# AWS Certified Solutions Architect – Associate SAA-C02 Exam Questions and Answers – Page 1

The latest AWS Certified Solutions Architect – Associate SAA-C02 certification actual real practice exam question and answer (Q&A) dumps are available free, which are helpful for you to pass the AWS Certified Solutions Architect – Associate SAA-C02 exam and earn AWS Certified Solutions Architect – Associate SAA-C02 certification.

#### Exam Question 1

A company is migrating from an on-premises infrastructure to the AWS Cloud. One of the company’s applications stores files on a Windows file server farm that uses Distributed File System Replication (DFSR) to keep data in sync. A solutions architect needs to replace the file server farm.

Which service should the solutions architect use?

A. Amazon EFS  
B. Amazon FSx  
C. Amazon S3  
D. AWS Storage Gateway

**Correct Answer:**  
B. Amazon FSx

**Answer Description:**  
Migrating Existing Files to Amazon FSx for Windows File Server Using AWS DataSync

We recommend using AWS DataSync to transfer data between Amazon FSx for Windows File Server file systems. DataSync is a data transfer service that simplifies, automates, and accelerates moving and replicating data between on-premises storage systems and other AWS storage services over the internet or AWS Direct Connect. DataSync can transfer your file system data and metadata, such as ownership, time stamps, and access permissions.

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 both Single-AZ and Multi-AZ deployments as can be seen in the feature comparison table below.

CORRECT: “Amazon FSx” is the correct answer.

INCORRECT: “Amazon EFS” is incorrect as EFS only supports Linux systems. INCORRECT: “Amazon S3” is incorrect as this is not a suitable replacement for a Microsoft filesystem.

INCORRECT: “AWS Storage Gateway” is incorrect as this service is primarily used for connecting on-premises storage to cloud storage. It consists of a software device installed on-premises and can be used with SMB shares but it actually stores the data on S3. It is also used for migration. However, in this case the company needs to replace the file server farm and Amazon FSx is the best choice for this job.

**References:** Amazon FSx for Windows File Server > Windows User Guide > [Availability and durability: Single-AZ and Multi-AZ file systems](https://docs.aws.amazon.com/fsx/latest/WindowsGuide/high-availability-multiAZ.html)

#### Exam Question 2

A company has a legacy application that processes data in two parts. The second part of the process takes longer than the first, so the company has decided to rewrite the application as two micro services running on Amazon ECS that can scale independently.

How should a solutions architect integrate the micro services?

A. Implement code in microservice 1 to send data to an Amazon S3 bucket. Use S3 event notifications to invoke microservice 2.  
B. Implement code in microservice 1 to publish data to an Amazon SNS topic. Implement code in microservice 2 to subscribe to this topic.  
C. Implement code in microservice 1 to send data to Amazon Kinesis Data Firehose. Implement code in microservice 2 to read from Kinesis Data Firehose.  
D. Implement code in microservice 1 to send data to an Amazon SQS queue. Implement code in microservice 2 to process messages from the queue.

**Correct Answer:**  
D. Implement code in microservice 1 to send data to an Amazon SQS queue. Implement code in microservice 2 to process messages from the queue.

**Answer Description:**  
This is a good use case for Amazon SQS. The microservices must be decoupled so they can scale independently. An Amazon SQS queue will enable microservice 1 to add messages to the queue. Microservice 2 can then pick up the messages and process them. This ensures that if there’s a spike in traffic on the frontend, messages do not get lost due to the backend process not being ready to process them.

CORRECT: “Implement code in microservice 1 to send data to an Amazon SQS queue. Implement code in microservice 2 to process messages from the queue” is the correct answer. INCORRECT: “Implement code in microservice 1 to send data to an Amazon S3 bucket. Use S3 event notifications to invoke microservice 2” is incorrect as a message queue would be preferable to an S3 bucket.

INCORRECT: “Implement code in microservice 1 to publish data to an Amazon SNS topic. Implement code in microservice 2 to subscribe to this topic” is incorrect as notifications to topics are pushed to subscribers. In this case we want the second microservice to pickup the messages when ready (pull them).

INCORRECT: “Implement code in microservice 1 to send data to Amazon Kinesis Data Firehose. Implement code in microservice 2 to read from Kinesis Data Firehose” is incorrect as this is not how Firehose works. Firehose sends data directly to destinations; it is not a message queue.

**References:**

* Amazon Simple Queue Service > Developer Guide > [What is Amazon Simple Queue Service?](https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html)

#### Exam Question 3

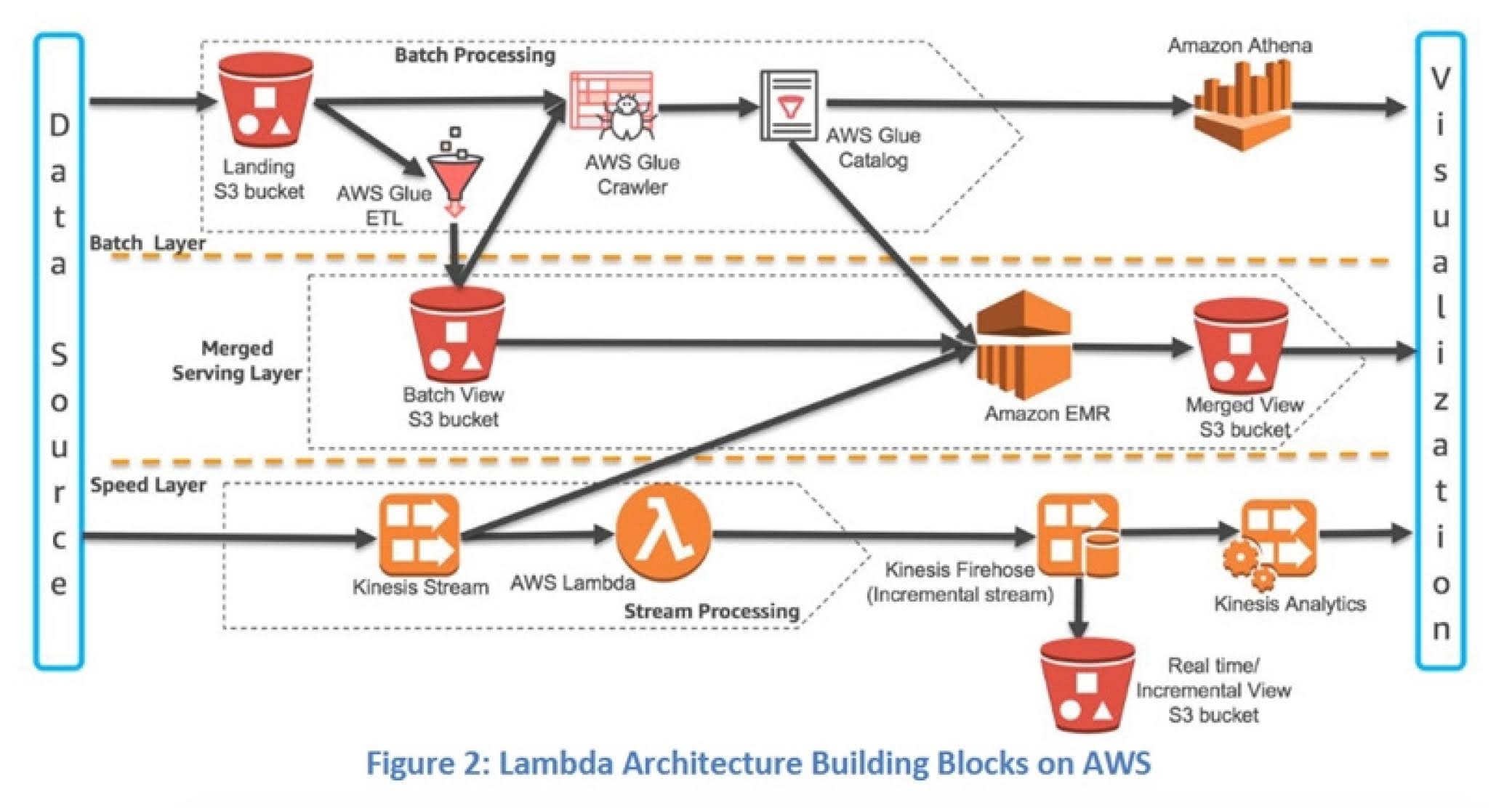
A company captures clickstream data from multiple websites and analyzes it using batch processing. The data is loaded nightly into Amazon Redshift and is consumed by business analysts. The company wants to move towards near-real-time data processing for timely insights. The solution should process the streaming data with minimal effort and operational overhead.

Which combination of AWS services is MOST cost-effective for this solution? (Choose two.)

A. Amazon EC2  
B. AWS Lambda  
C. Amazon Kinesis Data Streams  
D. Amazon Kinesis Data Firehose  
E. Amazon Kinesis Data Analytics

**Correct Answer:**  
A. Amazon EC2  
D. Amazon Kinesis Data Firehose

**Answer Description:**  
Kinesis Data Streams and Kinesis Client Library (KCL) – Data from the data source can be continuously captured and streamed in near real-time using Kinesis Data Streams. With the Kinesis Client Library (KCL), you can build your own application that can preprocess the streaming data as they arrive and emit the data for generating incremental views and downstream analysis. Kinesis Data Analytics – This service provides the easiest way to process the data that is streaming through Kinesis Data Stream or Kinesis Data Firehose using SQL. This enables customers to gain actionable insight in near real-time from the incremental stream before storing it in Amazon S3.



**References:**

* [Evolve from batch to real-time analytics](https://aws.amazon.com/kinesis/#Evolve_from_batch_to_real-time_analytics)

#### Exam Question 4

A company’s application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. On the first day of every month at midnight, the application becomes much slower when the month-end financial calculation batch executes. This causes the CPU utilization of the EC2 instances to immediately peak to 100%, which disrupts the application.

What should a solutions architect recommend to ensure the application is able to handle the workload and avoid downtime?

A. Configure an Amazon CloudFront distribution in front of the ALB.  
B. Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization.  
C. Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule.  
D. Configure Amazon ElastiCache to remove some of the workload from the EC2 instances.

**Correct Answer:**  
C. Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule.

**Answer Description:**  
Scheduled Scaling for Amazon EC2 Auto Scaling  
Scheduled scaling allows you to set your own scaling schedule. For example, let’s say that every week the traffic to your web application starts to increase on Wednesday, remains high on Thursday, and starts to decrease on Friday. You can plan your scaling actions based on the predictable traffic patterns of your web application. Scaling actions are performed automatically as a function of time and date.

Scheduled scaling allows you to set your own scaling schedule. In this case the scaling action can be scheduled to occur just prior to the time that the reports will be run each month. Scaling actions are performed automatically as a function of time and date. This will ensure that there are enough EC2 instances to serve the demand and prevent the application from slowing down.

CORRECT: “Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule” is the correct answer.

INCORRECT: “Configure an Amazon CloudFront distribution in front of the ALB” is incorrect as this would be more suitable for providing access to global users by caching content.

INCORRECT: “Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization” is incorrect as this would not prevent the slow-down from occurring as there would be a delay between when the CPU hits 100% and the metric being reported and additional instances being launched.

INCORRECT: “Configure Amazon ElastiCache to remove some of the workload from the EC2 instances” is incorrect as ElastiCache is a database cache, it cannot replace the compute functions of an EC2 instance.

**References:**

* Amazon EC2 Auto Scaling > User Guide > [Scheduled scaling for Amazon EC2 Auto Scaling](https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html)

#### Exam Question 5

A company runs a multi-tier web application that hosts news content. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones and use an Amazon Aurora database. A solutions architect needs to make the application more resilient to periodic increases in request rates.

Which architecture should the solutions architect implement? (Choose two.)

A. Add AWS Shield.  
B. Add Aurora Replica.  
C. Add AWS Direct Connect.  
D. Add AWS Global Accelerator.  
E. Add an Amazon CloudFront distribution in front of the Application Load Balancer.

**Correct Answer:**  
B. Add Aurora Replica.  
E. Add an Amazon CloudFront distribution in front of the Application Load Balancer.

**Answer Description:**  
AWS Global Accelerator: Acceleration for latency-sensitive applications. Many applications, especially in areas such as gaming, media, mobile apps, and financials, require very low latency for a great user experience. To improve the user experience, Global Accelerator directs user traffic to the application endpoint that is nearest to the client, which reduces internet latency and jitter.  
Global Accelerator routes traffic to the closest edge location by using Anycast, and then routes it to the closest regional endpoint over the AWS global network. Global Accelerator quickly reacts to changes in network performance to improve your users’ application performance.

Amazon CloudFront: Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment.

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.

INCORRECT: “Add and Amazon WAF in front of the ALB” is incorrect. A web application firewall protects applications from malicious attacks. It does not improve performance.

INCORRECT: “Add an Amazon Transit Gateway to the Availability Zones” is incorrect as this is used to connect on-premises networks to VPCs.

INCORRECT: “Add an Amazon Global Accelerator endpoint” is incorrect as this service is used for directing users to different instances of the application in different regions based on latency.

**References:**

* Amazon Aurora > User Guide for Aurora > [Replication with Amazon Aurora](https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html)
* Amazon CloudFront > Developer Guide > [What is Amazon CloudFront?](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html)

#### Exam Question 6

A product team is creating a new application that will store a large amount of data. The data will be analyzed hourly and modified by multiple Amazon EC2 Linux instances. The application team believes the amount of space needed will continue to grow for the next 6 months.

Which set of actions should a solutions architect take to support these needs?

A. Store the data in an Amazon EBS volume. Mount the EBS volume on the application instances.  
B. Store the data in an Amazon EFS file system. Mount the file system on the application instances.  
C. Store the data in Amazon S3 Glacier. Update the vault policy to allow access to the application instances.  
D. Store the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA). Update the bucket policy to allow access to the application instances.

**Correct Answer:**  
B. Store the data in an Amazon EFS file system. Mount the file system on the application instances.

**Answer Description:**  
Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. It is built to scale on demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth.

“The data will be analyzed hourly and modified by multiple Amazon EC2 Linux instances.”

Amazon EFS is designed to provide massively parallel shared access to thousands of Amazon EC2 instances, enabling your applications to achieve high levels of aggregate throughput and IOPS with consistent low latencies.

Amazon EFS is well suited to support a broad spectrum of use cases from home directories to business-critical applications. Customers can use EFS to lift-and-shift existing enterprise applications to the AWS Cloud. Other use cases include big data analytics, web serving and content management, application development and testing, media and entertainment workflows, database backups, and container storage.

Amazon EFS is a regional service storing data within and across multiple Availability Zones (AZs) for high availability and durability. Amazon EC2 instances can access your file system across AZs, regions, and VPCs, while on-premises servers can access using AWS Direct Connect or AWS VPN.

#### Exam Question 7

A company is migrating a three-tier application to AWS. The application requires a MySQL database. In the past, the application users reported poor application performance when creating new entries. These performance issues were caused by users generating different real-time reports from the application during working hours.

Which solution will improve the performance of the application when it is moved to AWS?

A. Import the data into an Amazon DynamoDB table with provisioned capacity. Refactor the application to use DynamoDB for reports.  
B. Create the database on a compute optimized Amazon EC2 instance. Ensure compute resources exceed the on-premises database.  
C. Create an Amazon Aurora MySQL Multi-AZ DB cluster with multiple read replicas. Configure the application to use the reader endpoint for reports.  
D. Create an Amazon Aurora MySQL Multi-AZ DB cluster. Configure the application to use the backup instance of the cluster as an endpoint for the reports.

**Correct Answer:**  
C. Create an Amazon Aurora MySQL Multi-AZ DB cluster with multiple read replicas. Configure the application to use the reader endpoint for reports.

**Answer Description:**  
Amazon RDS Read Replicas Now Support Multi-AZ Deployments

Starting today, Amazon RDS Read Replicas for MySQL and MariaDB now support Multi-AZ deployments. Combining Read Replicas with Multi-AZ enables you to build a resilient disaster recovery strategy and simplify your database engine upgrade process.

Amazon RDS Read Replicas enable you to create one or more read-only copies of your database instance within the same AWS Region or in a different AWS Region. Updates made to the source database are then asynchronously copied to your Read Replicas. In addition to providing scalability for read-heavy workloads, Read Replicas can be promoted to become a standalone database instance when needed.

Amazon RDS Multi-AZ deployments provide enhanced availability for database instances within a single AWS Region. With Multi-AZ, your data is synchronously replicated to a standby in a different Availability Zone (AZ). In the event of an infrastructure failure, Amazon RDS performs an automatic failover to the standby, minimizing disruption to your applications.

You can now use Read Replicas with Multi-AZ as part of a disaster recovery (DR) strategy for your production databases. A well-designed and tested DR plan is critical for maintaining business continuity after a disaster. A Read Replica in a different region than the source database can be used as a standby database and promoted to become the new production database in case of a regional disruption.

You can also combine Read Replicas with Multi-AZ for your database engine upgrade process. You can create a Read Replica of your production database instance and upgrade it to a new database engine version. When the upgrade is complete, you can stop applications, promote the Read Replica to a standalone database instance, and switch over your applications. Since the database instance is already a Multi-AZ deployment, no additional steps are needed.

Overview of Amazon RDS Read Replicas

Deploying one or more read replicas for a given source DB instance might make sense in a variety of scenarios, including the following:

Scaling beyond the compute or I/O capacity of a single DB instance for read-heavy database workloads. You can direct this excess read traffic to one or more read replicas.

Serving read traffic while the source DB instance is unavailable. In some cases, your source DB instance might not be able to take I/O requests, for example due to I/O suspension for backups or scheduled maintenance. In these cases, you can direct read traffic to your read replicas. For this use case, keep in mind that the data on the read replica might be “stale” because the source DB instance is unavailable.

Business reporting or data warehousing scenarios where you might want business reporting queries to run against a read replica, rather than your primary, production DB instance.

Implementing disaster recovery. You can promote a read replica to a standalone instance as a disaster recovery solution if the source DB instance fails.

The MySQL-compatible edition of Aurora delivers up to 5X the throughput of standard MySQL running on the same hardware, and enables existing MySQL applications and tools to run without requiring modification.

**References:**

* [Amazon Aurora Features: MySQL-Compatible Edition](https://aws.amazon.com/rds/aurora/mysql-features/)

#### Exam Question 8

A solutions architect is deploying a distributed database on multiple Amazon EC2 instances. The database stores all data on multiple instances so it can withstand the loss of an instance. The database requires block storage with latency and throughput to support several million transactions per second per server.

Which storage solution should the solutions architect use?

A. Amazon EBS  
B. Amazon EC2 instance store  
C. Amazon EFS  
D. Amazon S3

**Correct Answer:**  
B. Amazon EC2 instance store

**Answer Description:**  
It is block storage made for high throughput and low latency.

**References:**

* Amazon Elastic Compute Cloud > User Guide for Linux Instances > [Amazon EC2 instance store](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html)

#### Exam Question 9

Organizers for a global event want to put daily reports online as static HTML pages. The pages are expected to generate millions of views from users 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?

A. Generate presigned URLs for the files.  
B. Use cross-Region replication to all Regions.  
C. Use the geoproximity feature of Amazon Route 53.  
D. Use Amazon CloudFront with the S3 bucket as its origin.

**Correct Answer:**  
D. Use Amazon CloudFront with the S3 bucket as its origin.

**Answer Description:**  
Using Amazon S3 Origins, MediaPackage Channels, and Custom Origins for Web Distributions

Using Amazon S3 Buckets for Your Origin  
When you use Amazon S3 as an origin for your distribution, you place any objects that you want CloudFront to deliver in an Amazon S3 bucket. You can use any method that is supported by Amazon S3 to get your objects into Amazon S3, for example, the Amazon S3 console or API, or a third-party tool. You can create a hierarchy in your bucket to store the objects, just as you would with any other Amazon S3 bucket.

Using an existing Amazon S3 bucket as your CloudFront origin server doesn’t change the bucket in any way; you can still use it as you normally would to store and access Amazon S3 objects at the standard Amazon S3 price. You incur regular Amazon S3 charges for storing the objects in the bucket.

Using Amazon S3 Buckets Configured as Website Endpoints for Your Origin  
You can set up an Amazon S3 bucket that is configured as a website endpoint as custom origin with CloudFront.

When you configure your CloudFront distribution, for the origin, enter the Amazon S3 static website hosting endpoint for your bucket. This value appears in the Amazon S3 console, on the Properties tab, in the Static website hosting pane. For example: http://bucket-name.s3-website-region.amazonaws.com

For more information about specifying Amazon S3 static website endpoints, see Website endpoints in the Amazon Simple Storage Service Developer Guide.

When you specify the bucket name in this format as your origin, you can use Amazon S3 redirects and Amazon S3 custom error documents. For more information about Amazon S3 features, see the Amazon S3 documentation.

Using an Amazon S3 bucket as your CloudFront origin server doesn’t change it in any way. You can still use it as you normally would and you incur regular Amazon S3 charges.

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) 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.

INCORRECT: “Generate presigned URLs for the files” is incorrect as this is used to restrict access which is not a requirement.

INCORRECT: “Use cross-Region replication to all Regions” is incorrect as this does not provide a mechanism for directing users to the closest copy of the static webpages.

INCORRECT: “Use the geoproximity feature of Amazon Route 53” is incorrect as this does not include a solution for having multiple copies of the data in different geographic locations.

**References:**

* [How do I use CloudFront to serve a static website hosted on Amazon S3?](https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-serve-static-website/)

#### Exam Question 10

A start-up company has a web application based in the us-east-1 Region with multiple Amazon EC2 instances running behind an Application Load Balancer across multiple Availability Zones. As the company’s user base grows in the us-west-1 Region, it needs a solution with low latency and high availability.

What should a solutions architect do to accomplish this?

A. Provision EC2 instances in us-west-1. Switch the Application Load Balancer to a Network Load Balancer to achieve cross-Region load balancing.  
B. Provision EC2 instances and an Application Load Balancer in us-west-1. Make the load balancer distribute the traffic based on the location of the request.  
C. Provision EC2 instances and configure an Application Load Balancer in us-west-1. Create an accelerator in AWS Global Accelerator that uses an endpoint group that includes the load balancer endpoints in both Regions.  
D. Provision EC2 instances and configure an Application Load Balancer in us-west-1. Configure Amazon Route 53 with a weighted routing policy. Create alias records in Route 53 that point to the Application Load Balancer.

**Correct Answer:**  
C. Provision EC2 instances and configure an Application Load Balancer in us-west-1. Create an accelerator in AWS Global Accelerator that uses an endpoint group that includes the load balancer endpoints in both Regions.

**Answer Description:**  
Register endpoints for endpoint groups: You register one or more regional resources, such as Application Load Balancers, Network Load Balancers, EC2 Instances, or Elastic IP addresses, in each endpoint group. Then you can set weights to choose how much traffic is routed to each endpoint.

Endpoints in AWS Global Accelerator: Endpoints in AWS Global Accelerator can be Network Load Balancers, Application Load Balancers, Amazon EC2 instances, or Elastic IP addresses. A static IP address serves as a single point of contact for clients, and Global Accelerator then distributes incoming traffic across healthy endpoints. Global Accelerator directs traffic to endpoints by using the port (or port range) that you specify for the listener that the endpoint group for the endpoint belongs to.

Each endpoint group can have multiple endpoints. You can add each endpoint to multiple endpoint groups, but the endpoint groups must be associated with different listeners.

Global Accelerator continually monitors the health of all endpoints that are included in an endpoint group. It routes traffic only to the active endpoints that are healthy. If Global Accelerator doesn’t have any healthy endpoints to route traffic to, it routes traffic to all endpoints.

ELB provides load balancing within one Region, AWS Global Accelerator provides traffic management across multiple Regions […] AWS Global Accelerator complements ELB by extending these capabilities beyond a single AWS Region, allowing you to provision a global interface for your applications in any number of Regions. If you have workloads that cater to a global client base, we recommend that you use AWS Global Accelerator. If you have workloads hosted in a single AWS Region and used by clients in and around the same Region, you can use an Application Load Balancer or Network Load Balancer to manage your resources.

#### Exam Question 11

A solutions architect is designing a solution to access a catalog of images and provide users with the ability to submit requests to customize images. Image customization parameters will be in any request sent to an AWS API Gateway API. The customized image will be generated on demand, and users will receive a link they can click to view or download their customized image. The solution must be highly available for viewing and customizing images.

What is the MOST cost-effective solution to meet these requirements?

A. Use Amazon EC2 instances to manipulate the original image into the requested customization. Store the original and manipulated images in Amazon S3. Configure an Elastic Load Balancer in front of the EC2 instances.  
B. Use AWS Lambda to manipulate the original image to the requested customization. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.  
C. Use AWS Lambda to manipulate the original image to the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Elastic Load Balancer in front of the Amazon EC2 instances.  
D. Use Amazon EC2 instances to manipulate the original image into the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.

**Correct Answer:**  
B. Use AWS Lambda to manipulate the original image to the requested customization. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.

**Answer Description:**  
AWS Lambda is a compute service that lets you run code without provisioning or managing servers. AWS Lambda executes your code only when needed and scales automatically, from a few requests per day to thousands per second. You pay only for the compute time you consume – there is no charge when your code is not running. With AWS Lambda, you can run code for virtually any type of application or backend service – all with zero administration. AWS Lambda runs your code on a high-availability compute infrastructure and performs all of the administration of the compute resources, including server and operating system maintenance, capacity provisioning and automatic scaling, code monitoring, and logging.

All you need to do is supply your code in one of the languages that AWS Lambda supports.

Storing your static content with S3 provides a lot of advantages. But to help optimize your application’s performance and security while effectively managing cost, we recommend that you also set up Amazon CloudFront to work with your S3 bucket to serve and protect the content. CloudFront is a content delivery network (CDN) service that delivers static and dynamic web content, video streams, and APIs around the world, securely and at scale. By design, delivering data out of CloudFront can be more cost effective than delivering it from S3 directly to your users.

CloudFront serves content through a worldwide network of data centers called Edge Locations. Using edge servers to cache and serve content improves performance by providing content closer to where viewers are located. CloudFront has edge servers in locations all around the world.

All solutions presented are highly available. The key requirement that must be satisfied is that the solution should be cost-effective and you must choose the most cost-effective option.

Therefore, it’s best to eliminate services such as Amazon EC2 and ELB as these require ongoing costs even when they’re not used. Instead, a fully serverless solution should be used. AWS Lambda, Amazon S3 and CloudFront are the best services to use for these requirements.

CORRECT: “Use AWS Lambda to manipulate the original images to the requested customization. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin” is the correct answer.

INCORRECT: “Use Amazon EC2 instances to manipulate the original images into the requested customization. Store the original and manipulated images in Amazon S3. Configure an Elastic Load Balancer in front of the EC2 instances” is incorrect. This is not the most cost-effective option as the ELB and EC2 instances will incur costs even when not used.

INCORRECT: “Use AWS Lambda to manipulate the original images to the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Elastic Load Balancer in front of the Amazon EC2 instances” is incorrect. This is not the most cost-effective option as the ELB will incur costs even when not used. Also, Amazon DynamoDB will incur RCU/WCUs when running and is not the best choice for storing images.

INCORRECT: “Use Amazon EC2 instances to manipulate the original images into the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Amazon CloudFront distribution with the S3 bucket as the origin” is incorrect. This is not the most cost-effective option as the EC2 instances will incur costs even when not used.

**References:**

* [Serverless on AWS](https://aws.amazon.com/serverless/)

#### Exam Question 12

A company is planning to migrate a business-critical dataset to Amazon S3. The current solution design uses a single S3 bucket in the us-east-1 Region with versioning enabled to store the dataset. The company’s disaster recovery policy states that all data multiple AWS Regions.

How should a solutions architect design the S3 solution?

A. Create an additional S3 bucket in another Region and configure cross-Region replication.  
B. Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS).  
C. Create an additional S3 bucket with versioning in another Region and configure cross-Region replication.  
D. Create an additional S3 bucket with versioning in another Region and configure cross-origin resource (CORS).

**Correct Answer:**  
C. Create an additional S3 bucket with versioning in another Region and configure cross-Region replication.

**Answer Description:**  
Replication enables automatic, asynchronous copying of objects across Amazon S3 buckets. Buckets that are configured for object replication can be owned by the same AWS account or by different accounts. You can copy objects between different AWS Regions or within the same Region. Both source and destination buckets must have versioning enabled.

CORRECT: “Create an additional S3 bucket with versioning in another Region and configure cross-Region replication” is the correct answer.

INCORRECT: “Create an additional S3 bucket in another Region and configure cross-Region replication” is incorrect as the destination bucket must also have versioning enabled.

INCORRECT: “Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS)” is incorrect as CORS is not related to replication.

INCORRECT: “Create an additional S3 bucket with versioning in another Region and configure cross-origin resource sharing (CORS)” is incorrect as CORS is not related to replication.

**References:**  
Amazon Simple Storage Service > User Guide > [Replicating objects](https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication.html)

#### Exam Question 13

A company has application running on Amazon EC2 instances in a VPC. One of the applications needs to call an Amazon S3 API to store and read objects. The company’s security policies restrict any internet-bound traffic from the applications.

Which action will fulfill these requirements and maintain security?

A. Configure an S3 interface endpoint.  
B. Configure an S3 gateway endpoint.  
C. Create an S3 bucket in a private subnet.  
D. Create an S3 bucket in the same Region as the EC2 instance.

**Correct Answer:**  
B. Configure an S3 gateway endpoint.

**Answer Description:**  
VPC endpoints: A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

An interface endpoint is an elastic network interface with a private IP address from the IP address range of your subnet that serves as an entry point for traffic destined to a supported service. Interface endpoints are powered by AWS PrivateLink, a technology that enables you to privately access services by using private IP addresses. AWS PrivateLink restricts all network traffic between your VPC and services to the Amazon network. You do not need an internet gateway, a NAT device, or a virtual private gateway.

**References:**

* Amazon Virtual Private Cloud > AWS PrivateLink > [Endpoints for Amazon S3](https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html)
* Amazon Virtual Private Cloud > AWS PrivateLink > [Gateway VPC endpoints](https://docs.aws.amazon.com/vpc/latest/privatelink/vpce-gateway.html)

#### Exam Question 14

A company’s web application uses an Amazon RDS PostgreSQL DB instance to store its application data.

During the financial closing period at the start of every month, Accountants run large queries that impact the database’s performance due to high usage. The company wants to minimize the impact that the reporting activity has on the web application.

What should a solutions architect do to reduce the impact on the database with the LEAST amount of effort?

A. Create a read replica and direct reporting traffic to the replica.  
B. Create a Multi-AZ database and direct reporting traffic to the standby.  
C. Create a cross-Region read replica and direct reporting traffic to the replica.  
D. Create an Amazon Redshift database and direct reporting traffic to the Amazon Redshift database.

**Correct Answer:**  
A. Create a read replica and direct reporting traffic to the replica.

**Answer Description:**  
Amazon RDS uses the MariaDB, MySQL, Oracle, PostgreSQL, and Microsoft SQL Server DB engines’ built-in replication functionality to create a special type of DB instance called a read replica from a source DB instance. Updates made to the source DB instance are asynchronously copied to the read replica. You can reduce the load on your source DB instance by routing read queries from your applications to the read replica.

When you create a read replica, you first specify an existing DB instance as the source. Then Amazon RDS takes a snapshot of the source instance and creates a read-only instance from the snapshot. Amazon RDS then uses the asynchronous replication method for the DB engine to update the read replica whenever there is a change to the source DB instance. The read replica operates as a DB instance that allows only read-only connections. Applications connect to a read replica the same way they do to any DB instance.

Amazon RDS replicates all databases in the source DB instance.

**References:**

* Amazon Relational Database Service > User Guide > [Working with read replicas](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html)

#### Exam Question 15

A solutions architect needs to ensure that API calls to Amazon DynamoDB from Amazon EC2 instances in a VPC do not traverse the internet.

What should the solutions architect do to accomplish this? (Choose two.)

A. Create a route table entry for the endpoint.  
B. Create a gateway endpoint for DynamoDB.  
C. Create a new DynamoDB table that uses the endpoint.  
D. Create an ENI for the endpoint in each of the subnets of the VPC.  
E. Create a security group entry in the default security group to provide access.

**Correct Answer:**  
A. Create a route table entry for the endpoint.  
B. Create a gateway endpoint for DynamoDB.

**Answer Description:**  
A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection.

Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

Gateway endpoints: A gateway endpoint is a gateway that you specify as a target for a route in your route table for traffic destined to a supported AWS service. The following AWS services are supported:  
Amazon S3  
DynamoDB

Amazon DynamoDB and Amazon S3 support gateway endpoints, not interface endpoints. With a gateway endpoint you create the endpoint in the VPC, attach a policy allowing access to the service, and then specify the route table to create a route table entry in.

CORRECT: “Create a route table entry for the endpoint” is a correct answer. CORRECT: “Create a gateway endpoint for DynamoDB” is also a correct answer.

INCORRECT: “Create a new DynamoDB table that uses the endpoint” is incorrect as it is not necessary to create a new DynamoDB table.

INCORRECT: “Create an ENI for the endpoint in each of the subnets of the VPC” is incorrect as an ENI is used by an interface endpoint, not a gateway endpoint.

INCORRECT: “Create a VPC peering connection between the VPC and DynamoDB” is incorrect as you cannot create a VPC peering connection between a VPC and a public AWS service as public services are outside of VPCs.

**References:** Amazon Virtual Private Cloud > AWS PrivateLink > [Gateway VPC endpoints](https://docs.aws.amazon.com/vpc/latest/privatelink/vpce-gateway.html)

#### Exam Question 16

A company has been storing analytics data in an Amazon RDS instance for the past few years. The company asked a solutions architect to find a solution that allows users to access this data using an API.

The expectation is that the application will experience periods of inactivity but could receive bursts of traffic within seconds.

Which solution should the solution architect suggest?

A. Set up an Amazon API Gateway and use Amazon ECS.  
B. Set up an Amazon API Gateway and use AWS Elastic Beanstalk.  
C. Set up an Amazon API Gateway and use AWS Lambda functions.  
D. Set up an Amazon API Gateway and use Amazon EC2 with Auto Scaling.

**Correct Answer:**  
C. Set up an Amazon API Gateway and use AWS Lambda functions.

**Answer Description:**  
AWS Lambda: With Lambda, you can run code for virtually any type of application or backend service – all with zero administration. Just upload your code and Lambda takes care of everything required to run and scale your code with high availability. You can set up your code to automatically trigger from other AWS services or call it directly from any web or mobile app.

How it works  
  
Amazon API Gateway: Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. APIs act as the “front door” for applications to access data, business logic, or functionality from your backend services. Using API Gateway, you can create RESTful APIs and WebSocket APIs that enable real-time two-way communication applications. API Gateway supports containerized and serverless workloads, as well as web applications.

API Gateway handles all the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls, including traffic management, CORS support, authorization and access control, throttling, monitoring, and API version management. API Gateway has no minimum fees or startup costs.

You pay for the API calls you receive and the amount of data transferred out and, with the API Gateway tiered pricing model, you can reduce your cost as your API usage scales.

This question is simply asking you to work out the best compute service for the stated requirements. The key requirements are that the compute service should be suitable for a workload that can range quite broadly in demand from no requests to large bursts of traffic. AWS Lambda is an ideal solution as you pay only when requests are made and it can easily scale to accommodate the large bursts in traffic. Lambda works well with both API Gateway and Amazon RDS.

CORRECT: “Set up an Amazon API Gateway and use AWS Lambda functions” is the correct answer.

INCORRECT: “Set up an Amazon API Gateway and use Amazon ECS” is incorrect as Lambda is a better fit for this use case as the traffic patterns are highly dynamic.

INCORRECT: “Set up an Amazon API Gateway and use AWS Elastic Beanstalk” is incorrect as Lambda is a better fit for this use case as the traffic patterns are highly dynamic.

INCORRECT: “Set up an Amazon API Gateway and use Amazon EC2 with Auto Scaling” is incorrect as Lambda is a better fit for this use case as the traffic patterns are highly dynamic.

**References:**

AWS Lambda > Developer Guide > [Lambda function scaling](https://docs.aws.amazon.com/lambda/latest/dg/invocation-scaling.html)

#### Exam Question 17

A company must generate sales reports at the beginning of every month. The reporting process launches 20 Amazon EC2 instances on the first of the month. The process runs for 7 days and cannot be interrupted.

The company wants to minimize costs. Which pricing model should the company choose?

A. Reserved Instances  
B. Spot Block Instances  
C. On-Demand Instances  
D. Scheduled Reserved Instances

**Correct Answer:**  
D. Scheduled Reserved Instances

**Answer Description:**  
Scheduled Reserved Instances: Scheduled Reserved Instances (Scheduled Instances) enable you to purchase capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term. You reserve the capacity in advance, so that you know it is available when you need it. You pay for the time that the instances are scheduled, even if you do not use them.

Scheduled Instances are a good choice for workloads that do not run continuously, but do run on a regular schedule. For example, you can use Scheduled Instances for an application that runs during business hours or for batch processing that runs at the end of the week.

If you require a capacity reservation on a continuous basis, Reserved Instances might meet your needs and decrease costs.

**How Scheduled Instances Work**

Amazon EC2 sets aside pools of EC2 instances in each Availability Zone for use as Scheduled Instances.

Each pool supports a specific combination of instance type, operating system, and network.

To get started, you must search for an available schedule. You can search across multiple pools or a single pool. After you locate a suitable schedule, purchase it.

You must launch your Scheduled Instances during their scheduled time periods, using a launch configuration that matches the following attributes of the schedule that you purchased: instance type, Availability Zone, network, and platform. When you do so, Amazon EC2 launches EC2 instances on your behalf, based on the specified launch specification. Amazon EC2 must ensure that the EC2 instances have terminated by the end of the current scheduled time period so that the capacity is available for any other Scheduled Instances it is reserved for. Therefore, Amazon EC2 terminates the EC2 instances three minutes before the end of the current scheduled time period.

You can’t stop or reboot Scheduled Instances, but you can terminate them manually as needed. If you terminate a Scheduled Instance before its current scheduled time period ends, you can launch it again after a few minutes. Otherwise, you must wait until the next scheduled time period.

The following diagram illustrates the lifecycle of a Scheduled Instance.

**References:**

* Amazon Elastic Compute Cloud > User Guide for Linux Instances > [Scheduled Reserved Instances](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html)

#### Exam Question 18

A gaming company has multiple Amazon EC2 instances in a single Availability Zone for its multiplayer game that communicates with users on Layer 4. The chief technology officer (CTO) wants to make the architecture highly available and cost-effective.  
What should a solutions architect do to meet these requirements? (Choose two.)?

A. Increase the number of EC2 instances.  
B. Decrease the number of EC2 instances.  
C. Configure a Network Load Balancer in front of the EC2 instances.  
D. Configure an Application Load Balancer in front of the EC2 instances.  
E. Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically.

**Correct Answer:**  
C. Configure a Network Load Balancer in front of the EC2 instances.  
E. Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically.

**Answer Description:**  
Network Load Balancer overview: A Network Load Balancer functions at the fourth layer of the Open Systems Interconnection (OSI) model. It can handle millions of requests per second. After the load balancer receives a connection request, it selects a target from the target group for the default rule. It attempts to open a TCP connection to the selected target on the port specified in the listener configuration.

When you enable an Availability Zone for the load balancer, Elastic Load Balancing creates a load balancer node in the Availability Zone. By default, each load balancer node distributes traffic across the registered targets in its Availability Zone only. If you enable cross-zone load balancing, each load balancer node distributes traffic across the registered targets in all enabled Availability Zones. For more information, see Availability Zones.

If you enable multiple Availability Zones for your load balancer and ensure that each target group has at least one target in each enabled Availability Zone, this increases the fault tolerance of your applications. For example, if one or more target groups does not have a healthy target in an Availability Zone, we remove the IP address for the corresponding subnet from DNS, but the load balancer nodes in the other Availability Zones are still available to route traffic. If a client doesn’t honor the time-to-live (TTL) and sends requests to the IP address after it is removed from DNS, the requests fail.

For TCP traffic, the load balancer selects a target using a flow hash algorithm based on the protocol, source IP address, source port, destination IP address, destination port, and TCP sequence number. The TCP connections from a client have different source ports and sequence numbers, and can be routed to different targets. Each individual TCP connection is routed to a single target for the life of the connection.

For UDP traffic, the load balancer selects a target using a flow hash algorithm based on the protocol, source IP address, source port, destination IP address, and destination port. A UDP flow has the same source and destination, so it is consistently routed to a single target throughout its lifetime. Different UDP flows have different source IP addresses and ports, so they can be routed to different targets.

An Auto Scaling group contains a collection of Amazon EC2 instances that are treated as a logical grouping for the purposes of automatic scaling and management. An Auto Scaling group also enables you to use Amazon EC2 Auto Scaling features such as health check replacements and scaling policies. Both maintaining the number of instances in an Auto Scaling group and automatic scaling are the core functionality of the Amazon EC2 Auto Scaling service.

The size of an Auto Scaling group depends on the number of instances that you set as the desired capacity. You can adjust its size to meet demand, either manually or by using automatic scaling.

An Auto Scaling group starts by launching enough instances to meet its desired capacity. It maintains this number of instances by performing periodic health checks on the instances in the group. The Auto Scaling group continues to maintain a fixed number of instances even if an instance becomes unhealthy. If an instance becomes unhealthy, the group terminates the unhealthy instance and launches another instance to replace it.

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.

CORRECT: “Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically” is also a correct answer.

INCORRECT: “Increase the number of instances and use smaller EC2 instance types” is incorrect as this is not the most cost-effective option. Auto Scaling should be used to maintain the right number of active instances.

INCORRECT: “Configure an Auto Scaling group to add or remove instances in the Availability Zone automatically” is incorrect as this is not highly available as it’s a single AZ.

INCORRECT: “Configure an Application Load Balancer in front of the EC2 instances” is incorrect as an ALB operates at Layer 7 rather than Layer 4.

**References:**

* Amazon EC2 Auto Scaling > User Guide > [Elastic Load Balancing and Amazon EC2 Auto Scaling](https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html)

#### Exam Question 19

A solutions architect has created a new AWS account and must secure AWS account root user access.

Which combination of actions will accomplish this? (Choose two.)

A. Ensure the root user uses a strong password.  
B. Enable multi-factor authentication to the root user.  
C. Store root user access keys in an encrypted Amazon S3 bucket.  
D. Add the root user to a group containing administrative permissions.  
E. Apply the required permissions to the root user with an inline policy document.

**Correct Answer:**  
A. Ensure the root user uses a strong password.  
B. Enable multi-factor authentication to the root user.

**Answer Description:**  
“Enable MFA”  
The AWS Account Root User – https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_root- user.html  
“Choose a strong password”  
Changing the AWS Account Root User Password –

**References:**

* AWS Identity and Access Management > User Guide > [Changing the AWS account root user password](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_change-root.html)

#### Exam Question 20

A company’s website is used to sell products to the public. The site runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). There is also an Amazon CloudFront distribution, and AWS WAF is being used to protect against SQL injection attacks. The ALB is the origin for the CloudFront distribution. A recent 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. Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address.  
B. Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address.  
C. Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.  
D. Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.

**Correct Answer:**  
B. Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address.

**Answer Description:**  
If you want to allow or block web requests based on the IP addresses that the requests originate from, create one or more IP match conditions. An IP match condition lists up to 10,000 IP addresses or IP address ranges that your requests originate from. Later in the process, when you create a web ACL, you specify whether to allow or block requests from those IP addresses.

AWS Web Application Firewall (WAF) – Helps to protect your web applications from common application layer exploits that can affect availability or consume excessive resources. As you can see in my post (New – AWS WAF), WAF allows you to use access control lists (ACLs), rules, and conditions that define acceptable or unacceptable requests or IP addresses. You can selectively allow or deny access to specific parts of your web application and you can also guard against various SQL injection attacks. We launched WAF with support for Amazon CloudFront.

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.

INCORRECT: “Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address” is incorrect as CloudFront does not sit within a subnet so network ACLs do not apply to it.

INCORRECT: “Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address” is incorrect as the source IP addresses of the data in the EC2 instances’ subnets will be the ELB IP addresses.

INCORRECT: “Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.” is incorrect as you cannot create deny rules with security groups.

#### Exam Question 21

A web application is deployed in the AWS Cloud. It consists of a two-tier architecture that includes a web layer and a database layer. The web server is vulnerable to cross-site scripting (XSS) attacks.

What should a solutions architect do to remediate the vulnerability?

A. Create a Classic Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.  
B. Create a Network Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.  
C. Create an Application Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.  
D. Create an Application Load Balancer. Put the web layer behind the load balancer and use AWS Shield Standard.

**Correct Answer:**  
C. Create an Application Load Balancer. Put the web layer behind the load balancer and enable AWS WAF.

**Answer Description:**  
Working with cross-site scripting match conditions: Attackers sometimes insert scripts into web requests in an effort to exploit vulnerabilities in web applications. You can create one or more cross-site scripting match conditions to identify the parts of web requests, such as the URI or the query string, that you want AWS WAF Classic to inspect for possible malicious scripts. Later in the process, when you create a web ACL, you specify whether to allow or block requests that appear to contain malicious scripts.  
Web Application Firewall: You can now use AWS WAF to protect your web applications on your Application Load Balancers. AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.

The AWS Web Application Firewall (WAF) is available on the Application Load Balancer (ALB). You can use AWS WAF directly on Application Load Balancers (both internal and external) in a VPC, to protect your websites and web services.

Attackers sometimes insert scripts into web requests in an effort to exploit vulnerabilities in web applications. You can create one or more cross-site scripting match conditions to identify the parts of web requests, such as the URI or the query string, that you want AWS WAF to inspect for possible malicious scripts.

CORRECT: “Create an Application Load Balancer. Put the web layer behind the load balancer and enable AWS WAF” is the correct answer.

INCORRECT: “Create a Classic Load Balancer. Put the web layer behind the load balancer and enable AWS WAF” is incorrect as you cannot use AWS WAF with a classic load balancer.

INCORRECT: “Create a Network Load Balancer. Put the web layer behind the load balancer and enable AWS WAF” is incorrect as you cannot use AWS WAF with a network load balancer.

INCORRECT: “Create an Application Load Balancer. Put the web layer behind the load balancer and use AWS Shield Standard” is incorrect as you cannot use AWS Shield to protect against XSS attacks. Shield is used to protect against DDoS attacks.

**References:**AWS WAF, AWS Firewall Manager, and AWS Shield Advanced > Developer Guide > [Working with cross-site scripting match conditions](https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-xss-conditions.html)

#### Exam Question 22

A company’s website is using an Amazon RDS MySQL Multi-AZ DB instance for its transactional data storage. There are other internal systems that query this DB instance to fetch data for internal batch processing. The RDS DB instance slows down significantly when the internal systems fetch data. This impacts the website’s read and write performance, and the users experience slow response times.

Which solution will improve the website’s performance?

A. Use an RDS PostgreSQL DB instance instead of a MySQL database.  
B. Use Amazon ElastiCache to cache the query responses for the website.  
C. Add an additional Availability Zone to the current RDS MySQL Multi-AZ DB instance.  
D. Add a read replica to the RDS DB instance and configure the internal systems to query the read replica.

**Correct Answer:**  
D. Add a read replica to the RDS DB instance and configure the internal systems to query the read replica.

**Answer Description:**  
Amazon RDS Read Replicas  
Enhanced performance  
You can reduce the load on your source DB instance by routing read queries from your applications to the read replica. Read replicas allow you to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. Because read replicas can be promoted to master status, they are useful as part of a sharding implementation.

To further maximize read performance, Amazon RDS for MySQL allows you to add table indexes directly to Read Replicas, without those indexes being present on the master.

#### Exam Question 23

A financial services company has a web application that serves users in the United States and Europe. The application consists of a database tier and a web server tier. The database tier consists of a MySQL database hosted in us-east-1. Amazon Route 53 geoproximity routing is used to direct traffic to instances in the closest Region. A performance review of the system reveals that European users are not receiving the same level of query performance as those in the United States.

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

A. Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in one of the European Regions.  
B. Migrate the database to Amazon DynamoDB. Use DynamoDB global tables to enable replication to additional Regions.  
C. Deploy MySQL instances in each Region. Deploy an Application Load Balancer in front of MySQL to reduce the load on the primary instance.  
D. Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure read replicas in one of the European Regions.

**Correct Answer:**  
D. Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure read replicas in one of the European Regions.

**Answer Description:**  
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.

INCORRECT: “Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in the Australian Region” is incorrect. The database is located in UK. If the database is migrated to Australia then the reverse problem will occur. Multi-AZ does not assist with improving query performance across Regions.

INCORRECT: “Migrate the database to Amazon DynamoDB. Use DynamoDB global tables to enable replication to additional Regions” is incorrect as a relational database running on MySQL is unlikely to be compatible with DynamoDB.

INCORRECT: “Deploy MySQL instances in each Region. Deploy an Application Load Balancer in front of MySQL to reduce the load on the primary instance” is incorrect as you can only put ALBs in front of the web tier, not the DB tier.

**References:**

Amazon Aurora > User Guide for Aurora > [Using Amazon Aurora global databases](https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database.html)

#### Exam Question 24

A company is performing an AWS Well-Architected Framework review of an existing workload deployed on AWS. The review identified a public-facing website running on the same Amazon EC2 instance as a Microsoft Active Directory domain controller that was installed recently to support other AWS services. A solutions architect needs to recommend a new design that would improve the security of the architecture and minimize the administrative demand on IT staff.

What should the solutions architect recommend?

A. Use AWS Directory Service to create a managed Active Directory. Uninstall Active Directory on the current EC2 instance.  
B. Create another EC2 instance in the same subnet and reinstall Active Directory on it. Uninstall Active Directory.  
C. Use AWS Directory Service to create an Active Directory connector. Proxy Active Directory requests to the Active domain controller running on the current EC2 instance.  
D. Enable AWS Single Sign-On (AWS SSO) with Security Assertion Markup Language (SAML) 2.0 federation with the current Active Directory controller. Modify the EC2 instance’s security group to deny public access to Active Directory.

**Correct Answer:**  
A. Use AWS Directory Service to create a managed Active Directory. Uninstall Active Directory on the current EC2 instance.

**Answer Description:**  
AWS Managed Microsoft AD: AWS Directory Service lets you run Microsoft Active Directory (AD) as a managed service. AWS Directory Service for Microsoft Active Directory, also referred to as AWS Managed Microsoft AD, is powered by Windows Server 2012 R2. When you select and launch this directory type, it is created as a highly available pair of domain controllers connected to your virtual private cloud (VPC). The domain controllers run in different Availability Zones in a region of your choice. Host monitoring and recovery, data replication, snapshots, and software updates are automatically configured and managed for you.

Migrate AD to AWS Managed AD and keep the webserver alone. Reduce risk = remove AD from that EC2. Minimize admin = remove AD from any EC2

-> use AWS Directory Service

Active Directory connector is only for ON-PREM AD. The one they have exists in the cloud already.

#### Exam Question 25

A company hosts a static website within an Amazon S3 bucket. A solutions architect needs to ensure that data can be recovered in case of accidental deletion.

Which action will accomplish this?

A. Enable Amazon S3 versioning.  
B. Enable Amazon S3 Intelligent-Tiering.  
C. Enable an Amazon S3 lifecycle policy.  
D. Enable Amazon S3 cross-Region replication.

**Correct Answer:**  
A. Enable Amazon S3 versioning.

**Answer Description:**  
Data can be recover if versioning enable, also it provide a extra protection like file delete, MFA delete. MFA. Delete only works for CLI or API interaction, not in the AWS Management Console. Also, you cannot make version DELETE actions with MFA using IAM user credentials. You must use your root AWS account.

Object Versioning: Use Amazon S3 Versioning to keep multiple versions of an object in one bucket. For example, you could store my-image.jpg (version 111111) and my-image.jpg (version 222222) in a single bucket. S3 Versioning protects you from the consequences of unintended overwrites and deletions. You can also use it to archive objects so that you have access to previous versions.

You must explicitly enable S3 Versioning on your bucket. By default, S3 Versioning is disabled. Regardless of whether you have enabled Versioning, each object in your bucket has a version ID. If you have not enabled Versioning, Amazon S3 sets the value of the version ID to null. If S3 Versioning is enabled, Amazon S3 assigns a version ID value for the object. This value distinguishes it from other versions of the same key.

