\* Amazon FSx for Windows File Server provides fully managed, highly reliable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol.

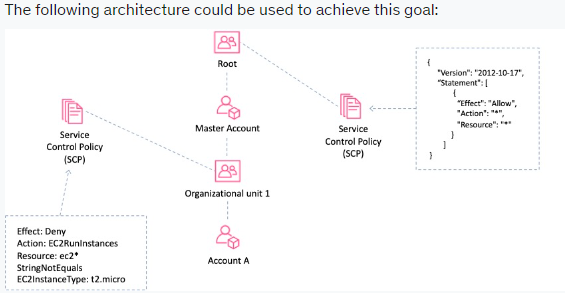
Amazon FSx is built on Windows Server and provides a rich set of administrative features that include end-user file restore, user quotas, and Access Control Lists (ACLs).

Additionally, Amazon FSX for Windows File Server supports Distributed File System Replication (DFSR) in Single-AZ deployments as can be seen in the feature comparison table below.



\* An AWS Organization has an OU with multiple member accounts in it. The company needs to restrict the ability to launch only specific Amazon EC2 instance types. How can this policy be applied across the accounts with the least effort?

To apply the restrictions across multiple member accounts you must use a Service Control Policy (SCP) in the AWS Organization. The way you would do this is to create a deny rule that applies to anything that does not equal the specific instance type you want to allow.



\* A company's application is running on Amazon EC2 instances in a single Region. In the event of a disaster, a solutions architect needs to ensure that the resources can also be deployed to a second Region.

Which combination of actions should the solutions architect take to accomplish this?

You can copy an Amazon Machine Image (AMI) within or across AWS Regions using the AWS Management Console, the AWS Command Line Interface or SDKs, or the Amazon EC2 API, all of which support the CopyImage action.

Using the copied AMI the solutions architect would then be able to launch an instance from the same EBS volume in the second Region.

**Note:**the AMIs are stored on Amazon S3, however you cannot view them in the S3 management console or work with them programmatically using the S3 API.

**CORRECT:**"Copy an Amazon Machine Image (AMI) of an EC2 instance and specify the second Region for the destination" is a correct answer.

**CORRECT:**"Launch a new EC2 instance from an Amazon Machine Image (AMI) in the second Region" is also a correct answer.

\* An organization want to share regular updates about their charitable work using static webpages. The pages are expected to generate a large amount of views from around the world. The files are stored in an Amazon S3 bucket. A solutions architect has been asked to design an efficient and effective solution.

Which action should the solutions architect take to accomplish this?

Amazon CloudFront can be used to cache the files in edge locations around the world and this will improve the performance of the webpages.

To serve a static website hosted on Amazon S3, you can deploy a CloudFront distribution using one of these configurations:

Using a REST API endpoint as the origin with access restricted by an [origin access identity (OAI)](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html)

Using a website endpoint as the origin with anonymous (public) access allowed

Using a website endpoint as the origin with access restricted by a Referer header

**CORRECT:**"Use Amazon CloudFront with the S3 bucket as its origin" is the correct answer.

\* A company runs an application in an on-premises data center that collects environmental data from production machinery. The data consists of JSON files stored on network attached storage (NAS) and around 5 TB of data is collected each day. The company must upload this data to Amazon S3 where it can be processed by an analytics application. The data must be transferred securely.

Which solution offers the MOST reliable and time-efficient data transfer?

The most reliable and time-efficient solution that keeps the data secure is to use AWS DataSync and synchronize the data from the NAS device directly to Amazon S3. This should take place over an AWS Direct Connect connection to ensure reliability, speed, and security.

AWS DataSync can copy data between Network File System (NFS) shares, Server Message Block (SMB) shares, self-managed object storage, AWS Snowcone, Amazon Simple Storage Service (Amazon S3) buckets, Amazon Elastic File System (Amazon EFS) file systems, and Amazon FSx for Windows File Server file systems.

**CORRECT:**"AWS DataSync over AWS Direct Connect" is the correct answer.

\* A new application will run across multiple Amazon ECS tasks. Front-end application logic will process data and then pass that data to a back-end ECS task to perform further processing and write the data to a datastore. The Architect would like to reduce-interdependencies so failures do no impact other components.

Which solution should the Architect use?

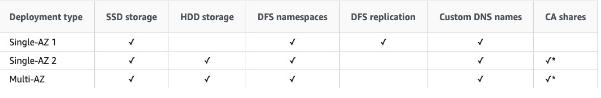
This is a good use case for Amazon SQS. SQS is a service that is used for decoupling applications, thus reducing interdependencies, through a message bus. The front-end application can place messages on the queue and the back-end can then poll the queue for new messages. Please remember that Amazon SQS is pull-based (polling) not push-based (use SNS for push-based).

CORRECT: "Create an Amazon SQS queue and configure the front-end to add messages to the queue and the back-end to poll the queue for messages" is the correct answer.

\* A Microsoft Windows file server farm uses Distributed File System Replication (DFSR) to synchronize data in an on-premises environment. The infrastructure is being migrated to the AWS Cloud.

Which service should the solutions architect use to replace the file server farm?

