**Solution Notes Practice Test - 3**

**Question 1**

**What does this IAM policy do?**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Mystery Policy",
      "Action": ["ec2:RunInstances"],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "34.50.31.0/24"
        }
      }
    }
  ]
}
```

**Correct Option:**

It allows starting an Amazon EC2 instance only when the IP where the call originates is within the 34.50.31.0/24 CIDR block.

**Explanation:**

- This IAM policy restricts the action of starting an EC2 instance based on the source IP address.
- The aws:SourceIp in the condition restricts actions to calls originating from the specified IP range.
- IAM policies manage access by defining permissions for AWS resources. These permissions are evaluated when an IAM principal (user or role) makes a request.
- Most policies are stored as JSON documents.

**Incorrect Options:**

- Public IP within 34.50.31.0/24
- Elastic IP within 34.50.31.0/24
- Private IP within 34.50.31.0/24

These options incorrectly suggest that the IP addresses of the Amazon EC2 instances must belong to the 34.50.31.0/24 CIDR block for the EC2 instances to start. Actually, the policy states that the Amazon EC2 instance should start only when the IP where the call originates is within the 34.50.31.0/24 CIDR block.

**Conclusion:**

- IAM policies can restrict actions based on the source IP.
- Understand the differences between Elastic, Public, and Private IP addresses.
- Private IP ranges are: 192.168.0.0 - 192.168.255.255, 172.16.0.0 - 172.31.255.255, 10.0.0.0 - 10.255.255.255.
- Remember that 34.50.31.0/24 is a public IP range.

**Question 2**

**A company is looking at storing their less frequently accessed files on AWS that can be concurrently accessed by hundreds of Amazon EC2 instances. The company needs the most cost-effective file storage service that provides immediate access to data whenever needed.**

**Correct Option:**

Amazon Elastic File System (EFS) Standard–IA storage class

**Explanation:**

- Amazon EFS is a file storage service for use with Amazon compute (EC2, containers, serverless) and on-premises servers.
- It provides a file system interface, file system access semantics (such as strong consistency and file locking), and concurrently accessible storage for up to thousands of Amazon EC2 instances.
- The Amazon S3 Standard–IA storage class reduces storage costs for files that are not accessed every day. It does this without sacrificing the high availability, high durability, elasticity, and POSIX file system access that Amazon EFS provides.

- AWS recommends Standard-IA storage if you need your full dataset to be readily accessible and want to automatically save on storage costs for files that are less frequently accessed.

**Incorrect Options:**

- Amazon S3 Standard-Infrequent Access (S3 Standard-IA): Amazon S3 is an object storage service. It is not a file storage service.
- Amazon EFS Standard storage class: Suitable for frequently accessed files.
- Amazon EBS: A block-level storage service for use with Amazon EC2. It is not designed for concurrent access by multiple instances.

**Conclusion:**

- EFS Standard–IA is best for less frequently accessed files requiring file storage capabilities.
- Understand the differences between file storage and object storage services and their use cases.
- EFS Standard–IA offers cost savings while maintaining high availability and durability.

**Question 3**

**A manufacturing company receives unreliable service from its data center provider because the company is located in an area prone to natural disasters. The company is not ready to fully migrate to the AWS Cloud, but it wants a failover environment on AWS in case the on-premises data center fails. The company runs web servers that connect to external vendors. The data available on AWS and on-premises must be uniform. Which of the following solutions would have the LEAST amount of downtime?**

**Correct Option:**

Set up a Route 53 failover record. Run application servers on Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group. Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3.

**Explanation:**

- If you have multiple resources that perform the same function, you can configure DNS failover so that Route 53 will route your traffic from an unhealthy resource to a healthy resource.
- Elastic Load Balancing is used to automatically distribute your incoming application traffic across all the Amazon EC2 instances that you are running.
- AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. It provides low-latency performance by caching frequently accessed data on-premises while storing data securely and durably in Amazon cloud storage services.

**Incorrect Options:**

- These options involve AWS CloudFormation as part of the solution. CloudFormation takes time to provision the resources and hence is not the right solution when the least amount of downtime is mandated for the given use case.

**Conclusion:**

- To minimize downtime, use Route 53 for DNS failover, Auto Scaling, and Application Load Balancer (ALB) for application availability, and Storage Gateway for data backup and caching.
- Understand the use cases for each of these services and how they can work together to provide a reliable failover environment.

**Question 4**

**You would like to store a database password in a secure place, and enable automatic rotation of that password every 90 days. What do you recommend?**

**Correct Option:**

AWS Secrets Manager

**Explanation:**

- AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources.
- The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.
- Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text.
- Secrets Manager offers secret rotation with built-in integration for Amazon RDS, Amazon Redshift, and Amazon DocumentDB.

**Incorrect Options:**

- AWS Key Management Service (AWS KMS): A service for key management and encryption, not for storing secrets.
- AWS CloudHSM: A hardware security module (HSM) for encryption keys, not for secrets management.
- AWS Systems Manager Parameter Store: Requires manual rotation of secrets, unlike Secrets Manager which automates it.

**Conclusion:**

- Use AWS Secrets Manager for securely storing and automatically rotating secrets such as database passwords.
- Secrets Manager simplifies secrets management by providing API-based access and built-in integration for rotation with various AWS services.
- Understand the different use cases for Secrets Manager, KMS, CloudHSM, and Parameter Store.

**Question 5**

**Your company has an on-premises Distributed File System Replication (DFSR) service to keep files synchronized on multiple Windows servers and would like to migrate to AWS cloud. What do you recommend as a replacement for the DFSR?**

**Correct Option:**

Amazon FSx for Windows File Server

**Explanation:**

- Amazon FSx for Windows File Server provides fully managed, highly reliable file storage that is accessible over the industry-standard Service Message Block (SMB) protocol.
- It is built on Windows Server, delivering a wide range of administrative features such as user quotas, end-user file restore, and Microsoft Active Directory (AD) integration.
- The Distributed File System Replication (DFSR) service is a multi-master replication engine that is used to keep folders synchronized on multiple servers. Amazon FSx supports the use of Microsoft's Distributed File System (DFS) to organize shares into a single folder structure up to hundreds of PB in size.

**Incorrect Options:**

- Amazon FSx for Lustre: High-performance computing, not suitable for DFS replication.
- Amazon Elastic File System (Amazon EFS): For Linux, not Windows.
- Amazon Simple Storage Service (Amazon S3): An object storage service, not a file system.

**Conclusion:**

- Amazon FSx for Windows File Server is ideal for Windows-based file storage with DFS capabilities.
- It provides the necessary replication and administrative features needed to replace on-premises DFSR.
- Understand the differences between FSx for Windows, FSx for Lustre, EFS, and S3, and their use cases.

**Question 6**

**Consider the following policy associated with an IAM group containing several users:**

```
{
 "Version": "2012-10-17",
 "Id": "EC2TerminationPolicy",
 "Statement": [
  {
   "Effect": "Deny",
   "Action": "ec2:*",
   "Resource": "*",
   "Condition": {
    "StringNotEquals": {
     "ec2:Region": "us-west-1"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": "ec2:TerminateInstances",
   "Resource": "*",
   "Condition": {
    "IpAddress": {
     "aws:SourceIp": "10.200.200.0/24"
```