Object versioning is a means of keeping multiple variants of an object in the same Amazon S3 bucket. Versioning provides the ability to recover from both unintended user actions and application failures. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket.

CORRECT: “Enable Amazon S3 versioning” is the correct answer.

INCORRECT: “Enable Amazon S3 Intelligent-Tiering” is incorrect. This is a storage class that automatically moves data between frequent access and infrequent access classes based on usage patterns.

INCORRECT: “Enable an Amazon S3 lifecycle policy” is incorrect. An S3 lifecycle policy is a set of rules that define actions that apply to groups of S3 objects such as transitioning objects to another storage class.

INCORRECT: “Enable Amazon S3 cross-Region replication” is incorrect as this is used to copy objects to different regions. CRR relies on versioning which is the feature that is required for protecting against accidental deletion.

**References:** [Protecting Amazon S3 Against Object Deletion](https://d0.awsstatic.com/whitepapers/protecting-s3-against-object-deletion.pdf)

#### Exam Question 26

A company’s production application runs online transaction processing (OLTP) transactions on an Amazon RDS MySQL DB instance. The company is launching a new reporting tool that will access the same data.

The reporting tool must be highly available and not impact the performance of the production application.

How can this be achieved?

A. Create hourly snapshots of the production RDS DB instance.  
B. Create a Multi-AZ RDS Read Replica of the production RDS DB instance.  
C. Create multiple RDS Read Replicas of the production RDS DB instance. Place the Read Replicas in an Auto Scaling group.  
D. Create a Single-AZ RDS Read Replica of the production RDS DB instance. Create a second Single-AZ RDS Read Replica from the replica.

**Correct Answer:**  
B. Create a Multi-AZ RDS Read Replica of the production RDS DB instance.

**Answer Description:**  
Amazon RDS Read Replicas Now Support Multi-AZ Deployments

Amazon RDS Read Replicas enable you to create one or more read-only copies of your database instance within the same AWS Region or in a different AWS Region. Updates made to the source database are then asynchronously copied to your Read Replicas. In addition to providing scalability for read-heavy workloads, Read Replicas can be promoted to become a standalone database instance when needed.

Amazon RDS Multi-AZ deployments provide enhanced availability for database instances within a single AWS Region. With Multi-AZ, your data is synchronously replicated to a standby in a different Availability Zone (AZ). In the event of an infrastructure failure, Amazon RDS performs an automatic failover to the standby, minimizing disruption to your applications.

You can now use Read Replicas with Multi-AZ as part of a disaster recovery (DR) strategy for your production databases. A well-designed and tested DR plan is critical for maintaining business continuity after a disaster. A Read Replica in a different region than the source database can be used as a standby database and promoted to become the new production database in case of a regional disruption.

You can create a read replica as a Multi-AZ DB instance. Amazon RDS creates a standby of your replica in another Availability Zone for failover support for the replica. Creating your read replica as a Multi-AZ DB instance is independent of whether the source database is a Multi-AZ DB instance.

CORRECT: “Create a Multi-AZ RDS Read Replica of the production RDS DB instance” is the correct answer.

INCORRECT: “Create a Single-AZ RDS Read Replica of the production RDS DB instance. Create a second Single-AZ RDS Read Replica from the replica” is incorrect. Read replicas are primarily used for horizontal scaling. The best solution for high availability is to use a Multi-AZ read replica.

INCORRECT: “Create a cross-region Multi-AZ deployment and create a read replica in the second region” is incorrect as you cannot create a cross-region Multi-AZ deployment with RDS. INCORRECT: “Use Amazon Data Lifecycle Manager to automatically create and manage snapshots” is incorrect as using snapshots is not the best solution for high availability.

**References:** Amazon Relational Database Service > User Guide > [What is Amazon Relational Database Service (Amazon RDS)?](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html)

#### Exam Question 27

A company runs an application in a branch office within a small data closet with no virtualized compute resources. The application data is stored on an NFS volume. Compliance standards require a daily offsite backup of the NFS volume.

Which solution meet these requirements?

A. Install an AWS Storage Gateway file gateway on premises to replicate the data to Amazon S3.  
B. Install an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3.  
C. Install an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3.  
D. Install an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3.

**Correct Answer:**  
B. Install an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3.

**Answer Description:**  
AWS Storage Gateway Hardware Appliance  
Hardware Appliance: Storage Gateway is available as a hardware appliance, adding to the existing support for VMware ESXi, Microsoft Hyper-V, and Amazon EC2. This means that you can now make use of Storage Gateway in situations where you do not have a virtualized environment, server-class hardware or IT staff with the specialized skills that are needed to manage them. You can order appliances from Amazon.com for delivery to branch offices, warehouses, and “outpost” offices that lack dedicated IT resources. Setup (as you will see in a minute) is quick and easy, and gives you access to three storage solutions:

File Gateway: A file interface to Amazon S3, accessible via NFS or SMB. The files are stored as S3 objects, allowing you to make use of specialized S3 features such as lifecycle management and cross region replication. You can trigger AWS Lambda functions, run Amazon Athena queries, and use Amazon Macie to discover and classify sensitive data.

Keyword: NFS + Compliance

File gateway provides a virtual on-premises file server, which enables you to store and retrieve files as objects in Amazon S3. It can be used for on-premises applications, and for Amazon EC2- resident applications that need file storage in S3 for object based workloads. Used for flat files only, stored directly on S3. File gateway offers SMB or NFS-based access to data in Amazon S3 with local caching.

WS Storage Gateway – File Gateway

The table below shows the different gateways available and the interfaces and use cases:

Storage Gateway Overview

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

INCORRECT: “Install an AWS Storage Gateway file gateway on premises to replicate the data to Amazon S3” is incorrect.

INCORRECT: “Install an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3” is incorrect as unsupported NFS. INCORRECT: “Install an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3” is incorrect as unsupported NFS.

**References:** AWS News Blog > [File Interface to AWS Storage Gateway](https://aws.amazon.com/blogs/aws/file-interface-to-aws-storage-gateway/)

#### Exam Question 28

A company’s web application is using multiple Linux Amazon EC2 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 and to provide storage that complies with atomicity, consistency, isolation, and durability (ACID).

What should a solutions architect do to meet these requirements?

A. Launch the application on EC2 instances in each Availability Zone. Attach EBS volumes to each EC2 instance.  
B. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Mount an instance store on each EC2 instance.  
C. 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.  
D. Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data using Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).

**Correct Answer:**  
C. 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.

**Answer Description:**  
How Amazon EFS Works with Amazon EC2  
The following illustration shows an example VPC accessing an Amazon EFS file system. Here, EC2 instances in the VPC have file systems mounted.

In this illustration, the VPC has three Availability Zones, and each has one mount target created in it. We recommend that you access the file system from a mount target within the same Availability Zone. One of the Availability Zones has two subnets. However, a mount target is created in only one of the subnets.

Benefits of Auto Scaling  
Better fault tolerance. Amazon EC2 Auto Scaling can detect when an instance is unhealthy, terminate it, and launch an instance to replace it. You can also configure Amazon EC2 Auto Scaling to use multiple Availability Zones. If one Availability Zone becomes unavailable, Amazon EC2 Auto Scaling can launch instances in another one to compensate.

Better availability. Amazon EC2 Auto Scaling helps ensure that your application always has the right amount of capacity to handle the current traffic demand.

Better cost management. Amazon EC2 Auto Scaling can dynamically increase and decrease capacity as needed. Because you pay for the EC2 instances you use, you save money by launching instances when they are needed and terminating them when they aren’t.

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.

INCORRECT: “Launch the application on EC2 instances in each Availability Zone. Attach EBS volumes to each EC2 instance” is incorrect as the EBS volumes are single points of failure which are not shared with other instances.

INCORRECT: “Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Mount an instance store on each EC2 instance” is incorrect as instance stores are ephemeral data stores which means data is lost when powered down. Also, instance stores cannot be shared between instances.

INCORRECT: “Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data using Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)” is incorrect as there are data retrieval charges associated with this S3 tier. It is not a suitable storage tier for application files.

**References:** [Amazon Elastic File System Documentation](https://docs.aws.amazon.com/efs/)

#### Exam Question 29

A data science team requires storage for nightly log processing. The size and number of logs is unknown and will persist for 24 hours only.

What is the MOST cost-effective solution?

A. Amazon S3 Glacier  
B. Amazon S3 Standard  
C. Amazon S3 Intelligent-Tiering  
D. Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

**Correct Answer:**  
B. Amazon S3 Standard

**Answer Description:**  
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.

INCORRECT: “S3 Standard-Infrequent Access (S3 Standard-IA)” is incorrect as if the data is accessed often retrieval fees could become expensive.

INCORRECT: “S3 One Zone-Infrequent Access (S3 One Zone-IA)” is incorrect as if the data is accessed often retrieval fees could become expensive.

INCORRECT: “S3 Glacier” is incorrect as if the data is accessed often retrieval fees could become expensive. Glacier also requires more work in retrieving the data from the archive and quick access requirements can add further costs.

**References:** [Unknown or changing access](https://aws.amazon.com/s3/storage-classes/#Unknown_or_changing_access)

#### Exam Question 30

A company is hosting a web application on AWS using a single Amazon EC2 instance that stores user uploaded documents in an Amazon EBS volume. For better scalability and availability, the company duplicated the architecture and created a second EC2 instance and EBS volume in another Availability Zone, placing both behind an Application Load Balancer. After completing this change, users reported that each time they refreshed the website, they could see one subset of their documents or the other, but never all of the documents at the same time.

What should a solutions architect propose to ensure users see all of their documents at once?

A. Copy the data so both EBS volumes contain all the documents.  
B. Configure the Application Load Balancer to direct a user to the server with the documents.  
C. Copy the data from both EBS volumes to Amazon EFS. Modify the application to save new documents to Amazon EFS.  
D. Configure the Application Load Balancer to send the request to both servers. Return each document from the correct server.

**Correct Answer:**  
C. Copy the data from both EBS volumes to Amazon EFS. Modify the application to save new documents to Amazon EFS.

**Answer Description:**  
Amazon EFS provides file storage in the AWS Cloud. With Amazon EFS, you can create a file system, mount the file system on an Amazon EC2 instance, and then read and write data to and from your file system. You can mount an Amazon EFS file system in your VPC, through the Network File System versions 4.0 and 4.1 (NFSv4) protocol. We recommend using a current generation Linux NFSv4.1 client, such as those found in the latest Amazon Linux, Redhat, and Ubuntu AMIs, in conjunction with the Amazon EFS Mount Helper. For instructions, see Using the amazon-efs-utils Tools.

For a list of Amazon EC2 Linux Amazon Machine Images (AMIs) that support this protocol, see NFS Support. For some AMIs, you’ll need to install an NFS client to mount your file system on your Amazon EC2 instance. For instructions, see Installing the NFS Client.

You can access your Amazon EFS file system concurrently from multiple NFS clients, so applications that scale beyond a single connection can access a file system. Amazon EC2 instances running in multiple Availability Zones within the same AWS Region can access the file system, so that many users can access and share a common data source.

How Amazon EFS Works with Amazon EC2

#### Exam Question 31

A company is planning to use Amazon S3 to store images uploaded by its users. The images must be encrypted at rest in Amazon S3. The company does not want to spend time managing and rotating the keys, but it does want to control who can access those keys.

What should a solutions architect use to accomplish this?

A. Server-Side Encryption with keys stored in an S3 bucket  
B. Server-Side Encryption with Customer-Provided Keys (SSE-C)  
C. Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)  
D. Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

**Correct Answer:**  
D. Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

**Answer Description:**  
“Server-Side Encryption with Customer Master Keys (CMKs) Stored in AWS Key Management Service (SSE-KMS) is similar to SSE-S3, but with some additional benefits and charges for using this service.

There are separate permissions for the use of a CMK that provides added protection against unauthorized access of your objects in Amazon S3. SSE-KMS also provides you with an audit trail that shows when your CMK was used and by whom.”

Server-Side Encryption: Using SSE-KMS  
You can protect data at rest in Amazon S3 by using three different modes of server-side encryption: SSES3, SSE-C, or SSE-KMS.  
SSE-S3 requires that Amazon S3 manage the data and master encryption keys. For more information about SSE-S3, see Protecting Data Using Server-Side Encryption with Amazon S3-Managed Encryption Keys (SSE-S3).

SSE-C requires that you manage the encryption key. For more information about SSE-C, see Protecting Data Using Server-Side Encryption with Customer-Provided Encryption Keys (SSE-C).

SSE-KMS requires that AWS manage the data key but you manage the customer master key (CMK) in AWS KMS.

The remainder of this topic discusses how to protect data by using server-side encryption with AWS KMS-managed keys (SSE-KMS).

You can request encryption and select a CMK by using the Amazon S3 console or API. In the console, check the appropriate box to perform encryption and select your CMK from the list. For the Amazon S3 API, specify encryption and choose your CMK by setting the appropriate headers in a GET or PUT request.

SSE-KMS requires that AWS manage the data key but you manage the customer master key (CMK) in AWS KMS. You can choose a customer managed CMK or the AWS managed CMK for Amazon S3 in your account.

Customer managed CMKs are CMKs in your AWS account that you create, own, and manage. You have full control over these CMKs, including establishing and maintaining their key policies, IAM policies, and grants, enabling and disabling them, rotating their cryptographic material, adding tags, creating aliases that refer to the CMK, and scheduling the CMKs for deletion.

For this scenario, the solutions architect should use SSE-KMS with a customer managed CMK. That way KMS will manage the data key but the company can configure key policies defining who can access the keys.

CORRECT: “Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)” is the correct answer.

INCORRECT: “Server-Side Encryption with keys stored in an S3 bucket” is incorrect as you cannot store your keys in a bucket with server-side encryption

INCORRECT: “Server-Side Encryption with Customer-Provided Keys (SSE-C)” is incorrect as the company does not want to manage the keys.

INCORRECT: “Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)” is incorrect as the company needs to manage access control for the keys which is not possible when they’re managed by Amazon.

**References:**

* AWS Key Management Service > Developer Guide > [Server-Side Encryption: Using SSE-KMS](https://docs.aws.amazon.com/kms/latest/developerguide/services-s3.html#sse)
* AWS Key Management Service > Developer Guide > [AWS KMS keys concepts](https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master_keys)

#### Exam Question 32

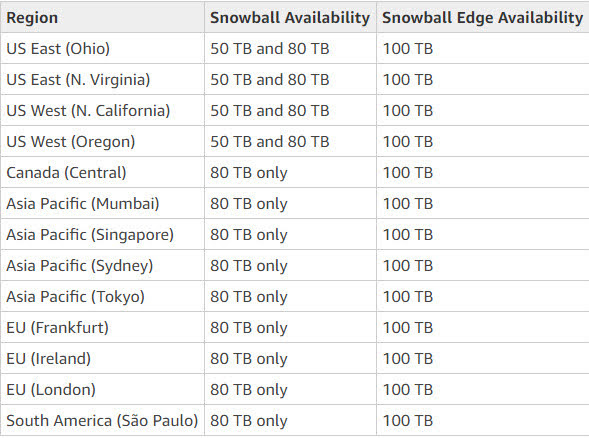
A solutions architect is tasked with transferring 750 TB of data from a network-attached file system located at a branch office Amazon S3 Glacier. The solution must avoid saturating the branch office’s low-bandwidth internet connection.

What is the MOST cost-effective solution?

A. Create a site-to-site VPN tunnel to an Amazon S3 bucket and transfer the files directly. Create a bucket policy to enforce a VPC endpoint.  
B. Order 10 AWS Snowball appliances and select an S3 Glacier vault as the destination. Create a bucket policy to enforce a VPC endpoint.  
C. Mount the network-attached file system to Amazon S3 and copy the files directly. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.  
D. Order 10 AWS Snowball appliances and select an Amazon S3 bucket as the destination. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.

**Correct Answer:**  
D. Order 10 AWS Snowball appliances and select an Amazon S3 bucket as the destination. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.

**Answer Description:**  
Regional Limitations for AWS Snowball  
The AWS Snowball service has two device types, the standard Snowball and the Snowball Edge. The following table highlights, which of these devices are available in which regions.



The following table highlights which of these devices are available in which regions.

Limitations on Jobs in AWS Snowball

The following limitations exist for creating jobs in AWS Snowball:

For security purposes, data transfers must be completed within 90 days of the Snowball being prepared.

Currently, AWS Snowball Edge device doesn’t support server-side encryption with customer-provided keys (SSE-C). AWS Snowball Edge device does support server-side encryption with Amazon S3–managed encryption keys (SSE-S3) and server-side encryption with AWS Key Management Service – managed keys (SSE-KMS). For more information, see Protecting Data Using Server-Side Encryption in the Amazon Simple Storage Service Developer Guide.

In the US regions, Snowballs come in two sizes: 50 TB and 80 TB. All other regions have the 80 TB Snowballs only. If you’re using Snowball to import data, and you need to transfer more data than will fit on a single Snowball, create additional jobs. Each export job can use multiple Snowballs.

The default service limit for the number of Snowballs you can have at one time is 1. If you want to increase your service limit, contact AWS Support.

All objects transferred to the Snowball have their metadata changed. The only metadata that remains the same is filename and filesize. All other metadata is set as in the following example: -rw-rw-r– 1 root root [filesize] Dec 31 1969 [path/filename].

Object lifecycle management  
To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their Amazon S3 Lifecycle. An S3 Lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. There are two types of actions:

Transition actions – Define when objects transition to another storage class. For example, you might choose to transition objects to the S3 Standard-IA storage class 30 days after you created them, or archive objects to the S3 Glacier storage class one year after creating them.

Expiration actions – Define when objects expire. Amazon S3 deletes expired objects on your behalf. The lifecycle expiration costs depend on when you choose to expire objects.

As the company’s internet link is low-bandwidth uploading directly to Amazon S3 (ready for transition to Glacier) would saturate the link. The best alternative is to use AWS Snowball appliances. The Snowball Edge appliance can hold up to 75 TB of data so 10 devices would be required to migrate 750 TB of data.

Snowball moves data into AWS using a hardware device and the data is then copied into an Amazon S3 bucket of your choice. From there, lifecycle policies can transition the S3 objects to Amazon S3 Glacier.

CORRECT: “Order 10 AWS Snowball appliances and select an Amazon S3 bucket as the destination. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier” is the correct answer.

INCORRECT: “Order 10 AWS Snowball appliances and select an S3 Glacier vault as the destination. Create a bucket policy to enforce a VPC endpoint” is incorrect as you cannot set a Glacier vault as the destination, it must be an S3 bucket. You also can’t enforce a VPC endpoint using a bucket policy.

INCORRECT: “Create an AWS Direct Connect connection and migrate the data straight into Amazon Glacier” is incorrect as this is not the most cost-effective option and takes time to setup. INCORRECT: “Use AWS Global Accelerator to accelerate upload and optimize usage of the available bandwidth” is incorrect as this service is not used for accelerating or optimizing the upload of data from on-premises networks.

**References:** AWS Snowball Edge Developer Guide > [AWS Snowball Edge Specifications](https://docs.aws.amazon.com/snowball/latest/developer-guide/specifications.html)

#### Exam Question 33

An application hosted on AWS is experiencing performance problems, and the application vendor wants to perform an analysis of the log file to troubleshoot further. The log file is stored on Amazon S3 and is 10 GB in size. The application owner will make the log file available to the vendor for a limited time.

What is the MOST secure way to do this?

A. Enable public read on the S3 object and provide the link to the vendor.  
B. Upload the file to Amazon WorkDocs and share the public link with the vendor.  
C. Generate a presigned URL and have the vendor download the log file before it expires.  
D. Create an IAM user for the vendor to provide access to the S3 bucket and the application. Enforce multi-factor authentication.

**Correct Answer:**  
C. Generate a presigned URL and have the vendor download the log file before it expires.

**Answer Description:**  
Share an object with others  
All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a presigned URL, using their own security credentials, to grant time-limited permission to download the objects.

When you create a presigned URL for your object, you must provide your security credentials, specify a bucket name, an object key, specify the HTTP method (GET to download the object) and expiration date and time. The presigned URLs are valid only for the specified duration.

Anyone who receives the presigned URL can then access the object. For example, if you have a video in your bucket and both the bucket and the object are private, you can share the video with others by generating a presigned URL.

#### Exam Question 34

A company allows its developers to attach existing IAM policies to existing IAM roles to enable faster experimentation and agility. However, the security operations team is concerned that the developers could attach the existing administrator policy, which would allow the developers to circumvent any other security policies.

How should a solutions architect address this issue?

A. Create an Amazon SNS topic to send an alert every time a developer creates a new policy.  
B. Use service control policies to disable IAM activity across all account in the organizational unit.  
C. Prevent the developers from attaching any policies and assign all IAM duties to the security operations team.  
D. Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy.

**Correct Answer:**  
D. Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy.

**Answer Description:**  
The permissions boundary for an IAM entity (user or role) sets the maximum permissions that the entity can have. This can change the effective permissions for that user or role. The effective permissions for an entity are the permissions that are granted by all the policies that affect the user or role. Within an account, the permissions for an entity can be affected by identity-based policies, resource-based policies, permissions boundaries, Organizations SCPs, or session policies.

Therefore, the solutions architect can set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy.

CORRECT: “Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy” is the correct answer.

INCORRECT: “Create an Amazon SNS topic to send an alert every time a developer creates a new policy” is incorrect as this would mean investigating every incident which is not an efficient solution.

INCORRECT: “Use service control policies to disable IAM activity across all accounts in the organizational unit” is incorrect as this would prevent the developers from being able to work with IAM completely.

INCORRECT: “Prevent the developers from attaching any policies and assign all IAM duties to the security operations team” is incorrect as this is not necessary. The requirement is to allow developers to work with policies, the solution needs to find a secure way of achieving this.

**References:**  
AWS Identity and Access Management > User Guide > [Permissions boundaries for IAM entities](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html)

#### Exam Question 35

A company has a multi-tier application that runs six front-end web servers in an Amazon EC2 Auto Scaling group in a single Availability Zone behind an Application Load Balancer (ALB). A solutions architect needs to modify the infrastructure to be highly available without modifying the application.

Which architecture should the solutions architect choose that provides high availability?

A. Create an Auto Scaling group that uses three instances across each of two Regions.  
B. Modify the Auto Scaling group to use three instances across each of two Availability Zones.  
C. Create an Auto Scaling template that can be used to quickly create more instances in another Region.  
D. Change the ALB in front of the Amazon EC2 instances in a round-robin configuration to balance traffic to the web tier.

**Correct Answer:**  
B. Modify the Auto Scaling group to use three instances across each of two Availability Zones.

**Answer Description:**  
Expanding Your Scaled and Load-Balanced Application to an Additional Availability Zone.

When one Availability Zone becomes unhealthy or unavailable, Amazon EC2 Auto Scaling launches new instances in an unaffected zone. When the unhealthy Availability Zone returns to a healthy state, Amazon EC2 Auto Scaling automatically redistributes the application instances evenly across all of the zones for your Auto Scaling group. Amazon EC2 Auto Scaling does this by attempting to launch new instances in the Availability Zone with the fewest instances. If the attempt fails, however, Amazon EC2 Auto Scaling attempts to launch in other Availability Zones until it succeeds.

You can expand the availability of your scaled and load-balanced application by adding an Availability Zone to your Auto Scaling group and then enabling that zone for your load balancer. After you’ve enabled the new Availability Zone, the load balancer begins to route traffic equally among all the enabled zones.

High availability can be enabled for this architecture quite simply by modifying the existing Auto Scaling group to use multiple availability zones. The ASG will automatically balance the load so you don’t actually need to specify the instances per AZ.

The architecture for the web tier will look like the one below:

CORRECT: “Modify the Auto Scaling group to use four instances across each of two Availability Zones” is the correct answer.

INCORRECT: “Create an Auto Scaling group that uses four instances across each of two Regions” is incorrect as EC2 Auto Scaling does not support multiple regions.

INCORRECT: “Create an Auto Scaling template that can be used to quickly create more instances in another Region” is incorrect as EC2 Auto Scaling does not support multiple regions. INCORRECT: “Create an Auto Scaling group that uses four instances across each of two subnets” is incorrect as the subnets could be in the same AZ.

**References:**

* [Amazon EC2 Auto Scaling](https://aws.amazon.com/ec2/autoscaling/)

#### Exam Question 36

A company runs an application on a group of Amazon Linux EC2 instances. The application writes log files using standard API calls. For compliance reasons, all log files must be retained indefinitely and will be analyzed by a reporting tool that must access all files concurrently.

Which storage service should a solutions architect use to provide the MOST cost-effective solution?

A. Amazon EBS  
B. Amazon EFS  
C. Amazon EC2 instance store  
D. Amazon S3

**Correct Answer:**  
D. Amazon S3

**Answer Description:**  
Amazon S3: Requests to Amazon S3 can be authenticated or anonymous. Authenticated access requires credentials that AWS can use to authenticate your requests. When making REST API calls directly from your code, you create a signature using valid credentials and include the signature in your request. Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Amazon S3 provides easy-to-use management features so you can organize your data and configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements. Amazon S3 is designed for 99.999999999% (11 9’s) of durability, and stores data for millions of applications for companies all around the world.

The application is writing the files using API calls which means it will be compatible with Amazon S3 which uses a REST API. S3 is a massively scalable key-based object store that is well-suited to allowing concurrent access to the files from many instances.

Amazon S3 will also be the most cost-effective choice. A rough calculation using the AWS pricing calculator shows the cost differences between 1TB of storage on EBS, EFS, and S3 Standard.

CORRECT: “Amazon S3” is the correct answer.

INCORRECT: “Amazon EFS” is incorrect as though this does offer concurrent access from many EC2 Linux instances, it is not the most cost-effective solution.

INCORRECT: “Amazon EBS” is incorrect. The Elastic Block Store (EBS) is not a good solution for concurrent access from many EC2 instances and is not the most cost-effective option either. EBS volumes are mounted to a single instance except when using multi-attach which is a new feature and has several constraints.

INCORRECT: “Amazon EC2 instance store” is incorrect as this is an ephemeral storage solution which means the data is lost when powered down.

Therefore, this is not an option for long-term data storage.

**References:**

* Amazon Simple Storage Service > User Guide > [Best practices design patterns: optimizing Amazon S3 performance](https://docs.aws.amazon.com/AmazonS3/latest/userguide/optimizing-performance.html)

#### Exam Question 37

A media streaming company collects real-time data and stores it in a disk-optimized database system. The company is not getting the expected throughput and wants an in-memory database storage solution that performs faster and provides high availability using data replication.

Which database should a solutions architect recommend?

A. Amazon RDS for MySQL  
B. Amazon RDS for PostgreSQL.  
C. Amazon ElastiCache for Redis  
D. Amazon ElastiCache for Memcached

**Correct Answer:**  
C. Amazon ElastiCache for Redis

**Answer Description:**  
In-memory databases on AWS Amazon Elasticache for Redis.  
Amazon ElastiCache for Redis is a blazing fast in-memory data store that provides submillisecond latency to power internet-scale, real-time applications. Developers can use ElastiCache for Redis as an in-memory nonrelational database. The ElastiCache for Redis cluster configuration supports up to 15 shards and enables customers to run Redis workloads with up to 6.1 TB of in-memory capacity in a single cluster.

ElastiCache for Redis also provides the ability to add and remove shards from a running cluster. You can dynamically scale out and even scale in your Redis cluster workloads to adapt to changes in demand.

Amazon ElastiCache is an in-memory database. With ElastiCache Memcached there is no data replication or high availability. As you can see in the diagram, each node is a separate partition of data:

Therefore, the Redis engine must be used which does support both data replication and clustering. The following diagram shows a Redis architecture with cluster mode enabled:

CORRECT: “Amazon ElastiCache for Redis” is the correct answer.

INCORRECT: “Amazon ElastiCache for Memcached” is incorrect as Memcached does not support data replication or high availability.

INCORRECT: “Amazon RDS for MySQL” is incorrect as this is not an in-memory database. INCORRECT: “Amazon RDS for PostgreSQL” is incorrect as this is not an in-memory database.

**References:**

* [Amazon ElastiCache for Redis](https://aws.amazon.com/elasticache/redis/)

#### Exam Question 38

A company has on-premises servers running a relational database. The current database serves high read traffic for users in different locations. The company wants to migrate to AWS with the least amount of effort.  
The database solution should support disaster recovery and not affect the company’s current traffic flow.

Which solution meets these requirements?

A. Use a database in Amazon RDS with Multi-AZ and at least one read replica.  
B. Use a database in Amazon RDS with Multi-AZ and at least one standby replica.  
C. Use databases hosted on multiple Amazon EC2 instances in different AWS Regions.  
D. Use databases hosted on Amazon EC2 instances behind an Application Load Balancer in different Availability Zones.

**Correct Answer:**  
A. Use a database in Amazon RDS with Multi-AZ and at least one read replica.

**References:**

* [Enabling data classification for Amazon RDS database with Macie](https://aws.amazon.com/blogs/security/enabling-data-classification-for-amazon-rds-database-with-amazon-macie/?nc1=b_rp)

#### Exam Question 39

A company’s application is running on Amazon EC2 instances within an Auto Scaling group behind an Elastic Load Balancer. Based on the application’s history the company anticipates a spike in traffic during a holiday each year. A solutions architect must design a strategy to ensure that the Auto Scaling group proactively increases capacity to minimize any performance impact on application users.

Which solution will meet these requirements?

A. Create an Amazon CloudWatch alarm to scale up the EC2 instances when CPU utilization exceeds 90%.  
B. Create a recurring scheduled action to scale up the Auto Scaling group before the expected period of peak demand.  
C. Increase the minimum and maximum number of EC2 instances in the Auto Scaling group during the peak demand period.  
D. Configure an Amazon Simple Notification Service (Amazon SNS) notification to send alerts when there are autoscaling EC2\_INSTANCE\_LAUNCH events.

**Correct Answer:**  
B. Create a recurring scheduled action to scale up the Auto Scaling group before the expected period of peak demand.

**Answer Description:**  
AWS Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. AWS Auto Scaling refers to a collection of Auto Scaling capabilities across several AWS services.

The services within the AWS Auto Scaling family include: Amazon EC2 (known as Amazon EC2 Auto Scaling).

Amazon ECS. Amazon DynamoDB. Amazon Aurora.

The scaling options define the triggers and when instances should be provisioned/de-provisioned. There are four scaling options:

Maintain – keep a specific or minimum number of instances running. Manual – use maximum, minimum, or a specific number of instances.

Scheduled – increase or decrease the number of instances based on a schedule. Dynamic – scale based on real-time system metrics (e.g. CloudWatch metrics).

The following table describes the scaling options available and when to use them:

The scaling options are configured through Scaling Policies which determine when, if, and how the ASG scales and shrinks.

The following table describes the scaling policy types available for dynamic scaling policies and when to use them (more detail further down the page):

The diagram below depicts an Auto Scaling group with a Scaling policy set to a minimum size of 1 instance, a desired capacity of 2 instances, and a maximum size of 4 instances:

Amazon EC2 Auto Scaling supports sending Amazon SNS notifications when the following events occur.

#### Exam Question 40

An Amazon EC2 administrator created the following policy associated with an IAM group containing several users:

What is the effect of this policy?

A. Users can terminate an EC2 instance in any AWS Region except us-east-1.  
B. Users can terminate an EC2 instance with the IP address 10.100.100.1 in the us-east-1 Region.  
C. Users can terminate an EC2 instance in the us-east-1 Region when the user’s source IP is 10.100.100.254.  
D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user’s source IP is 10.100.100.254.

**Correct Answer:**  
C. Users can terminate an EC2 instance in the us-east-1 Region when the user’s source IP is 10.100.100.254.

**Answer Description:**  
What the policy means:  
1. Allow termination of any instance if user’s source IP address is 100.100.254.  
2. Deny termination of instances that are not in the us-east-1 Combining this two, you get:  
“Allow instance termination in the us-east-1 region if the user’s source IP address is 10.100.100.254. Deny termination operation on other regions.”

#### Exam Question 41

A solutions architect is optimizing a website for an upcoming musical event. Videos of the performances will be streamed in real time and then will be available on demand. The event is expected to attract a global online audience.

Which service will improve the performance of both the real-time and on-demand streaming?

A. Amazon CloudFront  
B. AWS Global Accelerator  
C. Amazon Route S3  
D. Amazon S3 Transfer Acceleration

**Correct Answer:**  
A. Amazon CloudFront

#### Exam Question 42

A company built a food ordering application that captures user data and stores it for future analysis. The application’s static front end is deployed on an Amazon EC2 instance. The front-end application sends the requests to the backend application running on separate EC2 instance. The backend application then stores the data in Amazon RDS.

What should a solutions architect do to decouple the architecture and make it scalable?

A. Use Amazon S3 to serve the front-end application, which sends requests to Amazon EC2 to execute the backend application. The backend application will process and store the data in Amazon RDS.  
B. Use Amazon S3 to serve the front-end application and write requests to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe Amazon EC2 instances to the HTTP/HTTPS endpoint of the topic, and process and store the data in Amazon RDS.  
C. Use an EC2 instance to serve the front end and write requests to an Amazon SQS queue. Place the backend instance in an Auto Scaling group, and scale based on the queue depth to process and store the data in Amazon RDS.  
D. Use Amazon S3 to serve the static front-end application and send requests to Amazon API Gateway, which writes the requests to an Amazon SQS queue. Place the backend instances in an Auto Scaling group, and scale based on the queue depth to process and store the data in Amazon RDS.

**Correct Answer:**  
D. Use Amazon S3 to serve the static front-end application and send requests to Amazon API Gateway, which writes the requests to an Amazon SQS queue. Place the backend instances in an Auto Scaling group, and scale based on the queue depth to process and store the data in Amazon RDS.

**Answer Description:**  
Keyword: Static + Decouple + Scalable Static=S3

Decouple=SQS Queue Scalable=ASG

Option B will not be there in the race due to Auto-Scaling unavailability. Option A will not be there in the race due to Decouple unavailability.

Option C & D will be in the race and Option D will be correct answers due to all 3 combination matches [Static=S3; Decouple=SQS Queue; Scalable=ASG] & Option C will loose due to Static option unavailability

#### Exam Question 43

A solutions architect is designing a web application that will run on Amazon EC2 instances behind an Application Load Balancer (ALB). The company strictly requires that the application be resilient against malicious internet activity and attacks, and protect against new common vulnerabilities and exposures.

What should the solutions architect recommend?

A. Leverage Amazon CloudFront with the ALB endpoint as the origin.  
B. Deploy an appropriate managed rule for AWS WAF and associate it with the ALB.  
C. Subscribe to AWS Shield Advanced and ensure common vulnerabilities and exposures are blocked.  
D. Configure network ACLs and security groups to allow only ports 80 and 443 to access the EC2 instances.

**Correct Answer:**  
B. Deploy an appropriate managed rule for AWS WAF and associate it with the ALB.

**References:**

* [AWS WAF – Web Application Firewall](https://aws.amazon.com/waf/)
* [AWS Shield](https://aws.amazon.com/shield/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc)
* [AWS Shield Features](https://aws.amazon.com/shield/features/)

#### Exam Question 44

A company is managing health records on-premises. The company must keep these records indefinitely, disable any modifications to the records once they are stored, and granularly audit access at all levels. The chief technology officer (CTO) is concerned because there are already millions of records not being used by any application, and the current infrastructure is running out of space. The CTO has requested a solutions architect design a solution to move existing data and support future records.

Which services can the solutions architect recommend to meet these requirements?

A. Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with data events.  
B. Use AWS Storage Gateway to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events.  
C. Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events.  
D. Use AWS Storage Gateway to move existing data to AWS. Use Amazon Elastic Block Store (Amazon EBS) to store existing and new data. Enable Amazon S3 object lock and enable Amazon S3 server access logging.

**Correct Answer:**  
D. Use AWS Storage Gateway to move existing data to AWS. Use Amazon Elastic Block Store (Amazon EBS) to store existing and new data. Enable Amazon S3 object lock and enable Amazon S3 server access logging.

**Answer Description:**  
Keyword: Move existing data and support future records + Granular audit access at all levels

Use AWS DataSync to migrate existing data to Amazon S3, and then use the File Gateway configuration of AWS Storage Gateway to retain access to the migrated data and for ongoing updates from your on-premises file-based applications.

Need a solution to move existing data and support future records = AWS DataSync should be used for migration.

Need granular audit access at all levels = Data Events should be used in CloudTrail, Management Events is enabled by default.

CORRECT: “Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with data events” is the correct answer.

INCORRECT: “Use AWS Storage Gateway to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events” is incorrect as “current infrastructure is running out of space” INCORRECT: “Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events.” is incorrect as “Management Events is enabled by default” INCORRECT: “Use AWS Storage Gateway to move existing data to AWS. Use Amazon Elastic Block Store (Amazon EBS) to store existing and new data. Enable Amazon S3 object lock and enable Amazon S3 server access logging.” is incorrect as “current infrastructure is running out of space”

**References:**

* [AWS DataSync](https://aws.amazon.com/datasync/?whats-new-cards.sort&whats-new-cards&whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc)
* [AWS CloudTrail](https://aws.amazon.com/cloudtrail/)
* [AWS Storage Gateway](https://aws.amazon.com/storagegateway/?whats-new-cards&whats-new-cards&whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc)

#### Exam Question 45

A company wants to use Amazon S3 for the secondary copy of its on-premises dataset. The company would rarely need to access this copy. The storage solution’s cost should be minimal.

Which storage solution meets these requirements?

A. S3 Standard  
B. S3 Intelligent-Tiering  
C. S3 Standard-Infrequent Access (S3 Standard-IA)  
D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

**Correct Answer:**  
D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

#### Exam Question 46

A company’s operations team has an existing Amazon S3 bucket configured to notify an Amazon SQS queue when new objects are created within the bucket. The development team also wants to receive events when new objects are created. The existing operations team workflow must remain intact.

Which solution would satisfy these requirements?

A. Create another SQS queue. Update the S3 events in the bucket to also update the new queue when a new object is created.  
B. Create a new SQS queue that only allows Amazon S3 to access the queue. Update Amazon S3 to update this queue when a new object is created.  
C. Create an Amazon SNS topic and SQS queue for the bucket updates. Update the bucket to send events to the new topic. Updates both queues to poll Amazon SNS.  
D. Create an Amazon SNS topic and SQS queue for the bucket updates. Update the bucket to send events to the new topic. Add subscriptions for both queues in the topic.

**Correct Answer:**  
D. Create an Amazon SNS topic and SQS queue for the bucket updates. Update the bucket to send events to the new topic. Add subscriptions for both queues in the topic.

#### Exam Question 47

An application runs on Amazon EC2 instances in private subnets. The application needs to access an Amazon DynamoDB table. What is the MOST secure way to access the table while ensuring that the traffic does not leave the AWS network?

A. Use a VPC endpoint for DynamoDB.  
B. Use a NAT gateway in a public subnet.  
C. Use a NAT instance in a private subnet.  
D. Use the internet gateway attached to the VPC.

**Correct Answer:**  
A. Use a VPC endpoint for DynamoDB.

**Answer Description:**  
An Interface endpoint uses AWS PrivateLink and is an elastic network interface (ENI) with a private IP address that serves as an entry point for traffic destined to a supported service.

Using PrivateLink you can connect your VPC to supported AWS services, services hosted by other AWS accounts (VPC endpoint services), and supported AWS Marketplace partner services.

AWS PrivateLink access over Inter-Region VPC Peering:

Applications in an AWS VPC can securely access AWS PrivateLink endpoints across AWS Regions using Inter-Region VPC Peering.

AWS PrivateLink allows you to privately access services hosted on AWS in a highly available and scalable manner, without using public IPs, and without requiring the traffic to traverse the Internet.

Customers can privately connect to a service even if the service endpoint resides in a different AWS Region.

Traffic using Inter-Region VPC Peering stays on the global AWS backbone and never traverses the public Internet.

A gateway endpoint is a gateway that is a target for a specified route in your route table, used for traffic destined to a supported AWS service.

An interface VPC endpoint (interface endpoint) enables you to connect to services powered by AWS PrivateLink.

**References:**  
Amazon DynamoDB > Developer Guide > [What Is Amazon DynamoDB?](https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html)

#### Exam Question 48

A company has created a VPC with multiple private subnets in multiple Availability Zones (AZs) and one public subnet in one of the AZs. The public subnet is used to launch a NAT gateway. There are instances in the private subnets that use a NAT gateway to connect to the internet. In case of an AZ failure, the company wants to ensure that the instances are not all experiencing internet connectivity issues and that there is a backup plan ready.

Which solution should a solutions architect recommend that is MOST highly available?

A. Create a new public subnet with a NAT gateway in the same AZ. Distribute the traffic between the two NAT gateways.  
B. Create an Amazon EC2 NAT instance in a new public subnet. Distribute the traffic between the NAT gateway and the NAT instance.  
C. Create public subnets in each AZ and launch a NAT gateway in each subnet. Configure the traffic from the private subnets in each AZ to the respective NAT gateway.  
D. Create an Amazon EC2 NAT instance in the same public subnet. Replace the NAT gateway with the NAT instance and associate the instance with an Auto Scaling group with an appropriate scaling policy.

**Correct Answer:**  
C. Create public subnets in each AZ and launch a NAT gateway in each subnet. Configure the traffic from the private subnets in each AZ to the respective NAT gateway.

#### Exam Question 49

A company recently deployed a new auditing system to centralize information about operating system versions, patching, and installed software for Amazon EC2 instances. A solutions architect must ensure all instances provisioned through EC2 Auto Scaling groups successfully send reports to the auditing system as soon as they are launched and terminated.

Which solution achieves these goals MOST efficiently?

A. Use a scheduled AWS Lambda function and execute a script remotely on all EC2 instances to send data to the audit system.  
B. Use EC2 Auto Scaling lifecycle hooks to execute a custom script to send data to the audit system when instances are launched and terminated.  
C. Use an EC2 Auto Scaling launch configuration to execute a custom script through user data to send data to the audit system when instances are launched and terminated.  
D. Execute a custom script on the instance operating system to send data to the audit system. Configure the script to be executed by the EC2 Auto Scaling group when the instance starts and is terminated.

**Correct Answer:**  
B. Use EC2 Auto Scaling lifecycle hooks to execute a custom script to send data to the audit system when instances are launched and terminated.

#### Exam Question 50

A company recently implemented hybrid cloud connectivity using AWS Direct Connect and is migrating data to Amazon S3. The company is looking for a fully managed solution that will automate and accelerate the replication of data between the on-premises storage systems and AWS storage services.

Which solution should a solutions architect recommend to keep the data private?

A. Deploy an AWS DataSync agent for the on-premises environment. Configure a sync job to replicate the data and connect it with an AWS service endpoint.  
B. Deploy an AWS DataSync agent for the on-premises environment. Schedule a batch job to replicate point-in-time snapshots to AWS.  
C. Deploy an AWS Storage Gateway volume gateway for the on-premises environment. Configure it to store data locally, and asynchronously back up point-in-time snapshots to AWS.  
D. Deploy an AWS Storage Gateway file gateway for the on-premises environment. Configure it to store data locally, and asynchronously back up point-in-time snapshots to AWS.

**Correct Answer:**  
A. Deploy an AWS DataSync agent for the on-premises environment. Configure a sync job to replicate the data and connect it with an AWS service endpoint.

**Answer Description:**  
You can use AWS DataSync with your Direct Connect link to access public service endpoints or private VPC endpoints. When using VPC endpoints, data transferred between the DataSync agent and AWS services does not traverse the public internet or need public IP addresses, increasing the security of data as it is copied over the network.

#### Exam Question 51

A company has 150 TB of archived image data stored on-premises that needs to be moved to the AWS Cloud within the next month. The company’s current network connection allows up to 100 Mbps uploads for this purpose during the night only.

What is the MOST cost-effective mechanism to move this data and meet the migration deadline?

A. Use AWS Snowmobile to ship the data to AWS.  
B. Order multiple AWS Snowball devices to ship the data to AWS.  
C. Enable Amazon S3 Transfer Acceleration and securely upload the data.  
D. Create an Amazon S3 VPC endpoint and establish a VPN to upload the data.

**Correct Answer:**  
B. Order multiple AWS Snowball devices to ship the data to AWS.

#### Exam Question 52

A company is seeing access requests by some suspicious IP addresses. The security team discovers the requests are from different IP addresses under the same CIDR range.

What should a solutions architect recommend to the team?

A. Add a rule in the inbound table of the security to deny the traffic from that CIDR range.  
B. Add a rule in the outbound table of the security group to deny the traffic from that CIDR range.  
C. Add a deny rule in the inbound table of the network ACL with a lower number than other rules.  
D. Add a deny rule in the outbound table of the network ACL with a lower rule number than other rules.

**Correct Answer:**  
C. Add a deny rule in the inbound table of the network ACL with a lower number than other rules.

**Answer Description:**  
You can only create deny rules with network ACLs, it is not possible with security groups. Network ACLs process rules in order from the lowest numbered rules to the highest until they reach and allow or deny. The following table describes some of the differences between security groups and network ACLs:

Therefore, the solutions architect should add a deny rule in the inbound table of the network ACL with a lower rule number than other rules.

CORRECT: “Add a deny rule in the inbound table of the network ACL with a lower rule number than other rules” is the correct answer.

INCORRECT: “Add a deny rule in the outbound table of the network ACL with a lower rule number than other rules” is incorrect as this will only block outbound traffic.

INCORRECT: “Add a rule in the inbound table of the security group to deny the traffic from that CIDR range” is incorrect as you cannot create a deny rule with a security group.

INCORRECT: “Add a rule in the outbound table of the security group to deny the traffic from that CIDR range” is incorrect as you cannot create a deny rule with a security group.

**References:**  
Amazon Virtual Private Cloud > User Guide > [Network ACLs](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html)

#### Exam Question 53

A company recently expanded globally and wants to make its application accessible to users in those geographic locations. The application is deployed on Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group. The company needs the ability shift traffic from resources in one region to another.

What should a solutions architect recommend?

A. Configure an Amazon Route 53 latency routing policy.  
B. Configure an Amazon Route 53 geolocation routing policy.  
C. Configure an Amazon Route 53 geoproximity routing policy.  
D. Configure an Amazon Route 53 multivalue answer routing policy.

**Correct Answer:**  
C. Configure an Amazon Route 53 geoproximity routing policy.

**Answer Description:**  
Keyword: Users in those Geographic Locations

Condition: Ability Shift traffic from resources in One Region to Another Region The following table highlights the key function of each type of routing policy:

Geo-location:

Caters to different users in different countries and different languages.

Contains users within a particular geography and offers them a customized version of the workload based on their specific needs.

Geolocation can be used for localizing content and presenting some or all of your website in the language of your users.

Can also protect distribution rights.

Can be used for spreading load evenly between regions.

If you have multiple records for overlapping regions, Route 53 will route to the smallest geographic region.

You can create a default record for IP addresses that do not map to a geographic location.

**References:**

* Amazon Route 53 > Developer Guide > [Choosing a routing policy](https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html)
* [Amazon Route 53](https://aws.amazon.com/route53/?nc2=h_ql_prod_nt_r53)

#### Exam Question 54

A company wants to replicate its data to AWS to recover in the event of a disaster. Today, a system administrator has scripts that copy data to a NFS share Individual backup files need to be accessed with low latency by application administrators to deal with errors in processing.

What should a solutions architect recommend to meet these requirements?

A. Modify the script to copy data to an Amazon S3 bucket instead of the on-premises NFS share.  
B. Modify the script to copy data to an Amazon S3 Glacier Archive instead of the on-premises NFS share.  
C. Modify the script to copy data to an Amazon Elastic File System (Amazon EFS) volume instead of the on-premises NFS share.  
D. Modify the script to copy data to an AWS Storage Gateway for File Gateway virtual appliance instead of the on-premises NFS share.

**Correct Answer:**  
D. Modify the script to copy data to an AWS Storage Gateway for File Gateway virtual appliance instead of the on-premises NFS share.

#### Exam Question 55

A solutions architect is designing a mission-critical web application. It will consist of Amazon EC2 instances behind an Application Load Balancer and a relational database. The database should be highly available and fault tolerant.

Which database implementations will meet these requirements? (Choose two.)

A. Amazon Redshift  
B. Amazon DynamoDB  
C. Amazon RDS for MySQL  
D. MySQL-compatible Amazon Aurora Multi-AZ  
E. Amazon RDS for SQL Server Standard Edition Multi-AZ

**Correct Answer:**  
D. MySQL-compatible Amazon Aurora Multi-AZ  
E. Amazon RDS for SQL Server Standard Edition Multi-AZ

#### Exam Question 56

A company’s web application is running on Amazon EC2 instances behind an Application Load Balancer.

The company recently changed its policy, which now requires the application to be accessed from one specific country only.

Which configuration will meet this requirement?

A. Configure the security group for the EC2 instances.  
B. Configure the security group on the Application Load Balancer.  
C. Configure AWS WAF on the Application Load Balancer in a VPC.  
D. Configure the network ACL for the subnet that contains the EC2 instances.

**Correct Answer:**  
C. Configure AWS WAF on the Application Load Balancer in a VPC.

**References:**

* AWS Security Blog > [How to use AWS WAF to filter incoming traffic from embargoed countries](https://aws.amazon.com/es/blogs/security/how-to-use-aws-waf-to-filter-incoming-traffic-from-embargoed-countries/)

#### Exam Question 57

A solutions architect has created two IAM policies: Policy1 and Policy2. Both policies are attached to an IAM group.

A cloud engineer is added as an IAM user to the IAM group. Which action will the cloud engineer be able to perform?

A. Deleting IAM users  
B. Deleting directories  
C. Deleting Amazon EC2 instances  
D. Deleting logs from Amazon CloudWatch Logs

**Correct Answer:**  
C. Deleting Amazon EC2 instances

#### Exam Question 58

A company has an Amazon EC2 instance running on a private subnet that needs to access a public website to download patches and updates.

The company does not want external websites to see the EC2 instance IP address or initiate connections to it.

How can a solutions architect achieve this objective?

A. Create a site-to-site VPN connection between the private subnet and the network in which the public site is deployed.  
B. Create a NAT gateway in a public subnet. Route outbound traffic from the private subnet through the NAT gateway.  
C. Create a network ACL for the private subnet where the EC2 instance deployed only allows access from the IP address range of the public website.  
D. Create a security group that only allows connections from the IP address range of the public website. Attach the security group to the EC2 instance.

**Correct Answer:**  
B. Create a NAT gateway in a public subnet. Route outbound traffic from the private subnet through the NAT gateway.

#### Exam Question 59

A company must migrate 20 TB of data from a data center to the AWS Cloud within 30 days. The company’s network bandwidth is limited to 15 Mbps and cannot exceed 70% utilization. What should a solutions architect do to meet these requirements?

A. Use AWS Snowball.  
B. Use AWS DataSync.  
C. Use a secure VPN connection.  
D. Use Amazon S3 Transfer Acceleration.

**Correct Answer:**  
A. Use AWS Snowball.

#### Exam Question 60

A company has a website running on Amazon EC2 instances across two Availability Zones. The company is expecting spikes in traffic on specific holidays, and wants to provide a consistent user experience. How can a solutions architect meet this requirement?

A. Use step scaling.  
B. Use simple scaling.  
C. Use lifecycle hooks.  
D. Use scheduled scaling.

**Correct Answer:**  
D. Use scheduled scaling.

#### Exam Question 61

A company has an on-premises data center that is running out of storage capacity. The company wants to migrate its storage infrastructure to AWS while minimizing bandwidth costs. The solution must allow for immediate retrieval of data at no additional cost.

How can these requirements be met?

A. Deploy Amazon S3 Glacier Vault and enable expedited retrieval. Enable provisioned retrieval capacity for the workload.  
B. Deploy AWS Storage Gateway using cached volumes. Use Storage Gateway to store data in Amazon S3 while retaining copies of frequently accessed data subsets locally.  
C. Deploy AWS Storage Gateway using stored volumes to store data locally. Use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3.  
D. Deploy AWS Direct Connect to connect with the on-premises data center. Configure AWS Storage Gateway to store data locally. Use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3.