Amazon FSx for Windows file server supports DFS namespaces and DFS replication. This is the best solution for replacing the on-premises infrastructure. Note the limitations for deployment:



**CORRECT:**"Amazon FSx" is the correct answer.

\* A Solutions Architect has been tasked with re-deploying an application running on AWS to enable high availability. The application processes messages that are received in an ActiveMQ queue running on a single Amazon EC2 instance. Messages are then processed by a consumer application running on Amazon EC2. After processing the messages the consumer application writes results to a MySQL database running on Amazon EC2.

Which architecture offers the highest availability and low operational complexity?

The correct answer offers the highest availability as it includes Amazon MQ active/standby brokers across two AZs, an Auto Scaling group across two AZ,s and a Multi-AZ Amazon RDS MySQL database deployment.

This architecture not only offers the highest availability it is also operationally simple as it maximizes the usage of managed services.

CORRECT: "Deploy Amazon MQ with active/standby brokers configured across two Availability Zones. Create an Auto Scaling group for the consumer EC2 instances across two Availability Zones. Use an Amazon RDS MySQL database with Multi-AZ enabled" is the correct answer.

\* A company hosts a multiplayer game on AWS. The application uses Amazon EC2 instances in a single Availability Zone and users connect over Layer 4. Solutions Architect has been tasked with making the architecture highly available and also more cost-effective.

How can the solutions architect best meet these requirements? (Select TWO.)

The solutions architect must enable high availability for the architecture and ensure it is cost-effective. To enable high availability an Amazon EC2 Auto Scaling group should be created to add and remove instances across multiple availability zones.

In order to distribute the traffic to the instances the architecture should use a Network Load Balancer which operates at Layer 4. This architecture will also be cost-effective as the Auto Scaling group will ensure the right number of instances are running based on demand.

**CORRECT:**"Configure a Network Load Balancer in front of the EC2 instances" is a correct answer.

\* A manufacturing company captures data from machines running at customer sites. Currently, thousands of machines send data every 5 minutes, and this is expected to grow to hundreds of thousands of machines in the near future. The data is logged with the intent to be analyzed in the future as needed.

What is the SIMPLEST method to store this streaming data at scale?

Kinesis Data Firehose is the easiest way to load streaming data into data stores and analytics tools. It captures, transforms, and loads streaming data and you can deliver the data to “destinations” including Amazon S3 buckets for later analysis

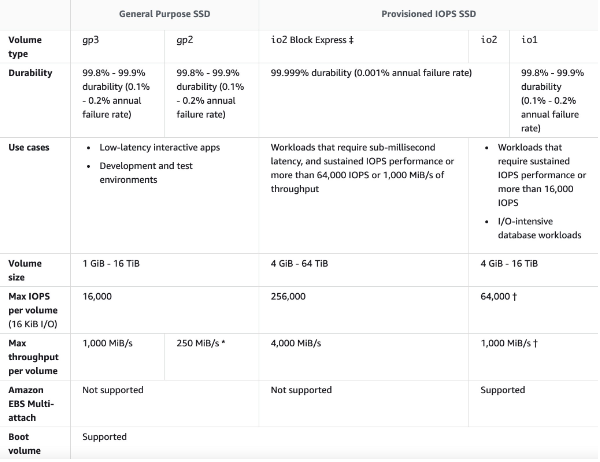
CORRECT: "Create an Amazon Kinesis Firehose delivery stream to store the data in Amazon S3" is the correct answer.

\* A persistent database must be migrated from an on-premises server to an Amazon EC2 instances. The database requires 64,000 IOPS and, if possible, should be stored on a single Amazon EBS volume.

Which solution should a Solutions Architect recommend?

Amazon EC2 Nitro-based systems are not required for this solution but do offer advantages in performance that will help to maximize the usage of the EBS volume. For the data storage volume an i01 volume can support up to 64,000 IOPS so a single volume with sufficient capacity (50 IOPS per GiB) can be deliver the requirements.

The current list of EBS volume types is in the table below:



**CORRECT:**"Create a Nitro-based Amazon EC2 instance with an Amazon EBS Provisioned IOPS SSD (i01) volume attached. Provision 64,000 IOPS for the volume" is the correct answer.

\* A company uses an Amazon RDS MySQL database instance to store customer order data. The security team have requested that SSL/TLS encryption in transit must be used for encrypting connections to the database from application servers. The data in the database is currently encrypted at rest using an AWS KMS key.

How can a Solutions Architect enable encryption in transit?

Amazon RDS creates an SSL certificate and installs the certificate on the DB instance when Amazon RDS provisions the instance. These certificates are signed by a certificate authority. The SSL certificate includes the DB instance endpoint as the Common Name (CN) for the SSL certificate to guard against spoofing attacks.

You can download a root certificate from AWS that works for all Regions or you can download Region-specific intermediate certificates.

**CORRECT:**"Download the AWS-provided root certificates. Use the certificates when connecting to the RDS DB instance" is the correct answer.

\* A solutions architect is creating a system that will run analytics on financial data for several hours a night, 5 days a week. The analysis is expected to run for the same duration and cannot be interrupted once it is started. The system will be required for a minimum of 1 year.

What should the solutions architect configure to ensure the EC2 instances are available when they are needed?

