retain the current setup for steady-state loads.

Correct Answer: D

Explanation of the Correct Answer and Analysis of Other Options:

- Why D is Correct:
  - Spot Fleet and Diversified Allocation Strategy: A Spot Fleet in AWS is a collection of Spot Instances and, optionally, On-Demand Instances. The fleet attempts to meet the capacity specified by the user, based on certain criteria like price, availability, and instance types. By using a diversified allocation strategy, the Spot Fleet distributes instances across different Availability Zones and instance types. This diversification enhances fault tolerance, as it reduces the likelihood of a significant impact on the application's availability if one AZ or a particular instance type experiences an interruption.
  - Auto Scaling for Dynamic Response: Auto Scaling in the context of a Spot Fleet allows the fleet to automatically adjust its size in response to changing demands, particularly useful during peak load times. This means the application can scale out (add more instances) when demand increases, and scale in (reduce instances) when

demand decreases, ensuring that only the necessary resources are used and paid for.

  - Cost-Effectiveness of Spot Instances: Spot Instances are available at up to a 90% discount compared to On-Demand prices. They are ideal for flexible, fault-tolerant applications that can withstand possible instance terminations (which occur when the Spot price exceeds the bid price).
  - Retaining Steady-State Load Setup: By keeping the existing architecture for handling steady-state loads, the system leverages the predictability and cost savings of Reserved Instances, which are ideal for baseline usage with their fixed pricing model. In the context of this explanation and scenario, a "steady-state load" refers to the normal, predictable level of demand or traffic that a web application experiences. This is the baseline level of resource utilization that remains relatively constant over time, as opposed to peak loads which are characterized by significant, often unpredictable spikes in demand.
  - Quick Recovery in AZ Unavailability: The combination of Spot Fleet's diversified allocation and Auto Scaling's dynamic nature ensures that the application can quickly recover from an AZ outage. If one AZ becomes unavailable, the Spot Fleet can automatically redistribute instances to other available AZs, maintaining application performance and availability.
- Why Other Options are Incorrect:
  - A: Solely relying on a combination of Reserved and On-Demand instances in each AZ doesn't provide the flexibility and cost-effectiveness of Spot instances, especially during unpredictable peak loads.
  - B: Using Reserved instances in Auto Scaling groups for peak loads could be less cost-effective than Spot instances and may not provide the necessary flexibility for dynamic scaling.
  - C: While Spot and On-Demand instances provide cost savings and flexibility, solely relying on this combination without a diversified Spot Fleet strategy may lead to potential availability issues during peak loads or if an AZ goes down.

Question 2

A federal agency operates several Virtual Private Clouds (VPCs) across different AWS regions in the United States and needs to connect these to their main office in Washington, D.C. The requirement is for each region's VPC to have a private, dedicated network link to the central office, ensuring enhanced security and stable data transfer performance. The challenge is to efficiently establish and manage this extensive network connectivity.

The best approach to achieve secure, highly available, and robust interconnectivity would be:

A. Set up a Link Aggregation Group (LAG) at the central office to consolidate multiple connections into a single managed connection at an AWS Direct Connect endpoint. Utilize AWS Direct Connect Gateway for inter-region VPC access, establish a virtual private gateway in each VPC, and create public virtual interfaces for each connection to the Direct Connect Gateway.

B. Implement a hub-and-spoke network model in each region, directing all traffic through a centralized network transit center using AWS Transit Gateway, and route traffic between VPCs and the on-premise network over AWS Site-to-Site VPN.

C. Employ AWS Direct Connect Gateway for inter-region VPC access. Install a virtual private gateway in each VPC, and establish a private virtual interface for every AWS Direct Connect link to the Direct Connect gateway.

D. Activate inter-region VPC peering, enabling peering connections between VPCs in different AWS regions. This ensures all traffic remains on the AWS global backbone and does not travel over the public Internet.

Correct Answer: C

Explanation of the Correct Answer and Analysis of Other Options:

- Why C is Correct:
  - AWS Direct Connect Gateway for Inter-Region VPC Access: This method leverages AWS Direct Connect Gateway, which allows for the establishment of a private, dedicated network connection between the AWS environment and the on-premise network. This setup is crucial for enhanced security and consistent data transfer performance.
  - Private Virtual Interface for Enhanced Security: By creating a private virtual interface for each Direct Connect link, this approach ensures that data does not traverse the public internet, maintaining a high level of security.
  - Virtual Private Gateway in Each VPC: Setting up a virtual private gateway in each VPC provides a secure, private tunnel between the VPC and the Direct Connect gateway, further enhancing security and reliability.
  - Minimized Management Overhead: This solution streamlines network management by using Direct Connect Gateways, reducing the complexity associated with handling multiple connections and regions.
- Why Other Options are Incorrect:
  - A: While LAG and Direct Connect provide a high bandwidth and reliable connection, using public virtual interfaces might not offer the same level of security as private interfaces. Additionally, this setup might be more complex to manage.

- B: A hub-and-spoke model using AWS Transit Gateway and Site-to-Site VPN is a viable solution for connecting multiple VPCs. However, it may not offer the same level of dedicated, high-performance connectivity as Direct Connect and might have higher latency and lower throughput.
- D: Inter-region VPC peering is a secure and efficient way to connect VPCs across regions, but it does not directly connect to the on-premise network. Also, it lacks the dedicated bandwidth and consistent performance provided by Direct Connect.

Question 3

A private bank operates a secure web application for its agents to access highly sensitive client information. The web traffic is constant and predictable, and the application employs SSL for data security. The Chief Information Security Officer (CISO) is particularly concerned about safeguarding the SSL private key to ensure it remains within the corporate boundaries. Additionally, the solutions architect is focused on the secure and durable storage of application logs, which might contain sensitive data. The data on EBS volumes is already encrypted, but there's a need to ensure that only authorized personnel can decrypt the application logs.

The optimal architecture to meet these security and availability requirements would be:

A. Route web traffic through an Elastic Load Balancer, uploading the SSL private key to the load balancer for SSL offloading. Store application logs on an encrypted instance store volume, using a randomly generated AES key.

B. Utilize an Elastic Load Balancer for TCP load balancing, employing CloudHSM in two Availability Zones for SSL processing. Securely store application logs in a private Amazon S3 bucket with server-side encryption.

C. Use an Elastic Load Balancer with TCP load balancing, retrieving the SSL private key from a private Amazon S3 bucket during server boot-up. Store web server logs in a separate private Amazon S3 bucket, using Amazon S3 server-side encryption.

D. Distribute traffic via an Elastic Load Balancer performing TCP load balancing, and process SSL transactions using AWS CloudHSM. Send application logs to a private Amazon S3 bucket, encrypted server-side.

Correct Answer: B

Explanation of the Correct Answer and Analysis of Other Options:

- Why B is Correct:

  - TCP Load Balancing with Elastic Load Balancer: This approach ensures efficient distribution of web traffic across multiple servers, offering high availability and fault tolerance.
  - CloudHSM for SSL Transaction Security: Using AWS CloudHSM (Hardware Security Module) deployed across two Availability Zones adds an extra layer of security for SSL transactions. CloudHSM provides dedicated hardware for key management, ensuring that the SSL private key is securely stored and processed within the AWS environment and in compliance with the CISO's concerns.
  - Secure Log Storage in Amazon S3 with Server-Side Encryption: Storing application logs in a private Amazon S3 bucket with server-side encryption offers both security and durability. This method ensures that logs are accessible only to authorized personnel and are protected from unauthorized access or alterations.
- Why Other Options are Incorrect:
  - A: Uploading the SSL private key to the load balancer and storing logs on an instance store volume, even if encrypted, does not offer the same level of security and durability as CloudHSM and Amazon S3. Instance store volumes have a risk of data loss if the underlying instance fails.
  - C: Retrieving the SSL private key from an S3 bucket at boot time poses a security risk, as the key might be exposed during transmission or if the S3 bucket is not properly secured. This method does not fully address the CISO's concern about keeping the key within a controlled environment.
  - D: This option is similar to B but lacks the mention of deploying CloudHSM across two Availability Zones, which is crucial for high availability and fault tolerance in the bank’s scenario.

Question 4

A corporation is leveraging AWS Organizations to administer its extensive, multi-account, multi-region AWS infrastructure. They are in the midst of implementing large-scale automation for their primary daily operations to reduce costs. A crucial part of this automation involves sharing certain AWS resources owned by an organizational account with other company AWS accounts using AWS Resource Access Manager (RAM). Previously, these tasks were overseen by a dedicated organization account moderator, who was responsible for specific configuration details.

To ensure the service can effectively perform its tasks across organization accounts on behalf of the previous moderator, the best solution would be:

A. Establish a service-linked role for AWS RAM and adjust the permissions policy to define the role's capabilities and limitations. Then, amend the role’s trust policy to enable other processes to utilize AWS RAM.

B. Activate cross-account access using AWS Organizations in the Resource Access Manager Console, replicating the configuration adjustments made by the account that previously managed this service.

C. Implement trusted access by executing the `enable-sharing-with-aws-organization` command in the AWS RAM Command Line Interface (CLI). Replicate the configuration changes previously made by the managing account.

D. Assign an IAM role to the service, specifying all permissible actions. Deploy an SSM agent on each worker VM and use AWS Systems Manager to create automation workflows for the daily key processes.

Correct Answer: C

Explanation of the Correct Answer and Analysis of Other Options:

- Why C is Correct:
  - Trusted Access with AWS RAM: Enabling trusted access through the AWS RAM CLI (`enable-sharing-with-aws-organization`) simplifies the process of sharing resources across AWS accounts within the same organization. This command allows the organization to centrally manage shared resources, reducing the complexity involved in individual account configurations.
  - Mirroring Previous Configurations: By replicating the configurations from the account that initially managed the service, the company ensures continuity and consistency in the automation process. This approach leverages existing successful configurations, minimizing the need for extensive reconfiguration.
- Why Other Options are Incorrect:
  - A: While configuring a service-linked role for AWS RAM is a valid approach for certain scenarios, it might not be as straightforward and efficient for sharing resources across multiple accounts as using trusted access with AWS RAM.
  - B: Enabling cross-account access in the RAM Console is part of the solution, but it lacks the specific command (`enable-sharing-with-aws-organization`) that streamlines the process for organization-wide resource sharing.
  - D: Assigning an IAM role and using AWS Systems Manager for workflow automation is more geared towards managing and automating tasks within VMs, rather than focusing on the sharing of resources across accounts using AWS RAM.

Question 5

An IT consultancy firm with offices in San Francisco, Cologne, Tokyo, and Singapore utilizes AWS Organizations to manage various AWS accounts across its regional offices and subsidiaries. Recently, a new AWS account was added to a specific Organizational Unit (OU) responsible for systems administration. This account operates an Amazon ECS Cluster created by the root user, which has an associated service-linked role. For compliance reasons, a solutions architect designed a custom Service Control Policy (SCP) to restrict certain ECS actions for this new account. However, despite applying the policy, the account remained capable of performing the restricted actions.

The primary reason for this issue is:

A. The default SCP grants all permissions to every root, OU, and account. To enforce stricter permissions, this policy must be modified.

B. A higher-level OU has an SCP that allows the actions of the service-linked role. This permission is inherited by the current OU and supersedes the SCP implemented by the administrator.

C. The ECS service operates outside the organization's jurisdiction. SCPs only impact principals managed by accounts within the organization.

D. SCPs do not influence service-linked roles. These roles are designed to facilitate integration of other AWS services with AWS Organizations and cannot be limited by SCPs.

Correct Answer: D

Explanation of the Correct Answer and Analysis of Other Options:

- Why D is Correct:
  - Service-Linked Roles and SCPs: Service-linked roles are specific types of IAM roles created by AWS services to perform actions on behalf of the user. These roles allow AWS services to integrate seamlessly with AWS Organizations. A key characteristic of service-linked roles is that they are not subject to SCPs. This means that even if an SCP is designed to restrict certain actions, these restrictions do not apply to service-linked roles, allowing them to operate as intended by the respective AWS service.
- Why Other Options are Incorrect:
  - A: While the default SCP does grant broad permissions, modifying it would normally restrict permissions across the organization. However, this doesn't apply to service-linked roles, which are exempt from SCP restrictions.
  - B: Although SCPs attached to higher-level OUs can indeed override policies at lower levels, the issue in this scenario specifically relates to the nature of service-linked roles, which are unaffected by any SCPs.
  - C: The jurisdiction of the ECS service or the location of operation is irrelevant in this context. SCPs apply to accounts within an AWS Organization regardless of

geographical location, but again, this does not extend to service-linked roles.

Question 6

A multinational tech company, with multiple Virtual Private Clouds (VPCs) assigned to its IT departments, is using VPC peering for necessary communication between these VPCs. The solutions architect is assigned to launch a new central database server accessible by other VPCs of the company using the domain name database.example.com. This server should be accessible and resolvable only within the associated VPCs, as it is intended solely for internal applications.

The best solution to achieve this would be:

A. Establish a public hosted zone with the domain name example.com and associate it with the desired VPCs. Create an A record for database.example.com pointing to the EC2 instance's IP address of the database server. Modify the enableDnsHostNames and enableDnsSupport attributes of your VPCs to true.

B. Set up a private hosted zone with the domain name example.com, specifying the VPCs for association. Add an A record for database.example.com that maps to the IP address of the database server's EC2 instance. Ensure the enableDnsHostNames and enableDnsSupport attributes of the VPCs are set to true.

C. Configure a private hosted zone with the domain name example.com and designate the VPCs for association. Make an A record for database.example.com linked to the Elastic IP address of the database server's EC2 instance. Set the enableDnsHostNames attribute of your VPCs to true and the enableDnsSupport attribute to false.

D. Create a public hosted zone with the domain name example.com, associating it with specified VPCs. Establish a CNAME record for database.example.com pointing to the EC2 instance's IP address of the database server. Adjust the enableDnsHostNames and enableDnsSupport attributes of the VPCs to false.

Correct Answer: B

Explanation of the Correct Answer and Analysis of Other Options:

- Why B is Correct:
  - Private Hosted Zone: Utilizing a private hosted zone with Amazon Route 53 allows DNS resolution within specified VPCs. This ensures that the database.example.com server is accessible only within the company's internal network.
  - A Record Creation: An A record pointing to the IP address of the database server's EC2 instance under the private hosted zone ensures that the domain name resolves

correctly within the private network.

  - DNS Attributes Configuration: Setting both the enableDnsHostNames and enableDnsSupport attributes to true in the VPCs is essential for proper DNS functionality within the VPCs, allowing for accurate domain name resolution.
- Why Other Options are Incorrect:
  - A & D: A public hosted zone would make the DNS records accessible from the internet, which would not meet the requirement for the database server to be only internally accessible.
  - C: Setting enableDnsSupport to false would disrupt DNS resolution within the VPC, impeding the accessibility of the database server.

Question 7

A company planning a multi-account strategy across its numerous research facilities requires a simplified DNS management solution. With around 50 teams needing individual AWS accounts, the challenge is to enable private DNS sharing among Virtual Private Clouds (VPCs) in different AWS accounts, managed by a single team responsible for all domains and subdomains organization-wide.

The most straightforward solution with the least complex DNS architecture to allow all VPCs to resolve necessary domain names is:

A. Utilize AWS Resource Access Manager (RAM) to create a shared services VPC in the central account. Establish VPC peering between this VPC and each team's VPC in other accounts. In Amazon Route 53, create a private hosted zone linked to the shared services VPC for managing all domains and subdomains. Programmatically link the VPCs from other accounts to this hosted zone.

B. Establish VPC peering connections among the VPCs of each account. Make sure every VPC has the attributes enableDnsHostnames and enableDnsSupport set to “TRUE”. On Amazon Route 53, create a private hosted zone in the central account’s VPC for all domain and subdomain management. In each of the other AWS Accounts, set up a Route 53 private hosted zone and adjust the Name Server entry to utilize the DNS of the central account.

C. Use AWS Resource Access Manager (RAM) to establish a shared services VPC in the central account. Create VPC peering between this VPC and each team's VPC in other accounts. On Amazon Route 53, generate a private hosted zone associated with the shared services VPC for domain and subdomain management. In each of the other AWS Accounts, create a Route 53 private hosted zone and configure the Name Server entry to align with the DNS of the central account.

D. Implement Direct Connect connections among the VPCs of each account using private virtual interfaces. Confirm that each VPC has the attributes enableDnsHostnames and enableDnsSupport set to “FALSE”. On Amazon Route 53, construct a private hosted zone linked to the central account’s VPC for managing all domains and subdomains. Programmatically connect the VPCs from other accounts to this hosted zone.

Correct Answer: A

Explanation of the Correct Answer and Analysis of Other Options:

- Why A is Correct:
  - AWS Resource Access Manager for Shared Services: AWS RAM facilitates the sharing of resources like VPCs across multiple AWS accounts. By setting up a shared services VPC in the central account and peering it with each team's VPC, a centralized network architecture is created.
  - Amazon Route 53 Private Hosted Zone: A private hosted zone in Route 53 associated with the shared services VPC allows for efficient DNS management. All domains and subdomains can be managed centrally and resolved across all peered VPCs.
  - Programmatic Association of VPCs: Associating VPCs from other accounts with the hosted zone via programmatic means provides a streamlined approach to extending DNS services to all teams' VPCs without complex configurations.
- Why Other Options are Incorrect:
  - B & C: While these options also involve Route 53 and VPC peering, the need to create and configure individual private hosted zones in each AWS account adds unnecessary complexity.
  - D: Using Direct Connect is not only more complex but also typically more costly. Additionally, setting enableDnsHostnames and enableDnsSupport to “FALSE” in each VPC would hinder the necessary DNS resolutions.

Question 8

A prominent media company with a hybrid architecture connecting its on-premises data center to AWS via Direct Connect has an extensive collection of over 50 TB of digital videos and media files stored in an on-premises tape library. These files are accessed by their Media Asset Management (MAM) system. The company aims to implement an automated catalog system capable of searching their files using facial recognition, and eventually, they plan to migrate these media files, including the MAM video contents, to AWS.

The optimal solution to achieve this with minimal ongoing management overhead and least disruption to the existing system is:

A. Deploy an on-premises tape gateway appliance connected to AWS Storage Gateway. Configure the MAM system to transfer media files to the tape gateway for storage in Amazon Glacier. Use Amazon Rekognition to build a facial recognition catalog. Employ an AWS Lambda function with the Rekognition JavaScript SDK to process videos in real-time from the tape gateway, extract metadata, and update the MAM system.

B. Implement Amazon Kinesis Video Streams for video ingestion and Amazon Rekognition to create a facial recognition catalog. Stream media files from the MAM system into Kinesis Video Streams. Configure Rekognition to process these files, and use a stream consumer to extract metadata and update the MAM system. Store the files in an Amazon S3 bucket.

C. Use an AWS Snowball Storage Optimized device to transfer media files from the on-premises library to Amazon S3. Set up a large EC2 instance with access to the S3 bucket and install an open-source facial recognition tool like OpenFace or OpenCV. Process the files to retrieve metadata and integrate this data into the MAM solution. Copy the files to another S3 bucket.

D. Integrate the local data center’s file system with AWS Storage Gateway using an on-premises file gateway appliance. Transfer media files from the current data store to the file gateway. Build a facial recognition catalog using Amazon Rekognition. Use an AWS Lambda function with the Rekognition JavaScript SDK to process media files from the S3 bucket backing the file gateway, extract metadata, and update the MAM system.

Correct Answer: D

Explanation of the Correct Answer and Analysis of Other Options:

- **Why D is Correct**:
  - **AWS Storage Gateway Integration**: The file gateway appliance seamlessly integrates the on-premises file system with AWS cloud storage, minimizing disruption to existing workflows.
  - **Facial Recognition with Amazon Rekognition**: Utilizing Amazon Rekognition to create a catalog of faces from the media files provides an advanced and automated facial recognition system.
  - **Lambda Function and Rekognition SDK**: The use of AWS Lambda and the Rekognition SDK enables efficient processing of media files directly from the S3 bucket, which is a scalable and low-management solution.
  - **Minimal Disruption and Management Overhead**: This solution leverages existing infrastructure and AWS services to automate the facial recognition process, thereby minimizing both disruption and ongoing management needs.
- **Why Other Options are Incorrect**:

- A: The tape gateway is part of AWS Storage Gateway that provides a virtual tape infrastructure. It is typically used for backup and archival solutions, where data is not frequently accessed. In this scenario, the requirement is to access and process a large volume of media files (over 50 TB) for facial recognition. Using a tape gateway for such a purpose is inefficient due to the nature of tape-based systems, which are generally slower and not designed for dynamic, real-time access or processing of data. This option also suggests storing the data in Amazon Glacier via the tape gateway. Glacier is a low-cost storage service designed for data archiving and long-term backup. It is not optimal for immediate, real-time data retrieval due to its retrieval times, which can range from a few minutes to several hours. This delay in accessing the data would significantly hinder the real-time processing capabilities of Amazon Rekognition and Lambda, leading to inefficient operation and potential bottlenecks.
- B: Kinesis Video Streams and Rekognition offer a robust solution, but streaming 50 TB of media files and real-time processing would be more complex and potentially disruptive to the existing system.
- C: Using Snowball for data transfer is viable for large data sets, but setting up and managing an EC2 instance with open-source tools adds significant management overhead and complexity.

Question 9

A company with a hybrid mobile application setup is experiencing high AWS Lambda costs. Their on-premises data center, connected to AWS via VPN, hosts a 3TB MySQL database server, processing write-intensive requests from the app. The serverless app on AWS uses Lambda, API Gateway, and DynamoDB. The Lambda function has a high execution time, mainly due to latency in connecting to the MySQL server. The company seeks a solution to reduce costs while handling unpredictable user traffic, which averages a 20% increase monthly.

The proposed solutions for cost optimization are:

A. Migrate the on-premises MySQL database to Amazon RDS for MySQL with Multi-AZ for high availability. Configure API Gateway caching to reduce Lambda invocations. Gradually adjust the Lambda functions' timeout and memory settings without affecting execution time. Implement Auto Scaling on DynamoDB based on user traffic.

B. Set up a CloudFront distribution with API Gateway as the origin to cache responses and reduce Lambda invocations. Gradually lower Lambda functions' timeout and memory settings. Enable DynamoDB Accelerator to cache frequently accessed records.

C. Provision AWS Direct Connect instead of VPN to reduce latency to the MySQL server. Convert Lambda functions to run on EC2 Reserved Instances with Spot instances for peak times. Create a CloudFront distribution to cache API Gateway responses. Configure Auto Scaling on DynamoDB with user traffic.

D. Replace VPN with AWS Direct Connect to decrease network latency to the MySQL server. Implement caching in the mobile app to reduce Lambda calls. Gradually reduce Lambda functions' timeout and memory settings. Add an Amazon Elasticache cluster in front of DynamoDB for caching frequently accessed records.

Correct Answer: A

Explanation of the Correct Answer and Analysis of Other Options:

- Why A is Correct:
  - Migrating to Amazon RDS for MySQL: Shifting the MySQL database from an on-premises setup to Amazon RDS addresses the primary issue of network latency, which is contributing to the high execution time of AWS Lambda functions. By hosting the database in AWS, the data retrieval time is significantly reduced, which in turn decreases the Lambda execution time and associated costs. RDS, being a managed service, also offers benefits such as automated backups, patching, and scaling. The Multi-AZ deployment ensures high availability and failover support, crucial for maintaining the application's uptime and performance.
  - Configuring API Gateway Caching: This strategy reduces the number of direct Lambda invocations by caching the responses of repeatable requests. By serving cached responses, the system minimizes the need to execute Lambda functions for each API call, thereby directly impacting and reducing the cost associated with Lambda invocations.
  - Optimizing Lambda Functions' Timeout and Memory: Lambda pricing is partly based on the number of requests and the duration of execution. By fine-tuning the timeout and memory configurations, the company can ensure that each Lambda function is using only the necessary amount of resources, avoiding over-provisioning and reducing execution time where possible. This can lead to a more cost-efficient use of Lambda.
  - Auto Scaling for DynamoDB: DynamoDB Auto Scaling dynamically adjusts the table's throughput capacity in response to actual traffic patterns. This ensures that the database can handle the load during peak times without provisioning excessive resources during quieter periods, optimizing cost and performance.
- Why Other Options are Incorrect:
  - B: While implementing CloudFront and DynamoDB Accelerator (DAX) can improve caching and performance, this option doesn't address the main issue of high latency

between the Lambda functions and the on-premises MySQL database. Without resolving this latency issue, the execution time of Lambda functions, and thus costs, will remain high.

- C: Provisioning AWS Direct Connect would reduce network latency, but converting Lambda functions to run on EC2 Reserved Instances introduces a significant shift in architecture. This shift might lead to increased complexity and management overhead, potentially offsetting the cost benefits. Additionally, the use of Spot Instances, while cost-effective, requires a well-managed strategy to handle instance interruptions, adding to the management complexity.
- D: Replacing the VPN with Direct Connect would indeed reduce latency, but adding caching in the mobile app and Elasticache in front of DynamoDB does not directly contribute to reducing the high costs associated with Lambda execution time. Elasticache might also be redundant given DynamoDB's performance capabilities, and the changes to the mobile app could be substantial, requiring additional development and maintenance efforts.

Question 10

A retail company's web application, running on an Auto Scaling group of Amazon EC2 instances across multiple Availability Zones, faced a significant outage. The application, behind an Application Load Balancer, performs health checks via a fixed HTTP page querying the database. The backend comprises a Multi-AZ Amazon RDS MySQL instance. The outage was caused by high CPU usage on the database, leading to EC2 health check timeouts and continuous instance replacement.

The proposed solutions to prevent future occurrences and handle increased traffic are:

A. Reduce the load on the database tier by creating multiple read replicas for the Amazon RDS MySQL Multi-AZ cluster. Configure the web application to use the single reader endpoint of RDS for all read operations.

B. Change the target group health check to a simple HTML page instead of a page that queries the database. Create an Amazon Route 53 health check for the database dummy item web page to ensure that the application works as expected. Set up an Amazon CloudWatch alarm to send a notification to Admins when the health check fails.

C. Change the target group health check to use a TCP check on the EC2 instances instead of a page that queries the database. Create an Amazon Route 53 health check for the database dummy item web page to ensure that the application works as expected. Set up an Amazon CloudWatch alarm to send a notification to Admins when the health check fails.

D. Reduce the load on the database tier by creating an Amazon ElastiCache cluster to cache frequently requested database queries. Configure the application to use this cache when querying the RDS MySQL instance.

E. Create an Amazon CloudWatch alarm to monitor the Amazon RDS MySQL instance if it has a high-load or in impaired status. Set the alarm action to recover the RDS instance. This will automatically reboot the database to reset the queries.

Correct Answers: B and D

Explanation of the Correct Answers:

- Why B is Correct:
  - Simplifying Health Checks: Changing the health check to a simple HTML page reduces unnecessary load on the database. This ensures that the health checks are not contributing to high CPU usage on the database, which was a major cause of the previous outage.
  - Dedicated Health Check for Database: Creating a separate Amazon Route 53 health check for the database-specific page allows for targeted monitoring of the database's performance. This way, issues with the database can be identified without impacting the overall health status of the EC2 instances.
  - CloudWatch Alarm for Proactive Monitoring: Setting up a CloudWatch alarm based on the Route 53 health check provides early warning to administrators, allowing them to take corrective actions before issues escalate into outages.
- Why D is Correct:
  - Implementing Amazon ElastiCache: Using ElastiCache to cache frequently accessed data significantly reduces the query load on the RDS instance. This helps in lowering the CPU utilization of the database, which addresses the direct cause of the health check timeouts and instance replacements.
  - Optimized Database Querying: Configuring the web application to query ElastiCache instead of directly hitting the RDS for every request improves response times and reduces the workload on the RDS instance, leading to better application performance and stability.

Analysis of Other Options:

- A: While read replicas can reduce the load on the primary database, managing multiple replicas adds complexity. Furthermore, it might not address the immediate CPU spikes caused by health check queries, as replicas are typically used for read-heavy workloads.
- C: Switching to a TCP health check reduces the database load, but it might not accurately reflect the application's health, particularly if the database is experiencing

issues. It's a less precise method compared to an HTTP check on a lightweight page.

- E: Creating a CloudWatch alarm for RDS high-load status is good practice, but automatically rebooting the RDS instance as a response can lead to service interruptions and potential data consistency issues. It's a reactive measure that doesn't proactively address the underlying performance problem.

Question 11

A company is planning to retire its legacy web application hosted on AWS and replace it with a new serverless architecture using AWS Lambda, API Gateway, and DynamoDB. Additionally, they want to establish a CI/CD pipeline for efficient build and deployment processes while supporting gradual deployments.

Which approach is the most suitable for developing, testing, and deploying the new AWS architecture?

A. Utilize AWS Serverless Application Model (AWS SAM) and configure AWS CodeBuild, AWS CodeDeploy, and AWS CodePipeline to create a CI/CD pipeline.

B. Employ the AWS Serverless Application Repository to organize related components, share configuration settings like memory and timeouts among resources, and deploy all related resources collectively as a single, versioned entity.

C. Opt for AWS Elastic Beanstalk as the deployment platform for the new application.

D. Set up a CI/CD pipeline using AWS CodeCommit, AWS CodeBuild, AWS CodeDeploy, and AWS CodePipeline to create the CI/CD pipeline. Then, use AWS Systems Manager Automation to automate the build process and facilitate gradual deployments.

Correct Answer: A

Explanation of the Correct Answer and Analysis of Other Options:

- Why A is Correct:
  - AWS SAM for Serverless Infrastructure: AWS SAM simplifies the definition of serverless applications, making it an ideal choice for setting up a new serverless architecture. It streamlines the creation of AWS resources such as Lambda functions, API Gateway APIs, and DynamoDB tables.
  - CI/CD Pipeline with AWS Code Services: Using AWS CodeBuild, AWS CodeDeploy, and AWS CodePipeline allows for the creation of a robust CI/CD pipeline that automates the build, test, and deployment phases. This approach ensures efficient development workflows and reliable deployments.

    - Best Practices: AWS SAM combined with AWS Code Services follows best practices for modern application development on AWS, promoting code quality, maintainability, and automation.
- Why Other Options are Incorrect:
    - B: While the AWS Serverless Application Repository is useful for sharing and reusing serverless applications, it is not the primary tool for building and managing CI/CD pipelines. It focuses on packaging and distributing serverless applications rather than automating the development process.
    - C: AWS Elastic Beanstalk is a platform-as-a-service (PaaS) offering that simplifies the deployment of web applications. However, it does not align with the serverless architecture requirements specified in the question. The new architecture is designed to be serverless, using AWS Lambda and related services, making Elastic Beanstalk less suitable.
    - D: While AWS CodeCommit, AWS CodeBuild, AWS CodeDeploy, and AWS CodePipeline are valuable tools for CI/CD pipelines, introducing AWS Systems Manager Automation adds complexity and may not align with the goal of building and deploying a serverless architecture. Automation is typically used for infrastructure management tasks rather than serverless application deployment.

Question 12

A multinational investment bank has a hybrid cloud architecture that relies on a single 1 Gbps AWS Direct Connect connection to integrate their on-premises network with the AWS Cloud. The bank operates a total of 10 VPCs, all connected to their on-premises data center via the same Direct Connect connection, which you manage. Following a recent IT audit, it was discovered that the existing network setup has a single point of failure that requires immediate attention.

Which of the following is the MOST cost-effective solution to improve connection redundancy in the hybrid network?

A. Establish another 1 Gbps AWS Direct Connect connection using a public Virtual Interface (VIF). Prepare a VPN tunnel that will terminate on the virtual private gateway (VGW) of the respective VPC using the public VIF. Manage failover to the VPN connection through the use of BGP.

B. Set up a new point-to-point Multiprotocol Label Switching (MPLS) connection to each of your 10 VPCs. Configure BGP for this new connection with an active/passive routing setup.

C. Create VPN tunnels from your on-premises data center to each of the 10 VPCs. Terminate each VPN tunnel connection at the virtual private gateway (VGW) of the respective VPC. Configure BGP for route management.

D. Establish an additional 1 Gbps AWS Direct Connect connection with corresponding private Virtual Interfaces (VIFs) to individually connect all 10 VPCs. Set up a Border Gateway Protocol (BGP) peering session for each of the VIFs.

Correct Answer:

C. Create VPN tunnels from your on-premises data center to each of the 10 VPCs. Terminate each VPN tunnel connection at the virtual private gateway (VGW) of the respective VPC. Configure BGP for route management.

Explanation of the Correct Answer and Analysis of Other Options:

- Why C is Correct:
  - VPN Tunnels for Redundancy: Establishing VPN tunnels from the on-premises data center to each of the 10 VPCs provides redundancy by creating multiple paths for network traffic. In case one tunnel or VPC fails, traffic can automatically failover to other functional tunnels and VPCs.
  - Termination at VGWs: Terminating each VPN tunnel connection at the virtual private gateway (VGW) of the respective VPC is a best practice for secure and efficient connectivity. VGWs are designed to handle VPN connections and route traffic appropriately.
  - BGP for Route Management: Configuring BGP for route management allows dynamic routing adjustments based on the availability of VPN tunnels and VPCs. This ensures that traffic is directed through the most reliable paths, further enhancing redundancy.
  - Cost-Effective: This solution minimizes costs by efficiently using VPN tunnels, which are cost-effective compared to dedicated Direct Connect connections.
- Why Other Options are Incorrect:
  - A: While establishing another Direct Connect connection with VPN failover is a viable option, it can be more costly than creating VPN tunnels directly from the on-premises data center to each VPC. Additionally, the use of a public VIF introduces potential security concerns.
  - B: Setting up new point-to-point MPLS connections to all 10 VPCs might provide redundancy, but it can be a costly and complex solution compared to VPN tunnels. Additionally, active/passive routing may not fully utilize available network resources.
  - D: Creating additional Direct Connect connections and VIFs for each VPC is a costly approach and may not be necessary to achieve redundancy. Managing multiple VIFs can also introduce complexity without a significant advantage over VPN tunnels.

Question 13

A company provides big data services to enterprise clients worldwide. One of the clients possesses a 60 TB raw data set from their on-premises Oracle data warehouse, which needs to be migrated to Amazon Redshift. The Oracle database receives minor daily updates, with major updates scheduled at the end of each month. It is crucial to complete the migration within approximately 30 days, just before the next major update on the Redshift database. The company can allocate only 50 Mbps of Internet connection for this activity to avoid affecting daily business operations.

Which of the following actions will meet the company's migration requirements while minimizing costs?

A. Configure VPN connectivity between AWS and the company's data center with a provisioned 1 Gbps AWS Direct Connect connection. Deploy an Oracle Real Application Clusters (RAC) database on an EC2 instance to fetch and synchronize data from the on-premises Oracle database. Once replication is complete, create an AWS Database Migration Service (DMS) task within an AWS Schema Conversion Tool (SCT) project to migrate the Oracle database to Amazon Redshift. Monitor and verify the data migration's completion before the cut-over.

B. Initiate an AWS Snowball Edge job using the AWS Snowball console. Export all data from the Oracle data warehouse to the Snowball Edge device. Upon the device's return to Amazon, import the data into an S3 bucket. Create an Oracle RDS instance for data import. Set up an AWS SCT project with AWS DMS task to migrate the Oracle database to Amazon Redshift. Copy the missing daily updates from Oracle in the data center to the RDS for Oracle database via the Internet. Monitor and verify data migration completion before the cut-over.