**Correct Answer:**  
C. Deploy AWS Storage Gateway using stored volumes to store data locally. Use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3.

**Answer Description:**  
Volume Gateway provides an iSCSI target, which enables you to create block storage volumes and mount them as iSCSI devices from your on-premises or EC2 application servers. The Volume Gateway runs in either a cached or stored mode:

In the cached mode, your primary data is written to S3, while retaining your frequently accessed data locally in a cache for low-latency access.

In the stored mode, your primary data is stored locally and your entire dataset is available for low-latency access while asynchronously backed up to AWS.

#### Exam Question 62

A company delivers files in Amazon S3 to certain users who do not have AWS credentials. These users must be given access for a limited time.

What should a solutions architect do to securely meet these requirements?

A. Enable public access on an Amazon S3 bucket.  
B. Generate a presigned URL to share with the users.  
C. Encrypt files using AWS KMS and provide keys to the users.  
D. Create and assign IAM roles that will grant GetObject permissions to the users.

**Correct Answer:**  
B. Generate a presigned URL to share with the users.

#### Exam Question 63

A company is investigating potential solutions that would collect, process, and store users’ service usage data. The business objective is to create an analytics capability that will enable the company to gather operational insights quickly using standard SQL queries. The solution should be highly available and ensure Atomicity, Consistency, Isolation, and Durability (ACID) compliance in the data tier.

Which solution should a solutions architect recommend?

A. Use Amazon DynamoDB transactions.  
B. Create an Amazon Neptune database in a Multi-AZ design  
C. Use a fully managed Amazon RDS for MySQL database in a Multi-AZ design.  
D. Deploy PostgreSQL on an Amazon EC2 instance that uses Amazon EBS Throughput Optimized HDD (st1) storage.

**Correct Answer:**  
C. Use a fully managed Amazon RDS for MySQL database in a Multi-AZ design.

#### Exam Question 64

An application running on an Amazon EC2 instance in VPC-A needs to access files in another EC2 instance in VPC-B. Both are in separate. AWS accounts. The network administrator needs to design a solution to enable secure access to EC2 instance in VPC-B from VPC-A. The connectivity should not have a single point of failure or bandwidth concerns.

Which solution will meet these requirements?

A. Set up a VPC peering connection between VPC-A and VPC-B.  
B. Set up VPC gateway endpoints for the EC2 instance running in VPC-B.  
C. Attach a virtual private gateway to VPC-B and enable routing from VPC-A.  
D. Create a private virtual interface (VIF) for the EC2 instance running in VPC-B and add appropriate routes from VPC-B.

**Correct Answer:**  
A. Set up a VPC peering connection between VPC-A and VPC-B.

**Answer Description:**  
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 traffic remains in the private IP space. All inter-region traffic is encrypted with no single point of failure, or bandwidth bottleneck.

**References:**  
Amazon Virtual Private Cloud > VPC Peering > [What is VPC peering?](https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html)

#### Exam Question 65

A company’s application hosted on Amazon EC2 instances needs to access an Amazon S3 bucket. Due to data sensitivity, traffic cannot traverse the internet.

How should a solutions architect configure access?

A. Create a private hosted zone using Amazon Route 53.  
B. Configure a VPC gateway endpoint for Amazon S3 in the VPC.  
C. Configure AWS PrivateLink between the EC2 instance and the S3 bucket.  
D. Set up a site-to-site VPN connection between the VPC and the S3 bucket.

**Correct Answer:**  
B. Configure a VPC gateway endpoint for Amazon S3 in the VPC.

#### Exam Question 66

A company has two applications it wants to migrate to AWS. Both applications process a large set of files by accessing the same files at the same time. Both applications need to read the files with low latency.

Which architecture should a solutions architect recommend for this situation?

A. Configure two AWS Lambda functions to run the applications. Create an Amazon EC2 instance with an instance store volume to store the data.  
B. Configure two AWS Lambda functions to run the applications. Create an Amazon EC2 instance with an Amazon Elastic Block Store (Amazon EBS) volume to store the data.  
C. Configure one memory optimized Amazon EC2 instance to run both applications simultaneously. Create an Amazon Elastic Block Store (Amazon EBS) volume with Provisioned IOPS to store the data.  
D. Configure two Amazon EC2 instances to run both applications. Configure Amazon Elastic File System (Amazon EFS) with General Purpose performance mode and Bursting Throughput mode to store the data.

**Correct Answer:**  
D. Configure two Amazon EC2 instances to run both applications. Configure Amazon Elastic File System (Amazon EFS) with General Purpose performance mode and Bursting Throughput mode to store the data.

#### Exam Question 67

An eCommerce company has noticed performance degradation of its Amazon RDS based web application.

The performance degradation is attributed to an increase in the number of read-only SQL queries triggered by business analysts. A solutions architect needs to solve the problem with minimal changes to the existing web application. What should the solutions architect recommend?

A. Export the data to Amazon DynamoDB and have the business analysts run their queries.  
B. Load the data into Amazon ElastiCache and have the business analysts run their queries.  
C. Create a read replica of the primary database and have the business analysts run their queries.  
D. Copy the data into an Amazon Redshift cluster and have the business analysts run their queries.

**Correct Answer:**  
C. Create a read replica of the primary database and have the business analysts run their queries.

#### Exam Question 68

A company is running a highly sensitive application on Amazon EC2 backed by an Amazon RDS database.

Compliance regulations mandate that all personally identifiable information (PII) be encrypted at rest.

Which solution should a solutions architect recommend to meet this requirement with the LEAST amount of changes to the infrastructure?

A. Deploy AWS Certificate Manager to generate certificates. Use the certificates to encrypt the database volume.  
B. Deploy AWS CloudHSM, generate encryption keys, and use the customer master key (CMK) to encrypt database volumes.  
C. Configure SSL encryption using AWS Key Management Service customer master keys (AWS KMS CMKs) to encrypt database volumes.  
D. Configure Amazon Elastic Block Store (Amazon EBS) encryption and Amazon RDS encryption with AWS Key Management Service (AWS KMS) keys to encrypt instance and database volumes.

**Correct Answer:**  
D. Configure Amazon Elastic Block Store (Amazon EBS) encryption and Amazon RDS encryption with AWS Key Management Service (AWS KMS) keys to encrypt instance and database volumes.

#### Exam Question 69

A company running an on-premises application is migrating the application to AWS to increase its elasticity and availability. The current architecture uses a Microsoft SQL Server database with heavy read activity.  
The company wants to explore alternate database options and migrate database engines, if needed. Every 4 hours, the development team does a full copy of the production database to populate a test database.

During this period, users experience latency. What should a solutions architect recommend as replacement database?

A. Use Amazon Aurora with Multi-AZ Aurora Replicas and restore from mysqldump for the test database.  
B. Use Amazon Aurora with Multi-AZ Aurora Replicas and restore snapshots from Amazon RDS for the test database.  
C. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas, and use the standby instance for the test database.  
D. Use Amazon RDS for SQL Server with a Multi-AZ deployment and read replicas, and restore snapshots from RDS for the test database.

**Correct Answer:**  
D. Use Amazon RDS for SQL Server with a Multi-AZ deployment and read replicas, and restore snapshots from RDS for the test database.

#### Exam Question 70

A company has enabled AWS CloudTrail logs to deliver log files to an Amazon S3 bucket for each of its developer accounts. The company has created a central AWS account for streamlining management and audit reviews. An internal auditor needs to access the CloudTrail logs, yet access needs to be restricted for all developer account users. The solution must be secure and optimized.

How should a solutions architect meet these requirements?

A. Configure an AWS Lambda function in each developer account to copy the log files to the central account. Create an IAM role in the central account for the auditor. Attach an IAM policy providing read only permissions to the bucket.  
B. Configure CloudTrail from each developer account to deliver the log files to an S3 bucket in the central account. Create an IAM user in the central account for the auditor. Attach an IAM policy providing full permissions to the bucket.  
C. Configure CloudTrail from each developer account to deliver the log files to an S3 bucket in the central account. Create an IAM role in the central account for the auditor. Attach an IAM policy providing read only permissions to the bucket.  
D. Configure an AWS Lambda function in the central account to copy the log files from the S3 bucket in each developer account. Create an IAM user in the central account for the auditor. Attach an IAM policy providing full permissions to the bucket.

**Correct Answer:**  
C. Configure CloudTrail from each developer account to deliver the log files to an S3 bucket in the central account. Create an IAM role in the central account for the auditor. Attach an IAM policy providing read only permissions to the bucket.

#### Exam Question 71

A company has a Microsoft Windows-based application that must be migrated to AWS. This application requires the use of a shared Windows file system attached to multiple Amazon EC2 Windows instances.

What should a solutions architect do to accomplish this?

A. Configure a volume using Amazon EFS. Mount the EFS volume to each Windows instance.  
B. Configure AWS Storage Gateway in Volume Gateway mode. Mount the volume to each Windows instance.  
C. Configure Amazon FSx for Windows File Server. Mount the Amazon FSx volume to each Windows instance.  
D. Configure an Amazon EBS volume with the required size. Attach each EC2 instance to the volume. Mount the file system within the volume to each Windows instance.

**Correct Answer:**  
C. Configure Amazon FSx for Windows File Server. Mount the Amazon FSx volume to each Windows instance.

#### Exam Question 72

A company has implemented one of its microservices on AWS Lambda that accesses an Amazon DynamoDB table named Books. A solutions architect is designing an IAM policy to be attached to the Lambda function’s IAM role, giving it access to put, update, and delete items in the Books table.

The IAM policy must prevent function from performing any other actions on the Books table or any other.

Which IAM policy would fulfill these needs and provide the LEAST privileged access?

A.

B.

C.

D.

**Correct Answer:**  
A

#### Exam Question 73

A company runs a website on Amazon EC2 instances behind an ELB Application Load Balancer. Amazon Route 53 is used for the DNS. The company wants to set up a backup website with a message including a phone number and email address that users can reach if the primary website is down.

How should the company deploy this solution?

A. Use Amazon S3 website hosting for the backup website and Route 53 failover routing policy.  
B. Use Amazon S3 website hosting for the backup website and Route 53 latency routing policy.  
C. Deploy the application in another AWS Region and use ELB health checks for failover routing.  
D. Deploy the application in another AWS Region and use server-side redirection on the primary website.

**Correct Answer:**  
A. Use Amazon S3 website hosting for the backup website and Route 53 failover routing policy.

#### Exam Question 74

A media company is evaluating the possibility of moving its systems to the AWS Cloud. The company needs at least 10 TB of storage with the maximum possible I/O performance for video processing, 300 TB of very durable storage for storing media content, and 900 TB of storage to meet requirements for archival media that is not in use anymore.

Which set of services should a solutions architect recommend to meet these requirements?

A. Amazon EBS for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage  
B. Amazon EBS for maximum performance, Amazon EFS for durable data storage, and Amazon S3 Glacier for archival storage  
C. Amazon EC2 instance store for maximum performance, Amazon EFS for durable data storage, and Amazon S3 for archival storage  
D. Amazon EC2 instance store for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage

**Correct Answer:**  
A. Amazon EBS for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage

#### Exam Question 75

An application is running on Amazon EC2 instances. Sensitive information required for the application is stored in an Amazon S3 bucket. The bucket needs to be protected from internet access while only allowing services within the VPC access to the bucket.

Which combination of actions should solutions archived take to accomplish this? (Choose two.)

A. Create a VPC endpoint for Amazon S3.  
B. Enable server access logging on the bucket.  
C. Apply a bucket policy to restrict access to the S3 endpoint.  
D. Add an S3 ACL to the bucket that has sensitive information.  
E. Restrict users using the IAM policy to use the specific bucket.

**Correct Answer:**  
A. Create a VPC endpoint for Amazon S3.  
C. Apply a bucket policy to restrict access to the S3 endpoint.

**Answer Description:**  
ACL is a property at object level not at bucket level. Also by just adding ACL you cant let the services in VPC allow access to the bucket.

#### Exam Question 76

A web application runs on Amazon EC2 instances behind an Application Load Balancer. The application allows users to create custom reports of historical weather data. Generating a report can take up to 5 minutes. These long-running requests use many of the available incoming connections, making the system unresponsive to other users.

How can a solutions architect make the system more responsive?

A. Use Amazon SQS with AWS Lambda to generate reports.  
B. Increase the idle timeout on the Application Load Balancer to 5 minutes.  
C. Update the client-side application code to increase its request timeout to 5 minutes.  
D. Publish the reports to Amazon S3 and use Amazon CloudFront for downloading to the user.

**Correct Answer:**  
A. Use Amazon SQS with AWS Lambda to generate reports.

#### Exam Question 77

A solutions architect must create a highly available bastion host architecture. The solution needs to be resilient within a single AWS Region and should require only minimal effort to maintain.

What should the solutions architect do to meet these requirements?

A. Create a Network Load Balancer backed by an Auto Scaling group with a UDP listener.  
B. Create a Network Load Balancer backed by a Spot Fleet with instances in a partition placement group.  
C. Create a Network Load Balancer backed by the existing servers in different Availability Zones as the target.  
D. Create a Network Load Balancer backed by an Auto Scaling group with instances in multiple Availability Zones as the target.

**Correct Answer:**  
D. Create a Network Load Balancer backed by an Auto Scaling group with instances in multiple Availability Zones as the target.

#### Exam Question 78

A three-tier web application processes orders from customers. The web tier consists of Amazon EC2 instances behind an Application Load Balancer, a middle tier of three EC2 instances decoupled from the web tier using Amazon SQS, and an Amazon DynamoDB backend. At peak times, customers who submit orders using the site have to wait much longer than normal to receive confirmations due to lengthy processing times. A solutions architect needs to reduce these processing times.

Which action will be MOST effective in accomplishing this?

A. Replace the SQS queue with Amazon Kinesis Data Firehose.  
B. Use Amazon ElastiCache for Redis in front of the DynamoDB backend tier.  
C. Add an Amazon CloudFront distribution to cache the responses for the web tier.  
D. Use Amazon EC2 Auto Scaling to scale out the middle tier instances based on the SQS queue depth.

**Correct Answer:**  
D. Use Amazon EC2 Auto Scaling to scale out the middle tier instances based on the SQS queue depth.

#### Exam Question 79

A solutions architect is designing an architecture for a new application that requires low network latency and high network throughput between Amazon EC2 instances. Which component should be included in the architectural design?

A. An Auto Scaling group with Spot Instance types.  
B. A placement group using a cluster placement strategy.  
C. A placement group using a partition placement strategy.  
D. An Auto Scaling group with On-Demand instance types.

**Correct Answer:**  
B. A placement group using a cluster placement strategy.

#### Exam Question 80

A company has global users accessing an application deployed in different AWS Regions, exposing public static IP addresses. The users are experiencing poor performance when accessing the application over the internet.

What should a solutions architect recommend to reduce internet latency?

A. Set up AWS Global Accelerator and add endpoints.  
B. Set up AWS Direct Connect locations in multiple Regions.  
C. Set up an Amazon CloudFront distribution to access an application.  
D. Set up an Amazon Route 53 geoproximity routing policy to route traffic.

**Correct Answer:**  
A. Set up AWS Global Accelerator and add endpoints.

**Answer Description:**  
AWS Global Accelerator is a service in which you create accelerators to improve availability and performance of your applications for local and global users. Global Accelerator directs traffic to optimal endpoints over the AWS global network. This improves the availability and performance of your internet applications that are used by a global audience. Global Accelerator is a global service that supports endpoints in multiple AWS Regions, which are listed in the AWS Region Table.

By default, Global Accelerator provides you with two static IP addresses that you associate with your accelerator. (Or, instead of using the IP addresses that Global Accelerator provides, you can configure these entry points to be IPv4 addresses from your own IP address ranges that you bring to Global Accelerator.)

The static IP addresses are anycast from the AWS edge network and distribute incoming application traffic across multiple endpoint resources in multiple AWS Regions, which increases the availability of your applications. Endpoints can be Network Load Balancers, Application Load Balancers, EC2 instances, or Elastic IP addresses that are located in one AWS Region or multiple Regions.

CORRECT: “Set up AWS Global Accelerator and add endpoints” is the correct answer. INCORRECT: “Set up AWS Direct Connect locations in multiple Regions” is incorrect as this is used to connect from an on-premises data center to AWS. It does not improve performance for users who are not connected to the on-premises data center.

INCORRECT: “Set up an Amazon CloudFront distribution to access an application” is incorrect as CloudFront cannot expose static public IP addresses.

INCORRECT: “Set up an Amazon Route 53 geoproximity routing policy to route traffic” is incorrect as this does not reduce internet latency as well as using Global Accelerator. GA will direct users to the closest edge location and then use the AWS global network.

#### Exam Question 81

A company wants to migrate a workload to AWS. The chief information security officer requires that all data be encrypted at rest when stored in the cloud. The company wants complete control of encryption key lifecycle management.

The company must be able to immediately remove the key material and audit key usage independently of AWS CloudTrail. The chosen services should integrate with other storage services that will be used on AWS.

Which services satisfies these security requirements?

A. AWS CloudHSM with the CloudHSM client  
B. AWS Key Management Service (AWS KMS) with AWS CloudHSM  
C. AWS Key Management Service (AWS KMS) with an external key material origin  
D. AWS Key Management Service (AWS KMS) with AWS managed customer master keys (CMKs)

**Correct Answer:**  
B. AWS Key Management Service (AWS KMS) with AWS CloudHSM

**Answer Description:**  
Took a bit of reading. Key points in question:

“The company must be able to immediately remove the key material and audit key usage independently”

“The chosen services should integrate with other storage services that will be used on AWS” Point 1: Q: Can I use CloudHSM to store keys or encrypt data used by other AWS services? Ans: Yes. You can do all encryption in your CloudHSM-integrated application. In this case, AWS services such as Amazon S3 or Amazon Elastic Block Store (EBS) would only see your data encrypted.

Point 2: AWS manages the hardware security module (HSM) appliance, but does not have access to your keys. You control and manage your own keys

**References:**

* [AWS CloudHSM features](https://aws.amazon.com/cloudhsm/features/)
* [AWS CloudHSM FAQs](https://aws.amazon.com/cloudhsm/faqs/)

#### Exam Question 82

A company has an application with a REST-based interface that allows data to be received in near-real time from a third-party vendor. Once received, the application processes and stores the data for further analysis.  
The application is running on Amazon EC2 instances.

The third-party vendor has received many 503 Service Unavailable Errors when sending data to the application. When the data volume spikes, the compute capacity reaches its maximum limit and the application is unable to process all requests.

Which design should a solutions architect recommend to provide a more scalable solution?

A. Use Amazon Kinesis Data Streams to ingest the data. Process the data using AWS Lambda functions.  
B. Use Amazon API Gateway on top of the existing application. Create a usage plan with a quota limit for the third-party vendor.  
C. Use Amazon Simple Notification Service (Amazon SNS) to ingest the data. Put the EC2 instances in an Auto Scaling group behind an Application Load Balancer.  
D. Repackage the application as a container. Deploy the application using Amazon Elastic Container Service (Amazon ECS) using the EC2 launch type with an Auto Scaling group.

**Correct Answer:**  
A. Use Amazon Kinesis Data Streams to ingest the data. Process the data using AWS Lambda functions.

#### Exam Question 83

A solutions architect is working on optimizing a legacy document management application running on Microsoft Windows Server in an on-premises data center. The application stores a large number of files on a network file share. The chief information officer wants to reduce the on-premises data center footprint and minimize storage costs by moving on-premises storage to AWS.

What should the solutions architect do to meet these requirements?

A. Set up an AWS Storage Gateway file gateway.  
B. Set up Amazon Elastic File System (Amazon EFS)  
C. Set up AWS Storage Gateway as a volume gateway  
D. Set up an Amazon Elastic Block Store (Amazon EBS) volume.

**Correct Answer:**  
A. Set up an AWS Storage Gateway file gateway.

#### Exam Question 84

A solutions architect is designing a hybrid application using the AWS cloud. The network between the on premises data center and AWS will use an AWS Direct Connect (DX) connection. The application connectivity between AWS and the on-premises data center must be highly resilient.

Which DX configuration should be implemented to meet these requirements?

A. Configure a DX connection with a VPN on top of it.  
B. Configure DX connections at multiple DX locations.  
C. Configure a DX connection using the most reliable DX partner.  
D. Configure multiple virtual interfaces on top of a DX connection.

**Correct Answer:**  
B. Configure DX connections at multiple DX locations.

#### Exam Question 85

A company runs an application on Amazon EC2 instances. The application is deployed in private subnets in three Availability Zones of the us-east-1 Region. The instances must be able to connect to the internet to download files. The company wants a design that is highly available across the Region.

Which solution should be implemented to ensure that there are no disruptions to internet connectivity?

A. Deploy a NAT instance in a private subnet of each Availability Zone.  
B. Deploy a NAT gateway in a public subnet of each Availability Zone.  
C. Deploy a transit gateway in a private subnet of each Availability Zone.  
D. Deploy an internet gateway in a public subnet of each Availability Zone.

**Correct Answer:**  
B. Deploy a NAT gateway in a public subnet of each Availability Zone.

#### Exam Question 86

A company is running a two-tier eCommerce website using services. The current architect uses a public facing Elastic Load Balancer that sends traffic to Amazon EC2 instances in a private subnet. The static content is hosted on EC2 instances, and the dynamic content is retrieved from a MYSQL database. The application is running in the United States. The company recently started selling to users in Europe and Australia. A solutions architect needs to design solution so their international users have an improved browsing experience.

Which solution is MOST cost-effective?

A. Host the entire website on Amazon S3.  
B. Use Amazon CloudFront and Amazon S3 to host static images.  
C. Increase the number of public load balancers and EC2 instances.  
D. Deploy the two-tier website in AWS Regions in Europe and Australia.

**Correct Answer:**  
B. Use Amazon CloudFront and Amazon S3 to host static images.

#### Exam Question 87

A company’s website provides users with downloadable historical performance reports. The website needs a solution that will scale to meet the company’s website demands globally. The solution should be cost effective, limit the provisioning of infrastructure resources, and provide the fastest possible response time.

Which combination should a solutions architect recommend to meet these requirements?

A. Amazon CloudFront and Amazon S3  
B. AWS Lambda and Amazon DynamoDB  
C. Application Load Balancer with Amazon EC2 Auto Scaling  
D. Amazon Route 53 with internal Application Load Balancers

**Correct Answer:**  
A. Amazon CloudFront and Amazon S3

#### Exam Question 88

A company wants to deploy a shared file system for its .NET application servers and Microsoft SQL Server databases running on Amazon EC2 instances with Windows Server 2016. The solution must be able to be integrated into the corporate Active Directory domain, be highly durable, be managed by AWS, and provide high levels of throughput and IOPS.

Which solution meets these requirements?

A. Use Amazon FSx for Windows File Server.  
B. Use Amazon Elastic File System (Amazon EFS).  
C. Use AWS Storage Gateway in file gateway mode.  
D. Deploy a Windows file server on two On Demand instances across two Availability Zones.

**Correct Answer:**  
A. Use Amazon FSx for Windows File Server.

**References:**

* [Amazon FSx for Windows File Server](https://aws.amazon.com/fsx/windows/)

#### Exam Question 89

A company that develops web applications has launched hundreds of Application Load Balancers (ALBs) in multiple Regions. The company wants to create an allow list (or the IPs of all the load balancers on its firewall device. A solutions architect is looking for a one-time, highly available solution to address this request, which will also help reduce the number of IPs that need to be allowed by the firewall.

What should the solutions architect recommend to meet these requirements?

A. Create a AWS Lambda function to keep track of the IPs for all the ALBs in different Regions. Keep refreshing this list.  
B. Set up a Network Load Balancer (NLB) with Elastic IPs. Register the private IPs of all the ALBs as targets to this NLB.  
C. Launch AWS Global Accelerator and create endpoints for all the Regions. Register all the ALBs in different Regions to the corresponding endpoints.  
D. Set up an Amazon EC2 instance, assign an Elastic IP to this EC2 instance, and configure the instance as a proxy to forward traffic to all the ALBs.

**Correct Answer:**  
C. Launch AWS Global Accelerator and create endpoints for all the Regions. Register all the ALBs in different Regions to the corresponding endpoints.

#### Exam Question 90

A company is planning to migrate its virtual server-based workloads to AWS. The company has internet facing load balancers backed by application servers. The application servers rely on patches from an internet-hosted repository.

Which services should a solutions architect recommend be hosted on the public subnet? (Choose two.)

A. NAT gateway  
B. Amazon RDS DB instances  
C. Application Load Balancers  
D. Amazon EC2 application servers  
E. Amazon Elastic File System (Amazon EFS) volumes

**Correct Answer:**  
A. NAT gateway  
C. Application Load Balancers

#### Exam Question 91

A company has established a new AWS account. The account is newly provisioned and no changed have been made to the default settings. The company is concerned about the security of the AWS account root user.

What should be done to secure the root user?

A. Create IAM users for daily administrative tasks. Disable the root user.  
B. Create IAM users for daily administrative tasks. Enable multi-factor authentication on the root user.  
C. Generate an access key for the root user. Use the access key for daily administration tasks instead of the AWS Management Console.  
D. Provide the root user credentials to the most senior solutions architect. Have the solutions architect use the root user for daily administration tasks.

**Correct Answer:**  
B. Create IAM users for daily administrative tasks. Enable multi-factor authentication on the root user.

#### Exam Question 92

A company requires a durable backup storage solution for its on-premises database servers while ensuring on-premises applications maintain access to these backups for quick recovery. The company will use AWS storage services as the destination for these backups. A solutions architect is designing a solution with minimal operational overhead.

Which solution should the solutions architect implement?

A. Deploy an AWS Storage Gateway file gateway on-premises and associate it with an Amazon S3 bucket.  
B. Back up the databases to an AWS Storage Gateway volume gateway and access it using the Amazon S3 API.  
C. Transfer the database backup files to an Amazon Elastic Block Store (Amazon EBS) volume attached to an Amazon EC2 instance.  
D. Back up the database directly to an AWS Snowball device and use lifecycle rules to move the data to Amazon S3 Glacier Deep Archive.

**Correct Answer:**  
A. Deploy an AWS Storage Gateway file gateway on-premises and associate it with an Amazon S3 bucket.

**Answer Description:**  
Network Load Balancer overview

A Network Load Balancer functions at the fourth layer of the Open Systems Interconnection (OSI) model. It can handle millions of requests per second. After the load balancer receives a connection request, it selects a target from the target group for the default rule. It attempts to open a TCP connection to the selected target on the port specified in the listener configuration.

When you enable an Availability Zone for the load balancer, Elastic Load Balancing creates a load balancer node in the Availability Zone. By default, each load balancer node distributes traffic across the registered targets in its Availability Zone only. If you enable cross-zone load balancing, each load balancer node distributes traffic across the registered targets in all enabled Availability Zones. For more information, see Availability Zones.

If you enable multiple Availability Zones for your load balancer and ensure that each target group has at least one target in each enabled Availability Zone, this increases the fault tolerance of your applications. For example, if one or more target groups does not have a healthy target in an Availability Zone, we remove the IP address for the corresponding subnet from DNS, but the load balancer nodes in the other Availability Zones are still available to route traffic. If a client doesn’t honor the time-to-live (TTL) and sends requests to the IP address after it is removed from DNS, the requests fail.

For TCP traffic, the load balancer selects a target using a flow hash algorithm based on the protocol, source IP address, source port, destination IP address, destination port, and TCP sequence number. The TCP connections from a client have different source ports and sequence numbers, and can be routed to different targets. Each individual TCP connection is routed to a single target for the life of the connection.

For UDP traffic, the load balancer selects a target using a flow hash algorithm based on the protocol, source IP address, source port, destination IP address, and destination port. A UDP flow has the same source and destination, so it is consistently routed to a single target throughout its lifetime. Different UDP flows have different source IP addresses and ports, so they can be routed to different targets.

An Auto Scaling group contains a collection of Amazon EC2 instances that are treated as a logical grouping for the purposes of automatic scaling and management. An Auto Scaling group also enables you to use Amazon EC2 Auto Scaling features such as health check replacements and scaling policies. Both maintaining the number of instances in an Auto Scaling group and automatic scaling are the core functionality of the Amazon EC2 Auto Scaling service.

The size of an Auto Scaling group depends on the number of instances that you set as the desired capacity. You can adjust its size to meet demand, either manually or by using automatic scaling.

An Auto Scaling group starts by launching enough instances to meet its desired capacity. It maintains this number of instances by performing periodic health checks on the instances in the group. The Auto Scaling group continues to maintain a fixed number of instances even if an instance becomes unhealthy. If an instance becomes unhealthy, the group terminates the unhealthy instance and launches another instance to replace it.

#### Exam Question 93

A company decides to migrate its three-tier web application from on-premises to the AWS Cloud. The new database must be capable of dynamically scaling storage capacity and performing table joins.

Which AWS service meets these requirements?

A. Amazon Aurora  
B. Amazon RDS for SqlServer  
C. Amazon DynamoDB Streams  
D. Amazon DynamoDB on-demand

**Correct Answer:**  
A. Amazon Aurora

#### Exam Question 94

A company is using a VPC peering strategy to connect its VPCs in a single Region to allow for cross communication.

A recent increase in account creations and VPCs has made it difficult to maintain the VPC peering strategy, and the company expects to grow to hundreds of VPCs. There are also new requests to create site-to-site VPNs with some of the VPCs. A solutions architect has been tasked with creating a centrally managed networking setup for multiple accounts, VPCs, and VPNs.

Which networking solution meets these requirements?

A. Configure shared VPCs and VPNs and share to each other.  
B. Configure a hub-and-spoke VPC and route all traffic through VPC peering.  
C. Configure an AWS Direct Connect connection between all VPCs and VPNs.  
D. Configure a transit gateway with AWS Transit Gateway and connect all VPCs and VPNs.

**Correct Answer:**  
D. Configure a transit gateway with AWS Transit Gateway and connect all VPCs and VPNs.

#### Exam Question 95

A solutions architect is helping a developer design a new eCommerce shopping cart application using AWS services. The developer is unsure of the current database schema and expects to make changes as the eCommerce site grows. The solution needs to be highly resilient and capable of automatically scaling read and write capacity.

Which database solution meets these requirements?

A. Amazon Aurora PostgreSQL  
B. Amazon DynamoDB with on-demand enabled  
C. Amazon DynamoDB with DynamoDB Streams enabled  
D. Amazon SQS and Amazon Aurora PostgreSQL

**Correct Answer:**  
B. Amazon DynamoDB with on-demand enabled

**References:**

* [Anúncio do Amazon DynamoDB sob demanda](https://aws.amazon.com/pt/about-aws/whats-new/2018/11/announcing-amazon-dynamodb-on-demand/)

#### Exam Question 96

A solutions architect must migrate a Windows internet information Services (IIS) web application to AWS.

The application currently relies on a file share hosted in the user’s on-premises network-attached storage (NAS). The solutions architected has proposed migrating the IIS web servers.

Which replacement to the on-premises file share is MOST resilient and durable?

A. Migrate the file Share to Amazon RDS.  
B. Migrate the file Share to AWS Storage Gateway  
C. Migrate the file Share to Amazon FSx for Windows File Server.  
D. Migrate the file share to Amazon Elastic File System (Amazon EFS)

**Correct Answer:**  
C. Migrate the file Share to Amazon FSx for Windows File Server.

#### Exam Question 97

A company needs to implement a relational database with a multi-Region disaster recovery Recovery Point Objective (RPO) of 1 second and a Recovery Time Objective (RTO) of 1 minute.

Which AWS solution can achieve this?

A. Amazon Aurora Global Database  
B. Amazon DynamoDB global tables  
C. Amazon RDS for MySQL with Multi-AZ enabled  
D. Amazon RDS for MySQL with a cross-Region snapshot copy

**Correct Answer:**  
A. Amazon Aurora Global Database

**Answer Description:**  
Cross-Region Disaster Recovery: If your primary region suffers a performance degradation or outage, you can promote one of the secondary regions to take read/write responsibilities. An Aurora cluster can recover in less than 1 minute even in the event of a complete regional outage. This provides your application with an effective Recovery Point Objective (RPO) of 1 second and a Recovery Time Objective (RTO) of less than 1 minute, providing a strong foundation for a global business continuity plan.

#### Exam Question 98

A company is reviewing its AWS Cloud deployment to ensure its data is not accessed by anyone without appropriate authorization. A solutions architect is tasked with identifying all open Amazon S3 buckets and recording any S3 bucket configuration changes.

What should the solutions architect do to accomplish this?

A. Enable AWS Config service with the appropriate rules  
B. Enable AWS Trusted Advisor with the appropriate checks.  
C. Write a script using an AWS SDK to generate a bucket report  
D. Enable Amazon S3 server access logging and configure Amazon CloudWatch Events.

**Correct Answer:**  
A. Enable AWS Config service with the appropriate rules

#### Exam Question 99

A company is planning to build a new web application on AWS. The company expects predictable traffic most of the year and very high traffic on occasion. The web application needs to be highly available and fault tolerant with minimal latency.

What should a solutions architect recommend to meet these requirements?

A. Use an Amazon Route 53 routing policy to distribute requests to two AWS Regions, each with one Amazon EC2 instance.  
B. Use Amazon EC2 instances in an Auto Scaling group with an Application Load Balancer across multiple Availability Zones.  
C. Use Amazon EC2 instances in a cluster placement group with an Application Load Balancer across multiple Availability Zones.  
D. Use Amazon EC2 instances in a cluster placement group and include the cluster placement group within a new Auto Scaling group.

**Correct Answer:**  
B. Use Amazon EC2 instances in an Auto Scaling group with an Application Load Balancer across multiple Availability Zones.

#### Exam Question 100

A solutions architect has configured the following IAM policy.

A solutions architect has configured the following IAM policy.

Which action will be allowed by the policy?

A. An AWS Lambda function can be deleted from any network.  
B. An AWS Lambda function can be created from any network.  
C. An AWS Lambda function can be deleted from the 100.220.0.0/20 network.  
D. An AWS Lambda function can be deleted from the 220.100.16.0/20 network.

**Correct Answer:**  
C. An AWS Lambda function can be deleted from the 100.220.0.0/20 network.

# AWS Certified Solutions Architect – Associate SAA-C02 Exam Questions and Answers – Page 2

The latest AWS Certified Solutions Architect – Associate SAA-C02 certification actual real practice exam question and answer (Q&A) dumps are available free, which are helpful for you to pass the AWS Certified Solutions Architect – Associate SAA-C02 exam and earn AWS Certified Solutions Architect – Associate SAA-C02 certification.

#### Exam Question 101

A solutions architect is using Amazon S3 to design the storage architecture of a new digital media application. The media files must be resilient to the loss of an Availability Zone. Some files are accessed frequently while other files are rarely accessed in an unpredictable pattern. The solutions architect must minimize the costs of storing and retrieving the media files.

Which storage option meets these requirements?

A. S3 Standard  
B. S3 Intelligent-Tiering  
C. S3 Standard-Infrequent Access (S3 Standard-IA)  
D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

**Correct Answer:**  
B. S3 Intelligent-Tiering

**Answer Description:**  
S3 Intelligent-Tiering is a new Amazon S3 storage class designed for customers who want to optimize storage costs automatically when data access patterns change, without performance impact or operational overhead. S3 Intelligent-Tiering is the first cloud object storage class that delivers automatic cost savings by moving data between two access tiers – frequent access and infrequent access – when access patterns change, and is ideal for data with unknown or changing access patterns.

S3 Intelligent-Tiering stores objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. For a small monthly monitoring and automation fee per object, S3 Intelligent-Tiering monitors access patterns and moves objects that have not been accessed for 30 consecutive days to the infrequent access tier. There are no retrieval fees in S3 Intelligent-Tiering. If an object in the infrequent access tier is accessed later, it is automatically moved back to the frequent access tier. No additional tiering fees apply when objects are moved between access tiers within the S3 Intelligent-Tiering storage class. S3 Intelligent-Tiering is designed for 99.9% availability and 99.999999999% durability, and offers the same low latency and high throughput performance of S3 Standard.

#### Exam Question 102

A company is running a three-tier web application to process credit card payments. The front-end user interface consists of static webpages. The application tier can have long-running processes. The database tier uses MySQL.

The application is currently running on a single, general-purpose large Amazon EC2 instance. A solutions architect needs to decouple the services to make the web application highly available.

Which solution would provide the HIGHEST availability?

A. Move static assets to Amazon CloudFront. Leave the application in EC2 in an Auto Scaling group. Move the database to Amazon RDS to deploy Multi-AZ.  
B. Move static assets and the application into a medium EC2 instance. Leave the database on the large instance. Place both instances in an Auto Scaling group.  
C. Move static assets to Amazon S3, Move the application to AWS Lambda with the concurrency limit set. Move the database to Amazon DynamoDB with on-demand enabled.  
D. Move static assets to Amazon S3. Move the application to Amazon Elastic Container Service (Amazon ECS) containers with Auto Scaling enabled. Move the database to Amazon RDS to deploy Multi-AZ.

**Correct Answer:**  
B. Move static assets and the application into a medium EC2 instance. Leave the database on the large instance. Place both instances in an Auto Scaling group.

#### Exam Question 103

A solutions architect is designing the cloud architecture for a new application being deployed to AWS. The application allows users to interactively download and upload files. Files older than 2 years will be accessed less frequently. The solutions architect needs to ensure that the application can scale to any number of files while maintaining high availability and durability.

Which scalable solutions should the solutions architect recommend? (Choose two.)

A. Store the files on Amazon S3 with a lifecycle policy that moves objects older than 2 years to S3 Glacier.  
B. Store the files on Amazon S3 with a lifecycle policy that moves objects older than 2 years to S3 Standard-Infrequent Access (S3 Standard-IA)  
C. Store the files on Amazon Elastic File System (Amazon EFS) with a lifecycle policy that moves objects older than 2 years to EFS Infrequent Access (EFS IA).  
D. Store the files in Amazon Elastic Block Store (Amazon EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data older than 2 years.  
E. Store the files in RAID-striped Amazon Elastic Block Store (Amazon EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data older than 2 years.

**Correct Answer:**  
A. Store the files on Amazon S3 with a lifecycle policy that moves objects older than 2 years to S3 Glacier.  
C. Store the files on Amazon Elastic File System (Amazon EFS) with a lifecycle policy that moves objects older than 2 years to EFS Infrequent Access (EFS IA).

#### Exam Question 104

A company has recently updated its internal security standards. The company must now ensure all Amazon S3 buckets and Amazon Elastic Block Store (Amazon EBS) volumes are encrypted with keys created and periodically rotated by internal security specialists. The company is looking for a native, software-based AWS service to accomplish this goal.

What should a solutions architect recommend as a solution?

A. Use AWS Secrets Manager with customer master keys (CMKs) to store master key material and apply a routine to create a new CMK periodically and replace it in AWS Secrets Manager.  
B. Use AWS Key Management Service (AWS KMS) with customer master keys (CMKs) to store master key material and apply a routine to re-create a new key periodically and replace it in AWS KMS.  
C. Use an AWS CloudHSM cluster with customer master keys (CMKs) to store master key material and apply a routine to re-create a new key periodically and replace it in the CloudHSM cluster nodes.  
D. Use AWS Systems Manager Parameter Store with customer master keys (CMKs) to store master key material and apply a routine to re-create a new key periodically and replace it in the Parameter Store.

**Correct Answer:**  
A. Use AWS Secrets Manager with customer master keys (CMKs) to store master key material and apply a routine to create a new CMK periodically and replace it in AWS Secrets Manager.

#### Exam Question 105

A company’s dynamic website is hosted using on-premises servers in the United States. The company is launching its product in Europe, and it wants to optimize site loading times for new European users. The site’s backend must remain in the United States. The product is being launched in a few days, and an immediate solution is needed.

What should the solutions architect recommend?

A. Launch an Amazon EC2 instance in us-east-1 and migrate the site to it.  
B. Move the website to Amazon S3. Use cross-Region replication between Regions.  
C. Use Amazon CloudFront with a custom origin pointing to the on-premises servers.  
D. Use an Amazon Route 53 geo-proximity routing policy pointing to on-premises servers.

**Correct Answer:**  
C. Use Amazon CloudFront with a custom origin pointing to the on-premises servers.

#### Exam Question 106

A company is hosting multiple websites for several lines of business under its registered parent domain.

Users accessing these websites will be routed to appropriate backend Amazon EC2 instances based on the subdomain. The websites host static webpages, images, and server-side scripts like PHP and JavaScript. Some of the websites experience peak access during the first two hours of business with constant usage throughout the rest of the day. A solutions architect needs to design a solution that will automatically adjust capacity to these traffic patterns while keeping costs low.

Which combination of AWS services or features will meet these requirements? (Choose two.)

A. AWS Batch  
B. Network Load Balancer  
C. Application Load Balancer  
D. Amazon EC2 Auto Scaling  
E. Amazon S3 website hosting

**Correct Answer:**  
C. Application Load Balancer  
D. Amazon EC2 Auto Scaling

**References:**

* Amazon Simple Storage Service > User Guide > [Hosting a static website using Amazon S3](https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteHosting.html)

#### Exam Question 107

A company uses an Amazon S3 bucket to store static images for its website. The company configured permissions to allow access to Amazon S3 objects by privileged users only.

What should a solutions architect do to protect against data loss? (Choose two.)

A. Enable versioning on the S3 bucket.  
B. Enable access logging on the S3 bucket.  
C. Enable server-side encryption on the S3 bucket.  
D. Configure an S3 lifecycle rule to transition objects to Amazon S3 Glacier.  
E. Use MFA Delete to require multi-factor authentication to delete an object.

**Correct Answer:**  
A. Enable versioning on the S3 bucket.  
E. Use MFA Delete to require multi-factor authentication to delete an object.

#### Exam Question 108

An operations team has a standard that states IAM policies should not be applied directly to users. Some new team members have not been following this standard. The operations manager needs a way to easily identify the users with attached policies.

What should a solutions architect do to accomplish this?

A. Monitor using AWS CloudTrail.  
B. Create an AWS Config rule to run daily.  
C. Publish IAM user changes to Amazon SNS.  
D. Run AWS Lambda when a user is modified.

**Correct Answer:**  
B. Create an AWS Config rule to run daily.

**Answer Description:**  
A new AWS Config rule is deployed in the account after you enable AWS Security Hub. The AWS Config rule reacts to resource configuration and compliance changes and send these change items to AWS CloudWatch. When AWS CloudWatch receives the compliance change, a CloudWatch event rule triggers the AWS Lambda function.

#### Exam Question 109

A company hosts its website on AWS. To address the highly variable demand, the company has implemented Amazon EC2 Auto Scaling.

Management is concerned that the company is over-provisioning its infrastructure, especially at the front end of the three-tier application. A solutions architect needs to ensure costs are optimized without impacting performance.

What should the solutions architect do to accomplish this?

A. Use Auto Scaling with Reserved Instances.  
B. Use Auto Scaling with a scheduled scaling policy.  
C. Use Auto Scaling with the suspend-resume feature.  
D. Use Auto Scaling with a target tracking scaling policy.

**Correct Answer:**  
D. Use Auto Scaling with a target tracking scaling policy.

**References:**

* Amazon EC2 Auto Scaling > User Guid > [Target tracking scaling policies for Amazon EC2 Auto Scaling](https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html)

#### Exam Question 110

A solutions architect is performing a security review of a recently migrated workload. The workload is a web application that consists of Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer.

The solution architect must improve the security posture and minimize the impact of a DDoS attack on resources.

Which solution is MOST effective?

A. Configure an AWS WAF ACL with rate-based rules. Create an Amazon CloudFront distribution that points to the Application Load Balancer. Enable the WAF ACL on the CloudFront distribution.  
B. Create a custom AWS Lambda function that adds identified attacks into a common vulnerability pool to capture a potential DDoS attack. Use the identified information to modify a network ACL to block access.  
C. Enable VPC Flow Logs and store them in Amazon S3. Create a custom AWS Lambda functions that parses the logs looking for a DDoS attack. Modify a network ACL to block identified source IP addresses.  
D. Enable Amazon GuardDuty and configure findings written to Amazon CloudWatch. Create an event with CloudWatch Events for DDoS alerts that triggers Amazon Simple Notification Service (Amazon SNS). Have Amazon SNS invoke a custom AWS Lambda function that parses the logs, looking for a DDoS attack. Modify a network ACL to block identified source IP addresses.

**Correct Answer:**  
B. Create a custom AWS Lambda function that adds identified attacks into a common vulnerability pool to capture a potential DDoS attack. Use the identified information to modify a network ACL to block access.

#### Exam Question 111

A company has multiple AWS accounts for various departments. One of the departments wants to share an Amazon S3 bucket with all other departments.

Which solution will require the LEAST amount of effort?

A. Enable cross-account S3 replication for the bucket.  
B. Create a pre-signed URL for the bucket and share it with other departments.  
C. Set the S3 bucket policy to allow cross-account access to other departments.  
D. Create IAM users for each of the departments and configure a read-only IAM policy.

**Correct Answer:**  
C. Set the S3 bucket policy to allow cross-account access to other departments.

**Answer Description:**  
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.

INCORRECT: “Amazon S3 Intelligent-Tiering” is incorrect as there is an additional fee for using this service and for a short-term requirement it may not be beneficial.

INCORRECT: “Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)” is incorrect as this storage class has a minimum capacity charge per object (128 KB) and a per GB retrieval fee. INCORRECT: “Amazon S3 Glacier Deep Archive” is incorrect as this storage class is used for archiving data. There are retrieval fees and it take hours to retrieve data from an archive.

**References:**

* [Amazon S3 Storage Classes](https://aws.amazon.com/s3/storage-classes/)

#### Exam Question 112

A company needs to share an Amazon S3 bucket with an external vendor. The bucket owner must be able to access all objects.

Which action should be taken to share the S3 bucket?

A. Update the bucket to be a Requester Pays bucket.  
B. Update the bucket to enable cross-origin resource sharing (CORS).  
C. Create a bucket policy to require users to grant bucket-owner-full-control when uploading objects.  
D. Create an IAM policy to require users to grant bucket-owner-full-control when uploading objects.

**Correct Answer:**  
C. Create a bucket policy to require users to grant bucket-owner-full-control when uploading objects.

**Answer Description:**  
By default, an S3 object is owned by the AWS account that uploaded it. This is true even when the bucket is owned by another account. To get access to the object, the object owner must explicitly grant you (the bucket owner) access. The object owner can grant the bucket owner full control of the object by updating the access control list (ACL) of the object. The object owner can update the ACL either during a put or copy operation, or after the object is added to the bucket.

Resolution Add a bucket policy that grants users access to put objects in your bucket only when they grant you (the bucket owner) full control of the object.

#### Exam Question 113

A company has a custom application running on an Amazon EC instance that:

* Reads a large amount of data from Amazon S3
* Performs a multi-stage analysis
* Writes the results to Amazon DynamoDB

The application writes a significant number of large, temporary files during the multi-stage analysis. The process performance depends on the temporary storage performance.

What would be the fastest storage option for holding the temporary files?

A. Multiple Amazon S3 buckets with Transfer Acceleration for storage.  
B. Multiple Amazon EBS drives with Provisioned IOPS and EBS optimization.  
C. Multiple Amazon EFS volumes using the Network File System version 4.1 (NFSv4.1) protocol.  
D. Multiple instance store volumes with software RAID 0.

**Correct Answer:**  
A. Multiple Amazon S3 buckets with Transfer Acceleration for storage.

#### Exam Question 114

A leasing company generates and emails PDF statements every month for all its customers. Each statement is about 400 KB in size.

Customers can download their statements from the website for up to 30 days from when the statements were generated. At the end of their 3-year lease, the customers are emailed a ZIP file that contains all the statements.

What is the MOST cost-effective storage solution for this situation?

A. Store the statements using the Amazon S3 Standard storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 1 day.  
B. Store the statements using the Amazon S3 Glacier storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier Deep Archive storage after 30 days.  
C. Store the statements using the Amazon S3 Standard storage class. Create a lifecycle policy to move the statements to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) storage after 30 days.  
D. Store the statements using the Amazon S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 30 days.

**Correct Answer:**  
B. Store the statements using the Amazon S3 Glacier storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier Deep Archive storage after 30 days.

#### Exam Question 115

A company recently released a new type of internet-connected sensor. The company is expecting to sell thousands of sensors, which are designed to stream high volumes of data each second to a central location. A solutions architect must design a solution that ingests and stores data so that engineering teams can analyze it in near-real-time with millisecond responsiveness.

Which solution should the solutions architect recommend?

A. Use an Amazon SQS queue to ingest the data. Consume the data with an AWS Lambda function, which then stores the data in Amazon Redshift.  
B. Use an Amazon SQS queue to ingest the data. Consume the data with an AWS Lambda function, which then stores the data in Amazon DynamoDB.  
C. Use Amazon Kinesis Data Streams to ingest the data. Consume the data with an AWS Lambda function, which then stores the data in Amazon Redshift.  
D. Use Amazon Kinesis Data Streams to ingest the data. Consume the data with an AWS Lambda function, which then stores the data in Amazon DynamoDB.

**Correct Answer:**  
D. Use Amazon Kinesis Data Streams to ingest the data. Consume the data with an AWS Lambda function, which then stores the data in Amazon DynamoDB.

**References:**

AWS Big Data Blog > [Analyze data in Amazon DynamoDB using Amazon SageMaker for real-time prediction](https://aws.amazon.com/blogs/big-data/analyze-data-in-amazon-dynamodb-using-amazon-sagemaker-for-real-time-prediction/)

#### Exam Question 116

A website runs a web application that receives a burst of traffic each day at noon. The users upload new pictures and content daily, but have been complaining of timeouts. The architecture uses Amazon EC2 Auto Scaling groups, and the custom application consistently takes 1 minute to initiate upon boot up before responding to user requests.

How should a solutions architect redesign the architecture to better respond to changing traffic?

A. Configure a Network Load Balancer with a slow start configuration.  
B. Configure AWS ElastiCache for Redis to offload direct requests to the servers.  
C. Configure an Auto Scaling step scaling policy with an instance warmup condition.  
D. Configure Amazon CloudFront to use an Application Load Balancer as the origin.

**Correct Answer:**  
C. Configure an Auto Scaling step scaling policy with an instance warmup condition.

**Answer Description:**  
If you are creating a step policy, you can specify the number of seconds that it takes for a newly launched instance to warm up. Until its specified warm-up time has expired, an instance is not counted toward the aggregated metrics of the Auto Scaling group. Using the example in the Step Adjustments section, suppose that the metric gets to 60, and then it gets to 62 while the new instance is still warming up. The current capacity is still 10 instances, so 1 instance is added (10 percent of 10 instances). However, the desired capacity of the group is already 11 instances, so the scaling policy does not increase the desired capacity further. If the metric gets to 70 while the new instance is still warming up, we should add 3 instances (30 percent of 10 instances). However, the desired capacity of the group is already 11, so we add only 2 instances, for a new desired capacity of 13 instances.

**References:**  
Amazon EC2 Auto Scaling > User Guide > [Step and simple scaling policies for Amazon EC2 Auto Scaling](https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-simple-step.html#as-step-%20scaling-warmup)

#### Exam Question 117

A company has an application that posts messages to Amazon SQS. Another application polls the queue and processes the messages in an I/O-intensive operation. The company has a service level agreement (SLA) that specifies the maximum amount of time that can elapse between receiving the messages and responding to the users. Due to an increase in the number of messages, the company has difficulty meeting its SLA consistently.

What should a solutions architect do to help improve the application’s processing time and ensure it can handle the load at any level?

A. Create an Amazon Machine Image (AMI) from the instance used for processing. Terminate the instance and replace it with a larger size.  
B. Create an Amazon Machine Image (AMI) from the instance used for processing. Terminate the instance and replace it with an Amazon EC2 Dedicated Instance.  
C. Create an Amazon Machine Image (AMI) from the instance used for processing. Create an Auto Scaling group using this image in its launch configuration. Configure the group with a target tracking policy to keep its aggregate CPU utilization below 70%.  
D. Create an Amazon Machine Image (AMI) from the instance used for processing. Create an Auto Scaling group using this image in its launch configuration. Configure the group with a target tracking policy based on the age of the oldest message in the SQS queue.