On-Demand Capacity Reservations enable you to reserve compute capacity for your Amazon EC2 instances in a specific Availability Zone for any duration. This gives you the ability to create and manage Capacity Reservations independently from the billing discounts offered by Savings Plans or Regional Reserved Instances.

By creating Capacity Reservations, you ensure that you always have access to EC2 capacity when you need it, for as long as you need it. You can create Capacity Reservations at any time, without entering a one-year or three-year term commitment, and the capacity is available immediately.

The table below shows the difference between capacity reservations and other



**CORRECT:**"On-Demand Capacity Reservations" is the correct answer.

\* An e-commerce application is hosted in AWS. The last time a new product was launched, the application experienced a performance issue due to an enormous spike in traffic. Management decided that capacity must be doubled this week after the product is launched.

What is the MOST efficient way for management to ensure that capacity requirements are met?

Scaling based on a schedule allows you to set your own scaling schedule for predictable load changes. To configure your Auto Scaling group to scale based on a schedule, you create a scheduled action. This is ideal for situations where you know when and for how long you are going to need the additional capacity.

**CORRECT:**"Add a Scheduled Scaling action" is the correct answer.

\* An application running on an Amazon ECS container instance using the EC2 launch type needs permissions to write data to Amazon DynamoDB.

How can you assign these permissions only to the specific ECS task that is running the application?

To specify permissions for a specific task on Amazon ECS you should use IAM Roles for Tasks. The permissions policy can be applied to tasks when creating the task definition, or by using an IAM task role override using the AWS CLI or SDKs. The taskRoleArn parameter is used to specify the policy.

CORRECT: "Create an IAM policy with permissions to DynamoDB and assign It to a task using the taskRoleArn parameter" is the correct answer.

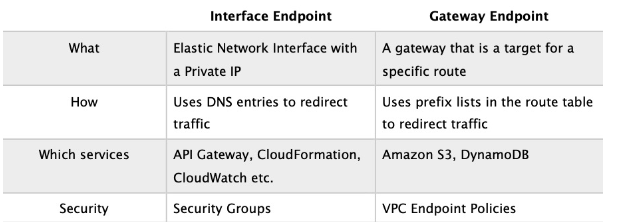
\* An Amazon RDS Read Replica is being deployed in a separate region. The master database is not encrypted but all data in the new region must be encrypted. How can this be achieved?

You cannot create an encrypted Read Replica from an unencrypted master DB instance. You also cannot enable encryption after launch time for the master DB instance. Therefore, you must create a new master DB by taking a snapshot of the existing DB, encrypting it, and then creating the new DB from the snapshot. You can then create the encrypted cross-region Read Replica of the master DB.

CORRECT: "Encrypt a snapshot from the master DB instance, create a new encrypted master DB instance, and then create an encrypted cross-region Read Replica" is the correct answer.

\* A company wishes to restrict access to their Amazon DynamoDB table to specific, private source IP addresses from their VPC. What should be done to secure access to the table?

There are two different types of VPC endpoint: interface endpoint, and gateway endpoint. With an interface endpoint you use an ENI in the VPC. With a gateway endpoint you configure your route table to point to the endpoint. Amazon S3 and DynamoDB use gateway endpoints. This solution means that all traffic will go through the VPC endpoint straight to DynamoDB using private IP addresses.



**CORRECT:**"Create a gateway VPC endpoint and add an entry to the route table" is the correct answer.

\* A company runs an application that uses an Amazon RDS PostgreSQL database. The database is currently not encrypted. A Solutions Architect has been instructed that due to new compliance requirements all existing and new data in the database must be encrypted. The database experiences high volumes of changes and no data can be lost.

How can the Solutions Architect enable encryption for the database without incurring any data loss?

You cannot change the encryption status of an existing RDS DB instance. Encryption must be specified when creating the RDS DB instance. The best way to encrypt an existing database is to take a snapshot, encrypt a copy of the snapshot and restore the snapshot to a new RDS DB instance. This results in an encrypted database that is a new instance. Applications must be updated to use the new RDS DB endpoint.

In this scenario as there is a high rate of change, the databases will be out of sync by the time the new copy is created and is functional. The best way to capture the changes between the source (unencrypted) and destination (encrypted) DB is to use AWS Database Migration Service (DMS) to synchronize the data.

The slide below depicts the process for encrypting an unencrypted RDS DB instance:

CORRECT: "Create a snapshot of the existing RDS DB instance. Create an encrypted copy of the snapshot. Create a new RDS DB instance from the encrypted snapshot and update the application. Use AWS DMS to synchronize data between the source and destination RDS DBs" is the correct answer.

\* CORRECT: "Create a snapshot of the existing RDS DB instance. Create an encrypted copy of the snapshot. Create a new RDS DB instance from the encrypted snapshot and update the application. Use AWS DMS to synchronize data between the source and destination RDS DBs" is the correct answer.