C. Establish a new Oracle Database on Amazon RDS. Configure a Site-to-Site VPN connection between the on-premises data center and the Amazon Virtual Private Cloud (VPC). Set up replication from the on-premises database to Amazon RDS. After replication finishes, create an AWS SCT project with AWS DMS task to migrate the Oracle database to Amazon Redshift. Monitor and verify data migration completion before the cut-over.

D. Create an AWS Snowball import job to request a Snowball Edge device. Utilize the AWS Schema Conversion Tool (SCT) to process the on-premises data warehouse and load it onto the Snowball Edge device. Install the extraction agent on a separate on-premises server and register it with AWS SCT. After the Snowball Edge imports the data into the S3 bucket, employ AWS SCT to migrate the data to Amazon Redshift. Configure a local task and AWS DMS task to replicate ongoing updates to the data warehouse. Monitor and verify data migration completion.

Correct Answer:

D. Create an AWS Snowball import job to request for a Snowball Edge device. Use the AWS Schema Conversion Tool (SCT) to process the on-premises data warehouse and load it to the Snowball Edge device. Install the extraction agent on a separate on-premises server and register it with AWS SCT. Once the Snowball Edge imports data to the S3 bucket, use AWS SCT to migrate the data to Amazon Redshift. Configure a local task and AWS DMS task to replicate the ongoing updates to the data warehouse. Monitor and verify that the data migration is complete.

Explanation of the Correct Answer and Analysis of Other Options:

Why D is Correct:

- AWS Snowball for Data Transfer: Using AWS Snowball Edge is a cost-effective and efficient approach for transferring large volumes of data (60 TB) from the on-premises Oracle data warehouse to AWS. Snowball Edge can be shipped to the customer's location, and once data is loaded onto it, it can be returned to AWS for fast data import to an S3 bucket. This method addresses the constraint of a limited 50 Mbps Internet connection, ensuring swift data transfer without impacting business operations.
- AWS SCT for Schema Conversion: AWS Schema Conversion Tool (SCT) is employed for processing the on-premises data warehouse and preparing it for migration. This step is crucial for ensuring data compatibility with Amazon Redshift. SCT performs schema analysis and conversion, making the data warehouse schema compatible with Redshift's requirements. This ensures that data can be smoothly migrated and queried in the Redshift environment.
- Extraction Agent for Ongoing Updates: Installing an extraction agent on a separate on-premises server allows for the efficient capture of ongoing updates to the data warehouse. This ensures that the latest changes are included in the migration process. By continuously capturing and replicating updates, the solution guarantees that the migrated data in Redshift remains up-to-date with minimal latency.
- AWS SCT for Schema Conversion (Again): After the initial schema conversion, AWS SCT is used once more in this solution. This time, it plays a critical role in the ongoing data migration process. SCT is utilized to configure a local task and AWS Database Migration Service (DMS) task for replicating the daily updates to the data warehouse. This ensures that the newly arrived data is compatible with the Redshift schema and is seamlessly integrated into the database.
- AWS DMS for Data Migration: AWS Database Migration Service (DMS) is used in conjunction with AWS SCT to migrate the processed data from S3 to Amazon Redshift. DMS provides a reliable and efficient way to migrate data to Redshift. It ensures data integrity and consistency during the migration process, minimizing the risk of data loss or corruption.

- Monitoring and Verification: The solution includes monitoring and verification to ensure that the data migration is complete and up-to-date before the cut-over. This critical step allows the company to confirm that all data, including the daily updates, has been successfully migrated to Amazon Redshift. It provides confidence that the system is ready for the next major update without any data gaps or inconsistencies.
- Why Other Options are Incorrect:
  - A: This option involves provisioning a 1 Gbps AWS Direct Connect connection and deploying Oracle RAC on EC2 instances. While it provides redundancy and robustness, it is more complex and costly compared to the Snowball Edge approach. It also requires setting up AWS SCT and AWS DMS, similar to Option D.
  - B: Exporting data to Snowball Edge and importing it into an S3 bucket is a viable data transfer approach. However, the additional steps of creating an Oracle RDS instance and copying daily updates over the Internet introduce complexity and potential data transfer delays.
  - C: While this option involves configuring a new Oracle Database on Amazon RDS and replication, it may not be as cost-effective and may not align with the constraint of a 50 Mbps Internet connection for data transfer. The direct Snowball Edge approach in Option D is more suitable for minimizing Internet usage.

Question 14

A company is aiming to optimize its infrastructure by deploying development environment workloads in AWS Fargate while also maintaining on-premises servers for cost-effectiveness. The goal is to create a solution that enables:

1. Running on-premises and Fargate workloads in the same cluster.
2. Effortless migration of development environment workloads from on-premises to Fargate.
3. Consistency in tooling and API experience for container-based workloads.

Which of the following solutions best achieves these operational efficiency objectives?

A. Implement AWS Outposts in the on-premises data center, configure Amazon ECS on AWS Outposts to launch development environment workloads, and migrate these workloads to production on AWS Fargate.

B. Utilize EKS Amazon Anywhere to simplify on-premises Kubernetes management with default configurations and automated cluster management. This enables easy migration of on-premises development workloads to EKS in an AWS region on Fargate.

C. Deploy AWS Outposts in the on-premises data center, run Amazon EKS Anywhere on AWS Outposts to launch container-based workloads, and migrate development workloads to production on AWS Fargate.

D. Opt for Amazon ECS Anywhere to streamline software management both on-premises and in AWS using a standardized container orchestrator. This solution facilitates the migration of on-premises development workloads to ECS in an AWS region on Fargate.

Correct Answer:

D. Utilize Amazon ECS Anywhere to streamline software management on-premises and on AWS with a standardized container orchestrator. This makes it easy to migrate the development workloads running on-premises to ECS in an AWS region on Fargate.

Explanation of the Correct Answer and Analysis of Other Options:

- Why D is Correct:
  - Amazon ECS Anywhere for Unified Management: Amazon ECS Anywhere is a solution that provides a consistent and unified way to manage container-based workloads both on-premises and in the AWS cloud. It offers operational efficiency by utilizing the same container orchestrator, Amazon ECS, for both environments. This aligns with the goal of ensuring consistent tooling and API experience across workloads.
  - Streamlined Software Management: By leveraging Amazon ECS Anywhere, the company can efficiently manage its container workloads across the hybrid infrastructure. It simplifies software management, ensuring that development workloads are compatible with the production environment.
  - Migration to AWS Fargate: With Amazon ECS Anywhere, it becomes straightforward to migrate the development environment workloads running on-premises to ECS in an AWS region on Fargate. This ensures a smooth transition while maintaining operational efficiency.
- Why Other Options are Incorrect:
- A: AWS Outposts Limitations: AWS Outposts is designed to extend AWS services to on-premises environments, primarily focusing on running AWS infrastructure on-premises. While configuring Amazon ECS on AWS Outposts is a valid approach, it's essential to note that AWS Fargate is not available on AWS Outposts. As a result, this option cannot fully meet the requirement of running development workloads on AWS Fargate while maintaining on-premises workloads. Additionally, migrating workloads from AWS Outposts to Fargate may introduce complexity due to differences in infrastructure.
- B: EKS Amazon Anywhere Limitations: EKS Amazon Anywhere simplifies Kubernetes management for hybrid environments but doesn't directly address the goal of running AWS Fargate workloads alongside on-premises workloads. This option introduces

Kubernetes-specific complexity and may not provide the operational efficiency required for this scenario.

- C: AWS Outposts and EKS Anywhere Combination: Running Amazon EKS Anywhere on AWS Outposts focuses on Kubernetes-centric solutions, which may not align with the goal of using a standardized container orchestrator like Amazon ECS Anywhere. Additionally, migrating workloads from EKS Anywhere to AWS Fargate could be complex, given the differences in underlying infrastructure and orchestrators.

Question 15

A company is migrating an interactive car registration web system hosted on its on-premises network to AWS Cloud. The current architecture of the system consists of a single NGINX web server and a MySQL database running on a Fedora server, which both reside in their on-premises data center. For the new cloud architecture, a load balancer must be used to evenly distribute the incoming traffic to the application servers. Route 53 must be used for both domain registration and domain management.

In this scenario, what would be the most efficient way to transfer the web application to AWS?

A. Launch two NGINX EC2 instances in two Availability Zones. Copy the web files from the on-premises web server to each Amazon EC2 web server, using Amazon S3 as the repository. Migrate the database using the AWS Database Migration Service. Create an ELB to front your web servers. Use Route 53 and create an alias A record pointing to the ELB.

B. Export web files to an Amazon S3 bucket in one Availability Zone using AWS Migration Hub. Run the website directly out of Amazon S3. Migrate the database using the AWS Database Migration Service and AWS Schema Conversion Tool (AWS SCT). Use Route 53 and create an alias record pointing to the ELB.

C. Use the AWS Application Discovery Service to migrate the NGINX web server. Configure Auto Scaling to launch two web servers in two Availability Zones. Launch a Multi-AZ MySQL Amazon Relational Database Service (RDS) instance in one Availability Zone only. Import the data into Amazon RDS from the latest MySQL backup. Use Amazon Route 53 to create a private hosted zone and point a non-alias A record to the ELB.

D. Use the AWS Application Migration Service (MGN) to create an EC2 AMI of the NGINX web server. Configure auto-scaling to launch in two Availability Zones. Launch a multi-AZ MySQL Amazon RDS instance in one availability zone only. Import the data into Amazon RDS from the latest MySQL backup. Create an ELB to front your web servers. Use Amazon Route 53 and create an A record pointing to the elastic load balancer.

Correct Answer:

A. Launch two NGINX EC2 instances in two Availability Zones. Copy the web files from the on-premises web server to each Amazon EC2 web server, using Amazon S3 as the repository. Migrate the database using the AWS Database Migration Service. Create an ELB to front your web servers. Use Route 53 and create an alias A record pointing to the ELB.

Explanation of the Correct Answer and Analysis of Other Options:

Why A is Correct:

- Launching EC2 Instances: Option A recommends launching two NGINX EC2 instances in two Availability Zones, ensuring redundancy and high availability for the web application.
- Copying Web Files to EC2 Instances: The option suggests copying the web files from the on-premises web server to each Amazon EC2 web server, using Amazon S3 for storage. This approach ensures reliable access to web files and leverages the durability and availability of S3.
- Database Migration with DMS: AWS Database Migration Service (DMS) is proposed for migrating the MySQL database to AWS. DMS is a reliable and efficient way to migrate data, minimizing downtime during the migration process.
- Creating an ELB: The option includes creating an Elastic Load Balancer (ELB) to distribute incoming traffic to the web servers, improving performance and fault tolerance.
- Using Route 53 for DNS: Route 53 is recommended for domain registration and management. An alias A record is created pointing to the ELB, providing efficient domain routing within AWS. For services like ELB, CloudFront, and S3, it's best practice to use a Type A Record with an Alias in Route 53.
- Why Other Options are Incorrect:
- Option B: Export web files to Amazon S3 and Run Website from S3: This approach is flawed for a dynamic, interactive web system. Amazon S3 is primarily suitable for hosting static websites and does not support the complexities of a dynamic web application that requires server-side processing, which is essential for the car registration system. This limitation makes Option B ineffective for the scenario.
- Option C: Use of AWS Application Discovery Service and AWS Application Migration Service (MGN): This option is not ideal for a couple of reasons. Firstly, the AWS Application Discovery Service is intended for gathering data about on-premises data centers to aid in migration planning, not for the actual migration of applications like a web server. Secondly, AWS Application Migration Service (MGN) is tailored for migrating virtual machines (e.g., VMware vSphere, Windows Hyper-V) rather than specific web server applications. Therefore, using these services for migrating the NGINX web server might not be the most effective or efficient method.
- Option D: Incorrect Use of Route 53 and A Record without Alias for ELB: The major flaw in this option is the use of a standard A record in Amazon Route 53 to point to an

Elastic Load Balancer (ELB). The recommended practice for AWS resources like ELB is to use an Alias A record, which allows DNS queries to be routed to an AWS resource more efficiently and reliably than a standard A record. This incorrect setup could lead to less efficient DNS routing and potential issues with load balancing.

Question 16

An international company specializing in foreign exchange has a serverless forex trading application developed using AWS Serverless Application Model (SAM) and hosted on the AWS Serverless Application Repository. This application is accessed by millions of users globally for currency trading through an online portal that operates continuously. Recently, the company has been facing challenges with slow login times and occasional HTTP 504 errors, negatively impacting user experience. As a Solutions Architect, your task is to enhance the system's performance and reduce login times significantly to boost customer satisfaction, while keeping costs minimal.

Which two measures should be implemented to achieve this objective with cost-effectiveness?

A. Implement Lambda@Edge to enable Lambda functions to modify the content delivered by CloudFront and to execute the authentication process at AWS locations nearer to the users.

B. Establish multiple geographically dispersed VPCs across various AWS regions and connect them through a transit VPC. Deploy the Lambda function in each region using AWS SAM for quicker request handling.

C. Deploy the application across multiple AWS regions worldwide. Configure a Route 53 record with a latency routing policy to direct traffic to the region offering the best latency for the user.

D. Enhance the cache hit ratio of the CloudFront distribution by configuring the origin to add a Cache-Control max-age directive to objects, setting the max-age to the longest feasible value.

E. Set up origin failover by creating an origin group with two origins: designate one as the primary and the other as the secondary. CloudFront will switch to the secondary origin when the primary origin returns certain HTTP status code failures.

Correct Answers:

A. Implement Lambda@Edge for content customization and authentication near users.

E. Set up origin failover with a primary and secondary origin in CloudFront.

Explanation of the Correct Answers and Analysis of Other Options:

Why A and E are Correct:

- Lambda@Edge (A): Utilizing Lambda@Edge allows the application to run Lambda functions closer to the end-users, reducing latency especially for authentication processes. This proximity improves response times and efficiency, addressing the issue of slow login times and HTTP 504 errors which are often related to timeouts or server unavailability.
- Origin Failover (E): Setting up an origin failover ensures that if the primary origin is failing (possibly contributing to the HTTP 504 errors), CloudFront automatically switches to a secondary origin. This redundancy can significantly reduce the occurrence of errors and improve application availability and performance.

Why Other Options are Incorrect:

- Multiple VPCs and Transit VPC (B): While deploying Lambda functions across multiple regions can improve response times, the complexity and cost of setting up and maintaining multiple VPCs and a transit VPC may not justify the potential performance gains, especially for a serverless architecture that is inherently designed to manage scalability and distribution.
- Multi-Region Deployment and Route 53 Latency Routing (C): Deploying the application in multiple regions and using Route 53 for latency-based routing can improve performance. However, this approach can be more costly and complex compared to using Lambda@Edge. It might be overkill for the issue at hand, which appears to be more related to specific functionalities (like login) rather than the overall application performance.
- Enhancing Cache Hit Ratio (D): Increasing the cache hit ratio can improve performance for delivering static content. However, since the issue is related to the login process, which is dynamic in nature, simply enhancing caching would not effectively address the specific problem of login delays and HTTP 504 errors.

Question 17

A company employing Lightweight Directory Access Protocol (LDAP) for employee authentication and authorization is preparing to launch a mobile application for its employees. This app, designed for smartphones, will facilitate federated access to AWS resources. Given stringent security and compliance mandates, the mobile app is required to utilize a custom-built authentication mechanism and employ IAM roles to assign user permissions for AWS resources. The Solutions Architect is tasked with devising a solution that adheres to these stipulations.

To establish authentication and authorization for the app, which two solutions should the Solutions Architect implement?

A. Develop a custom-built solution compatible with Security Assertion Markup Language (SAML) for user authentication. Utilize AWS IAM Identity Center for granting access to AWS resources.

B. Create a custom LDAP connector using Amazon API Gateway and an AWS Lambda function for user authentication. Employ Amazon DynamoDB to store user authorization tokens. Develop an additional Lambda function to validate user authorization requests based on the DynamoDB-stored tokens.

C. Construct a custom solution compatible with OpenID Connect, paired with AWS IAM Identity Center, to provide authentication and authorization features for the app.

D. Design a custom SAML-compatible solution for both authentication and authorization processes. Integrate the solution with LDAP for user authentication and utilize SAML assertions for authorization with the IAM identity provider.

E. Formulate a custom solution compatible with OpenID Connect for user authentication. Implement Amazon Cognito Identity Pools for the authorization of access to AWS resources.

Correct Answers:

D. Custom SAML-compatible solution integrating LDAP for authentication and using SAML assertions for IAM provider authorization.

E. Custom OpenID Connect-compatible solution for authentication paired with Amazon Cognito Identity Pools for AWS resource authorization.

Explanation of the Correct Answers and Analysis of Other Options:

Why D and E are Correct:

- Custom SAML-Compatible Solution (D): Building a SAML-compatible solution that uses LDAP for user authentication aligns perfectly with the company's current LDAP usage. SAML is widely used for single sign-on (SSO) processes and is compatible with AWS for federated access. By using SAML assertions, the solution can communicate authentication and authorization information to the AWS IAM identity provider, fulfilling the strict security requirements.
- Custom OpenID Connect-Compatible Solution (E): OpenID Connect is another popular standard for authentication, and when combined with Amazon Cognito Identity Pools, it provides a robust solution for federated access to AWS resources. Amazon Cognito seamlessly integrates with external identity providers and can generate temporary AWS

credentials for authenticated users, thus meeting the compliance and security needs of the application.

Why Other Options are Incorrect:

- SAML with AWS IAM Identity Center (A): While this option utilizes SAML, it proposes AWS IAM Identity Center for authorization, which may not align with the need for a custom-built solution, especially since the requirement is to use IAM roles for authorization.
- Custom LDAP Connector with API Gateway and Lambda (B): This option, involving Amazon API Gateway, Lambda, and DynamoDB, introduces unnecessary complexity and potential latency. It does not leverage existing standards like SAML or OpenID Connect, which are more streamlined for such scenarios.
- OpenID Connect with AWS IAM Identity Center (C): Similar to Option A, this integrates with AWS IAM Identity Center for authorization. This does not conform to the requirement of using a custom-built solution alongside IAM roles for resource access control.

Question 18

A company specializing in web application development using Docker containers in an on-premises data center is transitioning its workloads to the cloud, specifically to AWS Fargate. The solutions architect has prepared the required task definition and service for the Fargate cluster. To meet security standards, the cluster is configured within a private subnet of the VPC, which lacks direct external connectivity. However, an error has occurred when launching the Fargate task:

Error Message: `CannotPullContainerError: API error (500): Get [https://111122223333.dkr.ecr.us-east-1.amazonaws.com/v2/] (https://111122223333.dkr.ecr.us-east-1.amazonaws.com/v2/): net/http: request canceled while waiting for connection`

To address this issue, which of the following actions should be taken?

A. Switch the AWS Fargate definition to the “bridge” network mode instead of the “awsvpc” network mode to facilitate Internet connections.

B. Alter the AWS Fargate task definition to enable the auto-assign public IP option. Establish a VPC gateway endpoint for Amazon ECR and modify the route table for AWS Fargate to access Amazon ECR images via the endpoint.

C. Modify the AWS Fargate task definition to disable the auto-assign public IP option. Deploy a NAT gateway within the public subnet of the VPC and adjust the private subnet's route table to direct Internet requests through the NAT gateway.

D. Adjust the AWS Fargate task definition to keep the auto-assign public IP option disabled. Set up a NAT gateway in the private subnet of the VPC and update the route table of the same subnet for Internet routing.

Correct Answer:

C. Update the AWS Fargate task definition to set the auto-assign public IP option to DISABLED. Implement a NAT gateway in the public subnet of the VPC and revise the private subnet's route table to channel requests to the Internet.

Explanation of the Correct Answer and Analysis of Other Options:

Why C is Correct:

- Auto-Assign Public IP Option Disabled: Disabling the auto-assign public IP option in the Fargate task definition is in line with the security requirement to keep the cluster in a private subnet.
- NAT Gateway in Public Subnet: Establishing a NAT gateway in a public subnet and updating the route table of the private subnet to route outbound requests through the NAT gateway is a standard practice. This setup allows instances in a private subnet to access the Internet for tasks like pulling images from Amazon ECR, while still maintaining the security of not having a public IP address.

Why Other Options are Incorrect:

- Option A: Changing to “bridge” network mode is not applicable for AWS Fargate as it only supports the “awsvpc” network mode. This mode ensures that each task has its own elastic network interface.
- Option B: While creating a VPC endpoint for Amazon ECR is a valid approach for certain scenarios, enabling auto-assign public IP contradicts the security requirement of having the cluster in a private subnet. Furthermore, using a VPC endpoint does not address the underlying issue of the Fargate task not being able to access the Internet.
- Option D: Placing a NAT gateway in the private subnet does not align with AWS best practices. NAT gateways should be located in a public subnet to enable instances in a private subnet to initiate outbound traffic to the Internet or other AWS services, while preventing the Internet from initiating a connection with those instances.

Question 19

A media company is utilizing the AWS Cloud to process and convert its video collection. This process is handled by an Auto Scaling group of Amazon EC2 instances, which scales in response to the number of videos in the Amazon Simple Queue Service (SQS) queue. Each video processing task takes approximately 20-40 minutes. To ensure that videos are processed correctly, a redrive policy has been implemented on the SQS queue, serving as a dead-letter queue. The visibility timeout is set to 1 hour and the maxReceiveCount is configured to 1. Additionally, an Amazon CloudWatch alarm notifies the development team when messages are present in the dead-letter queue.

However, after a few days of operation, several videos failed to process and ended up in the dead-letter queue. Despite receiving notifications, the development team did not identify any operational errors from the application logs.

Which of the following solutions should the solutions architect implement to address this issue?

A. Increase the minimum number of EC2 instances in the Auto Scaling group to expedite the scale-up process, ensuring timely processing of videos.

B. Extend the visibility timeout of the Amazon SQS queue to 2 hours to accommodate the processing time of videos that exceed 1 hour.

C. Adjust the delivery delay setting on the Amazon SQS queue, allowing consumers additional time to retrieve messages from the queue.

D. Modify the SQS redrive policy by increasing the maxReceiveCount to 10, enabling multiple retries for messages before they are directed to the dead-letter queue.

Correct Answer:

D. Alter the SQS redrive policy to increase the maxReceiveCount to 10, thereby providing more opportunities for message retries prior to their movement to the dead-letter queue.

Explanation of the Correct Answer and Analysis of Other Options:

Why D is Correct:

- Increasing maxReceiveCount: The key issue seems to be that some videos might be taking longer than the visibility timeout (1 hour) to process, but not necessarily failing due to errors. By increasing the maxReceiveCount to 10, messages (videos) will have more opportunities to be processed successfully before being sent to the dead-letter queue. This approach addresses the potential problem of messages being prematurely marked as failed and moved to the dead-letter queue due to longer processing times.

Why Other Options are Incorrect:

- Option A: While scaling up the number of EC2 instances could reduce the queue length, it does not address the core issue of messages being sent to the dead-letter queue prematurely. The problem does not seem to be linked to insufficient resources but rather the configuration of the SQS queue itself.
- Option B: Extending the visibility timeout to 2 hours could be a plausible solution if the processing time is consistently exceeding 1 hour. However, since the processing time is between 20-40 minutes, this change is unlikely to address the actual issue, which appears to be related to the premature requeuing of messages.
- Option C: Configuring a higher delivery delay does not directly address the problem. The delay setting primarily affects how soon after a message is received it becomes visible to the consumer. It doesn't influence how long the message is processed or how soon it's moved to the dead-letter queue.

Question 20

A media company operating entirely on AWS cloud requires a solution to facilitate the sharing of resources like Amazon S3, AWS KMS, and Amazon ES with another AWS account. The requirement involves providing access to these resources for users from the other account while allowing them to retain their existing user permissions within their own account. Additionally, the solutions architect is tasked with implementing a system for ongoing assessment, auditing, and monitoring of the policy configurations.

In this context, which policy setup would be the most appropriate for meeting these requirements?

A. Implement a service-linked role coupled with an identity-based policy. Utilize AWS Systems Manager rules for regular auditing of IAM policy changes and to ensure configuration compliance.

B. Create a service-linked role with a service control policy. Employ AWS Systems Manager rules to conduct periodic audits of IAM policy changes and to monitor configuration compliance.

C. Establish cross-account access using a resource-based policy. Deploy AWS Config rules to frequently audit changes in the IAM policy and to oversee the configuration's compliance.

D. Configure cross-account access with a user-based policy. Apply AWS Config rules for routine audits of IAM policy alterations and for monitoring the compliance of the setup.

Correct Answer:

C. Set up cross-account access with a resource-based Policy. Utilize AWS Config rules for regular audits of IAM policy modifications and for monitoring the configuration's compliance.

Explanation of the Correct Answer and Analysis of Other Options:

Why C is Correct:

- Resource-Based Policy for Cross-Account Access: This approach enables users from another AWS account to access specified AWS resources (like S3, KMS, and ES) in the media company's account without forgoing their existing permissions in their own account. Resource-based policies are attached directly to the resources and specify who has what permissions to that resource, which is ideal in this scenario for controlled cross-account access.
- Using AWS Config for Audits and Monitoring: AWS Config is the right tool for continuous monitoring and auditing of AWS resources. It can track and record compliance of the AWS resource configurations and evaluate changes against desired configurations. This makes it suitable for ensuring that the cross-account access policies remain compliant with company standards and security requirements.

Why Other Options are Incorrect:

- Options A and B (Service-Linked Role with Identity-Based/Service Control Policies): Service-linked roles are designed for AWS services to access resources in your account on your behalf. They are not typically used for cross-account resource access scenarios described here. Additionally, using AWS Systems Manager for policy audits, while possible, is not as comprehensive as AWS Config in terms of monitoring resource configuration compliance.
- Option D (User-Based Policy Configuration): A user-based policy configures permissions for IAM users within the same account. This does not efficiently cater to the requirement of allowing users from another account to access resources without impacting their existing permissions in their own account.

Question 21

A technology company is in the process of deploying a website using an Amazon S3 bucket. The solutions architect has created an S3 bucket named "www.example.com" in the AWS us-west-2 region. They enabled static website hosting, uploaded static web content including an index.html file, and registered the custom domain www.example.com using Amazon Route 53. Subsequently, a new Route 53 Alias record set pointing to the S3 website endpoint (http://www.example.com.s3-website-us-west-2.amazonaws.com) was configured. Despite these setups, users are unable to view any content on the bucket, and the domains example.com and www.example.com are not functioning as expected.

What is the most probable cause of this issue that the Architect needs to address?

A. The URL does not end with a filename like "index.html", so it is necessary to use the URL www.example.com/index.html.

B. The domain name changes in Route 53 are still in the process of propagating. It is advised to wait another 12 hours before trying again.

C. The website is non-functional because an error.html file has not been specified, which is an essential step.

D. The S3 bucket is not configured with public read access, preventing visitors from accessing the website content.

Correct Answer:

D. The S3 bucket lacks public read access, which is preventing website visitors from accessing the content.

Explanation of the Correct Answer and Analysis of Other Options:

Why D is Correct:

- Public Read Access Requirement: For a website hosted on an Amazon S3 bucket to be accessible to the public, the bucket must be configured with public read access. This setting allows anyone to view or download the content. Without this access, the website's static files cannot be served to users, resulting in the website not being visible to the public.

Why Other Options are Incorrect:

- Option A: The need to append "index.html" to the URL is unnecessary. When static website hosting is enabled on an S3 bucket, the "index.html" file is automatically recognized as the default root document. Therefore, users don't need to specify "index.html" in their browser.
- Option B: Domain name propagation in Route 53 typically happens much faster than 12 hours. While propagation time can vary, issues persisting for more than a few hours are likely due to configuration errors rather than propagation delays.
- Option C: Setting a value for an "error.html" file, while a good practice for handling errors, is not mandatory for the website to work. The primary issue in this scenario is related to access permissions rather than error handling configuration.

Question 21

A stock brokerage firm has its legacy application hosted on Amazon EC2 within a private subnet of an Amazon VPC. Employees access this application via a specialized desktop program on their corporate laptops. The firm's network is connected to AWS through a Direct Connect (DX) link, ensuring fast and reliable access to the private EC2 instances in the VPC. Due to the stringent security requirements typical of financial institutions, the firm needs to encrypt the network traffic flowing from the employees' laptops to the VPC resources.

To fulfill this encryption requirement without compromising the performance provided by Direct Connect, which solution should be implemented?

A. Retain the existing Direct Connect connection, set up a new public virtual interface, and configure the network prefixes for advertisement. Establish a new site-to-site VPN over the Internet and have the employees' laptops connect to this VPN.

B. Maintain the current Direct Connect link, create a new private virtual interface, and specify the network prefixes for advertisement. Set up a new site-to-site VPN to the VPC using the BGP protocol over the DX connection, and adjust the company network to channel employee traffic through this VPN.

C. Keep the existing Direct Connect connection, establish a new private virtual interface, and define the network prefixes for advertisement. Create a new site-to-site VPN to the VPC over the Internet and configure the employees' laptops to use this VPN.

D. Use the current Direct Connect service, create a new public virtual interface, and input the network prefixes to be advertised. Form a new site-to-site VPN to the VPC using the BGP protocol through the DX connection, and route the company network traffic of the employees to this VPN.

Correct Answer:

D. Utilize the existing Direct Connect connection, set up a new public virtual interface and list the network prefixes to advertise. Establish a new site-to-site VPN to the VPC using the BGP protocol over the DX connection. Configure the company network to direct employee traffic through this VPN.

Explanation of the Correct Answer and Analysis of Other Options:

Why D is Correct:

- Public Virtual Interface Requirement: To establish a VPN over DX, a public virtual interface is mandatory. This interface allows the firm to connect to public AWS services, including the VPN endpoint, over the DX connection.
- Site-to-Site VPN with BGP over DX: Setting up a site-to-site VPN using the BGP protocol over the DX connection ensures that the traffic is encrypted, addressing the firm's security requirements. The use of BGP enhances routing efficiency and stability.

- Routing Company Network Traffic to VPN: By routing employee traffic through this VPN, the firm ensures that all communications between the employees' laptops and the AWS resources are encrypted, adhering to the financial industry's strict security standards.

Why Other Options are Incorrect:

- Options A and C: Both these options involve creating a VPN over the Internet, which does not fully utilize the existing DX connection's benefits. Without using a public virtual interface on the DX connection, these options do not comply with the requirement for setting up a VPN over DX.
- Option B: While this option suggests using a private virtual interface, it contradicts the specific requirement that a public virtual interface is necessary for establishing a VPN over a DX connection. Therefore, despite the use of DX and VPN, this setup would not be feasible.

Question 22

A company is developing new mobile applications for Android and iOS platforms and is considering using AWS to store user customization data. This approach aims to provide a consistent experience across different devices for their users, who are expected to number around 3 million and will authenticate using their social login accounts. Each user's preference data is estimated to be around 4 KB in size.

To design a solution that is highly available, cost-effective, scalable, and secure, which approach should the Solutions Architect adopt?

A. Set up an RDS MySQL instance across two availability zones to store user preference data. Implement a public-facing application on a server to manage authentication and access controls.

B. Create a DynamoDB table with an entry for each user, including attributes to store user preferences. Enable the mobile app to directly query user preferences from this table. Implement authentication and authorization using STS, Web Identity Federation, and DynamoDB's Fine-Grained Access Control.

C. Deploy an RDS MySQL instance with multiple read replicas across two availability zones for storing user preference data. Allow the mobile application to query user preferences from these read replicas. Use MySQL's user management and access privilege system for security and access control.

D. Store user preference data in S3, and create a DynamoDB table with an entry for each user, including an attribute pointing to the user's S3 object. Enable the mobile app to first retrieve the S3 URL from DynamoDB, then access the S3 object directly. Utilize STS, Web Identity Federation, and S3 Access Points for this purpose.

Correct Answer:

B. Provision a DynamoDB table for each user's data, with necessary attributes for user preferences. The mobile app will directly query this table. Use STS, Web Identity Federation, and DynamoDB's Fine-Grained Access Control for secure authentication and authorization.

Explanation of the Correct Answer and Analysis of Other Options:

Why B is Correct:

- DynamoDB for Scalability and Performance: DynamoDB is a highly scalable, fully managed NoSQL database service. It's ideal for handling large numbers of small items like user preference data, ensuring high performance and availability.
- Cost-Effectiveness: DynamoDB's pricing model is based on throughput and storage. Given the small size of each user's data (4 KB), DynamoDB can be a cost-effective solution for storing and retrieving millions of small records.
- Security and Access Control: The use of AWS Security Token Service (STS) for temporary credentials, along with Web Identity Federation for social login integration, provides a secure authentication mechanism. DynamoDB’s Fine-Grained Access Control allows precise control over data access at the item level, enhancing security.

Why Other Options are Incorrect:

- Option A: Using RDS MySQL involves more overhead in terms of management and may not be as scalable for millions of small records. Additionally, deploying a front-end server for authentication adds complexity and potential security risks.
- Option C: While RDS MySQL with read replicas offers high availability, it's less scalable for this use case compared to DynamoDB. Managing MySQL's user access controls can also be more complex compared to DynamoDB's integrated access control mechanisms.
- Option D: Storing user preferences in S3 and referencing them in DynamoDB could complicate the data retrieval process and might not be as efficient for small-sized user data. This approach also introduces unnecessary complexity in managing two different data stores.

Question 23

A fast-growing global real estate startup seeks a cost-effective solution to implement location-based alerts in their iOS and Android apps. With an existing user base of 2 million, the app needs to quickly alert users about real estate offers near their current location, ensuring that push notifications are delivered within a minute.

What architecture would be most effective for this purpose?

A. Implement an architecture utilizing an Auto Scaling group of On-Demand EC2 instances behind an API Gateway, which retrieves relevant offers from RDS. For distributing the offers to the mobile app, employ AWS AppSync.

B. Design an architecture where the mobile app sends the user's location to an API Gateway linked with Lambda functions. These functions process the data and fetch relevant offers from an RDS database. Utilize Amazon Pinpoint to dispatch the offers to the mobile app.

C. Configure an architecture where the mobile app transmits the user's location to an SQS queue. This queue is serviced by a fleet of On-Demand EC2 instances that pull relevant offers from a DynamoDB table. Use AWS SNS Mobile Push to forward the offers to the mobile app.

D. Establish an architecture where the mobile app sends the user's location to an SQS queue. A group of On-Demand EC2 instances then retrieves relevant offers from an Amazon Aurora database. To send out the offers, utilize AWS Device Farm.

Best Answer:

C. Configure an architecture where the mobile app transmits the user's location to an SQS queue. This queue is serviced by a fleet of On-Demand EC2 instances that pull relevant offers from a DynamoDB table. Use AWS SNS Mobile Push to forward the offers to the mobile app.

Explanation for Why This is the Best Answer:

- Use of SQS for Managing Requests: Amazon Simple Queue Service (SQS) is an excellent choice for decoupling incoming user location data from the processing servers. It efficiently manages the queue of location requests, ensuring that each user's request is processed without loss of data, even during high traffic periods.
- On-Demand EC2 Instances for Scalable Processing: A fleet of On-Demand EC2 instances can dynamically scale according to the load, ensuring that the processing of location data and retrieval of offers is done efficiently. This setup is crucial to handle the growing number of users and their requests.
- DynamoDB for Storing User Preferences and Offers: Amazon DynamoDB, being a fast and flexible NoSQL database service, is well-suited for handling large volumes of key-value data like user preferences and real estate offers. Its scalability and performance make it ideal for real-time applications like this one.
- AWS SNS Mobile Push for Timely Notifications: AWS Simple Notification Service (SNS) Mobile Push is designed to send vast numbers of notifications to iOS and Android devices efficiently. This service ensures that the push notifications are delivered within the required time frame of less than a minute, meeting the startup's need for prompt delivery of real estate offers.