```
} } } ]}
```

Which of the following options is correct?

**Correct Answer:**

Users belonging to the IAM user group can terminate an Amazon EC2 instance in the us-west-1 region when the user's source IP is 10.200.200.200.

**Explanation:**

- The given policy denies all EC2 actions on all resources when the region of the underlying resource is not us-west-1.
- The policy allows the terminate EC2 action on all resources when the source IP address is in the CIDR range 10.200.200.0/24.
- Therefore, it would allow the user with the source IP 10.200.200.200 to terminate the Amazon EC2 instance in the us-west-1 region.

**Incorrect Options:**

- **Users belonging to the IAM user group cannot terminate an Amazon EC2 instance in the us-west-1 region when the user's source IP is 10.200.200.200:** This contradicts the policy allowing termination if the source IP is within the specified range.
- **Users belonging to the IAM user group can terminate an Amazon EC2 instance in the us-west-1 region when the EC2 instance's IP address is 10.200.200.200:** This misinterprets the condition related to the user's source IP, not the EC2 instance's IP.
- **Users belonging to the IAM user group can terminate an Amazon EC2 instance belonging to any region except the us-west-1 region when the user's source IP is 10.200.200.200:** This contradicts the policy which specifically allows termination in us-west-1 when the source IP is in the specified range.

**Conclusion:**

- IAM policies can combine deny and allow statements with conditions.
- Understand how to structure IAM policies to control access based on conditions like source IP and region.
- Recognize the importance of defining precise conditions in policies to ensure correct application.
    - Ensure to check the specific conditions and regions stated in the policy to correctly interpret its effects.

**Question 7**

**Question:** An application is currently hosted on four Amazon EC2 instances (behind an Application Load Balancer) deployed in a single Availability Zone (AZ). To maintain an acceptable level of end-user experience, the application needs at least 4 instances to be always available. As a solutions architect, which of the following would you recommend so that the application achieves high availability with MINIMUM cost?

**Correct Option:**

Deploy the instances in three Availability Zones (AZs). Launch two instances in each Availability Zone (AZ)

**Explanation:**

- Spreading instances across three AZs ensures availability if one AZ fails.
- Even with one AZ down, the remaining instances can handle the load.
- This configuration maintains high availability while optimizing costs by using only six instances.

**Incorrect Options:**

- **Deploying in two AZs with two instances each:** This setup risks falling below the threshold of available instances if one AZ fails.
- **Deploying four instances in two AZs:** Not cost-effective as it involves more instances than necessary to maintain availability.
- **Deploying in a single AZ:** This does not meet high availability requirements as failure in the single AZ will cause downtime.

**Conclusion:**

- Distribute instances across multiple AZs for high availability.
- Understand the importance of redundancy and cost-effectiveness in designing high-availability solutions.
    - Recognize that using multiple AZs helps ensure that applications remain available even during failures in one AZ.

**Question 8**

**Question:** Which of the following would you identify as correct regarding the data transfer charges for Amazon RDS read replicas?

**Correct Option:**

There are data transfer charges for replicating data across AWS Regions.

**Explanation:**

1. Amazon RDS Read Replicas enhance performance and durability for RDS DB instances.
2. Read Replicas make it easy to scale out beyond the capacity constraints of a single DB instance for read-heavy workloads.
3. A read replica is billed as a standard DB Instance at the same rates.

4. There are no data transfer charges for replicating data within the same AWS Region.
5. There are data transfer charges for replicating data across different AWS Regions.

**Incorrect Options:**

1. There are data transfer charges for replicating data within the same Availability Zone (AZ).
   - Explanation: Data transfer within the same AZ does not incur charges.
2. There are data transfer charges for replicating data within the same AWS Region.
   - Explanation: Data transfer within the same region does not incur charges.
3. There are no data transfer charges for replicating data across AWS Regions.
   - Explanation: Data transfer across different regions does incur charges.

**Conclusion:**

Amazon RDS Read Replicas provide scalable read-heavy workloads with data transfer charges only when replicating across different AWS regions, not within the same region or AZ.

**Question 9**

**Question:** An engineering team wants to examine the feasibility of the user data feature of Amazon EC2 for an upcoming project. Which of the following are true about the Amazon EC2 user data configuration? (Select two)

**Correct Options:**

1. By default, scripts entered as user data are executed with root user privileges.
2. By default, user data runs only during the boot cycle when you first launch an instance.

**Explanation:**

1. User Data is used for automated configuration tasks and script execution after instance starts.
2. User Data scripts run with root privileges by default.
3. User Data runs during the initial boot cycle by default but can be configured to run on every restart.

**Incorrect Options:**

1. By default, user data is executed every time an Amazon EC2 instance is restarted.
   - Explanation: This is not the default behavior but can be configured.
2. When an instance is running, you can update user data by using root user credentials.
   - Explanation: User data cannot be changed while the instance is running, only viewed.
3. By default, scripts entered as user data do not have root user privileges for executing.
   - Explanation: User data scripts do have root privileges by default.

**Conclusion:**

Amazon EC2 user data allows for initial configuration tasks with scripts running as root by default during the first boot cycle, providing flexibility for automated setup and management.

**Question 10**

**Question:** The engineering team at a logistics company has noticed that the Auto Scaling group (ASG) is not terminating an unhealthy Amazon EC2 instance. As a Solutions Architect, which of the following options would you suggest to troubleshoot the issue? (Select three)

**Correct Options:**

1. The health check grace period for the instance has not expired.
2. The instance may be in Impaired status.
3. The instance has failed the Elastic Load Balancing (ELB) health check status.

**Explanation:**

1. ASG does not terminate instances until the health check grace period expires.
2. ASG waits for instances in Impaired status to recover before termination.
3. ELB health checks must be properly configured to terminate unhealthy instances.

**Incorrect Options:**

1. The Amazon EC2 instance could be a spot instance type, which cannot be terminated by the Auto Scaling group (ASG).
   - Explanation: ASG can terminate spot instances when necessary.

2. A user might have updated the configuration of the Auto Scaling group (ASG) and increased the minimum number of instances forcing ASG to keep all instances alive.
    - Explanation: Configuration changes would result in launching new instances, not keeping unhealthy ones alive.
3. A custom health check might have failed. The Auto Scaling group (ASG) does not terminate instances that are set unhealthy by custom checks.
    - Explanation: Custom health checks can trigger instance termination if configured.

**Conclusion:**

Auto Scaling group issues with terminating unhealthy instances can often be traced to health check configurations and grace periods, ensuring instances are only terminated when appropriate conditions are met.

**Question 11**

**Question:** A big-data consulting firm is working on a client engagement where the extract, transform, and load (ETL) workloads are currently handled via a Hadoop cluster deployed in the on-premises data center. The client wants to migrate their ETL workloads to AWS Cloud. The AWS Cloud solution needs to be highly available with about 50 Amazon Elastic Compute Cloud (Amazon EC2) instances per Availability Zone (AZ). As a solutions architect, which of the following Amazon EC2 placement groups would you recommend for handling the distributed ETL workload?

**Correct Option:**

Partition placement group

**Explanation:**

1. Partition placement groups spread instances across logical partitions to prevent shared underlying hardware failures.
2. Ideal for large distributed and replicated workloads such as Hadoop, Cassandra, and Kafka.

**Incorrect Options:**

1. Cluster placement group
    - Explanation: Designed for low-latency, high-throughput workloads, not suitable for distributed workloads.
2. Spread placement group
    - Explanation: Used to reduce correlated failures by spreading instances across distinct hardware, but not optimal for large distributed workloads.
3. Both Spread placement group and Partition placement group
    - Explanation: Spread placement group is not suited for large distributed workloads.

**Conclusion:**

Partition placement groups provide fault tolerance by spreading instances across partitions, making them ideal for handling large distributed ETL workloads in the AWS Cloud.

**Question 12**

**Question:** Which of the following IAM policies provides read-only access to the Amazon S3 bucket mybucket and its content?

**Correct Option:**

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:ListBucket"
      ],
      "Resource":"arn:aws:s3:::mybucket"
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:GetObject"
      ],
```

```
      "Resource":"arn:aws:s3:::mybucket/*"
    }
  ]
}
```

**Explanation:**

1. **Policy Actions and Resources:**
   - s3:ListBucket allows listing the bucket. Applied to the bucket itself.
   - s3:GetObject allows reading objects within the bucket. Applied to objects.
2. **Resource Specification:**
   - The ListBucket action applies to the bucket arn:aws:s3:::mybucket.
   - The GetObject action applies to all objects within the bucket, arn:aws:s3:::mybucket/*.

**Incorrect Options:**

| | | |
|---|---|---|
| { "Version":"2012-10-17", "Statement":[ { "Effect":"Allow", "Action":[ "s3:ListBucket" ], "Resource":"arn:aws:s3:::mybucket/*" }, { "Effect":"Allow", "Action":[ "s3:GetObject" ], "Resource":"arn:aws:s3:::mybucket" } ] } This option is incorrect as it provides listing access only to the bucket contents. | { "Version":"2012-10-17", "Statement":[ { "Effect":"Allow", "Action":[ "s3:ListBucket", "s3:GetObject" ], "Resource":"arn:aws:s3:::mybucket/*" } ] } This option is incorrect as it provides read-only access only to the objects within the bucket and it does not provide listBucket permissions to the bucket itself. | { "Version":"2012-10-17", "Statement":[ { "Effect":"Allow", "Action":[ "s3:ListBucket", "s3:GetObject" ], "Resource":"arn:aws:s3:::mybucket" } ] } This option is incorrect as it provides read-only access only to the bucket, not its contents. |

1. Policies that only grant s3:GetObject or s3:ListBucket incorrectly apply these permissions or miss one of the required actions.
2. Policies that do not differentiate between bucket-level and object-level permissions.

**Conclusion:**

The correct policy provides both listing and reading capabilities, differentiating between bucket-level and object-level permissions as required for full read-only access to the bucket and its contents.

**Question 13**

**Question:** A social photo-sharing web application hosted on Amazon EC2 instances behind an Application Load Balancer needs secure access to Amazon S3 and Amazon DynamoDB. What is the most secure option?

**Correct Option:**

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

**Explanation:**

1. **IAM Role Benefits:**
   - Provides temporary security credentials to the EC2 instance.
   - Removes the need for hard-coded credentials, enhancing security.
2. **How It Works:**
   - IAM roles manage temporary credentials for applications on EC2.
   - The role is specified during instance launch, providing necessary permissions.