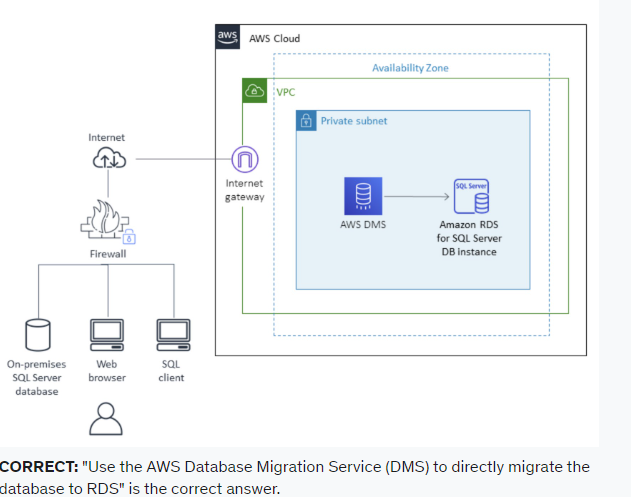
Amazon SQS supports resource-based policies. The best way to grant the permissions using the principle of least privilege is to use a resource-based policy attached to the SQS queue that grants the partner company’s AWS account the sqs:SendMessage privilege.

**CORRECT:**"Update the permission policy on the SQS queue to grant the sqs:SendMessage permission to the partner’s AWS account" is the correct answer.

\* The database tier of a web application is running on a Windows server on-premises. The database is a Microsoft SQL Server database. The application owner would like to migrate the database to an Amazon RDS instance.

How can the migration be executed with minimal administrative effort and downtime?

You can directly migrate Microsoft SQL Server from an on-premises server into Amazon RDS using the Microsoft SQL Server database engine. This can be achieved using the native Microsoft SQL Server tools, or using AWS DMS as depicted below:



\* Amazon EC2 instances in a development environment run between 9am and 5pm Monday-Friday. Production instances run 24/7. Which pricing models should be used? (choose 2)

Capacity reservations have no commitment and can be created and canceled as needed. This is ideal for the development environment as it will ensure the capacity is available. There is no price advantage but none of the other options provide a price advantage whilst also ensuring capacity is available

Reserved instances are a good choice for workloads that run continuously. This is a good option for the production environment.

CORRECT: "On-demand capacity reservations for the development environment" is a correct answer.

CORRECT: "Use Reserved instances for the production environment" is also a correct answer.

\* A company runs an application on an Amazon EC2 instance the requires 250 GB of storage space. The application is not used often and has small spikes in usage on weekday mornings and afternoons. The disk I/O can vary with peaks hitting a maximum of 3,000 IOPS. A Solutions Architect must recommend the most cost-effective storage solution that delivers the performance required.

Which configuration should the Solutions Architect recommend?

Which solution should the solutions architect recommend?

General Purpose SSD (gp2) volumes offer cost-effective storage that is ideal for a broad range of workloads. These volumes deliver single-digit millisecond latencies and the ability to burst to 3,000 IOPS for extended periods of time.

Between a minimum of 100 IOPS (at 33.33 GiB and below) and a maximum of 16,000 IOPS (at 5,334 GiB and above), baseline performance scales linearly at 3 IOPS per GiB of volume size. AWS designs gp2 volumes to deliver their provisioned performance 99% of the time. A gp2 volume can range in size from 1 GiB to 16 TiB.

In this configuration the volume will provide a baseline performance of 750 IOPS but will always be able to burst to the required 3,000 IOPS during periods of increased traffic.

CORRECT: "Amazon EBS General Purpose SSD (gp2)" is the correct answer.

\* A solutions architect is designing the infrastructure to run an application on Amazon EC2 instances. The application requires high availability and must dynamically scale based on demand to be cost efficient.

What should the solutions architect do to meet these requirements?

The Amazon EC2-based application must be highly available and elastically scalable. Auto Scaling can provide the elasticity by dynamically launching and terminating instances based on demand. This can take place across availability zones for high availability.

Incoming connections can be distributed to the instances by using an Application Load Balancer (ALB).

CORRECT: "Configure an Application Load Balancer in front of an Auto Scaling group to deploy instances to multiple Availability Zones" is the correct answer.

\* An eCommerce application consists of three tiers. The web tier includes EC2 instances behind an Application Load balancer, the middle tier uses EC2 instances and an Amazon SQS queue to process orders, and the database tier consists of an Auto Scaling DynamoDB table. During busy periods customers have complained about delays in the processing of orders. A Solutions Architect has been tasked with reducing processing times.

Which action will be MOST effective in accomplishing this requirement?

The most likely cause of the processing delays is insufficient instances in the middle tier where the order processing takes place. The most effective solution to reduce processing times in this case is to scale based on the backlog per instance (number of messages in the SQS queue) as this reflects the amount of work that needs to be done.

CORRECT: "Use Amazon EC2 Auto Scaling to scale out the middle tier instances based on the SQS queue depth" is the correct answer.

\* A company delivers content to subscribers distributed globally from an application running on AWS. The application uses a fleet of Amazon EC2 instance in a private subnet behind an Application Load Balancer (ALB). Due to an update in copyright restrictions, it is necessary to block access for specific countries.

What is the EASIEST method to meet this requirement?

When a user requests your content, CloudFront typically serves the requested content regardless of where the user is located. If you need to prevent users in specific countries from accessing your content, you can use the CloudFront geo restriction feature to do one of the following:

Allow your users to access your content only if they're in one of the countries on a whitelist of approved countries.