Let's analyze why the other proposed solutions are less suitable for the scenario described:

Option A: Auto Scaling EC2 with API Gateway and RDS, using AWS AppSync for Notifications

- **Inefficient for Real-Time Alerts**: Utilizing an Auto Scaling group of EC2 instances behind an API Gateway to retrieve data from RDS can handle the load, but this setup might not be the most efficient for real-time processing of location-based data due to potential latency in data retrieval and processing.
- **AppSync for Data Synchronization, Not Optimal for Push Notifications**: AWS AppSync is primarily designed for data synchronization and real-time updates in applications, rather than delivering push notifications like AWS SNS Mobile Push. While it can handle real-time data, it's not specifically optimized for the use case of sending time-sensitive push notifications.

Option B: API Gateway with Lambda and RDS, using Amazon Pinpoint

- **Potential Latency Issues**: While Lambda functions can efficiently process incoming requests, using RDS for storage might introduce latency, especially when scaling to millions of users. Retrieving individual user preferences from a relational database could be slower compared to a NoSQL solution like DynamoDB.
- **Amazon Pinpoint's Overhead**: Amazon Pinpoint is more focused on user engagement and analytics. While it can send push notifications, its primary use case is broader than just delivering notifications, potentially introducing unnecessary features and complexities for this specific requirement.

Option D: SQS with EC2 and Amazon Aurora, using AWS Device Farm

- **Complexity and Performance Concerns**: Using SQS with a fleet of EC2 instances to interact with Amazon Aurora for data retrieval introduces a level of complexity that might not be necessary. Aurora, being a relational database, may not provide the same level of performance for key-value data retrieval as DynamoDB in this context.
- **Inappropriate Use of AWS Device Farm**: AWS Device Farm is a service intended for testing mobile and web applications on real devices in the cloud. It is not designed for, nor capable of, sending push notifications to users, which makes it an unsuitable choice for this requirement.

Question 24

A company is contemplating a migration of its workload to AWS cloud. The objective for the solutions architect is to minimize the time spent on database instance management in their current on-premises data center by transitioning to a managed relational database service like Amazon RDS. Additionally, the architect aims to migrate the application from the on-premises data center to a fully managed platform such as AWS Elastic Beanstalk.

What would be the most cost-effective migration approach to achieve these objectives?

A. Switch to a different product (Repurchase)
B. Lift and shift the existing setup to the cloud (Rehost)
C. Move to a new platform with minimal changes (Replatform)
D. Completely overhaul and optimize the architecture (Refactor / Re-architect)

Best Answer:

C. Replatform

Explanation for Why Replatform is the Correct Answer and Analysis of Other Options:

Why Replatform is Correct:

- Minimal Alterations for Efficiency: Replatforming involves making a few adjustments to reap the benefits of the new platform without significantly altering the core architecture. Migrating to Amazon RDS and AWS Elastic Beanstalk fits this definition as it involves moving to managed services with only necessary modifications to the application and database.
- Balancing Cost and Benefit: Replatforming strikes a balance between the cost of migration and the benefits of cloud features. It avoids the higher costs associated with refactoring while delivering more significant benefits compared to simply rehosting.

Why Other Options are Less Suitable:

- A. Repurchase (Switching to a different product): Repurchasing, often referred to as "drop and shop," involves moving to a completely different product. This strategy might be more expensive and doesn't align with the goal of reducing management overhead while leveraging existing investments.
- B. Rehost (Lift and shift): Rehosting is about moving existing applications to the cloud as-is. While this might be a quick migration strategy, it doesn't fully utilize cloud-native features like managed database services (RDS) or managed application services (Elastic Beanstalk) that reduce management overhead.
- D. Refactor / Re-architect (Overhauling the architecture): This approach involves significant changes to the application to take full advantage of cloud-native features. While it can provide the most optimization, it is also the most costly and time-consuming option, which might not be necessary for the company’s current goals.

Question 25

A company is developing a cryptocurrency trading platform to be hosted on AWS, requiring a robust security setup within a single VPC. The architecture must effectively defend against distributed denial-of-service (DDoS) attacks and safeguard the applications and systems. This includes alerts for incoming Layer 3 or Layer 4 attacks, like SYN floods and UDP reflection, as well as protection against Layer 7 threats such as SQL injection and cross-site scripting.

To fulfill these requirements, which two solutions should the solutions architect combine?

A. Implement AWS Network Firewall for rule-based filtering of network traffic.

B. Utilize CloudFront web distribution to enhance cache hit ratio and position servers behind it.

C. Forward network logs to Amazon Fraud Detector for DDoS attack detection and send notifications to the security team.

D. Deploy AWS WAF to establish customizable web security rules that regulate traffic access to web applications.

E. Implement AWS Shield Advanced for improved DDoS attack detection and monitoring, particularly for application-layer traffic directed at AWS resources.

Best Answer:

D. Use AWS WAF to create custom web security rules that dictate which traffic is allowed to reach your web applications.

E. Implement AWS Shield Advanced for enhanced detection and monitoring of DDoS attacks, focusing on application-layer traffic to AWS resources.

Explanation for Why These Answers are Correct and Analysis of Other Options:

Why D and E are Correct:

- AWS WAF (D): AWS Web Application Firewall (WAF) is specifically designed to protect web applications from common web exploits that could affect availability, compromise security, or consume excessive resources. It allows for custom rule creation to block common attack patterns, such as SQL injection or cross-site scripting, addressing Layer 7 security concerns.
- AWS Shield Advanced (E): AWS Shield Advanced offers comprehensive protection against DDoS attacks, including Layer 3 and Layer 4 attacks. It provides additional detection and mitigation capabilities, especially for larger and more sophisticated

attacks, along with 24/7 access to the AWS DDoS Response Team (DRT) and detailed reports.

Why Other Options are Less Suitable:

- AWS Network Firewall (A): While AWS Network Firewall provides customizable network-level security, it's more focused on internal VPC traffic management and lacks the specialized DDoS protection and application-layer defense capabilities of AWS WAF and AWS Shield Advanced.
- CloudFront for Caching (B): Using CloudFront can indirectly help in mitigating DDoS attacks by distributing traffic. However, it primarily serves as a content delivery network and is not specifically designed for DDoS attack detection or protection, nor does it provide defenses against specific web application attacks like SQL injection.
- Amazon Fraud Detector (C): Amazon Fraud Detector is tailored for detecting fraudulent activities, such as online payment fraud and identity theft. It is not designed for detecting or notifying about DDoS attacks, nor does it provide the necessary web application layer protection.

Question 26

A startup, operating its customer support application on AWS, utilizes Auto Scaling EC2 on-demand instances behind an Elastic Load Balancer. The application, which extensively processes data stored in DynamoDB, runs on large EC2 instances. Deployments of new application versions occur weekly, necessitating an automated process for creating and testing new Amazon Machine Images. To address an increasing volume of support tickets, the startup plans to add a video chat feature to its support app, requiring hosting on separate servers. The startup aims to employ AWS OpsWorks for streamlined application management and deployment.

What is the most effective and cost-efficient method for incorporating the new video chat feature into the AWS environment?

A. Establish an AWS OpsWorks stack with dual layers and a single custom recipe.

B. Configure two separate AWS OpsWorks stacks, each having dual layers and a single custom recipe.

C. Implement an AWS OpsWorks stack containing a single layer and one custom recipe.

D. Set up two distinct AWS OpsWorks stacks, with each comprising two layers and two custom recipes.

Best Answer:

A. Create an AWS OpsWorks stack, with two layers, and one custom recipe.

Explanation for Why This is the Correct Answer and Analysis of Other Options:

Why A is Correct:

- Single OpsWorks Stack for Unified Management: Using a single AWS OpsWorks stack provides a centralized and unified framework for managing both the existing customer support application and the new video chat module. This approach simplifies administrative overhead and enhances coordination between different components of the application.
- Two Layers for Separate Components: Creating two layers within the OpsWorks stack allows for clear separation and independent management of the primary application and the new video chat feature. This separation is vital for ensuring that the different resource and scaling needs of each component are appropriately addressed.
- One Custom Recipe for Consistency: Utilizing a single custom recipe across both layers helps maintain consistency in configuration and deployment processes. It streamlines the automation of the environment setup, ensuring that both parts of the application adhere to the same standards and practices.

Why Other Options are Less Suitable:

- B. Two Separate OpsWorks Stacks: Having two separate OpsWorks stacks introduces unnecessary complexity and can lead to fragmented management of what is essentially a single application with different components. It complicates the deployment process and makes coordination more challenging.
- C. Single Layer in OpsWorks Stack: Implementing only one layer would imply a lack of clear separation between the main application and the video chat feature. This could lead to potential resource contention and difficulties in scaling and managing each component independently.
- D. Two Separate Stacks with Two Custom Recipes: This option not only separates the application into two different stacks, which adds complexity, but also introduces two different custom recipes. This could lead to inconsistencies in configuration and deployment practices between the two components.

Question 27

A corporation operates thousands of Linux and Microsoft Windows virtual servers in its local data center. These servers support Java and PHP applications that utilize MySQL and Oracle databases, and they are complemented by several departmental services hosted in an external data center. SAN storage is used for iSCSI disk provisioning to physical servers. Facing the challenge of outdated and incomplete technical documentation, the company intends to shift its data center to the AWS Cloud. A Solutions Architect is assigned the task of analyzing the existing setup and estimating the costs associated with the cloud migration.

To effectively orchestrate this cloud migration, what steps should the Solutions Architect take? (Choose THREE.)

A. Employ AWS Application Discovery Service to collect data about active virtual machines and applications within these servers.

B. Utilize AWS Application Migration Service (MGN) to automate the transfer of on-premises virtual machines to the AWS Cloud.

C. Apply Amazon Inspector to examine and evaluate the applications on the on-premises virtual machines, storing reports in an Amazon S3 bucket.

D. Implement AWS X-Ray to scrutinize applications in the servers and pinpoint potential migration-related errors.

E. Use the AWS Cloud Adoption Readiness Tool (CART) for creating a migration assessment report, identifying organizational skills and process gaps.

F. Deploy AWS Migration Hub for the identification and monitoring of application migration progress involving AWS and partner solutions.

Best Answer:

A. Utilize AWS Application Discovery Service for information gathering on operational virtual machines and server applications.

E. Leverage the AWS Cloud Adoption Readiness Tool (CART) to produce a migration evaluation report, pinpointing organizational skill and process deficiencies.

F. Implement AWS Migration Hub to detect and oversee application migration status via AWS and associated solutions.

Explanation for Why These Answers are Correct and Analysis of Other Options:

Why A, E, and F are Correct:

- A. AWS Application Discovery Service: This service aids in understanding the existing on-premises environment by collecting crucial information about VMs and running applications. This knowledge is vital for planning the migration and estimating costs.
- E. AWS Cloud Adoption Readiness Tool (CART): CART helps in assessing the organization's readiness for cloud adoption. It identifies areas where the company might

need to develop skills or modify processes, crucial for successful cloud migration planning.

- F. AWS Migration Hub: Migration Hub provides a central location to track and manage migrations from on-premises to AWS. It helps in overseeing the entire migration process, ensuring all components are accounted for and transitioned smoothly.

Why Other Options are Less Suitable:

- B. AWS Application Migration Service (MGN): While MGN is useful for the actual migration process, it does not contribute to the initial analysis and planning stages of the migration.
- C. Amazon Inspector: This service is designed for security assessment and compliance of running applications and does not specifically aid in migration planning or cost estimation.
- D. AWS X-Ray: X-Ray is focused on analyzing and debugging applications, particularly in a microservices architecture. It's more suited for performance analysis and troubleshooting, not for initial migration planning.

Question 28

An insurance company is looking to integrate their stock market data processing, which currently occurs in their on-premises data center using Apache Kafka, with AWS to provide near-real-time data to their web application. The web application is critical for production, so the solution requires consistent high-performance networking. The company aims to achieve this integration while ensuring scalability and reliability.

To meet these requirements, which three actions should the solutions architect take?

A. Set up a Site-to-Site VPN from the on-premises data center to the AWS VPC for cost-effective and consistent performance.

B. Develop a Lambda function to handle the Amazon Kinesis data stream and write a GraphQL API in AWS AppSync to trigger the function. Use the @connections command to send callback messages to connected clients.

C. Create a Lambda function to process the Amazon Kinesis data stream and establish a WebSocket API in Amazon API Gateway to invoke the function. Utilize the @connections command to dispatch callback messages to connected clients.

D. Retrieve messages from the on-premises Apache Kafka cluster using an Amazon EC2 Auto Scaling Group. Forward the data into an Amazon Kinesis Data Stream using the Amazon Kinesis Producer Library.

E. Acquire messages from the on-premises Apache Kafka cluster via an Auto Scaling group of EC2 instances. Channel the data into an Amazon Kinesis Data Stream using the Amazon Kinesis Consumer Library.

F. Request an AWS Direct Connect link from the on-premises data center to the AWS VPC for steadfast performance.

Best Answer:

C. Implement a Lambda function for processing Amazon Kinesis data stream and configure a WebSocket API in Amazon API Gateway to activate the function. Use the @connections command for relaying callback messages to clients.

D. Extract messages from the local Apache Kafka cluster with an Amazon EC2 Auto Scaling Group and transmit the data into an Amazon Kinesis Data Stream via the Amazon Kinesis Producer Library.

F. Opt for an AWS Direct Connect connection from the on-premises data center to the AWS VPC to ensure consistent and high-performance networking.

Explanation for Why These Answers are Correct and Analysis of Other Options:

Why C, D, and F are Correct:

- C. WebSocket API with Lambda and API Gateway: Utilizing a Lambda function to process Kinesis streams and a WebSocket API in API Gateway for real-time communication is highly effective for near-real-time data processing. It allows for a scalable solution that can handle high throughput and provides low-latency communication to the web app.
- D. EC2 Auto Scaling with Kinesis Producer Library: Using EC2 instances within an Auto Scaling group to pull data from Kafka and then pushing it to Kinesis via the Kinesis Producer Library provides a scalable and reliable way to ingest data into AWS. This setup is optimal for handling varying loads and ensures the data is readily available for processing by AWS services.
- F. AWS Direct Connect for Consistent Performance: Direct Connect provides a dedicated network connection between the on-premises data center and AWS, offering more consistent network performance compared to internet-based connections like VPN. This is crucial for mission-critical applications that require stable and high-throughput networking.

Why Other Options are Less Suitable:

- A. Site-to-Site VPN: While a VPN can connect on-premises to AWS, it may not offer the same level of consistent, high-performance networking as Direct Connect, especially for high-volume data transfers.
- B. GraphQL API in AWS AppSync: AppSync with GraphQL is more suited for managing and delivering application data with APIs but may not be the best fit for real-time, high-volume data processing tasks like the company's requirement.
- E. Kinesis Consumer Library: The Consumer Library is used for consuming data from Kinesis streams, not for producing or ingesting data into Kinesis from external sources like Kafka.

Question 29

A company is developing a mobile application for the Department of Transportation, enabling government personnel to upload recent photos of infrastructure projects across the country. These photos, upon being uploaded via the app, are sent to a web server on an EC2 instance, where a watermark containing project details and the date is added. The photos then need to be stored securely and durably in an S3 bucket. The task of the solutions architect is to devise a secure method for the EC2 instance to upload these watermarked photos to S3.

Which architecture ensures secure uploading of photos to S3 by the EC2 instance?

A. Establish an IAM role with the necessary permissions for listing and writing objects in the S3 bucket. Associate this IAM role with the EC2 instance, enabling it to acquire temporary security credentials from the instance metadata for uploading photos to S3.

B. Configure an IAM user with permissions to list and write objects in the S3 bucket. Launch the EC2 instance as this IAM user, which will allow the instance to obtain temporary security credentials from the instance user data for photo uploads to S3.

C. Create an IAM service role with the required permissions to list and write objects to the S3 bucket. Link this IAM role to the EC2 instance, granting it the capability to access temporary security credentials from the instance user data to upload photos to S3.

D. Implement a service control policy (SCP) with permissions for listing and writing objects to the S3 bucket. Attach this SCP to the EC2 instance, thus enabling it to fetch temporary security credentials from the instance metadata for S3 photo uploads.

Best Answer:

A. Configure an IAM role with necessary S3 access permissions and associate it with the EC2 instance. This will allow the instance to use temporary security credentials obtained from the instance metadata to upload photos to the S3 bucket.

Explanation for Why This Answer is Correct and Analysis of Other Options:

Why A is Correct:

- IAM Role for EC2 Instances: IAM roles for EC2 instances are the recommended way to grant permissions to applications running on EC2 instances. These roles provide temporary credentials that are automatically rotated and securely delivered via the instance metadata. This method is secure and efficient, as it does not involve managing static credentials.
- Permissions for S3 Access: The role can be configured with specific permissions to list and write objects to the S3 bucket, ensuring that the EC2 instance has the necessary access to perform its task without granting excessive permissions.

Why Other Options are Less Suitable:

- B. IAM User for EC2 Instance: IAM users are primarily intended for individuals. Using IAM users for EC2 instances is not recommended because it involves managing access keys, which can be less secure than the temporary credentials provided by IAM roles.
- C. IAM Service Role Misunderstanding: While IAM service roles are used in AWS, the description in Option C mixes concepts. The retrieval of temporary security credentials is not done through instance user data but through instance metadata.
- D. Service Control Policy (SCP): SCPs are used within AWS Organizations to manage permissions for all accounts in the organization. They are not designed for granting permissions to EC2 instances or for accessing S3 buckets. SCPs also do not provide a way to retrieve temporary security credentials as described.

Question 30

An electric utility company has implemented smart meters for its customers, enabling them to monitor their electricity usage effectively. These meters transmit data every five minutes to an Amazon API Gateway, and the data is then processed by AWS Lambda functions before being stored in an Amazon DynamoDB table. Initially, the processing time was about 5 to 10 seconds, but as the customer base expanded and new metrics were added, the processing time increased to 60 to 90 seconds. The system has started encountering errors like TooManyRequestsException and ProvisionedThroughputExceededException during PUT operations on the DynamoDB table.

To address these issues, which two actions should be taken?

A. Enhance the memory allocated to the Lambda functions to manage the increased processing load due to the additional metrics.

B. Modify the Write Capacity Unit (WCU) settings of the DynamoDB table to handle the increased write requests from the Lambda functions.

C. To reduce the number of requests, increase the payload size from the meters but decrease the frequency of data transmission to avoid exceeding the concurrency limit of Lambda functions.

D. Opt for batch processing of data to prevent exceeding DynamoDB's write limits. Consolidate requests from API Gateway by funneling the data through an Amazon Kinesis data stream.

E. Implement an Amazon SQS FIFO queue to manage the surge of data from the smart meters. Configure the Lambda function to execute upon receiving a message in the queue.

Best Answer:

B. Adjust the Write Capacity Unit (WCU) of the DynamoDB table to accommodate all the write requests processed by the Lambda functions.

D. Group and batch process the incoming data to avoid DynamoDB write limit issues. Streamline the requests from API Gateway by using an Amazon Kinesis data stream.

Explanation for Why These Answers are Correct and Analysis of Other Options:

Why B and D are Correct:

- B. Adjusting WCU of DynamoDB: Increasing the WCU for the DynamoDB table is crucial to handle the larger volume of write requests. This adjustment is directly related to the ProvisionedThroughputExceededException error and ensures that DynamoDB can efficiently accommodate the increased write load.
- D. Batch Processing with Kinesis: Utilizing Amazon Kinesis to batch and streamline data from the API Gateway before processing it in Lambda functions is an effective way to manage large volumes of data. This approach reduces the number of write requests to DynamoDB, helping to prevent throughput limitations and optimize processing efficiency.

Why Other Options are Less Suitable:

- A. Increasing Lambda Memory: While increasing Lambda memory might speed up processing, it does not address the fundamental issues causing the errors, namely the write throughput limitations of DynamoDB and the high volume of concurrent Lambda invocations.
- C. Increasing Payload Size and Reducing Frequency: Altering the payload size and frequency could potentially reduce the number of requests, but this doesn't solve the

underlying problem of DynamoDB's write capacity and could lead to data not being as current or up-to-date.

- E. Using SQS FIFO Queue: While SQS can help manage incoming data, it does not directly address the ProvisionedThroughputExceededException error with DynamoDB. Additionally, FIFO queues have their own limitations in terms of throughput (300 transactions per second), which might not be sufficient for this use case.

Question 31

A company with multiple business units, each having one or more AWS accounts, faces challenges in their production environment where resources like Amazon EC2 instances, Amazon EKS clusters, and Amazon Aurora Serverless databases are mistakenly terminated by developers from other business units. The solutions architect is tasked with devising a strategy to ensure that only the business unit owning specific AWS resources can terminate them.

What is the most effective multi-account strategy to achieve this goal?

A. Implement AWS Organizations for centralized management of all accounts. Group accounts related to each business unit into separate Organizational Units (OU). In the production account, establish a Service Control Policy (SCP) allowing access to EC2 instances, including resource-level permissions for termination specific to each business unit. Distribute cross-account access and the SCP to the OUs for inheritance by member accounts.

B. Utilize AWS Organizations to manage accounts centrally. Assign accounts of a particular business unit to distinct OUs. In the production account, create an IAM Role with a policy granting access to EC2 instances, including resource-level permissions to terminate instances owned by the respective business unit. Extend cross-account access and the IAM policy to all member accounts of the OU.

C. Leverage AWS Organizations for centralized account management. Allocate accounts from each business unit to an individual OU. Formulate a Service Control Policy in the production account for each business unit, specifying permissions to access and terminate EC2 instances they own. Provide cross-account access and the SCP to individual member accounts for strict control over instance termination.

D. Use AWS Organizations for centralized control of all accounts. Group business unit-specific accounts into individual OUs. In the production account, create an IAM Role for each business unit with policies for accessing and terminating their EC2 instances. Establish an AWSServiceRoleForOrganizations service-linked role for each member account in the OU to facilitate trusted access.

Best Answer:

B. Set up AWS Organizations to manage all accounts centrally. Organize accounts related to each business unit into individual OUs. Generate an IAM Role within the production account endowed with a policy that authorizes access to EC2 instances and resource-level termination permissions for instances belonging to a particular business unit. Provide this cross-account access and IAM policy to every account within the OU.

Explanation for Why This Answer is Correct and Analysis of Other Options:

Why B is Correct:

- Centralized Management with AWS Organizations: Utilizing AWS Organizations provides an efficient way to manage all accounts and group them into OUs based on business units.
- IAM Role for Resource-Level Permissions: Creating an IAM Role with specific policies in the production account allows for fine-grained control over which business unit can access and terminate their EC2 instances. This setup ensures that each business unit has the necessary permissions to manage only their resources, addressing the issue of accidental termination.
- Cross-Account Access: Distributing this IAM role and policy to every member account in the OU ensures that all accounts related to a specific business unit have the same level of access and control over their resources, maintaining consistency across the organization.

Why Other Options are Less Suitable:

- A and C. Service Control Policies (SCP): While SCPs are effective for defining what actions are allowed or denied in member accounts, they are not the best tool for granting specific resource-level permissions like terminating an EC2 instance. SCPs are more about setting guardrails for member accounts rather than granting detailed operational permissions.
- D. Service-Linked Role for Organizations: The creation of an IAM Role for each business unit in the production account with specific policies is a good approach, but the inclusion of an AWSServiceRoleForOrganizations service-linked role does not directly contribute to solving the issue of resource-level permissions for termination of instances.

Question 32

A multinational software provider in the US operates its development and test environments in separate AWS accounts, both hosted in the cloud. The company's CTO has decided to manage billing through a Master AWS account using Consolidated Billing. To ensure budget compliance, administrators in the master account need the capability to stop, delete, and terminate resources in both the development and test environment accounts.

What is the recommended course of action to enable the master account administrators to effectively manage resources in the development and test accounts?

A. Set up IAM users in the master account and establish a cross-account role with full administrative permissions for the Development and Test accounts.

B. Create IAM users with full administrative permissions in the master account. In the Development and Test accounts, configure cross-account roles that allow the master account to access resources in these accounts based on permissions set in the master account.

C. Rely on the linkage of all accounts under Consolidated Billing to automatically grant IAM users in the master account access to resources in the Development and Test accounts.

D. Initially, create IAM users in the master account. Subsequently, in the Development and Test accounts, set up cross-account roles endowed with full administrative permissions, authorizing access for the master account.

Best Answer:

D. Initially establish IAM users in the master account. Then, in both the Development and Test accounts, configure cross-account roles with complete administrative permissions, thereby granting access to the master account.

Explanation for Why This Answer is Correct and Analysis of Other Options:

Why D is Correct:

- IAM Users in Master Account: Creating IAM users in the master account is a good practice for managing access and permissions centrally. These users will be the ones managing resources across the Development and Test accounts.
- Cross-Account Roles for Access: Setting up cross-account roles in the Development and Test accounts with full administrative permissions is a secure and effective way to grant the necessary access to the master account. These roles ensure that administrators in the master account can perform required actions (stop, delete, terminate) in the Development and Test environments without compromising security best practices.

Why Other Options are Less Suitable:

- A. Single Cross-Account Role from Master Account: Creating a cross-account role in the master account that has administrative access to both Development and Test accounts is not practical nor secure. Roles should be created in the accounts to be accessed, not in the accessing account.

- B. Inherited Permissions from Master Account: The concept of inheriting permissions from the master account through cross-account roles is not how AWS IAM works. Each AWS account maintains its own set of roles and permissions, and permissions are not inherited across accounts in this manner.
- C. Consolidated Billing Does Not Grant Access: Linking accounts under Consolidated Billing for billing purposes does not grant IAM users in the master account automatic access to resources in the linked accounts. Access and permissions need to be set up separately.

Question 33

A company is planning to move its Oracle Real Application Clusters (RAC) database from an on-premises data center to AWS. In line with this, the company's Chief Information Security Officer (CISO) has mandated the automation of the operating system's patch management where the database operates and the establishment of scheduled backups for disaster recovery compliance.

What should the solutions architect implement to fulfill the company's requirements with minimal effort?

A. Initiate a Lambda function to automate database snapshot creation on the EC2 instance. Employ AWS CodeDeploy and CodePipeline for the database's operating system patch management.

B. Transition the database to Amazon Aurora, enabling automated backups for the Aurora RAC cluster. System patching in Aurora is automated during the maintenance window.

C. Migrate the database to Amazon RDS, which offers a multi-AZ failover feature suitable for the RAC cluster. This reduces Recovery Point Objective (RPO) and Recovery Time Objective (RTO) in case of system failure. RDS also provides automated patch management and underlying host maintenance.

D. Transfer the database to a cluster of EBS-backed Amazon EC2 instances spread across multiple Availability Zones (AZs). Automate EBS snapshot creation using Amazon Data Lifecycle Manager. Install the SSM Agent on the EC2 instances and automate the patch management process with AWS Systems Manager Patch Manager.

Best Answer:

D. Migrate the database to a cluster of EBS-backed Amazon EC2 instances across various AZs. Implement automated creation of EBS snapshots from these instances' EBS volumes using Amazon Data Lifecycle Manager. Install SSM Agent on the EC2 instances and manage the operating system patching process using AWS Systems Manager Patch Manager.

Explanation for Why This Answer is Correct and Analysis of Other Options:

Why D is Correct:

- EBS-Backed EC2 Instances for RAC Database: Oracle RAC databases require specific configurations that are best supported on EC2 instances. Using EBS-backed instances allows for the necessary customization and performance.
- Automated EBS Snapshots with Data Lifecycle Manager: Data Lifecycle Manager automates the creation of EBS snapshots, meeting the backup requirement efficiently.
- Patch Management with AWS Systems Manager: AWS Systems Manager Patch Manager automates the patching process of the operating system, ensuring compliance with the CISO's mandate for automated patch management.

Why Other Options are Less Suitable:

- A. Lambda for Snapshots and CodeDeploy/CodePipeline: While Lambda can automate snapshot creation, using AWS CodeDeploy and CodePipeline for OS patch management is more complex and less efficient than Systems Manager Patch Manager. This setup also requires additional effort to configure and maintain.
- B. Amazon Aurora: Aurora is a relational database service by AWS but does not support Oracle RAC. Thus, it is not suitable for the company’s specific database migration requirement.
- C. Amazon RDS for Oracle RAC: Amazon RDS supports Oracle databases but does not support Oracle RAC configurations. Thus, it cannot fulfill the specific requirements of the company's Oracle RAC database.

Question 34

A prominent call center company based in Seattle has its corporate web portal hosted on AWS, connected to its on-premises data center via a link aggregation group (LAG) that terminates at an AWS Direct Connect endpoint. This setup is linked to a private virtual interface (VIF) in their VPC. The portal needs to authenticate against the company's on-premises LDAP server, and each Amazon S3 bucket should only be accessible to the corresponding authenticated user.

To meet these requirements, what should the solutions architect implement in AWS? (Choose TWO.)

A. Develop an identity broker to assume an IAM role and obtain temporary AWS security credentials via IAM Security Token Service (STS). The application receives these temporary credentials from the identity broker for accessing the relevant S3 bucket.

B. Implement an identity broker for LDAP authentication and use it to call IAM Security Token Service (STS) to acquire IAM federated user credentials. The application then retrieves these federated credentials from the broker to access the specific S3 bucket.

C. The application initially authenticates against LDAP to ascertain the name of an IAM role linked to the user. It then assumes this role through IAM Security Token Service (STS), utilizing the role's temporary credentials to access the designated S3 bucket.

D. Replace the Direct Connect connection with a Direct Connect Gateway and establish a Transit VPC for LDAP authentication against the on-premises server.

E. The application authenticates via LDAP, then employs LDAP credentials to log into the IAM service. It then accesses the required S3 bucket using IAM temporary credentials.

Best Answer:

B. Set up an identity broker for LDAP authentication, and have it invoke IAM Security Token Service (STS) to obtain IAM federated user credentials. The application then utilizes these federated credentials, provided by the broker, to access the appropriate S3 bucket.

C. Initially, the application performs LDAP authentication to determine the associated IAM role's name. Subsequently, it assumes that role by contacting IAM Security Token Service (STS). The application then uses the temporary credentials from this role to access the relevant S3 bucket.

Explanation for Why These Answers are Correct and Analysis of Other Options:

Why B and C are Correct:

- B. IAM Federated User Credentials: Using an identity broker to facilitate LDAP authentication and then obtaining IAM federated user credentials via STS is an effective way to integrate AWS access with existing authentication systems. This approach allows for secure, controlled access to S3 buckets based on user identity.
- C. Assuming IAM Role via LDAP: This method allows the application to authenticate against LDAP, determine the IAM role linked to the user, and then assume this role to get temporary credentials. This is a secure and efficient way to grant access to AWS resources like S3 while leveraging existing LDAP infrastructure.

Why Other Options are Less Suitable:

- A. Identity Broker Assuming IAM Role: While this option involves an identity broker and STS, it does not explicitly mention LDAP authentication, which is a key requirement in this scenario.

- D. Direct Connect Gateway and Transit VPC: This solution addresses networking infrastructure but does not directly address the requirement for LDAP-based authentication and controlled access to S3 buckets.
- E. Using LDAP Credentials for IAM Login: LDAP credentials cannot be directly used to log into the IAM service. The preferred method is to use an identity broker with STS for secure, federated access to AWS resources.

Question 35

A company has a data analyst team that regularly uploads data points to an Amazon S3 bucket. These data points need to be replicated to other S3 buckets across various AWS Accounts within the company. To achieve this, a Solutions Architect set up an AWS Lambda function triggered by S3 PUT events on the primary bucket to handle the replication process. Given the high volume of uploads expected daily, there is a concern that this Lambda function might impact other critical Lambda functions due to AWS Lambda's regional concurrency limits. The replication process is not time-sensitive. The company seeks a solution to ensure that the replication Lambda function does not interfere with the execution of other critical Lambda functions.

Which of the following solutions would best address these requirements with minimal development effort?

A. Implement an exponential backoff strategy in the Lambda function to prevent it from running when the concurrency limit is hit. Monitor the Throttles metric for Lambda functions using Amazon CloudWatch alarms.

B. Separate the Amazon S3 event notifications by sending them to an Amazon SQS queue in a different AWS account. Also, set up the Lambda function in this account and trigger it upon receiving SQS messages.

C. Set a reserved concurrency limit for the new Lambda function to control its maximum concurrent executions. Employ Amazon CloudWatch alarms to keep track of the Throttles metric for Lambda functions to avoid reaching the concurrency limit.

D. Adjust the Lambda function's execution timeout to 5 minutes, allowing it to wait for the completion of other Lambda functions if the concurrency limit is reached. Utilize Amazon CloudWatch alarms to observe the Throttles metric for Lambda functions.

Best Answer:

C. Establish a reserved concurrency limit for the replication Lambda function to manage its concurrent executions. Use Amazon CloudWatch alarms to monitor the Throttles metric for

Lambda functions, ensuring the concurrency limit is not exceeded.

Explanation for Why This Answer is Correct and Analysis of Other Options:

Why C is Correct:

- Reserved Concurrency Control: Setting a reserved concurrency limit for the replication Lambda function is an efficient way to prevent it from consuming too many resources and affecting other critical Lambda functions. This approach allocates a specific number of concurrent executions to this function, ensuring it does not consume all available Lambda concurrency in the region.
- Monitoring with CloudWatch Alarms: Using CloudWatch alarms to monitor the Throttles metric allows for proactive management and alerts if the function approaches or hits its concurrency limit, enabling timely intervention.

Why Other Options are Less Suitable:

- A. Exponential Backoff Strategy: While exponential backoff can help manage retries when the function is throttled, it does not prevent the Lambda function from consuming too many concurrency resources in the first place. It also adds complexity to the function's code.
- B. Separate SQS Queue in a Different Account: Decoupling S3 events to an SQS queue in a different account adds unnecessary complexity and does not directly address the issue of Lambda concurrency in the primary account.
- D. Increasing Execution Timeout: Extending the execution timeout to 5 minutes does not prevent the function from consuming too many concurrency resources. It could also lead to inefficiencies, as the function might remain idle for extended periods, waiting for other executions to complete.

Question 36

A company overseeing numerous AWS client accounts has established a centralized logging service utilizing an Auto Scaling group of Amazon EC2 instances. This service receives logs from client accounts via AWS PrivateLink, with interface endpoints established in each client account. The EC2 instances for the logging service are distributed across several subnets, with a Network Load Balancer (NLB) to distribute incoming traffic. However, clients are currently unable to send logs through the VPC endpoint.

To resolve this issue, which two solutions are most appropriate? (Select TWO.)

A. Confirm that the Network Access Control List (NACL) linked to the subnets of the logging service permits traffic to and from the NLB subnets. Also, verify that the NACL associated with the NLB subnets allows traffic to and from the subnets hosting the EC2 instances for the logging service.

B. Ensure that the NACL for the logging service subnets facilitates traffic to and from the interface endpoint. Also, check that the NACL for the subnet of the interface endpoint permits traffic to and from the EC2 instances running the logging service.

C. Adjust the security group of the EC2 instances hosting the logging service to allow inbound traffic from the IP address range of the clients.

D. Modify the security group attached to the EC2 instances hosting the logging service to permit inbound traffic from the NLB's security group. Also, ensure the security group linked to the NLB authorizes inbound traffic from the subnet of the interface endpoint.

E. Verify that the Auto Scaling group is tied to a launch template with the latest Amazon Machine Image (AMI) and that the EC2 instances are using types optimized for log processing.