**Incorrect Options:**

1. **Storing Credentials on EC2:** Involves security risks due to potential exposure of credentials.
2. **Custom Encryption and CLI Configuration:** Adds complexity and security risks by managing credentials manually.

**Conclusion:**

Attaching an IAM role to the EC2 instance is the most secure and efficient way to grant necessary permissions to access AWS resources without managing long-term credentials.

**Question 14**

**Question:** A financial services company needs a log processing model for various log files that can be processed serverlessly and stored for analytics. What AWS service should be used?

**Correct Option:**

Amazon Kinesis Data Firehose

**Explanation:**

1. **Amazon Kinesis Data Firehose:**
   - Fully managed service for loading streaming data into data lakes, data stores, and analytics services.
   - Automatically scales to match throughput and requires no ongoing administration.
2. **Capabilities:**
   - Captures, transforms, and loads streaming data into Amazon S3, Redshift, Elasticsearch, and Splunk.
   - Enables near real-time analytics with existing BI tools.

**Incorrect Options:**

1. **Kinesis Data Streams:** Requires manual management of shards.
2. **Amazon EMR:** Involves managing underlying infrastructure.
3. **AWS Lambda:** Not suitable for production-grade serverless log analytics.

**Conclusion:**

Amazon Kinesis Data Firehose provides a scalable, managed solution for processing and storing log data serverlessly, fitting the company's requirements.

**Question 15**

**Question:** Multiple AWS accounts within a single AWS Region need to ensure all EC2 instances can communicate privately. What is the most cost-effective solution?

**Correct Option:**

Create a VPC in an account and share one or more of its subnets with the other accounts using AWS Resource Access Manager (RAM).

**Explanation:**

1. **AWS RAM:**
   - Enables sharing of AWS resources securely with any AWS account.
   - Allows sharing of subnets, eliminating the need for duplicate resources and reducing costs.
2. **Resource Sharing:**
   - Creates a central VPC with shared subnets.
   - Allows EC2 instances from different accounts to communicate within the same VPC.

**Incorrect Options:**

1. **Private Link:** Meant for private connections between services, not for inter-VPC communication.
2. **VPC Peering:** Complex to manage as the number of VPCs increases.
3. **Transit Gateway:** Effective but more expensive compared to using RAM.

**Conclusion:**

Using AWS Resource Access Manager to share subnets within a central VPC allows for cost-effective and secure private communication among EC2 instances across multiple accounts.

**Question 16**

**Question:** Upon a security review of your AWS account, an AWS consultant has found that a few Amazon RDS databases are unencrypted. As a Solutions Architect, what steps must be taken to encrypt the Amazon RDS databases?

**Correct Option:**

Take a snapshot of the database, copy it as an encrypted snapshot, and restore a database from the encrypted snapshot. Terminate the previous database.

**Explanation:**

1. **Amazon RDS Encryption:**
   - Encrypts data at rest, including automated backups, read replicas, and snapshots.
2. **Process to Encrypt Existing Unencrypted RDS:**
   - Create a snapshot of the unencrypted database.
   - Copy the snapshot with encryption enabled.
   - Restore the database from the encrypted snapshot.
   - Terminate the previous unencrypted database.

**Incorrect Options:**

1. **Create a Read Replica and Encrypt:** Incorrect because read replicas cannot be encrypted if the master is not encrypted.
2. **Enable Encryption Directly:** Not possible after the database is created.
3. **Enable Multi-AZ and Encrypt:** Multi-AZ is for high availability, not encryption.

**Conclusion:** AWS RDS does not support enabling encryption on existing unencrypted instances directly. The workaround involves creating and restoring from encrypted snapshots.

**Question 17**

**Question:** A social media application is hosted on an Amazon EC2 fleet running behind an Application Load Balancer. The application traffic is fronted by an Amazon CloudFront distribution. The engineering team wants to decouple the user authentication process for the application so that the application servers can just focus on the business logic.

**Correct Option:**

Use Amazon Cognito Authentication via Cognito User Pools for your Application Load Balancer.

**Explanation:**

1. **Amazon Cognito User Pools:**
   - Provides sign-up and sign-in services.
   - Can integrate with ALB to authenticate users.
2. **Decoupling Authentication:**
   - Offloads authentication from application servers.
   - Allows servers to focus on business logic.

**Incorrect Options:**

1. **Cognito Identity Pools for ALB:** Incorrect because Identity Pools are for federated identities, not direct user authentication.
2. **Cognito Identity Pools for CloudFront:** Incorrect as the primary need is for ALB.
3. **Cognito User Pools for CloudFront:** Misaligned with the need for ALB integration.

**Conclusion:** Cognito User Pools are ideal for decoupling authentication processes, allowing ALB to manage authentication seamlessly.

**Question 18**

**Question:** An IT company wants to optimize the costs incurred on its fleet of 100 Amazon EC2 instances for the next year. Based on historical analyses, the engineering team observed that 70 of these instances handle the compute services of its flagship application and need to be always available. The other 30 instances are used to handle batch jobs that can afford a delay in processing.

**Correct Option:**

Purchase 70 reserved instances (RIs) and 30 spot instances.

**Explanation:**

1. **Reserved Instances (RIs):**
   - Suitable for predictable workloads.
   - Provide cost savings for always-on instances.

2. **Spot Instances:**
    - Suitable for flexible workloads like batch jobs.
    - Offer significant cost savings.

**Incorrect Options:**

1. **70 On-Demand and 30 Spot:** Costlier than RIs.
2. **70 On-Demand and 30 RIs:** Suboptimal for cost savings.
3. **70 RIs and 30 On-Demand:** More expensive than using spot instances for batch jobs.

**Conclusion:** Combining RIs for predictable workloads and spot instances for flexible workloads offers optimal cost savings.

**Question 19**

**Question:** A company is developing a global healthcare application that requires the least possible latency for database read/write operations from users in several geographies across the world. The company has hired you as an AWS Certified Solutions Architect Associate to build a solution using Amazon Aurora that offers an effective recovery point objective (RPO) of seconds and a recovery time objective (RTO) of a minute.

**Correct Option:**

Set up an Amazon Aurora Global Database cluster.

**Explanation:**

1. **Amazon Aurora Global Database:**
    - Designed for globally distributed applications.
    - Offers low-latency read/write operations.
    - Provides RPO of seconds and RTO of less than a minute.

**Incorrect Options:**

1. **Aurora Serverless:** Works within a single region.
2. **Aurora Provisioned:** Limited to a single region.
3. **Aurora Multi-Master:** Not available for global setups.

**Conclusion:** Aurora Global Database is tailored for applications requiring global distribution and minimal latency.

**Question 20**

**Question:** An IT company is working on client engagement to build a real-time data analytics tool for the Internet of Things (IoT) data. The IoT data is funneled into Amazon Kinesis Data Streams which further acts as the source of a delivery stream for Amazon Kinesis Firehose. The engineering team has now configured a Kinesis Agent to send IoT data from another set of devices to the same Amazon Kinesis Firehose delivery stream. They noticed that data is not reaching Kinesis Firehose as expected. As a solutions architect, which of the following options would you attribute as the MOST plausible root cause behind this issue?

**Correct Option:**

Kinesis Agent cannot write to Amazon Kinesis Firehose for which the delivery stream source is already set as Amazon Kinesis Data Streams.

**Explanation:**

1. **Amazon Kinesis Data Firehose:**
    - Fully managed service for loading streaming data.
    - Kinesis Agent cannot write directly if the source is set to Kinesis Data Streams.

**Incorrect Options:**

1. **Kinesis Agent Only to Data Streams:** Incorrect as Kinesis Agent can write to both Data Streams and Firehose.
2. **Firehose Reached Limit:** Firehose auto-scales, no manual scaling needed.
3. **Configuration Error:** Distractor option, not the root cause.

**Conclusion:** Properly configure sources for Firehose delivery streams to ensure data flow.

**Question 21**

**Question:** A financial services company wants to store confidential data in Amazon S3 and it needs to meet the following data security and compliance norms:

1. Encryption key usage must be logged for auditing purposes.
2. Encryption Keys must be rotated every year.

3. The data must be encrypted at rest.

**Correct Option:**

Server-side encryption with AWS Key Management Service (AWS KMS) keys (SSE-KMS) with automatic key rotation.

**Explanation:**

1. **AWS KMS Keys:**
   - Supports automatic key rotation.
   - Logs key usage for auditing.
   - Ensures data encryption at rest.

**Incorrect Options:**

1. **SSE-S3 with Automatic Rotation:** Lacks detailed key usage logging.
2. **SSE-C with Automatic Rotation:** Requires manual management of customer-provided keys.
3. **SSE-KMS with Manual Rotation:** Less operationally efficient.