**Correct Answer:**  
D. Create an Amazon Machine Image (AMI) from the instance used for processing. Create an Auto Scaling group using this image in its launch configuration. Configure the group with a target tracking policy based on the age of the oldest message in the SQS queue.

#### Exam Question 118

A company is designing a new web service that will run on Amazon EC2 instances behind an Elastic Load Balancer. However, many of the web service clients can only reach IP addresses whitelisted on their firewalls.

What should a solutions architect recommend to meet the clients’ needs?

A. A Network Load Balancer with an associated Elastic IP address.  
B. An Application Load Balancer with an associated Elastic IP address  
C. An A record in an Amazon Route 53 hosted zone pointing to an Elastic IP address  
D. An EC2 instance with a public IP address running as a proxy in front of the load balancer

**Correct Answer:**  
C. An A record in an Amazon Route 53 hosted zone pointing to an Elastic IP address

**Answer Description:**  
Route 53 routes end users to Internet applications so the correct answer is C. Map one of the whitelisted IP addresses using an A record to the Elastic IP address.

#### Exam Question 119

A company’s packaged application dynamically creates and returns single-use text files in response to user requests. The company is using Amazon CloudFront for distribution, but wants to further reduce data transfer costs. The company cannot modify the application’s source code.

What should a solutions architect do to reduce costs?

A. Use Lambda@Edge to compress the files as they are sent to users.  
B. Enable Amazon S3 Transfer Acceleration to reduce the response times.  
C. Enable caching on the CloudFront distribution to store generated files at the edge.  
D. Use Amazon S3 multipart uploads to move the files to Amazon S3 before returning them to users.

**Correct Answer:**  
A. Use Lambda@Edge to compress the files as they are sent to users.

**Answer Description:**  
B seems more expensive; C does not seem right because they are single use files and will not be needed again from the cache; D multipart mainly for large files and will not reduce data and cost; A seems the best: change the application code to compress the files and reduce the amount of data transferred to save costs.

#### Exam Question 120

A company is planning to deploy an Amazon RDS DB instance running Amazon Aurora. The company has a backup retention policy requirement of 90 days. Which solution should a solutions architect recommend?

A. Set the backup retention period to 90 days when creating the RDS DB instance.  
B. Configure RDS to copy automated snapshots to a user-managed Amazon S3 bucket with a lifecycle policy set to delete after 90 days.  
C. Create an AWS Backup plan to perform a daily snapshot of the RDS database with the retention set to 90 days. Create an AWS Backup job to schedule the execution of the backup plan daily.  
D. Use a daily scheduled event with Amazon CloudWatch Events to execute a custom AWS Lambda function that makes a copy of the RDS automated snapshot. Purge snapshots older than 90 days.

**Correct Answer:**  
B. Configure RDS to copy automated snapshots to a user-managed Amazon S3 bucket with a lifecycle policy set to delete after 90 days.

#### Exam Question 121

A company currently has 250 TB of backup files stored in Amazon S3 in a vendor’s proprietary format.

Using a Linux-based software application provided by the vendor, the company wants to retrieve files from Amazon S3, transform the files to an industry-standard format, and re-upload them to Amazon S3. The company wants to minimize the data transfer charges associated with this conversation.

What should a solutions architect do to accomplish this?

A. Install the conversion software as an Amazon S3 batch operation so the data is transformed without leaving Amazon S3.  
B. Install the conversion software onto an on-premises virtual machine. Perform the transformation and reupload the files to Amazon S3 from the virtual machine.  
C. Use AWS Snowball Edge devices to export the data and install the conversion software onto the devices. Perform the data transformation and re-upload the files to Amazon S3 from the Snowball Edge devices.  
D. Launch an Amazon EC2 instance in the same Region as Amazon S3 and install the conversion software onto the instance. Perform the transformation and re-upload the files to Amazon S3 from the EC2 instance.

**Correct Answer:**  
D. Launch an Amazon EC2 instance in the same Region as Amazon S3 and install the conversion software onto the instance. Perform the transformation and re-upload the files to Amazon S3 from the EC2 instance.

#### Exam Question 122

A company is migrating a NoSQL database cluster to Amazon EC2. The database automatically replicates data to maintain at least three copies of the data. I/O throughput of the servers is the highest priority. Which instance type should a solutions architect recommend for the migration?

A. Storage optimized instances with instance store  
B. Burstable general purpose instances with an Amazon Elastic Block Store (Amazon EBS) volume  
C. Memory optimized instances with Amazon Elastic Block Store (Amazon EBS) optimization enabled  
D. Compute optimized instances with Amazon Elastic Block Store (Amazon EBS) optimization enabled

**Correct Answer:**  
A. Storage optimized instances with instance store

#### Exam Question 123

A company has a large Microsoft SharePoint deployment running on-premises that requires Microsoft Windows shared file storage. The company wants to migrate this workload to the AWS Cloud and is considering various storage options. The storage solution must be highly available and integrated with Active Directory for access control.

Which solution will satisfy these requirements?

A. Configure Amazon EFS storage and set the Active Directory domain for authentication.  
B. Create an SMB file share on an AWS Storage Gateway file gateway in two Availability Zones.  
C. Create an Amazon S3 bucket and configure Microsoft Windows Server to mount it as a volume.  
D. Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directory domain for authentication.

**Correct Answer:**  
D. Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directory domain for authentication.

**Answer Description:**  
Amazon FSx for Windows File Server provides fully managed, highly reliable, and scalable file storage that is accessible over the industry-standard Server 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. It offers single-AZ and multi-AZ deployment options, fully managed backups, and encryption of data at rest and in transit. You can optimize cost and performance for your workload needs with SSD and HDD storage options; and you can scale storage and change the throughput performance of your file system at any time. Amazon FSx file storage is accessible from Windows, Linux, and macOS compute instances and devices running on AWS or on premises.

Works with Microsoft Active Directory (AD) to easily integrate file systems with Windows environments.

CORRECT: “Amazon FSx” is the correct answer.

INCORRECT: “Amazon EFS” is incorrect as EFS only supports Linux systems. INCORRECT: “Amazon S3” is incorrect as this is not a suitable replacement for a Microsoft filesystem.

INCORRECT: “AWS Storage Gateway” is incorrect as this service is primarily used for connecting on-premises storage to cloud storage. It consists of a software device installed on-premises and can be used with SMB shares but it actually stores the data on S3. It is also used for migration. However, in this case the company need to replace the file server farm and Amazon FSx is the best choice for this job.

**References:**  
Amazon FSx for Windows File Server > Windows User Guide > [Availability and durability: Single-AZ and Multi-AZ file systems](https://docs.aws.amazon.com/fsx/latest/WindowsGuide/high-availability-multiAZ.html)

#### Exam Question 124

A company has a web application with sporadic usage patterns. There is heavy usage at the beginning of each month, moderate usage at the start of each week, and unpredictable usage during the week. The application consists of a web server and a MySQL database server running inside the data center. The company would like to move the application to the AWS Cloud, and needs to select a cost-effective database platform that will not require database modifications.

Which solution will meet these requirements?

A. Amazon DynamoDB  
B. Amazon RDS for MySQL  
C. MySQL-compatible Amazon Aurora Serverless  
D. MySQL deployed on Amazon EC2 in an Auto Scaling group

**Correct Answer:**  
B. Amazon RDS for MySQL

#### Exam Question 125

A solutions architect is creating an application that will handle batch processing of large amounts of data.

The input data will be held in Amazon S3 and the output data will be stored in a different S3 bucket. For processing, the application will transfer the data over the network between multiple Amazon EC2 instances.

What should the solutions architect do to reduce the overall data transfer costs?

A. Place all the EC2 instances in an Auto Scaling group.  
B. Place all the EC2 instances in the same AWS Region.  
C. Place all the EC2 instances in the same Availability Zone.  
D. Place all the EC2 instances in private subnets in multiple Availability Zones.

**Correct Answer:**  
C. Place all the EC2 instances in the same Availability Zone.

**Answer Description:**  
The transfer is between EC2 instances and not just between S3 and EC2.

Also, be aware of inter-Availability Zones data transfer charges between Amazon EC2 instances, even within the same region. If possible, the instances in a development or test environment that need to communicate with each other should be co-located within the same Availability Zone to avoid data transfer charges. (This doesn’t apply to production workloads which will most likely need to span multiple Availability Zones for high availability.)

**References:**

AWS Management & Governance Blog > [Using AWS Cost Explorer to analyze data transfer costs](https://aws.amazon.com/blogs/mt/using-aws-cost-explorer-to-analyze-data-transfer-costs/)

#### Exam Question 126

A company operates an eCommerce website on Amazon EC2 instances behind an Application Load Balancer (ALB) in an Auto Scaling group. The site is experiencing performance issues related to a high request rate from illegitimate external systems with changing IP addresses. The security team is worried about potential DDoS attacks against the website. The company must block the illegitimate incoming requests in a way that has a minimal impact on legitimate users.

What should a solutions architect recommend?

A. Deploy Amazon Inspector and associate it with the ALB.  
B. Deploy AWS WAF, associate it with the ALB, and configure a rate-limiting rule.  
C. Deploy rules to the network ACLs associated with the ALB to block the incoming traffic.  
D. Deploy Amazon GuardDuty and enable rate-limiting protection when configuring GuardDuty.

**Correct Answer:**  
B. Deploy AWS WAF, associate it with the ALB, and configure a rate-limiting rule.

**Answer Description:**  
Rate limit

For a rate-based rule, enter the maximum number of requests to allow in any five-minute period from an IP address that matches the rule’s conditions. The rate limit must be at least 100.

You can specify a rate limit alone, or a rate limit and conditions. If you specify only a rate limit, AWS WAF places the limit on all IP addresses. If you specify a rate limit and conditions, AWS WAF places the limit on IP addresses that match the conditions.

When an IP address reaches the rate limit threshold, AWS WAF applies the assigned action (block or count) as quickly as possible, usually within 30 seconds. Once the action is in place, if five minutes pass with no requests from the IP address, AWS WAF resets the counter to zero.

#### Exam Question 127

A company receives structured and semi-structured data from various sources once every day. A solutions architect needs to design a solution that leverages big data processing frameworks. The data should be accessible using SQL queries and business intelligence tools.

What should the solutions architect recommend to build the MOST high-performing solution?

A. Use AWS Glue to process data and Amazon S3 to store data.  
B. Use Amazon EMR to process data and Amazon Redshift to store data.  
C. Use Amazon EC2 to process data and Amazon Elastic Block Store (Amazon EBS) to store data.  
D. Use Amazon Kinesis Data Analytics to process data and Amazon Elastic File System (Amazon EFS) to store data.

**Correct Answer:**  
B. Use Amazon EMR to process data and Amazon Redshift to store data.

#### Exam Question 128

A company is hosting an election reporting website on AWS for users around the world. The website uses Amazon EC2 instances for the web and application tiers in an Auto Scaling group with Application Load Balancers. The database tier uses an Amazon RDS for MySQL database. The website is updated with election results once an hour and has historically observed hundreds of users accessing the reports.

The company is expecting a significant increase in demand because of upcoming elections in different countries. A solutions architect must improve the website’s ability to handle additional demand while minimizing the need for additional EC2 instances.

Which solution will meet these requirements?

A. Launch an Amazon ElastiCache cluster to cache common database queries.  
B. Launch an Amazon CloudFront web distribution to cache commonly requested website content.  
C. Enable disk-based caching on the EC2 instances to cache commonly requested website content.  
D. Deploy a reverse proxy into the design using an EC2 instance with caching enabled for commonly requested website content.

**Correct Answer:**  
B. Launch an Amazon CloudFront web distribution to cache commonly requested website content.

#### Exam Question 129

A company has a 143 TB MySQL database that it wants to migrate to AWS. The plan is to use Amazon Aurora MySQL as the platform going forward. The company has a 100 Mbps AWS Direct Connect connection to Amazon VPC.

Which solution meets the company’s needs and takes the LEAST amount of time?

A. Use a gateway endpoint for Amazon S3. Migrate the data to Amazon S3. Import the data into Aurora.  
B. Upgrade the Direct Connect link to 500 Mbps. Copy the data to Amazon S3. Import the data into Aurora.  
C. Order an AWS Snowmobile and copy the database backup to it. Have AWS import the data into Amazon S3. Import the backup into Aurora.  
D. Order four 50-TB AWS Snowball devices and copy the database backup onto them. Have AWS import the data into Amazon S3. Import the data into Aurora.

**Correct Answer:**  
D. Order four 50-TB AWS Snowball devices and copy the database backup onto them. Have AWS import the data into Amazon S3. Import the data into Aurora.

#### Exam Question 130

A company hosts an online shopping application that stores all orders in an Amazon RDS for PostgreSQL Single-AZ DB instance.

Management wants to eliminate single points of failure and has asked a solutions architect to recommend an approach to minimize database downtime without requiring any changes to the application code.

Which solution meets these requirements?

A. Convert the existing database instance to a Multi-AZ deployment by modifying the database instance and specifying the Multi-AZ option.  
B. Create a new RDS Multi-AZ deployment. Take a snapshot of the current RDS instance and restore the new Multi-AZ deployment with the snapshot.  
C. Create a read-only replica of the PostgreSQL database in another Availability Zone. Use Amazon Route 53 weighted record sets to distribute requests across the databases.  
D. Place the RDS for PostgreSQL database in an Amazon EC2 Auto Scaling group with a minimum group size of two. Use Amazon Route 53 weighted record sets to distribute requests across instances.

**Correct Answer:**  
A. Convert the existing database instance to a Multi-AZ deployment by modifying the database instance and specifying the Multi-AZ option.

#### Exam Question 131

A company has a 10 Gbps AWS Direct Connect connection from its on-premises servers to AWS. The workloads using the connection are critical. The company requires a disaster recovery strategy with maximum resiliency that maintains the current connection bandwidth at a minimum.

What should a solutions architect recommend?

A. Set up a new Direct Connect connection in another AWS Region.  
B. Set up a new AWS managed VPN connection in another AWS Region.  
C. Set up two new Direct Connect connections: one in the current AWS Region and one in another Region.  
D. Set up two new AWS managed VPN connections: one in the current AWS Region and one in another Region.

**Correct Answer:**  
C. Set up two new Direct Connect connections: one in the current AWS Region and one in another Region.

#### Exam Question 132

As part of budget planning, management wants a report of AWS billed items listed by user. The data will be used to create department budgets. A solutions architect needs to determine the most efficient way to obtain this report information.

Which solution meets these requirements?

A. Run a query with Amazon Athena to generate the report.  
B. Create a report in Cost Explorer and download the report.  
C. Access the bill details from the billing dashboard and download the bill.  
D. Modify a cost budget in AWS Budgets to alert with Amazon Simple Email Service (Amazon SES).

**Correct Answer:**  
B. Create a report in Cost Explorer and download the report.

#### Exam Question 133

A company with facilities in North America, Europe, and Asia is designing new distributed application to optimize its global supply chain and manufacturing process. The orders booked on one continent should be visible to all Regions in a second or less. The database should be able to support failover with a short Recovery Time Objective (RTO). The uptime of the application is important to ensure that manufacturing is not impacted.

What should a solutions architect recommend?

A. Use Amazon DynamoDB global tables.  
B. Use Amazon Aurora Global Database.  
C. Use Amazon RDS for MySQL with a cross-Region read replica.  
D. Use Amazon RDS for PostgreSQL with a cross-Region read replica.

**Correct Answer:**  
B. Use Amazon Aurora Global Database.

**Answer Description:**  
Cross-Region Disaster Recovery: If your primary region suffers a performance degradation or outage, you can promote one of the secondary regions to take read/write responsibilities. An Aurora cluster can recover in less than 1 minute even in the event of a complete regional outage. This provides your application with an effective Recovery Point Objective (RPO) of 1 second and a Recovery Time Objective (RTO) of less than 1 minute, providing a strong foundation for a global business continuity plan.

#### Exam Question 134

A company’s near-real-time streaming application is running on AWS. As the data is ingested, a job runs on the data and takes 30 minutes to complete. The workload frequently experiences high latency due to large amounts of incoming data. A solutions architect needs to design a scalable and serverless solution to enhance performance.

Which combination of steps should the solutions architect take? (Choose two.)

A. Use Amazon Kinesis Data Firehose to ingest the data.  
B. Use AWS Lambda with AWS Step Functions to process the data.  
C. Use AWS Database Migration Service (AWS DMS) to ingest the data.  
D. Use Amazon EC2 instances in an Auto Scaling group to process the data.  
E. Use AWS Fargate with Amazon Elastic Container Service (Amazon ECS) to process the data.

**Correct Answer:**  
A. Use Amazon Kinesis Data Firehose to ingest the data.  
E. Use AWS Fargate with Amazon Elastic Container Service (Amazon ECS) to process the data.

#### Exam Question 135

An application running on an Amazon EC2 instance needs to access an Amazon DynamoDB table. Both the EC2 instance and the DynamoDB table are in the same AWS account. A solutions architect must configure the necessary permissions.

Which solution will allow least privilege access to the DynamoDB table from the EC2 instance?

A. Create an IAM role with the appropriate policy to allow access to the DynamoDB table. Create an instance profile to assign this IAM role to the EC2 instance.  
B. Create an IAM role with the appropriate policy to allow access to the DynamoDB table. Add the EC2 instance to the trust relationship policy document to allow it to assume the role.  
C. Create an IAM user with the appropriate policy to allow access to the DynamoDB table. Store the credentials in an Amazon S3 bucket and read them from within the application code directly.  
D. Create an IAM user with the appropriate policy to allow access to the DynamoDB table. Ensure that the application stores the IAM credentials securely on local storage and uses them to make the DynamoDB calls.

**Correct Answer:**  
A. Create an IAM role with the appropriate policy to allow access to the DynamoDB table. Create an instance profile to assign this IAM role to the EC2 instance.

#### Exam Question 136

A solutions architect is designing a solution that involves orchestrating a series of Amazon Elastic Container Service (Amazon ECS) task types running on Amazon EC2 instances that are part of an ECS cluster. The output and state data for all tasks needs to be stored. The amount of data output by each task is approximately 10 MB, and there could be hundreds of tasks running at a time. The system should be optimized for high-frequency reading and writing. As old outputs are archived and deleted, the storage size is not expected to exceed 1 TB.

Which storage solution should the solutions architect recommend?

A. An Amazon DynamoDB table accessible by all ECS cluster instances.  
B. An Amazon Elastic File System (Amazon EFS) with Provisioned Throughput mode.  
C. An Amazon Elastic File System (Amazon EFS) file system with Bursting Throughput mode.  
D. An Amazon Elastic Block Store (Amazon EBS) volume mounted to the ECS cluster instances.

**Correct Answer:**  
C. An Amazon Elastic File System (Amazon EFS) file system with Bursting Throughput mode.

#### Exam Question 137

A company wants to migrate its MySQL database from on premises to AWS. The company recently experienced a database outage that significantly impacted the business. To ensure this does not happen again, the company wants a reliable database solution on AWS that minimizes data loss and stores every transaction on at least two nodes.

Which solution meets these requirements?

A. Create an Amazon RDS DB instance with synchronous replication to three nodes in three Availability Zones.  
B. Create an Amazon RDS MySQL DB instance with Multi-AZ functionality enabled to synchronously replicate the data.  
C. Create an Amazon RDS MySQL DB instance and then create a read replica in a separate AWS Region that synchronously replicates the data.  
D. Create an Amazon EC2 instance with a MySQL engine installed that triggers an AWS Lambda function to synchronously replicate the data to an Amazon RDS MySQL DB instance.

**Correct Answer:**  
A. Create an Amazon RDS DB instance with synchronous replication to three nodes in three Availability Zones.

#### Exam Question 138

A company stores user data in AWS. The data is used continuously with peak usage during business hours. Access patterns vary, with some data not being used for months at a time. A solutions architect must choose a cost-effective solution that maintains the highest level of durability while maintaining high availability.

Which storage solution meets these requirements?

A. Amazon S3 Standard  
B. Amazon S3 Intelligent-Tiering  
C. Amazon S3 Glacier Deep Archive  
D. Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

**Correct Answer:**  
B. Amazon S3 Intelligent-Tiering

#### Exam Question 139

A company receives inconsistent service from its data center provider because the company is headquartered in an area affected by natural disasters. The company is not ready to fully migrate to the AWS Cloud, but it wants a failure 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 solution should a solutions architect recommend that has the LEAST amount of downtime?

A. Configure an Amazon 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.  
B. Configure an Amazon Route 53 failover record. Execute an AWS CloudFormation template from a script to create Amazon EC2 instances behind an Application Load Balancer. Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3.  
C. Configure an Amazon Route 53 failover record. Set up an AWS Direct Connect connection between a VPC and the data center. Run application servers on Amazon EC2 in an Auto Scaling group. Run an AWS Lambda function to execute an AWS CloudFormation template to create an Application Load Balancer.  
D. Configure an Amazon Route 53 failover record. Run an AWS Lambda function to execute an AWS CloudFormation template to launch two Amazon EC2 instances. Set up AWS Storage Gateway with stored volumes to back up data to Amazon S3. Set up an AWS Direct Connect connection between a VPC and the data center.

**Correct Answer:**  
A. Configure an Amazon 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.

#### Exam Question 140

What should a solutions architect do to ensure that all objects uploaded to an Amazon S3 bucket are encrypted?

A. Update the bucket policy to deny if the PutObject does not have an s3:x-amz-acl header set.  
B. Update the bucket policy to deny if the PutObject does not have an s3:x-amz-acl header set to private.  
C. Update the bucket policy to deny if the PutObject does not have an aws:SecureTransport header set to true.  
D. Update the bucket policy to deny if the PutObject does not have an x-amz-server-side-encryption header set.

**Correct Answer:**  
D. Update the bucket policy to deny if the PutObject does not have an x-amz-server-side-encryption header set.

#### Exam Question 141

A company uses Application Load Balancers (ALBs) in different AWS Regions. The ALBs receive inconsistent traffic that can spike and drop throughout the year. The company’s networking team needs to allow the IP addresses of the ALBs in the on-premises firewall to enable connectivity.

Which solution is the MOST scalable with minimal configuration changes?

A. Write an AWS Lambda script to get the IP addresses of the ALBs in different Regions. Update the on-premises firewall’s rule to allow the IP addresses of the ALBs.  
B. Migrate all ALBs in different Regions to the Network Load Balancer (NLBs). Update the on-premises firewall’s rule to allow the Elastic IP addresses of all the NLBs.  
C. Launch AWS Global Accelerator. Register the ALBs in different Regions to the accelerator. Update the on-premises firewall’s rule to allow static IP addresses associated with the accelerator.  
D. Launch a Network Load Balancer (NLB) in one Region. Register the private IP addresses of the ALBs in different Regions with the NLB. Update the on-premises firewall’s rule to allow the Elastic IP address attached to the NLB.

**Correct Answer:**  
C. Launch AWS Global Accelerator. Register the ALBs in different Regions to the accelerator. Update the on-premises firewall’s rule to allow static IP addresses associated with the accelerator.

#### Exam Question 142

A company runs a high performance computing (HPC) workload on AWS. The workload required low latency network performance and high network throughput with tightly coupled node-to-node communication. The Amazon EC2 instances are properly sized for compute and storage capacity, and are launched using default options.

What should a solutions architect propose to improve the performance of the workload?

A. Choose a cluster placement group while launching Amazon EC2 instances.  
B. Choose dedicated instance tenancy while launching Amazon EC2 instances.  
C. Choose an Elastic Inference accelerator while launching Amazon EC2 instances.  
D. Choose the required capacity reservation while launching Amazon EC2 instances.

**Correct Answer:**  
A. Choose a cluster placement group while launching Amazon EC2 instances.

#### Exam Question 143

A solutions architect is designing a high performance computing (HPC) workload on Amazon EC2. The EC2 instances need to communicate to each other frequently and require network performance with low latency and high throughput.

Which EC2 configuration meets these requirements?

A. Launch the EC2 instances in a cluster placement group in one Availability Zone.  
B. Launch the EC2 instances in a spread placement group in one Availability Zone.  
C. Launch the EC2 instances in an Auto Scaling group in two Regions and peer the VPCs.  
D. Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones.

**Correct Answer:**  
A. Launch the EC2 instances in a cluster placement group in one Availability Zone.

**Answer Description:**  
When you launch a new EC2 instance, the EC2 service attempts to place the instance in such a way that all of your instances are spread out across underlying hardware to minimize correlated failures. You can use placement groups to influence the placement of a group of interdependent instances to meet the needs of your workload.

Depending on the type of workload, you can create a placement group using one of the following placement strategies:

Cluster • packs instances close together inside an Availability Zone. This strategy enables workloads to achieve the low-latency network performance necessary for tightly-coupled node-to-node communication that is typical of HPC applications.

Partition • spreads your instances across logical partitions such that groups of instances in one partition do not share the underlying hardware with groups of instances in different partitions. This strategy is typically used by large distributed and replicated workloads, such as Hadoop, Cassandra, and Kafka.

Spread • strictly places a small group of instances across distinct underlying hardware to reduce correlated failures.

For this scenario, a cluster placement group should be used as this is the best option for providing low-latency network performance for a HPC application.

CORRECT: “Launch the EC2 instances in a cluster placement group in one Availability Zone” is the correct answer.

INCORRECT: “Launch the EC2 instances in a spread placement group in one Availability Zone” is incorrect as the spread placement group is used to spread instances across distinct underlying hardware.

INCORRECT: “Launch the EC2 instances in an Auto Scaling group in two Regions. Place a Network Load Balancer in front of the instances” is incorrect as this does not achieve the stated requirement to provide low-latency, high throughput network performance between instances. Also, you cannot use an ELB across Regions.

INCORRECT: “Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones” is incorrect as this does not reduce network latency or improve performance.

**References:**

* Amazon Elastic Compute Cloud > User Guide for Linux Instances > [Placement groups](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html)

#### Exam Question 144

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? (Choose two.)

A. Detach a volume on an EC2 instance and copy it to Amazon S3.  
B. Launch a new EC2 instance from an Amazon Machine Image (AMI) in a new Region.  
C. Launch a new EC2 instance in a new Region and copy a volume from Amazon S3 to the new instance.  
D. Copy an Amazon Machine Image (AMI) of an EC2 instance and specify a different Region for the destination.  
E. Copy an Amazon Elastic Block Store (Amazon EBS) volume from Amazon S3 and launch an EC2 instance in the destination Region using that EBS volume.

**Correct Answer:**  
B. Launch a new EC2 instance from an Amazon Machine Image (AMI) in a new Region.  
D. Copy an Amazon Machine Image (AMI) of an EC2 instance and specify a different Region for the destination.

**Answer Description:**  
Cross Region EC2 AMI Copy  
We know that you want to build applications that span AWS Regions and we’re working to provide you with the services and features needed to do so. We started out by launching the EBS Snapshot Copy feature late last year. This feature gave you the ability to copy a snapshot from Region to Region with just a couple of clicks. In addition, last month we made a significant reduction (26% to 83%) in the cost of transferring data between AWS Regions, making it less expensive to operate in more than one AWS region.

Today we are introducing a new feature: Amazon Machine Image (AMI) Copy. AMI Copy enables you to easily copy your Amazon Machine Images between AWS Regions. AMI Copy helps enable several key scenarios including:

Simple and Consistent Multi-Region Deployment – You can copy an AMI from one region to another, enabling you to easily launch consistent instances based on the same AMI into different regions.

Scalability – You can more easily design and build world-scale applications that meet the needs of your users, regardless of their location.

Performance – You can increase performance by distributing your application and locating critical components of your application in closer proximity to your users. You can also take advantage of region specific features such as instance types or other AWS services.

Even Higher Availability – You can design and deploy applications across AWS regions, to increase availability. Once the new AMI is in an Available state the copy is complete.

Once the new AMI is in an Available state the copy is complete.

#### Exam Question 145

A manufacturing company wants to implement predictive maintenance on its machinery equipment. The company will install thousands of IoT sensors that will send data to AWS in real time. A solutions architect is tasked with implementing a solution that will receive events in an ordered manner for each machinery asset and ensure that data is saved for further processing at a later time.

Which solution would be MOST efficient?

A. Use Amazon Kinesis Data Streams for real-time events with a partition for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon S3.  
B. Use Amazon Kinesis Data Streams for real-time events with a shard for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon EBS.  
C. Use an Amazon SQS FIFO queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function for the SQS queue to save data to Amazon EFS.  
D. Use an Amazon SQS standard queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3.

**Correct Answer:**  
A. Use Amazon Kinesis Data Streams for real-time events with a partition for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon S3.

**Answer Description:**  
Amazon SQS Introduces FIFO Queues with Exactly-Once Processing and Lower Prices for Standard Queues

You can now use Amazon Simple Queue Service (SQS) for applications that require messages to be processed in a strict sequence and exactly once using First-in, First-out (FIFO) queues. FIFO queues are designed to ensure that the order in which messages are sent and received is strictly preserved and that each message is processed exactly once.

Amazon SQS is a reliable and highly-scalable managed message queue service for storing messages in transit between application components. FIFO queues complement the existing Amazon SQS standard queues, which offer high throughput, best-effort ordering, and at-least-once delivery. FIFO queues have essentially the same features as standard queues, but provide the added benefits of supporting ordering and exactly-once processing. FIFO queues provide additional features that help prevent unintentional duplicates from being sent by message producers or from being received by message consumers. Additionally, message groups allow multiple separate ordered message streams within the same queue.

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.

For this scenario, the solutions architect can use a partition key for each device. This will ensure the records for that device are grouped by shard and the shard will ensure ordering. Amazon S3 is a valid destination for saving the data records.

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.

INCORRECT: “Use Amazon Kinesis Data Streams for real-time events with a shard for each device. Use Amazon Kinesis Data Firehose to save data to Amazon EBS” is incorrect as you cannot save data to EBS from Kinesis.

INCORRECT: “Use an Amazon SQS FIFO queue for real-time events with one queue for each device. Trigger an AWS Lambda function for the SQS queue to save data to Amazon EFS” is incorrect as SQS is not the most efficient service for streaming, real time data.

INCORRECT: “Use an Amazon SQS standard queue for real-time events with one queue for each device. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3” is incorrect as SQS is not the most efficient service for streaming, real time data.

**References:**

* Amazon Kinesis Data Streams > Developer Guide > [Amazon Kinesis Data Streams Terminology and Concepts](https://docs.aws.amazon.com/streams/latest/dev/key-concepts.html)

#### Exam Question 146

A company currently operates a web application backed by an Amazon RDS MySQL database. It has automated backups that are run daily and are not encrypted. A security audit requires future backups to be encrypted and the unencrypted backups to be destroyed. The company will make at least one encrypted backup before destroying the old backups.

What should be done to enable encryption for future backups?

A. Enable default encryption for the Amazon S3 bucket where backups are stored.  
B. Modify the backup section of the database configuration to toggle the Enable encryption check box.  
C. Create a snapshot of the database. Copy it to an encrypted snapshot. Restore the database from the encrypted snapshot.  
D. Enable an encrypted read replica on RDS for MySQL. Promote the encrypted read replica to primary. Remove the original database instance.

**Correct Answer:**  
C. Create a snapshot of the database. Copy it to an encrypted snapshot. Restore the database from the encrypted snapshot.

**Answer Description:**  
However, because you can encrypt a copy of an unencrypted DB snapshot, you can effectively add encryption to an unencrypted DB instance. That is, you can create a snapshot of your DB instance, and then create an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted snapshot, and thus you have an encrypted copy of your original DB instance.

DB instances that are encrypted can’t be modified to disable encryption.

You can’t have an encrypted read replica of an unencrypted DB instance or an unencrypted read replica of an encrypted DB instance.

Encrypted read replicas must be encrypted with the same key as the source DB instance when both are in the same AWS Region.

You can’t restore an unencrypted backup or snapshot to an encrypted DB instance.

To copy an encrypted snapshot from one AWS Region to another, you must specify the KMS key identifier of the destination AWS Region. This is because KMS encryption keys are specific to the AWS Region that they are created in.

Amazon RDS uses snapshots for backup. Snapshots are encrypted when created only if the database is encrypted and you can only select encryption for the database when you first create it. In this case the database, and hence the snapshots, ad unencrypted.

However, you can create an encrypted copy of a snapshot. You can restore using that snapshot which creates a new DB instance that has encryption enabled. From that point on encryption will be enabled for all snapshots.

CORRECT: “Create a snapshot of the database. Copy it to an encrypted snapshot. Restore the database from the encrypted snapshot” is the correct answer. INCORRECT: “Enable an encrypted read replica on RDS for MySQL. Promote the encrypted read replica to primary.

Remove the original database instance” is incorrect as you cannot create an encrypted read replica from an unencrypted master.

INCORRECT: “Modify the backup section of the database configuration to toggle the Enable encryption check box” is incorrect as you cannot add encryption for an existing database.

INCORRECT: “Enable default encryption for the Amazon S3 bucket where backups are stored” is incorrect because you do not have access to the S3 bucket in which snapshots are stored.

**References:**

* Amazon Relational Database Service > User Guide > [Encrypting Amazon RDS resources](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html)

#### Exam Question 147

An application runs on Amazon EC2 instances across multiple Availability Zones. The instances run in an Amazon EC2 Auto Scaling group behind an Application Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 40%.

What should a solutions architect do to maintain the desired performance across all instances in the group?

A. Use a simple scaling policy to dynamically scale the Auto Scaling group.  
B. Use a target tracking policy to dynamically scale the Auto Scaling group.  
C. Use an AWS Lambda function to update the desired Auto Scaling group capacity.  
D. Use scheduled scaling actions to scale up and scale down the Auto Scaling group.

**Correct Answer:**  
B. Use a target tracking policy to dynamically scale the Auto Scaling group.

**Answer Description:**  
“With target tracking scaling policies, you select a scaling metric and set a target value. Amazon EC2 AutoScaling creates and manages the CloudWatch alarms that trigger the scaling policy and calculates the scaling adjustment based on the metric and the target value. The scaling policy adds or removes capacity as required to keep the metric at, or close to, the specified target value. In addition to keeping the metric close to the target value, a target tracking scaling policy also adjusts to changes in the metric due to a changing load pattern. For example, you can use target tracking scaling to: Configure a target tracking scaling policy to keep the average aggregate CPU utilization of your Auto Scaling group at 40 percent. Configure a target tracking scaling policy to keep the request count per target of your Application Load Balancer target group at 1000 for your AutoScaling group.”

With target tracking scaling policies, you select a scaling metric and set a target value. Amazon EC2 Auto Scaling creates and manages the CloudWatch alarms that trigger the scaling policy and calculates the scaling adjustment based on the metric and the target value.

The scaling policy adds or removes capacity as required to keep the metric at, or close to, the specified target value. In addition to keeping the metric close to the target value, a target tracking scaling policy also adjusts to the changes in the metric due to a changing load pattern.

CORRECT: “Use a target tracking policy to dynamically scale the Auto Scaling group” is the correct answer.

INCORRECT: “Use a simple scaling policy to dynamically scale the Auto Scaling group” is incorrect as target tracking is a better way to keep the aggregate CPU usage at around 40% INCORRECT: “Use an AWS Lambda function to update the desired Auto Scaling group capacity” is incorrect as this can be done automatically.

INCORRECT: “Use scheduled scaling actions to scale up and scale down the Auto Scaling group” is incorrect as dynamic scaling is required to respond to changes in utilization.

**References:**

* Amazon EC2 Auto Scaling > User Guide > [Target tracking scaling policies for Amazon EC2 Auto Scaling](https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html)

#### Exam Question 148

A company runs an internal browser-based application. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. The Auto Scaling group scales up to 20 instances during work hours, but scales down to 2 instances overnight. Staff are complaining that the application is very slow when the day begins, although it runs well by mid-morning.

How should the scaling be changed to address the staff complaints and keep costs to a minimum?

A. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens.  
B. Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period.  
C. Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period.  
D. Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens.

**Correct Answer:**  
A. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens.

**Answer Description:**  
Though this sounds like a good use case for scheduled actions, both answers using scheduled actions will have 20 instances running regardless of actual demand. A better option to be more cost effective is to use a target tracking action that triggers at a lower CPU threshold.

With this solution the scaling will occur before the CPU utilization gets to a point where performance is affected. This will result in resolving the performance issues whilst minimizing costs. Using a reduced cooldown period will also more quickly terminate unneeded instances, further reducing costs.

**References:**

* Amazon EC2 Auto Scaling > User Guide > [Target tracking scaling policies for Amazon EC2 Auto Scaling](https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html)

#### Exam Question 149

A company hosts a static website on-premises and wants to migrate the website to AWS. The website should load as quickly as possible for users around the world. The company also wants the most cost-effective solution.

What should a solutions architect do to accomplish this?

A. Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Replicate the S3 bucket to multiple AWS Regions.  
B. Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Configure Amazon CloudFront with the S3 bucket as the origin.  
C. Copy the website content to an Amazon EBS-backed Amazon EC2 instance running Apache HTTP Server. Configure Amazon Route 53 geolocation routing policies to select the closest origin.  
D. Copy the website content to multiple Amazon EBS-backed Amazon EC2 instances running Apache HTTP Server in multiple AWS Regions. Configure Amazon CloudFront geolocation routing policies to select the closest origin.

**Correct Answer:**  
B. Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Configure Amazon CloudFront with the S3 bucket as the origin.

**Answer Description:**  
What Is Amazon CloudFront?  
Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users. CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you’re serving with CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.

Using Amazon S3 Buckets for Your Origin  
When you use Amazon S3 as an origin for your distribution, you place any objects that you want CloudFront to deliver in an Amazon S3 bucket. You can use any method that is supported by Amazon S3 to get your objects into Amazon S3, for example, the Amazon S3 console or API, or a third-party tool. You can create a hierarchy in your bucket to store the objects, just as you would with any other Amazon S3 bucket.

Using an existing Amazon S3 bucket as your CloudFront origin server doesn’t change the bucket in any way; you can still use it as you normally would to store and access Amazon S3 objects at the standard Amazon S3 price. You incur regular Amazon S3 charges for storing the objects in the bucket.

The most cost-effective option is to migrate the website to an Amazon S3 bucket and configure that bucket for static website hosting. To enable good performance for global users the solutions architect should then configure a CloudFront distribution with the S3 bucket as the origin. This will cache the static content around the world closer to users.

CORRECT: “Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Configure Amazon CloudFront with the S3 bucket as the origin” is the correct answer.

INCORRECT: “Copy the website content to an Amazon S3 bucket. Configure the bucket to serve static webpage content. Replicate the S3 bucket to multiple AWS Regions” is incorrect as there is no solution here for directing users to the closest region. This could be a more cost-effective (though less elegant) solution if AWS Route 53 latency records are created.

INCORRECT: “Copy the website content to an Amazon EC2 instance. Configure Amazon Route 53 geolocation routing policies to select the closest origin” is incorrect as using Amazon EC2 instances is less cost-effective compared to hosting the website on S3. Also, geolocation routing does not achieve anything with only a single record.

INCORRECT: “Copy the website content to multiple Amazon EC2 instances in multiple AWS Regions. Configure AWS Route 53 geolocation routing policies to select the closest region” is incorrect as using Amazon EC2 instances is less cost-effective compared to hosting the website on S3.

**References:**

* [How do I use CloudFront to serve a static website hosted on Amazon S3?](https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-serve-static-website/)

#### Exam Question 150

A company has deployed an API in a VPC behind an internet-facing Application Load Balancer (ALB). An application that consumes the API as a client is deployed in a second account in private subnets behind a NAT gateway. When requests to the client application increase, the NAT gateway costs are higher than expected. A solutions architect has configured the ALB to be internal.

Which combination of architectural changes will reduce the NAT gateway costs? (Choose two.)

A. Configure a VPC peering connection between the two VPCs. Access the API using the private address.  
B. Configure an AWS Direct Connect connection between the two VPCs. Access the API using the private address.  
C. Configure a ClassicLink connection for the API into the client VPC. Access the API using the ClassicLink address.  
D. Configure a PrivateLink connection for the API into the client VPC. Access the API using the PrivateLink address.  
E. Configure an AWS Resource Access Manager connection between the two accounts. Access the API using the private address.

**Correct Answer:**  
A. Configure a VPC peering connection between the two VPCs. Access the API using the private address.  
D. Configure a PrivateLink connection for the API into the client VPC. Access the API using the PrivateLink address.

**Answer Description:**  
PrivateLink makes it easy to connect services across different accounts and VPCs to significantly simplify the network architecture. There is no API listed in shareable resources for RAM.

#### Exam Question 151

A company has a two-tier application architecture that runs in public and private subnets. Amazon EC2 instances running the web application are in the public subnet and a database runs on the private subnet.

The web application instances and the database are running in a single Availability Zone (AZ).

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

A. Create new public and private subnets in the same AZ for high availability.  
B. Create an Amazon EC2 Auto Scaling group and Application Load Balancer spanning multiple AZs.  
C. Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer.  
D. Create new public and private subnets in a new AZ. Create a database using Amazon EC2 in one AZ.  
E. 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.

**Correct Answer:**  
B. Create an Amazon EC2 Auto Scaling group and Application Load Balancer spanning multiple AZs.  
E. 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.

**Answer Description:**

You would the EC2 instances to have high availability by placing them in multiple AZs.

#### Exam Question 152

A marketing company is storing CSV files in an Amazon S3 bucket for statistical analysis. An application on an Amazon EC2 instance needs permission to efficiently process the CSV data stored in the S3 bucket.

Which action will MOST securely grant the EC2 instance access to the S3 bucket?

A. Attach a resource-based policy to the S3 bucket.  
B. Create an IAM user for the application with specific permissions to the S3 bucket.  
C. Associate an IAM role with least privilege permissions to the EC2 instance profile.  
D. Store AWS credentials directly on the EC2 instance for applications on the instance to use for API calls.

**Correct Answer:**  
C. Associate an IAM role with least privilege permissions to the EC2 instance profile.

**Answer Description:**  
Keyword: Privilege Permission + IAM Role

AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

IAM is a feature of your AWS account offered at no additional charge. You will be charged only for use of other AWS services by your users.

IAM roles for Amazon EC2  
Applications must sign their API requests with AWS credentials. Therefore, if you are an application developer, you need a strategy for managing credentials for your applications that run on EC2 instances. For example, you can securely distribute your AWS credentials to the instances, enabling the applications on those instances to use your credentials to sign requests, while protecting your credentials from other users. However, it’s challenging to securely distribute credentials to each instance, especially those that AWS creates on your behalf, such as Spot Instances or instances in Auto Scaling groups. You must also be able to update the credentials on each instance when you rotate your AWS credentials.

We designed IAM roles so that your applications can securely make API requests from your instances, without requiring you to manage the security credentials that the applications use.

Instead of creating and distributing your AWS credentials, you can delegate permission to make API requests using IAM roles as follows:

Create an IAM role.

Define which accounts or AWS services can assume the role.

Define which API actions and resources the application can use after assuming the role. Specify the role when you launch your instance, or attach the role to an existing instance. Have the application retrieve a set of temporary credentials and use them.

For example, you can use IAM roles to grant permissions to applications running on your instances that need to use a bucket in Amazon S3. You can specify permissions for IAM roles by creating a policy in JSON format. These are similar to the policies that you create for IAM users. If you change a role, the change is propagated to all instances.

When creating IAM roles, associate least privilege IAM policies that restrict access to the specific API calls the application requires.

**References:**

* [AWS Identity and Access Management (IAM) FAQs](https://aws.amazon.com/iam/faqs/)
* Amazon Elastic Compute Cloud > User Guide for Linux Instances > [IAM roles for Amazon EC2](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html)

#### Exam Question 153

A company hosts an application on multiple Amazon EC2 instances. The application processes messages from an Amazon SQS queue, writes for an Amazon RDS table, and deletes the message from the queue. Occasional duplicate records are found in the RDS table. The SQS queue does not contain any duplicate messages.

What should a solutions architect do to ensure messages are being processed once only?

A. Use the CreateQueue API call to create a new queue.  
B. Use the AddPermission API call to add appropriate permissions.  
C. Use the ReceiveMessage API call to set an appropriate wait time.  
D. Use the ChangeMessageVisibility API call to increase the visibility timeout.

**Correct Answer:**  
D. Use the ChangeMessageVisibility API call to increase the visibility timeout.

**Answer Description:**  
Keyword: SQS queue writes to an Amazon RDS

From this, Option D best suite & other Options ruled out [Option A – You can’t introduce one more Queue in the existing one; Option B – only Permission & Option C – Only Retrieves Messages]

FIFO queues are designed to never introduce duplicate messages. However, your message producer might introduce duplicates in certain scenarios: for example, if the producer sends a message, does not receive a response, and then resends the same message. Amazon SQS APIs provide deduplication functionality that prevents your message producer from sending duplicates. Any duplicates introduced by the message producer are removed within a 5-minute deduplication interval.

For standard queues, you might occasionally receive a duplicate copy of a message (at least once delivery). If you use a standard queue, you must design your applications to be idempotent (that is, they must not be affected adversely when processing the same message more than once).

CreateQueue – You can’t change the queue type after you create it and you can’t convert an existing standard queue into a FIFO queue. You must either create a new FIFO queue for your application or delete your existing standard queue and recreate it as a FIFO queue.

AddPermission – You create a queue, you have full control access rights for the queue. Only you, the owner of the queue, can grant or deny permissions to the queue.

ReceiveMessage – Retrieves one or more messages (up to 10), from the specified queue.

FIFO queues provide exactly-once processing, which means that each message is delivered once and remains available until a consumer processes it and deletes it.

**References:**

* [Amazon Simple Queue Service](https://aws.amazon.com/sqs/?nc2=h_ql_prod_ap_sqs)
* [Amazon SQS FAQs](https://aws.amazon.com/sqs/faqs/)
* Amazon Simple Queue Service > Developer Guide > [What is Amazon Simple Queue Service?](https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html)

#### Exam Question 154

A company has a three-tier image-sharing application. It uses an Amazon EC2 instance for the front-end layer, another for the backend tier, and a third for the MySQL database. A solutions architect has been tasked with designing a solution that is highly available, and requires the least amount of changes to the application.

Which solution meets these requirements?

A. Use Amazon S3 to host the front-end layer and AWS Lambda functions for the backend layer. Move the database to an Amazon DynamoDB table and use Amazon S3 to store and serve users’ images.  
B. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers. Move the database to an Amazon RDS instance with multiple read replicas to store and serve users’ images.  
C. Use Amazon S3 to host the front-end layer and a fleet of Amazon EC2 instances in an Auto Scaling group for the backend layer. Move the database to a memory optimized instance type to store and serve users’ images.  
D. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers. Move the database to an Amazon RDS instance with a Multi-AZ deployment. Use Amazon S3 to store and serve users’ images.

**Correct Answer:**  
D. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers. Move the database to an Amazon RDS instance with a Multi-AZ deployment. Use Amazon S3 to store and serve users’ images.

**Answer Description:**  
Keyword: Highly available + Least amount of changes to the application High Availability = Multi-AZ

Least amount of changes to the application = Elastic Beanstalk Automatically handles the deployment, from capacity provisioning, Load Balancing, Auto Scaling to application health monitoring

Option – D will be the right choice and Option – A; Option – B and Option – C out of race due to Cost & inter-operability.

HA with Elastic Beanstalk and RDS

AWS Elastic Beanstalk

AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS.

You can simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. At the same time, you retain full control over the AWS resources powering your application and can access the underlying resources at any time.

There is no additional charge for Elastic Beanstalk – you pay only for the AWS resources needed to store and run your applications.

AWS RDS  
Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups. It frees you to focus on your applications so you can give them the fast performance, high availability, security and compatibility they need.

Amazon RDS is available on several database instance types – optimized for memory, performance or I/O – and provides you with six familiar database engines to choose from, including Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and SQL Server. You can use the AWS Database Migration Service to easily migrate or replicate your existing databases to Amazon RDS.

AWS S3  
Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Amazon S3 provides easy-to-use management features so you can organize your data and configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements. Amazon S3 is designed for 99.999999999% (11 9’s) of durability, and stores data for millions of applications for companies all around the world.

**References:**

* [AWS Elastic Beanstalk](https://aws.amazon.com/elasticbeanstalk/?nc2=h_ql_prod_cp_ebs)
* [Amazon Relational Database Service (RDS)](https://aws.amazon.com/rds/?nc2=h_ql_prod_db_rds)
* [Amazon S3](https://aws.amazon.com/s3/?nc2=h_ql_prod_st_s3)

#### Exam Question 155

A solutions architect is designing a system to analyze the performance of financial markets while the markets are closed. The system will run a series of compute-intensive jobs for 4 hours every night. The time to complete the compute jobs is expected to remain constant, and jobs cannot be interrupted once started. Once completed, the system is expected to run for a minimum of 1 year.

Which type of Amazon EC2 instances should be used to reduce the cost of the system?

A. Spot Instances  
B. On-Demand Instances  
C. Standard Reserved Instances  
D. Scheduled Reserved Instances

**Correct Answer:**  
D. Scheduled Reserved Instances

**Answer Description:**  
Scheduled Reserved Instances (Scheduled Instances) enable you to purchase capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term. You reserve the capacity in advance, so that you know it is available when you need it. You pay for the time that the instances are scheduled, even if you do not use them.

Scheduled Instances are a good choice for workloads that do not run continuously, but do run on a regular schedule. For example, you can use Scheduled Instances for an application that runs during business hours or for batch processing that runs at the end of the week.

CORRECT: “Scheduled Reserved Instances” is the correct answer.

INCORRECT: “Standard Reserved Instances” is incorrect as the workload only runs for 4 hours a day this would be more expensive.

INCORRECT: “On-Demand Instances” is incorrect as this would be much more expensive as there is no discount applied.

INCORRECT: “Spot Instances” is incorrect as the workload cannot be interrupted once started. With Spot instances workloads can be terminated if the Spot price changes or capacity is required.

**References:**

* Amazon Elastic Compute Cloud > User Guide for Linux Instances > [Scheduled Reserved Instances](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html)

#### Exam Question 156

A bicycle sharing company is developing a multi-tier architecture to track the location of its bicycles during peak operating hours. The company wants to use these data points in its existing analytics platform. A solutions architect must determine the most viable multi-tier option to support this architecture. The data points must be accessible from the REST API.

Which action meets these requirements for storing and retrieving location data?

A. Use Amazon Athena with Amazon S3.  
B. Use Amazon API Gateway with AWS Lambda.  
C. Use Amazon QuickSight with Amazon Redshift.  
D. Use Amazon API Gateway with Amazon Kinesis Data Analytics.

**Correct Answer:**  
B. Use Amazon API Gateway with AWS Lambda.

**Answer Description:**  
Keyword: Data points in its existing analytics platform + Data points must be accessible from the REST API + Track the location of its bicycles during peak operating hours

They already have an analytics platform, A (Athena) and D (Kinesis Data Analytics) are out of the race even though S3 & APT Gateway Support REST API. Now B and C are in Race. C will not support REST API. So answer should be B as per below details.

Now if we talk about data type, we are talking about GEO location data for their bicycles. API Gateway will be support REST API. So, exact solution should be API Gateway with AWS Lambda along with Amazon Kinesis Data Analytics (Assume its used already).

CORRECT: “Use Amazon API Gateway with AWS Lambda” is the correct answer. INCORRECT: “Use Amazon Athena with Amazon S3” is incorrect as they already have analytics platform.

INCORRECT: “Use Amazon QuickSight with Amazon Redshift” is incorrect. This is not support REST API.

INCORRECT: “Use Amazon API Gateway with Amazon Kinesis Data Analytics” is incorrect as they already have analytics platform.

**References:**

* [Amazon API Gateway](https://aws.amazon.com/api-gateway/)
* [AWS Lambda](https://aws.amazon.com/lambda/)
* [Amazon Kinesis Data Analytics](https://aws.amazon.com/kinesis/data-analytics/)

#### Exam Question 157

An application requires a development environment (DEV) and production environment (PROD) for several years. The DEV instances will run for 10 hours each day during normal business hours, while the PROD instances will run 24 hours each day. A solutions architect needs to determine a compute instance purchase strategy to minimize costs.

Which solution is the MOST cost-effective?