Best Answer:

A. Check that the NACL associated with the logging service's subnets permits communication to and from the NLB subnets, and that the NACL associated with the NLB subnets allows traffic to and from the subnets of the EC2 instances running the logging service.

D. Ensure the security group for the EC2 instances hosting the logging service allows inbound traffic from the NLB's security group, and that the NLB's security group allows inbound traffic from the subnet of the interface endpoint.

Explanation for Why These Answers are Correct and Analysis of Other Options:

Why A and D are Correct:

- A. NACL Configuration: Proper NACL configuration is crucial for allowing traffic between subnets. In this case, ensuring that the NACLs for both the logging service and the NLB subnets are correctly configured to allow necessary communication is essential for the functionality of the logging service.
- D. Security Group Configuration: Security groups act as virtual firewalls for EC2 instances. The security group attached to the EC2 instances needs to allow inbound traffic from the NLB's security group, and conversely, the NLB's security group should permit traffic from the interface endpoint subnet. This bidirectional allowance ensures that the traffic from the client accounts can reach the logging service through the NLB.

Why Other Options are Less Suitable:

- B. NACL for Interface Endpoint and Logging Service: While NACLs are important, this option doesn’t focus on the correct traffic flow needed between the NLB and the EC2 instances.
- C. Inbound Traffic from Client IP Range: Allowing traffic based on the IP range of clients does not align with the architecture involving PrivateLink and NLB. It's more relevant to ensure the security group configurations are correct in relation to the NLB and EC2 instances.
- E. Launch Template and Instance Types: While using the latest AMI and appropriate instance types is generally a good practice, it does not address the immediate connectivity issue faced by the logging service in this scenario.

Question 37

A gaming company's new mobile game has gone viral, leading to a surge in user registrations globally. The registration website, hosted on Amazon EC2 instances in an Auto Scaling group and balanced by an Application Load Balancer, serves static content that varies based on the user's device type. Due to the unexpected spike in traffic, the EC2 instances are experiencing high CPU usage, and users are experiencing slow website performance.

To enhance website response time, which solution should the Solutions Architect implement?

A. Set up distinct Auto Scaling groups for each device type and pair them with separate Application Load Balancers (ALB). Use Amazon Route 53 to direct users to the correct ALB based on their User-Agent HTTP header.

B. Host the static content in an Amazon S3 bucket and designate this bucket as the source for an Amazon CloudFront distribution. Configure CloudFront to deliver varied content based on the user’s User-Agent HTTP header.

C. Place the static content in an Amazon S3 bucket and use it as the origin for an Amazon CloudFront distribution. Implement a Lambda@Edge function to interpret the User-Agent HTTP header and provide the right content according to the user's device type.

D. Switch to a Network Load Balancer (NLB) instead of an ALB for distributing user traffic. Create dedicated Auto Scaling groups for different device types and set up the NLB to filter traffic based on the User-Agent HTTP header, directing users to the appropriate EC2 Auto Scaling group.

Best Answer:

C. Create an Amazon S3 bucket to house the static content and establish it as the origin for an Amazon CloudFront distribution. Utilize a Lambda@Edge function to analyze the User-Agent HTTP header and serve suitable content depending on the user's device type.

Explanation for Why This Answer is Correct and Analysis of Other Options:

Why C is Correct:

- Offloading Static Content to S3 and CloudFront: Using Amazon S3 and CloudFront to host and deliver static content efficiently offloads the demand from the EC2 instances. This approach reduces the load on the EC2 instances, addressing the high CPU usage issue.
- Lambda@Edge for Device-Specific Content: Implementing Lambda@Edge allows for dynamic content delivery at the edge locations based on the user's device type, as identified in the User-Agent header. This ensures that users receive optimized content for their specific devices, enhancing user experience.

Why Other Options are Less Suitable:

- A. Separate ALBs for Device Types: Creating separate Auto Scaling groups and ALBs for different device types adds unnecessary complexity and may not efficiently address the issue of high CPU usage on the EC2 instances.
- B. CloudFront with User-Agent Header Configuration: While using CloudFront to deliver static content is a good approach, this option does not mention the use of Lambda@Edge for dynamic content delivery based on the device type, which is crucial for optimizing the user experience.
- D. Using NLB and Device-Specific Auto Scaling Groups: Switching to an NLB and segmenting Auto Scaling groups by device type is more complex and may not provide the desired improvement in website performance. NLBs are typically used for routing TCP/UDP traffic and do not offer the same level of content-based routing capabilities as ALBs or the dynamic content optimization offered by CloudFront with Lambda@Edge.

Question 38

A company operating a logistics and shipment tracking application on AWS for its warehouse operations is seeking to transition from an email-based system to a serverless application model. This change aims to reduce operational overhead and reliance on emails for package shipping processes.

What solution should the Solutions Architect implement to align with the company's requirements?

A. Implement AWS Batch jobs for various packaging tasks. Use an AWS Lambda function with AWS Batch as the trigger for creating and printing shipping labels. When the package is scanned and dispatched, trigger another Lambda function to advance the AWS Batch job to the subsequent shipping stage.

B. Utilize an Amazon SQS queue to store new orders. Schedule a Lambda function to check the queue every 5 minutes for orders and begin processing if found. Employ another Lambda function for printing shipping labels. After package dispatch, use Amazon Pinpoint to notify customers about their order status.

C. Record order details in an Amazon DynamoDB table. Configure an AWS Step Functions workflow to be activated with each new order. This workflow should mark the order as “in progress,” print the shipping label, and, upon scanning and dispatching the package, trigger a Lambda function to update the order status to “shipped” and conclude the Step Functions workflow.

D. Use Amazon EFS to store new order data. Set up an instance to retrieve order details from the EFS share and print shipping labels. Following package dispatch, utilize an Amazon API Gateway call to the instances to erase the order data from the EFS share.

Best Answer:

C. Store order information in an Amazon DynamoDB table. Establish an AWS Step Functions workflow for each new order, marking the order as “in progress” and managing the printing of shipping labels. Once the package is scanned and exits the warehouse, activate a Lambda function to label the order as “shipped” and finalize the Step Functions workflow.

Explanation for Why This Answer is Correct and Analysis of Other Options:

Why C is Correct:

- DynamoDB for Order Storage: Using Amazon DynamoDB for storing order information is efficient and scalable, suitable for a serverless architecture.
- Step Functions for Workflow Management: AWS Step Functions is ideal for orchestrating multiple steps (like marking the order, printing labels, and updating status). It provides a clear, visual workflow and ensures each step is executed in sequence.
- Lambda for Status Update: Using AWS Lambda to update the order status after dispatch is a serverless solution that aligns with the goal of reducing operational overhead.

Why Other Options are Less Suitable:

- A. AWS Batch and Lambda: This option introduces unnecessary complexity with AWS Batch, which is more suited for batch processing workloads and not ideal for real-time order processing in this scenario.
- B. SQS Queue and Pinpoint: While using SQS for order storage is feasible, polling every 5 minutes could introduce delays. Using Amazon Pinpoint for customer notifications is not directly related to internal order processing and shipping label printing.

- D. Amazon EFS and API Gateway: This approach does not align with the serverless model the company is aiming for. Managing an EFS volume and an EC2 instance for pulling and processing orders introduces additional complexity and maintenance.

Question 39

A company is utilizing AWS Managed Active Directory Service to manage their Active Directory with a custom domain name, private.tutorialsdojo.com, in the AWS Cloud. They have set up a pair of default domain controllers within their VPC and created a VPC interface endpoint for Amazon Kinesis using AWS Private Link. Despite these configurations, the EC2 instances launched in the VPC are unable to resolve the company's custom AD domain name.

To enable the instances to resolve both the AWS VPC endpoints and the AWS Managed Microsoft AD domain’s Fully Qualified Domain Name (FQDN), what steps should the Solutions Architect take? (Choose TWO.)

A. Establish an outbound endpoint in the Amazon Route 53 console and configure AmazonProvidedDNS as the DNS resolver for the VPC.

B. Implement a forwarding rule within the endpoint to direct queries for private.tutorialsdojo.com to the IP addresses of the two domain controllers.

C. Modify the DNS settings on each client in the VPC to use split DNS queries, utilizing the Active Directory servers for the custom AD domain and the VPC resolver for all other DNS queries.

D. Set up an inbound endpoint in the Amazon Route 53 console and designate AmazonProvidedDNS as the DNS resolver for the VPC.

E. Create a conditional forwarder within the endpoint to reroute any queries for private.tutorialsdojo.com to the IP addresses of the domain controllers.

Best Answer:

A. Configure an outbound endpoint on the Amazon Route 53 console, setting AmazonProvidedDNS as the VPC's DNS resolver.

B. Construct a forwarding rule inside the endpoint to relay queries for private.tutorialsdojo.com to the domain controllers' IP addresses.

Explanation for Why These Answers are Correct and Analysis of Other Options:

Why A and B are Correct:

- A. Outbound Endpoint with AmazonProvidedDNS: Creating an outbound endpoint in Amazon Route 53 and using AmazonProvidedDNS as the DNS resolver for the VPC ensures that DNS queries within the VPC are handled correctly. This configuration allows the VPC to resolve both AWS service endpoints and custom AD domain names.
- B. Forwarding Rule for Custom AD Domain: Implementing a forwarding rule to direct queries for the custom AD domain name to the domain controllers ensures that DNS requests for the AD domain are accurately resolved. This step is crucial to correctly integrate the custom AD domain with AWS services.

Why Other Options are Less Suitable:

- C. Split DNS Configuration on Each Client: Configuring split DNS on every client in the VPC is not practical and does not leverage the centralized DNS management capabilities of Route 53. This approach would be more complex and harder to maintain.
- D. Inbound Endpoint in Route 53: Setting up an inbound endpoint is not relevant in this context, as the requirement is to resolve DNS queries within the VPC, which is better achieved through an outbound endpoint.
- E. Conditional Forwarder within the Endpoint: While creating a conditional forwarder might seem like a viable option, it is not necessary in this case. The combination of an outbound endpoint and a forwarding rule (Options A and B) is sufficient and more straightforward for the given requirements.

Question 40

A technology company operating an industrial chain orchestration software on AWS wishes to enhance its service to be more cost-effective, scalable, highly available, and less reliant on manual intervention. The software currently utilizes a web application tier running on a fixed number of Amazon EC2 instances and a database tier on Amazon RDS, with the web tier in a public subnet and the database tier in a private subnet of the VPC.

To improve availability and load balancing in this cloud architecture, which two actions should the Solutions Architect take?

A. Implement an Application Load Balancer in front of the web servers and create an Alias Record in Amazon Route 53 that directs to the load balancer's DNS name.

B. Set up an Amazon CloudFront distribution pointing to the private IP addresses of the web servers and establish a CNAME record in Route 53 linked to the CloudFront distribution.

C. Install a NAT instance in the VPC and modify the route table to include a default route via the NAT instance for all subnets. Configure a DNS A Record in Route 53 pointing to the NAT instance's public IP address.

D. Deploy a load balancer in front of the web servers and establish a Non-Alias Record in Route 53 that corresponds to the load balancer's DNS name.

E. Create a Non-Alias Record in Route 53 using Multivalue Answer Routing and include all IP addresses of the web servers.

Best Answer:

A. Deploy an Application Load Balancer in front of all web servers and configure a new Alias Record in Route 53 that maps to the load balancer’s DNS name.

E. Configure a Non-Alias Record in Route 53 with Multivalue Answer Routing and add all IP addresses of the web servers.

Explanation for Why These Answers are Correct and Analysis of Other Options:

Why A and E are Correct:

- A. Application Load Balancer with Alias Record: An Application Load Balancer efficiently distributes incoming web traffic across multiple EC2 instances, enhancing scalability and availability. Using an Alias Record in Route 53 to point to the load balancer allows for seamless integration and DNS-level load balancing.
- E. Multivalue Answer Routing in Route 53: Creating a Non-Alias Record with Multivalue Answer Routing in Route 53 and including the IP addresses of all web servers offers a simple method to distribute traffic across multiple servers, improving fault tolerance and availability.

Why Other Options are Less Suitable:

- B. CloudFront with CNAME Record: Using CloudFront and pointing it to the private IP addresses of the web servers isn’t typically used for internal load balancing and doesn’t align with the goal of improving availability and scalability within the AWS environment.
- C. NAT Instance with DNS A Record: Configuring a NAT instance and a DNS A Record pointing to its public IP address is more relevant for allowing instances in a private subnet to access the internet, not for improving internal load distribution and availability.
- D. Load Balancer with Non-Alias Record: While deploying a load balancer is beneficial, using a Non-Alias Record in Route 53 for the load balancer's DNS name is less effective compared to an Alias Record. Alias Records are specifically designed for AWS resources like load balancers and provide better integration and management.

Question 41

An international insurance company stores financial files in an Amazon S3 bucket, accessible via S3 URLs or through a CloudFront distribution. The company now needs to ensure that only a specific client in California can access this data.

To fulfill this requirement, which two actions should be taken?

A. Implement CloudFront Signed Cookies to restrict access to the files, ensuring only the specified client can access them. Activate HTTPS on the CloudFront distribution.

B. Create a new S3 bucket in the US West (N. California) region, upload the files there, and establish an origin access control (OAC) to permit reading the files from the bucket. Also, enable HTTPS on the CloudFront distribution.

C. Use CloudFront signed URLs to guarantee exclusive access to the files by the intended client. Implement field-level encryption in the CloudFront distribution.

D. Utilize CloudFront signed URLs to restrict file access to the specific client. Set up an origin access control (OAC) granting read permission for the files in the bucket. Disallow the use of Amazon S3 URLs for file access by anyone else.

E. Create a new S3 bucket in the US West (N. California) region, upload the files, and use S3 pre-signed URLs to control access to the files. Prohibit the use of standard Amazon S3 URLs for accessing the files by others.

Best Answer:

D. Use CloudFront signed URLs to ensure exclusive client access to the files. Establish an origin access control (OAC) with read permission for the bucket files. Restrict the use of Amazon S3 URLs for file access by others.

E. Create a new S3 bucket in the US West (N. California) region, transfer the files, and generate S3 pre-signed URLs for controlled file access. Prevent access to the files using standard Amazon S3 URLs by others.

Explanation for Why These Answers are Correct and Analysis of Other Options:

Why D and E are Correct:

- D. CloudFront Signed URLs and OAC: CloudFront signed URLs are an effective way to control access to content, allowing only specific users (in this case, the client in California) to access the files. Combined with OAC, which restricts bucket access to only the CloudFront distribution, this ensures secure and exclusive access.
- E. New S3 Bucket and Pre-Signed URLs: Creating a new S3 bucket in the specific region (US West - N. California) and utilizing S3 pre-signed URLs further ensures that only the intended recipient can access the files. By disabling standard S3 URL access, unauthorized access is prevented.

Why Other Options are Less Suitable:

- A. CloudFront Signed Cookies: While CloudFront Signed Cookies can restrict access, they are more suited for scenarios where multiple files need to be accessed, such as an entire directory, rather than specific files. Signed URLs are more appropriate for limited file access.
- B. New S3 Bucket and OAC: Although creating a new bucket in a specific region and setting up OAC is viable, this option lacks a mechanism (like signed URLs) to ensure that only the specific client can access the files.
- C. CloudFront Signed URLs and Field-Level Encryption: While signed URLs are suitable, field-level encryption is unnecessary for this scenario and adds complexity without addressing the core requirement of exclusive client access.

Question 42

A multinational healthcare company is preparing to launch a new MedTech information website, and the Solutions Architect plans to deploy a three-tier web application using Amazon CloudFormation. This application comprises a web tier, an application tier, and a database tier using Amazon DynamoDB. To ensure secure access to the database tier, the architect needs to safeguard any credentials used for database access.

Which method will allow application instances to access DynamoDB tables without revealing API credentials?

A. In the CloudFormation template, create an IAM User with permissions for DynamoDB table read and write access. Use CloudFormation's GetAtt function to extract the access and secret keys, then pass these to the application instance via user-data.

B. Establish an IAM Role with DynamoDB access. Utilize AWS::SSM::Parameter to create an SSM parameter in AWS Systems Manager Parameter Store containing the IAM role's Amazon Resource Name (ARN). Link the application instance's instance profile property to this role.

C. Prompt users to provide access and secret keys for an existing IAM User with DynamoDB read/write permissions, rather than using the Parameter section in the CloudFormation template.

D. Create an IAM Role with the necessary permissions for DynamoDB read and write access. Link the application instance's instance profile property to this role.

Best Answer:

D. Generate an IAM Role with appropriate DynamoDB access permissions. Connect the instance profile property of the application instance to this role.

Explanation for Why This Answer is Correct and Analysis of Other Options:

Why D is Correct:

- IAM Role for Secure Access: Creating an IAM Role with specific DynamoDB permissions and associating it with the EC2 instance profile is a secure and best practice method. This approach allows application instances to access DynamoDB without the need to manage or expose API credentials. IAM roles provide temporary credentials automatically to the instances, reducing the risk associated with long-term credentials.

Why Other Options are Less Suitable:

- A. Creating IAM User in Template: This method involves passing access and secret keys directly to instances, which is not a secure practice. It risks exposing sensitive credentials and is not recommended, especially when IAM roles provide a safer alternative.
- B. Using AWS Systems Manager Parameter Store: While using the Parameter Store for storing credentials is secure, in this scenario, it's unnecessary since IAM roles can provide the needed permissions without the need to manage credentials.
- C. User-Entered IAM User Credentials: Asking users to enter IAM User credentials directly into CloudFormation is insecure and cumbersome. It poses a significant security risk as it involves handling long-term credentials manually.

Question 43

A telecommunications company needs to enhance data leak protection for its Amazon EC2 instances within an AWS VPC. The requirement is to restrict internet access for these instances, permitting only the ability to fetch product updates and patches from specific URLs on the internet, while explicitly denying all other outbound connections.

What should the solutions architect do to align with these requirements?

A. Configure security groups with outbound access rules that specifically allow fetching software packages from the internet.

B. Relocate all instances from public to private subnets, remove default routes from routing tables, and replace them with routes targeting the specific package locations.

C. Implement network Access Control List (ACL) rules that authorize network access only to designated package destinations and include an implicit deny rule for all other scenarios.

D. Deploy a forward web proxy server in the VPC and control outbound access via URL-based rules, while also removing the default routes.

Best Answer:

D. Set up a forward web proxy server in the VPC, managing outbound access through URL-based rules. Concurrently, eliminate default routes.

Explanation for Why This Answer is Correct and Analysis of Other Options:

Why D is Correct:

- Forward Web Proxy for Controlled Access: A forward web proxy server within the VPC enables granular control over internet access based on URLs. This setup allows the company to specifically permit access to URLs for software packages while denying all other outbound internet connections, effectively meeting the data leak protection goal.
- URL-Based Rules and Route Management: Managing outbound access through URL-based rules on the proxy server aligns precisely with the requirement to limit access to specific internet locations. Removing default routes further ensures that no outbound traffic is allowed except for the permitted URLs through the proxy.

Why Other Options are Less Suitable:

- A. Security Groups with Outbound Rules: While security groups can restrict outbound traffic, they are not capable of filtering traffic based on URLs. Security groups work on IP addresses and ports, which may not be sufficient for the company's specific need to allow access to certain URLs only.
- B. Moving to Private Subnets and Routing Table Changes: Simply moving instances to private subnets and modifying routing tables might not provide the necessary level of control for accessing specific URLs while blocking others.
- C. Network ACL with Specific Access Rules: Network ACLs offer broader network-level control and, like security groups, they do not offer URL-based filtering. They work with IP ranges, ports, and protocols, which does not align with the requirement for URL-specific access control.

Question 44

An online stock trading application operating in multiple Availability Zones in the us-east-1 region uses RDS for its database. The company requires a disaster recovery strategy that ensures scalability, high availability, and resilience, with a Recovery Time Objective (RTO) of less than 2 hours and a Recovery Point Objective (RPO) of 10 minutes.

Which two disaster recovery strategies should be implemented to meet these RTO and RPO requirements?

A. Implement synchronous “source-replica” replication between multiple Availability Zones for the database.

B. Schedule 15-minute database backups to Glacier with transaction logs stored in S3 every 5 minutes.

C. Conduct hourly database backups to an S3 bucket with transaction logs stored in S3 every 5 minutes, and establish Cross-Region Replication (CRR) to another AWS Region.

D. Create an AWS Backup plan for the Amazon RDS database, enabling continuous backups for point-in-time recovery (PITR).

E. Store hourly database backups on an EC2 instance store volume, and save transaction logs to an S3 bucket every 5 minutes.

Best Answer:

C. Perform hourly database backups to an S3 bucket, store transaction logs in S3 every 5 minutes, and configure Cross-Region Replication (CRR) to another AWS Region.

D. Set up an AWS Backup plan for the Amazon RDS database with continuous backups for point-in-time recovery (PITR) enabled.

Explanation for Why These Answers are Correct and Analysis of Other Options:

Why C and D are Correct:

- C. Hourly Backups with CRR: Performing hourly backups with transaction logs stored every 5 minutes ensures that the most recent data is available for recovery, meeting the 10-minute RPO. Cross-Region Replication provides geographical redundancy, enhancing disaster resilience and contributing to meeting the RTO requirement.
- D. AWS Backup with PITR: Enabling continuous backups for PITR on RDS using AWS Backup ensures that the database can be restored to any point in time within a retention period. This meets the RPO requirement and helps ensure high availability and disaster resilience.

Why Other Options are Less Suitable:

- A. Synchronous Replication in AZs: While synchronous replication across AZs provides high availability, it does not address the RTO and RPO requirements for disaster recovery in a different region.
- B. 15-minute Backups to Glacier: Storing backups in Glacier every 15 minutes does not align with the required 10-minute RPO. Additionally, Glacier’s retrieval time may not meet the 2-hour RTO due to its longer access times.

- E. Hourly Backups on Instance Store: Storing backups on an EC2 instance store volume is risky as this storage is ephemeral. If the instance fails, the data is lost, which does not align with the required resilience and RPO/RTO requirements.

Question 45

A finance company is launching a new website featuring tutorials for their mobile app, with static media files stored in a private Amazon S3 bucket and dynamic contents hosted on an AWS Fargate cluster behind an Application Load Balancer (ALB). Both static and dynamic contents are accessible via a CloudFront distribution, with an Amazon Route 53 Alias record directing the website URL to CloudFront. The company seeks to ensure exclusive access to both static and dynamic content through CloudFront.

To achieve this, which two solutions should be implemented?

A. Configure CloudFront to inject a custom header into all origin requests. Utilize AWS WAF to create a rule that blocks requests lacking this custom header, and associate this web ACL with the CloudFront distribution.

B. Adjust the Amazon S3 bucket ACL to deny all access except for requests originating from the Amazon CloudFront distribution.

C. Establish a network ACL (NACL) that permits connections only from Amazon CloudFront, and link this NACL to the subnets hosting the Application Load Balancer.

D. Formulate a specific CloudFront user known as an origin access control (OAC) and link it to the distribution. Modify the S3 bucket policy to allow access exclusively from the OAC.

E. Implement CloudFront to add a custom header to all origin requests. With AWS WAF, create a rule that rejects requests without this custom header, and attach this web ACL to the Application Load Balancer.

Best Answer:

D. Create an origin access control (OAC) user for CloudFront and associate it with the distribution. Amend the S3 bucket policy to permit access solely from the OAC.

E. Utilize CloudFront to add a custom header to all origin requests. Develop a web rule in AWS WAF that denies requests missing this custom header, and link this web ACL to the Application Load Balancer.

Explanation for Why These Answers are Correct and Analysis of Other Options:

Why D and E are Correct:

- D. Origin Access Control (OAC) for CloudFront: Establishing an OAC for CloudFront and configuring the S3 bucket policy to accept requests only from this OAC ensures that static content in the S3 bucket is accessed exclusively through CloudFront.
- E. Custom Header and AWS WAF Rule with ALB: Adding a custom header to CloudFront origin requests and creating a corresponding AWS WAF rule that blocks requests without this header, associated with the ALB, ensures that dynamic content hosted on AWS Fargate is also accessed solely via CloudFront.

Why Other Options are Less Suitable:

- A. WAF Rule with CloudFront Distribution: While adding a custom header and a corresponding WAF rule is effective, associating this rule with the CloudFront distribution itself does not specifically restrict access to the Fargate cluster behind the ALB.
- B. S3 Bucket ACL: Modifying S3 bucket ACLs can help restrict access to the bucket, but it's not as secure or flexible as using an OAC, which is specifically designed for use with CloudFront.
- C. Network ACL for ALB: Configuring a NACL to allow only CloudFront traffic is less practical and effective compared to using WAF with custom headers. NACLs operate at a lower level and are not designed for controlling access based on specific CloudFront distributions or custom headers.

Question 46

A prominent fast-food chain with a hybrid cloud infrastructure extending into AWS Cloud requires a solution to enable on-premises users, already authenticated via corporate accounts, to manage AWS resources without necessitating separate IAM users for each individual. This approach aims to eliminate the need for multiple login credentials.

What is the most effective method to manage user authentication in this hybrid architecture?

A. Integrate the company's authentication system with Amazon AppFlow, utilize Amazon STS to obtain temporary AWS credentials through OAuth 2.0, facilitating AWS Console access for users.

B. Leverage the company's on-premises SAML 2.0-compliant identity provider (IDP) to authenticate, use STS to acquire temporary credentials, and provide federated access to the AWS console through the AWS IAM Identity Center.

C. Use the on-premises SAML 2.0-compliant IDP for authentication, apply STS with AssumeRoleWithWebIdentity to get temporary security credentials, allowing users to access the AWS console via a browser.

D. Obtain temporary AWS security credentials via Web Identity Federation using STS and AssumeRoleWithWebIdentity, enabling user access to the AWS console.

Best Answer:

B. Authenticate with the on-premises SAML 2.0-compliant identity provider (IDP), retrieve temporary credentials through STS, and enable federated access to the AWS console using the AWS IAM Identity Center.

Explanation for Why This Answer is Correct and Analysis of Other Options:

Why B is Correct:

- SAML 2.0-Compliant IDP for Authentication: Using the existing SAML 2.0-compliant IDP allows for seamless integration of on-premises user authentication with AWS. This method leverages the existing corporate credentials, thus eliminating the need for separate IAM users.
- Temporary Credentials via STS: The AWS Security Token Service (STS) enables the generation of temporary, limited-privilege credentials for federated users, ensuring secure access without long-term credentials.
- Federated Access via AWS IAM Identity Center: The AWS IAM Identity Center provides a centralized location to manage federated access, simplifying the process of granting on-premises users access to AWS resources.

Why Other Options are Less Suitable:

- A. Amazon AppFlow with OAuth 2.0: This option is not viable as Amazon AppFlow is intended for data integration and does not support the scenario described. OAuth 2.0 is not typically used for federating identity with AWS services in this context.
- C. AssumeRoleWithWebIdentity: While using AssumeRoleWithWebIdentity is a valid approach for certain scenarios, it is more commonly used with web identity providers like Google, Facebook, or Amazon. For corporate credentials, SAML 2.0 integration (as in option B) is more appropriate.
- D. Web Identity Federation: This is generally used with identity providers for consumer applications (like Google, Facebook, or Amazon), not for corporate identity providers.

Question 47

A shipping firm with web applications in its on-premises data center, reliant on non-x86 hardware, is looking to AWS to augment its data storage capabilities. The backup application requires POSIX-compatible block-based storage, and there's a need to mount 1,000 TB of data files to a single folder on the file server. Additionally, it's crucial that users have access to parts of this data during the backup process.

Among the available backup solutions, which one is most suitable for these requirements?

A. Utilize Amazon Glacier as the storage destination for data backups.

B. Set up Gateway Stored Volumes through AWS Storage Gateway.

C. Configure Gateway Cached Volumes via AWS Storage Gateway.

D. Opt for Amazon S3 as the storage target for data backups.

Best Answer:

C. Implement Gateway Cached Volumes using AWS Storage Gateway.

Explanation for Why This Answer is Correct and Analysis of Other Options:

Why C is Correct:

- Gateway Cached Volumes: Gateway Cached Volumes in AWS Storage Gateway provide a solution that caches frequently accessed data on-premises while storing the entire dataset in AWS. This setup meets the POSIX-compatible block-based storage requirement and allows for mounting a large dataset (1,000 TB) to a single folder. Importantly, it enables users to access the data even during backup processes, as only a cache of the most used data is kept on-premises while the rest is stored in AWS.

Why Other Options are Less Suitable:

- A. Amazon Glacier: While Glacier is a cost-effective solution for long-term backups, it doesn't provide the immediate, block-level access required in this scenario. Glacier is more suitable for archival purposes rather than for scenarios requiring frequent access.
- B. Gateway Stored Volumes: Gateway Stored Volumes keep the entire dataset on-premises and asynchronously back it up to AWS. This would not be as effective for scaling on-premises data storage to AWS, especially given the large volume (1,000 TB) of data involved.
- D. Amazon S3: Directly using Amazon S3 for backups doesn't align well with the need for POSIX-compatible block-based storage and might not integrate seamlessly with the company's existing backup application.

Question 48

A mobile game startup developing an augmented reality (AR) multiplayer shooter game hosted on AWS has experienced slow loading times for game assets and static content. To improve load times, caching has been recommended.

Which cache services should be utilized for enhancing the performance of their gaming applications?

A. Implement Amazon CloudFront for distributing static content and use Apache Ignite ElastiCache as an in-memory data store.

B. Deploy Amazon CloudFront for static content distribution and utilize Amazon DynamoDB as an in-memory data store.

C. Use AWS ElastiCache for distributing static content and employ CloudFront as an in-memory data store.

D. Utilize Amazon CloudFront to distribute static content and Amazon ElastiCache as an in-memory data store.

Best Answer:

D. Employ Amazon CloudFront for distributing static content and Amazon ElastiCache as an in-memory data store.

Explanation for Why This Answer is Correct and Analysis of Other Options:

Why D is Correct:

- CloudFront for Static Content: Amazon CloudFront is a content delivery network (CDN) service that is ideal for distributing static content globally, thereby reducing latency and improving load times for static assets.
- ElastiCache as In-Memory Data Store: Amazon ElastiCache provides an in-memory data store, which is perfect for caching frequently accessed game data and assets. This can significantly reduce load times and enhance overall game performance.

Why Other Options are Less Suitable:

- A. Apache Ignite ElastiCache: Apache Ignite is not part of AWS ElastiCache. AWS ElastiCache primarily supports Redis and Memcached, which are more appropriate and integrated solutions within the AWS ecosystem.
- B. DynamoDB as In-Memory Data Store: While Amazon DynamoDB is a powerful NoSQL database service, it is not primarily designed as an in-memory data store. For caching purposes, ElastiCache is a more fitting choice.
- C. ElastiCache for Static Content and CloudFront as In-Memory Data Store: This option misplaces the roles of ElastiCache and CloudFront. ElastiCache is not suitable for distributing static content, and CloudFront is not an in-memory data store.

Question 49

A company utilizes an on-premises identity provider (IdP) for employee authentication and has established a SAML 2.0 based federated identity solution integrating with this IdP for AWS environment access. The Solutions Architect can access AWS via this federation, but other test users cannot.

To ensure proper configuration of identity federation, which three aspects should be verified?

A. Confirm that AWS environment resources within the VPC can reach the on-premises IdP using its DNS hostname.

B. Check that the IAM policy for each user includes "Allow" permissions for SAML federation.

C. Verify that the trust policy of IAM roles for federated users or groups designates the SAML provider as the principal.

D. Ensure inclusion of the SAML provider's ARN, the ARN of the created IAM role, and the SAML assertion from the IdP in the federated identity web portal's call to the AWS STS AssumeRoleWithSAML API.

E. Check the company's IdP to make sure that users are part of the default AWSFederatedUser IAM group, a standard feature in AWS.

F. Confirm that appropriate IAM roles are mapped to company users and groups in the IdP's SAML assertions.

Best Answer:

C. Ensure the IAM roles' trust policies for federated users/groups correctly set the SAML provider as the principal.

D. Validate that the federated identity web portal's call to AWS STS AssumeRoleWithSAML API includes the SAML provider's ARN, the IAM role's ARN, and the SAML assertion from the IdP.

F. Verify the correct mapping of IAM roles to company users and groups in the SAML assertions from the IdP.

Explanation for Why These Answers are Correct and Analysis of Other Options:

Why C, D, and F are Correct:

- C. Trust Policy of IAM Roles: Correct trust policy configuration in IAM roles is critical. This policy must correctly reference the SAML provider as the principal to allow users authenticated by the IdP to assume these roles.

- D. STS AssumeRoleWithSAML API Call: The call to AWS STS AssumeRoleWithSAML API must include the SAML provider's ARN, IAM role's ARN, and the SAML assertion from the IdP. This ensures that the federation process operates correctly, mapping the authenticated user to the right AWS permissions.
- F. IAM Role Mapping in SAML Assertions: Proper mapping of IAM roles in the SAML assertions is crucial for federated identity to work correctly. This mapping tells AWS which IAM roles are accessible to the users authenticated by the IdP.

Why Other Options are Less Suitable:

- A. Resources Reaching IdP via DNS: While network connectivity to the IdP is important, it's unlikely the cause of the issue if the Solutions Architect can authenticate successfully.
- B. IAM Policy for SAML Federation: IAM policies for individual users are not directly relevant in a SAML federation scenario, as access is managed through IAM roles specified in the SAML assertion.
- E. Default AWSFederatedUser IAM Group: There is no default AWSFederatedUser IAM group in AWS. Access is managed through the mapping of federation users to IAM roles, not IAM groups.

Question 50

A car parts manufacturer has implemented IP cameras on their production line to capture images for quality inspection. These images are used to identify defects by comparing them with baseline images through a machine learning (ML) model trained using Amazon SageMaker. The setup requires that workers receive immediate feedback from an API hosted on a local on-premises Linux server. The company needs this system to remain operational even during internet outages.

Which deployment strategy should be adopted to integrate the ML model and meet the operational requirements?

A. Install the AWS IoT Greengrass software on an additional server located on-site. Execute ML inferences on this Greengrass server using the model developed in Amazon SageMaker. Configure Greengrass components to communicate with the on-premises Linux server's API upon detecting any defects.

B. Utilize AWS IoT Analytics to process data from the images captured. Perform ML analysis on each image and compile a report to be sent to the on-premises Linux server's API.

C. Implement an AWS Outposts server in the local data center to establish an AWS private cloud environment. Use Amazon SageMaker on this server for ML training and integrate Amazon Rekognition to identify defects in the car parts.

D. Acquire an AWS Snowball Edge Compute Optimized device for its computational capabilities to handle the ML training model. Transition the Linux server to an Amazon EC2 instance on the Snowball device and configure the IP cameras to forward images to Snowball's local storage for processing by the EC2 server.

Best Answer:

A. Integrate AWS IoT Greengrass client software onto a supplementary local server. Conduct ML inference on this server drawing from the SageMaker-trained model. Employ Greengrass components for interaction with the Linux server's API when defects are identified.

Explanation for Why This Answer is Correct and Analysis of Other Options:

Why A is Correct:

- Local Execution with IoT Greengrass: AWS IoT Greengrass enables local compute, messaging, data caching, sync, and ML inference capabilities to edge devices. This allows the company to run the inference locally, ensuring the system operates effectively even when internet connectivity is compromised.
- ML Model Inference: The local Greengrass server can run the ML model trained in Amazon SageMaker directly on the premises, providing quick and reliable defect detection.
- API Interaction: Greengrass components can directly interact with the local Linux server API, enabling immediate feedback to workers without the need for cloud connectivity.