**Conclusion:** SSE-KMS with automatic key rotation best meets security and compliance requirements.

**Question 22**

**Question:** A junior DevOps engineer wants to change the default configuration for Amazon EBS volume termination. By default, the root volume of an Amazon EC2 instance for an EBS-backed AMI is deleted when the instance terminates. Which option below helps change this default behavior to ensure that the volume persists even after the instance terminates?

**Correct Option:**

Set the DeleteOnTermination attribute to false.

**Explanation:**

1. **Amazon EBS Volume Termination:**
   - Default behavior deletes the root volume on instance termination.
   - Modify DeleteOnTermination attribute to false to retain the volume.

**Incorrect Options:**

1. **TerminateOnDelete True/False:** Non-existent attribute.
2. **DeleteOnTermination True:** Ensures volume deletion, opposite of the requirement.

**Conclusion:** Use the DeleteOnTermination attribute to control volume persistence.

**Question 23**

**Question:** An IT company has built a solution wherein an Amazon Redshift cluster writes data to an Amazon S3 bucket belonging to a different AWS account. However, it is found that the files created in the Amazon S3 bucket using the UNLOAD command from the Amazon Redshift cluster are not even accessible to the Amazon S3 bucket owner.

**Correct Option:**

Use bucket policies in Amazon S3.

**Explanation:**

1. **Bucket Policies:**
   - Manage permissions for S3 buckets.
   - Ensure access for different accounts.

**Incorrect Options:**

1. **IAM Policies:** Only manage permissions within the same account.
2. **Access Control Lists (ACLs):** Less flexible than bucket policies.
3. **Security Groups:** Not applicable to S3.

**Conclusion:** Use bucket policies to manage cross-account access in Amazon S3.

**Question 24**

**Question:** An IT company has launched a new mobile gaming application that users are adopting rapidly. The company uses Amazon RDS MySQL as the database. The engineering team wants an urgent solution to this issue where the rapidly increasing workload might exceed the available database storage.

**Correct Option:**

Enable storage auto-scaling for Amazon RDS MySQL.

**Explanation:**

1. **Storage Auto-Scaling:**
   - Automatically adjusts storage size.
   - Ideal for handling unpredictable workload growth.

**Incorrect Options:**

1. **Migrate to DynamoDB:** High development effort.
2. **Create Read Replica:** Does not solve storage issues.
3. **Migrate to Aurora:** High operational effort.

**Conclusion:** Auto-scaling provides a seamless and low-effort solution to handle increased storage demands.

**Question 25**

**Question:** A developer needs to implement an AWS Lambda function in AWS account A that accesses an Amazon S3 bucket in AWS account B.

**Correct Option:**

Create an IAM role for the AWS Lambda function that grants access to the Amazon S3 bucket. Set the IAM role as the AWS Lambda function's execution role. Make sure that the bucket policy also grants access to the AWS Lambda function's execution role.

**Explanation:**

1. **Cross-Account Access:**
   - IAM role and bucket policy must be configured for cross-account access.
   - Role should be assumed by Lambda function.

**Incorrect Options:**

1. **Use Identity Federation:** Not required for Lambda-S3 access.
2. **Public Bucket:** Security risk and not recommended.
3. **Single IAM Role Configuration:** Insufficient for cross-account access.

**Conclusion:** Properly configured IAM roles and bucket policies ensure secure cross-account access.

**Question 26**

**Question:** An IT company wants to optimize the costs incurred on its fleet of 100 Amazon EC2 instances for the next year. Based on historical analyses, the engineering team observed that 70 of these instances handle the compute services of its flagship application and need to be always available. The other 30 instances are used to handle batch jobs that can afford a delay in processing.

**Correct Option:**

Purchase 70 reserved instances (RIs) and 30 spot instances.

**Explanation:**

1. **Reserved Instances (RIs):** Suitable for predictable workloads, providing cost savings.
2. **Spot Instances:** Suitable for flexible workloads like batch jobs, offering significant cost savings.

**Incorrect Options:**

1. **70 On-Demand and 30 Spot:** More expensive than RIs for always-on instances.
2. **70 On-Demand and 30 RIs:** Suboptimal for cost savings.

**Conclusion:** Combining RIs for predictable workloads and spot instances for flexible workloads offers optimal cost savings.

**Question 27**

**Question:** A company has recently launched a new mobile gaming application that the users are adopting rapidly. The company uses Amazon RDS MySQL as the database. The engineering team wants an urgent solution to this issue where the rapidly increasing workload might exceed the available database storage.

**Correct Option:**

Enable storage auto-scaling for Amazon RDS MySQL.

**Explanation:**

1. **Storage Auto-Scaling:** Automatically adjusts storage size.
2. **Solution:** Ideal for handling unpredictable workload growth.

**Incorrect Options:**

1. **Migrate to DynamoDB:** High development effort.
2. **Create Read Replica:** Does not solve storage issues.
3. **Migrate to Aurora:** High operational effort.

**Conclusion:** Auto-scaling provides a seamless and low-effort solution to handle increased storage demands.

**Question 28**

**Question:** A company is developing a global healthcare application that requires the least possible latency for database read/write operations from users in several geographies across the world. The company has hired you as an AWS Certified Solutions Architect Associate to build a solution using Amazon Aurora that offers an effective recovery point objective (RPO) of seconds and a recovery time objective (RTO) of a minute.

**Correct Option:**

Set up an Amazon Aurora Global Database cluster.

**Explanation:**

1. **Amazon Aurora Global Database:**
   - Designed for globally distributed applications.
   - Offers low-latency read/write operations.
   - Provides RPO of seconds and RTO of less than a minute.

**Incorrect Options:**

1. **Aurora Serverless:** Works within a single region.
2. **Aurora Provisioned:** Limited to a single region.
3. **Aurora Multi-Master:** Not available for global setups.

**Conclusion:** Aurora Global Database is tailored for applications requiring global distribution and minimal latency.

**Question 29**

**Question:** You would like to mount a network file system on Linux instances, where files will be stored and accessed frequently at first, and then infrequently. What solution is the MOST cost-effective?

**Correct Option:**

Amazon EFS Infrequent Access.

**Explanation:**

1. **Amazon EFS Infrequent Access (IA):**
   - Provides cost-optimized storage for files not accessed daily.
   - Offers up to 92% lower storage prices compared to EFS Standard.

**Incorrect Options:**

1. **Amazon S3 Intelligent Tiering:** Not suitable for mounting as a network file system.
2. **Amazon S3 Glacier Deep Archive:** Designed for data archiving, not frequent access.
3. **Amazon FSx for Lustre:** Expensive and suited for high-performance computing.

**Conclusion:** EFS IA provides a cost-effective solution for mounting network file systems with infrequent access patterns.