Prevent your users from accessing your content if they're in one of the countries on a blacklist of banned countries.

For example, if a request comes from a country where, for copyright reasons, you are not authorized to distribute your content, you can use CloudFront geo restriction to block the request.

This is the easiest and most effective way to implement a geographic restriction for the delivery of content.

**CORRECT:**"Use Amazon CloudFront to serve the application and deny access to blocked countries" is the correct answer.

\* A website runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB) which serves as an origin for an Amazon CloudFront distribution. An AWS WAF is being used to protect against SQL injection attacks. A review of security logs revealed an external malicious IP that needs to be blocked from accessing the website.

What should a solutions architect do to protect the application?

A new version of the AWS Web Application Firewall was released in November 2019. With AWS WAF classic you create “IP match conditions”, whereas with AWS WAF (new version) you create “IP set match statements”. Look out for wording on the exam.

The IP match condition / IP set match statement inspects the IP address of a web request's origin against a set of IP addresses and address ranges. Use this to allow or block web requests based on the IP addresses that the requests originate from.

AWS WAF supports all IPv4 and IPv6 address ranges. An IP set can hold up to 10,000 IP addresses or IP address ranges to check.

CORRECT: "Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address" is the correct answer.

\* A team are planning to run analytics jobs on log files each day and require a storage solution. The size and number of logs is unknown and data will persist for 24 hours only.

What is the MOST cost-effective solution?

S3 standard is the best choice in this scenario for a short term storage solution. In this case the size and number of logs is unknown and it would be difficult to fully assess the access patterns at this stage. Therefore, using S3 standard is best as it is cost-effective, provides immediate access, and there are no retrieval fees or minimum capacity charge per object.

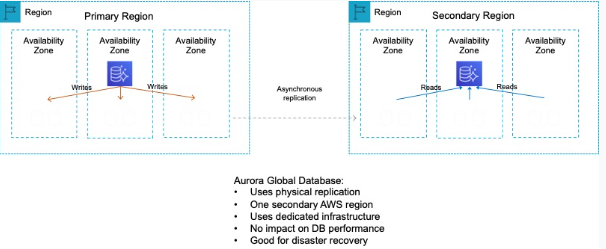
**CORRECT:**"Amazon S3 Standard" is the correct answer.

\* An insurance company has a web application that serves users in the United Kingdom and Australia. The application includes a database tier using a MySQL database hosted in eu-west-2. The web tier runs from eu-west-2 and ap-southeast-2. Amazon Route 53 geoproximity routing is used to direct users to the closest web tier. It has been noted that Australian users receive slow response times to queries.

Which changes should be made to the database tier to improve performance?

The issue here is latency with read queries being directed from Australia to UK which is great physical distance. A solution is required for improving read performance in Australia.

An Aurora global database consists of one primary AWS Region where your data is mastered, and up to five read-only, secondary AWS Regions. Aurora replicates data to the secondary AWS Regions with typical latency of under a second. You issue write operations directly to the primary DB instance in the primary AWS Region.



This solution will provide better performance for users in the Australia Region for queries. Writes must still take place in the UK Region but read performance will be greatly improved.

CORRECT: "Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure read replicas in ap-southeast-2" is the correct answer.

\* A web application allows users to upload photos and add graphical elements to them. The application offers two tiers of service: free and paid. Photos uploaded by paid users should be processed before those submitted using the free tier. The photos are uploaded to an Amazon S3 bucket which uses an event notification to send the job information to Amazon SQS.

How should a Solutions Architect configure the Amazon SQS deployment to meet these requirements?

AWS recommend using separate queues when you need to provide prioritization of work. The logic can then be implemented at the application layer to prioritize the queue for the paid photos over the queue for the free photos.

CORRECT: "Use a separate SQS Standard queue for each tier. Configure Amazon EC2 instances to prioritize polling for the paid queue over the free queue" is the correct answer.

\* A financial services company has a web application with an application tier running in the U.S and Europe. The database tier consists of a MySQL database running on Amazon EC2 in us-west-1. Users are directed to the closest application tier using Route 53 latency-based routing. The users in Europe have reported poor performance when running queries.

Which changes should a Solutions Architect make to the database tier to improve performance?

Amazon Aurora Global Database is designed for globally distributed applications, allowing a single Amazon Aurora database to span multiple AWS regions. It replicates your data with no impact on database performance, enables fast local reads with low latency in each region, and provides disaster recovery from region-wide outages.

A global database can be configured in the European region and then the application tier in Europe will need to be configured to use the local database for reads/queries. The diagram below depicts an Aurora Global Database deployment.

CORRECT: "Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure the application tier in Europe to use the local reader endpoint" is the correct answer.

\* A solutions architect needs to backup some application log files from an online ecommerce store to Amazon S3. It is unknown how often the logs will be accessed or which logs will be accessed the most. The solutions architect must keep costs as low as possible by using the appropriate S3 storage class.

Which S3 storage class should be implemented to meet these requirements?

The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead.

It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. This is an ideal use case for intelligent-tiering as the access patterns for the log files are not known.

CORRECT: "S3 Intelligent-Tiering" is the correct answer.