Why Other Options are Less Suitable:

- B. AWS IoT Analytics: IoT Analytics is primarily for processing and analyzing data streams over the internet, not for local processing without internet connectivity.
- C. AWS Outposts: Outposts bring native AWS services to on-premises locations, but they require consistent internet connectivity to AWS Regions to operate fully, which does not support the requirement for internet outage resilience.
- D. AWS Snowball Edge: While Snowball Edge provides local compute and storage, it's more tailored for data transfer and edge computing workloads, not as a permanent solution for running ongoing ML inference models as required in the manufacturer's operational environment.

Question 51

A company with a widely-used blogging platform hosted on AWS experiences a high volume of blog entries, with a noticeable decrease in access rate six months post-publishing and minimal access after one year. The entries are frequently updated in the initial three months but see no updates after six months. The company aims to utilize CloudFront to enhance the loading speed of the platform.

What is the most effective AWS implementation for this use case?

A. Set up two distinct CloudFront distributions, one optimized for US/Europe users with the US-Europe price class, and another for the rest of the world with all edge locations enabled.

B. Utilize a single Amazon S3 bucket, organized by the month of blog entry submission, to store the entries in corresponding partitions. Establish a CloudFront distribution that has permissions to access this S3 bucket exclusively.

C. Configure a CloudFront distribution with the 'Restrict Viewer Access' setting enabled and the 'Forward Query String' option set to true, with a minimum Time-to-Live (TTL) of zero.

D. Maintain two versions of each blog entry in separate S3 buckets, each linked to its own CloudFront distribution, with S3 access allowed only for the associated CloudFront identity.

Best Answer:

B. Employ a single S3 source bucket, structured by submission month for blog entries, storing each entry in the relevant partition. Create a CloudFront distribution with permissions set to access the S3 bucket and configured to allow access solely through it.

Explanation for Why This Answer is Correct and Analysis of Other Options:

Why B is Correct:

- S3 Partitioning for Organization: Partitioning the S3 bucket according to the month of submission helps manage the lifecycle of blog entries effectively, aligning with their access patterns and update frequency.
- Single CloudFront Distribution: A single CloudFront distribution with exclusive S3 bucket access simplifies the architecture. Restricting the distribution access to the S3 bucket enhances security and ensures that CloudFront is the primary access point for users, which can improve caching effectiveness and loading times.

Why Other Options are Less Suitable:

- A. Multiple CloudFront Distributions: Creating separate distributions for different geographic regions is unnecessary and could complicate management without significant performance gain, given CloudFront's global presence and intelligent routing.
- C. Forward Query String with TTL: Setting the 'Forward Query String' to true and a minimum TTL of zero does not leverage CloudFront's caching capabilities effectively, which is essential for improving load times for frequently accessed content.

- D. Duplicate Entries in Separate Buckets: Storing two copies of each entry in different S3 buckets with individual CloudFront distributions is inefficient and increases storage costs without providing a clear performance benefit.

Question 52

A financial startup, operating an online portal for short-term loans on AWS, uses S3 for storage, DynamoDB as their database, and EC2 instances for web hosting. The company is approaching a compliance audit and must furnish auditors with access to their AWS resource logs.

How should the auditor be given access to the AWS logs?

A.

1. Establish an SNS Topic.
2. Set up SNS to dispatch an email with CloudTrail log files attached to the auditor's email each time logs are delivered to S3.

B.

1. Activate CloudTrail logging for the necessary AWS resources.
2. Generate an IAM user with read-only access to the relevant AWS resources.
3. Share the login credentials with the auditor.

C.

1. Formulate an IAM role with appropriate permissions for the auditor.
2. Associate this role with the EC2, S3, and DynamoDB services.

D.

1. Notify AWS about the impending audit.
2. AWS provides the necessary access for the third-party auditor to review the logs.

Correct Answer: B

Explanation:

B is the correct answer because it ensures that the auditor has the necessary access to the logs while maintaining security and auditability within the AWS environment:

1. CloudTrail Logging: By enabling AWS CloudTrail, the company ensures that all actions across the AWS infrastructure are logged and auditable, which is a fundamental

requirement for compliance checks.

2. Read-Only IAM User: Creating an IAM user with read-only permissions restricts the auditor to only viewing the logs without making any changes to the AWS resources, adhering to the principle of least privilege.
3. Providing Credentials: Giving the auditor the access credentials for this IAM user is a controlled way to grant access. It allows the company to monitor the auditor’s activities, reinforcing security and compliance.

The other options are less suitable:

A exposes a risk by sending potentially sensitive log files over email, which is not a secure method of transferring such data.

C is incorrect because IAM roles are not meant to be directly attached to services like EC2, S3, and DynamoDB for the purpose of auditing access.

D is not a viable option as AWS does not provide direct access to third-party auditors to view logs; this responsibility lies with the AWS account holder to facilitate.

Question 53

A global enterprise web application utilizes a private S3 bucket named MANILATECH-CONFIG for storing its regional configuration files, secured with SSE-S3 encryption. Following a spate of database modifications and feature adjustments, versioning was enabled on the bucket to track changes and facilitate the restoration of previous settings. Subsequently, a new file for the Oceania region (MNL-O.config) was added, and updates were made to the files for North America (MNL-NA.config), Latin America (MNL-LA.config), and Oceania. The files for Europe (MNL-EUR.config) and Asia (MNL-ASIA.config) remained unchanged.

In light of the changes and the addition of versioning, what is accurate about the files in the MANILATECH-CONFIG S3 bucket? (Choose two correct statements.)

A. The files for Europe and Asia will retain a Version ID indicating the initial upload, traditionally denoted as null since they have not been modified since versioning was enabled.

B. Each of the files for North America, Latin America, and Oceania will have two versions post-versioning: the original and the updated one. The original versions of these files will have a Version ID of null, which is assigned to the first version when versioning is initially enabled on a bucket.

C. The latest versions of the files for North America and Latin America will have a Version ID assigned by S3 upon the subsequent updates post-versioning enablement.

D. The files for Europe and Asia will have a Version ID set to null because they have not been updated since versioning was turned on.

E. The initial versions of the files for North America and Latin America are tagged with a Version ID of 1, a common misconception since S3 assigns a unique ID that is not numerically incremental.

Correct Statements:

B. There will be two versions for each of the files MNL-NA.config, MNL-LA.config, and MNL-O.config. The original, or first version of these files, will have a Version ID of null.

D. The MNL-EUR.config and MNL-ASIA.config files will have a Version ID of null since they have not been edited or updated since versioning was activated on the bucket.

Explanation:

When versioning is enabled on an S3 bucket, AWS S3 assigns a unique version ID to each new version of the file. For files that existed before versioning was enabled, the first version (the version that existed before any updates after versioning was turned on) is assigned a version ID of null. Any subsequent updates to these files will result in new, unique version IDs being assigned by S3.

For files that have not been updated since versioning was enabled (MNL-EUR.config and MNL-ASIA.config), they will maintain the initial version ID of null, as no new versions have been created.

The other options are incorrect because AWS S3 does not assign a literal '1' as a version ID, and the latest versions of updated files do not retain a version ID of null; instead, they receive a new, system-generated unique version ID.

Question 54

A company adheres to a policy of using CloudFormation for all cloud deployment activities, treating CloudFormation templates as code and storing them in a private GIT repository. A junior solutions architect, taking over from a senior colleague, is tasked with understanding a CloudFormation template that describes a distributed system. The system is to be migrated to a different VPC. During the review, the architect encounters the following segment in the CloudFormation template:

```
"SNSTopic" : {
  "Type" : "AWS::SNS::Topic",
  "Properties" : {
    "Subscription" : [{
      "Protocol" : "sqs",
      "Endpoint" : { "Fn::GetAtt" : [ "TutorialsDojoQueue", "Arn" ] }
    }]
  }
}
```

What is the function of this snippet within CloudFormation?

A. It instantiates an SNS topic configured to permit subscriptions from SQS queue endpoints.

B. It establishes an SNS topic and subsequently triggers the creation of an SQS queue labeled 'TutorialsDojoQueue'.

C. It generates an SNS topic and appends a subscription by referencing the ARN of an SQS queue designated as 'TutorialsDojoQueue'.

D. It provisions an SNS topic that accepts SQS subscription endpoints to be specified as a parameter in the template.

Correct Answer: C

Explanation:

C is the correct answer because the code snippet outlines the creation of an SNS topic with an associated subscription. The subscription is configured to use an SQS queue as the endpoint. Specifically, the 'Fn::GetAtt' intrinsic function retrieves the ARN (Amazon Resource Name) of the SQS queue, which is presumed to exist in the same CloudFormation template under the logical name 'TutorialsDojoQueue'. This ARN is then used to establish the connection between the SNS topic and the SQS queue.

Why the Other Answers Are Incorrect:

A is not correct because, while the SNS topic is configured to allow subscriptions from SQS endpoints, the focus of this snippet is on the subscription itself, which utilizes the ARN of an existing SQS queue defined elsewhere in the template.

B is incorrect because the code does not initiate the creation of an SQS queue; it assumes that the queue already exists as defined by 'TutorialsDojoQueue' within the CloudFormation template.

D is incorrect as the snippet does not indicate that the SQS subscription endpoints are intended to be added as parameters. The ARN is directly retrieved within the template, not passed as a parameter.

Question 55

A BPO company operates a multi-tiered Java-based CMS on-premises with a JBoss Application server in the application layer and an Oracle database in the database tier. The Oracle database is periodically backed up to S3 via Oracle RMAN, and the application's static files reside on a 512 GB Storage Gateway volume connected through iSCSI. The company requires a disaster recovery strategy with an optimal Recovery Time Objective (RTO) utilizing AWS.

What AWS disaster recovery strategy would offer the most rapid RTO?

A. Set up EC2 instances to host both the JBoss application and the Oracle database. Recover the database from backups stored in S3. Integrate an AWS Storage Gateway on EC2, configured as an iSCSI volume, to the JBoss EC2 instance to serve the static content.

B. Migrate the Oracle database to Amazon RDS and deploy the JBoss application server on EC2. Retrieve Oracle RMAN backups from Amazon Glacier and establish an EBS volume with the static content from Storage Gateway, attaching it to the JBoss EC2 instance.

C. Configure EC2 instances for the JBoss application and Oracle database, and restore the database from S3 backups. Use an AWS Storage Gateway in Virtual Tape Library (VTL) mode on EC2 to recover static content.

D. Prepare EC2 instances for both the JBoss application and Oracle database. Restore the database from S3 backups and provision an EBS volume with static content from Storage Gateway, connecting it to the JBoss EC2 instance.

Correct Answer: D

Explanation:

D is correct because it provides a straightforward and efficient approach to disaster recovery. It involves:

- Provisioning EC2 Instances: Quickly provisioning EC2 instances for the application and database tiers is a standard recovery strategy that can be pre-configured and automated for rapid deployment.
- Database Restoration from S3: Restoring the database directly from S3 backups is faster than using Amazon Glacier due to the immediate availability of S3 objects.
- EBS Volume for Static Content: Using an EBS volume for static content, which can be quickly attached to an EC2 instance, allows for seamless and swift access to the necessary files without the complexities of configuring additional services.

Why Other Options are Less Suitable:

- A is not as optimal since using an AWS Storage Gateway on EC2 as an iSCSI volume could introduce unnecessary complexity and potential latency compared to using an EBS volume.
- B involves retrieving backups from Glacier, which has longer retrieval times compared to S3, potentially increasing the RTO. Additionally, migrating to RDS could be a more time-consuming process than directly provisioning an EC2 instance.
- C mentions using Storage Gateway-VTL, which is typically used for backup and archival purposes and is not as quick to restore from as an EBS volume would be.

Question 56

A photo-sharing website utilizes an Amazon CloudFront distribution with the default domain name (example.cloudfront.net) to serve static content. The site's infrastructure also includes an Elastic Load Balancer (ELB) set in front of a group of Spot EC2 instances spread across two Availability Zones. Currently, the site's Google search ranking is negatively impacted due to the lack of HTTPS/SSL usage.

What are the valid methods to enforce HTTPS when users are interacting with CloudFront? (Select two options.)

A. Implement a self-signed certificate on the ELB.

B. Adjust CloudFront's configuration to employ its own SSL/TLS certificate by modifying the Viewer Protocol Policy of one or more cache behaviors to mandate HTTPS for communication.

C. Set up the ELB with its own default SSL/TLS certificate.

D. Employ a self-signed SSL/TLS certificate on the ELB, storing it within a private S3 bucket.

E. Alter the Viewer Protocol Policy to either 'Redirect HTTP to HTTPS' or to 'HTTPS Only'.

Correct Answers: B and E

Explanation:

B is correct because CloudFront can use the default SSL/TLS certificate provided by AWS. By changing the Viewer Protocol Policy for the cache behaviors, you can enforce HTTPS, ensuring secure communication between viewers and the CloudFront distribution.

E is correct as it directly addresses the issue by redirecting all HTTP requests to HTTPS or by only allowing HTTPS requests, thus enforcing secure connections.

Why the Other Options Are Incorrect:

A and D are incorrect because self-signed certificates are generally not trusted by browsers and can lead to security warnings for users. While you could use a self-signed certificate on the ELB for backend encryption, this does not influence the CloudFront viewer protocol policy nor does it help with the site's search ranking on Google.

C is incorrect because ELBs do not come with a default SSL/TLS certificate; you must provide one. Even if you could use a default certificate with ELB, this would not enforce HTTPS for the CloudFront distribution which is what affects the viewer's connection and consequently the site's search ranking.

Question 57

A company hosts a three-tier web application on AWS's us-east-1 region, comprising stateless web and application tiers on separate EC2 instance fleets with Auto Scaling, and a database tier on a 40 TB Amazon Aurora database. The company requires a disaster recovery plan with an RTO of 30 minutes for the application and an RPO of 5 minutes for the data tier.

To fulfill these business continuity requirements cost-effectively, which two strategies should the Solutions Architect implement?

A. Implement a routine schedule for taking daily snapshots of the EC2 instances in the web and application tiers. Copy these snapshots to a secondary region and restore them in the event of a primary region failure.

B. Employ AWS Backup to create a backup job that replicates EC2 EBS volumes and RDS data to an Amazon S3 bucket in a different region, restoring these backups if a disaster occurs in the primary region.

C. Establish a cross-Region read replica for the Amazon Aurora database in an alternate region. In case of a disaster, promote this read replica to become the primary database.

D. Configure automated snapshots of the Amazon Aurora database every 5 minutes and expedite database restoration in the backup region if a disaster strikes the primary region.

E. Set up a hot-standby environment for the web and application tiers in a backup region, rerouting traffic there if a disaster impacts the primary region.

Correct Answers: A and C

Explanation:

A is correct because creating daily snapshots of the EC2 instances for the web and application tiers and copying them to a backup region is a cost-effective way to ensure quick recovery (meeting the 30-minute RTO). In a disaster scenario, these snapshots can be restored to bring the application back online.

C is correct as setting up a cross-Region read replica of the Amazon Aurora database in a secondary region aligns with the required 5-minute RPO for the data tier. This replica can be quickly promoted to a primary database in case of a regional failure, thus ensuring minimal data loss and meeting the RTO requirements.

Why the Other Options Are Incorrect:

B is less efficient than A and C because using AWS Backup for EBS volumes and RDS data involves more complex restoration processes, which might not meet the 30-minute RTO for the application and 5-minute RPO for the database.

D is not feasible because Aurora doesn't support creating snapshots every 5 minutes, and even if it did, the restoration process might not meet the 30-minute RTO due to the size of the database (40 TB).

E is not the most cost-effective approach. Maintaining a hot-standby environment in a backup region involves running and managing duplicate resources constantly, leading to higher costs compared to A and C.

Question 58

A media company is testing a new CMS on a Windows-based EC2 instance with a 1 TB EBS volume for static content storage. The future production environment will require high availability across multiple Availability Zones with at least three EC2 instances. These instances must share data consistently, support Windows ACLs, and integrate with the company’s Active Directory domain. The goal is to minimize management overhead.

What strategy should the Solutions Architect adopt to meet these requirements?

A. Implement a new Windows AMI for an Auto Scaling group spanning three Availability Zones. Utilize Amazon FSx for Windows File Server for shared storage. Incorporate a user data script to install the CMS, mount the FSx filesystem, and join the instances to the Active Directory domain.

B. Generate an AMI from the test EC2 instance. Apply this AMI to an Auto Scaling group across three AZs. Establish an Amazon FSx for Lustre filesystem for shared storage. Use a user data script to join the instances to the Active Directory domain and mount the FSx share on boot.

C. Set up a new Windows AMI for an Auto Scaling group across three AZs. Apply an EBS volume with Multi-Attach enabled for shared storage. Include a user data script for CMS installation and AD domain integration.

D. Create an AMI from the test EC2 instance. Use this AMI for an Auto Scaling group across three AZs. Implement an Amazon Elastic Filesystem (EFS) for shared storage. Integrate a user data script to join the instances to the AD domain and mount the EFS share at startup.

Correct Answer: A

Explanation:

A is the correct choice as it effectively addresses all the company’s requirements:

- Amazon FSx for Windows File Server: This service provides a fully managed native Microsoft Windows file system with built-in Windows ACLs support, meeting the need for shared storage with access control.
- Auto Scaling Group: Deploying an Auto Scaling group across multiple AZs with a minimum of three instances ensures high availability.
- User Data Script: Automating the CMS installation, mounting the FSx filesystem, and joining the instances to the AD domain simplifies the management overhead.

Why Other Options Are Incorrect:

B is incorrect because Amazon FSx for Lustre is optimized for high-performance computing workloads and does not support Windows ACLs, which is a requirement for the company’s CMS.

C is incorrect for several reasons:

- EBS Multi-Attach Limitation: Amazon EBS volumes with Multi-Attach capability are limited to usage within the same Availability Zone. This constraint conflicts with the requirement for the application to be hosted across multiple Availability Zones, which is crucial for achieving high availability.
- Incompatibility with Windows AMIs: EBS Multi-Attach is only supported by Linux-based AMIs. The company's CMS, however, is running on a Windows-based EC2 instance, making this option incompatible with their current setup.
- Lack of File Locking Mechanism: Even if the Windows compatibility issue were to be disregarded, EBS Multi-Attach does not provide a file locking mechanism needed for a shared file system, which is essential for the CMS's functionality and to prevent data corruption.

D is not suitable since Amazon EFS does not natively support Windows file system features like ACLs, which are needed for the CMS's functionality and integration with Active Directory.

Question 59

A company seeks to bolster the security of its cloud infrastructure by ensuring that all active EC2 instances are launched using only AMIs pre-approved by their Security team. Their Development team operates on a fast-paced CI/CD process, and any new security solution must be implemented without hindering this workflow.

Which two options best enforce these security controls with minimal impact on the development process?

A. Implement IAM policies that limit users' abilities to launch EC2 instances exclusively to a specified set of pre-approved AMIs, tagged by the Security team.

B. Configure AWS Config rules to detect launches of EC2 instances from non-approved AMIs, triggering an AWS Lambda function to automatically terminate such instances. Subsequently, send a notification to the Security team via an SNS topic.

C. Utilize Amazon Inspector to regularly conduct scans with a custom assessment template, identifying EC2 instances not based on pre-approved AMIs. Terminate non-compliant instances and email the Security team regarding the breach.

D. Schedule a Lambda function to review the list of running EC2 instances within your VPC, identifying those based on unauthorized AMIs. Notify the Security team through an SNS topic and terminate the identified EC2 instances.

E. Assign the responsibility of security approval processes to a centralized IT Operations team, who will manually ensure that EC2 instances are launched from pre-approved AMIs only.

Correct Answers: B and D

Explanation:

B is correct because it automates the process of identifying and terminating instances launched from non-approved AMIs. AWS Config rules can continuously monitor for such instances, and the integration with Lambda and SNS ensures immediate action and communication without delaying the Development team's CI/CD process.

D is also correct, offering an automated solution through a scheduled Lambda function to audit running EC2 instances against the approved AMIs list. This approach ensures compliance while maintaining the agility of the development process, with automated notifications and actions.

Why the Other Options Are Incorrect:

A is less suitable because IAM policy restrictions on launching instances might impede the Development team's agility and CI/CD process. It could lead to delays in deployment if the team needs to wait for specific AMIs to be tagged or approved.

C is not ideal because regular scans by Amazon Inspector may not provide real-time detection of non-compliant instances. Also, terminating instances and sending emails post-analysis could result in significant delays, affecting both security and development workflows.

E introduces a manual process, which could significantly slow down the Development team's CI/CD pipeline. Relying on a centralized team for approval also adds a bottleneck, contrasting with the company's need for minimal impact on the development process.

Question 60

A leading commercial bank utilizing a hybrid network architecture and Amazon S3 for storing sensitive records is looking to implement Server-Side Encryption with Customer-Provided Encryption Keys (SSE-C) on their S3 bucket. The objective is to ensure data security both at rest and in transit.

To achieve this, which two steps should the solutions architect take?

A. Restrict the upload and updating of objects to the S3 console with SSE-C encryption only.

B. When using presigned URLs, include the algorithm specification via the `x-amz-server-side-encryption-customer-key-MD5` request header.

C. Implement WSS (WebSocket Secure).

D. For presigned URLs, specify the encryption algorithm using the `x-amz-server-side-encryption-customer-algorithm` request header.

E. In Amazon S3 REST API calls, utilize the following HTTP request headers:

- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

Correct Answers: D and E

Explanation:

D is correct because when using presigned URLs with SSE-C, it's necessary to specify the encryption algorithm in the request header. This header tells S3 to use SSE-C for the object and indicates the algorithm to be used for encryption.

E is correct as these headers are required for using SSE-C with Amazon S3 REST API calls. The `x-amz-server-side-encryption-customer-algorithm` specifies the encryption algorithm, the `x-amz-server-side-encryption-customer-key` provides the encryption key, and the `x-amz-server-side-encryption-customer-key-MD5` is a message digest of the key. These ensure secure transmission and handling of the encryption key.

Why the Other Options Are Incorrect:

A is incorrect because using the S3 console alone for uploads and updates is overly restrictive and impractical for a commercial bank's operations. It doesn't facilitate automated or programmable interactions with the S3 bucket, which are often necessary in a banking environment.

B is incorrect as the `x-amz-server-side-encryption-customer-key-MD5` header is not for specifying the algorithm but for providing the MD5 digest of the encryption key, which is a validation mechanism.

C is irrelevant in this context as WSS (WebSocket Secure) is a protocol for secure communication over a computer network and is unrelated to server-side encryption for Amazon S3.

Question 61

A company developing an application for biologists to submit and share plant genomic data requires a data platform that can process and analyze large volumes of data in near real-time, store it durably, and deliver processed data to a data warehouse. The company is evaluating different AWS services to build this data platform.

Which AWS solution should the Solutions Architect implement to meet these requirements?

A. Utilize Amazon API Gateway for receiving genomic data, forwarding it to an Amazon SQS queue. Employ an AWS Lambda function to process the queue messages, and leverage Amazon EMR for saving the processed results into an Amazon Redshift cluster.

B. Directly store all inbound data files in an Amazon S3 bucket. Analyze the data using Amazon Kinesis and Amazon SQS, and subsequently transmit the processed results to an Amazon Redshift cluster.

C. Implement an Amazon Kinesis Data Streams stream for collecting the inbound data. Analyze the genomic data with a Kinesis client. Post-processing, save the results to an Amazon Redshift cluster using Amazon EMR.

D. Create an Amazon Kinesis Data Firehose delivery stream to route the inbound data to an Amazon S3 bucket. Analyze the data stored in S3 with a Kinesis client. Use AWS Lake

Formation to register the S3 bucket as a data lake and employ Amazon Quicksight for querying the data lake.

Correct Answer: C

Explanation:

C is correct because it effectively integrates various AWS services to fulfill all the company's requirements:

- Amazon Kinesis Data Streams: Ideal for collecting and processing large streams of data records in real-time, meeting the near-real-time processing requirement.
- Kinesis Client for Analysis: A Kinesis client can efficiently process and analyze the data stream, providing the needed analytics capability.
- Amazon EMR and Amazon Redshift: EMR can handle complex processing tasks and subsequently save the results to Redshift, a data warehousing service, fulfilling the requirement for durable storage and data warehousing.

Why the Other Options Are Incorrect:

A is not optimal because the use of Amazon SQS introduces unnecessary complexity for real-time data processing and might not meet the near-real-time requirement. Additionally, Lambda functions have execution time limits that could be restrictive for continuous data processing.

B is less efficient for real-time processing. While S3 is suitable for durable storage, using Kinesis and SQS for analyzing data already stored in S3 might not provide the real-time analytics capability required.

D is incorrect as it prioritizes storage over real-time processing. While Kinesis Data Firehose efficiently delivers data to S3, the subsequent use of Lake Formation and Quicksight for querying does not align with the need for real-time data processing and analytics.

Question 62

A company is preparing for the public beta release of its new video game, which is about 5GB in size. Anticipating millions of global downloads, the company seeks a cost-effective solution that ensures fast download performance worldwide, moving away from their current Linux-based FTP website hosted on-premises.

Which option best fulfills the company's requirements?

A. Deploy the FTP service on an Auto Scaling group of Amazon EC2 instances, storing game files on Amazon EBS volumes mounted on each instance. Use an Application Load Balancer, and link it with an Amazon Route 53 entry published as the FTP website URL for game downloads.

B. Set up the FTP service on an Auto Scaling group of Amazon EC2 instances, keeping game files on Amazon EFS volumes attached to each instance. Implement a Network Load Balancer, connecting it with an Amazon Route 53 entry published as the FTP website URL for game downloads.

C. Enable website hosting on an Amazon S3 bucket and upload the game package there. Establish an Amazon CloudFront distribution with the S3 bucket as its origin. Link this to an Amazon Route 53 entry and publish it as the FTP website URL to facilitate game downloads.

D. Activate website hosting on an Amazon S3 bucket and upload the game package, turning on the “Requestor Pays” option for cost-effectiveness. Direct an Amazon Route 53 entry to the S3 bucket and publish it as the FTP website URL for game downloads.

Correct Answer: C

Explanation:

C is the ideal solution because it leverages Amazon S3 for reliable and scalable storage, and Amazon CloudFront for content delivery. This setup ensures that the game is distributed efficiently to a global audience:

- Amazon S3 for Storage and Website Hosting: S3 is not only a highly durable and scalable storage service but also supports static website hosting. This means it can serve content directly over HTTP/HTTPS. For a large file like a 5GB game package, S3 provides reliable and resilient storage. The website hosting feature is particularly suitable in this scenario for its simplicity and efficiency in serving static content, like a downloadable game file, without the need for running a server.
- Amazon CloudFront: A content delivery network (CDN) that caches content at edge locations around the world, significantly improving download speeds for users regardless of their geographical location.
- Amazon Route 53: Integrates with CloudFront to route users to the nearest edge location for faster downloads.

Why the Other Options Are Incorrect:

A and B are not as optimal for global distribution. While Auto Scaling and load balancers provide scalability and high availability, they don't offer the same level of global content delivery performance as CloudFront. The latency for users far from the hosted region would be higher compared to using a CDN.

D is less desirable due to the “Requestor Pays” model, which shifts the cost of data transfer to downloaders. This could be a deterrent for potential users, as they would incur costs for downloading the game. Additionally, serving content directly from S3 without CloudFront does not provide the same level of performance enhancement for a global audience.

Question 63

A company operating an ERP application on AWS, involving Lambda functions, DynamoDB, and Amazon OpenSearch, seeks a deployment strategy that ensures no downtime and prevents failed deployments. The system must maintain full capacity during API deployments to avoid service degradation.

Which approach should the Architect adopt to meet these requirements most effectively?

A. Implement blue/green deployments for all changes using Amazon Lightsail, which manages database instances, EC2 instances, and load balancers for the application. Deploy AWS Lambda functions, DynamoDB tables, and Amazon OpenSearch domain using CloudFormation.

B. Conduct blue/green deployments for all upcoming changes with AWS CodeDeploy. Use AWS CloudFormation to establish Amazon DynamoDB tables, AWS Lambda functions, and Amazon OpenSearch domain in the AWS VPC. Host the web application in AWS Elastic Beanstalk, setting the deployment policy to Immutable.

C. Execute in-place deployments for all changes using AWS CodeDeploy. Utilize AWS SAM to set up Amazon DynamoDB tables, Lambda functions, and Amazon OpenSearch domain within the AWS VPC. Host the web application in AWS Elastic Beanstalk with a Rolling deployment policy.

D. Perform blue/green deployments for all changes using AWS CodeDeploy. Deploy DynamoDB tables, Lambda functions, and Amazon OpenSearch domain in the AWS VPC through AWS SAM. Host the web application in AWS Elastic Beanstalk with an All at Once deployment policy.

Correct Answer: B

Explanation:

B is the correct choice because:

- Blue/Green Deployment with AWS CodeDeploy: This approach ensures zero downtime by creating a parallel environment (green) for the new version. Traffic is switched only after the green environment is fully operational, allowing for easy rollback if needed.

- AWS CloudFormation: Efficiently manages and deploys AWS resources like DynamoDB, Lambda, and OpenSearch in a structured and repeatable manner.
- AWS Elastic Beanstalk with Immutable Deployment Policy: This policy ensures that any changes are deployed to fresh instances. It mitigates risks by preventing changes to the existing environment and only redirects traffic once the new environment passes health checks, ensuring full capacity is maintained.

Why the Other Options Are Incorrect:

A is incorrect because Amazon Lightsail, designed for simpler applications, lacks the advanced deployment and management capabilities required for an enterprise-level ERP application.

C is not suitable as in-place deployments with a Rolling policy in Elastic Beanstalk can lead to temporary reduced capacity, which contradicts the requirement of maintaining full capacity during deployments.

D is inappropriate because an All at Once deployment policy in Elastic Beanstalk can cause downtime during updates, as all instances are updated simultaneously. This method poses a risk if the new version fails, directly impacting the service's availability.

Question 64

A company is deploying a three-tier web application on AWS using a CloudFormation template, which includes a custom AMI for an Auto Scaling group of EC2 instances. With each new application version, a new AMI is introduced. The company aims for zero downtime during deployments and needs to streamline its AMI deployment process, which involves updating the CloudFormation template with the new AMI and replacing old EC2 instances with new ones using the `UpdateStack` API.

Which action should the Solutions Architect take to meet these requirements?

A. Implement a new CloudFormation change set to preview the changes in the updated template, ensuring the new AMI is correctly listed before executing the change set.

B. Modify the AWS::AutoScaling::LaunchConfiguration resource in the CloudFormation template, adding a `DeletionPolicy` attribute with `MinSuccessfulInstancesPercent` set to 50.

C. Revise the AWS::AutoScaling::AutoScalingGroup resource in the CloudFormation template to include an `UpdatePolicy` attribute with an `AutoScalingRollingUpdate` policy.

D. Duplicate the updated template and deploy it to a new CloudFormation stack. Post successful deployment, update the Amazon Route 53 records to direct traffic to the new stack and subsequently delete the old stack.

Correct Answer: C

Explanation:

C is correct because specifying an `UpdatePolicy` attribute with an `AutoScalingRollingUpdate` policy in the Auto Scaling group resource allows for a rolling update of EC2 instances. This policy ensures that the Auto Scaling group gradually replaces instances with the new AMI without downtime, as it maintains the desired capacity during the update process.

Why the Other Options Are Incorrect:

A is not sufficient as creating a change set allows for reviewing changes but does not address how the deployment of the new AMI is handled. A change set can confirm that the correct AMI is specified, but it doesn't ensure zero downtime during the update.

B is incorrect because the `DeletionPolicy` attribute with `MinSuccessfulInstancesPercent` is not applicable to the AWS::AutoScaling::LaunchConfiguration resource. This approach does not facilitate a rolling update of the instances with the new AMI.

D is not the most efficient method as deploying an entirely new stack and updating Route 53 records to switch traffic involves more complexity and potential risk of downtime. This approach is less streamlined compared to an in-place rolling update policy.

Question 65

A company operating an application on Amazon EC2 instances in the us-east-2 region is experiencing erratic behavior due to heavy write requests to its on-premises database, which follows the BASE model. The company seeks a cost-effective solution to improve application performance.

Which strategy should be adopted to address this issue effectively?

A. Establish a Hadoop cluster using Amazon Elastic Map Reduce (EMR) and synchronize data between the on-premises database and the Hadoop cluster using the S3DistCp tool.

B. Set up an Amazon RDS multi-AZ instance to synchronize with the on-premises database server using Amazon EventBridge. Redirect the application's write operations to the RDS endpoint through the Amazon Elastic Transcoder service.

C. Implement an Amazon SQS queue, coupled with a consumer process that flushes the queue to the on-premises database server. Modify the application to write to the SQS queue.

D. Revise the application to write to an Amazon DynamoDB table. Connect the table to an Amazon EMR cluster and create a map function that updates the on-premises database for every DynamoDB table update.

Correct Answer: C

Explanation:

C is the most suitable option because it effectively decouples the write operations from the immediate processing by the on-premises database. By using Amazon SQS, a managed message queuing service, the application can quickly enqueue write requests. The consumer process can then asynchronously flush these requests to the database, managing the load more efficiently. This approach aligns with the BASE model's eventual consistency principle and improves application stability by preventing it from being directly affected by database write load.

Why the Other Options Are Incorrect:

A is incorrect as it introduces unnecessary complexity. While EMR and Hadoop are powerful for big data processing, using them for simple database synchronization is overkill and may not effectively address the issue of erratic application behavior due to heavy write requests.

B is not optimal. Although Amazon RDS is a robust solution for database management, the scenario does not indicate a need for a full-fledged RDS instance. Moreover, using Amazon Elastic Transcoder in this context is irrelevant, as it is a media transcoding service and does not contribute to database synchronization or handling write operations.

D is also not ideal. While DynamoDB offers high scalability, introducing it and an EMR cluster adds significant complexity and might not efficiently solve the immediate problem of erratic application behavior due to heavy database write loads. This approach also involves more components than necessary, increasing maintenance overhead and costs.

Question 66

A company operating a suite of web applications in AWS needs to secure its system to allow multiple domains to serve SSL traffic, with the flexibility to add new domain names without re-authenticating or re-provisioning a new certificate. This shift from HTTP to HTTPS is aimed at enhancing SEO and Google search ranking.

Which two solutions best meet these requirements?

A. Replace the Application Load Balancer with a Gateway Load Balancer, and upload all SSL certificates of the domains, leveraging Server Name Indication (SNI).

B. Implement a wildcard certificate to manage multiple sub-domains and distinct domains.

C. Add a Subject Alternative Name (SAN) for each new domain to your existing certificate.

D. Upload all SSL certificates of the domains to the Application Load Balancer (ALB) and bind multiple certificates to the same secure listener. The ALB will automatically select the best TLS certificate for each client using Server Name Indication (SNI).

E. Set up a new CloudFront web distribution configured to handle HTTPS requests using dedicated IP addresses, associating alternate domain names with a dedicated IP address in each CloudFront edge location.

Correct Answers: D and E

Explanation:

D is a valid solution because it allows the ALB to handle SSL/TLS traffic for multiple domains without needing a new certificate for each domain addition. By uploading all SSL certificates to the ALB and using SNI, the ALB can intelligently choose the appropriate certificate for each client based on the domain they request. This approach is efficient, flexible, and minimizes the need for certificate management each time a new domain is added.

E is correct as it offers an alternative approach using Amazon CloudFront. By configuring a CloudFront distribution to serve HTTPS requests with dedicated IP addresses, the solution can associate alternate domain names with specific IP addresses in CloudFront edge locations. This setup ensures that each domain's SSL/TLS certificate is correctly used, enhancing security while supporting multiple domains.