**Question 30**

**Question:** What does this IAM policy do?

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "Mystery Policy",
```

```
"Action": [
 "ec2:RunInstances"
],
"Effect": "Allow",
"Resource": "*",
"Condition": {
 "StringEquals": {
  "aws:RequestedRegion": "eu-west-1"
 }} }]}
```

**Correct Option:**

It allows running Amazon EC2 instances only in the eu-west-1 region, and the API call can be made from anywhere in the world.

**Explanation:**

1. **Policy Analysis:**
   - Action: Allows ec2:RunInstances.
   - Condition: Restricts the action to the eu-west-1 region.

**Incorrect Options:**

1. **Run Instances Anywhere but eu-west-1:** Contradicts the condition in the policy.
2. **Run Instances in any Region from eu-west-1:** Misinterprets the aws:RequestedRegion condition.
3. **Run Instances in eu-west-1 from eu-west-1:** Incorrect interpretation of condition scope.

**Conclusion:** The policy specifically allows running instances in eu-west-1, regardless of the API call's origin.

**Question 31**

**Question:** A financial services company wants to store confidential data in Amazon S3 and it needs to meet the following data security and compliance norms:

1. Encryption key usage must be logged for auditing purposes.
2. Encryption Keys must be rotated every year.
3. The data must be encrypted at rest.

**Correct Option:**

Server-side encryption with AWS Key Management Service (AWS KMS) keys (SSE-KMS) with automatic key rotation

**Explanation:**

1. **Server-side encryption:** Encrypts data at the destination by the application or service that receives it.
2. **AWS KMS Keys:**
   - Provides secure key management at scale.
   - Supports automatic key rotation.
   - Logs key usage for auditing purposes.
   - Encrypts data at rest.

**Incorrect Options:**

1. **SSE-KMS with manual key rotation:** Less operationally efficient due to the manual process.
2. **SSE-S3 with automatic key rotation:** Cannot log the usage of the encryption key for auditing purposes.
3. **SSE-C with automatic key rotation:** Requires developing an underlying solution to automate key rotation.

**Conclusion:**

Using AWS KMS keys with automatic key rotation for server-side encryption ensures data is encrypted at rest, key usage is logged for auditing, and keys are rotated automatically, meeting all compliance and security norms efficiently.

**Question 32**

**Question:** A retail company wants to roll out and test a blue-green deployment for its global application in the next 48 hours. Most of the customers use mobile phones prone to DNS caching. What would you recommend to test the deployment on as many users as possible in the given time frame?

**Correct Option:**

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

**Explanation:**

1. **AWS Global Accelerator:**
   - Provides two static anycast IP addresses as a fixed entry point.
   - Uses endpoint weights and traffic dials to control traffic distribution.
   - Effective within seconds, bypassing DNS caching issues.

**Incorrect Options:**

1. **Amazon Route 53 weighted routing:** Subject to DNS caching, making it unsuitable for quick traffic transition.
2. **Elastic Load Balancing (ELB):** Cannot distribute traffic globally across regions.
3. **AWS CodeDeploy:** Not meant for traffic distribution, only for deployment processes.

**Conclusion:**

AWS Global Accelerator allows for rapid, controlled traffic distribution, essential for blue-green deployments requiring quick transition without being affected by DNS caching.

**Question 33**

**Question:** A startup has a two-tier architecture with web servers in public subnets and MSSQL database instances in private subnets. Which configuration would be the MOST secure?

**Correct Options:**

1. For security group A: Add an inbound rule that allows traffic from all sources on port 443. Add an outbound rule with the destination as security group B on port 1433.
2. For security group B: Add an inbound rule that allows traffic only from security group A on port 1433.

**Explanation:**

1. **Security Group A:**
   - Inbound rule allows HTTPS traffic from all sources.
   - Outbound rule restricts traffic to MSSQL servers in security group B on port 1433.
2. **Security Group B:**
   - Inbound rule restricts traffic to only come from security group A on port 1433.

**Incorrect Options:**

1. Allowing outbound traffic on port 443 in security group A.
2. Allowing inbound traffic from all sources on port 1433 in security group B.
3. Allowing traffic on incorrect ports.

**Conclusion:**

Proper security group configurations ensure that web servers only communicate with database servers on specific ports, enhancing security by limiting unnecessary access.

**Question 34**

**Question:** A company needs built-in user management for authorizing API calls within Amazon API Gateway. What is the best solution?

**Correct Option:**

Use Amazon Cognito User Pools

**Explanation:**

1. **Amazon Cognito User Pools:**
   - Provides built-in user management.
   - Supports sign-up, sign-in, and user directory management.
   - Integrates with external identity providers.
   - Offers security features like MFA, account takeover protection, and more.

**Incorrect Options:**

1. **AWS IAM authorization:** Suitable for internal users with AWS credentials.
2. **AWS Lambda authorizer:** Requires custom validation logic.
3. **Amazon Cognito Identity Pools:** Used for providing AWS credentials to users, not for direct user management.

**Conclusion:**

Amazon Cognito User Pools provide comprehensive user management and integration with API Gateway, making it the best solution for managing user authentication and authorization.

**Question 35**

**Question:** An IT company faces performance issues with Amazon RDS for MySQL despite using Read Replicas. What is the most cost-effective and high-performance solution?

**Correct Option:**

Use Amazon Aurora Global Database to enable fast local reads with low latency in each region.

**Explanation:**

1. **Amazon Aurora Global Database:**
   - Designed for globally distributed applications.
   - Provides low-latency reads with data replicated across multiple regions.
   - Ensures high performance and availability.

**Incorrect Options:**

1. **Amazon DynamoDB Global Tables:** NoSQL database, not compatible with relational database schema.
2. **Amazon Redshift clusters:** Not suited for transactional relational databases.
3. **Amazon EC2 instances with MySQL:** High maintenance and complexity.

**Conclusion:**

Amazon Aurora Global Database offers the best performance and cost-efficiency for relational databases, addressing global performance issues effectively.

**Question 36**

**Question:** A research group wants to minimize the application bootstrap time on an Amazon EC2 instance. What solution should be recommended?

**Correct Option:**

Use Amazon EC2 Instance Hibernate

**Explanation:**

1. **Amazon EC2 Instance Hibernate:**
   - Saves the instance's RAM contents to the EBS root volume.
   - Restores the instance to its previous state, reducing startup time.
   - Retains the instance ID and attached data volumes.

**Incorrect Options:**

1. **Amazon EC2 User-Data:** Executes scripts at launch but does not reduce application startup time.
2. **Amazon EC2 Meta-Data:** Provides configuration details but does not affect startup time.
3. **Amazon Machine Image (AMI):** Does not address the need to reduce startup time after stopping and starting instances.

**Conclusion:**

Amazon EC2 Instance Hibernate is the optimal solution to resume instances quickly with minimal application startup time.

**Question 37**

**Question:** A healthcare solutions company needs to run applications on single-tenant hardware. What is the most cost-effective way to isolate Amazon EC2 instances to a single tenant?

**Correct Option:**

Dedicated Instances

**Explanation:**

1. **Dedicated Instances:**
   - Run on hardware dedicated to a single customer.
   - Provide physical isolation from instances in other accounts.
   - More cost-effective than Dedicated Hosts.

**Incorrect Options:**

1. **Spot Instances:** Do not meet single-tenant requirements.

2. **Dedicated Hosts:** Offer more control but are costlier.
3. **On-Demand Instances:** Do not provide hardware isolation.

**Conclusion:**

Dedicated Instances ensure single-tenant hardware isolation at a lower cost compared to Dedicated Hosts.

**Question 38**

**Question:** A systems administrator's DNS queries for a private hosted zone remain unresolved. What VPC options need to be configured?

**Correct Option:**

Enable DNS hostnames and DNS resolution for private hosted zones.

**Explanation:**

1. **DNS Hostnames:** Required for private hosted zones to resolve DNS queries.
2. **DNS Resolution:** Allows VPC DNS server to resolve DNS queries for the private hosted zone.

**Incorrect Options:**

1. **Fixing NS and SOA records:** Relevant for public hosted zones, not private.
2. **Removing overlapping namespaces:** Does not affect DNS resolution.
3. **Fixing conflicts with Resolver rules:** Does not result in unresolved queries.

**Conclusion:**

Enabling DNS hostnames and DNS resolution ensures that DNS queries for private hosted zones are resolved correctly.

**Question 39**

**Question:** A startup with customers in the US and Europe faces performance issues. What would you recommend to improve application performance?

**Correct Options:**

1. Setup another fleet of Amazon EC2 instances for the web tier in the eu-west-1 region. Enable latency routing policy in Amazon Route 53.
2. Create Amazon Aurora read replicas in the eu-west-1 region.

**Explanation:**

1. **Latency Routing Policy:**
   - Routes traffic to the region with the lowest latency.
   - Improves application performance for users in Europe.
2. **Amazon Aurora Read Replicas:**
   - Scale out reads across regions.
   - Enhance performance by reducing read latency.

**Incorrect Options:**

1. **Geolocation routing policy:** Routes traffic based on user location but does not reduce latency.
2. **Failover routing policy:** Routes traffic based on resource health, not suitable for latency reduction.
3. **Aurora Multi-AZ standby instance:** Enhances availability, not read performance.

**Conclusion:**

Using latency routing and read replicas effectively improves application performance for geographically distributed users.

**Question 40**

**Question:** How can you prevent developers from granting themselves the AdministratorAccess managed policy while allowing them to experiment with AWS Managed Policies?

**Correct Option:**

For each developer, define an IAM permission boundary that will restrict the managed policies they can attach to themselves.