A. DEV with Spot Instances and PROD with On-Demand Instances  
B. DEV with On-Demand Instances and PROD with Spot Instances  
C. DEV with Scheduled Reserved Instances and PROD with Reserved Instances  
D. DEV with On-Demand Instances and PROD with Scheduled Reserved Instances

**Correct Answer:**  
C. DEV with Scheduled Reserved Instances and PROD with Reserved Instances

#### Exam Question 158

A solutions architect observes that a nightly batch processing job is automatically scaled up for 1 hour before the desired Amazon EC2 capacity is reached. The peak capacity is the same every night and the batch jobs always start at 1 AM. The solutions architect needs to find a cost-effective solution that will allow for the desired EC2 capacity to be reached quickly and allow the Auto Scaling group to scale down after the batch jobs are complete.

What should the solutions architect do to meet these requirements?

A. Increase the minimum capacity for the Auto Scaling group.  
B. Increase the maximum capacity for the Auto Scaling group.  
C. Configure scheduled scaling to scale up to the desired compute level.  
D. Change the scaling policy to add more EC2 instances during each scaling operation.

**Correct Answer:**  
C. Configure scheduled scaling to scale up to the desired compute level.

#### Exam Question 159

A Solutions Architect must design a web application that will be hosted on AWS, allowing users to purchase access to premium, shared content that is stored in an S3 bucket. Upon payment, content will be available for download for 14 days before the user is denied access.

Which of the following would be the LEAST complicated implementation?

A. Use an Amazon CloudFront distribution with an origin access identity (OAI). Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design a Lambda function to remove data that is older than 14 days.  
B. Use an S3 bucket and provide direct access to the file. Design the application to track purchases in a DynamoDB table. Configure a Lambda function to remove data that is older than 14 days based on a query to Amazon DynamoDB.  
C. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 14 days for the URL.  
D. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 60 minutes for the URL and recreate the URL as necessary.

**Correct Answer:**  
C. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 14 days for the URL.

#### Exam Question 160

A company wants to run a hybrid workload for data processing. The data needs to be accessed by on-premises applications for local data processing using an NFS protocol, and must also be accessible from the AWS Cloud for further analytics and batch processing.

Which solution will meet these requirements?

A. Use an AWS Storage Gateway file gateway to provide file storage to AWS, then perform analytics on this data in the AWS Cloud.  
B. Use an AWS storage Gateway tape gateway to copy the backup of the local data to AWS, then perform analytics on this data in the AWS cloud.  
C. Use an AWS Storage Gateway volume gateway in a stored volume configuration to regularly take snapshots of the local data, then copy the data to AWS.  
D. Use an AWS Storage Gateway volume gateway in a cached volume configuration to back up all the local storage in the AWS cloud, then perform analytics on this data in the cloud.

**Correct Answer:**  
A. Use an AWS Storage Gateway file gateway to provide file storage to AWS, then perform analytics on this data in the AWS Cloud.

#### Exam Question 161

A solutions architect is moving the static content from a public website hosted on Amazon EC2 instances to an Amazon S3 bucket. An Amazon CloudFront distribution will be used to deliver the static assets. The security group used by the EC2 instances restricts access to a limited set of IP ranges. Access to the static content should be similarly restricted.

Which combination of steps will meet these requirements? (Choose two.)

A. Create an origin access identity (OAI) and associate it with the distribution. Change the permissions in the bucket policy so that only the OAI can read the objects.  
B. Create an AWS WAF web ACL that includes the same IP restrictions that exist in the EC2 security group. Associate this new web ACL with the CloudFront distribution.  
C. Create a new security group that includes the same IP restrictions that exist in the current EC2 security group. Associate this new security group with the CloudFront distribution.  
D. Create a new security group that includes the same IP restrictions that exist in the current EC2 security group. Associate this new security group with the S3 bucket hosting the static content.  
E. Create a new IAM role and associate the role with the distribution. Change the permissions either on the S3 bucket or on the files within the S3 bucket so that only the newly created IAM role has read and download permissions.

**Correct Answer:**  
A. Create an origin access identity (OAI) and associate it with the distribution. Change the permissions in the bucket policy so that only the OAI can read the objects.  
B. Create an AWS WAF web ACL that includes the same IP restrictions that exist in the EC2 security group. Associate this new web ACL with the CloudFront distribution.

#### Exam Question 162

A company recently launched its website to serve content to its global user base. The company wants to store and accelerate the delivery of static content to its users by leveraging Amazon CloudFront with an Amazon EC2 instance attached as its origin.

How should a solutions architect optimize high availability for the application?

A. Use Lambda@Edge for CloudFront.  
B. Use Amazon S3 Transfer Acceleration for CloudFront.  
C. Configure another EC2 instance in a different Availability Zone as part of the origin group.  
D. Configure another EC2 instance as part of the origin server cluster in the same Availability Zone.

**Correct Answer:**  
A. Use Lambda@Edge for CloudFront.

#### Exam Question 163

A company has created an isolated backup of its environment in another Region. The application is running in warm standby mode and is fronted by an Application Load Balancer (ALB). The current failover process is manual and requires updating a DNS alias record to point to the secondary ALB in another Region. What should a solutions architect do to automate the failover process?

A. Enable an ALB health check  
B. Enable an Amazon Route 53 health check.  
C. Crate an CNAME record on Amazon Route 53 pointing to the ALB endpoint.  
D. Create conditional forwarding rules on Amazon Route 53 pointing to an internal BIND DNS server.

**Correct Answer:**  
C. Crate an CNAME record on Amazon Route 53 pointing to the ALB endpoint.

**References:**

* [How do I use Route 53 health checks for DNS failover?](https://aws.amazon.com/premiumsupport/knowledge-center/route-53-dns-health-checks/)

#### Exam Question 164

A company relies on an application that needs at least 4 Amazon EC2 instances during regular traffic and must scale up to 12 EC2 instances during peak loads. The application is critical to the business and must be highly available.

Which solution will meet these requirements?

A. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 4 and the maximum to 12, with 2 in Availability Zone A and 2 in Availability Zone B.  
B. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 4 and the maximum to 12, with all 4 in Availability Zone A.  
C. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 8 and the maximum to 12, with 4 in Availability Zone A and 4 in Availability Zone B.  
D. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 8 and the maximum to 12, with all 8 in Availability Zone A.

**Correct Answer:**  
C. Deploy the EC2 instances in an Auto Scaling group. Set the minimum to 8 and the maximum to 12, with 4 in Availability Zone A and 4 in Availability Zone B.

#### Exam Question 165

A solutions architect must design a solution for a persistent database that is being migrated from on-premises to AWS. The database requires 64,000 IOPS according to the database administrator. If possible, the database administrator wants to use a single Amazon Elastic Block Store (Amazon EBS) volume to host the database instance.

Which solution effectively meets the database administrator’s criteria?

A. Use an instance from the I3 I/O optimized family and leverage local ephemeral storage to achieve the IOPS requirement.  
B. Create an Nitro-based Amazon EC2 instance with an Amazon EBS Provisioned IOPS SSD (io1) volume attached. Configure the volume to have 64,000 IOPS.  
C. Create and map an Amazon Elastic File System (Amazon EFS) volume to the database instance and use the volume to achieve the required IOPS for the database.  
D. Provision two volumes and assign 32,000 IOPS to each. Create a logical volume at the operating system level that aggregates both volumes to achieve the IOPS requirements.

**Correct Answer:**  
B. Create an Nitro-based Amazon EC2 instance with an Amazon EBS Provisioned IOPS SSD (io1) volume attached. Configure the volume to have 64,000 IOPS.

#### Exam Question 166

A company recently deployed a two-tier application in two Availability Zones in the us-east-1 Region. The databases are deployed in a private subnet while the web servers are deployed in a public subnet. An internet gateway is attached to the VPC. The application and database run on Amazon EC2 instances. The database servers are unable to access patches on the internet. A solutions architect needs to design a solution that maintains database security with the least operational overhead.

Which solution meets these requirements?

A. Deploy a NAT gateway inside the public subnet for each Availability Zone and associate it with an Elastic IP address. Update the routing table of the private subnet to use it as the default route.  
B. Deploy a NAT gateway inside the private subnet for each Availability Zone and associate it with an Elastic IP address. Update the routing table of the private subnet to use it as the default route.  
C. Deploy two NAT instances inside the public subnet for each Availability Zone and associate them with Elastic IP addresses. Update the routing table of the private subnet to use it as the default route.  
D. Deploy two NAT instances inside the private subnet for each Availability Zone and associate them with Elastic IP addresses. Update the routing table of the private subnet to use it as the default route.

**Correct Answer:**  
A. Deploy a NAT gateway inside the public subnet for each Availability Zone and associate it with an Elastic IP address. Update the routing table of the private subnet to use it as the default route.

**Answer Description:**  
VPC with public and private subnets (NAT)

The configuration for this scenario includes a virtual private cloud (VPC) with a public subnet and a private subnet. We recommend this scenario if you want to run a public-facing web application, while maintaining back-end servers that aren’t publicly accessible. A common example is a multi-tier website, with the web servers in a public subnet and the database servers in a private subnet. You can set up security and routing so that the web servers can communicate with the database servers.

The instances in the public subnet can send outbound traffic directly to the Internet, whereas the instances in the private subnet can’t. Instead, the instances in the private subnet can access the Internet by using a network address translation (NAT) gateway that resides in the public subnet. The database servers can connect to the Internet for software updates using the NAT gateway, but the Internet cannot establish connections to the database servers.

**References:**

* Amazon Virtual Private Cloud > User Guide > [VPC with public and private subnets (NAT)](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html)

#### Exam Question 167

A solutions architect needs to design a low-latency solution for a static single-page application accessed by users utilizing a custom domain name. The solution must be serverless, encrypted in transit, and cost-effective.

Which combination of AWS services and features should the solutions architect use? (Choose two.)

A. Amazon S3  
B. Amazon EC2  
C. AWS Fargate  
D. Amazon CloudFront  
E. Elastic Load Balancer

**Correct Answer:**  
A. Amazon S3  
D. Amazon CloudFront

#### Exam Question 168

A company has migrated an on-premises Oracle database to an Amazon RDS for Oracle Multi-AZ DB instance in the us-east-l Region. A solutions architect is designing a disaster recovery strategy to have the database provisioned in the us-west-2 Region in case the database becomes unavailable in the us-east-1 Region. The design must ensure the database is provisioned in the us-west-2 Region in a maximum of 2 hours, with a data loss window of no more than 3 hours.

How can these requirements be met?

A. Edit the DB instance and create a read replica in us-west-2. Promote the read replica to master in us-west-2 in case the disaster recovery environment needs to be activated.  
B. Select the multi-Region option to provision a standby instance in us-west-2. The standby instance will be automatically promoted to master in us-west-2 in case the disaster recovery environment needs to be created.  
C. Take automated snapshots of the database instance and copy them to us-west-2 every 3 hours. Restore the latest snapshot to provision another database instance in us-west-2 in case the disaster recovery environment needs to be activated.  
D. Create a multimaster read/write instances across multiple AWS Regions Select VPCs in us-east-1 and us-west-2 to make that deployment. Keep the master read/write instance in us-west-2 available to avoid having to activate a disaster recovery environment.

**Correct Answer:**  
A. Edit the DB instance and create a read replica in us-west-2. Promote the read replica to master in us-west-2 in case the disaster recovery environment needs to be activated.

#### Exam Question 169

A monolithic application was recently migrated to AWS and is now running on a single Amazon EC2 instance. Due to application limitations, it is not possible to use automatic scaling to scale out the application. The chief technology officer (CTO) wants an automated solution to restore the EC2 instance in the unlikely event the underlying hardware fails.

What would allow for automatic recovery of the EC2 instance as quickly as possible?

A. Configure an Amazon CloudWatch alarm that triggers the recovery of the EC2 instance if it becomes impaired.  
B. Configure an Amazon CloudWatch alarm to trigger an SNS message that alerts the CTO when the EC2 instance is impaired.  
C. Configure AWS CloudTrail to monitor the health of the EC2 instance, and if it becomes impaired, trigger instance recovery.  
D. Configure an Amazon EventBridge event to trigger an AWS Lambda function once an hour that checks the health of the EC2 instance and triggers instance recovery if the EC2 instance is unhealthy.

**Correct Answer:**  
A. Configure an Amazon CloudWatch alarm that triggers the recovery of the EC2 instance if it becomes impaired.

**References:**

* Amazon Elastic Compute Cloud > User Guide for Linux Instances > [Recover your instance](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-recover.html)

#### Exam Question 170

Application developers have noticed that a production application is very slow when business reporting users run large production reports against the Amazon RDS instance backing the application. The CPU and memory utilization metrics for the RDS instance do not exceed 60% while the reporting queries are running.

The business reporting users must be able to generate reports without affecting the application’s performance.

Which action will accomplish this?

A. Increase the size of the RDS instance.  
B. Create a read replica and connect the application to it.  
C. Enable multiple Availability Zones on the RDS instance.  
D. Create a read replica and connect the business reports to it.

**Correct Answer:**  
D. Create a read replica and connect the business reports to it.

#### Exam Question 171

A company is using a tape backup solution to store its key application data offsite. The daily data volume is around 50 TB. The company needs to retain the backups for 7 years for regulatory purposes. The backups are rarely accessed, and a week’s notice is typically given if a backup needs to be restored.

The company is now considering a cloud-based option to reduce the storage costs and operational burden of managing tapes. The company also wants to make sure that the transition from tape backups to the cloud minimizes disruptions.

Which storage solution is MOST cost-effective?

A. Use Amazon Storage Gateway to back up to Amazon Glacier Deep Archive.  
B. Use AWS Snowball Edge to directly integrate the backups with Amazon S3 Glacier.  
C. Copy the backup data to Amazon S3 and create a lifecycle policy to move the data to Amazon S3 Glacier.  
D. Use Amazon Storage Gateway to back up to Amazon S3 and create a lifecycle policy to move the backup to Amazon S3 Glacier.

**Correct Answer:**  
A. Use Amazon Storage Gateway to back up to Amazon Glacier Deep Archive.

#### Exam Question 172

A company collects temperature, humidity, and atmospheric pressure data in cities across multiple continents. The average volume of data collected per site each day is 500 GB. Each site has a high-speed internet connection. The company’s weather forecasting applications are based in a single Region and analyze the data daily.

What is the FASTEST way to aggregate data from all of these global sites?

A. Enable Amazon S3 Transfer Acceleration on the destination bucket. Use multipart uploads to directly upload site data to the destination bucket.  
B. Upload site data to an Amazon S3 bucket in the closest AWS Region. Use S3 cross-Region replication to copy objects to the destination bucket.  
C. Schedule AWS Snowball jobs daily to transfer data to the closest AWS Region. Use S3 cross-Region replication to copy objects to the destination bucket.  
D. Upload the data to an Amazon EC2 instance in the closest Region. Store the data in an Amazon EBS volume. Once a day take an EBS snapshot and copy it to the centralized Region. Restore the EBS volume in the centralized Region and run an analysis on the data daily.

**Correct Answer:**  
B. Upload site data to an Amazon S3 bucket in the closest AWS Region. Use S3 cross-Region replication to copy objects to the destination bucket.

#### Exam Question 173

A company has a web server running on an Amazon EC2 instance in a public subnet with an Elastic IP address. The default security group is assigned to the EC2 instance. The default network ACL has been modified to block all traffic. A solutions architect needs to make the web server accessible from everywhere on port 443.

Which combination of steps will accomplish this task? (Choose two.)

A. Create a security group with a rule to allow TCP port 443 from source 0.0.0.0/0.  
B. Create a security group with a rule to allow TCP port 443 to destination 0.0.0.0/0.  
C. Update the network ACL to allow TCP port 443 from source 0.0.0.0/0.  
D. Update the network ACL to allow inbound/outbound TCP port 443 from source 0.0.0.0/0 and to destination 0.0.0.0/0.  
E. Update the network ACL to allow inbound TCP port 443 from source 0.0.0.0/0 and outbound TCP port 32768-65535 to destination 0.0.0.0/0.

**Correct Answer:**  
A. Create a security group with a rule to allow TCP port 443 from source 0.0.0.0/0.  
B. Create a security group with a rule to allow TCP port 443 to destination 0.0.0.0/0.

#### Exam Question 174

A database is on an Amazon RDS MySQL 5.6 Multi-AZ DB instance that experiences highly dynamic reads.

Application developers notice a significant slowdown when testing read performance from a secondary AWS Region. The developers want a solution that provides less than 1 second of read replication latency.

What should the solutions architect recommend?

A. Install MySQL on Amazon EC2 in the secondary Region.  
B. Migrate the database to Amazon Aurora with cross-Region replicas.  
C. Create another RDS for MySQL read replica in the secondary Region.  
D. Implement Amazon ElastiCache to improve database query performance.

**Correct Answer:**  
B. Migrate the database to Amazon Aurora with cross-Region replicas.

#### Exam Question 175

A company hosts its core network services, including directory services and DNS, in its on-premises data center. The data center is connected to the AWS Cloud using AWS Direct Connect (DX). Additional AWS accounts are planned that will require quick, cost-effective, and consistent access to these network services.

What should a solutions architect implement to meet these requirements with the LEAST amount of operational overhead?

A. Create a DX connection in each new account. Route the network traffic to the on-premises servers.  
B. Configure VPC endpoints in the DX VPC for all required services. Route the network traffic to the on-premises servers.  
C. Create a VPN connection between each new account and the DX VPC. Route the network traffic to the on-premises servers.  
D. Configure AWS Transit Gateway between the accounts. Assign DX to the transit gateway and route network traffic to the on-premises servers.

**Correct Answer:**  
D. Configure AWS Transit Gateway between the accounts. Assign DX to the transit gateway and route network traffic to the on-premises servers.

#### Exam Question 176

A solutions architect is designing a solution where users will be directed to a backup static error page if the primary website is unavailable. The primary website’s DNS records are hosted in Amazon Route 53 where their domain is pointing to an Application Load Balancer (ALB).

Which configuration should the solutions architect use to meet the company’s needs while minimizing changes and infrastructure overhead?

A. Point a Route 53 alias record to an Amazon CloudFront distribution with the ALB as one of its origins. Then, create custom error pages for the distribution.  
B. Set up a Route 53 active-passive failover configuration. Direct traffic to a static error page hosted within an Amazon S3 bucket when Route 53 health checks determine that the ALB endpoint is unhealthy.  
C. Update the Route 53 record to use a latency-based routing policy. Add the backup static error page hosted within an Amazon S3 bucket to the record so the traffic is sent to the most responsive endpoints.  
D. Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance hosting a static error page as endpoints. Route 53 will only send requests to the instance if the health checks fail for the ALB.

**Correct Answer:**  
B. Set up a Route 53 active-passive failover configuration. Direct traffic to a static error page hosted within an Amazon S3 bucket when Route 53 health checks determine that the ALB endpoint is unhealthy.

**Answer Description:**  
Active-passive failover  
Use an active-passive failover configuration when you want a primary resource or group of resources to be available the majority of the time and you want a secondary resource or group of resources to be on standby in case all the primary resources become unavailable. When responding to queries, Route 53 includes only the healthy primary resources. If all the primary resources are unhealthy, Route 53 begins to include only the healthy secondary resources in response to DNS queries.

To create an active-passive failover configuration with one primary record and one secondary record, you just create the records and specify Failover for the routing policy. When the primary resource is healthy, Route 53 responds to DNS queries using the primary record. When the primary resource is unhealthy, Route 53 responds to DNS queries using the secondary record.

How Amazon Route 53 averts cascading failures  
As the first defense against cascading failures, each request routing algorithm (such as weighted and failover) has a mode of last resort. In this special mode, when all records are considered unhealthy, the Route 53 algorithm reverts to considering all records healthy.

For example, if all instances of an application, on several hosts, are rejecting health check requests, Route 53 DNS servers will choose an answer anyway and return it rather than returning no DNS answer or returning an NXDOMAIN (non-existent domain) response. An application can respond to users but still fail health checks, so this provides some protection against misconfiguration.

Similarly, if an application is overloaded, and one out of three endpoints fails its health checks, so that it’s excluded from Route 53 DNS responses, Route 53 distributes responses between the two remaining endpoints. If the remaining endpoints are unable to handle the additional load and they fail, Route 53 reverts to distributing requests to all three endpoints.

Using Amazon CloudFront as the front-end provides the option to specify a custom message instead of the default message. To specify the specific file that you want to return and the errors for which the file should be returned, you update your CloudFront distribution to specify those values.

For example, the following is a customized error message:

The CloudFront distribution can use the ALB as the origin, which will cause the website content to be cached on the CloudFront edge caches.

This solution represents the most operationally efficient choice as no action is required in the event of an issue, other than troubleshooting the root cause.

**References:**

* Amazon CloudFront > Developer Guide > [What is Amazon CloudFront?](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html)

#### Exam Question 177

An application running on AWS uses an Amazon Aurora Multi-AZ deployment for its database. When evaluating performance metrics, a solutions architect discovered that the database reads are causing high I/O and adding latency to the write requests against the database.

What should the solutions architect do to separate the read requests from the write requests?

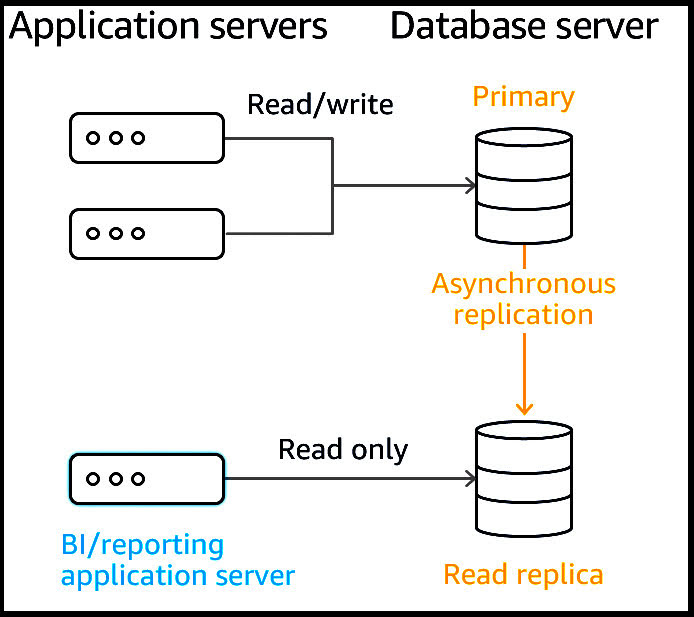
A. Enable read-through caching on the Amazon Aurora database.  
B. Update the application to read from the Multi-AZ standby instance.  
C. Create a read replica and modify the application to use the appropriate endpoint.  
D. Create a second Amazon Aurora database and link it to the primary database as a read replica.

**Correct Answer:**  
C. Create a read replica and modify the application to use the appropriate endpoint.

**Answer Description:**  
Amazon RDS Read Replicas provide enhanced performance and durability for RDS database (DB) instances. They make it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances. Read replicas are available in Amazon RDS for MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server as well as Amazon Aurora.

For the MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server database engines, Amazon RDS creates a second DB instance using a snapshot of the source DB instance. It then uses the engines’ native asynchronous replication to update the read replica whenever there is a change to the source DB instance. The read replica operates as a DB instance that allows only read-only connections; applications can connect to a read replica just as they would to any DB instance. Amazon RDS replicates all databases in the source DB instance.

Amazon Aurora further extends the benefits of read replicas by employing an SSD-backed virtualized storage layer purpose-built for database workloads. Amazon Aurora replicas share the same underlying storage as the source instance, lowering costs and avoiding the need to copy data to the replica nodes. For more information about replication with Amazon Aurora, see the online documentation.



Aurora Replicas are independent endpoints in an Aurora DB cluster, best used for scaling read operations and increasing availability. Up to 15 Aurora Replicas can be distributed across the Availability Zones that a DB cluster spans within an AWS Region.

The DB cluster volume is made up of multiple copies of the data for the DB cluster. However, the data in the cluster volume is represented as a single, logical volume to the primary instance and to Aurora Replicas in the DB cluster.

As well as providing scaling for reads, Aurora Replicas are also targets for multi-AZ. In this case the solutions architect can update the application to read from the Multi-AZ standby instance.

**References:**

* Amazon Aurora > User Guide for Aurora > [Replication with Amazon Aurora](https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html)

#### Exam Question 178

A recently acquired company is required to build its own infrastructure on AWS and migrate multiple applications to the cloud within a month. Each application has approximately 50 TB of data to be transferred. After the migration is complete, this company and its parent company will both require secure network connectivity with consistent throughput from their data centers to the applications. A solutions architect must ensure one-time data migration and ongoing network connectivity.

Which solution will meet these requirements?

A. AWS Direct Connect for both the initial transfer and ongoing connectivity.  
B. AWS Site-to-Site VPN for both the initial transfer and ongoing connectivity.  
C. AWS Snowball for the initial transfer and AWS Direct Connect for ongoing connectivity.  
D. AWS Snowball for the initial transfer and AWS Site-to-Site VPN for ongoing connectivity.

**Correct Answer:**  
C. AWS Snowball for the initial transfer and AWS Direct Connect for ongoing connectivity.

**Answer Description:**  
“Each application has approximately 50 TB of data to be transferred” = AWS Snowball; “secure network connectivity with consistent throughput from their data centers to the applications”

What are the benefits of using AWS Direct Connect and private network connections? In many circumstances, private network connections can reduce costs, increase bandwidth, and provide a more consistent network experience than Internet-based connections. “more consistent network experience”, hence AWS Direct Connect.

Direct Connect is better than VPN; reduced cost+increased bandwith+(remain connection or consistent network) = direct connect

#### Exam Question 179

A company serves content to its subscribers across the world using an application running on AWS. The application has several Amazon EC2 instances in a private subnet behind an Application Load Balancer (ALB). Due to a recent change in copyright restrictions, the chief information officer (CIO) wants to block access for certain countries.

Which action will meet these requirements?

A. Modify the ALB security group to deny incoming traffic from blocked countries.  
B. Modify the security group for EC2 instances to deny incoming traffic from blocked countries.  
C. Use Amazon CloudFront to serve the application and deny access to blocked countries.  
D. Use ALB listener rules to return access denied responses to incoming traffic from blocked countries.

**Correct Answer:**  
C. Use Amazon CloudFront to serve the application and deny access to blocked countries.

**Answer Description:**  
“block access for certain countries.” You can use geo restriction, also known as geo blocking, to prevent users in specific geographic locations from accessing content that you’re distributing through a CloudFront web distribution.

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.

INCORRECT: “Use a Network ACL to block the IP address ranges associated with the specific countries” is incorrect as this would be extremely difficult to manage.

INCORRECT: “Modify the ALB security group to deny incoming traffic from blocked countries” is incorrect as security groups cannot block traffic by country.

INCORRECT: “Modify the security group for EC2 instances to deny incoming traffic from blocked countries” is incorrect as security groups cannot block traffic by country.

**References:**

* Amazon CloudFront > Developer Guide > [Restricting the geographic distribution of your content](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html)

#### Exam Question 180

A company wants to migrate a high performance computing (HPC) application and data from on-premises to the AWS Cloud. The company uses tiered storage on-premises with hot high-performance parallel storage to support the application during periodic runs of the application, and more economical cold storage to hold the data when the application is not actively running.

Which combination of solutions should a solutions architect recommend to support the storage needs of the application? (Choose two.)

A. Amazon S3 for cold data storage  
B. Amazon EFS for cold data storage  
C. Amazon S3 for high-performance parallel storage  
D. Amazon FSx for Lustre for high-performance parallel storage  
E. Amazon FSx for Windows for high-performance parallel storage

**Correct Answer:**  
A. Amazon S3 for cold data storage  
D. Amazon FSx for Lustre for high-performance parallel storage

**Answer Description:**  
[Amazon FSx for Lustre](https://aws.amazon.com/fsx/lustre/) makes it easy and cost effective to launch and run the world’s most popular high-performance file system. Use it for workloads where speed matters, such as machine learning, high performance computing (HPC), video processing, and financial modeling.

Amazon FSx for Lustre provides a high-performance file system optimized for fast processing of workloads such as machine learning, high-performance computing (HPC), video processing, financial modeling, and electronic design automation (EDA).

These workloads commonly require data to be presented via a fast and scalable file system interface, and typically have data sets stored on long-term data stores like Amazon S3.

Amazon FSx works natively with Amazon S3, making it easy to access your S3 data to run data processing workloads. Your S3 objects are presented as files in your file system, and you can write your results back to S3. This lets you run data processing workloads on FSx for Lustre and store your long-term data on S3 or on-premises data stores.

Therefore, the best combination for this scenario is to use S3 for cold data and FSx for Lustre for the parallel HPC job.

CORRECT: “Amazon S3 for cold data storage” is the correct answer.

CORRECT: “Amazon FSx for Lustre for high-performance parallel storage” is the correct answer. INCORRECT: “Amazon EFS for cold data storage” is incorrect as FSx works natively with S3 which is also more economical.

INCORRECT: “Amazon S3 for high-performance parallel storage” is incorrect as S3 is not suitable for running high-performance computing jobs.

INCORRECT: “Amazon FSx for Windows for high-performance parallel storage” is incorrect as FSx for Lustre should be used for HPC use cases and use cases that require storing data on S3.

#### Exam Question 181

A company’s legacy application is currently relying on a single-instance Amazon RDS MySQL database without encryption. Due to new compliance requirements, all existing and new data in this database must be encrypted.

How should this be accomplished?

A. Create an Amazon S3 bucket with server-side encryption enabled. Move all the data to Amazon S3. Delete the RDS instance.  
B. Enable RDS Multi-AZ mode with encryption at rest enabled. Perform a failover to the standby instance to delete the original instance.  
C. Take a Snapshot of the RDS instance. Create an encrypted copy of the snapshot. Restore the RDS instance from the encrypted snapshot.  
D. Create an RDS read replica with encryption at rest enabled. Promote the read replica to master and switch the over to the new master. Delete the old RDS instance.

**Correct Answer:**  
C. Take a Snapshot of the RDS instance. Create an encrypted copy of the snapshot. Restore the RDS instance from the encrypted snapshot.

**Answer Description:**  
How do I encrypt Amazon RDS snapshots?  
The following steps are applicable to Amazon RDS for MySQL, Oracle, SQL Server, PostgreSQL, or MariaDB.

Important: If you use Amazon Aurora, you can restore an unencrypted Aurora DB cluster snapshot to an encrypted Aurora DB cluster if you specify an AWS Key Management Service (AWS KMS) encryption key when you restore from the unencrypted DB cluster snapshot. For more information, see Limitations of Amazon RDS Encrypted DB Instances.

Open the Amazon RDS console, and then choose Snapshots from the navigation pane.

Select the snapshot that you want to encrypt.

Under Snapshot Actions, choose Copy Snapshot.

Choose your Destination Region, and then enter your New DB Snapshot Identifier.

Change Enable Encryption to Yes.

Select your Master Key from the list, and then choose Copy Snapshot.

After the snapshot status is available, the Encrypted field will be True to indicate that the snapshot is encrypted.

You now have an encrypted snapshot of your DB. You can use this encrypted DB snapshot to restore the DB instance from the DB snapshot.

#### Exam Question 182

A solutions architect at an eCommerce company wants to back up application log data to Amazon S3. The solutions architect is unsure how frequently the logs will be accessed or which logs will be accessed the most. The company wants to keep costs as low as possible by using the appropriate S3 storage class.

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

A. S3 Glacier  
B. S3 Intelligent-Tiering  
C. S3 Standard-Infrequent Access (S3 Standard-IA)  
D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

**Correct Answer:**  
B. S3 Intelligent-Tiering

**Answer Description:**  
S3 Intelligent-Tiering is a new Amazon S3 storage class designed for customers who want to optimize storage costs automatically when data access patterns change, without performance impact or operational overhead. S3 Intelligent-Tiering is the first cloud object storage class that delivers automatic cost savings by moving data between two access tiers – frequent access and infrequent access – when access patterns change, and is ideal for data with unknown or changing access patterns.

S3 Intelligent-Tiering stores objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. For a small monthly monitoring and automation fee per object, S3 Intelligent-Tiering monitors access patterns and moves objects that have not been accessed for 30 consecutive days to the infrequent access tier.

There are no retrieval fees in S3 Intelligent-Tiering. If an object in the infrequent access tier is accessed later, it is automatically moved back to the frequent access tier. No additional tiering fees apply when objects are moved between access tiers within the S3 Intelligent-Tiering storage class. S3 Intelligent-Tiering is designed for 99.9% availability and 99.999999999% durability, and offers the same low latency and high throughput performance of S3 Standard.

#### Exam Question 183

A solutions architect is designing storage for a high performance computing (HPC) environment based on Amazon Linux. The workload stores and processes a large amount of engineering drawings that require shared storage and heavy computing.

Which storage option would be the optimal solution?

A. Amazon Elastic File System (Amazon EFS)  
B. Amazon FSx for Lustre  
C. Amazon EC2 instance store  
D. Amazon EBS Provisioned IOPS SSD (io1)

**Correct Answer:**  
B. Amazon FSx for Lustre

**Answer Description:**  
Amazon FSx for Lustre is a new, fully managed service provided by AWS based on the Lustre file system.

Amazon FSx for Lustre provides a high-performance file system optimized for fast processing of workloads such as machine learning, high performance computing (HPC), video processing, financial modeling, and electronic design automation (EDA).

FSx for Lustre allows customers to create a Lustre filesystem on demand and associate it to an Amazon S3 bucket. As part of the filesystem creation, Lustre reads the objects in the buckets and adds that to the file system metadata. Any Lustre client in your VPC is then able to access the data, which gets cached on the high-speed Lustre filesystem. This is ideal for HPC workloads, because you can get the speed of an optimized Lustre file system without having to manage the complexity of deploying, optimizing, and managing the Lustre cluster.

Additionally, having the filesystem work natively with Amazon S3 means you can shut down the Lustre filesystem when you don’t need it but still access objects in Amazon S3 via other AWS Services. FSx for Lustre also allows you to also write the output of your HPC job back to Amazon S3.

#### Exam Question 184

A company is running an eCommerce application on Amazon EC2. The application consists of a stateless web tier that requires a minimum of 10 instances, and a peak of 250 instances to support the application’s usage. The application requires 50 instances 80% of the time.

Which solution should be used to minimize costs?

A. Purchase Reserved Instances to cover 250 instances.  
B. Purchase Reserved Instances to cover 80 instances. Use Spot Instances to cover the remaining instances.  
C. Purchase On-Demand Instances to cover 40 instances. Use Spot Instances to cover the remaining instances.  
D. Purchase Reserved Instances to cover 50 instances. Use On-Demand and Spot Instances to cover the remaining instances.

**Correct Answer:**  
D. Purchase Reserved Instances to cover 50 instances. Use On-Demand and Spot Instances to cover the remaining instances.

**Answer Description:**  
Reserved Instances  
Having 50 EC2 RIs provide a discounted hourly rate and an optional capacity reservation for EC2 instances. AWS Billing automatically applies your RI’s discounted rate when attributes of EC2 instance usage match attributes of an active RI.

If an Availability Zone is specified, EC2 reserves capacity matching the attributes of the RI. The capacity reservation of an RI is automatically utilized by running instances matching these attributes.

You can also choose to forego the capacity reservation and purchase an RI that is scoped to a region. RIs that are scoped to a region automatically apply the RI’s discount to instance usage across AZs and instance sizes in a region, making it easier for you to take advantage of the RI’s discounted rate.

On-Demand Instance  
On-Demand instances let you pay for compute capacity by the hour or second (minimum of 60 seconds) with no long-term commitments. This frees you from the costs and complexities of planning, purchasing, and maintaining hardware and transforms what are commonly large fixed costs into much smaller variable costs.

The pricing below includes the cost to run private and public AMIs on the specified operating system (“Windows Usage” prices apply to Windows Server 2003 R2, 2008, 2008 R2, 2012, 2012 R2, 2016, and 2019). Amazon also provides you with additional instances for Amazon EC2 running Microsoft Windows with SQL Server, Amazon EC2 running SUSE Linux Enterprise Server, Amazon EC2 running Red Hat Enterprise Linux and Amazon EC2 running IBM that are priced differently.

Spot Instances  
A Spot Instance is an unused EC2 instance that is available for less than the On-Demand price. Because Spot Instances enable you to request unused EC2 instances at steep discounts, you can lower your Amazon EC2 costs significantly. The hourly price for a Spot Instance is called a Spot price. The Spot price of each instance type in each Availability Zone is set by Amazon EC2, and adjusted gradually based on the long-term supply of and demand for Spot Instances. Your Spot Instance runs whenever capacity is available and the maximum price per hour for your request exceeds the Spot price.

#### Exam Question 185

A solutions architect is implementing a document review application using an Amazon S3 bucket for storage. The solution must prevent an accidental deletion of the documents and ensure that all versions of the documents are available. Users must be able to download, modify, and upload documents.

Which combination of actions should be taken to meet these requirements? (Choose two.)

A. Enable a read-only bucket ACL.  
B. Enable versioning on the bucket.  
C. Attach an IAM policy to the bucket.  
D. Enable MFA Delete on the bucket.  
E. Encrypt the bucket using AWS KMS.

**Correct Answer:**  
B. Enable versioning on the bucket.  
D. Enable MFA Delete on the bucket.

**Answer Description:**  
Object Versioning  
Use Amazon S3 Versioning to keep multiple versions of an object in one bucket. For example, you could store my-image.jpg (version 111111) and my-image.jpg (version 222222) in a single bucket. S3 Versioning protects you from the consequences of unintended overwrites and deletions. You can also use it to archive objects so that you have access to previous versions.

To customize your data retention approach and control storage costs, use object versioning with Object lifecycle management. For information about creating S3 Lifecycle policies using the AWS Management Console, see How Do I Create a Lifecycle Policy for an S3 Bucket? in the Amazon Simple Storage Service Console User Guide.

If you have an object expiration lifecycle policy in your non-versioned bucket and you want to maintain the same permanent delete behavior when you enable versioning, you must add a noncurrent expiration policy. The noncurrent expiration lifecycle policy will manage the deletes of the noncurrent object versions in the version-enabled bucket. (A version-enabled bucket maintains one current and zero or more noncurrent object versions.)

You must explicitly enable S3 Versioning on your bucket. By default, S3 Versioning is disabled. Regardless of whether you have enabled Versioning, each object in your bucket has a version ID. If you have not enabled Versioning, Amazon S3 sets the value of the version ID to null. If S3 Versioning is enabled, Amazon S3 assigns a version ID value for the object. This value distinguishes it from other versions of the same key.

Enabling and suspending versioning is done at the bucket level. When you enable versioning on an existing bucket, objects that are already stored in the bucket are unchanged. The version IDs (null), contents, and permissions remain the same. After you enable S3 Versioning for a bucket, each object that is added to the bucket gets a version ID, which distinguishes it from other versions of the same key.

Only Amazon S3 generates version IDs, and they can’t be edited. Version IDs are Unicode, UTF-8 encoded, URL-ready, opaque strings that are no more than 1,024 bytes long. The following is an example: 3/L4kqtJlcpXroDTDmJ+rmSpXd3dIbrHY+MTRCxf3vjVBH40Nr8X8gdRQBpUMLUo.

Using MFA delete  
If a bucket’s versioning configuration is MFA Delete–enabled, 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. Requests that include x-amz-mfa must use HTTPS. The header’s value is the concatenation of your authentication device’s serial number, a space, and the authentication code displayed on it. If you do not include this request header, the request fails.

None of the options present a good solution for specifying permissions required to write and modify objects so that requirement needs to be taken care of separately. The other requirements are to prevent accidental deletion and the ensure that all versions of the document are available. The two solutions for these requirements are versioning and MFA delete. Versioning will retain a copy of each version of the document and multi-factor authentication delete (MFA delete) will prevent any accidental deletion as you need to supply a second factor when attempting a delete. CORRECT: “Enable versioning on the bucket” is a correct answer.

CORRECT: “Enable MFA Delete on the bucket” is also a correct answer.

INCORRECT: “Set read-only permissions on the bucket” is incorrect as this will also prevent any writing to the bucket which is not desired.

INCORRECT: “Attach an IAM policy to the bucket” is incorrect as users need to modify documents which will also allow delete. Therefore, a method must be implemented to just control deletes.

INCORRECT: “Encrypt the bucket using AWS SSE-S3” is incorrect as encryption doesn’t stop you from deleting an object.

**References:**

* Amazon Simple Storage Service > User Guide > [Using versioning in S3 buckets](https://docs.aws.amazon.com/AmazonS3/latest/userguide/Versioning.html)
* Amazon Simple Storage Service > User Guide > [Deleting an object from an MFA delete-enabled bucket](https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingMFADelete.html)

#### Exam Question 186

A solutions architect is designing a two-tier web application. The application consists of a public-facing web tier hosted on Amazon EC2 in public subnets. The database tier consists of Microsoft SQL Server running on Amazon EC2 in a private subnet. Security is a high priority for the company.

How should security groups be configured in this situation? (Choose two.)

A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0.  
B. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0.  
C. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier.  
D. Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier.  
E. Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier.

**Correct Answer:**  
A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0.  
C. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier.

**Answer Description:**  
In this scenario an inbound rule is required to allow traffic from any internet client to the web front end on SSL/TLS port 443. The source should therefore be set to 0.0.0.0/0 to allow any inbound traffic.

To secure the connection from the web frontend to the database tier, an outbound rule should be created from the public EC2 security group with a destination of the private EC2 security group. The port should be set to 1433 for MySQL. The private EC2 security group will also need to allow inbound traffic on 1433 from the public EC2 security group.

This configuration can be seen in the diagram:

CORRECT: “Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0” is a correct answer.

CORRECT: “Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier” is also a correct answer.

INCORRECT: “Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0” is incorrect as this is configured backwards.

INCORRECT: “Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier” is incorrect as the MySQL database instance does not need to send outbound traffic on either of these ports.

INCORRECT: “Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier” is incorrect as the database tier does not need to allow inbound traffic on port 443.

**References:**  
Amazon Virtual Private Cloud > User Guide > [Security groups for your VPC](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html)

#### Exam Question 187

A company hosts its product information webpages on AWS. The existing solution uses multiple Amazon C2 instances behind an Application Load Balancer in an Auto Scaling group. The website also uses a custom DNS name and communicates with HTTPS only using a dedicated SSL certificate. The company is planning a new product launch and wants to be sure that users from around the world have the best possible experience on the new website.

What should a solutions architect do to meet these requirements?

A. Redesign the application to use Amazon CloudFront.  
B. Redesign the application to use AWS Elastic Beanstalk.  
C. Redesign the application to use a Network Load Balancer.  
D. Redesign the application to use Amazon S3 static website hosting.

**Correct Answer:**  
A. Redesign the application to use Amazon CloudFront.

**Answer Description:**  
What Is Amazon CloudFront?  
Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users. CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you’re serving with CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.

If the content is already in the edge location with the lowest latency, CloudFront delivers it immediately.

If the content is not in that edge location, CloudFront retrieves it from an origin that you’ve defined – such as an Amazon S3 bucket, a MediaPackage channel, or an HTTP server (for example, a web server) that you have identified as the source for the definitive version of your content.

As an example, suppose that you’re serving an image from a traditional web server, not from CloudFront. For example, you might serve an image, sunsetphoto.png, using the URL http://example.com/sunsetphoto.png.

Your users can easily navigate to this URL and see the image. But they probably don’t know that their request was routed from one network to another – through the complex collection of interconnected networks that comprise the internet – until the image was found.

CloudFront speeds up the distribution of your content by routing each user request through the AWS backbone network to the edge location that can best serve your content. Typically, this is a CloudFront edge server that provides the fastest delivery to the viewer. Using the AWS network dramatically reduces the number of networks that your users’ requests must pass through, which improves performance. Users get lower latency – the time it takes to load the first byte of the file – and higher data transfer rates.

You also get increased reliability and availability because copies of your files (also known as objects) are now held (or cached) in multiple edge locations around the world.

#### Exam Question 188

A solutions architect is designing the cloud architecture for a new application being deployed on AWS. The process should run in parallel while adding and removing application nodes as needed based on the number of jobs to be processed. The processor application is stateless. The solutions architect must ensure that the application is loosely coupled and the job items are durably stored.

Which design should the solutions architect use?

A. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on CPU usage.  
B. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on network usage.  
C. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue.  
D. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of messages published to the SNS topic.

**Correct Answer:**  
C. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue.

**Answer Description:**  
Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message oriented middleware, and empowers developers to focus on differentiating work. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available. Get started with SQS in minutes using the AWS console, Command Line Interface or SDK of your choice, and three simple commands.

SQS offers two types of message queues. Standard queues offer maximum throughput, best-effort ordering, and at-least-once delivery. SQS FIFO queues are designed to guarantee that messages are processed exactly once, in the exact order that they are sent.

**Scaling Based on Amazon SQS**  
There are some scenarios where you might think about scaling in response to activity in an Amazon SQS queue. For example, suppose that you have a web app that lets users upload images and use them online. In this scenario, each image requires resizing and encoding before it can be published. The app runs on EC2 instances in an Auto Scaling group, and it’s configured to handle your typical upload rates. Unhealthy instances are terminated and replaced to maintain current instance levels at all times. The app places the raw bitmap data of the images in an SQS queue for processing. It processes the images and then publishes the processed images where they can be viewed by users. The architecture for this scenario works well if the number of image uploads doesn’t vary over time. But if the number of uploads changes over time, you might consider using dynamic scaling to scale the capacity of your Auto Scaling group.

In this case we need to find a durable and loosely coupled solution for storing jobs. Amazon SQS is ideal for this use case and can be configured to use dynamic scaling based on the number of jobs waiting in the queue.

To configure this scaling you can use the backlog per instance metric with the target value being the acceptable backlog per instance to maintain. You can calculate these numbers as follows: Backlog per instance: To calculate your backlog per instance, start with the ApproximateNumberOfMessages queue attribute to determine the length of the SQS queue (number of messages available for retrieval from the queue). Divide that number by the fleet’s running capacity, which for an Auto Scaling group is the number of instances in the InService state, to get the backlog per instance.

Acceptable backlog per instance: To calculate your target value, first determine what your application can accept in terms of latency. Then, take the acceptable latency value and divide it by the average time that an EC2 instance takes to process a message.

This solution will scale EC2 instances using Auto Scaling based on the number of jobs waiting in the SQS queue.

CORRECT: “Create an Amazon SQS queue to hold the jobs that needs to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue” is the correct answer.

INCORRECT: “Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the Auto Scaling group to add and remove nodes based on network usage” is incorrect as scaling on network usage does not relate to the number of jobs waiting to be processed.

INCORRECT: “Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the

Auto Scaling group to add and remove nodes based on CPU usage” is incorrect. Amazon SNS is a notification service so it delivers notifications to subscribers. It does store data durably but is less suitable than SQS for this use case. Scaling on CPU usage is not the best solution as it does not relate to the number of jobs waiting to be processed.

INCORRECT: “Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of messages published to the SNS topic” is incorrect. Amazon SNS is a notification service so it delivers notifications to subscribers. It does store data durably but is less suitable than SQS for this use case. Scaling on the number of notifications in SNS is not possible.

**References:**

* Amazon EC2 Auto Scaling > User Guide > [Scaling based on Amazon SQS](https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html)

#### Exam Question 189

A company has an application that calls AWS Lambda functions. A recent code review found database credentials stored in the source code. The database credentials need to be removed from the Lambda source code. The credentials must then be securely stored and rotated on an ongoing basis to meet security policy requirements.

What should a solutions architect recommend to meet these requirements?

A. Store the password in AWS CloudHSM. Associate the Lambda function with a role that can retrieve the password from CloudHSM given its key ID.  
B. Store the password in AWS Secrets Manager. Associate the Lambda function with a role that can retrieve the password from Secrets Manager given its secret ID.  
C. Move the database password to an environment variable associated with the Lambda function. Retrieve the password from the environment variable upon execution.  
D. Store the password in AWS Key Management Service (AWS KMS). Associate the Lambda function with a role that can retrieve the password from AWS KMS given its key ID.

**Correct Answer:**  
B. Store the password in AWS Secrets Manager. Associate the Lambda function with a role that can retrieve the password from Secrets Manager given its secret ID.

#### Exam Question 190

A company built an application that lets users check in to places they visit, rank the places, and add reviews about their experiences. The application is successful with a rapid increase in the number of users every month.

The chief technology officer fears the database supporting the current Infrastructure may not handle the new load the following month because the single Amazon RDS for MySQL instance has triggered alarms related to resource exhaustion due to read requests.

What can a solutions architect recommend to prevent service Interruptions at the database layer with minimal changes to code?

A. Create RDS read replicas and redirect read-only traffic to the read replica endpoints. Enable a Multi-AZ deployment.  
B. Create an Amazon EMR cluster and migrate the data to a Hadoop Distributed File System (HDFS) with a replication factor of 3.  
C. Create an Amazon ElastiCache cluster and redirect all read-only traffic to the cluster. Set up the cluster to be deployed in three Availability Zones.  
D. Create an Amazon DynamoDB table to replace the RDS instance and redirect all read-only traffic to the DynamoDB table. Enable DynamoDB Accelerator to offload traffic from the main table.

**Correct Answer:**  
A. Create RDS read replicas and redirect read-only traffic to the read replica endpoints. Enable a Multi-AZ deployment.

#### Exam Question 191

A company is looking for a solution that can store video archives in AWS from old news footage. The company needs to minimize costs and will rarely need to restore these files. When the files are needed, they must be available in a maximum of five minutes.

What is the MOST cost-effective solution?

A. Store the video archives in Amazon S3 Glacier and use Expedited retrievals.  
B. Store the video archives in Amazon S3 Glacier and use Standard retrievals.  
C. Store the video archives in Amazon S3 Standard-Infrequent Access (S3 Standard-IA).  
D. Store the video archives in Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).

**Correct Answer:**  
A. Store the video archives in Amazon S3 Glacier and use Expedited retrievals.

#### Exam Question 192

A healthcare company stores highly sensitive patient records. Compliance requires that multiple copies be stored in different locations. Each record must be stored for 7 years. The company has a service level agreement (SLA) to provide records to government agencies immediately for the first 30 days and then within 4 hours of a request thereafter.

What should a solutions architect recommend?

A. Use Amazon S3 with cross-Region replication enabled. After 30 days, transition the data to Amazon S3 Glacier using lifecycle policy.  
B. Use Amazon S3 with cross-origin resource sharing (CORS) enabled. After 30 days, transition the data to Amazon S3 Glacier using a lifecycle policy.  
C. Use Amazon S3 with cross-Region replication enabled. After 30 days, transition the data to Amazon S3 Glacier Deep Achieve using a lifecycle policy.  
D. Use Amazon S3 with cross-origin resource sharing (CORS) enabled. After 30 days, transition the data to Amazon S3 Glacier Deep Archive using a lifecycle policy.

**Correct Answer:**  
A. Use Amazon S3 with cross-Region replication enabled. After 30 days, transition the data to Amazon S3 Glacier using lifecycle policy.

#### Exam Question 193

A public-facing web application queries a database hosted on an Amazon EC2 instance in a private subnet.

A large number of queries involve multiple table joins, and the application performance has been degrading due to an increase in complex queries. The application team will be performing updates to improve performance.

What should a solutions architect recommend to the application team? (Choose two.)

A. Cache query data in Amazon SQS  
B. Create a read replica to offload queries  
C. Migrate the database to Amazon Athena  
D. Implement Amazon DynamoDB Accelerator to cache data.  
E. Migrate the database to Amazon RDS

**Correct Answer:**  
B. Create a read replica to offload queries  
E. Migrate the database to Amazon RDS

#### Exam Question 194

A company runs multiple Amazon EC2 Linux instances in a VPC with applications that use a hierarchical directory structure. The applications need to rapidly and concurrently read and write to shared storage.

How can this be achieved?

A. Create an Amazon EFS file system and mount it from each EC2 instance.  
B. Create an Amazon S3 bucket and permit access from all the EC2 instances in the VPC.  
C. Create a file system on an Amazon EBS Provisioned IOPS SSD (io1) volume. Attach the volume to all the EC2 instances.  
D. Create file systems on Amazon EBS volumes attached to each EC2 instance. Synchronize the Amazon EBS volumes across the different EC2 instances.