Why the Other Options Are Incorrect:

A is not as suitable because a Gateway Load Balancer focuses on layer 4 (transport layer) traffic, typically used for network and security appliances. It's not designed for handling web traffic and SSL/TLS termination like an ALB, which operates at layer 7 (application layer).

B is incorrect in this context because a wildcard certificate covers multiple sub-domains of a single domain but does not extend to different domains. Therefore, it would not fulfill the requirement of managing SSL traffic for multiple distinct domains.

C is less practical for this scenario. While adding SANs to a certificate can cover multiple domains, it becomes cumbersome and less manageable as the number of domains grows, especially when frequent additions are expected. This method also requires re-issuing the certificate each time a new domain is added.

Question 67

A major telecommunications company needs a disaster recovery solution for its Amazon Redshift cluster, which is encrypted using AWS KMS and requires a recovery site at least 500 miles away from the primary location. The goal is to ensure high availability and data security.

Which strategy best meets these requirements?

A. Enable cross-region snapshot copy feature in the Redshift cluster to duplicate snapshots to another region.

B. Create a new AWS CloudFormation stack for deploying the cluster in another region and set up regular backups to an S3 bucket with cross-region replication. In an outage, use the snapshot from the S3 bucket to start the cluster.

C. Implement a snapshot copy grant for a master key in the destination region and activate cross-region snapshots in the Redshift cluster to copy snapshots to another region.

D. Develop an AWS Lambda scheduled job to routinely capture a snapshot of the Redshift cluster and transfer it to another region.

Correct Answer: C

Explanation:

C is the most appropriate solution because:

- Snapshot Copy Grant for KMS: When using KMS for encryption, a snapshot copy grant is essential to authorize Amazon Redshift to use the customer master key (CMK) in the destination region. This setup is crucial for encrypted clusters.
- Cross-Region Snapshots: Enabling this feature in the Redshift cluster allows for copying snapshots to a secondary region. This ensures data replication in a geographically distant location, fulfilling the requirement for a disaster recovery site at least 500 miles away.

Why the Other Options Are Incorrect:

A is insufficient as it doesn't address the KMS encryption aspect. Simply enabling cross-region snapshot copying without considering encryption key management in the destination region can lead to issues in restoring from these snapshots.

B involves unnecessary complexity. While CloudFormation is powerful for infrastructure deployment, this method doesn't directly leverage Redshift's native disaster recovery capabilities. Additionally, managing snapshots in S3 and ensuring proper encryption handling adds overhead and potential for error.

D is also less effective. Manually developing a Lambda function for snapshot management increases the maintenance burden and potential for errors. Redshift's built-in cross-region snapshot feature is a more integrated and reliable solution compared to a custom Lambda job.

Question 68

A financial company has developed an online document portal system where employees and developers can upload files to a private S3 bucket. The developers created IAM users with read and write access to the S3 bucket and used pre-signed URLs for file uploads. Initially, uploads were successful, but later, the development team encountered issues with uploading files using the online portal.

Which two reasons could be causing this issue?

A. The AWS credentials required in the `~/.aws/credentials` file on the EC2 instances hosting the online portal are missing, preventing proper generation of pre-signed URLs.

B. A recent change in the S3 bucket settings enabled object versioning, which invalidated all pre-signed URLs.

C. The application developers lack access to read or upload objects to the S3 bucket.

D. The expiration time set for the pre-signed URLs is too short, causing them to expire before they are used.

E. The S3 bucket's access control list (ACL) blocks the online portal, preventing developers from uploading files.

Correct Answers: A and D

Explanation:

A is correct because the presence of valid AWS credentials on the EC2 instances is crucial for generating functional pre-signed URLs. If these credentials are missing or incorrect in the `~/.aws/credentials` file, the application running on the EC2 instances cannot generate valid pre-signed URLs for S3 uploads. This scenario is plausible, especially if the initial testing by the developer was done in a different environment where the credentials were correctly set.

D is also correct as pre-signed URLs have an expiration time. If this time is set too short, the URLs may expire before they are used, leading to failed upload attempts. This can occur if the developer sets an inappropriate expiration time while integrating the pre-signed URL functionality into the online portal.

Why the Other Options Are Incorrect:

B is incorrect because enabling object versioning in an S3 bucket does not invalidate existing pre-signed URLs. Object versioning is a feature that preserves, retrieves, and restores every version of every object stored in the S3 bucket, but it doesn't impact the validity of pre-signed URLs.

C is unlikely because the developers initially had success in uploading files, indicating they had the necessary permissions. The issue arose later, suggesting the problem is not with IAM permissions but likely with the way the online portal interacts with S3.

E is incorrect because if the S3 bucket's ACL was the problem, it would have prevented file uploads from the beginning. Since the developers were initially able to upload files successfully, it indicates that the S3 bucket's ACL settings are likely not the cause of the recent upload issues.

Question 69

A global finance company is seeking a durable and cost-effective solution to archive sensitive data from its current on-premises tape-based backup infrastructure to AWS Cloud.

Which solution would be most appropriate to meet these requirements?

A. Implement a Tape Gateway to back up data in Amazon S3 with point-in-time backups acting as tapes stored in the Virtual Tape Shelf (VTS).

B. Deploy a Stored Volume Gateway to back up data in Amazon S3 with point-in-time backups as EBS snapshots.

C. Configure a File Gateway to back up data in Amazon S3 and archive it in Amazon Glacier, leveraging existing tape-based processes.

D. Establish a Tape Gateway to back up data in Amazon S3 and archive it in Amazon Glacier, utilizing existing tape-based processes.

Correct Answer: D

Explanation:

D is the most suitable solution because:

- Tape Gateway Integration: Tape Gateway on AWS Storage Gateway offers a seamless integration with existing tape-based backup infrastructure. It allows for the use of existing tape-based backup workflows, facilitating a smooth transition to cloud-based storage.
- Backup and Archive: By backing up data to Amazon S3 and archiving in Amazon Glacier, the solution leverages AWS's durable and cost-effective storage services. S3 offers

reliability for backup storage, while Glacier provides low-cost, long-term archiving, which is suitable for sensitive financial data.

- Utilizing Existing Processes: Leveraging existing tape-based processes reduces the need for major changes in backup workflows, thus simplifying the transition and reducing implementation complexity.

Why the Other Options Are Incorrect:

A is incorrect as the Virtual Tape Shelf (VTS) stores the backups but doesn't directly facilitate archiving to Glacier. The key requirement is not just backup but also archiving, which is explicitly addressed in option D.

B is not ideal because Stored Volume Gateways primarily deal with storing data on local storage devices and backing up point-in-time snapshots to S3, not archiving to Glacier. This approach doesn't align well with the company's need for a tape-based backup solution transitioning to the cloud.

C is not the best choice because File Gateways are more suited for file-based storage and don't align with the existing tape-based backup processes. While File Gateway can back up data to S3 and archive to Glacier, it does not mimic the tape-based workflow, which is a specific requirement.

Question 70

A leading insurance firm needs to provision access for new development team members to create and configure AWS resources, including deploying Windows EC2 servers, and to view information about the organization in AWS Organizations. The goal is to follow the principle of least privilege in granting access.

Which approach is most suitable for this requirement?

A. Attach the PowerUserAccess AWS managed policy to the IAM users.

B. Attach the AdministratorAccess AWS managed policy to the IAM users.

C. Create a new IAM role and attach the SystemAdministrator AWS managed policy to it. Assign the IAM Role to the IAM users.

D. Create a new IAM role and attach the AdministratorAccess AWS managed policy to it. Assign the IAM Role to the IAM users.

Correct Answer: A

Explanation:

A is the correct choice because:

- PowerUserAccess Policy: This policy provides full access to AWS services and resources, but it doesn't allow management of users and groups. It's designed for users who need a wide range of permissions to work with AWS resources without the ability to affect user accounts and permissions. This balance makes it ideal for development team members who require significant access to resources for development tasks without the risk of altering IAM configurations or other sensitive settings.
- Least Privilege Principle: This policy aligns with the principle of least privilege, which suggests providing only the necessary permissions to perform a job. It's a key practice in securing AWS environments and minimizes potential security risks.

Why the Other Options Are Incorrect:

B is overly permissive. The AdministratorAccess policy grants full control over all AWS services and resources, which goes beyond the principle of least privilege. It could potentially allow the development team to make critical changes to IAM and other sensitive configurations, increasing security risks.

C is not entirely suitable. The SystemAdministrator managed policy provides broad permissions for many AWS services but is more focused on administrative tasks rather than development tasks. While it might be suitable for system administration, it may not provide all the necessary permissions for application development.

D is also overly permissive, similar to option B. Creating a role with AdministratorAccess and assigning it to the development team gives extensive privileges that exceed the scope of their development tasks. This approach contradicts the principle of least privilege.

Question 71

An aerospace engineering company is rapidly growing and requires an expansion of its cloud services, hosted on AWS, to support a heavily utilized online flight-tracking service. This service is reliant on resources from multiple on-premises data centers and accesses static content stored in an S3 bucket. To accommodate this growth, the technical lead has proposed extending the on-premises data centers into the AWS cloud. A dual-tunnel VPN connection has been established between the company's Customer Gateway (CGW) and the AWS Virtual Private Gateway (VGW).

Given this scenario, which element in the cloud architecture could be a potential single point of failure, and should be addressed to enhance the solution's availability?

A. Set up a NAT Gateway in a different data center and configure another dual-tunnel VPN connection.

B. Create an additional Customer Gateway in a different data center and establish a new dual-tunnel VPN connection.

C. Implement an extra Virtual Gateway in a different Availability Zone and set up a new dual-tunnel VPN connection.

D. Install a second Virtual Gateway in a separate Availability Zone and a Customer Gateway in another data center, followed by the creation of an additional dual-tunnel connection for improved high-availability and fault tolerance.

Correct Answer:

B. Create another Customer Gateway in a different data center and establish another dual-tunnel VPN connection.

Explanation:

B is correct because it directly addresses the potential single point of failure in the VPN connection setup:

- Customer Gateway Redundancy: By having a Customer Gateway in another data center, the company ensures that if one data center goes down, the other can maintain the VPN connection. This setup is essential for a fault-tolerant system, particularly for a service as critical as an online flight-tracking system.
- Distributed Risk: Placing the Customer Gateways in different data centers distributes the risk. It ensures that local issues (like power outages or network disruptions) in one data center don't impact the overall connectivity to AWS.
- Dual-Tunnel VPN: This further enhances reliability. Each tunnel in a dual-tunnel VPN setup can operate independently, providing a backup in case one tunnel fails.

Why the Other Options Are Incorrect:

A is incorrect because adding a NAT Gateway addresses a different aspect of network infrastructure. A NAT Gateway is primarily used for controlling outbound Internet traffic from private subnets in a VPC and doesn't serve the same purpose as a Customer Gateway in terms of VPN connectivity and redundancy.

C is incorrect because the Virtual Gateway (VGW) in AWS is already highly available across all Availability Zones in the region. Adding another VGW doesn't add significant redundancy or high availability compared to adding another Customer Gateway.

D is overly complex and partly redundant. While adding a second Virtual Gateway provides an additional connection point, it's the on-premises end (the Customer Gateway) that represents the single point of failure in this scenario. The VGW in AWS is inherently designed for high availability across AZs, so the focus should be on the Customer Gateway redundancy.

Question 72

A prominent telecommunications company is transitioning its critical multi-tier applications from an on-premises setup to AWS. Their existing architecture consists of desktop client applications and several servers located within their on-premises data center. The application tier utilizes a MySQL database hosted on a single VM, while the presentation and business logic layers are distributed across various VMs. Users accessing these applications remotely are experiencing increased latency and slow loading times.

Given this situation, which solution would be the most cost-effective in enhancing application uptime, requiring minimal changes, and improving overall user experience?

A. Implement Amazon ElastiCache to boost desktop application performance. Migrate the MySQL database to DynamoDB. Deploy application and presentation layers on AWS Fargate containers, backed by an Application Load Balancer.

B. Establish a CloudFront web distribution to enhance desktop application performance. Transition the MySQL database to a Redshift cluster. Utilize ECS containers for the application and presentation layers, supported by a Network Load Balancer.

C. Utilize Amazon AppStream 2.0 for centralized management of desktop applications, enhancing user experience. Migrate the MySQL database to Amazon Aurora. Host application and presentation layers in an EC2 Auto Scaling group, fronted by an Application Load Balancer.

D. Deploy Amazon WorkSpaces, providing each user with a workspace for enhanced experience. Migrate the MySQL database to a self-hosted MySQL instance on a large EC2. Arrange application and presentation layers in Amazon ECS containers, backed by an Application Load Balancer.

Correct Answer: C

Explanation:

C is the correct answer because:

- Amazon AppStream 2.0: This service enables central management of desktop applications and delivers them to users anywhere, which is crucial for improving remote access and reducing latency issues experienced by users.
- Migration to Amazon Aurora: Moving from a MySQL database on a VM to Amazon Aurora, a MySQL-compatible database, involves minimal changes. Aurora offers better

performance, scalability, and reliability, which are key for mission-critical applications.

- Auto Scaling with EC2 and ALB: Hosting application and presentation layers on EC2 instances within an Auto Scaling group ensures scalability and high availability. The Application Load Balancer optimizes the distribution of user traffic to the EC2 instances, further enhancing performance.

Why the Other Options Are Incorrect:

A is not optimal because DynamoDB, a NoSQL database, might require significant changes to the application's database layer, which is currently MySQL-based. Also, Fargate is more suited for containerized applications, which may not align with the company’s current architecture.

B is less suitable as Redshift is a data warehousing solution, not a direct replacement for operational databases like MySQL. Additionally, CloudFront is typically used for caching static content, which may not address the latency issues related to the application's dynamic content.

D is incorrect because Amazon WorkSpaces is a desktop-as-a-service offering, more suited for providing individual virtual desktops rather than improving application performance. Self-hosting MySQL on EC2 could be complex and might not offer the same scalability and performance benefits as Aurora.

Question 73

A prominent financial company with multiple AWS accounts under a single AWS Organization requires a solution to ensure that tags are automatically added whenever resources are created across all accounts. The solutions architect is tasked with implementing a system to enforce this tagging policy.

The best approaches to meet this requirement are:

A. Implement AWS Systems Manager Automation for automatic tagging of provisioned resources.

B. Activate AWS-generated tags in the Billing and Cost Management console of each member account.

C. Utilize AWS Service Catalog to automatically tag provisioned resources with unique identifiers related to the portfolio, product, and users.

D. Configure AWS Config to add tags to resources immediately upon their creation.

E. Employ CloudFormation's Resource Tags property to apply tags to certain resource types at the time of their creation.

Correct Answer:

C. Set up AWS Service Catalog to tag the provisioned resources with corresponding unique identifiers for portfolio, product, and users.

E. Set up the CloudFormation Resource Tags property to apply tags to certain resource types upon creation.

Explanation:

C is correct because:

- AWS Service Catalog: It allows the creation of standardized products that include predefined tags. When users provision resources using these products, the tags are automatically applied. This ensures consistent tagging across resources created via the Service Catalog.
- Unique Identifiers: By tagging resources with unique identifiers for portfolio, product, and user, the company can efficiently manage and track resource usage and ownership.

E is correct because:

- CloudFormation Resource Tags: This feature enables automatic tagging of resources during their creation via CloudFormation templates. By defining tags in the templates, the architect ensures that all resources created using these templates are consistently tagged.
- Resource Type Specific: CloudFormation allows tagging of various resource types, providing flexibility and coverage across different AWS services.

Why the Other Options Are Incorrect:

A is incorrect because AWS Systems Manager Automation primarily focuses on operational tasks like patching and configuration management. While it can potentially be used for tagging, it's not a direct or efficient method compared to Service Catalog and CloudFormation.

B is incorrect as AWS-generated tags in the Billing and Cost Management console are used for cost allocation and reporting purposes. They don't automatically tag resources upon creation across different AWS services.

D is incorrect because AWS Config is a service used for monitoring and assessing resource configurations. While it can detect untagged resources, it doesn't inherently have the capability to add tags to resources as they are created.

Question 74

A business news portal, experiencing high traffic and needing to optimize content delivery speed, runs on Spot EC2 instances behind an ALB. The database is currently on-premises, and there's a need to enhance the portal’s page load time. The Solutions Architect is tasked with finding a quick, cost-effective way to reduce latency for customers.

Given these requirements, which solution would be most effective?

A. Migrate the on-premises database to Amazon Aurora using AWS DMS and SCT. Create Aurora Replicas across Availability Zones and reconfigure the web servers to query the Aurora database.

B. Implement a CloudFront web distribution to accelerate data delivery globally. Migrate the entire portal to an S3 bucket, enable static web hosting, and set the S3 bucket as the CloudFront origin.

C. Replace the on-premises database with Amazon Elasticsearch Service (Amazon ES) using an ELK stack (Elasticsearch, Logstash, Kibana) for a full-text search engine. Utilize a CloudFront web distribution to enhance global data delivery.

D. Integrate Amazon ElastiCache for Redis as an in-memory datastore to alleviate database load. Enable Redis replication for scalable database reads and high availability.

Correct Answer: D

Explanation:

D is correct because:

- Amazon ElastiCache for Redis: This is an in-memory caching solution that significantly reduces the load on the database by caching frequently accessed data. For a news portal, this can greatly improve page load times by caching content like articles and comments.
- Redis Replication: Enhances scalability by allowing read operations to be distributed across replicas. This is particularly effective for read-heavy applications like a news portal.
- Highly Available Clusters: Ensures that the cache is available and resilient, providing consistent performance even with high traffic.

Why the Other Options Are Incorrect:

A is less ideal because while migrating to Aurora might improve database performance, it's a more complex and time-consuming process compared to setting up a caching layer. Additionally, the major issue here seems to be related to content delivery rather than database performance alone.

B is not suitable as it assumes that the portal is entirely static, which is unlikely given that it allows reader comments. Migrating dynamic content to an S3 static website isn't practical or feasible without significant changes to the application architecture.

C is incorrect because replacing the database with Amazon ES for full-text search isn't aligned with the primary requirement of reducing latency. While ES might improve search functionality, it doesn't directly address the page load time issue. Furthermore, setting up an ELK stack could introduce additional complexity.

Question 75

A cryptocurrency trading platform has integrated a Lambda function with DynamoDB Streams. They require a phased traffic shift for new deployments and the ability to trace the event source and downstream calls of the Lambda function. The Solutions Architect needs to select the most suitable deployment strategy and tracing tool.

Here are the options:

A. Configure a Canary deployment configuration for your Lambda function. Enable active tracing to integrate AWS X-Ray to your Lambda function.

B. Configure an All-at-once deployment configuration for your Lambda function and use AWS Config to trace the event source and downstream calls.

C. Configure a Rolling with additional batch deployment configuration for your Lambda function and use X-Ray to trace the event source and downstream calls.

D. Configure a Linear deployment configuration for your Lambda function and use AWS Config to trace the event source and downstream calls.

Correct Answer: A

Explanation:

A is correct because:

- Canary Deployment Configuration: This allows for the incremental shift of traffic to a new version of the Lambda function, which aligns with the requirement to shift 10% of traffic initially, followed by the remaining 90%. It's a gradual and controlled way to introduce changes.

- AWS X-Ray for Tracing: X-Ray enables detailed tracing of both the event source and the downstream calls made by the Lambda function. It provides insights into the function's performance and is the suitable tool for tracing in AWS.

Why the Other Options Are Incorrect:

B is incorrect as the All-at-once deployment configuration doesn’t support incremental traffic shifting. It deploys the new version to all traffic at once, which doesn’t meet the requirement for phased deployment. Additionally, AWS Config isn’t designed for tracing Lambda invocations and downstream calls like AWS X-Ray.

C is incorrect because Rolling with additional batch deployment allows for incremental deployment but doesn’t provide the specific control over traffic percentages as required in the scenario. AWS X-Ray is suitable for tracing, but the deployment strategy doesn’t match the requirement.

D is incorrect as Linear deployment configuration involves a linear increase in traffic over a specified period, but it does not allow for the specific two-step traffic shift as required. Also, AWS Config is not the appropriate tool for tracing Lambda function invocations and downstream calls, whereas AWS X-Ray is.

Question 76

A company's multi-tier web application, hosted in AWS and using Amazon CloudFront, faces slow response times due to a decreasing cache hit ratio. The cause is identified as inconsistent query strings with varying case sensitivity. The task is to find an action that increases the cache hit ratio of the CloudFront distribution.

Here are the options:

A. Launch a reverse proxy inside the application VPC to intercept the requests going to the origin instances. Process the query parameters to sort them by name and convert them to lowercase letters before forwarding them to the instances.

B. Reconfigure the CloudFront distribution to remove the caching behavior based on query string parameters. This will cache the requests regardless of the order or case of the query parameters.

C. Reconfigure the CloudFront distribution to ensure that the “case insensitive” option is enabled for processing query string parameters.

D. Write a Lambda@Edge function that will normalize the query parameters by sorting them in alphabetical order and converting them into lower case. Deploy this function with the CloudFront distribution and set “viewer request” as the trigger to invoke the function.

Correct Answer: D

Explanation:

D is correct because Lambda@Edge functions are designed to modify and process requests at AWS edge locations, nearest to the user. This solution:

- Normalizes Query Parameters: By converting all query parameters to lowercase and sorting them, it ensures consistent cache behavior. It effectively handles the issue of varying cases and query string order.
- Efficiency and Scalability: Lambda@Edge operates at the edge locations, reducing latency and unnecessary load on the origin server by handling the requests before they reach the origin.
- Trigger: Setting the function to trigger on “viewer request” ensures it processes the request as it arrives at CloudFront, before checking the cache.

Why the Other Options Are Incorrect:

A is less efficient as it involves setting up and managing a reverse proxy, adding complexity and potential latency. While it can normalize the query parameters, doing so inside the VPC is not as efficient as processing at the edge location with Lambda@Edge.

B is incorrect as removing caching based on query string parameters can lead to inappropriate caching of dynamic content. This does not address the issue of inconsistent query strings and can result in caching incorrect or outdated content.

C is incorrect because CloudFront does not have a built-in "case insensitive" option for query string parameters. The solution does not exist in CloudFront’s current feature set.

Question 77

A small telecommunications company, using a hybrid cloud architecture with AWS, needs a disaster recovery plan for their on-premises web application. They are using a 5 TB gateway-stored volume in AWS Storage Gateway for storing static files. The goal is to run the web application on AWS if there are issues with the on-premises network.

Here are the options:

A. Generate an EBS snapshot of the static content from the AWS Storage Gateway service. Afterward, restore it to an EBS volume that you can then attach to the EC2 instance where the application server is hosted.

B. For the static content, create an EFS file system from the AWS Storage Gateway service and mount it to the EC2 instance where the application server is hosted.

C. Restore the static content by attaching the AWS Storage Gateway to the EC2 instance that hosts the application server.

D. Restore the static content from an AWS Storage Gateway to an S3 bucket and link it to the EC2 instance where the app server is running.

Correct Answer: A

Explanation:

A is the most suitable solution for this scenario because:

- Disaster Recovery: EBS snapshots created from the Storage Gateway's stored volumes allow for the rapid restoration of data in AWS. In a disaster recovery scenario, these snapshots can be converted into EBS volumes and attached to an EC2 instance, effectively mirroring the on-premises environment.
- Compatibility: EBS volumes are compatible with EC2 instances and can be used to store static content for the web application, ensuring a smooth transition in case of a disaster.
- Flexibility and Speed: Using EBS snapshots for disaster recovery provides flexibility and speed in restoring the necessary data, critical for maintaining business continuity.

Why the Other Options Are Incorrect:

B is incorrect because AWS Storage Gateway does not directly create an EFS file system. While EFS could be used for shared file storage, the process of creating an EFS file system from Storage Gateway stored volumes is not straightforward or native to AWS services.

C is incorrect as AWS Storage Gateway cannot be directly attached to an EC2 instance. Storage Gateway is typically used to connect on-premises environments to AWS storage services, not directly to EC2 instances.

D is incorrect because while AWS Storage Gateway can integrate with S3, the process described is not a standard or simple method for disaster recovery. Restoring static content to an S3 bucket and then linking it to an EC2 instance is not as direct or efficient as creating and using EBS snapshots.

Question 78

The company's requirement is to refactor their web service portal to use AWS-managed services for scalability, high availability, and fault tolerance, with optimal user experience during system load spikes. The service should also be resilient to regional AWS failures.

The options are:

A. Create an Amazon Aurora global database and Auto Scaling replicas. Run the web service on Amazon EC2 instances in Auto Scaling groups behind ALBs in two regions. Use Route 53 Alias record with multi-value answer routing policy and health checks.

B. Use DocumentDB and an edge-optimized Amazon API Gateway and AWS Lambda-based web service. Set it as the origin of a global Amazon CloudFront distribution. Create a Route 53 Alias record pointed to CloudFront.

C. Store data in a primary Amazon S3 bucket with Cross-Region Replication. Create an API Gateway and AWS Lambda-based web service in each region, set as origins for two CloudFront distributions. Use Route 53 Alias records with a failover routing policy.

D. Create an Amazon DynamoDB global table for data storage in two regions. Use on-demand capacity mode. Run the web service on Auto Scaling Amazon ECS Fargate clusters in each region, behind their own ALBs. Use Route 53 Alias records with a latency routing policy and health checks.

Correct Answer: D

Explanation:

D is the most suitable solution for the following reasons:

- DynamoDB Global Tables: Provides a fully-managed, multi-region, and multi-master database that automatically replicates data across chosen AWS regions. This meets the need for high availability and fault tolerance across regions.
- On-demand Capacity Mode: Enables DynamoDB to handle sudden spikes in traffic without manual intervention, providing scalability and maintaining optimal user experience.
- ECS Fargate: Offers serverless compute for containers, allowing the company to run their web service without managing servers or clusters. Fargate's Auto Scaling ensures scalability.
- ALB with Route 53 Latency Routing: ALB efficiently distributes incoming traffic across multiple targets in AWS regions. Route 53 with latency routing ensures users are routed to the region providing the best possible latency.

Why Other Options Are Incorrect:

A is less suitable because Aurora, while highly available, is not as scalable for semi-structured data and load spikes as DynamoDB. Multi-value answer routing in Route 53 does not provide the same latency optimization as latency routing policy.

B is not ideal because DocumentDB, though suitable for semi-structured data, lacks the global, multi-region distribution of DynamoDB Global Tables. CloudFront is unnecessary for this scenario as it's more suited for content delivery rather than operational database queries.

C is incorrect because using S3 for semi-structured data storage in a web service context is not as efficient or scalable as DynamoDB. Also, S3 replication and the proposed CloudFront setup don't support the required database operations and real-time data consistency.

Question 79

The website www.example.com, running on the WordPress platform and hosted on a group of Amazon EC2 instances behind an Application Load Balancer (ALB), is experiencing customer complaints about slow loading times. To address this, a solutions architect has set up a CloudFront distribution with the ALB as its origin to boost read performance. However, a few days later, the IT Security team pointed out security concerns with this setup, emphasizing the need for enabling end-to-end HTTPS connections from the user’s browser to the origin through CloudFront.

Which of the following options should be implemented to meet these requirements?

A. Configure CloudFront with its default certificate and set the distribution to redirect HTTP to HTTPS. For the origin, generate a new SSL certificate using AWS Certificate Manager.

B. Set CloudFront to redirect HTTP to HTTPS. Generate a new SSL certificate with AWS Certificate Manager and apply it to both CloudFront and the ALB.

C. Implement a self-signed certificate for both CloudFront and the ALB.

D. Use a third-party Certificate Authority (CA) certificate for both CloudFront and the ALB.

Correct Answer: B

Explanation:

B is the correct solution because:

- HTTPS Redirect: Configuring CloudFront to redirect HTTP to HTTPS ensures that all user connections are secure, fulfilling the security requirement.
- SSL Certificate from AWS Certificate Manager: Generating a new SSL certificate in AWS Certificate Manager and using it for both CloudFront and the origin (ALB) ensures a consistent and trusted certificate authority across the entire path from user to origin. AWS Certificate Manager seamlessly integrates with CloudFront and ALB, simplifying certificate management and deployment.

- End-to-End HTTPS: This setup ensures that the connection is encrypted from the user's browser all the way to the origin, providing end-to-end security as required.

Why Other Options Are Incorrect:

A is partially correct but incomplete. While it secures the CloudFront distribution with its default SSL certificate and ensures HTTP to HTTPS redirection, it does not address the requirement for the origin's SSL certificate. It's crucial to have a valid SSL certificate at the origin to establish a secure connection from CloudFront to the origin.

C is incorrect because self-signed certificates are generally not trusted by browsers and can lead to security warnings. This could undermine user trust and does not meet typical security best practices for a public-facing website.

D is technically feasible but not as seamless or cost-effective as using AWS Certificate Manager. Managing third-party CA certificates involves additional steps for procurement, renewal, and deployment, which can be more complex compared to using AWS Certificate Manager.

Question 80

A company operates a legacy web application within its on-premises data center. A solutions architect is tasked with migrating this web application, which currently runs on a virtual machine in the data center, to an Amazon Virtual Private Cloud (VPC). However, the application needs a private and dedicated connection to various servers in the on-premises network to function properly.

Which combination of options provides the most suitable configuration for the web application inside the VPC to access its internal dependencies on the company's on-premises network? (Select TWO.)

A. An Internet Gateway to allow a VPN connection.

B. An Elastic IP address on the VPC instance.

C. An AWS Direct Connect link between the VPC and the network housing the internal services.

D. Set up a Transit VPC between your on-premises data center and your VPC.

E. A network device in your data center that supports Border Gateway Protocol (BGP) and BGP MD5 authentication.

Correct Answer: C & E

Explanation:

C. An AWS Direct Connect link between the VPC and the network housing the internal services and E. A network device in your data center that supports Border Gateway Protocol (BGP) and BGP MD5 authentication are the correct choices because:

- Dedicated Connection: AWS Direct Connect provides a dedicated network connection between the on-premises data center and the Amazon VPC. This satisfies the requirement for a private and dedicated connection.
- BGP Support: The use of a network device that supports BGP and BGP MD5 authentication is essential for establishing a stable and secure connection via AWS Direct Connect. BGP is used for routing between the on-premises network and AWS, ensuring optimal path selection and network resilience.
- Compatibility and Performance: Direct Connect offers consistent network performance, which is crucial for legacy applications that may have specific networking requirements. Also, BGP support ensures compatibility with standard network protocols used in enterprise environments.

Why Other Options Are Incorrect:

A. An Internet Gateway to allow a VPN connection is incorrect because an Internet Gateway is used for connecting a VPC to the internet, not for establishing a private, dedicated connection to an on-premises network.

B. An Elastic IP address on the VPC instance is incorrect as it is primarily used for providing a static, public IP address to an instance in a VPC for internet-facing access, not for internal connectivity to on-premises servers.

D. Set up a Transit VPC between your on-premises data center and your VPC is also incorrect for this scenario. A Transit VPC is typically used to connect multiple VPCs and on-premises networks via a central hub. This adds complexity and may not be necessary for the described requirement of a direct, dedicated connection.

Question 81

A financial services firm relies on hardware security modules (HSMs) for generating master encryption keys. The firm's application logs contain sensitive personal data, necessitating encryption for regulatory compliance. The logs are to be stored in a central Amazon S3 bucket, with a requirement for encryption at rest. The security team seeks to utilize the firm's HSMs for creating the Customer Master Key (CMK) material for S3 bucket encryption.

Which of the following solutions should the solutions architect implement to align with the company's requirements?

A. Request an AWS Direct Connect setup from the on-premises data center to AWS VPC. Avoid overlapping network addresses. Implement an S3 bucket policy for the central log bucket to enforce encrypted object uploads only. Configure applications to create a unique CMK for each log entry by accessing the on-premises HSMs via Direct Connect.

B. Use AWS CLI to create a new CMK with AWS-provided key material and set AWS_KMS as the key origin. Replace this CMK with a key from the on-premises HSMs using AWS's public key and import token. Set a one-year automatic key rotation for the CMK. Apply an S3 bucket policy to mandate AWS KMS for encryption and prohibit unencrypted uploads.

C. Establish a new AWS CloudHSM cluster and select it as the key material source in AWS KMS when generating a new CMK. Set a one-year auto-rotation for the CMK. Apply an S3 bucket policy to require AWS KMS for encryption and block unencrypted uploads.

D. Use AWS CLI to create a new CMK without key material, choosing EXTERNAL as the key origin. Generate a key from the on-premises HSMs and import it as CMK using AWS's public key and import token. Implement an S3 bucket policy to necessitate AWS KMS as the encryption source and disallow unencrypted uploads.

Correct Answer: D

Explanation:

D is the correct solution because:

- EXTERNAL Key Origin: By creating a CMK with no key material and specifying EXTERNAL as the origin, the solution aligns with the requirement to use the company's HSMs for generating the key material.
- Importing Key Material: Importing a key from the on-premises HSMs into AWS KMS is a direct way to leverage the existing HSM infrastructure for S3 encryption.
- Bucket Policy for Encryption Enforcement: Applying an S3 bucket policy to require AWS KMS as the encryption source and deny unencrypted uploads ensures that all data stored in the bucket complies with the company's encryption standards.

Why Other Options Are Incorrect:

A is incorrect because it involves a complex setup with AWS Direct Connect and does not directly leverage the on-premises HSMs for CMK creation in AWS. Generating a new CMK for each log event is also inefficient and could lead to management challenges.

B is incorrect as it starts with an AWS-generated CMK, which does not meet the requirement of using the company's HSMs for key generation. Overwriting the AWS-generated key with an imported key is unnecessary when you can directly create a CMK with external key material.

C is incorrect because it suggests using AWS CloudHSM, which, while providing HSM capabilities, does not utilize the company's existing HSM infrastructure. The solution should integrate with the company's current HSMs rather than replace them.

Question 82

A gaming store platform, hosted in an on-premises data center and offering a wide range of digital games, recently faced downtime due to a surge in web traffic from a year-end sale. With a similar promotion anticipated soon, the solutions architects are tasked with enhancing the infrastructure's capability to handle sudden traffic spikes. The current web application architecture includes a 2-tier web tier, comprising a load balancer and multiple web app servers, and a database tier with an Oracle database.

Which infrastructure modifications should be implemented to prevent future downtime, given the imminent promotion?

A. Utilize AWS VM Import to migrate the environment to AWS, converting the web server into an AMI. Establish an Auto Scaling group with the imported AMI and migrate the Oracle database to an RDS instance via replication, including RDS read replicas.

B. Generate an AMI to launch new EC2 web servers. Set up an Auto Scaling group with this AMI for web tier scalability. Deploy an Application Load Balancer to distribute traffic between on-premises and AWS servers.

C. Implement a CloudFront distribution to cache content from a custom origin, thus alleviating traffic load from the on-premises setup. Adjust object cache behavior and set an appropriate time-to-live for cached objects.

D. Configure an Amazon S3 bucket for website hosting. Transition DNS to Route 53 using zone import, and apply DNS failover to switch to the S3-hosted site as needed.

Correct Answer: C

Explanation:

C is the appropriate solution because:

- CloudFront for Traffic Offload: Using Amazon CloudFront to cache content from the platform's custom origin effectively reduces direct traffic to the on-premises servers. This is crucial for handling traffic bursts without impacting server performance.
- Customizable Cache Behavior: By customizing cache behavior and setting a suitable time-to-live for cached objects, CloudFront can efficiently serve repeated requests, reducing the load on the origin servers. This is particularly effective for a gaming platform where certain static assets are frequently accessed.