**Explanation:**

1. **IAM Permission Boundary:**
   - Sets the maximum permissions an IAM entity can grant.
   - Restricts developers from attaching excessive privileges, including AdministratorAccess.

**Incorrect Options:**

1. **Service Control Policy (SCP):** Not mentioned, applicable only within AWS Organizations.
2. **IAM Policy:** Developers can remove this policy and escalate privileges.
3. **Permission Boundary on IAM Group:** Not applicable, boundaries are for roles or users only.

**Conclusion:**

IAM permission boundaries provide a secure way to control the managed policies developers can attach, preventing privilege escalation.

**Question 41**

**Question:** A company wants to improve application availability for a Supply Chain Management application with users in the US. What is the MOST resource-efficient solution?

**Correct Option:**

Deploy the web-tier Amazon EC2 instances in two Availability Zones (AZs), behind an Elastic Load Balancer. Deploy the Amazon RDS MySQL database in Multi-AZ configuration.

**Explanation:**

1. **Elastic Load Balancing:**
   - Distributes traffic across multiple targets, ensuring high availability.
   - Works within a single region across multiple AZs.
2. **Amazon RDS Multi-AZ:**
   - Enhances availability and durability.
   - Provides automatic failover to a standby instance in a different AZ.

**Incorrect Options:**

1. **Deploying in two regions:** ELB does not support cross-region distribution.
2. **Using Read Replica:** Improves scalability, not availability.
3. **Read Replica configuration for RDS:** Does not provide high availability.

**Conclusion:**

Deploying EC2 instances across AZs with Multi-AZ RDS ensures high availability and resource efficiency for users in the same region.

**Question 42**

**Question:** How can a cybersecurity company be notified via email when CPU utilization for Amazon EC2 instances breaches a certain threshold with minimal development effort?

**Correct Options:**

1. Amazon Simple Notification Service (Amazon SNS)
2. Amazon CloudWatch

**Explanation:**

1. **Amazon SNS:** Sends notifications via email or other protocols.
2. **Amazon CloudWatch:** Monitors EC2 instances and creates alarms based on metrics like CPU utilization.

**Incorrect Options:**

1. **AWS Lambda:** Executes code but not suited for monitoring EC2 metrics directly.
2. **Amazon SQS:** Message queuing service, not for direct notifications.
3. **AWS Step Functions:** Orchestrates workflows but not for monitoring EC2 metrics.

**Conclusion:**

Combining Amazon CloudWatch and Amazon SNS provides an efficient solution for monitoring EC2 metrics and sending notifications with minimal setup.

**Question 43**

**Question:** What solution reduces administrative overhead and costs while providing shared access to services required by workloads in interconnected VPCs?

**Correct Option:**

Build a shared services Amazon Virtual Private Cloud (Amazon VPC)

**Explanation:**

1. **Shared Services VPC:**
    - Centralizes common services like directory services or VPC endpoints.
    - Reduces the need to duplicate services in each VPC.
    - Lowers administrative overhead and costs.

**Incorrect Options:**

1. **Transit VPC:** Requires managing EC2-based VPN appliances, increasing costs.
2. **Fully meshed VPC Peering:** Complex to manage with limited scalability.
3. **AWS Direct Connect:** Requires physical setup and is not suitable for rapid deployment.

**Conclusion:**

A shared services VPC centralizes shared resources, streamlining management and reducing costs across multiple interconnected VPCs.

**Question 44**

**Question:** Amazon EC2 Auto Scaling needs to terminate an instance from Availability Zone (AZ) us-east-1a as it has the most number of instances among the Availability Zones (AZs) being used currently. There are 4 instances in the Availability Zone (AZ) us-east-1a as follows: Instance A has the oldest launch template, Instance B has the oldest launch configuration, Instance C has the newest launch configuration, and Instance D is closest to the next billing hour. Which of the following instances would be terminated per the default termination policy?

**Correct Option:**

Instance B

**Explanation:**

1. **Default Termination Policy:**
    - The first priority is given to any allocation strategy for On-Demand vs. Spot instances. Since no such information is provided, this criterion can be ignored.
    - The next priority is to consider any instance with the oldest launch template unless there is an instance that uses a launch configuration.
    - Instance B has the oldest launch configuration, making it the highest priority for termination according to the default policy.

**Incorrect Options:**

1. **Instance A:** It has the oldest launch template but is not prioritized over instances with launch configurations.
2. **Instance C:** It has the newest launch configuration, which is not prioritized for termination.
3. **Instance D:** Closest to the next billing hour, but this criterion is the last in the order of priority.

**Conclusion:**

The default termination policy for Amazon EC2 Auto Scaling prioritizes instances with the oldest launch configuration for termination, ensuring that newer configurations and more cost-effective instances remain active.

**Question 45**

**Question:** Your company has a monthly big data workload, running for about 2 hours, which can be efficiently distributed across multiple servers of various sizes, with a variable number of CPUs. The solution for the workload should be able to withstand server failures. Which is the MOST cost-optimal solution for this workload?

**Correct Option:**

Run the workload on a Spot Fleet

**Explanation:**

1. **Spot Fleet:**
    - A Spot Fleet selects the Spot Instance pools that meet your needs and launches Spot Instances to meet the target capacity for the fleet.
    - By default, Spot Fleets are set to maintain target capacity by launching replacement instances after Spot Instances in the fleet are terminated.
    - Spot Instances are unused Amazon EC2 instances available for less than the On-Demand price, providing significant cost savings.

**Incorrect Options:**

1. **Dedicated Hosts:** Provides single-tenant hardware but is much more expensive than Spot Instances.
2. **Spot Instances:** While cost-effective, Spot Instances alone do not offer the fleet management and replacement capabilities of Spot Fleets.
3. **Reserved Instances (RI):** Suitable for predictable, long-term workloads but not as cost-effective for a short, monthly workload.

**Conclusion:**

Running the workload on a Spot Fleet provides the most cost-effective solution with the ability to maintain target capacity and handle server failures, making it ideal for short, flexible workloads that can tolerate interruptions.

**Question 46**

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

**Correct Option:**

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

**Explanation:**

1. **AWS DataSync:** Automates, accelerates, and simplifies copying large amounts of data between on-premises storage and AWS storage services.
2. **PrivateLink Interface VPC Endpoint:** Allows private connection to AWS services within a VPC using private IP addresses.
3. **Scheduled Task:** Ensures regular and automated transfer of files.

**Incorrect Options:**

1. **VPC Peering Endpoint:** VPC peering does not support data transfer over Direct Connect.
2. **Public VIF with S3:** Involves unnecessary complexity and is not operationally efficient.
3. **Gateway Endpoint with S3:** Not suitable for direct data transfer from on-premises to AWS storage.

**Conclusion:**

Using AWS DataSync with a PrivateLink interface VPC endpoint ensures efficient and secure data transfer from on-premises to Amazon EFS, automating the process with scheduled tasks.

**Question 47**

**Question:** A media company is migrating its flagship application from its on-premises data center to AWS for improving the application's read-scaling capability as well as its availability. The existing architecture leverages a Microsoft SQL Server database that sees a heavy read load. The engineering team does a full copy of the production database at the start of the business day to populate a dev database. During this period, application users face high latency leading to a bad user experience.

**Correct Option:**

Leverage Amazon Aurora MySQL with Multi-AZ Aurora Replicas and create the dev database by restoring from the automated backups of Amazon Aurora.

**Explanation:**

1. **Amazon Aurora:** A fully managed relational database compatible with MySQL and PostgreSQL.
2. **Multi-AZ Aurora Replicas:** Improve read-scaling and availability.
3. **Automated Backups:** Continuous and incremental, allowing quick restoration without impacting performance.

**Incorrect Options:**

1. **Restore via mysqldump:** Adds significant load on the primary database.
2. **Use Standby Instance:** Standby instances are for failover, not for dev databases.
3. **RDS for SQL Server with Read Replicas:** Read replicas are for read-scaling, not for dev database use.

**Conclusion:**

Amazon Aurora with Multi-AZ Aurora Replicas and automated backups ensures high availability, read-scaling, and efficient creation of dev databases without impacting user experience.

**Question 48**

**Question:** To improve the performance and security of the application, the engineering team at a company has created an Amazon CloudFront distribution with an Application Load Balancer as the custom origin. The team has also set up an AWS Web Application Firewall (AWS WAF) with Amazon CloudFront distribution. The security team at the company has noticed a surge in malicious attacks from a specific IP address to steal sensitive data stored on the Amazon EC2 instances.

**Correct Option:** Create an IP match condition in the AWS WAF to block the malicious IP address.

**Explanation:**

1. **AWS WAF:** Protects web applications by filtering and monitoring HTTP and HTTPS requests.
2. **IP Match Condition:** Blocks traffic from specific IP addresses.

**Incorrect Options:**

1. **Network ACL Deny Rule:** Network ACLs are associated with subnets, not instances.
2. **Security Group Deny Rule:** Security groups do not support deny rules.
3. **AWS Support Ticket:** Security is the responsibility of the user, not AWS support.

**Conclusion:**

Using AWS WAF with an IP match condition provides a scalable and efficient way to block malicious IP addresses, enhancing application security.