**Correct Answer:**  
A. Create an Amazon EFS file system and mount it from each EC2 instance.

#### Exam Question 195

An ecommerce company is running a multi-tier application on AWS. The front-end and backend tiers both run on Amazon EC2, and the database runs on Amazon RDS for MySQL. The backend tier communicates with the RDS instance. There are frequent calls to return identical datasets from the database that are causing performance slowdowns.

Which action should be taken to improve the performance of the backend?

A. Implement Amazon SNS to store the database calls.  
B. Implement Amazon ElastiCache to cache the large datasets.  
C. Implement an RDS for MySQL read replica to cache database calls.  
D. Implement Amazon Kinesis Data Firehose to stream the calls to the database.

**Correct Answer:**  
B. Implement Amazon ElastiCache to cache the large datasets.

#### Exam Question 196

A company currently stores symmetric encryption keys in a hardware security module (HSM). A solutions architect must design a solution to migrate key management to AWS. The solution should allow for key rotation and support the use of customer provided keys.

Where should the key material be stored to meet these requirements?

A. Amazon S3  
B. AWS Secrets Manager  
C. AWS Systems Manager Parameter store  
D. AWS Key Management Service (AWS KMS)

**Correct Answer:**  
B. AWS Secrets Manager

**Answer Description:**  
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.

**References:**

* [AWS Secrets Manager](https://aws.amazon.com/secrets-manager/)

#### Exam Question 197

A recent analysis of a company’s IT expenses highlights the need to reduce backup costs. The company’s chief information officer wants to simplify the on-premises backup infrastructure and reduce costs by eliminating the use of physical backup tapes. The company must preserve the existing investment in the on-premises backup applications and workflows.

What should a solutions architect recommend?

A. Set up AWS Storage Gateway to connect with the backup applications using the NFS interface.  
B. Set up an Amazon EFS file system that connects with the backup applications using the NFS interface.  
C. Set up an Amazon EFS file system that connects with the backup applications using the iSCSI interface.  
D. Set up AWS Storage Gateway to connect with the backup applications using the iSCSI-virtual tape library (VTL) interface.

**Correct Answer:**  
D. Set up AWS Storage Gateway to connect with the backup applications using the iSCSI-virtual tape library (VTL) interface.

#### Exam Question 198

A company hosts an application on an Amazon EC2 instance that requires a maximum of 200 GB storage space. The application is used infrequently, with peaks during mornings and evenings. Disk I/O varies, but peaks at 3,000 IOPS. The chief financial officer of the company is concerned about costs and has asked a solutions architect to recommend the most cost-effective storage option that does not sacrifice performance.

Which solution should the solutions architect recommend?

A. Amazon EBS Cold HDD (sc1)  
B. Amazon EBS General Purpose SSD (gp2)  
C. Amazon EBS Provisioned IOPS SSD (io1)  
D. Amazon EBS Throughput Optimized HDD (st1)

**Correct Answer:**  
B. Amazon EBS General Purpose SSD (gp2)

**Answer Description:**  
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 case the volume would have a baseline performance of 3 x 200 = 600 IOPS. The volume could also burst to 3,000 IOPS for extended periods. As the I/O varies, this should be suitable. CORRECT: “Amazon EBS General Purpose SSD (gp2)” is the correct answer.

INCORRECT: “Amazon EBS Provisioned IOPS SSD (io1) ” is incorrect as this would be a more expensive option and is not required for the performance characteristics of this workload.

INCORRECT: “Amazon EBS Cold HDD (sc1)” is incorrect as there is no IOPS SLA for HDD volumes and they would likely not perform well enough for this workload.

INCORRECT: “Amazon EBS Throughput Optimized HDD (st1)” is incorrect as there is no IOPS SLA for HDD volumes and they would likely not perform well enough for this workload.

**References:**  
Amazon Elastic Compute Cloud > User Guide for Linux Instances > [Amazon EBS volume types](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html)

#### Exam Question 199

A company is using Amazon EC2 to run its big data analytics workloads. These variable workloads run each night, and it is critical they finish by the start of business the following day. A solutions architect has been tasked with designing the MOST cost-effective solution.

Which solution will accomplish this?

A. Spot Fleet  
B. Spot Instances  
C. Reserved Instances  
D. On-Demand Instances

**Correct Answer:**  
A. Spot Fleet

#### Exam Question 200

A company hosts its website on Amazon S3. The website serves petabytes of outbound traffic monthly, which accounts for most of the company’s AWS costs. What should a solutions architect do to reduce costs?

A. Configure Amazon CloudFront with the existing website as the origin.  
B. Move the website to Amazon EC2 with Amazon EBS volumes for storage.  
C. Use AWS Global Accelerator and specify the existing website as the endpoint.  
D. Rearchitect the website to run on a combination of Amazon API Gateway and AWS Lambda.

**Correct Answer:**  
A. Configure Amazon CloudFront with the existing website as the origin.

**Answer Description:**  
A textbook case for CloudFront. The data transfer cost in CloudFront is lower than in S3. With heavy read operations of static content, it’s more economical to add CloudFront in front of your S3 bucket.

# AWS Certified Solutions Architect – Associate SAA-C02 Exam Questions and Answers – Page 3

# AWS Certified Solutions Architect – Associate SAA-C02 Exam Questions and Answers – Page 3

The latest AWS Certified Solutions Architect – Associate SAA-C02 certification actual real practice exam question and answer (Q&A) dumps are available free, which are helpful for you to pass the AWS Certified Solutions Architect – Associate SAA-C02 exam and earn AWS Certified Solutions Architect – Associate SAA-C02 certification.

#### Exam Question 201

A company is migrating to the AWS Cloud. A file server is the first workload to migrate. Users must be able to access the file share using the Server Message Block (SMB) protocol. Which AWS managed service meets these requirements?

A. Amazon EBS  
B. Amazon EC2  
C. Amazon FSx  
D. Amazon S3

**Correct Answer:**  
C. Amazon FSx

**Answer Description:**  
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 both Single-AZ and Multi-AZ deployments as can be seen in the feature comparison table below.

CORRECT: “Amazon FSx” is the correct answer.

INCORRECT: “Amazon Elastic Block Store (EBS)” is incorrect. EFS and EBS are not good use cases for this solution. Neither storage solution is capable of presenting Amazon S3 objects as files to the application.

INCORRECT: “Amazon EC2” is incorrect as no SMB support.

INCORRECT: “Amazon S3” is incorrect as this is not a suitable replacement for a Microsoft filesystem.

#### Exam Question 202

A solutions architect is designing a customer-facing application. The application is expected to have a variable amount of reads and writes depending on the time of year and clearly defined access patterns throughout the year. Management requires that database auditing and scaling be managed in the AWS Cloud. The Recovery Point Objective (RPO) must be less than 5 hours.

Which solutions can accomplish this? (Choose two.)

A. Use Amazon DynamoDB with auto scaling. Use on-demand backups and AWS CloudTrail.  
B. Use Amazon DynamoDB with auto scaling. Use on-demand backups and Amazon DynamoDB Streams.  
C. Use Amazon Redshift Configure concurrency scaling. Enable audit logging. Perform database snapshots every 4 hours.  
D. Use Amazon RDS with Provisioned IOPS. Enable the database auditing parameter. Perform database snapshots every 5 hours.  
E. Use Amazon RDS with auto scaling. Enable the database auditing parameter. Configure the backup retention period to at least 1 day.

**Correct Answer:**  
A. Use Amazon DynamoDB with auto scaling. Use on-demand backups and AWS CloudTrail.  
E. Use Amazon RDS with auto scaling. Enable the database auditing parameter. Configure the backup retention period to at least 1 day.

**Answer Description:**

1. Use Amazon DynamoDB with auto scaling. Use on-demand backups and AWS CloudTrail. CORRECT – Scalable, with backup and AWS Managed Auditing
2. Use Amazon DynamoDB with auto scaling. Use on-demand backups and Amazon DynamoDB Streams.

INCORRECT – AWS DDB Streams can be used for auditing, but its not AWS managed auditing.

Use Amazon Redshift Configure concurrency scaling. Enable audit logging. Perform database snapshots every 4

INCORRECT – Not a database. Data lake

Use Amazon RDS with Provisioned IOPS. Enable the database auditing parameter. Perform database snapshots every 5

INCORRECT – This does not scale

Use Amazon RDS with auto scaling. Enable the database auditing parameter. Configure the backup retention period to at least 1

CORRECT – Scalable, AWS managed auditing and backup. The backup frequency is not stated but have no technical limitation which states it cannot be less 5 hours (1 day is retention period of the backup).

#### Exam Question 203

A company runs an application using Amazon ECS. The application creates resized versions of an original image and then makes Amazon S3 API calls to store the resized images in Amazon S3. How can a solutions architect ensure that the application has permission to access Amazon S3?

A. Update the S3 role in AWS IAM to allow read/write access from Amazon ECS, and then relaunch the container.  
B. Create an IAM role with S3 permissions, and then specify that role as the taskRoleArn in the task definition.  
C. Create a security group that allows access from Amazon ECS to Amazon S3, and update the launch configuration used by the ECS cluster.  
D. Create an IAM user with S3 permissions, and then relaunch the Amazon EC2 instances for the ECS cluster while logged in as this account.

**Correct Answer:**  
B. Create an IAM role with S3 permissions, and then specify that role as the taskRoleArn in the task definition.

#### Exam Question 204

A company mandates that an Amazon S3 gateway endpoint must allow traffic to trusted buckets only.

Which method should a solutions architect implement to meet this requirement?

A. Create a bucket policy for each of the company’s trusted S3 buckets that allows traffic only from the company’s trusted VPCs.  
B. Create a bucket policy for each of the company’s trusted S3 buckets that allows traffic only from the company’s S3 gateway endpoint IDs.  
C. Create an S3 endpoint policy for each of the company’s S3 gateway endpoints that blocks access from any VPC other than the company’s trusted VPCs.  
D. Create an S3 endpoint policy for each of the company’s S3 gateway endpoints that provides access to the Amazon Resource Name (ARN) of the trusted S3 buckets.

**Correct Answer:**  
D. Create an S3 endpoint policy for each of the company’s S3 gateway endpoints that provides access to the Amazon Resource Name (ARN) of the trusted S3 buckets.

#### Exam Question 205

A company runs a web service on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across two Availability Zones. The company needs a minimum of four instances at all times to meet the required service level agreement (SLA) while keeping costs low.

If an Availability Zone fails, how can the company remain compliant with the SLA?

A. Add a target tracking scaling policy with a short cooldown period.  
B. Change the Auto Scaling group launch configuration to use a larger instance type.  
C. Change the Auto Scaling group to use six servers across three Availability Zones.  
D. Change the Auto Scaling group to use eight servers across two Availability Zones.

**Correct Answer:**  
A. Add a target tracking scaling policy with a short cooldown period.

#### Exam Question 206

A company is designing a web application using AWS that processes insurance quotes. Users will request quotes from the application. Quotes must be separated by quote type must be responded to within 24 hours, and must not be lost. The solution should be simple to set up and maintain.

Which solution meets these requirements?

A. Create multiple Amazon Kinesis data streams based on the quote type. Configure the web application to send messages to the proper data stream. Configure each backend group of application servers to pool messages from its own data stream using the Kinesis Client Library (KCL).  
B. Create multiple Amazon Simple Notification Service (Amazon SNS) topics and register Amazon SQS queues to their own SNS topic based on the quote type. Configure the web application to publish messages to the SNS topic queue. Configure each backend application server to work its own SQS queue.  
C. Create a single Amazon Simple Notification Service (Amazon SNS) topic and subscribe the Amazon SQS queues to the SNS topic. Configure SNS message filtering to publish messages to the proper SQS queue based on the quote type. Configure each backend application server to work its own SQS queue.  
D. Create multiple Amazon Kinesis Data Firehose delivery streams based on the quote type to deliver data streams to an Amazon Elasticsearch Service (Amazon ES) cluster. Configure the web application to send messages to the proper delivery stream. Configure each backend group of application servers to search for the messages from Amazon ES and process them accordingly.

**Correct Answer:**  
C. Create a single Amazon Simple Notification Service (Amazon SNS) topic and subscribe the Amazon SQS queues to the SNS topic. Configure SNS message filtering to publish messages to the proper SQS queue based on the quote type. Configure each backend application server to work its own SQS queue.

**Answer Description:**  
It all depends on where you want to do the quote type classification i.e. in the app and send to a different/multiple SNS topics (B) or use SNS filtering to do the type classification (C). The question doesn’t really give you enough info to make a clear choice but configuring SNS filtering is probably less work and easier to maintain than maintaining app code.

**References:**  
Amazon Simple Notification Service > Developer Guide > [Amazon SNS message filtering](https://docs.aws.amazon.com/sns/latest/dg/sns-message-filtering.html)

#### Exam Question 207

A company wants to use an AWS Region as a disaster recovery location for its on-premises infrastructure.

The company has 10 TB of existing data, and the on-premise data center has a 1 Gbps internet connection.

A solutions architect must find a solution so the company can have its existing data on AWS in 72 hours without transmitting it using an unencrypted channel.

Which solution should the solutions architect select?

A. Send the initial 10 TB of data to AWS using FTP.  
B. Send the initial 10 TB of data to AWS using AWS Snowball.  
C. Establish a VPN connection between Amazon VPC and the company’s data center.  
D. Establish an AWS Direct Connect connection between Amazon VPC and the company’s data center.

**Correct Answer:**  
C. Establish a VPN connection between Amazon VPC and the company’s data center.

#### Exam Question 208

A company is building applications in containers. The company wants to migrate its on-premises development and operations services from its on-premises data center to AWS. Management states that production system must be cloud agnostic and use the same configuration and administrator tools across production systems. A solutions architect needs to design a managed solution that will align open-source software.

Which solution meets these requirements?

A. Launch the containers on Amazon EC2 with EC2 instance worker nodes.  
B. Launch the containers on Amazon Elastic Kubernetes Service (Amazon EKS) and EKS workers nodes.  
C. Launch the containers on Amazon Elastic Containers service (Amazon ECS) with AWS Fargate instances.  
D. Launch the containers on Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 instance worker nodes.

**Correct Answer:**  
B. Launch the containers on Amazon Elastic Kubernetes Service (Amazon EKS) and EKS workers nodes.

**Answer Description:**  
When talking about containerized applications, the leading technologies which will always come up during the conversation are Kubernetes and Amazon ECS (Elastic Container Service).

While Kubernetes is an open-sourced container orchestration platform that was originally developed by Google, Amazon ECS is AWS’ proprietary, managed container orchestration service.

#### Exam Question 209

A company is developing a real-time multiplier game that uses UDP for communications between client and servers in an Auto Scaling group. Spikes in demand are anticipated during the day, so the game server platform must adapt accordingly. Developers want to store gamer scores and other non-relational data in a database solution that will scale without intervention.

Which solution should a solutions architect recommend?

A. Use Amazon Route 53 for traffic distribution and Amazon Aurora Serverless for data storage.  
B. Use a Network Load Balancer for traffic distribution and Amazon DynamoDB on-demand for data storage.  
C. Use a Network Load Balancer for traffic distribution and Amazon Aurora Global Database for data storage.  
D. Use an Application Load Balancer for traffic distribution and Amazon DynamoDB global tables for data storage.

**Correct Answer:**  
B. Use a Network Load Balancer for traffic distribution and Amazon DynamoDB on-demand for data storage.

#### Exam Question 210

A company operates a website on Amazon EC2 Linux instances. Some of the instances are failing.

Troubleshooting points to insufficient swap space on the failed instances. The operations team lead needs a solution to monitor this.

What should a solutions architect recommend?

A. Configure an Amazon CloudWatch SwapUsage metric dimension. Monitor the SwapUsage dimension in the EC2 metrics in CloudWatch.  
B. Use EC2 metadata to collect information, then publish it to Amazon CloudWatch custom metrics. Monitor SwapUsage metrics in CloudWatch.  
C. Install an Amazon CloudWatch agent on the instances. Run an appropriate script on a set schedule. Monitor SwapUtilization metrics in CloudWatch.  
D. Enable detailed monitoring in the EC2 console. Create an Amazon CloudWatch SwapUtilization custom metric. Monitor SwapUtilization metrics in CloudWatch.

**Correct Answer:**  
C. Install an Amazon CloudWatch agent on the instances. Run an appropriate script on a set schedule. Monitor SwapUtilization metrics in CloudWatch.

**References:**

* Amazon Elastic Compute Cloud > User Guide for Linux Instances > [Monitor memory and disk metrics for Amazon EC2 Linux instances](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mon-scripts.html)

#### Exam Question 211

A company must re-evaluate its need for the Amazon EC2 instances it currently has provisioned in an Auto Scaling group. At present, the Auto Scaling group is configured for a minimum of two instances and a maximum of four instances across two Availability Zones. A Solutions architect reviewed Amazon CloudWatch metrics and found that CPU utilization is consistently low for all the EC2 instances.

What should the solutions architect recommend to maximize utilization while ensuring the application remains fault-tolerant?

A. Remove some EC2 instances to increase the utilization of remaining instances.  
B. Increase the Amazon Elastic Block Store (Amazon EBS) capacity of instances with less CPU utilization.  
C. Modify the Auto Scaling group scaling policy to scale in and out based on a higher CPU utilization metric.  
D. Create a new launch configuration that uses smaller instance types. Update the existing Auto Scaling group.

**Correct Answer:**  
D. Create a new launch configuration that uses smaller instance types. Update the existing Auto Scaling group.

**Answer Description:**  
As the Launch Configuration can’t be modified once created, only way to update the Launch Configuration for an Auto Scaling group is to create a new one and associate it with the Auto Scaling group.

#### Exam Question 212

A solutions architect is designing the storage architecture for a new web application used for storing and viewing engineering drawings. All application components will be deployed on the AWS infrastructure.

The application design must support caching to minimize the amount of time that users wait for the engineering drawings to load. The application must be able to store petabytes of data. Which combination of storage and caching should the solutions architect use?

A. Amazon S3 with Amazon CloudFront  
B. Amazon S3 Glacier with Amazon ElastiCache  
C. Amazon Elastic Block Store (Amazon EBS) volumes with Amazon CloudFront  
D. AWS Storage Gateway with Amazon ElastiCache

**Correct Answer:**  
A. Amazon S3 with Amazon CloudFront

**Answer Description:**  
CloudFront for caching and S3 as the origin. Glacier is used for archiving which is not the case for this scenario.

#### Exam Question 213

A company is building a website that relies on reading and writing to an Amazon DynamoDB database. The traffic associated with the website predictably peaks during business hours on weekdays and declines overnight and during weekends. A solutions architect needs to design a cost-effective solution that can handle the load.

What should the solutions architect do to meet these requirements?

A. Enable DynamoDB Accelerator (DAX) to cache the data.  
B. Enable Multi-AZ replication for the DynamoDB database.  
C. Enable DynamoDB auto scaling when creating the tables.  
D. Enable DynamoDB On-Demand capacity allocation when creating the tables.

**Correct Answer:**  
C. Enable DynamoDB auto scaling when creating the tables.

#### Exam Question 214

A company uses Amazon Redshift for its data warehouse. The company wants to ensure high durability for its data in case of any component failure.

What should a solutions architect recommend?

A. Enable concurrency scaling.  
B. Enable cross-Region snapshots.  
C. Increase the data retention period.  
D. Deploy Amazon Redshift in Multi-AZ.

**Correct Answer:**  
B. Enable cross-Region snapshots.

#### Exam Question 215

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

What should the solutions architect do to enable internet access for the private subnets?

A. Create three NAT gateways, one for each public subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ.  
B. Create three NAT instances, one for each private subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT instance in its AZ.  
C. Create a second internet gateway on one of the private subnets. Update the route table for the private subnets that forward non-VPC traffic to the private internet gateway.  
D. Create an egress-only internet gateway on one of the public subnets. Update the route table for the private subnets that forward non-VPC traffic to the egress-only internet gateway.

**Correct Answer:**  
B. Create three NAT instances, one for each private subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT instance in its AZ.

#### Exam Question 216

An online photo application lets users upload photos and perform image editing operations. The application offers two classes of service: free and paid. Photos submitted by paid users are processed before those submitted by free users. Photos are uploaded to Amazon S3 and the job information is sent to Amazon SQS.

Which configuration should a solutions architect recommend?

A. Use one SQS FIFO queue. Assign a higher priority to the paid photos so they are processed first.  
B. Use two SQS FIFO queues: one for paid and one for free. Set the free queue to use short polling and the paid queue to use long polling.  
C. Use two SQS standard queues: one for paid and one for free. Configure Amazon EC2 instances to prioritize polling for the paid queue over the free queue.  
D. Use one SQS standard queue. Set the visibility timeout of the paid photos to zero. Configure Amazon EC2 instances to prioritize visibility settings so paid photos are processed first.

**Correct Answer:**  
A. Use one SQS FIFO queue. Assign a higher priority to the paid photos so they are processed first.

#### Exam Question 217

A company has three VPCs named Development, Testing, and Production in the us-east-1 Region. The three VPCs need to be connected to an on-premises data center and are designed to be separate to maintain security and prevent any resource sharing. A solutions architect needs to find a scalable and secure solution.

What should the solutions architect recommend?

A. Create an AWS Direct Connect connection and a VPN connection for each VPC to connect back to the data center.  
B. Create VPC peers from all the VPCs to the Production VPC. Use an AWS Direct Connect connection from the Production VPC back to the data center.  
C. Connect VPN connections from all the VPCs to a VPN in the Production VPC. Use a VPN connection from the Production VPC back to the data center.  
D. Create a new VPC called Network. Within the Network VPC, create an AWS Transit Gateway with an AWS Direct Connect connection back to the data center. Attach all the other VPCs to the Network VPC.

**Correct Answer:**  
B. Create VPC peers from all the VPCs to the Production VPC. Use an AWS Direct Connect connection from the Production VPC back to the data center.

#### Exam Question 218

A company is deploying a web portal. The company wants to ensure that only the web portion of the application is publicly accessible. To accomplish this, the VPC was designed with two public subnets and two private subnets. The application will run on several Amazon EC2 instances in an Auto Scaling group. SSL termination must be offloaded from the EC2 instances.

What should a solutions architect do to ensure these requirements are met?

A. Configure the Network Load Balancer in the public subnets. Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer.  
B. Configure the Network Load Balancer in the public subnets. Configure the Auto Scaling group in the public subnets and associate it with the Application Load Balancer.  
C. Configure the Application Load Balancer in the public subnets. Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer.  
D. Configure the Application Load Balancer in the private subnets. Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer.

**Correct Answer:**  
C. Configure the Application Load Balancer in the public subnets. Configure the Auto Scaling group in the private subnets and associate it with the Application Load Balancer.

#### Exam Question 219

A company is experiencing growth as demand for its product has increased. The company’s existing purchasing application is slow when traffic spikes. The application is a monolithic three-tier application that uses synchronous transactions and sometimes sees bottlenecks in the application tier. A solutions architect needs to design a solution that can meet required application response times while accounting for traffic volume spikes.

Which solution will meet these requirements?

A. Vertically scale the application instance using a larger Amazon EC2 instance size.  
B. Scale the application’s persistence layer horizontally by introducing Oracle RAC on AWS.  
C. Scale the web and application tiers horizontally using Auto Scaling groups and an Application Load Balancer.  
D. Decouple the application and data tiers using Amazon Simple Queue Service (Amazon SQS) with asynchronous AWS Lambda calls.

**Correct Answer:**  
C. Scale the web and application tiers horizontally using Auto Scaling groups and an Application Load Balancer.

**Answer Description:**  
The Application uses synchronous transactions each operation is dependent on the previous one. Using asynchronous lambda calls may not work here.

#### Exam Question 220

A company has copied 1 PB of data from a colocation facility to an Amazon S3 bucket in the us-east-1 Region using an AWS Direct Connect link. The company now wants to copy the data to another S3 bucket in the us-west-2 Region. The colocation facility does not allow the use of AWS Snowball.

What should a solutions architect recommend to accomplish this?

A. Order a Snowball Edge device to copy the data from one Region to another Region.  
B. Transfer contents from the source S3 bucket to a target S3 bucket using the S3 console.  
C. Use the aws S3 sync command to copy data from the source bucket to the destination bucket.  
D. Add a cross-Region replication configuration to copy objects across S3 buckets in different Regions.

**Correct Answer:**  
C. Use the aws S3 sync command to copy data from the source bucket to the destination bucket.

**References:**

* [How can I copy all objects from one Amazon S3 bucket to another bucket?](https://aws.amazon.com/premiumsupport/knowledge-center/move-objects-s3-bucket/)

The latest AWS Certified Solutions Architect – Associate SAA-C02 certification actual real practice exam question and answer (Q&A) dumps are available free, which are helpful for you to pass the AWS Certified Solutions Architect – Associate SAA-C02 exam and earn AWS Certified Solutions Architect – Associate SAA-C02 certification.

#### Exam Question 221

A company is using a fleet of Amazon EC2 instances to ingest data from on-premises data sources. The data is in JSON format and ingestion rates can be as high as 1 MB/s. When an EC2 instance is rebooted, the data in-flight is lost. The company’s data science team wants to query ingested data in near-real time.

Which solution provides near-real-time data querying that is scalable with minimal data loss?

A. Publish data to Amazon Kinesis Data Streams. Use Kinesis Data Analytics to query the data.  
B. Publish data to Amazon Kinesis Data Firehose with Amazon Redshift as the destination. Use Amazon Redshift to query the data.  
C. Store ingested data in an EC2 instance store. Publish data to Amazon Kinesis Data Firehose with Amazon S3 as the destination. Use Amazon Athena to query the data.  
D. Store ingested data in an Amazon Elastic Block Store (Amazon EBS) volume. Publish data to Amazon ElastiCache for Redis. Subscribe to the Redis channel to query the data.

**Correct Answer:**  
B. Publish data to Amazon Kinesis Data Firehose with Amazon Redshift as the destination. Use Amazon Redshift to query the data.

**Answer Description:**  
Kinesis data streams consists of shards. The more throughput is needed, the more shards you add, the less throughput, the more shards you remove, so it’s scalable. Each shard can handle up to 1MB/s of writes.

However Kinesis data streams stores ingested data for only 1 to 7 days so there is a chance of data loss. Additionally,

Kinesis data analytics and kinesis data streams are both for real-time ingestion and analytics. Firehouse on the other hand is also scalable and processes data in near real time as per the requirement. It also transfers data into Redshift which is a data warehouse so data won’t be lost. Redshift also has a SQL interface for performing queries for data analytics.

#### Exam Question 222

A solutions architect is designing a security solution for a company that wants to provide developers with individual AWS accounts through AWS Organizations, while also maintaining standard security controls.

Because the individual developers will have AWS account root user-level access to their own accounts, the solutions architect wants to ensure that the mandatory AWS CloudTrail configuration that is applied to new developer accounts is not modified.

Which action meets these requirements?

A. Create an IAM policy that prohibits changes to CloudTrail, and attach it to the root user.  
B. Create a new trail in CloudTrail from within the developer accounts with the organization trails option enabled.  
C. Create a service control policy (SCP) the prohibits changes to CloudTrail, and attach it the developer accounts.  
D. Create a service-linked role for CloudTrail with a policy condition that allows changes only from an Amazon Resource Name (ARN) in the master account.

**Correct Answer:**  
C. Create a service control policy (SCP) the prohibits changes to CloudTrail, and attach it the developer accounts.

#### Exam Question 223

A company has an automobile sales website that stores its listings in a database on Amazon RDS. When an automobile is sold, the listing needs to be removed from the website and the data must be sent to multiple target systems.

Which design should a solutions architect recommend?

A. Create an AWS Lambda function triggered when the database on Amazon RDS is updated to send the information to an Amazon Simple Queue Service (Amazon SQS) queue for the targets to consume.  
B. Create an AWS Lambda function triggered when the database on Amazon RDS is updated to send the information to an Amazon Simple Queue Service (Amazon SQS) FIFO queue for the targets to consume.  
C. Subscribe to an RDS event notification and send an Amazon Simple Queue Service (Amazon SQS) queue fanned out to multiple Amazon Simple Notification Service (Amazon SNS) topics. Use AWS Lambda functions to update the targets.  
D. Subscribe to an RDS event notification and send an Amazon Simple Notification Service (Amazon SNS) topic fanned out to multiple Amazon Simple Queue Service (Amazon SQS) queues. Use AWS Lambda functions to update the targets.

**Correct Answer:**  
A. Create an AWS Lambda function triggered when the database on Amazon RDS is updated to send the information to an Amazon Simple Queue Service (Amazon SQS) queue for the targets to consume.

**Answer Description:**  
You can use AWS Lambda to process event notifications from an Amazon Relational Database Service (Amazon RDS) database. Amazon RDS sends notifications to an Amazon Simple Notification Service (Amazon SNS) topic, which you can configure to invoke a Lambda function. Amazon SNS wraps the message from Amazon RDS in its own event document and sends it to your function.

**References:**

* AWS Lambda > Developer Guide > [Using AWS Lambda with Amazon SNS](https://docs.aws.amazon.com/lambda/latest/dg/with-sns.html)
* AWS Compute Blog > [Messaging Fanout Pattern for Serverless Architectures Using Amazon SNS](https://aws.amazon.com/blogs/compute/messaging-fanout-pattern-for-serverless-architectures-using-amazon-sns/)

#### Exam Question 224

A company is building a media sharing application and decides to use Amazon S3 for storage. When a media file is uploaded, the company starts a multi-step process to create thumbnails, identify objects in the images, transcode videos into standard formats and resolutions, and extract and store the metadata to an Amazon DynamoDB table. The metadata is used for searching and navigation.

The amount of traffic is variable. The solution must be able to scale to handle spikes in load without unnecessary expenses.

What should a solutions architect recommend to support this workload?

A. Build the processing into the website or mobile app used to upload the content to Amazon S3. Save the required data to the DynamoDB table when the objects are uploaded.  
B. Trigger AWS Step Functions when an object is stored in the S3 bucket. Have the Step Functions perform the steps needed to process the object and then write the metadata to the DynamoDB table.  
C. Trigger an AWS Lambda function when an object is stored in the S3 bucket. Have the Lambda function start AWS Batch to perform the steps to process the object. Place the object data in the DynamoDB table when complete.  
D. Trigger an AWS Lambda function to store an initial entry in the DynamoDB table when an object is uploaded to Amazon S3. Use a program running on an Amazon EC2 instance in an Auto Scaling group to poll the index for unprocessed items, and use the program to perform the processing.

**Correct Answer:**  
C. Trigger an AWS Lambda function when an object is stored in the S3 bucket. Have the Lambda function start AWS Batch to perform the steps to process the object. Place the object data in the DynamoDB table when complete.

#### Exam Question 225

A company provides an API to its users that automates inquiries for tax computations based on item prices.

The company experiences a larger number of inquiries during the holiday season only that cause slower response times. A solutions architect needs to design a solution that is scalable and elastic.

What should the solutions architect do to accomplish this?

A. Provide an API hosted on an Amazon EC2 instance. The EC2 instance performs the required computations when the API request is made.  
B. Design a REST API using Amazon API Gateway that accepts the item names. API Gateway passes item names to AWS Lambda for tax computations.  
C. Create an Application Load Balancer that has two Amazon EC2 instances behind it. The EC2 instances will compute the tax on the received item names.  
D. Design a REST API using Amazon API Gateway that connects with an API hosted on an Amazon EC2 instance. API Gateway accepts and passes the item names to the EC2 instance for tax computations.

**Correct Answer:**  
B. Design a REST API using Amazon API Gateway that accepts the item names. API Gateway passes item names to AWS Lambda for tax computations.

#### Exam Question 226

An application is running on an Amazon EC2 instance and must have millisecond latency when running the workload. The application makes many small reads and writes to the file system, but the file system itself is small.

Which Amazon Elastic Block Store (Amazon EBS) volume type should a solutions architect attach to their EC2 instance?

A. Cold HDD (sc1)  
B. General Purpose SSD (gp2)  
C. Provisioned IOPS SSD (io1)  
D. Throughput Optimized HDD (st1)

**Correct Answer:**  
B. General Purpose SSD (gp2)

#### Exam Question 227

A solutions architect needs to ensure that all Amazon Elastic Block Store (Amazon EBS) volumes restored from unencrypted EBC snapshots are encrypted.

What should the solutions architect do to accomplish this?

A. Enable EBS encryption by default for the AWS Region.  
B. Enable EBS encryption by default for the specific volumes.  
C. Create a new volume and specify the symmetric customer master key (CMK) to use for encryption.  
D. Create a new volume and specify the asymmetric customer master key (CMK) to use for encryption.

**Correct Answer:**  
A. Enable EBS encryption by default for the AWS Region.

**Answer Description:**  
Question asked is to ensure that all volumes restored are encrypted. So have to be “[Enable encryption by default](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html#encryption-by-default)”.

#### Exam Question 228

A company runs a static website through its on-premises data center. The company has multiple servers that handle all of its traffic, but on busy days, services are interrupted and the website becomes unavailable.

The company wants to expand its presence globally and plans to triple its website traffic.

What should a solutions architect recommend to meet these requirements?

A. Migrate the website content to Amazon S3 and host the website on Amazon CloudFront.  
B. Migrate the website content to Amazon EC2 instances with public Elastic IP addresses in multiple AWS Regions.  
C. Migrate the website content to Amazon EC2 instances and vertically scale as the load increases.  
D. Use Amazon Route 53 to distribute the loads across multiple Amazon CloudFront distributions for each AWS Region that exists globally.

**Correct Answer:**  
D. Use Amazon Route 53 to distribute the loads across multiple Amazon CloudFront distributions for each AWS Region that exists globally.

#### Exam Question 229

A company has a highly dynamic batch processing job that uses many Amazon EC2 instances to complete it. The job is stateless in nature, can be started and stopped at any given time with no negative impact, and typically takes upwards of 60 minutes total to complete. The company has asked a solutions architect to design a scalable and cost-effective solution that meets the requirements of the job.

What should the solutions architect recommend?

A. Implement EC2 Spot Instances.  
B. Purchase EC2 Reserved Instances.  
C. Implement EC2 On-Demand Instances.  
D. Implement the processing on AWS Lambda.

**Correct Answer:**  
A. Implement EC2 Spot Instances.

#### Exam Question 230

A company is hosting its static website in an Amazon S3 bucket, which is the origin for Amazon CloudFront.

The company has users in the United States, Canada, and Europe and wants to reduce costs.

What should a solutions architect recommend?

A. Adjust the CloudFront caching time to live (TTL) from the default to a longer timeframe.  
B. Implement CloudFront events with Lambda@Edge to run the website’s data processing.  
C. Modify the CloudFront price class to include only the locations of the countries that are served.  
D. Implement a CloudFront Secure Sockets Layer (SSL) certificate to push security closer to the locations of the countries that are served.

**Correct Answer:**  
C. Modify the CloudFront price class to include only the locations of the countries that are served.

#### Exam Question 231

A company is designing a website that uses an Amazon S3 bucket to store static images. The company wants all future requests to have faster response times while reducing both latency and cost.

Which service configuration should a solutions architect recommend?

A. Deploy a NAT server in front of Amazon S3.  
B. Deploy Amazon CloudFront in front of Amazon S3.  
C. Deploy a Network Load Balancer in front of Amazon S3.  
D. Configure Auto Scaling to automatically adjust the capacity of the website.

**Correct Answer:**  
B. Deploy Amazon CloudFront in front of Amazon S3.

#### Exam Question 232

A company needs to comply with a regulatory requirement that states all emails must be stored and archived externally for 7 years. An administrator has created compressed email files on premises and wants a managed service to transfer the files to AWS storage.

Which managed service should a solutions architect recommend?

A. Amazon Elastic File System (Amazon EFS)  
B. Amazon S3 Glacier  
C. AWS Backup  
D. AWS Storage Gateway

**Correct Answer:**  
D. AWS Storage Gateway

#### Exam Question 233

A company that hosts its web application on AWS wants to ensure all Amazon EC2 instances, Amazon RDS DB instances, and Amazon Redshift clusters are configured with tags. The company wants to minimize the effort of configuring and operating this check.

What should a solutions architect do to accomplish this?

A. Use AWS Config rules to define and detect resources that are not properly tagged.  
B. Use Cost Explorer to display resources that are not properly tagged. Tag those resources manually.  
C. Write API calls to check all resources for proper tag allocation. Periodically run the code on an EC2 instance.  
D. Write API calls to check all resources for proper tag allocation. Schedule an AWS Lambda function through Amazon CloudWatch to periodically run the code.

**Correct Answer:**  
A. Use AWS Config rules to define and detect resources that are not properly tagged.

#### Exam Question 234

A company has a live chat application running on its on-premises servers that use WebSockets. The company wants to migrate the application to AWS. Application traffic is inconsistent, and the company expects there to be more traffic with sharp spikes in the future.

The company wants a highly scalable solution with no server maintenance nor advanced capacity planning.

Which solution meets these requirements?

A. Use Amazon API Gateway and AWS Lambda with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for provisioned capacity.  
B. Use Amazon API Gateway and AWS Lambda with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for on-demand capacity.  
C. Run Amazon EC2 instances behind an Application Load Balancer in an Auto Scaling group with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for on-demand capacity.  
D. Run Amazon EC2 instances behind a Network Load Balancer in an Auto Scaling group with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for provisioned capacity.

**Correct Answer:**  
B. Use Amazon API Gateway and AWS Lambda with an Amazon DynamoDB table as the data store. Configure the DynamoDB table for on-demand capacity.

#### Exam Question 235

A company hosts its static website content from an Amazon S3 bucket in the us-east-1 Region. Content is made available through an Amazon CloudFront origin pointing to that bucket. Cross-Region replication is set to create a second copy of the bucket in the ap-southeast-1 Region. Management wants a solution that provides greater availability for the website.

Which combination of actions should a solutions architect take to increase availability? (Choose two.)

A. Add both buckets to the CloudFront origin.  
B. Configure failover routing in Amazon Route 53.  
C. Create a record in Amazon Route 53 pointing to the replica bucket.  
D. Create an additional CloudFront origin pointing to the ap-southeast-1 bucket.  
E. Set up a CloudFront origin group with the us-east-1 bucket as the primary and the ap-southeast-1 bucket as the secondary.

**Correct Answer:**  
B. Configure failover routing in Amazon Route 53.  
E. Set up a CloudFront origin group with the us-east-1 bucket as the primary and the ap-southeast-1 bucket as the secondary.

#### Exam Question 236

A company hosts a training site on a fleet of Amazon EC2 instances. The company anticipates that its new course, which consists of dozens of training videos on the site, will be extremely popular when it is released in 1 week.

What should a solutions architect do to minimize the anticipated server load?

A. Store the videos in Amazon ElastiCache for Redis. Update the web servers to serve the videos using the ElastiCache API.  
B. Store the videos in Amazon Elastic File System (Amazon EFS). Create a user data script for the web servers to mount the EFS volume.  
C. Store the videos in an Amazon S3 bucket. Create an Amazon CloudFront distribution with an origin access identity (OAI) of that S3 bucket. Restrict Amazon S3 access to the OAI.  
D. Store the videos in an Amazon S3 bucket. Create an AWS Storage Gateway file gateway to access the S3 bucket. Create a user data script for the web servers to mount the file gateway.

**Correct Answer:**  
C. Store the videos in an Amazon S3 bucket. Create an Amazon CloudFront distribution with an origin access identity (OAI) of that S3 bucket. Restrict Amazon S3 access to the OAI.

#### Exam Question 237

A company runs a production application on a fleet of Amazon EC2 instances. The application reads the data from an Amazon SQS queue and processes the messages in parallel. The message volume is unpredictable and often has intermittent traffic. This application should continually process messages without any downtime.

Which solution meets these requirements MOST cost-effectively?

A. Use Spot Instances exclusively to handle the maximum capacity required.  
B. Use Reserved Instances exclusively to handle the maximum capacity required.  
C. Use Reserved Instances for the baseline capacity and use Spot Instances to handle additional capacity.  
D. Use Reserved Instances for the baseline capacity and use On-Demand Instances to handle additional capacity.

**Correct Answer:**  
C. Use Reserved Instances for the baseline capacity and use Spot Instances to handle additional capacity.

#### Exam Question 238

Management has decided to deploy all AWS VPCs with IPv6 enabled. After some time, a solutions architect tries to launch a new instance and receives an error stating that there is not enough IP address space available in the subnet.

What should the solutions architect do to fix this?

A. Check to make sure that only IPv6 was used during the VPC creation.  
B. Create a new IPv4 subnet with a larger range, and then launch the instance.  
C. Create a new IPv6-only subnet with a large range, and then launch the instance.  
D. Disable the IPv4 subnet and migrate all instances to IPv6 only. Once that is complete, launch the instance.

**Correct Answer:**  
B. Create a new IPv4 subnet with a larger range, and then launch the instance.

**Answer Description:**  
First of all, there is no IPv6-only VPC on AWS. A VPC is always IPv4 enabled, but you can optionally enable IPv6 (dual-stack).

**References:**

* [Getting started with IPv6 on AWS](https://cloudonaut.io/getting-started-with-ipv6-on-aws/)

#### Exam Question 239

A company has an image processing workload running on Amazon Elastic Container Service (Amazon ECS) in two private subnets. Each private subnet uses a NAT instance for internet access. All images are stored in Amazon S3 buckets. The company is concerned about the data transfer costs between Amazon ECS and Amazon S3.

What should a solutions architect do to reduce costs?

A. Configure a NAT gateway to replace the NAT instances.  
B. Configure a gateway endpoint for traffic destined to Amazon S3.  
C. Configure an interface endpoint for traffic destined to Amazon S3.  
D. Configure Amazon CloudFront for the S3 bucket storing the images.

**Correct Answer:**  
C. Configure an interface endpoint for traffic destined to Amazon S3.

**Answer Description:**  
S3 and Dynamo DB does not support interface endpoints. Both S3 and DynamoDB are routed via Gateway endpoint.  
Interface Endpoint only supports services that are integrated with PrivateLink.

**References:**

* Amazon Virtual Private Cloud > AWS PrivateLink > [VPC endpoints](https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints.html)
* Amazon Virtual Private Cloud > AWS PrivateLink > [AWS services that integrate with AWS PrivateLink](https://docs.aws.amazon.com/vpc/latest/privatelink/integrated-services-vpce-list.html)

#### Exam Question 240

A company has an on-premises volume backup solution that has reached its end of life. The company wants to use AWS as part of a new backup solution and wants to maintain local access to all the data while it is backed up on AWS. The company wants to ensure that the data backed up on AWS is automatically and securely transferred.

Which solution meets these requirements?

A. Use AWS Snowball to migrate data out of the on-premises solution to Amazon S3. Configure on-premises systems to mount the Snowball S3 endpoint to provide local access to the data.  
B. Use AWS Snowball Edge to migrate data out of the on-premises solution to Amazon S3. Use the Snowball Edge file interface to provide on-premises systems with local access to the data.  
C. Use AWS Storage Gateway and configure a cached volume gateway. Run the Storage Gateway software appliance on-premises and configure a percentage of data to cache locally. Mount the gateway storage volumes to provide local access to the data.  
D. Use AWS Storage Gateway and configure a stored volume gateway. Run the Storage Gateway software appliance on premises and map the gateway storage volumes to on-premises storage. Mount the gateway storage volumes to provide local access to the data.

**Correct Answer:**  
D. Use AWS Storage Gateway and configure a stored volume gateway. Run the Storage Gateway software appliance on premises and map the gateway storage volumes to on-premises storage. Mount the gateway storage volumes to provide local access to the data.

**References:**

* AWS Snowball Edge Developer Guide > [Best Practices for the AWS Snowball Edge Device](https://docs.aws.amazon.com/snowball/latest/developer-guide/BestPractices.html)

#### Exam Question 241

A company is using a third-party vendor to manage its marketplace analytics. The vendor needs limited programmatic access to resources in the company’s account. All the needed policies have been created to grant appropriate access.

Which additional component will provide the vendor with the MOST secure access to the account?

A. Create an IAM user.  
B. Implement a service control policy (SCP)  
C. Use a cross-account role with an external ID.  
D. Configure a single sign-on (SSO) identity provider.

**Correct Answer:**  
B. Implement a service control policy (SCP)

#### Exam Question 242

A solutions architect is designing the cloud architecture for a company that needs to host hundreds of machine learning models for its users. During startup, the models need to load up to 10 GB of data from Amazon S3 into memory, but they do not need disk access. Most of the models are used sporadically, but the users expect all of them to be highly available and accessible with low latency.

Which solution meets the requirements and is MOST cost-effective?

A. Deploy models as AWS Lambda functions behind an Amazon API Gateway for each model.  
B. Deploy models as Amazon Elastic Container Service (Amazon ECS) services behind an Application Load Balancer for each model.  
C. Deploy models as AWS Lambda functions behind a single Amazon API Gateway with path-based routing where one path corresponds to each model.  
D. Deploy models as Amazon Elastic Container Service (Amazon ECS) services behind a single Application Load Balancer with path-based routing where one path corresponds to each model.

**Correct Answer:**  
C. Deploy models as AWS Lambda functions behind a single Amazon API Gateway with path-based routing where one path corresponds to each model.

**Answer Description:**  
AWS just update Lambda to support 10G memory and helping compute intensive applications like machine learning…  
No disk access, lowest cost.

**References:**

[AWS Lambda now supports up to 10 GB of memory and 6 vCPU cores for Lambda Functions](https://aws.amazon.com/about-aws/whats-new/2020/12/aws-lambda-supports-10gb-memory-6-vcpu-cores-lambda-functions/)

#### Exam Question 243

A company has created a multi-tier application for its eCommerce website. The website uses an Application Load Balancer that resides in the public subnets, a web tier in the public subnets, and a MySQL cluster hosted on Amazon EC2 instances in the private subnets. The MySQL database needs to retrieve product catalog and pricing information that is hosted on the internet by a third-party provider. A solutions architect must devices a strategy that maximizes security without increasing operational overhead.

What should the solutions architect do to meet these requirements?

A. Deploy a NAT instance in the VPC. Route all the internet-based traffic through the NAT instance.  
B. Deploy a NAT gateway in the public subnets. Modify the private subnet route table to direct all internet-bound traffic to the NAT gateway.  
C. Configure an internet gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the internet gateway.  
D. Configure a virtual private gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the virtual private gateway.

**Correct Answer:**  
C. Configure an internet gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the internet gateway.

**References:**

* Amazon Virtual Private Cloud > User Guide > [NAT gateways](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html)

#### Exam Question 244

A solutions architect is designing a new API using Amazon API Gateway that will receive requests from users. The volume of requests is highly variable; several hours can pass without receiving a single request.

The data processing will take place asynchronously, but should be completed within a few seconds after a request is made.

Which compute service should the solutions architect have the API invoke to deliver the requirements at the lowest cost?

A. An AWS Glue job  
B. An AWS Lambda function  
C. A containerized service hosted in Amazon Elastic Kubernetes Service (Amazon EKS)  
D. A containerized service hosted in Amazon ECS with Amazon EC2

**Correct Answer:**  
B. An AWS Lambda function

#### Exam Question 245

A company hosts its application in the AWS Cloud. The application runs on Amazon EC2 instances behind an Elastic Load Balancer in an Auto Scaling group and with an Amazon DynamoDB table. The company wants to ensure the application can be made available in another AWS Region with minimal downtime.

What should a solutions architect do to meet these requirements with the LEAST amount of downtime?

A. Create an Auto Scaling group and a load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region’s load balancer.  
B. Create an AWS CloudFormation template to create EC2 instances, load balancers, and DynamoDB tables to be executed when needed. Configure DNS failover to point to the new disaster recovery Region’s load balancer.  
C. Create an AWS CloudFormation template to create EC2 instances and a load balancer to be executed when needed. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region’s load balancer.  
D. Create an Auto Scaling group and load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Create an Amazon CloudWatch alarm to trigger and AWS Lambda function that updates Amazon Route 53 pointing to the disaster recovery load balancer.

**Correct Answer:**  
D. Create an Auto Scaling group and load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Create an Amazon CloudWatch alarm to trigger and AWS Lambda function that updates Amazon Route 53 pointing to the disaster recovery load balancer.

#### Exam Question 246

A business application is hosted on Amazon EC2 and uses Amazon S3 for encrypted object storage. The chief information security officer has directed that no application traffic between the two services should traverse the public internet.

Which capability should the solutions architect use to meet the compliance requirements?

A. AWS Key Management Service (AWS KMS)  
B. VPC endpoint  
C. Private subnet  
D. Virtual private gateway

**Correct Answer:**  
A. AWS Key Management Service (AWS KMS)

**References:**

* [Amazon VPC FAQs](https://aws.amazon.com/vpc/faqs/)

#### Exam Question 247

A company runs an application on an Amazon EC2 instance backed by Amazon Elastic Block Store (Amazon EBS). The instance needs to be available for 12 hours daily. The company wants to save costs by making the instance unavailable outside the window required for the application. However, the contents of the instance’s memory must be preserved whenever the instance is unavailable.

What should a solutions architect do to meet this requirement?

A. Stop the instance outside the application’s availability window. Start up the instance again when required.  
B. Hibernate the instance outside the application’s availability window. Start up the instance again when required.  
C. Use Auto Scaling to scale down the instance outside the application’s availability window. Scale up the instance when required.  
D. Terminate the instance outside the application’s availability window. Launch the instance by using a preconfigured Amazon Machine Image (AMI) when required.

**Correct Answer:**  
A. Stop the instance outside the application’s availability window. Start up the instance again when required.

#### Exam Question 248

A solutions architect is creating a new VPC design. There are two public subnets for the load balancer, two private subnets for web servers, and two private subnets for MySQL. The web servers use only HTTPS.

The solutions architect has already created a security group for the load balancer allowing port 443 from 0.0.0.0/0. Company policy requires that each resource has the least access required to still be able to perform its tasks.

Which additional configuration strategy should the solutions architect use to meet these requirements?

A. Create a security group for the web servers and allow port 443 from 0.0.0.0/0. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.  
B. Create a network ACL for the web servers and allow port 443 from 0.0.0.0/0. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.  
C. Create a security group for the web servers and allow port 443 from the load balancer. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.  
D. Create a network ACL for the web servers and allow port 443 from the load balancer. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.

**Correct Answer:**  
B. Create a network ACL for the web servers and allow port 443 from 0.0.0.0/0. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.

#### Exam Question 249

A company hosts historical weather records in Amazon S3. The records are downloaded from the company’s website by a way of a URL that resolves to a domain name. Users all over the world access this content through subscriptions. A third-party provider hosts the company’s root domain name, but the company recently migrated some of its services to Amazon Route 53. The company wants to consolidate contracts, reduce latency for users, and reduce costs related to serving the application to subscribers.

Which solution meets these requirements?

A. Create a web distribution on Amazon CloudFront to serve the S3 content for the application. Create a CNAME record in a Route 53 hosted zone that points to the CloudFront distribution, resolving to the application’s URL domain name.  
B. Create a web distribution on Amazon CloudFront to serve the S3 content for the application. Create an ALIAS record in the Amazon Route 53 hosted zone that points to the CloudFront distribution, resolving to the application’s URL domain name.  
C. Create an A record in a Route 53 hosted zone for the application. Create a Route 53 traffic policy for the web application, and configure a geolocation rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.  
D. Create an A record in a Route 53 hosted zone for the application. Create a Route 53 traffic policy for the web application, and configure a geoproximity rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.

**Correct Answer:**  
B. Create a web distribution on Amazon CloudFront to serve the S3 content for the application. Create an ALIAS record in the Amazon Route 53 hosted zone that points to the CloudFront distribution, resolving to the application’s URL domain name.

#### Exam Question 250

company owns an asynchronous API that is used to ingest user requests and, based on the request type, dispatch requests to the appropriate microservice for processing. The company is using Amazon API Gateway to deploy the API front end, and an AWS Lambda function that invokes Amazon DynamoDB to store user requests before dispatching them to the processing microservices.

The company provisioned as much DynamoDB throughput as its budget allows, but the company is still experiencing availability issues and is losing user requests.

What should a solutions architect do to address this issue without impacting existing users?