- Rapid Implementation: Given the short timeframe before the next promotion, setting up a CloudFront distribution is a quick and efficient solution that doesn't require extensive infrastructure changes or migrations.

Why Other Options Are Incorrect:

A is overly complex for the given timeframe. Migrating to AWS using VM Import and setting up an Auto Scaling group and RDS involves significant changes and testing, which might not be feasible before the upcoming promotion.

B proposes a hybrid solution involving AWS, but it requires substantial changes to the existing infrastructure. Additionally, managing traffic distribution between on-premises and AWS can be challenging and may not address the immediate need to handle traffic spikes.

D suggests a major migration to S3 for website hosting, which is a significant shift from the current architecture. This approach requires substantial time and resources for migration and testing, making it less suitable for the immediate requirement.

Question 83

A finance-focused application operated by a company is hosted on a group of Amazon EC2 instances within a private subnet of an AWS VPC. These instances are accessible via an internet-facing Application Load Balancer (ALB). As part of their security compliance, the company must implement a solution to inspect the network payloads directed towards the application, aiding in the analysis and reverse-engineering of complex network attacks.

Which solution should the solutions architect implement to meet these requirements?

A. Enable “Access logs” for the ALB in the Amazon EC2 console, direct these logs to Amazon AppFlow for payload inspection, and to an Amazon S3 bucket for extended storage.

B. Implement Traffic Mirroring on the EC2 instances' elastic network interfaces, channeling mirrored traffic to a monitoring appliance for storage and analysis.

C. Create a VPC flow log in the Amazon VPC console and configure its data to be sent to an Amazon S3 bucket for review.

D. Establish a new AWS web ACL with empty rules and a default “Allow” action, associating it with the ALB. Activate logging on the web ACL and forward the logs to Amazon CloudWatch Logs for assessment.

Correct Answer: B

Explanation:

B is the most suitable choice as it allows:

- Direct Traffic Inspection: Traffic Mirroring captures and duplicates the inbound and outbound traffic of the network interfaces of EC2 instances, providing a thorough inspection of the actual network payloads.
- Advanced Analysis: The mirrored traffic can be forwarded to a specialized monitoring appliance, enabling detailed analysis, which is crucial for understanding sophisticated network attacks.

Why Other Options Are Incorrect:

A is inappropriate as ALB Access logs only provide information about requests made to the load balancer, like request paths, client IP addresses, and latencies. They do not include detailed payload data necessary for the depth of analysis required for reverse-engineering network attacks.

C is not a viable option because VPC Flow Logs capture information about the IP traffic going to and from network interfaces in the VPC. While useful for monitoring network traffic, they do not provide payload data, which is essential for detailed security analysis.

D involves using AWS WAF (Web ACL) for logging, which is more focused on web request and response details. While this can be useful for some forms of analysis, it does not capture the detailed network payloads as required for comprehensive security analysis in this scenario. Traffic Mirroring is more suited for this purpose.

Question 84

A prominent software company operates an on-premises LDAP server and a web application hosted in an AWS VPC. Having established an IPSec VPN connection between the AWS VPC and the company's on-premises network, the company now aims to enable its employees to access the web application and other AWS resources using their existing corporate accounts.

Which steps should the solutions architect take to fulfill these requirements? (SELECT TWO.)

A. Set up an identity broker that utilizes STS for IAM role assumption to generate temporary AWS security credentials. Modify the web application to authenticate via the identity broker for AWS temporary security credentials.

B. Modify the web application to authenticate against the on-premises LDAP server, retrieving the name of a user-associated IAM role. Subsequently, the application should invoke STS to assume this IAM role, allowing access to AWS resources using temporary credentials.

C. Establish an identity broker that authenticates against the LDAP server, followed by an STS call for IAM federated user credentials. Alter the web application to interact with this broker for IAM federated user credentials, facilitating access to designated AWS services.

D. Integrate the LDAP server directly with IAM, enabling users to log into IAM using their corporate LDAP credentials. Post-authentication, they can use the generated temporary credentials to access AWS resources.

Correct Answer: B and C

Explanation:

B and C are correct because:

- LDAP Authentication: Both options utilize the on-premises LDAP server for initial user authentication, maintaining the existing corporate authentication mechanism.
- Identity Broker Role: In both scenarios, an identity broker plays a critical role. It bridges the gap between the on-premises LDAP authentication and AWS resource access, either by generating temporary AWS credentials (B) or by obtaining IAM federated user credentials (C).
- Temporary AWS Credentials: Both solutions leverage AWS STS (Security Token Service) to provide temporary credentials that are securely used to access AWS resources. This approach aligns with AWS best practices for secure access management.

Why Other Options Are Incorrect:

A is incorrect because it suggests creating an identity broker that authenticates against STS directly. In reality, the broker should authenticate against the LDAP server first, then use STS to assume an IAM role based on LDAP authentication.

D is not feasible as there is no direct integration mechanism between on-premises LDAP servers and AWS IAM for user authentication. IAM does not support direct LDAP integrations for login purposes; instead, identity brokers are used as intermediaries in such scenarios.

Question 85

A business operates a sizeable Microsoft Windows Server in a public subnet, with associated EC2 instances in a private subnet enabling Remote Desktop Protocol (RDP) connections through port 3389 for administrative access. The server requires continuous OS upgrades for enhanced security and must remain accessible at all times. The company seeks a solution to efficiently manage server patching, even beyond standard maintenance windows, with minimal administrative burden.

Which approach ensures the lowest administrative overhead for server management?

A. Deploy a secured machine image from the AWS Marketplace on AWS Cloud9, and manage patches using AWS Systems Manager Patch Manager. Utilize Amazon AppStream 2.0 as a bastion host.

B. Set up the Windows Server on Amazon WorkSpaces, using Amazon WorkSpaces Application Manager (WAM) for server hardening. Configure daily automatic Windows updates.

C. Implement an AWS AppSync environment with a single Windows Server EC2 instance, using a hardened custom AMI from the AWS Marketplace. Arrange for AWS Systems Manager Patch Manager to automatically apply OS updates.

D. Host the server on Amazon Lightsail using the recommended Amazon AMI. Employ a combination of Amazon EventBridge and AWS Lambda scheduled events to trigger the Upgrade Operating System API in Amazon Lightsail for system updates.

Correct Answer: B

Explanation:

B is the best solution because:

- WorkSpaces Flexibility: Amazon WorkSpaces, a managed Desktop-as-a-Service (DaaS), offers the flexibility and security to run Windows Server environments. It simplifies patch management and reduces administrative overhead.
- WAM for Hardening and Updates: Amazon WorkSpaces Application Manager provides a streamlined approach for server hardening and application management. Its capability to configure daily automatic updates ensures the server is always up-to-date, addressing the need for continuous security enhancements.
- Reduced Administrative Tasks: This approach significantly reduces the administrative tasks associated with server maintenance and patch management, as WorkSpaces handles these aspects efficiently.

Why Other Options Are Incorrect:

A is not ideal as it introduces complexity by combining multiple services (Cloud9, Systems Manager Patch Manager, and AppStream 2.0). This setup increases administrative overhead rather than minimizing it.

C is less optimal because it involves setting up an environment in AWS AppSync with a single EC2 instance, which might not be as straightforward or as managed as using Amazon WorkSpaces. The use of a custom AMI also adds to the administrative tasks.

D is incorrect as Amazon Lightsail is generally used for simpler applications and does not offer the same level of management and automation for Windows Server patching compared to Amazon WorkSpaces. The combination of EventBridge and Lambda for triggering system updates in Lightsail adds unnecessary complexity.

Question 86

A retail conglomerate with multiple subsidiaries across Southeast Asia seeks to enhance oversight and cost management for its various AWS accounts, each hosting a region-specific retail website. The parent company aims to achieve comprehensive cost reports, consolidated invoicing, unhindered administrative access across subsidiary accounts, and the ability to enforce policy-driven service restrictions.

Which steps should be taken to meet these objectives? (Select TWO.)

A. Establish an AWS account for the parent company, and create individual AWS organizations for each subsidiary. Invite every subsidiary's AWS account to join their respective organization under the parent company.

B. Formulate a single AWS Organization with Consolidated Billing from the parent company's AWS account. Invite each subsidiary's AWS account to join this AWS Organization.

C. Implement service quotas to limit services and features based on the parent company's policy guidelines. Apply these quotas to every subsidiary's AWS account.

D. Initiate an AWS Organization from the parent company's AWS account and incorporate all subsidiary AWS accounts. Ensure the activation of consolidated billing in the AWS Billing and Cost Management console of the parent account.

E. Develop Service Control Policy (SCP) documents to permit only the services and features specified by the parent company's policy. Apply appropriate SCPs to each subsidiary's AWS account.

Correct Answer: D & E

Explanation:

D is correct because:

- AWS Organization for Centralized Management: Establishing an AWS Organization under the parent company's account offers centralized governance over all subsidiary AWS accounts.
- Consolidated Billing: Enabling consolidated billing within the AWS Organization facilitates a single invoice for all accounts, meeting the cost management requirement.

E is correct because:

- **Policy Enforcement with SCPs**: Service Control Policies allow the parent company to define and enforce policy restrictions on services and features at the organizational level, aligning with the objective of restricting subsidiary accounts according to the parent company's policy.
- **Granular Control**: SCPs provide the granularity needed to restrict specific AWS services and features across subsidiary accounts without impeding their full administrative privileges.

Why Other Options Are Incorrect:

A is incorrect because creating separate AWS organizations for each subsidiary complicates management and does not support the goal of consolidated billing or centralized control under a single parent account.

B is partially correct regarding the establishment of a single AWS Organization and consolidated billing. However, it lacks the necessary component of enforcing service restrictions through SCPs.

C is incorrect because service quotas primarily manage resource consumption limits, not the type of services and features used. While quotas can limit resource usage, they don't directly address the requirement to control service access based on the parent company's policy.

Question 87

An AWS Partner company, with all its infrastructure in the AWS cloud in the us-east-1 region, plans to expand its business to Europe and Asia. The company is looking to provision resources across multiple regions and AWS accounts within its AWS Organization. The solutions architect needs to find the best way to achieve this.

What is the most effective solution to fulfill these requirements?

A. Utilize infrastructure-as-code for consistency. Develop AWS CloudFormation templates and create IAM policies for multi-account control. Deploy these templates in different regions using regional parameters.

B. Implement infrastructure-as-code for uniformity. Create nested stacks using AWS CloudFormation templates with global parameters to designate target regions and accounts for resource provisioning.

C. Employ AWS Organizations to centrally manage the deployment of AWS CloudFormation templates from a central account. Use AWS Control Tower for orchestrating resource deployment across various accounts and regions.

D. Apply infrastructure-as-code to ensure uniformity. Utilize AWS Organizations for centralized orchestration of AWS CloudFormation template deployment from a main account. Employ CloudFormation StackSets for simplified permissions and automated resource provisioning across multiple regions and accounts.

Correct Answer: D

Explanation:

D is the correct solution because:

- Infrastructure-as-Code Consistency: Using CloudFormation ensures consistency in infrastructure deployment. It allows defining and provisioning AWS infrastructure through code, ensuring that all environments are configured identically.
- Centralized Orchestration with AWS Organizations: This approach allows for centralized management and governance over multiple AWS accounts, streamlining the deployment process.
- Efficient Multi-region and Account Deployment with StackSets: CloudFormation StackSets extend the functionality of CloudFormation by enabling you to deploy stacks into AWS accounts across different regions with a single operation. This is ideal for scenarios where resources need to be deployed uniformly across various geographical locations and accounts.

Why Other Options Are Incorrect:

A is incorrect because, while it utilizes infrastructure-as-code and CloudFormation, it does not leverage the full capabilities of CloudFormation StackSets for simplified multi-region and account deployments. Manually specifying regional parameters for each deployment is less efficient compared to the automated approach offered by StackSets.

B is incorrect as it suggests using global parameters in nested stacks, which is not a standard feature of CloudFormation. CloudFormation templates are region-specific and do not inherently support global parameters for multi-region deployments.

C is incorrect because AWS Control Tower is primarily used for setting up and governing a secure, multi-account AWS environment based on best practices. While it provides some orchestration capabilities, it is not specifically designed for deploying resources across multiple regions and accounts like CloudFormation StackSets. Control Tower is more about environment setup and governance, rather than detailed resource deployment.

Question 88

A tech company employs AWS CloudFormation to set up a three-tier web application encompassing a web tier, application tier, and database tier. This application relies on an Amazon DynamoDB table for its database storage, and all components are to be created using a CloudFormation template.

How should the application instances be configured to access the DynamoDB tables securely without revealing API credentials?

A. In the CloudFormation template, instantiate an IAM user with read/write permissions for the DynamoDB table. Utilize the `GetAtt` function to extract the Access and Secret keys, and transmit these to the web application instance via its instance user-data.

B. Deploy an IAM Role with necessary permissions for DynamoDB table access. In the CloudFormation template, link this IAM Role to the AWS::IAM::InstanceProfile property of the application instance.

C. Use the Parameter section of the CloudFormation template to prompt the user to input AWS Access and Secret Keys from an existing IAM user with required DynamoDB interaction privileges.

D. Create an IAM Role with necessary permissions for DynamoDB table access. Associate this Role with application instances by referencing it in the AWS::IAM::InstanceRoleName Property in the CloudFormation template.

Correct Answer: B

Explanation:

B is the correct choice because:

- **Role-Based Access**: Assigning an IAM Role to EC2 instances for accessing DynamoDB ensures that no explicit AWS credentials need to be stored or passed. IAM Roles provide a secure way to grant permissions to AWS resources without the need to manage static access keys.
- **AWS::IAM::InstanceProfile**: This CloudFormation property enables the association of the IAM Role with the EC2 instances. This setup ensures that the application instances have the necessary permissions to interact with the DynamoDB table securely.
- **No Exposed Credentials**: By using IAM Roles, API credentials are not exposed or hard-coded, maintaining security best practices.

Why the Other Options Are Incorrect:

A is incorrect because it involves creating IAM users and handling access and secret keys. This method is less secure as it requires the management of static credentials, which can be a security risk.

C is incorrect as it requires manual input of Access and Secret Keys, which is not a scalable or secure approach. This method also exposes the risk of credential mismanagement.

D is incorrect because `AWS::IAM::InstanceRoleName` is not a valid CloudFormation property. The proper way to associate an IAM Role with EC2 instances in CloudFormation is through the `AWS::IAM::InstanceProfile` resource.

Question 89

A digital banking company operates its production workload on AWS Cloud and has multi-region support enabled for an AWS CloudTrail trail. The company's security policy mandates that all IAM user creations require approval from the security team. Upon the creation of an IAM user, all permissions for that user should be automatically revoked, followed by a notification to the security team for approval.

What steps should the solutions architect take to adhere to these company requirements? (Choose THREE)

A. Utilize Amazon EventBridge to trigger an AWS Step Function state machine, which will revoke permissions from the newly created IAM user.

B. Implement an Amazon EventBridge rule to monitor for specific patterns in AWS CloudTrail API activities, particularly the `CreateUser` event.

C. Configure Amazon EventBridge to launch AWS Fargate tasks for revoking permissions from the newly created IAM user.

D. Set up a filter in AWS CloudTrail for the `CreateUser` event and link it to notify an Amazon Simple Notification Service (Amazon SNS) topic.

E. Dispatch a message to an Amazon Simple Notification Service (Amazon SNS) topic, to which the security team is subscribed.

F. Employ AWS Audit Manager to continuously audit new user creations and alert the security team.

Correct Answer: A, B, E

Explanation:

A is correct because:

- Automated Permission Revocation: By using Amazon EventBridge to trigger an AWS Step Functions state machine, the process to automatically remove permissions from a newly created IAM user can be orchestrated. This aligns with the company's security policy.
- Workflow Management: AWS Step Functions enable the creation of complex workflows that can be used to automate the process of revoking permissions, ensuring compliance with security policies.

B is correct because:

- Event Pattern Matching: By creating a rule in Amazon EventBridge to monitor specific AWS CloudTrail API call patterns, particularly the `CreateUser` eventName, the system can detect when a new IAM user is created.
- Integration with CloudTrail: This setup leverages CloudTrail logs to trigger appropriate actions, which is key for monitoring IAM activities.

E is correct because:

- Notification to Security Team: Sending a message to an Amazon SNS topic, which the security team subscribes to, ensures that the team is promptly notified when a new IAM user is created. This step is crucial for the security team to review and approve the user creation.

Why the Other Options Are Incorrect:

C is incorrect because:

- Inefficient for Permission Revocation: While AWS Fargate could technically be used to run tasks, invoking AWS Fargate for the specific task of removing permissions from an IAM user is overly complex and not the most efficient solution compared to using AWS Step Functions.

D is incorrect because:

- Not Directly Applicable: While AWS CloudTrail can be configured to monitor `CreateUser` events, it cannot directly send notifications. The integration with Amazon EventBridge (as in option B) is required to initiate further actions like notifications.

F is incorrect because:

- Audit, Not Immediate Action: AWS Audit Manager is designed for auditing purposes and is not suited for real-time response actions like revoking permissions or sending immediate notifications to a security team. It focuses on compliance checks rather than operational tasks.

Question 90

A company has been operating a blockchain application on AWS using AWS OpsWorks for the past year. Recently, there have been numerous security updates for the Linux servers that support the blockchain application, necessitating updates to the OpsWorks stack instances.

In this context, which practices are most effective for updating an AWS stack? (Choose TWO)

A. Execute the Update Dependencies stack command on Windows-based instances.

B. Use the Update Dependencies stack command for Linux-based instances.

C. Implement CloudFormation to roll out the security patches.

D. Remove the entire stack and establish a new one.

E. Generate and activate new instances to substitute your existing online instances, and then decommission the current instances. The new instances will automatically incorporate the latest security patches during their setup.

F. Apply WAF to implement the security patches.

Correct Answer: B, E

Explanation:

B is correct because:

- Relevant Command for Linux Instances: The Update Dependencies stack command in AWS OpsWorks is specifically designed for updating software dependencies on Linux-based instances, making it directly applicable for the situation described.
- Efficient Patch Deployment: Running this command ensures that the latest security patches are applied efficiently, adhering to best practices in maintaining updated and secure instances.

E is correct because:

- Latest Security Patches on New Instances: By creating and starting new instances to replace the currently operational ones, the company can ensure that these new instances are set up with the most recent security patches, a crucial step in maintaining a secure environment.

- Minimal Downtime and Continuous Operation: This approach allows for a seamless transition with minimal downtime, as new instances can be brought online before decommissioning the old ones.

Why the Other Options Are Incorrect:

A is incorrect because:

- Windows-based Instances Not Mentioned: The question specifically mentions Linux servers, making the application of the Update Dependencies stack command on Windows-based instances irrelevant in this scenario.

C is incorrect because:

- CloudFormation Not for Patch Deployment: AWS CloudFormation is an infrastructure-as-code service for automating the setup of AWS resources. It is not typically used for deploying patches to existing instances.

D is incorrect because:

- Unnecessarily Disruptive: Completely deleting and recreating the stack

for patch updates is overly disruptive and inefficient. It would result in unnecessary downtime and the loss of configuration and state data, which is not ideal for ongoing operations.

F is incorrect because:

- WAF Is Not for Patch Management: AWS WAF (Web Application Firewall) is designed to protect web applications from common web exploits. It does not have a role in deploying operating system or software patches to instances.

Question 91

A company has a vast archive of user-submitted stock photos. They use an AWS Lambda function to analyze and extract metadata from these photos, forming a searchable catalog. This metadata extraction process is guided by specific rules, and the output is channeled to an Amazon ElastiCache for Redis cluster. The entire extraction operation for a batch takes around 45 minutes. Manual updates are initiated whenever there's a change in the extraction rules. With a growing volume of photo submissions, the company is looking to expedite the metadata extraction timeframe.

In this situation, which method should the Solutions Architect implement to accelerate the metadata extraction process?

A. Divide the single Lambda function into multiple functions, each focusing on a specific type of metadata. Utilize AWS Step Functions to concurrently execute these Lambda functions. Develop an additional workflow to gather the photo batch for processing and initiate the metadata extraction workflow for each image.

B. Break down the Lambda function into various functions targeted at distinct metadata types. Link these functions to an AWS Batch compute environment. Design another Lambda function to compile the photo batch for processing and dispatch each photo to the AWS Batch job queue.

C. Segment the Lambda function into separate functions, each dedicated to a particular metadata type. Construct a workflow with AWS Step Functions to run these Lambda functions simultaneously. Craft another Lambda function to assemble the photo batch for processing and route each photo to an Amazon SQS queue. Designate this SQS queue as the input for the Step Functions workflow.

D. Divide the Lambda function into distinct functions, each tailored to a specific metadata type. Develop another Lambda function to collect the photo batch for processing and dispatch each photo to an Amazon SQS queue. Set up all the metadata extraction Lambda functions to subscribe to this SQS queue with an increased batch size.

Correct Answer: A

Explanation:

A is correct because:

- Parallel Processing with AWS Step Functions: Using AWS Step Functions to manage multiple Lambda functions running in parallel significantly enhances the processing speed. This approach allows for the concurrent execution of various metadata extraction tasks, drastically reducing the total time required for processing a batch of photos.
- Workflow Efficiency: Implementing an additional workflow to sequentially retrieve and process each photo ensures that the metadata extraction workflow is executed efficiently for each image, further streamlining the process.

Why the Other Options Are Incorrect:

B is incorrect because:

- AWS Batch Limitation: AWS Batch is primarily designed for batch computing workloads and might not be as effective for Lambda-based event-driven processing tasks like metadata extraction. This approach could introduce unnecessary complexity and may not significantly reduce processing time.

C is incorrect because:

- Inefficiency with SQS and Step Functions: While using SQS as an input for the Step Functions workflow is possible, it introduces an additional layer of complexity and may not offer the same level of efficiency and simplicity as directly triggering a Step Functions workflow for each photo.

D is incorrect because:

- Potential Throttling with Lambda and SQS: Configuring all Lambda extraction functions to subscribe to an SQS queue can lead to throttling issues, especially when dealing with a high volume of photos. This approach may not provide the desired reduction in processing time and could lead to inefficiencies in handling the photo batch.

Question 92

A travel and tourism company operates with multiple AWS accounts assigned to different departments. The marketing department, using its own AWS account, stores campaign images and media files in an encrypted S3 bucket. The marketing team wishes to share this bucket with the management team for review purposes. An IAM role named mgmt_reviewer was created in the Management AWS account, and a custom AWS KMS key was set up in the Marketing AWS account, linked to the S3 bucket. Despite this, users from the Management account encounter an Access Denied error when assuming the IAM role and attempting to access the bucket.

What steps should the solutions architect take to ensure that users in the Management AWS account can access the Marketing team's S3 bucket with the necessary permissions? (Select THREE)

A. Update the policy of the custom AWS KMS key in the Marketing account to grant decrypt permissions to the mgmt_reviewer IAM role.

B. Modify the mgmt_reviewer IAM role policy to include read access to the Amazon S3 bucket and decrypt permissions for the custom AWS KMS key.

C. Implement an S3 bucket policy granting read permissions, setting the Principal to the Marketing team's AWS account ID.

D. Implement an S3 bucket policy granting read permissions, setting the Principal to the Management team's AWS account ID.

E. Adjust the custom AWS KMS key policy in the Marketing account to grant decrypt permissions using the Management team's AWS account ID.

F. Grant the mgmt_reviewer IAM role in the Management account full access to the S3 bucket, along with decrypt permissions for the custom KMS key via the IAM policy.

Correct Answer: A, B, D

Explanation:

A, B, D are correct because:

- KMS Key Policy Update (A): Updating the AWS KMS key policy in the Marketing account to include decrypt permissions for the mgmt_reviewer IAM role is critical. This change ensures that the role has the necessary permissions to decrypt objects in the S3 bucket, which is essential given the bucket's encryption with a custom AWS KMS key.
- IAM Role Policy (B): The mgmt_reviewer IAM role policy must have read access to the S3 bucket and decrypt permissions for the custom AWS KMS key. This setup is crucial to allow users assuming the role to access and decrypt the files in the bucket.
- S3 Bucket Policy (D): An S3 bucket policy granting read permissions with the Principal set to the Management team’s AWS account ID is necessary. This policy explicitly allows access to the S3 bucket for all users in the Management AWS account, facilitating the review process by the management team.

Why the Other Options Are Incorrect:

C is incorrect because:

- Principal Set to Marketing Team’s Account ID: Setting the Principal to the Marketing team's AWS account ID in the S3 bucket policy is redundant, as the Marketing team already owns the bucket and inherently has access. The requirement is to grant access to the Management team.

E is incorrect because:

- Decrypt Permissions Using Account ID: Granting decrypt permissions using the Management team’s AWS account ID is less precise and could lead to broader access than necessary. It's more secure and precise to grant permissions directly to the specific IAM role (mgmt_reviewer) intended for use by the Management team.

F is incorrect because:

- Full Access to S3 Bucket: Granting full access to the S3 bucket for the mgmt_reviewer IAM role could violate the principle of least privilege. The requirement is for read access to review files, not full access. Furthermore, adding decrypt permissions for the custom

KMS key in the IAM policy is redundant if the KMS key policy (Option A) is correctly configured.

Question 93

A company, after a security audit of its application, recognized the need for enhanced security measures for handling Amazon RDS for MySQL credentials. The credentials should be randomly generated, securely stored, and rotated every 90 days, with the infrastructure managed via AWS CloudFormation. The solutions architect is tasked with creating a CloudFormation template to meet these requirements.

What implementation should the solutions architect use to fulfill the company's needs with minimal operational overhead?

A. Utilize AWS Systems Manager Parameter Store to create a SecureString parameter for the database password. Develop an AWS Lambda function for password rotation. In AWS CloudFormation, define a Parameter Store RotationSchedule resource for rotating the password every 90 days.

B. In AWS Systems Manager Parameter Store, create a SecureString parameter for the database password. Use an AWS CloudFormation template to define an AWS KMS resource to manage password rotation every 90 days.

C. Employ AWS Secrets Manager to establish a secret resource for generating a secure database password. Script an AWS Lambda function for password rotation. In AWS CloudFormation, include a Secrets Manager RotationSchedule resource to automate password rotation every 90 days.

D. Implement AWS Secrets Manager to create a secret resource and generate a secure database password. Develop an AWS Lambda function for password rotation and set up an Amazon EventBridge scheduled rule to trigger this Lambda function for rotating the database password every 90 days.

Correct Answer: C

Explanation:

C is the appropriate choice because:

- AWS Secrets Manager: This service is specifically designed for managing secrets like database credentials. It supports secret rotation, which aligns with the requirement for automatic credential rotation every 90 days.
- Secrets Manager RotationSchedule: Integrating a RotationSchedule resource within AWS CloudFormation ensures an automated and scheduled rotation of the database

password. This setup minimizes operational overhead and ensures compliance with the company's security policy.
- Lambda for Password Rotation: Writing a Lambda function to handle the password rotation logic provides flexibility and control over the rotation process. This function can be linked with the Secrets Manager RotationSchedule for automated execution.

Why the Other Options Are Incorrect:

A is not optimal because:

- Systems Manager Parameter Store: While it can store database credentials securely, it doesn't natively support automatic password rotation like AWS Secrets Manager. Implementing a custom Lambda function for rotation adds operational complexity compared to the built-in rotation features of Secrets Manager.

B is incorrect because:

- KMS for Rotation: AWS KMS is not designed for rotating database credentials. It's primarily used for creating and managing encryption keys, not for password management or rotation.

D is less efficient because:

- EventBridge for Scheduling: While using Amazon EventBridge with Lambda for rotation is feasible, it introduces additional complexity compared to using the built-in rotation features of AWS Secrets Manager. The RotationSchedule resource in Secrets Manager provides a more streamlined approach for managing rotation schedules within CloudFormation.

Question 94

A leading insurance company in Southeast Asia recently introduced a web portal for account management, insurance plan viewing, and premium payments. The company noticed a significant amount of traffic from a country where they don't operate, leading to performance issues. This traffic was identified as a series of attacks from specific IP ranges.

What is the recommended solution to block these attacks coming from the identified IP ranges?

A. Implement a Security Group with specific deny rules to block the attacking IP addresses.

B. Construct a custom route table for the web tier and block the attacking IP addresses at the Internet Gateway.

C. Relocate the online portal to a private subnet.

D. Establish an inbound Network Access Control List (NACL) with explicit deny rules to block the attacking IP addresses.

Correct Answer: D

Explanation:

D is the correct choice because:

- Network Access Control Lists (NACLs): NACLs provide a layer of security at the subnet level. They act as a firewall for controlling traffic entering and leaving a subnet. NACLs can be configured with both allow and deny rules and are evaluated in order, providing the flexibility to explicitly deny traffic from specific IP ranges.
- Explicit Deny Rules: By creating deny rules in the NACLs for the identified attacking IP addresses, the unwanted traffic can be blocked before it reaches the EC2 instances or other resources within the subnet. This helps in mitigating the performance issues caused by the attack.

Why the Other Options Are Incorrect:

A is less effective because:

- Security Groups: While security groups are a type of virtual firewall, they are stateful and primarily used for allowing traffic. They do not support explicit deny rules, which limits their effectiveness in blocking specific unwanted traffic.

B is not feasible because:

- Custom Route Tables: Route tables control the routing of traffic within a VPC and between subnets but are not designed for blocking specific IP addresses. Their primary function is to define rules for network routing, not security.

C is not a direct solution because:

- Private Subnet: Moving the portal to a private subnet might limit public access, but it doesn't address the specific issue of blocking unwanted traffic from certain IP ranges. Additionally, making the portal private could restrict legitimate users from accessing it.

Question 95

A government agency is developing a mobile tax app allowing users to upload, view, and download their tax documents directly from an Amazon S3 bucket. The app will be widely used, hence it requires robust user authentication and security measures.

How should the infrastructure be configured for new user registrations on the app?

A. Generate long-term credentials using AWS Security Token Service (STS) with appropriate permissions, and store these credentials in the mobile app for S3 access.

B. Store user information in Amazon RDS. Create an IAM role with proper permissions. Use STS 'AssumeRole' to create temporary credentials when the app is used, storing them in the app's memory for S3 access. Regenerate credentials on each app launch.

C. Use Amazon DynamoDB to store user information. Create access credentials with STS having the necessary permissions. Store these credentials in the app's memory for S3 access each time the app is used.

D. Create an IAM user and assign the needed permissions. Generate an access key and secret key, store them in the app, and use these for S3 access.

Correct Answer: B

Explanation:

B is the correct option because:

- **Amazon RDS for User Information:** Utilizing Amazon RDS to store user information ensures a robust and scalable database solution that can handle the expected high volume of users.
- **IAM Role and STS AssumeRole:** Creating an IAM role with the required permissions and using STS's 'AssumeRole' function to generate temporary credentials each time the app is used enhances security. Temporary credentials reduce the risk of long-term credential exposure and misuse.
- **Storing Credentials Temporarily:** Storing these credentials in the app’s memory, rather than persistently, further enhances security by ensuring credentials are not stored long-term on the user’s device.

Why Other Options Are Incorrect:

A is incorrect because:

- **Long-term Credentials Risks:** Using long-term credentials increases the risk of security breaches, as these credentials could be exposed or misused if the mobile device is compromised.

C is incorrect because:

- DynamoDB for User Information: While DynamoDB is a powerful NoSQL database, the use case does not specify a need for its specific features over RDS.
- Credentials Management: It suggests storing credentials in the app's memory for repeated use, which could be a security risk if the credentials are not refreshed regularly.

D is incorrect because:

- IAM User Risks: Creating individual IAM users for each app user is not scalable or secure. It also implies storing long-term credentials on the user’s device, which poses a significant security risk.

Question 96

A retail company operates its customer support call system in-house. The Solutions Architect has been instructed to transfer this system to AWS, utilizing managed services for reduced overhead. The system needs to handle current functions like call reception and flow creation, scale for increased call volumes, and incorporate deep learning for caller intent recognition to minimize agent interaction. The goal is to identify caller intent through keywords and manage basic tasks, as well as support call center agents with relevant information.

Which two actions should the Solutions Architect implement to meet these requirements?

A. Queue incoming calls in an Amazon SQS queue and utilize Amazon Lex for analyzing the voice data to discern caller intent.

B. Direct incoming calls to an Amazon Kinesis stream, using Amazon Comprehend to interpret voice data for determining caller intent.

C. Develop an AI-based query response system with Amazon Alexa for Business to answer customer queries, reducing direct agent communication.

D. Implement Amazon Connect to establish a cloud-based, multi-channel contact center for agent interactions.

E. Employ Amazon Rekognition for caller identification and Amazon Polly for voice analysis to understand caller intent.

Correct Answer:

A. Queue incoming calls in an Amazon SQS queue and utilize Amazon Lex for analyzing the voice data to discern caller intent.

D. Implement Amazon Connect to establish a cloud-based, multi-channel contact center for agent interactions.

Explanation:

A is correct because:

- Amazon SQS as a Queue System: SQS effectively manages and queues incoming calls, ensuring a structured process for handling call data, especially during peak times.
- Amazon Lex for Voice Analysis: Lex specializes in understanding human language and can process voice data to recognize caller intent. This aligns with the requirement for deep learning capabilities in the call system.

D is correct because:

- **Amazon Connect

for Call Center Operations:** Amazon Connect is specifically designed as a cloud-based contact center service. It offers omnichannel capabilities, making it ideal for handling various forms of customer interactions, including calls. Its scalability and integration with other AWS services like Amazon Lex make it a fitting choice for the company's expanding needs.

Why Other Options Are Incorrect:

B. Direct incoming calls to an Amazon Kinesis stream, using Amazon Comprehend to interpret voice data for determining caller intent.

- Inappropriate for Voice Data: Amazon Kinesis is more suitable for large-scale data streaming and analytics, not specifically for handling call data. Additionally, Amazon Comprehend is primarily a text analysis service and would not be effective for processing voice data for caller intent.

C. Develop an AI-based query response system with Amazon Alexa for Business to answer customer queries, reducing direct agent communication.

- Different Use Case: While Amazon Alexa for Business can be used to build AI-based response systems, it's more tailored towards enterprise efficiency and productivity. It may not be the best fit for a customer support call system that requires specific integration with existing telephony infrastructure.

E. Employ Amazon Rekognition for caller identification and Amazon Polly for voice analysis to understand caller intent.

- Misaligned Services: Amazon Rekognition is a service for image and video analysis and is not suitable for voice or audio analysis. Amazon Polly is a text-to-speech service and does not analyze or interpret incoming voice data for caller intent. Therefore, this option does not align with the requirements for processing and understanding incoming call data.

Question 97

A prominent media enterprise headquartered in Los Angeles, California, operates a MySQL RDS instance within an AWS VPC. This organization utilizes a proprietary analytics application in its local data center, which necessitates read-only connectivity to the database. The objective is to establish a read replica of the active MySQL RDS instance in the AWS cloud, connecting it to the on-premises data center to serve as the endpoint for the analytics application.

Among the proposed methods to achieve this secure replication, which is the most advisable?

A. Set up the RDS instance as the primary server and initiate replication over the public Internet using an SSL endpoint directed at the on-premises server. Employ mysqldump for transferring database contents from Amazon S3 to the local MySQL instance, followed by initiating replication.

B. Since RDS cannot directly replicate to an on-premises database server, configure the RDS instance to replicate to an EC2 instance running core MySQL, and then implement replication over a secure VPN/VPG connection.