**Question 49**

**Question:** A retail company wants to share sensitive accounting data that is stored in an Amazon RDS database instance with an external auditor. The auditor has its own AWS account and needs its own copy of the database.

**Correct Option:**

Create an encrypted snapshot of the database, share the snapshot, and allow access to the AWS Key Management Service (AWS KMS) encryption key.

**Explanation:**

1. **Encrypted Snapshot:** Ensures data security during sharing.
2. **KMS Key Sharing:** Allows the auditor's account to decrypt the snapshot.

**Incorrect Options:**

1. **Snapshot in S3:** Direct access to RDS snapshots in S3 is not possible.
2. **Read Replica:** Overkill for auditing purposes and does not provide a separate database copy.
3. **Export to Text Files:** Inefficient and difficult to manage.

**Conclusion:**

Creating and sharing an encrypted snapshot with access to the KMS key is a secure and efficient method for sharing sensitive data across AWS accounts.

**Question 50**

**Question:** A startup has just developed a video backup service hosted on a fleet of Amazon EC2 instances. The Amazon EC2 instances are behind an Application Load Balancer and the instances are using Amazon Elastic Block Store (Amazon EBS) Volumes for storage. The service provides authenticated users the ability to upload videos that are then saved on the EBS volume attached to a given instance. On the first day of the beta launch, users start complaining that they can see only some of the videos in their uploaded videos backup. Every time the users log into the website, they claim to see a different subset of their uploaded videos.

**Correct Options:**

1. **Write a one-time job to copy the videos from all Amazon EBS volumes to Amazon S3 and then modify the application to use Amazon S3 standard for storing the videos.**
2. **Mount Amazon Elastic File System (Amazon EFS) on all Amazon EC2 instances. Write a one-time job to copy the videos from all Amazon EBS volumes to Amazon EFS. Modify the application to use Amazon EFS for storing the videos.**

**Explanation:**

1. **Amazon S3:** Provides scalable object storage, ideal for static content like videos.
2. **Amazon EFS:** Offers scalable and elastic file storage, accessible by multiple EC2 instances simultaneously.

**Incorrect Options:**

1. **S3 Glacier Deep Archive:** Not suitable for frequently accessed content.
2. **Amazon RDS:** Not designed for storing videos.
3. **Amazon DynamoDB:** Not suitable for storing video files.

**Conclusion:**

Using Amazon S3 or Amazon EFS ensures centralized storage accessible by all EC2 instances, resolving the issue of dispersed video files and providing a scalable solution.

**Question 51**

**Question:** The engineering team at an e-commerce company is working on cost optimizations for Amazon Elastic Compute Cloud (Amazon EC2) instances. The team wants to manage the workload using a mix of on-demand and spot instances across multiple instance types. They would like to create an Auto Scaling group with a mix of these instances.

**Correct Option:** You can only use a launch template to provision capacity across multiple instance types using both On-Demand Instances and Spot Instances to achieve the desired scale, performance, and cost.

**Explanation:**

1. **Launch Templates:** Support multiple versions and allow provisioning of a mix of instance types using On-Demand and Spot Instances.
2. **Auto Scaling:** Efficiently manages capacity to meet demand and optimize costs.

**Incorrect Options:**

1. **Launch Configuration:** Does not support multiple instance types or mixed instance policies.
2. **Both Launch Configuration and Template:** Only launch templates support the required functionality.

**Conclusion:**

Using launch templates allows the creation of a cost-efficient and scalable Auto Scaling group with mixed instance types and purchasing options.

**Question 52**

**Question:** A weather forecast agency collects key weather metrics across multiple cities in the US and sends this data in the form of key-value pairs to AWS Cloud at a one-minute frequency.

**Correct Options:**

1. **AWS Lambda**
2. **Amazon DynamoDB**

**Explanation:**

1. **AWS Lambda:** Serverless compute service that processes data without managing servers.
2. **Amazon DynamoDB:** NoSQL database optimized for key-value pairs with high availability and performance.

**Incorrect Options:**

1. **Amazon Redshift:** Not suitable for capturing and processing key-value data.
2. **Amazon ElastiCache:** Used for caching, not long-term data storage.
3. **Amazon RDS:** Relational database not ideal for key-value pair storage.

**Conclusion:**

AWS Lambda and Amazon DynamoDB together provide a scalable, high-performance solution for processing and storing weather metrics.

**Question 53**

**Question:** A developer has configured inbound traffic for the relevant ports in both the Security Group of the Amazon EC2 instance as well as the network access control list (network ACL) of the subnet for the Amazon EC2 instance. The developer is, however, unable to connect to the service running on the Amazon EC2 instance.

**Correct Option:**

Security Groups are stateful, so allowing inbound traffic to the necessary ports enables the connection. Network access control list (network ACL) are stateless, so you must allow both inbound and outbound traffic.

**Explanation:**

1. **Security Groups:** Stateful, automatically allow return traffic.
2. **Network ACLs:** Stateless, must explicitly allow both inbound and outbound traffic.

**Incorrect Options:**

1. **Stateful ACLs:** Incorrect, ACLs are stateless.

2. **IAM Role Confusion:** Distractor, IAM roles are not related to this issue.

3. **Command Line Modification:** Irrelevant and incorrect.

**Conclusion:**

Proper configuration of network ACLs and understanding the stateful nature of security groups ensures correct connectivity to services on EC2 instances.

**Question 54**

**Question:** A big data consulting firm needs to set up a data lake on Amazon S3 for a Health-Care client. The data lake is split in raw and refined zones. For compliance reasons, the source data needs to be kept for a minimum of 5 years. The source data arrives in the raw zone and is then processed via an AWS Glue based extract, transform, and load (ETL) job into the refined zone. The business analysts run ad-hoc queries only on the data in the refined zone using Amazon Athena. The team is concerned about the cost of data storage in both the raw and refined zones as the data is increasing at a rate of 1 terabyte daily in each zone.

**Correct Options:**

1. **Setup a lifecycle policy to transition the raw zone data into Amazon S3 Glacier Deep Archive after 1 day of object creation.**
2. **Use AWS Glue ETL job to write the transformed data in the refined zone using a compressed file format.**

**Explanation:**

1. **Lifecycle Policy:** Automatically transitions infrequently accessed data to cost-effective storage.
2. **Compressed File Format:** Reduces storage costs for the refined zone by minimizing data size.

**Incorrect Options:**

1. **Delete Raw Data After 1 Day:** Violates compliance requirements.
2. **Transition Refined Data to Glacier Deep Archive:** Refined data is needed for ad-hoc queries and should be readily accessible.
3. **Use CSV Format:** Less efficient than compressed formats, leading to higher storage costs.

**Conclusion:**

Using lifecycle policies for raw data and compressing refined data optimizes storage costs while meeting compliance and accessibility requirements.

**Question 55**

**Question:** A Hollywood studio is planning a series of promotional events leading up to the launch of the trailer of its next sci-fi thriller. The executives at the studio want to create a static website with lots of animations in line with the theme of the movie. The studio has hired you as a solutions architect to build a scalable serverless solution.

**Correct Option:** Build the website as a static website hosted on Amazon S3. Create an Amazon CloudFront distribution with Amazon S3 as the origin. Use Amazon Route 53 to create an alias record that points to your Amazon CloudFront distribution.

**Explanation:**

1. **Amazon S3:** Ideal for hosting static websites.
2. **Amazon CloudFront:** Distributes content globally with low latency.
3. **Amazon Route 53:** Manages DNS and supports alias records for CloudFront distributions.

**Incorrect Options:**

1. **Host on Lambda:** Lambda is not suitable for hosting static websites.
2. **Host on EC2 or On-Premises:** Not serverless and less scalable.

**Conclusion:**

Using Amazon S3, CloudFront, and Route 53 provides a cost-effective, scalable, and serverless solution for hosting a static website with global reach and high performance.

**Question 56**

**Question:** A company has many Amazon Virtual Private Cloud (Amazon VPC) in various accounts, that need to be connected in a star network with one another and connected with on-premises networks through AWS Direct Connect. What do you recommend?

**Correct Option:**

AWS Transit Gateway

**Explanation:**

1. **AWS Transit Gateway:**
   - Acts as a central hub to connect multiple VPCs and on-premises networks.
   - Simplifies network management by reducing the number of connections required.
   - Provides high availability and scalability.

**Incorrect Options:**

1. **VPC Peering Connection:**

- Only connects two VPCs, not transitive, requiring multiple connections for a star network.

2. **Virtual Private Gateway (VGW):**
   - Endpoint on the VPC side of a VPN connection, not suitable for connecting multiple VPCs.
3. **AWS PrivateLink:**
   - Used for private connectivity between VPCs and AWS services, not for connecting multiple VPCs in a star network.

**Conclusion:**

AWS Transit Gateway is the optimal solution for connecting multiple VPCs and on-premises networks in a star network, simplifying management and ensuring high availability.

**Question 57**

**Question:** An HTTP application is deployed on an Auto Scaling Group, is accessible from an Application Load Balancer (ALB) that provides HTTPS termination, and accesses a PostgreSQL database managed by Amazon RDS. How should you configure the security groups? (Select three)

**Correct Options:**

1. The security group of Amazon RDS should have an inbound rule from the security group of the Amazon EC2 instances in the Auto Scaling group on port 5432.