\* A company is deploying a fleet of Amazon EC2 instances running Linux across multiple Availability Zones within an AWS Region. The application requires a data storage solution that can be accessed by all of the EC2 instances simultaneously. The solution must be highly scalable and easy to implement. The storage must be mounted using the NFS protocol.

Which solution meets these requirements?

Amazon EFS provides scalable file storage for use with Amazon EC2. You can use an EFS file system as a common data source for workloads and applications running on multiple instances. The EC2 instances can run in multiple AZs within a Region and the NFS protocol is used to mount the file system.

With EFS you can create mount targets in each AZ for lower latency. The application instances in each AZ will mount the file system using the local mount target.

CORRECT: "Create an Amazon EFS file system with mount targets in each Availability Zone. Configure the application instances to mount the file system" is the correct answer.

\* A solutions architect is designing a new service that will use an Amazon API Gateway API on the frontend. The service will need to persist data in a backend database using key-value requests. Initially, the data requirements will be around 1 GB and future growth is unknown. Requests can range from 0 to over 800 requests per second.

Which combination of AWS services would meet these requirements? (Select TWO.)

In this case AWS Lambda can perform the computation and store the data in an Amazon DynamoDB table. Lambda can scale concurrent executions to meet demand easily and DynamoDB is built for key-value data storage requirements and is also serverless and easily scalable. This is therefore a cost effective solution for unpredictable workloads.

CORRECT: "AWS Lambda" is a correct answer.

CORRECT: "Amazon DynamoDB" is also a correct answer.

\* A company has two accounts for perform testing and each account has a single VPC: VPC-TEST1 and VPC-TEST2. The operations team require a method of securely copying files between Amazon EC2 instances in these VPCs. The connectivity should not have any single points of failure or bandwidth constraints.

Which solution should a Solutions Architect recommend?

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network.

You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection).

**CORRECT:**"Create a VPC peering connection between VPC-TEST1 and VPC-TEST2" is the correct answer.

\* A video production company is planning to move some of its workloads to the AWS Cloud. The company will require around 5 TB of storage for video processing with the maximum possible I/O performance. They also require over 400 TB of extremely durable storage for storing video files and 800 TB of storage for long-term archival.

Which combinations of services should a Solutions Architect use to meet these requirements?

The best I/O performance can be achieved by using instance store volumes for the video processing. This is safe to use for use cases where the data can be recreated from the source files so this is a good use case.

For storing data durably Amazon S3 is a good fit as it provides 99.999999999% of durability. For archival the video files can then be moved to Amazon S3 Glacier which is a low cost storage option that is ideal for long-term archival.

CORRECT: "Amazon EC2 instance store for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage" is the correct answer.

\* An eCommerce company runs an application on Amazon EC2 instances in public and private subnets. The web application runs in a public subnet and the database runs in a private subnet. Both the public and private subnets are in a single Availability Zone.

Which combination of steps should a solutions architect take to provide high availability for this architecture? (Select TWO.)

High availability can be achieved by using multiple Availability Zones within the same VPC. An EC2 Auto Scaling group can then be used to launch web application instances in multiple public subnets across multiple AZs and an ALB can be used to distribute incoming load.

The database solution can be made highly available by migrating from EC2 to Amazon RDS and using a Multi-AZ deployment model. This will provide the ability to failover to another AZ in the event of a failure of the primary database or the AZ in which it runs.

CORRECT: "Create an EC2 Auto Scaling group and Application Load Balancer that spans across multiple AZs" is a correct answer.

CORRECT: "Create new public and private subnets in a different AZ. Migrate the database to an Amazon RDS multi-AZ deployment" is also a correct answer.

\* A company plans to make an Amazon EC2 Linux instance unavailable outside of business hours to save costs. The instance is backed by an Amazon EBS volume. There is a requirement that the contents of the instance’s memory must be preserved when it is made unavailable.

How can a solutions architect meet these requirements?

When you hibernate an instance, Amazon EC2 signals the operating system to perform hibernation (suspend-to-disk). Hibernation saves the contents from the instance memory (RAM) to your Amazon Elastic Block Store (Amazon EBS) root volume. Amazon EC2 persists the instance's EBS root volume and any attached EBS data volumes. When you start your instance:

- The EBS root volume is restored to its previous state

- The RAM contents are reloaded

- The processes that were previously running on the instance are resumed

- Previously attached data volumes are reattached and the instance retains its instance ID

CORRECT: "Hibernate the instance outside business hours. Start the instance again when required" is the correct answer.

\* A company provides a REST-based interface to an application that allows a partner company to send data in near-real time. The application then processes the data that is received and stores it for later analysis. The application runs on Amazon EC2 instances.

The partner company has received many 503 Service Unavailable Errors when sending data to the application and the compute capacity reaches its limits and is unable to process requests when spikes in data volume occur.

Which design should a Solutions Architect implement to improve scalability?

Amazon Kinesis enables you to ingest, buffer, and process streaming data in real-time. Kinesis can handle any amount of streaming data and process data from hundreds of thousands of sources with very low latencies. This is an ideal solution for data ingestion.

To ensure the compute layer can scale to process increasing workloads, the EC2 instances should be replaced by AWS Lambda functions. Lambda can scale seamlessly by running multiple executions in parallel.