C. Implement a Data Pipeline that exports the MySQL data nightly, followed by securely downloading the data from an S3 HTTPS endpoint. Utilize mysqldump to transfer the database from Amazon S3 to the on-premises MySQL instance, initiating replication subsequently.

D. Establish an IPSec VPN connection using either OpenVPN or VPN/VGW via the Virtual Private Cloud service. Prepare an external MySQL instance separate from Amazon RDS. Set the MySQL DB instance as the replication source. Utilize mysqldump to transfer the database from the Amazon RDS instance to the on-premises MySQL instance and commence replication from the Amazon RDS Read Replica.

Best Answer:

D. Create an IPSec VPN connection using either OpenVPN or VPN/VGW through the Virtual Private Cloud service. Prepare an instance of MySQL running external to Amazon RDS. Configure the MySQL DB instance to be the replication source. Use mysqldump to transfer the database from the Amazon RDS instance to the on-premises MySQL instance and start the replication from the Amazon RDS Read Replica.

Explanation:

This answer is the most appropriate for several reasons:

- **Security and Encryption:** An IPSec VPN connection within the AWS VPC ensures a secure and encrypted data transfer channel. This is crucial for data integrity and confidentiality.
- **Control over MySQL Instance:** Having a separate MySQL instance outside Amazon RDS allows more flexibility and control over the replication process.
- **Replication Consistency and Integrity:** Using the MySQL DB instance as the source and mysqldump for data transfer ensures consistent and integral replication, vital for accurate analytics.
- **Use of Amazon RDS Read Replica:** Replicating from the RDS Read Replica optimizes performance and resource utilization, reducing the load on the primary RDS instance.

Why Other Options Are Incorrect:

A. Replicating over the public Internet, even with SSL, is less secure compared to a VPN. It could expose the process to security risks.

B. Direct RDS to on-premises replication is unsupported. Replicating to an EC2 instance adds complexity and potential security issues.

C. Data Pipeline exports introduce delays in data synchronization and may not suit near real-time data analytics. This method also increases complexity and failure points.

Question 98

A data analytics firm has recently transitioned to a hybrid cloud setup with AWS. Their operations involve collecting and processing large quantities of data, where each data set results in thousands of files, varying between 10 MB and 1 GB. They archive this data, which is infrequently accessed, but if needed, must be retrievable within 24 hours. The data sets are searchable by file ID, set name, authors, tags, and other attributes.

Which architecture option would be the most cost-effective while fulfilling these requirements?

A. Archive individual files in Glacier, labeling each with its filename. Retrieve data by searching the Glacier vault based on the search criteria.

B. Consolidate files of complete data sets into a single S3 bucket. Record the S3 object keys for the compressed files and other search metadata in a DynamoDB table. Retrieve data by querying the DynamoDB table and then restore files from the S3 bucket.

C. Store individually compressed files in an S3 bucket, along with the search metadata and S3 object keys in a separate S3 bucket. Implement a lifecycle rule to shift data from S3

Standard to Glacier after a set period. Retrieve data by querying the S3 bucket and then access the file from the alternate S3 bucket.

D. Compress and combine all files of each completed data set into a single Glacier archive. Record the archive ID and other search metadata in a DynamoDB table. Retrieve data by querying the DynamoDB table and restoring files using the identified archive ID.

Best Answer:

D. Compress and combine all files of each completed data set into a single Glacier archive. Store the archive ID and other search metadata in a DynamoDB table. To retrieve data, query the DynamoDB table for files that meet the search criteria, then restore files from the Glacier using the obtained archive ID.

Explanation:

This approach is the most suitable due to several reasons:

- Efficiency in Data Storage: By compressing and concatenating all files into a single Glacier archive for each data set, the company minimizes the storage footprint. This is especially cost-effective considering Glacier's pricing model, which favors larger, less frequently accessed files.
- Rapid Metadata Access: Storing search metadata along with the archive ID in DynamoDB ensures quick and efficient search capability. DynamoDB's fast access times complement the 24-hour retrieval requirement well.
- Streamlined Retrieval Process: With all relevant information stored in DynamoDB, the retrieval process is simplified. Once the required data set is identified in DynamoDB, the corresponding Glacier archive can be directly accessed using the stored archive ID.

Why Other Options Are Incorrect:

A. Archiving individual files in Glacier increases complexity and might incur higher costs due to the large number of archives created. Also, Glacier does not support querying archives based on custom search criteria directly.

B. While using S3 and DynamoDB provides quick access, continuously storing large files in S3, especially when rarely accessed, may not be as cost-effective as using Glacier for long-term storage.

C. Storing individual files in S3 and transitioning them to Glacier via lifecycle rules involves managing two storage locations. Additionally, querying metadata in an S3 bucket is not as efficient as using a database like DynamoDB.

Question 99

A multinational corporation has its data centers located across Europe, Asia, and North America. Each of these centers is connected to AWS through a 10Gbps Direct Connect link, and the company employs a custom VPN solution for encrypted data transfer to AWS. The data centers collectively house approximately 500 physical servers, which support a variety of applications and database services on Windows and Linux platforms. The company is now looking to shut down these data centers and transition its entire infrastructure to the AWS cloud. They require separate accounts for staging and deploying virtual machines (VMs) and the capability for AWS Region to Region Virtual Private Cloud (VPC) stack creation.

Which strategy should be adopted for this migration?

A. Utilize AWS Application Migration Service (AWS MGN). Deploy the AWS Replication agent on every physical server to initiate replication to the AWS Cloud. Following synchronization completion, launch test instances and proceed with the cutover to AWS.

B. Implement the Application Discovery Service from AWS. Install its agents on all physical servers and monitor the infrastructure through the AWS Migration Hub console. Start replication to transfer servers to AWS, and upon replication completion, begin the cutover to AWS.

C. Use AWS DataSync for the migration. Install the AWS DataSync agent on each physical server and begin replication to AWS using the AWS Management Console, copying server images to an Amazon S3 bucket as Amazon Machine Images (AMIs). Once done, use these AMIs to launch Amazon EC2 instances.

D. Apply AWS Outposts service for the migration. Install the AWS Outposts server agent in the data centers for incremental replication of servers into Amazon Machine Images (AMIs). Then, deploy these AMIs as Amazon EC2 instances to start the cutover.

Best Answer:

A. Leverage AWS Application Migration Service (AWS MGN) for the migration. Install the AWS Replication agent on each physical machine to start the replication to the AWS Cloud. After

syncing is completed, launch test instances and initiate cutover to the AWS Cloud.

Explanation:

The AWS Application Migration Service (AWS MGN) is the most suitable solution for this scenario for several reasons:

- Comprehensive Migration Solution: AWS MGN provides an end-to-end solution for migrating applications from physical or virtual infrastructure to AWS. It simplifies the process of migrating entire data centers.

- **Minimal Downtime:** AWS MGN allows for continuous replication of server data, which means that the migration can occur with minimal downtime. This is essential for maintaining business continuity during the transition.
- **Flexibility in Cutover:** After replication, AWS MGN enables testing in AWS without impacting the source production system. This ensures that everything functions correctly in AWS before the final cutover, reducing the risk of migration.
- **Compatibility with Physical Servers:** AWS MGN is designed to work with physical servers, making it well-suited for a scenario involving a mix of Windows and Linux servers.

Why Other Options Are Incorrect:

B. The Application Discovery Service is primarily for discovering and understanding on-premises infrastructure before migration. While it's useful for initial planning, it doesn't provide a complete migration solution like AWS MGN.

C. AWS DataSync is more focused on transferring data rather than complete server images. It's useful for moving large amounts of data to AWS, but it doesn't cover all aspects of a full infrastructure migration, such as application settings and server configurations.

D. AWS Outposts is designed to extend AWS infrastructure and services to on-premises facilities, not for migrating existing physical servers to AWS. It doesn't suit the requirement of decommissioning physical data centers and moving entirely to the AWS cloud.

Question 100

A legal consulting firm operates a WordPress website on EC2 instances distributed across multiple Availability Zones, supported by a Multi-AZ RDS MySQL database. The website employs an eventual consistency model and manages a high volume of read and write operations. However, users have been encountering slow website performance due to delayed read processes in the database layer. The firm has optimized its current database instances within its operational budget, focusing on cost-effectiveness and resource efficiency.

Which set of strategies would effectively resolve this performance issue? (Select THREE.)

A. Upgrade the RDS MySQL instance to provisioned IOPS.

B. Implement sharding to distribute the incoming load across several RDS MySQL instances.

C. Add an RDS MySQL Read Replica in each Availability Zone.

D. Deploy an Amazon ElastiCache Cluster with nodes in each Availability Zone.

E. Integrate Amazon CloudFront with the website for faster delivery of static media assets and consider using AWS Compute Optimizer for optimal sizing of Amazon EC2 instances.

F. Increase the size of the RDS MySQL database instance to a larger instance type.

Best Answer:

B. Implement sharding to distribute the incoming load to multiple RDS MySQL instances.

C. Add an RDS MySQL Read Replica in each Availability Zone.

D. Deploy an Amazon ElastiCache Cluster with nodes running in each Availability Zone.

Explanation:

These options are the most suitable because:

- B. Sharding: Sharding divides a database into smaller parts or shards, each managed by a separate RDS MySQL instance. This approach evenly distributes the load, enhancing the database's read and write capacity and performance.
- C. RDS MySQL Read Replica: Creating a Read Replica in each Availability Zone allows the website to manage increased read traffic by distributing the load across several servers. This setup is effective for applications that have a higher read-to-write ratio, as the read replicas can handle the read requests, reducing the load on the primary database.
- D. Amazon ElastiCache Cluster: ElastiCache enhances the speed of web applications by enabling faster data retrieval from in-memory caches instead of relying on slower disk-based databases. This can significantly improve the performance for read-intensive workloads and decrease the load on the database.

Why Other Options Are Less Effective:

- A. Provisioned IOPS: While increasing IOPS could enhance performance, it is more expensive and may not align with the firm's budget-focused strategy.
- E. CloudFront and Compute Optimizer: While CloudFront can accelerate the delivery of static content, it doesn't directly solve the database read performance issue. AWS Compute Optimizer might improve EC2 instance efficiency but doesn't directly address database performance.
- F. Larger Instance Type: Upgrading to a larger RDS instance may improve performance but can also lead to higher costs, potentially conflicting with the firm's emphasis on cost-effectiveness and resource efficiency.

Question 101

A prominent aerospace engineering firm is planning to transition to a hybrid cloud architecture and needs to migrate over 1 TB of crucial aeronautical data from their on-premises network to AWS. This data, varying from a few megabytes to multiple gigabytes per file, is frequently accessed and modified by their data scientists. To minimize business disruption, the migration must occur over the weekend. However, their current 50-Mbps Internet connection can only transfer the data in approximately 48 hours, which poses a time constraint.

Which strategy should the solutions architect employ to transfer all the aeronautical data to AWS within the required timeframe?

A. Over the weekend, sync the data from the on-premises data center to an S3 bucket using Multipart upload for large files. Configure the AWS-hosted application to access the aeronautical data files from the S3 bucket.

B. Begin transferring data to a Snowball Edge device after business hours on Friday. Once the Snowball Edge completes the data transfer to AWS, copy the data to multiple EBS volumes. On Sunday afternoon, attach these EBS volumes to your EC2 instances.

C. Implement a Gateway-Stored volume gateway using AWS Storage Gateway. Establish an iSCSI connection between the on-premises data center and AWS, then copy the data to the Storage Gateway volume. After successfully copying all data, create an EBS snapshot of the volume, and on Sunday, restore these snapshots as EBS volumes and attach them to EC2 instances.

D. Start syncing the on-premises data to an S3 bucket a week before the scheduled migration using the AWS CLI's S3 sync command. Conduct a final sync on Friday after business hours end. Configure the application in AWS to use the data from the S3 bucket in a large EC2 instance.

Best Answer:

D. Begin synchronizing the on-premises data to an S3 bucket one week before the migration schedule using the AWS CLI's S3 sync command. Perform a final synchronization task after business hours on Friday. Set up your application on a large EC2 instance in your VPC to utilize the S3 bucket.

Explanation:

This option is most effective due to:

- Timely Data Transfer: By starting the synchronization a week early, the bulk of the data is transferred ahead of time. This approach ensures that the 48-hour limitation posed by the 50-Mbps connection is circumvented.

- **Minimal Downtime:** The final sync on Friday evening will only need to transfer the data changed during the last week (estimated at 10%), significantly reducing the transfer time and ensuring the data is current with minimal downtime.
- **Immediate Availability:** The data in the S3 bucket is immediately available for use by applications hosted on EC2 instances. This ensures that the migration doesn't interfere with business operations and the applications have access to the latest data.

Why Other Options Are Ineffective:

A. Syncing over a single weekend might not be feasible given the data size and bandwidth limitations. This could lead to incomplete migration and extended downtime.

B. Using Snowball

Edge would typically be efficient for large data transfers, but the time constraints in this scenario make it impractical. The process of transferring data to Snowball Edge, shipping it to AWS, and then copying it to EBS volumes is unlikely to be completed within the limited timeframe available.

C. Setting up a Gateway-Stored volume gateway and transferring data via iSCSI involves complex configuration and might not meet the tight deadline for migration. Additionally, creating and restoring EBS snapshots can be time-consuming, especially for 1 TB of data.

Question 102

A technology firm focused on developing cloud-native applications currently employs AWS CloudFormation templates for application deployment on AWS. The team stores its application artifacts and templates in a version-controlled Amazon S3 bucket. Developers use Amazon EC2 instances equipped with integrated development environments (IDEs) to download, modify, and re-upload these artifacts to S3, conducting unit testing on their local EC2 instances. The company aims to refine this deployment process through a CI/CD pipeline to enhance developer productivity, with the following specific requirements:

- Adoption of AWS CodeCommit for storing application code and CloudFormation templates.
- Automated testing and security scanning of created artifacts.
- Notifications when unit testing fails.
- Flexibility to toggle application features on or off and customize deployments within the CI/CD pipeline.
- Lead Developer's approval required before deploying applications to production.

Which approach should the solutions architect adopt to fulfill these needs?

A. Employ AWS CodeArtifact for artifact storage, where AWS conducts vulnerability scans and runs custom actions for unit testing. Set up an Amazon CloudWatch rule to trigger Amazon SNS alerts on unit test failures. Use distinct Docker images for feature

selection in applications. Incorporate a manual approval stage within the pipeline for the Lead Developer to authorize deployments to production.

B. Configure a Jenkins job for artifact testing and security scanning. Establish an Amazon EventBridge rule to issue Amazon SES alerts when unit tests fail. Leverage AWS CloudFormation with nested stacks for feature toggling in applications. Introduce an AWS Lambda function in the pipeline for Lead Developer's approval before production deployment.

C. Write an AWS Lambda function to execute unit tests and security scans on the artifacts. Implement a subsequent Lambda trigger in the pipeline to notify developers of unit test failures. Utilize AWS Amplify plugins for feature toggling. Add an AWS SES action in the pipeline to seek the Lead Developer's approval for production deployment.

D. Set up an AWS CodeBuild job to conduct tests and security scans on the artifacts. Create an Amazon EventBridge rule to send Amazon SNS alerts upon unit test failures. Utilize AWS Cloud Development Kit (AWS CDK) constructs with a manifest file for feature management in the AWS CDK application. Integrate a manual approval stage in the pipeline for the Lead Developer to sanction production deployments.

Best Answer:

D. Establish an AWS CodeBuild job to perform tests and security scans on the created artifacts. Configure an Amazon EventBridge rule to dispatch Amazon SNS alerts in case of unit test failures. Implement AWS Cloud Development Kit (AWS CDK) constructs with a manifest file for controlling application features. Include a manual approval stage in the pipeline for the Lead Developer to approve before progressing to production deployment.

Explanation:

This solution aligns perfectly with the company's requirements for several reasons:

- AWS CodeBuild: It provides a fully managed build service that can compile source code, run tests, and produce software packages. CodeBuild can efficiently handle both automated testing and security scanning of artifacts, meeting the CI/CD pipeline needs.
- Amazon EventBridge and Amazon SNS Alerts: EventBridge can monitor and react to events in AWS services, like test outcomes in CodeBuild. Coupled with SNS, it ensures timely notifications are sent when unit tests fail, keeping developers informed.
- AWS Cloud Development Kit (AWS CDK): The AWS CDK allows defining cloud infrastructure using familiar programming languages. By using CDK constructs with a

manifest file, the company can dynamically manage application features, enabling easy toggling on or off as part of the deployment process.

- Manual Approval Stage: Adding a manual approval stage in the CI/CD pipeline for the Lead Developer ensures that changes are reviewed and authorized before being deployed to production, which is a critical governance requirement.

Why Other Options Are Less Effective:

A. While AWS CodeArtifact is a tool for artifact management, it doesn't inherently provide the specific testing and CI/CD integration that CodeBuild offers.

B. Jenkins is a popular automation server but would require additional configuration and management compared to using native AWS services like CodeBuild and CodePipeline.

C. Writing custom AWS Lambda functions for these tasks would be more labor-intensive and less integrated compared to leveraging AWS's managed services specifically designed for CI/CD workflows.

Question 103

A business operates a vital application on a constant array of Amazon EC2 instances, interfaced with an Application Load Balancer. The application functions by accessing a 120GB dataset, necessitating high throughput and low latency storage. Consequently, the dataset is stored on Provisioned IOPS (PIOPS) Amazon EBS volumes, each set to 3000 IOPS. The EC2 instances are provisioned using a launch template that attaches a 120GB PIOPS EBS volume to each instance. However, the cost of operating these EBS volumes has become a financial concern. The Solutions Architect is now tasked with devising a cost-effective strategy that maintains the application's performance and data durability.

Among the given options, which one would fulfill the company's requirements?

A. Implement an Amazon EFS volume, shared across all EC2 instances. Opt for the Provisioned Throughput mode on the EFS volume to achieve the necessary IOPS.

B. Modify the EC2 launch template to exclude the PIOPS EBS volume. Instead, integrate a 120GB instance store volume on each EC2 instance to provide sufficient IOPS for the application.

C. Switch to more economical General Purpose SSD (gp2) EBS volumes rather than PIOPS EBS volumes. A 1TB gp2 EBS volume offers a throughput of 3000 IOPS. Update the launch template to allocate this type of volume.

D. Set up an Amazon EFS volume, accessible by all EC2 instances. Enable Max I/O performance mode on the EFS volume to ensure it meets the required IOPS.

Best Answer:

A. Construct an Amazon EFS volume and connect it across all Amazon EC2 instances. Utilize the Provisioned Throughput mode on the EFS volume to guarantee reaching the needed IOPS.

Explanation:

The selected solution is ideal due to several factors:

- Shared Storage: Amazon EFS provides a shared file system that can be mounted across multiple EC2 instances. This eliminates the need for individual EBS volumes on each instance, leading to cost savings.
- Provisioned Throughput: By choosing Provisioned Throughput mode, the EFS volume can be configured to deliver the specific throughput required by the application, ensuring that performance requirements are met without over-provisioning resources.
- Cost-Effectiveness: EFS with Provisioned Throughput can be more cost-effective than using multiple high-IOPS EBS volumes, especially when high throughput is needed without the high IOPS characteristic of PIOPS volumes.

Why Other Options Are Less Suitable:

B. Instance store volumes provide ephemeral storage, which means the data is lost if the instance is stopped or terminated. This presents a significant risk to data durability, making it unsuitable for mission-critical applications.

C. Although gp2 volumes are more affordable, they might not consistently deliver the required IOPS for the application, especially under peak loads. The large size (1TB) needed to achieve 3000 IOPS also may result in under-utilized storage, negating some cost benefits.

D. Max I/O mode in Amazon EFS is designed for workloads that require the highest levels of throughput, often above what Provisioned Throughput mode offers. While it could potentially provide high IOPS, it's typically more expensive than Provisioned Throughput mode and may be overkill for the application's requirements.

Question 104

A company operates a high-performance computing (HPC) application within their AWS VPC, utilizing hundreds of private EC2 instances arranged in a cluster placement group for high-speed intercommunication (up to 10 Gbps). Additionally, they have a custom cluster controller EC2 instance, configured identically to the other instances in terms of instance type and AMI. This controller, equipped with a public IP address, is situated outside the cluster placement group and is responsible for tightly managing and monitoring the system performance of each cluster instance. The Solutions Architect is now charged with enhancing the network performance between the cluster controller and the instances within the placement group, aiming to maintain low-latency network interactions.

What is the most effective solution the Architect should implement to meet this requirement?

A. Terminate the current cluster controller instance and relaunch it within the same placement group. Add an Elastic Network Adapter (ENA) to the cluster controller for boosted network performance. Alter the placement group's strategy to 'Spread'.

B. Assign an Elastic IP address to the cluster controller instance to enhance its network capacity to 10 Gbps.

C. Terminate the existing cluster controller EC2 instance and halt all running instances in the current placement group. Relocate the cluster controller to this placement group and then reboot all instances.

D. Halt the cluster controller instance and reposition it within the existing placement group.

Best Answer:

D. Cease the operation of the cluster controller instance and transfer it into the pre-existing placement group.

Explanation:

This solution is optimal because:

- Efficient Relocation: By stopping (not terminating) the cluster controller instance, it can be effectively moved to the placement group without losing its configuration or data. This approach is less disruptive compared to terminating and relaunching the instance.
- Enhanced Network Performance: Placing the cluster controller within the same placement group as the other EC2 instances ensures that it can communicate with them at the high network speeds (up to 10 Gbps) that are characteristic of cluster placement groups. This proximity minimizes latency, which is crucial for the controller's role in monitoring and managing the cluster.
- Preservation of Settings: Since the controller instance is configured with a public IP address, stopping and moving it to the placement group retains its accessibility, along with its specific configuration and role.

Why Other Options Are Less Suitable:

A. Terminating and relaunching the cluster controller would unnecessarily disrupt its configuration and the overall operation. Adding an ENA does not fundamentally address the issue of placement for improved network performance. Changing to a 'Spread' placement strategy is more suited for resilience rather than network performance optimization.

B. Assigning an Elastic IP does not inherently increase the instance’s network capacity to 10 Gbps. The limitation here is not the IP addressing but the placement of the controller outside the high-speed network environment of the cluster placement group.

C. Stopping all running instances in the placement group to move the cluster controller instance is excessively disruptive, leading to unnecessary downtime for the entire HPC application. This approach is not practical for a mission-critical application where continuity is important.

Question 105

A prominent electronics company is gearing up for a significant public reveal of its new smartphone. Their official website, fronted by an Application Load Balancer, relies on an Auto Scaling group of On-Demand EC2 instances dispersed across various Availability Zones, coupled with a Multi-AZ RDS MySQL database. Ahead of the product launch, a solutions architect evaluated the website's performance and observed delayed data retrieval from the database under the strain of over 100,000 concurrent requests, although static content like images and videos loaded efficiently. The aim is to resolve this issue cost-effectively.

Which two actions should be taken to address this problem?

A. Deploy a CloudFront web distribution to address the latency issue.

B. Introduce Read Replicas for RDS in each Availability Zone.

C. Enhance the size of the RDS MySQL database instance and augment the provisioned IOPS for quicker processing.

D. Apply sharding in the database layer, spreading the incoming load across several RDS MySQL instances.

E. Establish a caching mechanism using ElastiCache in-memory cache in each Availability Zone.

F. Transition the database to Amazon Keyspaces, which inherently supports sharding to disperse database queries across multiple nodes.

Best Answer:

B. Incorporate Read Replicas for RDS in each Availability Zone.

E. Implement an ElastiCache in-memory caching system in every Availability Zone.

Explanation:

These solutions are most effective due to:

- **B. Read Replicas in RDS:** Adding Read Replicas in each Availability Zone enhances the database's ability to handle high read loads, like those expected during the product launch. This allows the primary database to handle writes, while read operations are distributed across the replicas, reducing the load on the primary instance and improving response times for data retrieval.
- **E. ElastiCache In-Memory Cache:** ElastiCache provides a high-performance in-memory cache. By caching frequently accessed data, it significantly reduces the need to access the database for every request, leading to faster data retrieval and reduced load on the RDS instance. This is particularly effective for dynamic content that is accessed frequently but changes infrequently.

Why Other Options Are Less Suitable:

A. CloudFront is effective for distributing static content but doesn’t directly alleviate the database load, which is the core issue identified.

C. Upgrading the RDS instance size and IOPS can improve performance but may not be the most cost-effective approach, especially under highly variable load conditions.

D. Database sharding could distribute the load but would require significant changes to the database architecture and application logic. It's a more complex and potentially costly solution compared to adding Read Replicas and implementing caching.

F. Migrating to Amazon Keyspaces involves a major change in database technology and could incur significant migration costs and complexity. This is not necessary for the issue at hand and might not be the most cost-effective or timely solution.

Question 106

A logistics company utilizes Amazon EC2 instances for its business application, with a web application running on an Auto Scaling group of EC2 instances behind an Application Load Balancer. The database, a self-managed MySQL instance on a large EC2 instance, is designed for heavy I/O operations. While the application manages regular traffic effectively, it experiences significant slowdowns during the last four days of each month when users intensify month-end report activities. The Solutions Architect is tasked with enhancing application performance during these peak periods, focusing on minimizing any impact on availability.

Which strategy should the Solutions Architect implement to achieve this?

A. Upgrade all EC2 instance EBS volumes to GP2 volumes for better I/O performance. Scale up the EC2 instances to larger types. Pre-warm the Application Load Balancer to manage sudden traffic surges.

B. Transition the Amazon EC2 database instance to Amazon RDS for MySQL. Introduce additional read replicas in the database cluster towards month-end to accommodate the traffic spike.

C. Snapshot the EBS volumes handling heavy I/O operations and switch them to Provisioned IOPS volumes during the month's end. Post-peak period, revert to the original EBS volume types to economize.

D. Set up Amazon CloudWatch metrics for tracking EC2 instance CPU usage or ALB response time. Configure an AWS Lambda function to modify the EC2 instance size, type, and allocated IOPS of the EBS volumes when thresholds are exceeded.

Best Answer:

B. Migrate the Amazon EC2 database instance to Amazon RDS for MySQL and augment the database cluster with additional read replicas towards the end of the month to manage the increased load.

Explanation:

This solution is the most effective due to:

- Managed Database Service: Amazon RDS provides a managed database service that can offer improved performance and scalability compared to a self-managed EC2 database instance. RDS handles routine database tasks like provisioning, patching, backup, recovery, failure detection, and repair.
- Read Replicas: Adding read replicas in Amazon RDS efficiently handles increased read traffic, which is typical for report generation activities. This setup allows the primary database to focus on write operations while replicas handle the read queries, thereby enhancing overall performance.
- Scalability: Amazon RDS can automatically scale to meet the demands of the application, especially during peak usage times. This scalability is crucial for maintaining performance during the high-demand period at month-end.

Why Other Options Are Less Suitable:

A. Upgrading to GP2 volumes and scaling up EC2 instances can improve performance but might not be as effective in managing database-specific loads. Pre-warming the ALB addresses only part of the issue and doesn't directly improve database performance.

C. Changing EBS volumes to Provisioned IOPS and then reverting them is a complex process that may introduce risks and potential downtime, which can affect application availability.

D. Automating instance resizing and IOPS allocation based on CloudWatch metrics with Lambda is technically feasible but adds complexity. It may not adequately address the specific performance issues related to high database read operations during peak times.

Question 107

A stock trading company currently operates its application on AWS, with a crucial database hosted on an Amazon RDS for MySQL instance in a Multi-AZ setup. Hourly automated snapshots are taken through AWS Backup. Following a test of RDS database failover, the operations team observed an outage lasting about 40 seconds. The management now seeks a solution from the solutions architect to cut down this outage to under 20 seconds. The objective is to maintain most connections during failovers, barring those engaged in transactions or SQL statements. New database connections should be accepted, and incoming write requests queued during the failover.

To meet these requirements, which three actions should the solutions architect take (CHOOSE THREE)?

A. Switch the Amazon RDS for MySQL cluster to an Amazon Aurora for MySQL cluster.

B. Implement an Amazon RDS Proxy to manage traffic direction to operational RDS instances.

C. Verify that Multi-AZ is active on Amazon RDS for MySQL, and add one or more read replicas to ensure rapid failover.

D. Activate Amazon RDS Optimized Reads and deploy an Amazon ElastiCache for Redis cluster before the database layer to temporarily handle queries during RDS downtime.

E. Enable Amazon RDS Optimized Writes and set up an Amazon ElastiCache for Memcached cluster before the database layer to cache frequently accessed queries.

F. Confirm that Multi-AZ is operational on Amazon Aurora, and introduce one or more Aurora Replicas.

Best Answer:

A. Migrate the Amazon RDS for MySQL cluster to an Amazon Aurora for MySQL cluster.

B. Establish an Amazon RDS Proxy in front of the database layer for automated traffic routing to healthy RDS instances.

F. Ensure Multi-AZ is functional on Amazon Aurora and create one or more Aurora Replicas.

Explanation:

These solutions are the most effective due to:

- A. Amazon Aurora for MySQL Migration: Aurora provides enhanced performance and availability compared to standard MySQL RDS instances. It features faster failover times, often less than 20 seconds, thus aligning with the company's requirement to reduce outage duration.
- B. Amazon RDS Proxy: RDS Proxy can manage database connections more efficiently. It preserves connections during failovers, ensuring that new connections are accepted and write requests are queued as necessary. This contributes to reducing application disruption during a database failover.
- F. Aurora Replicas and Multi-AZ in Aurora: Aurora Replicas in a Multi-AZ deployment provide additional redundancy and facilitate quicker failover compared to standard RDS instances

. This setup helps in achieving the desired failover time of less than 20 seconds, maintaining high availability and resilience.

Why Other Options Are Less Suitable:

C. While enabling Multi-AZ and creating read replicas in Amazon RDS for MySQL can provide high availability, they may not significantly reduce the failover time to the desired 20 seconds or less, especially compared to the performance enhancements offered by Aurora.

D. Amazon RDS Optimized Reads with ElastiCache for Redis can improve read performance but does not directly impact the failover time of the database. Additionally, it doesn't address the queuing of write requests during failovers.

E. RDS Optimized Writes with ElastiCache for Memcached improves caching of frequently requested queries but does not significantly contribute to reducing the database failover time or maintaining connections during the failover process.

Question 108

A company's serverless application on AWS, consisting of Amazon API Gateway, AWS Lambda, and Amazon DynamoDB, facilitates features like creating posts and replying to comments on various topics. The API currently includes methods such as `GET /posts/[postid]`, `GET /users/[userid]`, and `GET /comments/[commentid]`. The application doesn't employ API keys for authorization. Aiming to boost user engagement, the company seeks to reduce comment latency and enable comments to appear in real-time.

What solution should be implemented to achieve these goals and enhance user experience?

A. Establish a distribution on Amazon CloudFront with edge-optimized APIs. Cache API responses in CloudFront for improved comment latency.

B. Modify the application code to frequently invoke the `GET /comments/[commentid]` API, such as every 3 seconds, to display comments in real-time, without compromising performance.

C. Utilize AWS AppSync to create GraphQL APIs, employing Websockets for real-time comment delivery.

D. Decrease API response times by raising the concurrency limit of the Lambda functions, allowing them to execute in parallel and deliver comments in real-time.

Best Answer:

C. Implement AWS AppSync, developing GraphQL APIs and utilizing Websockets for the real-time delivery of comments.

Explanation:

- C. AWS AppSync with GraphQL and Websockets: This approach is ideal because AWS AppSync supports real-time updates using GraphQL subscriptions. Websockets, a key feature of GraphQL subscriptions, enable the server to push updates to the client (web app) in real-time whenever a new comment is made. This setup is inherently designed for real-time data delivery, thus significantly enhancing user engagement by showing comments as they happen without requiring manual refreshing or polling by the client.

Why Other Options Are Less Effective:

- A. CloudFront with Cached Responses: While Amazon CloudFront can improve latency by caching content at edge locations, it isn't suitable for delivering real-time data. Cached responses mean that users might see outdated comments until the cache is refreshed, which doesn't align with the requirement for real-time updates.
- B. Frequent API Polling: Updating the application to call the `GET` API every few seconds is a form of polling, which can lead to increased load on the backend and isn't as efficient or scalable as using real-time communication protocols like Websockets. This approach can also introduce unnecessary delays in comment visibility.
- D. Increased Lambda Concurrency: Enhancing Lambda concurrency limits can improve the overall performance and scalability of the backend. However, it doesn't address the fundamental need for real-time data delivery to the client. The application would still rely on periodic requests to the server for updates, rather than receiving them instantaneously as they occur.

Question 109

An adventure company is experiencing scalability issues with their PostgreSQL database in their on-premises data center, which is used to store event data from a monitoring application. The database struggles to handle frequent write events. The company wants a hybrid solution that connects to AWS via an existing VPN and meets the following requirements:

- Use AWS-managed services for reduced operational overhead.
- Implement a scalable buffer for ingesting events.
- Include a visualization tool for near real-time event monitoring with dashboard capabilities.
- Accommodate dynamic schemas and semi-structured JSON data.

Which two solutions should the solutions architect implement to fulfill these requirements?

A. Set up an Amazon Aurora PostgreSQL DB cluster for event ingestion and use Amazon QuickSight for near-real-time dashboards and visualizations.

B. Utilize Amazon Neptune DB with its auto-scaling feature for event ingestion and Amazon QuickSight as the visualization tool.

C. Ingest events using Amazon Kinesis Data Firehose and process/transform the buffered events with an AWS Lambda function.

D. Employ Amazon Kinesis Data Stream for reliable event ingestion and an AWS Lambda function for processing and transforming events.

E. Create an Amazon OpenSearch Service domain for event ingestion and use OpenSearch Dashboards for near-real-time visualizations and dashboards.

Best Answer:

C. Ingest events using Amazon Kinesis Data Firehose and utilize an AWS Lambda function to process and transform the buffered events.

E. Establish an Amazon OpenSearch Service domain for reliable event ingestion and leverage OpenSearch Dashboards for creating near-real-time dashboards and visualizations.

Explanation:

- C. Kinesis Data Firehose and AWS Lambda: Kinesis Data Firehose is designed for efficiently capturing, transforming, and loading streaming data into AWS. It can handle high throughput and scale automatically, meeting the requirement for a scalable event ingestion buffer. AWS Lambda can be used to process and transform the incoming data (e.g., converting JSON data into the desired format), fitting the requirement for handling semi-structured JSON data and dynamic schemas.

- **E. Amazon OpenSearch Service:** OpenSearch Service (formerly known as Amazon Elasticsearch Service) is capable of handling large volumes of streaming data, making it well-suited for ingesting events from Kinesis Data Firehose. It supports semi-structured data like JSON and allows for the creation of near-real-time dashboards and visualizations through OpenSearch Dashboards, fulfilling the visualization requirement.

Why Other Options Are Less Suitable:

- **A. Amazon Aurora PostgreSQL and QuickSight:** While Aurora PostgreSQL is a powerful database service, it is not specifically optimized for the high-volume event ingestion scenario described. QuickSight is suitable for visualization but would be more effective when paired with a service designed for handling streaming data.
- **B. Amazon Neptune DB and QuickSight:** Neptune is a graph database service optimized for storing and querying highly connected data, not for high-throughput event ingestion like Kinesis Data Firehose or OpenSearch Service.
- **D. Amazon Kinesis Data Stream and AWS Lambda:** While Kinesis Data Streams can handle real-time streaming data, it requires more management and fine-tuning compared to Kinesis Data Firehose, which offers a simpler, more automated solution for the use case.