2. The security group of the Amazon EC2 instances should have an inbound rule from the security group of the Application Load Balancer on port 80.
3. The security group of the Application Load Balancer should have an inbound rule from anywhere on port 443.

**Explanation:**

1. **Security Groups:**
   - Control traffic to instances.
   - Ensure only required traffic is allowed.
2. **Port Configurations:**
   - Port 5432: PostgreSQL database.
   - Port 80: HTTP traffic from ALB to EC2 instances.
   - Port 443: HTTPS traffic to ALB.

**Incorrect Options:**

1. **Inbound Rule on ALB from Anywhere on Port 80:** Incorrect because HTTPS traffic is on port 443.
2. **Inbound Rule from RDS to EC2 on Port 5432:** Misconfigured, should be the other way around.
3. **Inbound Rule from EC2 to RDS on Port 80:** Incorrect, as PostgreSQL uses port 5432.

**Conclusion:**

Properly configuring security groups ensures secure and correct traffic flow between ALB, EC2 instances, and RDS.

**Question 58**

**Question:** A financial services company has developed its flagship application on AWS Cloud with data security requirements such that the encryption key must be stored in a custom application running on-premises. The company wants to offload the data storage as well as the encryption process to Amazon S3 but continue to use the existing encryption key. Which of the following Amazon S3 encryption options allows the company to leverage Amazon S3 for storing data with given constraints?

**Correct Option:**

Server-Side Encryption with Customer-Provided Keys (SSE-C)

**Explanation:**

1. **SSE-C:**
   - Allows using custom encryption keys managed outside AWS.
   - S3 manages encryption and decryption but uses provided keys.
   - Meets the requirement to use an on-premises key.

**Incorrect Options:**

1. **SSE-S3:** Uses AWS-managed keys, not suitable for custom key requirements.
2. **SSE-KMS:** Uses AWS KMS for key management, not on-premises keys.
3. **Client-Side Encryption:** Requires managing encryption/decryption outside of S3, not offloading the encryption process to S3.

**Conclusion:**

SSE-C allows using custom keys managed on-premises while offloading encryption/decryption to S3, meeting the company's security requirements.

**Question 59**

**Question:** You are establishing a monitoring solution for desktop systems that will be sending telemetry data into AWS every 1 minute. Data for each system must be processed in order, independently, and you would like to scale the number of consumers to be possibly equal to the number of desktop systems being monitored. What do you recommend?

**Correct Option:**

Use an Amazon Simple Queue Service (Amazon SQS) FIFO (First-In-First-Out) queue, and make sure the telemetry data is sent with a Group ID attribute representing the value of the Desktop ID.

**Explanation:**

1. **Amazon SQS FIFO:**
   - Ensures messages are processed in order.
   - Group ID allows scaling consumers to handle data independently for each desktop system.
   - Guarantees exactly-once processing.

**Incorrect Options:**

1. **SQS Standard Queue:** Does not ensure ordering.
2. **SQS FIFO without Group ID:** Limits to single consumer, cannot scale per desktop.
3. **Kinesis Data Stream:** Suitable but less optimal for large-scale individual processing compared to SQS FIFO.

**Conclusion:**

Using SQS FIFO with Group ID ensures ordered processing and scalability per desktop system, meeting the monitoring solution requirements.

**Question 60**

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

**Correct Option:**

Set up a read replica and modify the application to use the appropriate endpoint.

**Explanation:**

1. **Read Replicas:**
   - Offload read requests from the primary instance.
   - Improve performance by reducing I/O contention.
2. **Aurora Cluster:**
   - Consists of a primary DB instance for writes and replicas for reads.
   - Use reader endpoint for load-balanced read operations.

**Incorrect Options:**

1. **Provision Another Aurora Database:** Not feasible for read operations.
2. **Multi-AZ Standby Instance:** Used for failover, not read scaling.
3. **Read-through Caching:** Not natively supported, requires additional setup.

**Conclusion:**

Setting up read replicas in Aurora allows efficient separation of read and write operations, enhancing overall database performance.

**Question 61**

**Question:** An application runs big data workloads on Amazon EC2 instances. The application runs 24x7 all year round and needs at least 20 instances to maintain a minimum acceptable performance threshold and the application needs 300 instances to handle spikes in the workload. Based on historical workloads processed by the application, it needs 80 instances 80% of the time. As a solutions architect, which of the following would you recommend as the MOST cost-optimal solution so that it can meet the workload demand in a steady state?

**Correct Option:**

Purchase 80 reserved instances (RIs). Provision additional on-demand and spot instances per the workload demand (Use Auto Scaling Group with a launch template to provision the mix of on-demand and spot instances).

**Explanation:**

1. **Reserved Instances (RIs):**
   - Cost-effective for steady-state usage (80 instances 80% of the time).
   - Provides savings over on-demand pricing.
2. **On-demand and Spot Instances:**
   - Handle variable demand.
   - Cost-efficient for spikes in workload.

**Incorrect Options:**

1. **20 On-demand and Spot Instances:** Insufficient for steady-state requirement.
2. **80 On-demand Instances:** Costlier than RIs.
3. **80 Spot Instances:** No guarantee of availability, risky for steady-state demand.

**Conclusion:**

Using reserved instances for steady-state and combining on-demand and spot instances for variable demand ensures cost optimization and availability for big data workloads.

**Question 62**

**Question:** You would like to migrate an AWS account from an AWS Organization A to an AWS Organization B. What are the steps to do it?

**Correct Option:**

Remove the member account from the old organization. Send an invite to the member account from the new Organization. Accept the invite to the new organization from the member account.

**Explanation:**

1. **AWS Organizations:**
   - Manage multiple AWS accounts.
   - Simplify billing and apply policies centrally.
2. **Migration Steps:**
   - Remove the account from the old organization.
   - Send an invite from the new organization.
   - Accept the invite to join the new organization.

**Incorrect Options:**

1. **Sending Invite Before Removal:** Incorrect sequence.
2. **AWS Support Ticket:** Not required for account migration.
3. **Removing Before Sending Invite:** Incorrect sequence and steps.

**Conclusion:**

Following the correct steps ensures a smooth migration of AWS accounts between organizations, maintaining governance and billing structures.

**Question 63**

**Question:** Your company has deployed an application that will perform a lot of overwrites and deletes on data and require the latest information to be available anytime data is read via queries on database tables. As a Solutions Architect, which database technology will you recommend?

**Correct Option:**

Amazon Relational Database Service (Amazon RDS)

**Explanation:**

1. **Amazon RDS:**
   - Provides ACID-compliant transactions.
   - Ensures data integrity and consistency.
   - Suitable for applications requiring frequent updates and deletions.

**Incorrect Options:**

1. **Amazon ElastiCache:** Ideal for caching, not for frequent updates/deletes.

2. **Amazon S3:** Object storage, not suitable for database transactions.
3. **Amazon Neptune:** Graph database, not suitable for this use case.

**Conclusion:**

Amazon RDS ensures data integrity and consistency, making i t suitable for applications with frequent overwrites and deletes, requiring real-time availability.

**Question 64**

**Question:** An analytics company wants to improve the performance of its big data processing workflows running on Amazon Elastic File System (Amazon EFS). Which of the following performance modes should be used for Amazon EFS to address this requirement?

**Correct Option:**

Max I/O

**Explanation:**

1. **Max I/O Performance Mode:**
   - Provides higher aggregate throughput and operations per second.
   - Suitable for highly parallelized applications like big data processing.

**Incorrect Options:**

1. **Provisioned Throughput:** Refers to throughput mode, not performance mode.
2. **Bursting Throughput:** Refers to throughput mode, not performance mode.
3. **General Purpose:** Suitable for latency-sensitive applications, not high throughput.

**Conclusion:**

Max I/O performance mode is ideal for big data processing on Amazon EFS, providing the necessary throughput and scalability.

**Question 65**

**Question:** A company has historically operated only in the us-east-1 region and stores encrypted data in Amazon S3 using SSE-KMS. As part of enhancing its security posture as well as improving the backup and recovery architecture, the company wants to store the encrypted data in Amazon S3 that is replicated into the us-west-1 AWS region. The security policies mandate that the data must be encrypted and decrypted using the same key in both AWS regions. Which of the following represents the best solution to address these requirements?

**Correct Option:**

Create a new Amazon S3 bucket in the us-east-1 region with replication enabled from this new bucket into another bucket in the us-west-1 region. Enable SSE-KMS encryption on the new bucket in us-east-1 region by using an AWS KMS multi-region key. Copy the existing data from the current Amazon S3 bucket in us-east-1 region into this new Amazon S3 bucket in us-east-1 region.

**Explanation:**

1. **AWS KMS Multi-Region Keys:**
   - Allow encryption and decryption across multiple regions with the same key material and ID.
   - Ensures compliance with security policies for encryption and decryption.
2. **Data Replication:**
   - Replicate data between S3 buckets in different regions.
   - Use multi-region keys for seamless encryption and decryption.

**Incorrect Options:**

1. **Batch Replication with Single-Region Key:** Not feasible to convert single-region to multi-region key.
2. **Sharing KMS Key Across Regions:** Not supported by AWS.
3. **Using CloudWatch and Lambda:** Involves significant effort and potential data loss, not optimal.

**Conclusion:**

Using AWS KMS multi-region keys and enabling replication between S3 buckets ensures secure and compliant data encryption and decryption across regions, improving backup and recovery.