A. Add throttling on the API Gateway with server-side throttling limits.  
B. Use DynamoDB Accelerator (DAX) and Lambda to buffer writes to DynamoDB.  
C. Create a secondary index in DynamoDB for the table with the user requests.  
D. Use the Amazon Simple Queue Service (Amazon SQS) queue and Lambda to buffer writes to DynamoDB.

**Correct Answer:**  
B. Use DynamoDB Accelerator (DAX) and Lambda to buffer writes to DynamoDB.

#### Exam Question 251

A company is moving its on-premises applications to Amazon EC2 instances. However, as a result of fluctuating compute requirements, the EC2 instances must always be ready to use between 8 AM and 5 PM in specific Availability Zones.

Which EC2 instances should the company choose to run the applications?

A. Scheduled Reserved Instances  
B. On-Demand Instances  
C. Spot Instances as part of a Spot Fleet  
D. EC2 instances in an Auto Scaling group

**Correct Answer:**  
A. Scheduled Reserved Instances

#### Exam Question 252

A company is building an application on Amazon EC2 instances that generates temporary transactional data. The application requires access to data storage that can provide configurable and consistent IOPS.

What should a solutions architect recommend?

A. Provision an EC2 instance with a Throughput Optimized HDD (st1) root volume and a Cold HDD (sc1) data volume.  
B. Provision an EC2 instance with a Throughput Optimized HDD (st1) volume that will serve as the root and data volume.  
C. Provision an EC2 instance with a General Purpose SSD (gp2) root volume and Provisioned IOPS SSD (io1) data volume.  
D. Provision an EC2 instance with a General Purpose SSD (gp2) root volume. Configure the application to store its data in an Amazon S3 bucket.

**Correct Answer:**  
C. Provision an EC2 instance with a General Purpose SSD (gp2) root volume and Provisioned IOPS SSD (io1) data volume.

#### Exam Question 253

A solutions architect needs to design a resilient solution for Windows users’ home directories. The solution must provide fault tolerance, file-level backup and recovery, and access control, based upon the company’s Active Directory.

Which storage solution meets these requirements?

A. Configure Amazon S3 to store the users’ home directories. Join Amazon S3 to Active Directory.  
B. Configure a Multi-AZ file system with Amazon FSx for Windows File Server. Join Amazon FSx to Active Directory.  
C. Configure Amazon Elastic File System (Amazon EFS) for the users’ home directories. Configure AWS Single Sign-On with Active Directory.  
D. Configure Amazon Elastic Block Store (Amazon EFS) to store the users’ home directories. Configure AWS Single Sign-On with Active Directory.

**Correct Answer:**  
C. Configure Amazon Elastic File System (Amazon EFS) for the users’ home directories. Configure AWS Single Sign-On with Active Directory.

#### Exam Question 254

A company wants to move a multi-tiered application from on-premises to the AWS Cloud to improve the application’s performance. The application consists of application tiers that communicate with each other by way of RESTful services.

Transactions are dropped when one tier becomes overloaded. A solutions architect must design a solution that resolves these issues and modernizes the application.

Which solution meets these requirements and is the MOST operationally efficient?

A. Use Amazon API Gateway and direct transactions to the AWS Lambda functions as the application layer. Use Amazon Simple Queue Service (Amazon SQS) as the communication layer between application services.  
B. Use Amazon CloudWatch metrics to analyze the application performance history to determine the server’s peak utilization during the performance failures. Increase the size of the application server’s Amazon EC2 instances to meet the peak requirements.  
C. Use Amazon Simple Notification Service (Amazon SNS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SNS queue length and scale up and down as required.  
D. Use Amazon Simple Queue Service (Amazon SQS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SQS queue length and scale up when communication failures are detected.

**Correct Answer:**  
D. Use Amazon Simple Queue Service (Amazon SQS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SQS queue length and scale up when communication failures are detected.

#### Exam Question 255

A company serves a multilingual website from a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). This architecture is currently running in the us-west-1 Region but is exhibiting high request latency for users located in other parts of the world.

The website needs to serve requests quickly and efficiently regardless of a user’s location. However, the company does not want to recreate the existing architecture across multiple Regions.

How should a solutions architect accomplish this?

A. Replace the existing architecture with a website served from an Amazon S3 bucket. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.  
B. Configure an Amazon CloudFront distribution with the ALB as the origin. Set the cache behavior settings to only cache based on the Accept-Language request header.  
C. Set up Amazon API Gateway with the ALB as an integration. Configure API Gateway to use an HTTP integration type. Set up an API Gateway stage to enable the API cache.  
D. Launch an EC2 instance in each additional Region and configure NGINX to act as a cache server for that Region. Put all the instances plus the ALB behind an Amazon Route 53 record set with a geolocation routing policy.

**Correct Answer:**  
B. Configure an Amazon CloudFront distribution with the ALB as the origin. Set the cache behavior settings to only cache based on the Accept-Language request header.

#### Exam Question 256

A software vendor is deploying a new software-as-a-service (SaaS) solution that will be utilized by many AWS users. The service is hosted in a VPC behind a Network Load Balancer. The software vendor wants to provide access to this service to users with the least amount of administrative overhead and without exposing the service to the public internet.

What should a solutions architect do to accomplish this goal?

A. Create a peering VPC connection from each user’s VPC to the software vendor’s VPC.  
B. Deploy a transit VPC in the software vendor’s AWS account. Create a VPN connection with each user account.  
C. Connect the service in the VPC with an AWS Private Link endpoint. Have users subscribe to the endpoint.  
D. Deploy a transit VPC in the software vendor’s AWS account. Create an AWS Direct Connect connection with each user account.

**Correct Answer:**  
C. Connect the service in the VPC with an AWS Private Link endpoint. Have users subscribe to the endpoint.

#### Exam Question 257

A company has two applications: a sender application that sends messages with payloads to be processed and a processing application intended to receive messages with payloads. The company wants to implement an AWS service to handle messages between the two applications. The sender application can send about 1,000 messages each hour. The messages may take up to 2 days to be processed. If the messages fail to process, they must be retained so that they do not impact the processing of any remaining messages.

Which solution meets these requirements and is the MOST operationally efficient?

A. Set up an Amazon EC2 instance running a Redis database. Configure both applications to use the instance. Store, process, and delete the messages, respectively.  
B. Use an Amazon Kinesis data stream to receive the messages from the sender application. Integrate the processing application with the Kinesis Client Library (KCL).  
C. Integrate the sender and processor applications with an Amazon Simple Queue Service (Amazon SQS) queue. Configure a dead-letter queue to collect the messages that failed to process.  
D. Subscribe the processing application to an Amazon Simple Notification Service (Amazon SNS) topic to receive notifications to process. Integrate the sender application to write to the SNS topic.

**Correct Answer:**  
C. Integrate the sender and processor applications with an Amazon Simple Queue Service (Amazon SQS) queue. Configure a dead-letter queue to collect the messages that failed to process.

#### Exam Question 258

A company wants to host a scalable web application on AWS. The application will be accessed by users from different geographic regions of the world. Application users will be able to download and upload unique data up to gigabytes in size. The development team wants a cost-effective solution to minimize upload and download latency and maximize performance.

What should a solutions architect do to accomplish this?

A. Use Amazon S3 with Transfer Acceleration to host the application.  
B. Use Amazon S3 with CacheControl headers to host the application.  
C. Use Amazon EC2 with Auto Scaling and Amazon CloudFront to host the application.  
D. Use Amazon EC2 with Auto Scaling and Amazon ElastiCache to host the application.

**Correct Answer:**  
A. Use Amazon S3 with Transfer Acceleration to host the application.

**Answer Description:**  
The maximum size of a single file that can be delivered through Amazon CloudFront is 20 GB. This limit applies to all Amazon CloudFront distributions.

#### Exam Question 259

A solutions architect is designing a new service behind Amazon API Gateway. The request patterns for the service will be unpredictable and can change suddenly from 0 requests to over 500 per second. The total size of the data that needs to be persisted in a backend database is currently less than 1 GB with unpredictable future growth. Data can be queried using simple key-value requests.

Which combination of AWS services would meet these requirements? (Choose two.)

A. AWS Fargate  
B. AWS Lambda  
C. Amazon DynamoDB  
D. Amazon EC2 Auto Scaling  
E. MySQL-compatible Amazon Aurora

**Correct Answer:**  
B. AWS Lambda  
C. Amazon DynamoDB

**Answer Description:**  
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.

INCORRECT: “AWS Fargate” is incorrect as containers run constantly and therefore incur costs even when no requests are being made.

INCORRECT: “Amazon EC2 Auto Scaling” is incorrect as this uses EC2 instances which will incur costs even when no requests are being made.

INCORRECT: “Amazon RDS” is incorrect as this is a relational database not a No-SQL database. It is therefore not suitable for key-value data storage requirements.

**References:**

* [AWS Lambda Features](https://aws.amazon.com/lambda/features/)
* [Amazon DynamoDB](https://aws.amazon.com/dynamodb/)

#### Exam Question 260

A company’s website runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The website has a mix of dynamic and static content. Users around the globe are reporting that the website is slow.

Which set of actions will improve website performance for users worldwide?

A. Create an Amazon CloudFront distribution and configure the ALB as an origin. Then update the Amazon Route 53 record to point to the CloudFront distribution.  
B. Create a latency-based Amazon Route 53 record for the ALB. Then launch new EC2 instances with larger instance sizes and register the instances with the ALB.  
C. Launch new EC2 instances hosting the same web application in different Regions closer to the users. Then register instances with the same ALB using cross-region VPC peering.  
D. Host the website in an Amazon S3 bucket in the Regions closest to the users and delete the ALB and EC2 instances. Then update an Amazon Route 53 record to point to the S3 buckets.

**Correct Answer:**  
A. Create an Amazon CloudFront distribution and configure the ALB as an origin. Then update the Amazon Route 53 record to point to the CloudFront distribution.

**Answer Description:**  
What Is Amazon CloudFront?

Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files, to your users. CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you’re serving with CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance.

Routing Traffic to an Amazon CloudFront web distribution by using your domain name.

If you want to speed up delivery of your web content, you can use Amazon CloudFront, the AWS content delivery network (CDN). CloudFront can deliver your entire website – including dynamic, static, streaming, and interactive content – by using a global network of edge locations. Requests for your content are automatically routed to the edge location that gives your users the lowest latency.

To use CloudFront to distribute your content, you create a web distribution and specify settings such as the Amazon S3 bucket or HTTP server that you want CloudFront to get your content from, whether you want only selected users to have access to your content, and whether you want to require users to use HTTPS.

When you create a web distribution, CloudFront assigns a domain name to the distribution, such asd111111abcdef8.cloudfront.net. You can use this domain name in the URLs for your content, for example:

http://d111111abcdef8.cloudfront.net/logo.jpg

Alternatively, you might prefer to use your own domain name in URLs, for example:

http://example.com/logo.jpg

If you want to use your own domain name, use Amazon Route 53 to create an alias record that points to your CloudFront distribution. An alias record is a Route 53 extension to DNS. It’s similar to a CNAME record, but you can create an alias record both for the root domain, such as example.com, and for subdomains, such aswww.example.com. (You can create CNAME records only for subdomains.) When Route 53 receives a DNS query that matches the name and type of an alias record, Route 53 responds with the domain name that is associated with your distribution.

Amazon CloudFront is a content delivery network (CDN) that improves website performance by caching content at edge locations around the world. It can serve both dynamic and static content.

This is the best solution for improving the performance of the website.

CORRECT: “Create an Amazon CloudFront distribution and configure the ALB as an origin. Then update the Amazon Route 53 record to point to the CloudFront distribution” is the correct answer. INCORRECT: “Create a latency-based Amazon Route 53 record for the ALB. Then launch new EC2 instances with larger instance sizes and register the instances with the ALB” is incorrect.

Latency routing routes based on the latency between the client and AWS. There is no mention in the answer about creating the new instances in another region therefore the only advantage is in using larger instance sizes. For a dynamic site this adds complexity in keeping the instances in sync.

INCORRECT: “Launch new EC2 instances hosting the same web application in different Regions closer to the users. Use an AWS Transit Gateway to connect customers to the closest region” is incorrect as Transit Gateway is a service for connecting on-premises networks and VPCs to a single gateway.

INCORRECT: “Migrate the website to an Amazon S3 bucket in the Regions closest to the users. Then create an Amazon Route 53 geolocation record to point to the S3 buckets” is incorrect as with S3 you can only host static websites, not dynamic websites.

**References:**

* [Amazon CloudFront Dynamic Content Delivery](https://aws.amazon.com/cloudfront/dynamic-content/)

#### Exam Question 261

A company is hosting a website behind multiple Application Load Balancers. The company has different distribution rights for its content around the world. A solutions architect needs to ensure that users are served the correct content without violating distribution rights.

Which configuration should the solutions architect choose to meet these requirements?

A. Configure Amazon CloudFront with AWS WAF.  
B. Configure Application Load Balancers with AWS WAF.  
C. Configure Amazon Route 53 with a geolocation policy.  
D. Configure Amazon Route 53 with a geoproximity routing policy.

**Correct Answer:**  
C. Configure Amazon Route 53 with a geolocation policy.

**Answer Description:**  
Geolocation routing policy C Use when you want to route traffic based on the location of your users.

**References:**

* Amazon Route 53 > Developer Guide > [Choosing a routing policy](https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html)

#### Exam Question 262

A security team to limit access to specific services or actions in all of the team’s AWS accounts. All accounts belong to a large organization in AWS Organizations. The solution must be scalable and there must be a single point where permissions can be maintained.

What should a solutions architect do to accomplish this?

A. Create an ACL to provide access to the services or actions.  
B. Create a security group to allow accounts and attach it to user groups.  
C. Create cross-account roles in each account to deny access to the services or actions.  
D. Create a service control policy in the root organizational unit to deny access to the services or actions.

**Correct Answer:**  
D. Create a service control policy in the root organizational unit to deny access to the services or actions.

**Answer Description:**  
Service Control Policy concepts  
SCPs offer central access controls for all IAM entities in your accounts. You can use them to enforce the permissions you want everyone in your business to follow. Using SCPs, you can give your developers more freedom to manage their own permissions because you know they can only operate within the boundaries you define.

You create and apply SCPs through AWS Organizations. When you create an organization, AWS Organizations automatically creates a root, which forms the parent container for all the accounts in your organization. Inside the root, you can group accounts in your organization into organizational units (OUs) to simplify management of these accounts. You can create multiple OUs within a single organization, and you can create OUs within other OUs to form a hierarchical structure. You can attach SCPs to the organization root, OUs, and individual accounts. SCPs attached to the root and OUs apply to all OUs and accounts inside of them.

SCPs use the AWS Identity and Access Management (IAM) policy language; however, they do not grant permissions. SCPs enable you set permission guardrails by defining the maximum available permissions for IAM entities in an account. If a SCP denies an action for an account, none of the entities in the account can take that action, even if their IAM permissions allow them to do so. The guardrails set in SCPs apply to all IAM entities in the account, which include all users, roles, and the account root user.

Service control policies (SCPs) offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization’s access control guidelines.

SCPs alone are not sufficient for allowing access in the accounts in your organization. Attaching an SCP to an AWS Organizations entity (root, OU, or account) defines a guardrail for what actions the principals can perform. You still need to attach identity-based or resource-based policies to principals or resources in your organization’s accounts to actually grant permissions to them.

CORRECT: “Create a service control policy in the root organizational unit to deny access to the services or actions” is the correct answer.

INCORRECT: “Create an ACL to provide access to the services or actions” is incorrect as access control lists are not used for permissions associated with IAM. Permissions policies are used with IAM.

INCORRECT: “Create a security group to allow accounts and attach it to user groups” is incorrect as security groups are instance level firewalls. They do not limit service actions.

INCORRECT: “Create cross-account roles in each account to deny access to the services or actions” is incorrect as this is a complex solution and does not provide centralized control.

**References:**

* AWS Organizations > User Guide > [Service control policies (SCPs)](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html)

#### Exam Question 263

A solutions architect needs to design a managed storage solution for a company’s application that includes high-performance machine learning. This application runs on AWS Fargate, and the connected storage needs to have concurrent access to files and deliver high performance.

Which storage option should the solutions architect recommend?

A. Create an Amazon S3 bucket for the application and establish an IAM role for Fargate to communicate with Amazon S3.  
B. Create an Amazon FSx for Lustre file share and establish an IAM role that allows Fargate to communicate with FSx for Lustre.  
C. Create an Amazon Elastic File System (Amazon EFS) file share and establish an IAM role that allows Fargate to communicate with Amazon EFS.  
D. Create an Amazon Elastic Block Store (Amazon EBS) volume for the application and establish an IAM role that allows Fargate to communicate with Amazon EBS.

**Correct Answer:**  
B. Create an Amazon FSx for Lustre file share and establish an IAM role that allows Fargate to communicate with FSx for Lustre.

**Answer Description:**  
Keyword: Concurrent Access to files + Deliver High Performance  
Amazon FSx: A high-performance file system optimized for fast processing of workloads. Lustre is a popular open-source parallel file system. Also supports concurrent access to the same file or directory from thousands of compute instances.

Amazon IAM with FSx: Amazon FSx is integrated with AWS Identity and Access Management (IAM). This integration means that you can control the actions your AWS IAM users and groups can take to manage your file systems (such as creating and deleting file systems). You can also tag your Amazon FSx resources and control the actions that your IAM users and groups can take based on those.

Fargate Launch Type – So, Answer C & D Ruled-out as per Neal David. Fargate automatically provisions resources Fargate provisions and manages compute Charged for running tasks. No EFS and EBS integration Fargate handles cluster optimization.

Limited control, infrastructure is automated

**References:**

* [Amazon Elastic File System](https://aws.amazon.com/efs/)

#### Exam Question 264

A Solutions Architect must design a web application that will be hosted on AWS, allowing users to purchase access to premium, shared content that is stored in an S3 bucket. Upon payment, content will be available for download for 14 days before the user is denied access.

Which of the following would be the LEAST complicated implementation?

A. Use an Amazon CloudFront distribution with an origin access identity (OAI). Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design a Lambda function to remove data that is older than 14 days.  
B. Use an S3 bucket and provide direct access to the file. Design the application to track purchases in a DynamoDB table. Configure a Lambda function to remove data that is older than 14 days based on a query to Amazon DynamoDB.  
C. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 14 days for the URL.  
D. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 60 minutes for the URL and recreate the URL as necessary.

**Correct Answer:**  
C. Use an Amazon CloudFront distribution with an OAI. Configure the distribution with an Amazon S3 origin to provide access to the file through signed URLs. Design the application to set an expiration of 14 days for the URL.

#### Exam Question 265

A company is processing data on a daily basis. The results of the operations are stored in an Amazon S3 bucket, analyzed daily for one week, and then must remain immediately accessible for occasional analysis.

What is the MOST cost-effective storage solution alternative to the current configuration?

A. Configure a lifecycle policy to delete the objects after 30 days.  
B. Configure a lifecycle policy to transition the objects to Amazon S3 Glacier after 30 days.  
C. Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.  
D. Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.

**Correct Answer:**  
D. Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.

#### Exam Question 266

A company plans to store sensitive user data on Amazon S3. Internal security compliance requirement mandate encryption of data before sending it to Amazon S3.

What should a solutions architect recommend to satisfy these requirements?

A. Server-side encryption with customer-provided encryption keys  
B. Client-side encryption with Amazon S3 managed encryption keys  
C. Server-side encryption with keys stored in AWS Key Management Service (AWS KMS)  
D. Client-side encryption with a master key stored in AWS Key Management Service (AWS KMS)

**Correct Answer:**  
D. Client-side encryption with a master key stored in AWS Key Management Service (AWS KMS)

**References:**

* Amazon Simple Storage Service > User Guide > [Protecting data using client-side encryption](https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingClientSideEncryption.html)

#### Exam Question 267

A company has several business systems that require access to data stored in a file share. The business systems will access the file share using the Server Message Block (SMB) protocol. The file share solution should be accessible from both of the company’s legacy on-premises environments and with AWS.

Which services meet the business requirements? (Choose two.)

A. Amazon EBS  
B. Amazon EFS  
C. Amazon FSx for Windows  
D. Amazon S3  
E. AWS Storage Gateway file gateway

**Correct Answer:**  
C. Amazon FSx for Windows  
E. AWS Storage Gateway file gateway

#### Exam Question 268

A company has migrated an on-premises Oracle database to an Amazon RDS for Oracle Multi-AZ DB instance in the us-east-l Region. A solutions architect is designing a disaster recovery strategy to have the database provisioned in the us-west-2 Region in case the database becomes unavailable in the us-east-1 Region. The design must ensure the database is provisioned in the us-west-2 Region in a maximum of 2 hours, with a data loss window of no more than 3 hours.

How can these requirements be met?

A. Edit the DB instance and create a read replica in us-west-2. Promote the read replica to master in us-west-2 in case the disaster recovery environment needs to be activated.  
B. Select the multi-Region option to provision a standby instance in us-west-2. The standby instance will be automatically promoted to master in us-west-2 in case the disaster recovery environment needs to be created.  
C. Take automated snapshots of the database instance and copy them to us-west-2 every 3 hours. Restore the latest snapshot to provision another database instance in us-west-2 in case the disaster recovery environment needs to be activated.  
D. Create a multimaster read/write instances across multiple AWS Regions. Select VPCs in us-east-1 and us-west-2 to make that deployment. Keep the master read/write instance in us-west-2 available to avoid having to activate a disaster recovery environment.

**Correct Answer:**  
B. Select the multi-Region option to provision a standby instance in us-west-2. The standby instance will be automatically promoted to master in us-west-2 in case the disaster recovery environment needs to be created.

#### Exam Question 269

A development team needs to host a website that will be accessed by other teams. The website contents consist of HTML, CSS, client-side JavaScript, and images.

Which method is the MOST cost-effective for hosting the website?

A. Containerize the website and host it in AWS Fargate.  
B. Create an Amazon S3 bucket and host the website there.  
C. Deploy a web server on an Amazon EC2 instance to host the website.  
D. Configure an Application Load Balancer with an AWS Lambda target that uses the Express is framework.

**Correct Answer:**  
B. Create an Amazon S3 bucket and host the website there.

#### Exam Question 270

A solutions architect must design a solution that uses Amazon CloudFront with an Amazon S3 origin to store a static website. The company’s security policy requires that all website traffic be inspected by AWS WAF.

How should the solutions architect comply with these requirements?

A. Configure an S3 bucket policy to accept requests coming from the AWS WAF Amazon Resource Name (ARN) only.  
B. Configure Amazon CloudFront to forward all incoming requests to AWS WAF before requesting content from the S3 origin.  
C. Configure a security group that allows Amazon CloudFront IP addresses to access Amazon S3 only. Associate AWS WAF to CloudFront.  
D. Configure Amazon CloudFront and Amazon S3 to use an origin access identity (OAI) to restrict access to the S3 bucket. Enable AWS WAF on the distribution.

**Correct Answer:**  
D. Configure Amazon CloudFront and Amazon S3 to use an origin access identity (OAI) to restrict access to the S3 bucket. Enable AWS WAF on the distribution.

**Exam Question 271**

As part of budget planning, management wants a report of AWS billed items listed by user. The data will be used to create department budgets. A solutions architect needs to determine the most efficient way to obtain this report information.

Which solution meets these requirements?

A. Run a query with Amazon Athena to generate the report.  
B. Create a report in Cost Explorer and download the report.  
C. Access the bill details from the billing dashboard and download the bill.  
D. Modify a cost budget in AWS Budgets to alert with Amazon Simple Email Service (Amazon SES).

**Correct Answer:**  
B. Create a report in Cost Explorer and download the report.

**Exam Question 272**

A company needs a secure connection between its on-premises environment and AWS. This connection does not need high bandwidth and will handle a small amount of traffic. The connection should be set up quickly.

What is the MOST cost-effective method to establish this type of connection?

A. Implement a client VPN.  
B. Implement AWS Direct Connect.  
C. Implement a bastion host on Amazon EC2.  
D. Implement an AWS Site-to-Site VPN connection.

**Correct Answer:**  
D. Implement an AWS Site-to-Site VPN connection.

**Exam Question 273**

A company uses a legacy on-premises analytics application that operates on gigabytes of .csv files and represents months of data. The legacy application cannot handle the growing size of .csv files. New .csv files are added daily from various data sources to a central on-premises storage location. The company wants to continue to support the legacy application while users learn AWS analytics services. To achieve this, a solutions architect wants to maintain two synchronized copies of all the .csv files on-premises and in Amazon S3.

Which solution should the solutions architect recommend?

A. Deploy AWS DataSync on-premises. Configure DataSync to continuously replicate the .csv files between the company’s on-premises storage and the company’s S3 bucket.  
B. Deploy an on-premises file gateway. Configure data sources to write the .csv files to the file gateway. Point the legacy analytics application to the file gateway. The file gateway should replicate the .csv files to Amazon S3.  
C. Deploy an on-premises volume gateway. Configure data sources to write the .csv files to the volume gateway. Point the legacy analytics application to the volume gateway. The volume gateway should replicate data to Amazon S3.  
D. Deploy AWS DataSync on-premises. Configure DataSync to continuously replicate the .csv files between on-premises and Amazon Elastic File System (Amazon EFS). Enable replication from Amazon EFS to the company’s S3 bucket.

**Correct Answer:**  
B. Deploy an on-premises file gateway. Configure data sources to write the .csv files to the file gateway. Point the legacy analytics application to the file gateway. The file gateway should replicate the .csv files to Amazon S3.

**Exam Question 274**

A company has media and application files that need to be shared internally. Users currently are authenticated using Active Directory and access files from a Microsoft Windows platform. The chief executive officer wants to keep the same user permissions, but wants the company to improve the process as the company is reaching its storage capacity limit.

What should a solutions architect recommend?

A. Set up a corporate Amazon S3 bucket and move all media and application files.  
B. Configure Amazon FSx for Windows File Server and move all the media and application files.  
C. Configure Amazon Elastic File System (Amazon EFS) and move all media and application files.  
D. Set up Amazon EC2 on Windows, attach multiple Amazon Elastic Block Store (Amazon EBS) volumes, and move all media and application files.

**Correct Answer:**  
B. Configure Amazon FSx for Windows File Server and move all the media and application files.

**Exam Question 275**

A company hosts an application used to upload files to an Amazon S3 bucket. Once uploaded, the files are processed to extract metadata, which takes less than 5 seconds. The volume and frequency of the uploads varies from a few files each hour to hundreds of concurrent uploads. The company has asked a solutions architect to design a cost-effective architecture that will meet these requirements.

What should the solutions architect recommend?

A. Configure AWS CloudTrail trails to log S3 API calls. Use AWS AppSync to process the files.  
B. Configure an object-created event notification within the S3 bucket to invoke an AWS Lambda function to process the files.  
C. Configure Amazon Kinesis Data Streams to process and send data to Amazon S3. Invoke an AWS Lambda function to process the files.  
D. Configure an Amazon Simple Notification Service (Amazon SNS) topic to process the files uploaded to Amazon S3. Invoke an AWS Lambda function to process the files.

**Correct Answer:**  
B. Configure an object-created event notification within the S3 bucket to invoke an AWS Lambda function to process the files.

**Exam Question 276**

A company is deploying a multi-instance application within AWS that requires minimal latency between the instances.

What should a solutions architect recommend?

A. Use an Auto Scaling group with a cluster placement group.  
B. Use an Auto Scaling group with single Availability Zone in the same AWS Region.  
C. Use an Auto Scaling group with multiple Availability Zones in the same AWS Region.  
D. Use a Network Load Balancer with multiple Amazon EC2 Dedicated Hosts as the targets.

**Correct Answer:**  
A. Use an Auto Scaling group with a cluster placement group.

**Exam Question 277**

A company wants to share forensic accounting data that is stored in an Amazon RDS DB instance with an external auditor. The auditor has its own AWS account and requires its own copy of the database.

How should the company securely share the database with the auditor?

A. Create a read replica of the database and configure IAM standard database authentication to grant the auditor access.  
B. Copy a snapshot of the database to Amazon S3 and assign an IAM role to the auditor to grant access to the object in that bucket.  
C. Export the database contents to text files, store the files in Amazon S3, and create a new IAM user for the auditor with access to that bucket.  
D. Make an encrypted snapshot of the database, share the snapshot, and allow access to the AWS Key Management Service (AWS KMS) encryption key.

**Correct Answer:**  
A. Create a read replica of the database and configure IAM standard database authentication to grant the auditor access.

**Exam Question 278**

A solutions architect is designing a multi-region disaster recovery solution for an application that will provide public API access. The application will use Amazon EC2 instances with a user data script to load application code and an Amazon RDS for MySQL database. The Recovery Time Objective (RTO) is 3 hours and the Recovery Point Objective (RPO) is 24 hours.

Which architecture would meet these requirements at the LOWEST cost?

A. Use an Application Load Balancer for Region failover. Deploy new EC2 instances with the user data script. Deploy separate RDS instances in each Region.  
B. Use Amazon Route 53 for Region failover. Deploy new EC2 instances with the user data script. Create a read replica of the RDS instance in a backup Region.  
C. Use Amazon API Gateway for the public APIs and Region failover. Deploy new EC2 instances with the user data script. Create a MySQL read replica of the RDS instance in a backup Region.  
D. Use Amazon Route 53 for Region failover. Deploy new EC2 instances with the user data script for APIs, and create a snapshot of the RDS instance daily for a backup. Replicate the snapshot to a backup Region.

**Correct Answer:**  
D. Use Amazon Route 53 for Region failover. Deploy new EC2 instances with the user data script for APIs, and create a snapshot of the RDS instance daily for a backup. Replicate the snapshot to a backup Region.

**Exam Question 279**

A company is planning to migrate a commercial off-the-shelf application from its on-premises data center to AWS. The software has a software licensing model using sockets and cores with predictable capacity and uptime requirements. The company wants to use its existing licenses, which were purchased earlier this year.

Which Amazon EC2 pricing option is the MOST cost-effective?

A. Dedicated Reserved Hosts  
B. Dedicated On-Demand Hosts  
C. Dedicated Reserved Instances  
D. Dedicated On-Demand Instances

**Correct Answer:**  
C. Dedicated Reserved Instances

**Exam Question 280**

A company has an on-premises MySQL database used by the global sales team with infrequent access patterns. The sales team requires the database to have minimal downtime. A database administrator wants to migrate this database to AWS without selecting a particular instance type in anticipation of more users in the future.

Which service should a solutions architect recommend?

A. Amazon Aurora MySQL  
B. Amazon Aurora Serverless for MySQL  
C. Amazon Redshift Spectrum  
D. Amazon RDS for MySQL

**Correct Answer:**  
B. Amazon Aurora Serverless for MySQL

**Answer Description:**  
A database administrator wants to migrate this database to AWS without selecting a particular instance type in anticipation of more users in the future” Serverless sounds right, and it’s compatible with MySQL and PostgreSQL.

#### Exam Question 281

A company has an eCommerce application that stores data in an on-premises SQL database. The company has decided to migrate this database to AWS. However, as part of the migration, the company wants to find a way to attain sub-millisecond responses to common read requests.

A solutions architect knows that the increase in speed is paramount and that a small percentage of stale data returned in the database reads is acceptable.

What should the solutions architect recommend?

A. Build Amazon RDS read replicas.  
B. Build the database as a larger instance type.  
C. Build a database cache using Amazon ElastiCache.  
D. Build a database cache using Amazon Elasticsearch Service (Amazon ES).

**Correct Answer:**  
C. Build a database cache using Amazon ElastiCache.

**Answer Description:**  
To attain sub-millisecond responses to common read requests. [REDIS (REmote DIctionary Server)](https://aws.amazon.com/redis/) delivers sub-millisecond response times enabling millions of requests per second for real-time applications.

#### Exam Question 282

A company has an application that ingests incoming messages. These messages are then quickly consumed by dozens of other applications and microservices. The number of messages varies drastically and sometimes spikes as high as 100,000 each second. The company wants to decouple the solution and increase scalability.

Which solution meets these requirements?

A. Persist the messages to Amazon Kinesis Data Analytics. All the applications will read and process the messages.  
B. Deploy the application on Amazon EC2 instances in an Auto Scaling group, which scales the number of EC2 instances based on CPU metrics.  
C. Write the messages to Amazon Kinesis Data Streams with a single shard. All applications will read from the stream and process the messages.  
D. Publish the messages to an Amazon Simple Notification Service (Amazon SNS) topic with one or more Amazon Simple Queue Service (Amazon SQS) subscriptions. All applications then process the messages from the queues.

**Correct Answer:**  
D. Publish the messages to an Amazon Simple Notification Service (Amazon SNS) topic with one or more Amazon Simple Queue Service (Amazon SQS) subscriptions. All applications then process the messages from the queues.

**Answer Description:**  
Q: How large can Amazon SQS message queues be?  
A single Amazon SQS message queue can contain an unlimited number of messages. However, there is a 120,000 quota for the number of inflight messages for a standard queue and 20,000 for a FIFO queue. Messages are inflight after they have been received from the queue by a consuming component, but have not yet been deleted from the queue.

**References:**

* [Amazon SQS FAQs](https://aws.amazon.com/sqs/faqs/)

#### Exam Question 283

A company is backing up on-premises databases to local file server shares using the SMB protocol. The company requires immediate access to 1 week of backup files to meet recovery objectives. Recovery after a week is less likely to occur, and the company can tolerate a delay in accessing those older backup files.

What should a solutions architect do to meet these requirements with the LEAST operational effort?

A. Deploy Amazon FSx for Windows File Server to create a file system with exposed file shares with sufficient storage to hold all the desired backups.  
B. Deploy an AWS Storage Gateway file gateway with sufficient storage to hold 1 week of backups. Point the backups to SMB shares from the file gateway.  
C. Deploy Amazon Elastic File System (Amazon EFS) to create a file system with exposed NFS shares with sufficient storage to hold all the desired backups.  
D. Continue to back up to the existing file shares. Deploy AWS Database Migration Service (AWS DMS) and define a copy task to copy backup files older than 1 week to Amazon S3, and delete the backup files from the local file store.

**Correct Answer:**  
A. Deploy Amazon FSx for Windows File Server to create a file system with exposed file shares with sufficient storage to hold all the desired backups.

**References:**

* AWS Storage Blog > [Back up your on-premises applications to the cloud using AWS Storage Gateway](https://aws.amazon.com/blogs/storage/back-up-your-on-premises-applications-to-the-cloud-using-aws-storage-gateway/)

#### Exam Question 284

A company has developed a microservices application. It uses a client-facing API with Amazon API Gateway and multiple internal services hosted on Amazon EC2 instances to process user requests. The API is designed to support unpredictable surges in traffic, but internal services may become overwhelmed and unresponsive for a period of time during surges. A solutions architect needs to design a more reliable solution that reduces errors when internal services become unresponsive or unavailable.

Which solution meets these requirements?

A. Use AWS Auto Scaling to scale up internal services when there is a surge in traffic.  
B. Use different Availability Zones to host internal services. Send a notification to a system administrator when an internal service becomes unresponsive.  
C. Use an Elastic Load Balancer to distribute the traffic between internal services. Configure Amazon CloudWatch metrics to monitor traffic to internal services.  
D. Use Amazon Simple Queue Service (Amazon SQS) to store user requests as they arrive. Change the internal services to retrieve the requests from the queue for processing.

**Correct Answer:**  
D. Use Amazon Simple Queue Service (Amazon SQS) to store user requests as they arrive. Change the internal services to retrieve the requests from the queue for processing.

#### Exam Question 285

A company is hosting 60 TB of production-level data in an Amazon S3 bucket. A solution architect needs to bring that data on-premises for quarterly audit requirements. This export of data must be encrypted while in transit. The company has low network bandwidth in place between AWS and its on-premises data center.

What should the solutions architect do to meet these requirements?

A. Deploy AWS Migration Hub with 90-day replication windows for data transfer.  
B. Deploy an AWS Storage Gateway volume gateway on AWS. Enable a 90-day replication window to transfer the data.  
C. Deploy Amazon Elastic File System (Amazon EFS), with lifecycle policies enabled, on AWS. Use it to transfer the data.  
D. Deploy an AWS Snowball device in the on-premises data center after completing an export job request in the AWS Snowball console.

**Correct Answer:**  
D. Deploy an AWS Snowball device in the on-premises data center after completing an export job request in the AWS Snowball console.

**Answer Description:**  
AWS Snowball with the Snowball device has the following features: 80 TB and 50 TB models are available in US Regions; 50 TB model available in all other AWS Regions.

**References:**

* AWS Snowball > User Guide > [What Is an AWS Snowball Device?](https://docs.aws.amazon.com/snowball/latest/ug/whatissnowball.html)

#### Exam Question 286

A company uses Amazon S3 to store its confidential audit documents. The S3 bucket uses bucket policies to restrict access to audit team IAM user credentials according to the principle of least privilege. Company managers are worried about accidental deletion of documents in the S3 bucket and want a more secure solution.

What should a solutions architect do to secure the audit documents?

A. Enable the versioning and MFA Delete features on the S3 bucket.  
B. Enable multi-factor authentication (MFA) on the IAM user credentials for each audit team IAM user account.  
C. Add an S3 Lifecycle policy to the audit team’s IAM user accounts to deny the s3:DeleteObject action during audit dates.  
D. Use AWS Key Management Service (AWS KMS) to encrypt the S3 bucket and restrict audit team IAM user accounts from accessing the KMS key.

**Correct Answer:**  
A. Enable the versioning and MFA Delete features on the S3 bucket.

**References:**

* Amazon Simple Storage Service > User Guide > [Security Best Practices for Amazon S3](https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html)

#### Exam Question 287

A company is launching a new application deployed on an Amazon Elastic Container Service (Amazon ECS) cluster and is using the Fargate launch type for ECS tasks. The company is monitoring CPU and memory usage because it is expecting high traffic to the application upon its launch. However, the company wants to reduce costs when utilization decreases.

What should a solutions architect recommend?

A. Use Amazon EC2 Auto Scaling to scale at certain periods based on previous traffic patterns.  
B. Use an AWS Lambda function to scale Amazon ECS based on metric breaches that trigger an Amazon CloudWatch alarm.  
C. Use Amazon EC2 Auto Scaling with simple scaling policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm.  
D. Use AWS Application Auto Scaling with target tracking policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm.

**Correct Answer:**  
A. Use Amazon EC2 Auto Scaling to scale at certain periods based on previous traffic patterns.

#### Exam Question 288

A user wants to list the IAM role that is attached to their Amazon EC2 instance. The user has login access to the EC2 instance but does not have IAM permissions.

What should a solutions architect do to retrieve this information?

A. Run the following EC2 command:curl http://169.254.169.254/latest/meta-data/iam/info  
B. Run the following EC2 command:curl http://169.254.169.254/latest/user-data/iam/info  
C. Run the following EC2 command:http://169.254.169.254/latest/dynamic/instance-identity/  
D. Run the following AWS CLI command:aws iam get-instance-profile --instance-profile-name ExampleInstanceProfile

**Correct Answer:**  
A. Run the following EC2 command:curl http://169.254.169.254/latest/meta-data/iam/info

**References:**

* Amazon Elastic Compute Cloud > User Guide for Linux Instances > [IAM roles for Amazon EC2](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html)

#### Exam Question 289

A company has an application that is hosted on Amazon EC2 instances in two private subnets. A solutions architect must make the application available on the public internet with the least amount of administrative effort.

What should the solutions architect recommend?

A. Create a load balancer and associate two public subnets from the same Availability Zones as the private instances. Add the private instances to the load balancer.  
B. Create a load balancer and associate two private subnets from the same Availability Zones as the private instances. Add the private instances to the load balancer.  
C. Create an Amazon Machine Image (AMI) of the instances in the private subnet and restore in the public subnet. Create a load balancer and associate two public subnets from the same Availability Zones as the public instances.  
D. Create an Amazon Machine Image (AMI) of the instances in the private subnet and restore in the public subnet. Create a load balancer and associate two private subnets from the same Availability Zones as the public instances.

**Correct Answer:**  
C. Create an Amazon Machine Image (AMI) of the instances in the private subnet and restore in the public subnet. Create a load balancer and associate two public subnets from the same Availability Zones as the public instances.

#### Exam Question 290

A company is moving its on-premises Oracle database to Amazon Aurora PostgreSQL. The database has several applications that write to the same tables. The applications need to be migrated one by one with a month in between each migration Management has expressed concerns that the database has a high number of reads and writes. The data must be kept in sync across both databases throughout tie migration.

What should a solutions architect recommend?

A. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a change data capture (CDC) replication task and a table mapping to select all cables.  
B. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.  
C. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a memory optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.  
D. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a compute optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select the largest tables.

**Correct Answer:**  
C. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a memory optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.

**Answer Description:**  
As you can see, we have three important memory buffers in this architecture for CDC in AWS DMS. If any of these buffers experience memory pressure, the migration can have performance issues that can potentially cause failures.

**References:**

* AWS Database Migration Service > User Guide > [Choosing the right AWS DMS replication instance for your migration](https://docs.aws.amazon.com/dms/latest/userguide/CHAP_ReplicationInstance.Types.html)

**Exam Question 291**

A company hosts its application using Amazon Elastic Container Service (Amazon ECS) and wants to ensure high availability. The company wants to be able to deploy updates to its application even if nodes in one Availability Zone are not accessible.

The expected request volume for the application is 100 requests per second, and each container task is able to serve at least 60 requests per second. The company set up Amazon ECS with a rolling update deployment type with the minimum healthy percent parameter set to 50% and the maximum percent set to 100%.

Which configuration of tasks and Availability Zones meets these requirements?

A. Deploy the application across two Availability Zones, with one task in each Availability Zone.  
B. Deploy the application across two Availability Zones, with two tasks in each Availability Zone.  
C. Deploy the application across three Availability Zones, with one task in each Availability Zone.  
D. Deploy the application across three Availability Zones, with two tasks in each Availability Zone.

**Correct Answer:**  
A. Deploy the application across two Availability Zones, with one task in each Availability Zone.

**Exam Question 292**

A solutions architect wants all new users to have specific complexity requirements and mandatory rotation periods for IAM user passwords. What should the solutions architect do to accomplish this?

A. Set an overall password policy for the entire AWS account  
B. Set a password policy for each IAM user in the AWS account.  
C. Use third-party vendor software to set password requirements.  
D. Attach an Amazon CloudWatch rule to the Create\_newuser event to set the password with the appropriate requirements.

**Correct Answer:**  
A. Set an overall password policy for the entire AWS account

**Exam Question 293**

A company wants to improve the availability and performance of its hybrid application. The application consists of a stateful TCP-based workload hosted on Amazon EC2 instances in different AWS Regions and a stateless UOP-based workload hosted on-premises.

Which combination of actions should a solutions architect take to improve availability and performance? (Choose two.)

A. Create an accelerator using AWS Global Accelerator. Add the load balancers as endpoints.  
B. Create an Amazon CloudFront distribution with an origin that uses Amazon Route 53 latency-based routing to route requests to the load balancers.  
C. Configure two Application Load Balancers in each Region. The first will route to the EC2 endpoints and the second will route to the on-premises endpoints.  
D. Configure a Network Load Balancer in each Region to address the EC2 endpoints. Configure a Network Load Balancer in each Region that routes to the on-premises endpoints.  
E. Configure a Network Load Balancer in each Region to address the EC2 endpoints. Configure an Application Load Balancer in each Region that routes to the on-premises endpoints.

**Correct Answer:**  
A. Create an accelerator using AWS Global Accelerator. Add the load balancers as endpoints.  
D. Configure a Network Load Balancer in each Region to address the EC2 endpoints. Configure a Network Load Balancer in each Region that routes to the on-premises endpoints.

**Exam Question 294**

A solutions architect is designing the architecture of a new application being deployed to the AWS Cloud.

The application will run on Amazon EC2 On-Demand Instances and will automatically scale across multiple Availability Zones. The EC2 instances will scale up and down frequently throughout the day. An Application Load Balancer (ALB) will handle the load distribution. The architecture needs to support distributed session data management. The company is willing to make changes to code if needed.

What should the solutions architect do to ensure that the architecture supports distributed session data management?

A. Use Amazon ElastiCache to manage and store session data.  
B. Use session affinity (sticky sessions) of the ALB to manage session data.  
C. Use Session Manager from AWS Systems Manager to manage the session.  
D. Use the GetSessionToken API operation in AWS Security Token Service (AWS STS) to manage the session.

**Correct Answer:**  
A. Use Amazon ElastiCache to manage and store session data.

**Exam Question 295**

A company has an eCommerce application running in a single VPC. The application stack has a single web server and an Amazon RDS Multi-AZ DB instance.

The company launches new products twice a month. This increases website traffic by approximately 400% for a minimum of 72 hours. During product launches, users experience slow response times and frequent timeout errors in their browsers.

What should a solutions architect do to mitigate the slow response times and timeout errors while minimizing operational overhead?

A. Increase the instance size of the web server.  
B. Add an Application Load Balancer and an additional web server.  
C. Add Amazon EC2 Auto Scaling and an Application Load Balancer.  
D. Deploy an Amazon ElastiCache cluster to store frequently accessed data.

**Correct Answer:**  
A. Increase the instance size of the web server.

**Exam Question 296**

A solutions architect is designing an architecture to run a third-party database server. The database software is memory intensive and has a CPU-based licensing model where the cost increases with the number of vCPU cores within the operating system. The solutions architect must select an Amazon EC2 instance with sufficient memory to run the database software, but the selected instance has a large number of vCPUs. The solutions architect must ensure that the vCPUs will not be underutilized and must minimize costs.

Which solution meets these requirements?

A. Select and launch a smaller EC2 instance with an appropriate number of vCPUs.  
B. Configure the CPU cores and threads on the selected EC2 instance during instance launch.  
C. Create a new EC2 instance and ensure multithreading is enabled when configuring the instance details.  
D. Create a new Capacity Reservation and select the appropriate instance type. Launch the instance into this new Capacity Reservation.

**Correct Answer:**  
A. Select and launch a smaller EC2 instance with an appropriate number of vCPUs.

**Exam Question 297**

A company receives 10 TB of instrumentation data each day from several machines located at a single factory. The data consists of JSON files stored on a storage area network (SAN) in an on-premises data center located within the factory. The company wants to send this data to Amazon S3 where it can be accessed by several additional systems that provide critical near-real-lime analytics. A secure transfer is important because the data is considered sensitive.

Which solution offers the MOST reliable data transfer?

A. AWS DataSync over public internet  
B. AWS DataSync over AWS Direct Connect  
C. AWS Database Migration Service (AWS DMS) over public internet  
D. AWS Database Migration Service (AWS DMS) over AWS Direct Connect

**Correct Answer:**  
D. AWS Database Migration Service (AWS DMS) over AWS Direct Connect

**Exam Question 298**

A company hosts more than 300 global websites and applications. The company requires a platform to analyze more than 30 TB of clickstream data each day. What should a solutions architect do to transmit and process the clickstream data?

A. Design an AWS Data Pipeline to archive the data to an Amazon S3 bucket and run an Amazon EMR cluster with the data to generate analytics.  
B. Create an Auto Scaling group of Amazon EC2 instances to process the data and send it to an Amazon S3 data lake for Amazon Redshift to use for analysis.  
C. Cache the data to Amazon CloudFront. Store the data in an Amazon S3 bucket. When an object is added to the S3 bucket, run an AWS Lambda function to process the data for analysis.  
D. Collect the data from Amazon Kinesis Data Streams. Use Amazon Kinesis Data firehose to transmit the data to an Amazon S3 data lake. Load the data in Amazon Redshift for analysis.

**Correct Answer:**  
C. Cache the data to Amazon CloudFront. Store the data in an Amazon S3 bucket. When an object is added to the S3 bucket, run an AWS Lambda function to process the data for analysis.

**Exam Question 299**

A company wants to build an online marketplace application on AWS as a set of loosely coupled microservices. For this application, when a customer submits a new order, two microservices should handle the event simultaneously. The Email microservice will send a confirmation email, and the order processing microservice will start the order delivery process. If a customer cancels an order, the OrderCancelation and Email microservices should handle the event simultaneously.

A solutions architect wants to use Amazon Simple Queue Service (Amazon SQS) and Amazon Simple

Notification Service (Amazon SNS) to design the messaging between the microservices.

How should the solutions architect design the solution?

A. Create a single SQS queue and publish order events to it. The Email OrderProcessing and Order Cancellation microservices can then consume messages of the queue.  
B. Create three SNS topics for each microservice. Publish order events to the three topics. Subscribe each of the Email OrderProcessing and Order Cancellation microservices to its own topic.  
C. Create an SNS topic and publish order events to it. Create three SQS queues for the Email OrderProcessing and Order Cancellation microservices. Subscribe all SQS queues to the SNS topic with message filtering.  
D. Create two SQS queues and publish order events to both queues simultaneously. One queue is for the Email and OrderProcessing microservices. The second queue is for the Email and Order Cancellation microservices.

**Correct Answer:**  
D. Create two SQS queues and publish order events to both queues simultaneously. One queue is for the Email and OrderProcessing microservices. The second queue is for the Email and Order Cancellation microservices.

**Exam Question 300**

A company is running a multi-tier eCommerce web application in the AWS Cloud. The application runs on Amazon EC2 Instances with an Amazon RDS MySQL Multi-AZ DB instance. Amazon RDS is configured with the latest generation instance with 2,000 GB of storage in an Amazon EBS General Purpose SSD (gp2) volume. The database performance impacts the application during periods of high demand.

After analyzing the logs in Amazon CloudWatch Logs, a database administrator finds that the application performance always degrades when the number of read and write IOPS is higher than 6.000.

What should a solutions architect do to improve the application performance?

A. Replace the volume with a Magnetic volume.  
B. Increase the number of IOPS on the gp2 volume.  
C. Replace the volume with a Provisioned IOPS (PIOPS) volume.  
D. Replace the 2,000 GB gp2 volume with two 1,000 GBgp2 volumes.

**Correct Answer:**  
C. Replace the volume with a Provisioned IOPS (PIOPS) volume.

**AWS Certified Solutions Architect – Associate SAA-C02 Exam Questions and Answers – Page 4**

The latest AWS Certified Solutions Architect – Associate SAA-C02 certification actual real practice exam question and answer (Q&A) dumps are available free, which are helpful for you to pass the AWS Certified Solutions Architect – Associate SAA-C02 exam and earn AWS Certified Solutions Architect – Associate SAA-C02 certification.

**Exam Question 321**

A company is building its web application using containers on AWS. The company requires three instances of the web application to run at all times. The application must be able to scale to meet increases in demand. Management is extremely sensitive to cost but agrees that the application should be highly available.

What should a solutions architect recommend?

A. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Fargate launch type. Create a task definition for the web application. Create an ECS service with a desired count of three tasks.  
B. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Amazon EC2 launch type with three container instances in one Availability Zone. Create a task definition for the web application. Place one task for each container instance.  
C. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Fargate launch type with one container instance in three different Availability Zones. Create a task definition for the web application. Create an ECS service with a desired count of three tasks.  
D. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Amazon EC2 launch type with one container instance in two different Availability Zones. Create a task definition for the web application. Place two tasks on one container instance and one task on the remaining container instance.

**Correct Answer:**  
D. Create an Amazon Elastic Container Service (Amazon ECS) cluster using the Amazon EC2 launch type with one container instance in two different Availability Zones. Create a task definition for the web application. Place two tasks on one container instance and one task on the remaining container instance.

**Exam Question 322**

A company is launching an eCommerce website on AWS. This website is built with a three-tier architecture that includes a MySQL database in a Multi-AZ deployment of Amazon Aurora MySQL. The website application must be highly available and will initially be launched in an AWS Region with three Availability Zones The application produces a metric that describes the load the application experiences.

Which solution meets these requirements?

A. Configure an Application Load Balancer (ALB) with Amazon EC2 Auto Scaling behind the ALB with scheduled scaling  
B. Configure an Application Load Balancer (ALB) and Amazon EC2 Auto Scaling behind the ALB with a simple scaling policy.  
C. Configure a Network Load Balancer (NLB) and launch a Spot Fleet with Amazon EC2 Auto Scaling behind the NLB.  
D. Configure an Application Load Balancer (ALB) and Amazon EC2 Auto Scaling behind the ALB with a target tracking scaling policy.