CORRECT: "Use Amazon Kinesis Data Streams to ingest the data. Process the data using AWS Lambda functions" is the correct answer.

\* A company has uploaded some highly critical data to an Amazon S3 bucket. Management are concerned about data availability and require that steps are taken to protect the data from accidental deletion. The data should still be accessible, and a user should be able to delete the data intentionally.

Which combination of steps should a solutions architect take to accomplish this? (Select TWO.)

Multi-factor authentication (MFA) delete adds an additional step before an object can be deleted from a versioning-enabled bucket.

With MFA delete the bucket owner must include the x-amz-mfa request header in requests to permanently delete an object version or change the versioning state of the bucket.

CORRECT: "Enable versioning on the S3 bucket" is a correct answer.

CORRECT: "Enable MFA Delete on the S3 bucket" is also a correct answer.

\* A retail company with many stores and warehouses is implementing IoT sensors to gather monitoring data from devices in each location. The data will be sent to AWS in real time. A solutions architect must provide a solution for ensuring events are received in order for each device and ensure that data is saved for future processing.

Which solution would be MOST efficient?

Amazon Kinesis Data Streams collect and process data in real time. A Kinesis data stream is a set of shards. Each shard has a sequence of data records. Each data record has a sequence number that is assigned by Kinesis Data Streams. A shard is a uniquely identified sequence of data records in a stream.

A partition key is used to group data by shard within a stream. Kinesis Data Streams segregates the data records belonging to a stream into multiple shards. It uses the partition key that is associated with each data record to determine which shard a given data record belongs to.

CORRECT: "Use Amazon Kinesis Data Streams for real-time events with a partition key for each device. Use Amazon Kinesis Data Firehose to save data to Amazon S3" is the correct answer.

\* A new application is to be published in multiple regions around the world. The Architect needs to ensure only 2 IP addresses need to be whitelisted. The solution should intelligently route traffic for lowest latency and provide fast regional failover.

How can this be achieved?

AWS Global Accelerator uses the vast, congestion-free AWS global network to route TCP and UDP traffic to a healthy application endpoint in the closest AWS Region to the user.

This means it will intelligently route traffic to the closest point of presence (reducing latency). Seamless failover is ensured as AWS Global Accelerator uses anycast IP address which means the IP does not change when failing over between regions so there are no issues with client caches having incorrect entries that need to expire.

This is the only solution that provides deterministic failover.

CORRECT: "Launch EC2 instances into multiple regions behind an NLB and use AWS Global Accelerator" is the correct answer.

\* A company runs a large batch processing job at the end of every quarter. The processing job runs for 5 days and uses 15 Amazon EC2 instances. The processing must run uninterrupted for 5 hours per day. The company is investigating ways to reduce the cost of the batch processing job.

Which pricing model should the company choose?

Each EC2 instance runs for 5 hours a day for 5 days per quarter or 20 days per year. This is time duration is insufficient to warrant reserved instances as these require a commitment of a minimum of 1 year and the discounts would not outweigh the costs of having the reservations unused for a large percentage of time. In this case, there are no options presented that can reduce the cost and therefore on-demand instances should be used.

CORRECT: "On-Demand Instances" is the correct answer.

\* A company runs a web application that serves weather updates. The application runs on a fleet of Amazon EC2 instances in a Multi-AZ Auto scaling group behind an Application Load Balancer (ALB). The instances store data in an Amazon Aurora database. A solutions architect needs to make the application more resilient to sporadic increases in request rates.

Which architecture should the solutions architect implement? (Select TWO.)

The architecture is already highly resilient but the may be subject to performance degradation if there are sudden increases in request rates. To resolve this situation Amazon Aurora Read Replicas can be used to serve read traffic which offloads requests from the main database. On the frontend an Amazon CloudFront distribution can be placed in front of the ALB and this will cache content for better performance and also offloads requests from the backend.

CORRECT: "Add Amazon Aurora Replicas" is the correct answer.

CORRECT: "Add an Amazon CloudFront distribution in front of the ALB" is the correct answer.

\* A company has deployed a new website on Amazon EC2 instances behind an Application Load Balancer (ALB). Amazon Route 53 is used for the DNS service. The company has asked a Solutions Architect to create a backup website with support contact details that users will be directed to automatically if the primary website is down.

How should the Solutions Architect deploy this solution cost-effectively?

The most cost-effective solution is to create a static website using an Amazon S3 bucket and then use a failover routing policy in Amazon Route 53. With a failover routing policy users will be directed to the main website as long as it is responding to health checks successfully.

If the main website fails to respond to health checks (its down), Route 53 will begin to direct users to the backup website running on the Amazon S3 bucket. It’s important to set the TTL on the Route 53 records appropriately to ensure that users resolve the failover address within a short time.

CORRECT: "Configure a static website using Amazon S3 and create a Route 53 failover routing policy" is the correct answer.

\* A web application runs in public and private subnets. The application architecture consists of a web tier and database tier running on Amazon EC2 instances. Both tiers run in a single Availability Zone (AZ).

Which combination of steps should a solutions architect take to provide high availability for this architecture? (Select TWO.)

To add high availability to this architecture both the web tier and database tier require changes. For the web tier an Auto Scaling group across multiple AZs with an ALB will ensure there are always instances running and traffic is being distributed to them.

The database tier should be migrated from the EC2 instances to Amazon RDS to take advantage of a managed database with Multi-AZ functionality. This will ensure that if there is an issue preventing access to the primary database a secondary database can take over.

CORRECT: "Create an Amazon EC2 Auto Scaling group and Application Load Balancer (ALB) spanning multiple AZs" is the correct answer.

CORRECT: "Create new public and private subnets in the same VPC, each in a new AZ. Migrate the database to an Amazon RDS multi-AZ deployment" is the correct answer.

\* A developer created an application that uses Amazon EC2 and an Amazon RDS MySQL database instance. The developer stored the database user name and password in a configuration file on the root EBS volume of the EC2 application instance. A Solutions Architect has been asked to design a more secure solution.

What should the Solutions Architect do to achieve this requirement?

The key problem here is having plain text credentials stored in a file. Even if you encrypt the volume there is still as security risk as the credentials are loaded by the application and passed to RDS.

The best way to secure this solution is to get rid of the credentials completely by using an IAM role instead. The IAM role can be assigned permissions to the database instance and can be attached to the EC2 instance. The instance will then obtain temporary security credentials from AWS STS which is much more secure.

CORRECT: "Create an IAM role with permission to access the database. Attach this IAM role to the EC2 instance" is the correct answer.

\* A recent security audit uncovered some poor deployment and configuration practices within your VPC. You need to ensure that applications are deployed in secure configurations.

How can this be achieved in the most operationally efficient manner?

CloudFormation helps users to deploy resources in a consistent and orderly way. By ensuring the CloudFormation templates are created and administered with the right security configurations for your resources, you can then repeatedly deploy resources with secure settings and reduce the risk of human error.

CORRECT: "Use CloudFormation with securely configured templates" is the correct answer.

\* A company offers an online product brochure that is delivered from a static website running on Amazon S3. The company’s customers are mainly in the United States, Canada, and Europe. The company is looking to cost-effectively reduce the latency for users in these regions.

What is the most cost-effective solution to these requirements?

With Amazon CloudFront you can set the price class to determine where in the world the content will be cached. One of the price classes is “U.S, Canada and Europe” and this is where the company’s users are located. Choosing this price class will result in lower costs and better performance for the company’s users.

CORRECT: "Create an Amazon CloudFront distribution and set the price class to use only U.S, Canada and Europe." is the correct answer.

\* A company's web application is using multiple Amazon EC2 Linux instances and storing data on Amazon EBS volumes. The company is looking for a solution to increase the resiliency of the application in case of a failure.

What should a solutions architect do to meet these requirements?

To increase the resiliency of the application the solutions architect can use Auto Scaling groups to launch and terminate instances across multiple availability zones based on demand. An application load balancer (ALB) can be used to direct traffic to the web application running on the EC2 instances.

Lastly, the Amazon Elastic File System (EFS) can assist with increasing the resilience of the application by providing a shared file system that can be mounted by multiple EC2 instances from multiple availability zones.

CORRECT: "Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data on Amazon EFS and mount a target on each instance" is the correct answer.

\* A company is investigating methods to reduce the expenses associated with on-premises backup infrastructure. The Solutions Architect wants to reduce costs by eliminating the use of physical backup tapes. It is a requirement that existing backup applications and workflows should continue to function.

What should the Solutions Architect recommend?

The AWS Storage Gateway Tape Gateway enables you to replace using physical tapes on premises with virtual tapes in AWS without changing existing backup workflows. Tape Gateway emulates physical tape libraries, removes the cost and complexity of managing physical tape infrastructure, and provides more durability than physical tapes.

CORRECT: "Connect the backup applications to an AWS Storage Gateway using an iSCSI-virtual tape library (VTL)" is the correct answer.

\* A company runs an application in a factory that has a small rack of physical compute resources. The application stores data on a network attached storage (NAS) device using the NFS protocol. The company requires a daily offsite backup of the application data.

Which solution can a Solutions Architect recommend to meet this requirement?

The AWS Storage Gateway Hardware Appliance is a physical, standalone, validated server configuration for on-premises deployments. It comes pre-loaded with Storage Gateway software, and provides all the required CPU, memory, network, and SSD cache resources for creating and configuring File Gateway, Volume Gateway, or Tape Gateway.

A file gateway is the correct type of appliance to use for this use case as it is suitable for mounting via the NFS and SMB protocols.

CORRECT: "Use an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3" is the correct answer.

\*54 A Solutions Architect has deployed an application on several Amazon EC2 instances across three private subnets. The application must be made accessible to internet-based clients with the least amount of administrative effort.

How can the Solutions Architect make the application available on the internet?

To make the application instances accessible on the internet the Solutions Architect needs to place them behind an internet-facing Elastic Load Balancer. The way you add instances in private subnets to a public facing ELB is to add public subnets in the same AZs as the private subnets to the ELB. You can then add the instances and to the ELB and they will become targets for load balancing.

CORRECT: "Create an Application Load Balancer and associate three public subnets from the same Availability Zones as the private instances. Add the private instances to the ALB" is the correct answer.