**Correct Answer:**  
B. Configure an Application Load Balancer (ALB) and Amazon EC2 Auto Scaling behind the ALB with a simple scaling policy.

**Exam Question 323**

A solutions architect is creating a new Amazon CloudFront distribution for an application. Some of the information submitted by users is sensitive. The application uses HTTPS but needs another layer of security. The sensitive information should be protected throughout the entire application stack, and access to the information should be restricted to certain applications.

Which action should the solutions architect take?

A. Configure a CloudFront signed URL  
B. Configure a CloudFront signed cookie.  
C. Configure a CloudFront field-level encryption profile.  
D. Configure a CloudFront and set the Origin Protocol Policy setting to HTTPS. Only for the Viewer Protocol Pokey.

**Correct Answer:**  
A. Configure a CloudFront signed URL

**Exam Question 324**

A solutions architect is redesigning a monolithic application to be a loosely coupled application composed of two microservices: Microservice A and Microservice B.

Microservice A places messages in a main Amazon Simple Queue Service (Amazon SQS) queue for Microservice B to consume. When Microservice B fails to process a message after four retries, the message needs to be removed from the queue and stored for further investigation.

What should the solutions architect do to meet these requirements?

A. Create an SQS dead-letter queue. Microservice B adds failed messages to that queue after it receives and fails to process the message four times.  
B. Create an SQS dead-letter queue. Configure the main SQS queue to deliver messages to the dead letter queue after the message has been received four times.  
C. Create an SQS queue for failed messages. Microservice A adds failed messages to that queue after Microservice B receives and fails to process the message four times.  
D. Create an SQS queue for failed messages. Configure the SQS queue for failed messages to pull messages from the main SQS queue after the original message has been received four times.

**Correct Answer:**  
B. Create an SQS dead-letter queue. Configure the main SQS queue to deliver messages to the dead letter queue after the message has been received four times.

**Exam Question 325**

A company has multiple applications that use Amazon RDS for MySQL as is database. The company recently discovered that a new custom reporting application has increased the number of Queries on the database. This is slowing down performance.

How should a solutions architect resolve this issue with the LEAST amount of application changes?

A. Add a secondary DB instance using Multi-AZ.  
B. Set up a road replica and Multi-AZ on Amazon RDS.  
C. Set up a standby replica and Multi-AZ on Amazon RDS.  
D. Use caching on Amazon RDS to improve the overall performance.

**Correct Answer:**  
D. Use caching on Amazon RDS to improve the overall performance.

**Exam Question 326**

A company wants to automate the security assessment of its Amazon EC2 instances. The company needs to validate and demonstrate that security and compliance standards are being followed throughout the development process.

What should a solutions architect do to meet these requirements?

A. Use Amazon Macie to automatically discover, classify and protect the EC2 instances.  
B. Use Amazon GuardDuty to publish Amazon Simple Notification Service (Amazon SNS) notifications.  
C. Use Amazon Inspector with Amazon CloudWatch to publish Amazon Simple Notification Service (Amazon SNS) notifications  
D. Use Amazon EventBridge (Amazon CloudWatch Events) to detect and react to changes in the status of AWS Trusted Advisor checks.

**Correct Answer:**  
C. Use Amazon Inspector with Amazon CloudWatch to publish Amazon Simple Notification Service (Amazon SNS) notifications

**Exam Question 327**

A company stores 200 GB of data each month in Amazon S3. The company needs to perform analytics on this data at the end of each month to determine the number of items sold in each sales region for the previous month.

Which analytics strategy is MOST cost-effective for the company to use?

A. Create an Amazon Elasticsearch Service (Amazon ES) cluster. Query the data in Amazon ES. Visualize the data by using Kibana.  
B. Create a table in the AWS Glue Data Catalog. Query the data in Amazon S3 by using Amazon Athena. Visualize the data in Amazon QuickSight.  
C. Create an Amazon EMR cluster. Query the data by using Amazon EMR, and store the results in Amazon S3. Visualize the data in Amazon QuickSight.  
D. Create an Amazon Redshift cluster. Query the data in Amazon Redshift, and upload the results to Amazon S3. Visualize the data in Amazon QuickSight.

**Correct Answer:**  
A. Create an Amazon Elasticsearch Service (Amazon ES) cluster. Query the data in Amazon ES. Visualize the data by using Kibana.

**Exam Question 328**

A company plans to host a survey website on AWS. The company anticipates an unpredictable amount of traffic. This traffic results in asynchronous updates to the database. The company wants to ensure that writes to the database hosted on AWS do not get dropped.

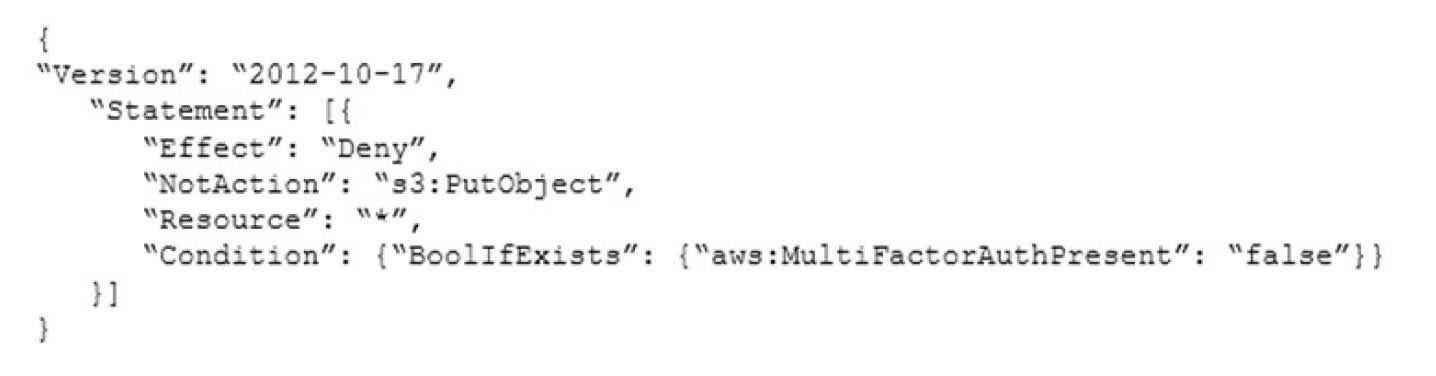
How should the company write its application to handle these database requests?

A. Configure the application to publish to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the database to the SNS topic.  
B. Configure the application to subscribe to an Amazon Simple Notification Service (Amazon SNS) topic. Publish the database updates to the SNS topic.  
C. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues to queue the database connection until the database has resources to write the data.  
D. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues for capturing the writes and draining the queue as each write is made to the database.

**Correct Answer:**  
A. Configure the application to publish to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the database to the SNS topic.

**Exam Question 329**

A solutions architect must analyze and update a company’s existing IAM policies prior to deploying a new workload. The solutions architect created the following policy:



What is the net effect of this policy?

A. Users will be allowed all actions except s3:PutObject if multi-factor authentication (MFA) is enabled.  
B. Users will be allowed all actions except s3:PutObject if multi-factor authentication (MFA) is not enabled.  
C. Users will be denied all actions except s3:PutObject if multi-factor authentication (MFA) is enabled.  
D. Users will be denied all actions except s3:PutObject if multi-factor authentication (MFA) is not enabled.

**Correct Answer:**  
C. Users will be denied all actions except s3:PutObject if multi-factor authentication (MFA) is enabled.

**Exam Question 330**

A company is using Amazon DynamoDB with provisioned throughput for the database tier of its eCommerce website. During flash sales, customers experience periods of time when the database cannot handle the high number of transactions taking place. This causes the company to lose transactions. During normal periods, the database performs appropriately.

Which solution solves the performance problem the company faces?

A. Switch DynamoDB to on-demand mode during flash sales.  
B. Implement DynamoDB Accelerator for fast in memory performance.  
C. Use Amazon Kinesis to queue transactions for processing to DynamoDB.  
D. Use Amazon Simple Queue Service (Amazon SQS) to queue transactions to DynamoDB.

**Correct Answer:**  
A. Switch DynamoDB to on-demand mode during flash sales.

**Exam Question 331**

A company is reviewing a recent migration of a three-tier application to a VPC. The security team discovers that the principle of least privilege is not being applied to Amazon EC2 security group ingress and egress rules between the application tiers.

What should a solutions architect do to correct this issue?

A. Create security group rules using the instance ID as the source or destination.  
B. Create security group rules using the security group ID as the source or destination.  
C. Create security group rules using the VPC CIDR blocks as the source or destination.  
D. Create security group rules using the subnet CIDR blocks as the source or destination.

**Correct Answer:**  
B. Create security group rules using the security group ID as the source or destination.

**Exam Question 332**

A development team is collaborating with another company to create an integrated product. The other company needs to access an Amazon Simple Queue Service (Amazon SQS) queue that is contained in the development team’s account. The other company wants to poll the queue without giving up its own account permissions to do so.

How should a solutions architect provide access to the SQS queue?

A. Create an instance profile that provides the other company access to the SQS queue.  
B. Create an IAM policy that provides the other company access to the SQS queue.  
C. Create an SQS access policy that provides the other company access to the SQS queue.  
D. Create an Amazon Simple Notification Service (Amazon SNS) access policy that provides the other company access to the SQS queue.

**Correct Answer:**  
C. Create an SQS access policy that provides the other company access to the SQS queue.

**Exam Question 333**

A company has applications hosted on Amazon EC2 instances with IPv6 addresses. The applications must initiate communications with other external applications using the internet. However, the company’s security policy states that any external service cannot initiate a connection to the EC2 instances. What should a solutions architect recommend to resolve this issue?

A. Create a NAT gateway and make it the destination of the subnet’s route table.  
B. Create an internet gateway and make it the destination of the subnet’s route table.  
C. Create a virtual private gateway and make it the destination of the subnet’s route table.  
D. Create an egress-only internet gateway and make it the destination of the subnet’s route table.

**Correct Answer:**  
D. Create an egress-only internet gateway and make it the destination of the subnet’s route table.

**Exam Question 334**

A company provides an online service for posting video content and transcoding it for use by any mobile platform. The application architecture uses Amazon Elastic File System (Amazon EFS) Standard to collect and store the videos so that multiple Amazon EC2 Linux instances can access the video content for processing. As the popularity of the service has grown over time, the storage costs have become too expensive.

Which storage solution is MOST cost-effective?

A. Use AWS Storage Gateway for files to store and process the video content.  
B. Use AWS Storage Gateway for volumes to store and process the video content.  
C. Use Amazon EFS for storing the video content. Once processing is complete, transfer the files to Amazon Elastic Block Store (Amazon EBS).  
D. Use Amazon S3 for storing the video content. Move the files temporarily over to an Amazon ElasticBlock Store (Amazon EBS) volume attached to the server for processing.

**Correct Answer:**  
A. Use AWS Storage Gateway for files to store and process the video content.

**Exam Question 335**

A solutions architect is planning the deployment of a new static website. The solution must minimize costs and provide at least 99% availability. Which solution meets these requirements?

A. Deploy the application to an Amazon S3 bucket in one AWS Region that has versioning disabled.  
B. Deploy the application to Amazon EC2 instances that run in two AWS Regions and two Availability Zones.  
C. Deploy the application to an Amazon S3 bucket that has versioning and cross-Region replication enabled.  
D. Deploy the application to an Amazon EC2 instance that runs in one AWS Region and one Availability Zone.

**Correct Answer:**  
A. Deploy the application to an Amazon S3 bucket in one AWS Region that has versioning disabled.

**Exam Question 336**

A recently created startup built a three-tier web application. The front end has static content. The application layer is based on microservices. User data is stored as JSON documents that need to be accessed with low latency. The company expects regular traffic to be low during the first year, with peaks in traffic when it publicizes new features every month. The startup team needs to minimize operational overhead costs.

What should a solutions architect recommend to accomplish this?

A. Use Amazon S3 static website hosting to store and serve the front end. Use AWS Elastic Beanstalk for the application layer. Use Amazon DynamoDB to store user data.  
B. Use Amazon S3 static website hosting to store and serve the front end. Use Amazon Elastic KubernetesService (Amazon EKS) for the application layer. Use Amazon DynamoDB to store user data.  
C. Use Amazon S3 static website hosting to store and serve the front end. Use Amazon API Gateway and AWS Lambda functions for the application layer. Use Amazon DynamoDB to store user data.  
D. Use Amazon S3 static website hosting to store and serve the front end. Use Amazon API Gateway and AWS Lambda functions for the application layer. Use Amazon RDS with read replicas to store user data.

**Correct Answer:**  
C. Use Amazon S3 static website hosting to store and serve the front end. Use Amazon API Gateway and AWS Lambda functions for the application layer. Use Amazon DynamoDB to store user data.

**Exam Question 337**

A company is building a payment application that must be highly available even during regional service disruptions. A solutions architect must design a data storage solution that can be easily replicated and used in other AWS Regions. The application also requires low-latency atomicity, consistency, isolation, and durability (ACID) transactions that need to be immediately available to generate reports The development team also needs to use SQL.

Which data storage solution meets these requirements?

A. Amazon Aurora Global Database  
B. Amazon DynamoDB global tables  
C. Amazon S3 with cross-Region replication and Amazon Athena  
D. MySQL on Amazon EC2 instances with Amazon Elastic Block Store (Amazon EBS) snapshot replication

**Correct Answer:**  
C. Amazon S3 with cross-Region replication and Amazon Athena

**Exam Question 338**

A company stores call recordings on a monthly basis. Statistically, the recorded data may be referenced randomly within a year but accessed rarely after 1 year. Files that are newer than 1 year old must be queried and retrieved as quickly as possible. A delay in retrieving older files is acceptable. A solutions architect needs to store the recorded data at a minimal cost.

Which solution is MOST cost-effective?

A. Store individual files in Amazon S3 Glacier and store search metadata in object tags created in S3 Glacier Query S3 Glacier tags and retrieve the files from S3 Glacier.  
B. Store individual files in Amazon S3. Use lifecycle policies to move the files to Amazon S3 Glacier after1 year. Query and retrieve the files from Amazon S3 or S3 Glacier.  
C. Archive individual files and store search metadata for each archive in Amazon S3. Use lifecycle policies to move the files to Amazon S3 Glacier after 1 year. Query and retrieve the files by searching for metadata from Amazon S3.  
D. Archive individual files in Amazon S3. Use lifecycle policies to move the files to Amazon S3 Glacier after 1 year. Store search metadata in Amazon DynamoDB. Query the files from DynamoDB and retrieve them from Amazon S3 or S3 Glacier.

**Correct Answer:**  
B. Store individual files in Amazon S3. Use lifecycle policies to move the files to Amazon S3 Glacier after1 year. Query and retrieve the files from Amazon S3 or S3 Glacier.

**Exam Question 339**

A company has no existing file share services. A new project requires access to file storage that is mountable as a drive for on-premises desktops. The file server must authenticate users to an Active Directory domain before they are able to access the storage.

Which service will allow Active Directory users to mount storage as a drive on their desktops?

A. Amazon S3 Glacier  
B. AWS DataSync  
C. AWS Snowball Edge  
D. AWS Storage Gateway

**Correct Answer:**  
D. AWS Storage Gateway

**Exam Question 340**

A company has a custom application with embedded credentials that retrieves information from an Amazon RDS MySQL DB instance. Management says the application must be made more secure with the least amount of programming effort.

What should a solutions architect do to meet these requirements?

A. Use AWS Key Management Service (AWS KMS) customer master keys (CMKs) to create keys. Configure the application to load the database credentials from AWS KMS. Enable automatic key rotation.  
B. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Create an AWS Lambda function that rotates the credentials in Secret Manager.  
C. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager.  
D. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Systems Manager Parameter Store. Configure the application to load the database credentials from Parameter Store. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Parameter Store.

**Correct Answer:**  
D. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Systems Manager Parameter Store. Configure the application to load the database credentials from Parameter Store. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Parameter Store.

**Exam Question 341**

A company is running a multi-tier web application on AWS. The application runs its database tier on Amazon Aurora MySQL. The application and database tiers are in the us-east-1 Region. A database administrator who regularly monitors the Aurora DB cluster finds that an intermittent increase in read traffic is creating high CPU utilization on the read replica and causing increased read latency of the application.

What should a solutions architect do to improve read scalability?

A. Reboot the Aurora DB cluster.  
B. Create a cross-Region read replica  
C. Increase the instance class of the read replica.  
D. Configure Aurora Auto Scaling for the read replica.

**Correct Answer:**  
D. Configure Aurora Auto Scaling for the read replica.

**Exam Question 342**

A company is planning to transfer multiple terabytes of data to AWS. The data is collected offline from ships. The company want to run complex transformation before transferring the data.

Which AWS service should a solutions architect recommend for this migration?

A. AWS Snowball  
B. AWS Snowmobile  
C. AWS Snowball Edge Storage Optimize  
D. AWS Snowball Edge Compute Optimize

**Correct Answer:**  
D. AWS Snowball Edge Compute Optimize

**Exam Question 343**

A company is selling up an application to use an Amazon RDS MySQL DB instance. The database must be architected for high availability across Availability Zones and AWS Regions with minimal downtime.

How should a solutions architect meet this requirement?

A. Set up an RDS MySQL Multi-AZ DB instance. Configure an appropriate backup window.  
B. Set up an RDS MySQL Multi-AZ DB instance. Configure a read replica in a different Region.  
C. Set up an RDS MySQL Single-AZ DB instance. Configure a read replica in a different Region.  
D. Set up an RDS MySQL Single-AZ DB instance. Copy automated snapshots to at least one other Region.

**Correct Answer:**  
C. Set up an RDS MySQL Single-AZ DB instance. Configure a read replica in a different Region.

**Exam Question 344**

A company has 700 TB of backup data stored in network attached storage (NAS) in its data center This backup data need to be accessible for infrequent regulatory requests and must be retained 7 years. The company has decided to migrate this backup data from its data center to AWS. The migration must be complete within 1 month. The company has 500 Mbps of dedicated bandwidth on its public internet connection available for data transfer.

What should a solutions architect do to migrate and store the data at the LOWEST cost?

A. Order AWS Snowball devices to transfer the data. Use a lifecycle policy to transition the files to Amazon S3 Glacier Deep Archive.  
B. Deploy a VPN connection between the data center and Amazon VPC. Use the AWS CLI to copy the data from on-premises to Amazon S3 Glacier.  
C. Provision a 500 Mbps AWS Direct Connect connection and transfer the data to Amazon S3. Use a lifecycle policy to transition the files to Amazon S3 Glacier Deep Archive.  
D. Use AWS DataSync to transfer the data and deploy a DataSync agent on-premises. Use the DataSync task to copy files from the on-premises NAS storage to Amazon S3 Glacier.

**Correct Answer:**  
A. Order AWS Snowball devices to transfer the data. Use a lifecycle policy to transition the files to Amazon S3 Glacier Deep Archive.

**Exam Question 345**

A company is preparing to deploy a data lake on AWS. A solutions architect must define the encryption strategy tor data at rest m Amazon S3/ The company’s security policy states:

* Keys must be rotated every 90 days.
* Strict separation of duties between key users and key administrators must be implemented.
* Auditing key usage must be possible.

What should the solutions architect recommend?

A. Server-side encryption with AWS KMS managed keys (SSE-KMS) with customer managed customer master keys (CMKs)  
B. Server-side encryption with AWS KMS managed keys (SSE-KMS) with AWS managed customer master keys (CMKs)  
C. Server-side encryption with Amazon S3 managed keys (SSE-S3) with customer managed customer master keys (CMKs)  
D. Server-side encryption with Amazon S3 managed keys (SSE-S3) with AWS managed customer master keys (CMKs)

**Correct Answer:**  
A. Server-side encryption with AWS KMS managed keys (SSE-KMS) with customer managed customer master keys (CMKs)

**Exam Question 346**

A company has an application that generates a large number of files, each approximately 5 MB in size. The files are stored in Amazon S3. Company policy requires the files to be stored for 4 years before they can be deleted. Immediate accessibility is always required as the files contain critical business data that is not easy to reproduce. The files are frequently accessed in the first 30 days of the object creation but are rarely accessed after the first 30 days.

Which storage solution is MOST cost-effective?

A. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 Glacier 30 days from object creation. Delete the files 4 years after object creation.  
B. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) 30 days from object creation. Delete the files 4 years after object creation.  
C. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 30 days from object creation. Delete the files 4 years after object creation.  
D. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 30 days from object creation. Move the files to S3 Glacier 4 years after object creation.

**Correct Answer:**  
C. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 30 days from object creation. Delete the files 4 years after object creation.

**Exam Question 347**

A company hosts a website on-premises and wants to migrate it to the AWS Cloud. The website exposes a single hostname to the internet but it routes its functions to different on-premises server groups based on the path of the URL. The server groups are scaled independently depending on the needs of the functions they support. The company has an AWS Direct Connect connection configured to its on-premises network.

What should a solutions architect do to provide path-based routing to send the traffic to the correct group of servers?

A. Route all traffic to an internet gateway. Configure pattern matching rules at the internet gateway to route traffic to the group of servers supporting that path.  
B. Route all traffic to a Network Load Balancer (NLB) with target groups for each group of servers. Use pattern matching rules at the NLB to route traffic to the correct target group.  
C. Route all traffic to an Application Load Balancer (ALB). Configure path-based routing at the ALB to route traffic to the correct target group for the servers supporting that path.  
D. Use Amazon Route 53 as the DNS server. Configure Route 53 path-based alias records to route traffic to the correct Elastic Load Balancer for the group of servers supporting that path.

**Correct Answer:**  
B. Route all traffic to a Network Load Balancer (NLB) with target groups for each group of servers. Use pattern matching rules at the NLB to route traffic to the correct target group.

**Exam Question 348**

An application uses an Amazon RDS MySQL DB instance. The RDS database is becoming low on disk space. A solutions architect wants to increase the disk space without downtime. Which solution meets these requirements with the LEAST amount of effort?

A. Enable storage auto scaling in RDS.  
B. Increase the RDS database instance size.  
C. Change the RDS database instance storage type to Provisioned IOPS.  
D. Back up the RDS database, increase the storage capacity, restore the database and stop the previous instance.

**Correct Answer:**  
C. Change the RDS database instance storage type to Provisioned IOPS.

**Exam Question 349**

A company has a website deployed on AWS. The database backend is hosted on Amazon RDS for MySQL with a primary instance and five read replicas to support scaling needs. The read replicas should lag no more than 1 second behind the primary instance to support the user experience.

As traffic on the website continues to increase, the replicas are falling further behind during periods of peak load, resulting in complaints from users when searches yield inconsistent results. A solutions architect needs to reduce the replication lag as much as possible, with minimal changes to the application code or operational requirements.

Which solution meets these requirements?

A. Migrate the database to Amazon Aurora MySQL. Replace the MySQL read replicas with Aurora Replicas and enable Aurora Auto Scaling  
B. Deploy an Amazon ElastiCache for Redis cluster in front of the database. Modify the website to check the cache before querying the database read endpoints.  
C. Migrate the database from Amazon RDS to MySQL running on Amazon EC2 compute instances. Choose very large compute optimized instances for all replica nodes.  
D. Migrate the database to Amazon DynamoDB. Initially provision a large number of read capacity units (RCUs) to support the required throughput with on-demand capacity scaling enabled.

**Correct Answer:**  
B. Deploy an Amazon ElastiCache for Redis cluster in front of the database. Modify the website to check the cache before querying the database read endpoints.

**Exam Question 350**

A company has an API-based inventory reporting application running on Amazon EC2 instances. The application stores information in an Amazon DynamoDB table. The company’s distribution centers have an on-premises shipping application that calls an API to update the inventory before printing shipping labels.

The company has been experiencing application interruptions several times each day, resulting in lost transactions.

What should a solutions architect recommend to improve application resiliency?

A. Modify the shipping application to write to a local database.  
B. Modify the application APIs to run serverless using AWS Lambda  
C. Configure Amazon API Gateway to call the EC2 inventory application APIs.  
D. Modify the application to send inventory updates using Amazon Simple Queue Service (Amazon SQS).

**Correct Answer:**  
A. Modify the shipping application to write to a local database.

**Exam Question 351**

A company has a three-tier environment on AWS that ingests sensor data from its users’ devices. The traffic flows through a Network Load Balancer (NLB) then to Amazon EC2 instances for the web tier, and finally toEC2 instances for the application tier that makes database calls.

What should a solutions architect do to improve the security of data in transit to the web tier?

A. Configure a TLS listener and add the server certificate on the NLB.  
B. Configure AWS Shield Advanced and enable AWS WAF on the NLB.  
C. Change the load balancer to an Application Load Balancer and attach AWS WAF to it.  
D. Encrypt the Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instances using AWS Key Management Service (AWS KMS).

**Correct Answer:**  
A. Configure a TLS listener and add the server certificate on the NLB.

**Answer Description:**  
User – NLB – EC2 (Web) + DB

**Exam Question 352**

An online shopping application accesses an Amazon RDS Multi-AZ DB instance. Database performance is slowing down the application. After upgrading to the next-generation instance type, there was no significant performance improvement.

Analysis shows approximately 700 IOPS are sustained, common queries run for long durations and memory utilization is high.

Which application change should a solutions architect recommend to resolve these issues?

A. Migrate the RDS instance to an Amazon Redshift cluster and enable weekly garbage collection.  
B. Separate the long-running queries into a new Multi-AZ RDS database and modify the application to query whichever database is needed.  
C. Deploy a two-node Amazon ElastiCache cluster and modify the application to query the cluster first and query the database only if needed.  
D. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue for common queries and query it first and query the database only if needed.

**Correct Answer:**  
C. Deploy a two-node Amazon ElastiCache cluster and modify the application to query the cluster first and query the database only if needed.

**Exam Question 353**

A company is preparing to migrate its on-premises application to AWS. The application consists of application servers and a Microsoft SQL Server database The database cannot be migrated to a different engine because SQL Server features are used in the application’s NET code. The company wants to attain the greatest availability possible while minimizing operational and management overhead.

What should a solutions architect do to accomplish this?

A. Install SQL Server on Amazon EC2 in a Multi-AZ deployment.  
B. Migrate the data to Amazon RDS for SQL Server in a Multi-AZ deployment.  
C. Deploy the database on Amazon RDS for SQL Server with Multi-AZ Replicas.  
D. Migrate the data to Amazon RDS for SQL Server in a cross-Region Multi-AZ deployment.

**Correct Answer:**  
B. Migrate the data to Amazon RDS for SQL Server in a Multi-AZ deployment.

**Exam Question 354**

A company has an application running on Amazon EC2 instances in a private subnet. The application needs to store and retrieve data in Amazon S3. To reduce costs, the company wants to configure its AWS resources in a cost-effective manner.

How should the company accomplish this?

A. Deploy a NAT gateway to access the S3 buckets.  
B. Deploy AWS Storage Gateway to access the S3 buckets.  
C. Deploy an S3 gateway endpoint to access the S3 buckets.  
D. Deploy an S3 interface endpoint to access the S3 buckets.

**Correct Answer:**  
B. Deploy AWS Storage Gateway to access the S3 buckets.

**Exam Question 355**

A company runs an application that uses multiple Amazon EC2 instances to gather data from its users. The data is then processed and transferred to Amazon S3 for long-term storage. A review of the application shows that there were long periods of time when the EC2 instances were not being used. A solutions architect needs to design a solution that optimizes utilization and reduces costs.

Which solution meets these requirements?

A. Use Amazon EC2 in an Auto Scaling group with On-Demand instances.  
B. Build the application to use Amazon Lightsail with On-Demand Instances.  
C. Create an Amazon CloudWatch cron job to automatically stop the EC2 instances when there is no activity.  
D. Redesign the application to use an event-driven design with Amazon Simple Queue Service (Amazon SQS) and AWS Lambda.

**Correct Answer:**  
D. Redesign the application to use an event-driven design with Amazon Simple Queue Service (Amazon SQS) and AWS Lambda.

**Exam Question 356**

A company has several Amazon EC2 instances set up in a private subnet for security reasons. These instances host applications that read and write large amounts of data to and from Amazon S3 regularly.

Currently, subnet routing directs all the traffic destined for the internet through a NAT gateway. The company wants to optimize the overall cost without impacting the ability of the application to communicate with Amazon S3 or the outside internet.

What should a solutions architect do to optimize costs?

A. Create an additional NAT gateway. Update the route table to route to the NAT gateway. Update the network ACL to allow S3 traffic.  
B. Create an internet gateway. Update the route table to route traffic to the internet gateway. Update the network ACL to allow S3 traffic.  
C. Create a VPC endpoint for Amazon S3. Attach an endpoint policy to the endpoint. Update the route table to direct traffic to the VPC endpoint.  
D. Create an AWS Lambda function outside of the VPC to handle S3 requests. Attach an IAM policy to the EC2 instances, allowing them to invoke the Lambda function.

**Correct Answer:**  
C. Create a VPC endpoint for Amazon S3. Attach an endpoint policy to the endpoint. Update the route table to direct traffic to the VPC endpoint.

**Exam Question 357**

A company has an application workflow that uses an AWS Lambda function to download and decrypt files from Amazon S3. These files are encrypted using AWS Key Management Service Customer Master Keys (AWS KMS CMKs). A solutions architect needs to design a solution that will ensure the required permissions are set correctly.

Which combination of actions accomplish this? (Choose two.)

A. Attach the kms:decrypt permission to the Lambda function’s resource policy.  
B. Grant the decrypt permission for the Lambda IAM role in the KMS key’s policy.  
C. Grant the decrypt permission for the Lambda resource policy in the KMS key’s policy.  
D. Create a new IAM policy with the kms:decrypt permission and attach the policy to the Lambda function.  
E. Create a new IAM role with the kms:decrypt permission and attach the execution role to the Lambda function.

**Correct Answer:**  
B. Grant the decrypt permission for the Lambda IAM role in the KMS key’s policy.  
E. Create a new IAM role with the kms:decrypt permission and attach the execution role to the Lambda function.

**Exam Question 358**

A solutions architect is developing a multiple-subnet VPC architecture. The solution will consist of six subnets in two Availability Zones. The subnets are defined as public, private and dedicated for databases.

Only the Amazon EC2 instances running in the private subnets should be able to access a database.

Which solution meets these requirements?

A. Create a new route table that excludes the route to the public subnets’ CIDR blocks. Associate the route table to the database subnets.  
B. Create a security group that denies ingress from the security group used by instances in the public subnets. Attach the security group to an Amazon RDS DB instance.  
C. Create a security group that allows ingress from the security group used by instances in the private subnets. Attach the security group to an Amazon RDS DB instance.  
D. Create a new peering connection between the public subnets and the private subnets. Create a different peering connection between the private subnets and the database subnets.

**Correct Answer:**  
C. Create a security group that allows ingress from the security group used by instances in the private subnets. Attach the security group to an Amazon RDS DB instance.

**Exam Question 359**

A disaster response team is using drones to collect images of recent storm damage. The response team’s laptops lack the storage and compute capacity to transfer the images and process the data. While the team has Amazon EC2 instances for processing and Amazon S3 buckets for storage, network connectivity is intermittent and unreliable. The images need to be processed to evaluate the damage.

What should a solutions architect recommend?

A. Use AWS Snowball Edge devices to process and store the images.  
B. Upload the images to Amazon Simple Queue Service (Amazon SQS) during intermittent connectivity to EC2 instances.  
C. Configure Amazon Kinesis Data Firehose to create multiple delivery streams aimed separately at the S3 buckets for storage and the EC2 instances for processing the images.  
D. Use AWS Storage Gateway pre-installed on a hardware appliance to cache the images locally for Amazon S3 to process the images when connectivity becomes available.

**Correct Answer:**  
B. Upload the images to Amazon Simple Queue Service (Amazon SQS) during intermittent connectivity to EC2 instances.

**Exam Question 360**

An engineering team is developing and deploying AWS Lambda functions. The team needs to create roles and manage policies in AWS IAM to configure the permissions of the Lambda functions.

How should the permissions for the team be configured so they also adhere to the concept of least privilege?

A. Create an IAM role with a managed policy attached. Allow the engineering team and the Lambda functions to assume this role.  
B. Create an IAM group for the engineering team with an IAMFullAccess policy attached. Add all the users from the team to this IAM group.  
C. Create an execution role for the Lambda functions. Attach a managed policy that has permission boundaries specific to these Lambda functions.  
D. Create an IAM role with a managed policy attached that has permission boundaries specific to the Lambda functions. Allow the engineering team to assume this role.

**Correct Answer:**  
A. Create an IAM role with a managed policy attached. Allow the engineering team and the Lambda functions to assume this role.

**Exam Question 361**

A company has an Amazon S3 bucket that contains mission-critical data. The company wants to ensure this data is protected 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? (Choose two.)

A. Enable versioning on the S3 bucket.  
B. Enable MFA Delete on the S3 bucket.  
C. Create a bucket policy on the S3 bucket.  
D. Enable default encryption on the S3 bucket.  
E. Create a lifecycle policy for the objects in the S3 bucket.

**Correct Answer:**  
A. Enable versioning on the S3 bucket.  
B. Enable MFA Delete on the S3 bucket.

**Exam Question 362**

A company has an on-premises business application that generates hundreds of files each day. These files are stored on an SMB file share and require a low-latency connection to the application servers. A new company policy states all application-generated files must be copied to AWS. There is already a VPN connection to AWS.

The application development team does not have time to make the necessary code modifications to move the application to AWS.

Which service should a solutions architect recommend to allow the application to copy files to AWS?

A. Amazon Elastic File System (Amazon EFS)  
B. Amazon FSx for Windows File Server  
C. AWS Snowball  
D. AWS Storage Gateway

**Correct Answer:**  
D. AWS Storage Gateway

**Answer Description:**  
The files will be on the storage gateway with low latency and copied to AWS as a second copy. FSx in AWS will not provide low latency for the on-prem apps over a VPN to the FSx file system.

**Exam Question 363**

A solutions architect plans to convert a company’s monolithic web application into a multi-tier application.

The company wants to avoid managing its own infrastructure. The minimum requirements for the web application are high availability, scalability, and regional low latency during peak hours. The solution should also store and retrieve data with millisecond latency using the application’s API.

Which solution meets these requirements?

A. Use AWS Fargate to host the web application with backend Amazon RDS Multi-AZ DB instances.  
B. Use Amazon API Gateway with an edge-optimized API endpoint, AWS Lambda for compute, and Amazon DynamoDB as the data store.  
C. Use an Amazon Route 53 routing policy with geolocation that points to an Amazon S3 bucket with static website hosting and Amazon DynamoDB as the data store.  
D. Use an Amazon CloudFront distribution that points to an Elastic Load Balancer with an Amazon EC2 Auto Scaling group, along with Amazon RDS Multi-AZ DB instances.

**Correct Answer:**  
A. Use AWS Fargate to host the web application with backend Amazon RDS Multi-AZ DB instances.

**Exam Question 364**

A company is planning to migrate a legacy application to AWS. The application currently uses NFS to communicate to an on-premises storage solution to store application data. The application cannot be modified to use any other communication protocols other than NFS for this purpose.

Which storage solution should a solutions architect recommend for use after the migration?

A. AWS DataSync  
B. Amazon Elastic Block Store (Amazon EBS)  
C. Amazon Elastic File System (Amazon EFS)  
D. Amazon EMR File System (Amazon EMRFS)

**Correct Answer:**  
C. Amazon Elastic File System (Amazon EFS)

**Exam Question 365**

A company wants to reduce its Amazon S3 storage costs in its production environment without impacting durability or performance of the stored objects.

What is the FIRST step the company should take to meet these objectives?

A. Enable Amazon Macie on the business-critical S3 buckets to classify the sensitivity of the objects.  
B. Enable S3 analytics to identify S3 buckets that are candidates for transitioning to S3 Standard- Infrequent Access (S3 Standard-IA).  
C. Enable versioning on all business-critical S3 buckets.  
D. Migrate the objects in all S3 buckets to S3 Intelligent-Tiering.

**Correct Answer:**  
D. Migrate the objects in all S3 buckets to S3 Intelligent-Tiering.

**Exam Question 366**

A development team is deploying a new product on AWS and is using AWS Lambda as part of the deployment. The team allocates 512 MB of memory for one of the Lambda functions. With this memory allocation, the function is completed in 2 minutes. The function runs millions of times monthly, and the development team is concerned about cost. The team conducts tests to see how different Lambda memory allocations affect the cost of the function.

Which steps will reduce the Lambda costs for the product? (Choose two.)

A. Increase the memory allocation for this Lambda function to 1,024 MB if this change causes the execution time of each function to be less than 1 minute.  
B. Increase the memory allocation for this Lambda function to 1,024 MB if this change causes the execution time of each function to be less than 90 seconds.  
C. Reduce the memory allocation for this Lambda function to 256 MB if this change causes the execution time of each function to be less than 4 minutes.  
D. Increase the memory allocation for this Lambda function to 2,048 MB if this change causes the execution time of each function to be less than 1 minute.  
E. Reduce the memory allocation for this Lambda function to 256 MB if this change causes the execution time of each function to be less than 5 minutes.

**Correct Answer:**  
A. Increase the memory allocation for this Lambda function to 1,024 MB if this change causes the execution time of each function to be less than 1 minute.  
E. Reduce the memory allocation for this Lambda function to 256 MB if this change causes the execution time of each function to be less than 5 minutes.

**Exam Question 367**

A company has a build server that is in an Auto Scaling group and often has multiple Linux instances running. The build server requires consistent and mountable shared NFS storage for jobs and configurations.

Which storage option should a solutions architect recommend?

A. Amazon S3  
B. Amazon FSx  
C. Amazon Elastic Block Store (Amazon EBS)  
D. Amazon Elastic File System (Amazon EFS)

**Correct Answer:**  
D. Amazon Elastic File System (Amazon EFS)

**Exam Question 368**

A solutions architect is designing a solution that requires frequent updates to a website that is hosted on Amazon S3 with versioning enabled. For compliance reasons, the older versions of the objects will not be accessed frequently and will need to be deleted after 2 years.

What should the solutions architect recommend to meet these requirements at the LOWEST cost?

A. Use S3 batch operations to replace object tags. Expire the objects based on the modified tags.  
B. Configure an S3 Lifecycle policy to transition older versions of objects to S3 Glacier. Expire the objects after 2 years.  
C. Enable S3 Event Notifications on the bucket that sends older objects to the Amazon Simple Queue Service (Amazon SQS) queue for further processing.  
D. Replicate older object versions to a new bucket. Use an S3 Lifecycle policy to expire the objects in the new bucket after 2 years.

**Correct Answer:**  
B. Configure an S3 Lifecycle policy to transition older versions of objects to S3 Glacier. Expire the objects after 2 years.

**Exam Question 369**

A company hosts its multi-tier public web application in the AWS Cloud. The web application runs on Amazon EC2 instances and its database runs on Amazon RDS. The company is anticipating a large increase in sales during an upcoming holiday weekend. A solutions architect needs to build a solution to analyze the performance of the web application with a granularity of no more than 2 minutes.

What should the solutions architect do to meet this requirement?

A. Send Amazon CloudWatch logs to Amazon Redshift. Use Amazon QuickSight to perform further analysis.  
B. Enable detailed monitoring on all EC2 instances. Use Amazon CloudWatch metrics to perform further analysis.  
C. Create an AWS Lambda function to fetch EC2 logs from Amazon CloudWatch Logs. Use Amazon CloudWatch metrics to perform further analysis.  
D. Send EC2 logs to Amazon S3. Use Amazon Redshift to fetch logs from the S3 bucket to process raw data for further analysis with Amazon QuickSight.

**Correct Answer:**  
B. Enable detailed monitoring on all EC2 instances. Use Amazon CloudWatch metrics to perform further analysis.

**Exam Question 370**

A company has developed a new video game as a web application. The application is in a three-tier architecture in a VPC with Amazon RDS for MySQL. In the database layer several players will compete concurrently online. The game’s developers want to display a top-10 scoreboard in near-real-time and offer the ability to stop and restore the game while preserving the current scores.

What should a solutions architect do to meet these requirements?

A. Set up an Amazon ElastiCache for Memcached cluster to cache the scores for the web application to display.  
B. Set up an Amazon ElastiCache for Redis cluster to compute and cache the scores for the web application to display.  
C. Place an Amazon CloudFront distribution in front of the web application to cache the scoreboard in a section of the application.  
D. Create a read replica on Amazon RDS for MySQL to run queries to compute the scoreboard and serve the read traffic to the web application.

**Correct Answer:**  
D. Create a read replica on Amazon RDS for MySQL to run queries to compute the scoreboard and serve the read traffic to the web application.

#### Exam Question 371

A solutions architect is designing an application for a two-step order process. The first step is synchronous and must return to the user with little latency. The second step takes longer, so it will be implemented in a separate component. Orders must be processed exactly once and in the order in which they are received.

How should the solutions architect integrate these components?

A. Use Amazon SQS FIFO queues.  
B. Use an AWS Lambda function along with Amazon SQS standard queues.  
C. Create an SNS topic and subscribe an Amazon SQS FIFO queue to that topic.  
D. Create an SNS topic and subscribe an Amazon SQS Standard queue to that topic.

**Correct Answer:**  
A. Use Amazon SQS FIFO queues.

**Answer Description:**  
“Standard queues provide at-least-once delivery, which means that each message is delivered at least once.

FIFO queues provide exactly-once processing, which means that each message is delivered once and remains available until a consumer processes it and deletes it. Duplicates are not introduced into the queue.”

**References:**

* Amazon Simple Queue Service > Developer Guide > [What is Amazon Simple Queue Service?](https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html)

#### Exam Question 372

A company is creating an architecture for a mobile app that requires minimal latency for its users. The company’s architecture consists of Amazon EC2 instances behind an Application Load Balancer running in an Auto Scaling group. The EC2 instances connect to Amazon RDS. Application beta testing showed there was a slowdown when reading the data. However the metrics indicate that the EC2 instances do not cross any CPU utilization thresholds.

How can this issue be addressed?

A. Reduce the threshold for CPU utilization in the Auto Scaling group.  
B. Replace the Application Load Balancer with a Network Load Balancer.  
C. Add read replicas for the RDS instances and direct read traffic to the replica.  
D. Add Multi-AZ support to the RDS instances and direct read traffic to the new EC2 instance.

**Correct Answer:**  
C. Add read replicas for the RDS instances and direct read traffic to the replica.

#### Exam Question 373

A company uses Amazon S3 as its object storage solution. The company has thousands of S3 buckets it uses to store data. Some of the S3 buckets have data that is accessed less frequently than others. A solutions architect found that lifecycle policies are not consistently implemented or are implemented partially, resulting in data being stored in high-cost storage.

Which solution will lower costs without compromising the availability of objects?

A. Use S3 ACLs.  
B. Use Amazon Elastic Block Store (Amazon EBS) automated snapshots.  
C. Use S3 Intelligent-Tiering storage.  
D. Use S3 One Zone-Infrequent Access (S3 One Zone-IA).

**Correct Answer:**  
C. Use S3 Intelligent-Tiering storage.

#### Exam Question 374

A media company stores video content in an Amazon Elastic Block Store (Amazon EBS) volume. A certain video file has become popular and a large number of users across the world are accessing this content.

This has resulted in a cost increase.

Which action will DECREASE cost without compromising user accessibility?

A. Change the EBS volume to Provisioned IOPS (PIOPS).  
B. Store the video in an Amazon S3 bucket and create an Amazon CloudFront distribution.  
C. Split the video into multiple, smaller segments so users are routed to the requested video segments only.  
D. Clear an Amazon S3 bucket in each Region and upload the videos so users are routed to the nearest S3 bucket.

**Correct Answer:**  
B. Store the video in an Amazon S3 bucket and create an Amazon CloudFront distribution.

#### Exam Question 375

A company is concerned that two NAT instances in use will no longer be able to support the traffic needed for the company’s application. A solutions architect wants to implement a solution that is highly available fault tolerant, and automatically scalable.

What should the solutions architect recommend?

A. Remove the two NAT instances and replace them with two NAT gateways in the same Availability Zone.  
B. Use Auto Scaling groups with Network Load Balancers for the NAT instances in different Availability Zones.  
C. Remove the two NAT instances and replace them with two NAT gateways in different Availability Zones.  
D. Replace the two NAT instances with Spot Instances in different Availability Zones and deploy a Network Load Balancer.

**Correct Answer:**  
C. Remove the two NAT instances and replace them with two NAT gateways in different Availability Zones.

#### Exam Question 376

A company wants to host a web application on AWS that will communicate to a database within a VPC. The application should be highly available.

What should a solutions architect recommend?

A. Create two Amazon EC2 instances to host the web servers behind a load balancer, and then deploy the database on a large instance.  
B. Deploy a load balancer in multiple Availability Zones with an Auto Scaling group for the web servers, and then deploy Amazon RDS in multiple Availability Zones.  
C. Deploy a load balancer in the public subnet with an Auto Scaling group for the web servers, and then deploy the database on an Amazon EC2 instance in the private subnet.  
D. Deploy two web servers with an Auto Scaling group, configure a domain that points to the two web servers, and then deploy a database architecture in multiple Availability Zones.

**Correct Answer:**  
B. Deploy a load balancer in multiple Availability Zones with an Auto Scaling group for the web servers, and then deploy Amazon RDS in multiple Availability Zones.

#### Exam Question 377

A company has data stored in an on-premises data center that is used by several on-premises applications.

The company wants to maintain its existing application environment and be able to use AWS services for data analytics and future visualizations.

Which storage service should a solutions architect recommend?

A. Amazon Redshift  
B. AWS Storage Gateway for files  
C. Amazon Elastic Block Store (Amazon EBS)  
D. Amazon Elastic File System (Amazon EFS)

**Correct Answer:**  
B. AWS Storage Gateway for files

#### Exam Question 378

A company is developing a mobile game that streams score updates to a backend processor and then posts results on a leaderboard. A solutions architect needs to design a solution that can handle large traffic spikes, process the mobile game updates in order of receipt, and store the processed updates in a highly available database. The company also wants to minimize the management overhead required to maintain the solution.

What should the solutions architect do to meet these requirements?

A. Push score updates to Amazon Kinesis Data Streams. Process the updates in Kinesis Data Streams with AWS Lambda. Store the processed updates in Amazon DynamoDB.  
B. Push score updates to Amazon Kinesis Data Streams. Process the updates with a fleet of Amazon EC2 instances set up for Auto Scaling. Store the processed updates in Amazon Redshift.  
C. Push score updates to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe an AWS Lambda function to the SNS topic to process the updates. Store the processed updates in a SQL database running on Amazon EC2.  
D. Push score updates to an Amazon Simple Queue Service (Amazon SQS) queue. Use a fleet of Amazon EC2 instances with Auto Scaling to process the updates in the SQS queue. Store the processed updates in an Amazon RDS Multi-AZ DB instance.

**Correct Answer:**  
A. Push score updates to Amazon Kinesis Data Streams. Process the updates in Kinesis Data Streams with AWS Lambda. Store the processed updates in Amazon DynamoDB.

**Answer Description:**  
Keywords to focus on would be highly available database – DynamoDB would be a better choice for leaderboard.

#### Exam Question 379

A company is building a document storage application on AWS. The application runs on Amazon EC2 instances in multiple Availability Zones. The company requires the document store to be highly available.

The documents need to be returned immediately when requested. The lead engineer has configured the application to use Amazon Elastic Block Store (Amazon EBS) to store the documents, but is willing to consider other options to meet the availability requirement.

What should a solutions architect recommend?

A. Snapshot the EBS volumes regularly and build new volumes using those snapshots in additional Availability Zones.  
B. Use Amazon EBS for the EC2 instance root volumes. Configure the application to build the document store on Amazon S3.  
C. Use Amazon EBS for the EC2 instance root volumes. Configure the application to build the document store on Amazon S3 Glacier.  
D. Use at least three Provisioned IOPS EBS volumes for EC2 instances. Mount the volumes to the EC2 instances in a RAID 5 configuration.

**Correct Answer:**  
B. Use Amazon EBS for the EC2 instance root volumes. Configure the application to build the document store on Amazon S3.

#### Exam Question 380

A company has a hybrid application hosted on multiple on-premises servers with static IP addresses. There is already a VPN that provides connectivity between the VPC and the on-premises network. The company wants to distribute TCP traffic across the on-premises servers for internet users.

What should a solutions architect recommend to provide a highly available and scalable solution?

A. Launch an internet-facing Network Load Balancer (NLB) and register on-premises IP addresses with the NLB.  
B. Launch an internet-facing Application Load Balancer (ALB) and register on-premises IP addresses with the ALB.  
C. Launch an Amazon EC2 instance, attach an Elastic IP address, and distribute traffic to the on-premises servers.  
D. Launch an Amazon EC2 instance with public IP addresses in an Auto Scaling group and distribute traffic to the on-premises servers.

**Correct Answer:**  
A. Launch an internet-facing Network Load Balancer (NLB) and register on-premises IP addresses with the NLB.

**Exam Question 381**

A company is planning on deploying a newly built application on AWS in a default VPC. The application will consist of a web layer and database layer. The web server was created in public subnets, and the MySQL database was created in private subnets. All subnets are created with the default network ACL settings, and the default security group in the VPC will be replaced with new custom security groups.  
The following are the key requirements:

* The web servers must be accessible only to users on an SSL connection.
* The database should be accessible to the web layer, which is created in a public subnet only.
* All traffic to and from the IP range 182.20.0.0/16 subnet should be blocked.

Which combination of steps meets these requirements? (Select two.)

A. Create a database server security group with inbound and outbound rules for MySQL port 3306 traffic to and from anywhere (0 0.0.0/0).  
B. Create a database server security group with an inbound rule for MySQL port 3306 and specify the source as a web server security group.  
C. Create a web server security group with an inbound allow rule for HTTPS port 443 traffic from anywhere (0.0.0.0/0) and an inbound deny rule for IP range 182.20.0.0/16.  
D. Create a web server security group with an inbound rule for HTTPS port 443 traffic from anywhere (0.0.0.0/0). Create network ACL inbound and outbound deny rules for IP range 182.20.0.0/16.  
E. Create a web server security group with inbound and outbound rules for HTTPS port 443 traffic to and from anywhere (0.0.0.0/0). Create a network ACL inbound deny rule for IP range 182.20.0.0/16.

**Correct Answer:**  
B. Create a database server security group with an inbound rule for MySQL port 3306 and specify the source as a web server security group.  
D. Create a web server security group with an inbound rule for HTTPS port 443 traffic from anywhere (0.0.0.0/0). Create network ACL inbound and outbound deny rules for IP range 182.20.0.0/16.

**Exam Question 382**

A company has an on-premises application that collects data and stores it to an on-premises NFS server.

The company recently set up a 10 Gbps AWS Direct Connect connection. The company is running out of storage capacity on-premises. The company needs to migrate the application data from on-premises to the AWS Cloud while maintaining low-latency access to the data from the on-premises application.

What should a solutions architect do to meet these requirements?

A. Deploy AWS Storage Gateway for the application data, and use the file gateway to store the data in Amazon S3. Connect the on-premises application servers to the file gateway using NFS.  
B. Attach an Amazon Elastic File System (Amazon EFS) file system to the NFS server, and copy the application data to the EFS file system. Then connect the on-premises application to Amazon EFS.  
C. Configure AWS Storage Gateway as a volume gateway. Make the application data available to the on-premises application from the NFS server and with Amazon Elastic Block Store (Amazon EBS) snapshots.  
D. Create an AWS DataSync agent with the NFS server as the source location and an Amazon Elastic File System (Amazon EFS) file system as the destination for application data transfer. Connect the on-premises application to the EFS file system.

**Correct Answer:**  
A. Deploy AWS Storage Gateway for the application data, and use the file gateway to store the data in Amazon S3. Connect the on-premises application servers to the file gateway using NFS.

**Exam Question 383**

A solutions architect needs to design a network that will allow multiple Amazon EC2 instances to access a common data source used for mission-critical data that can be accessed by all the EC2 instances simultaneously. The solution must be highly scalable, easy to implement and support the NFS protocol.

Which solution meets these requirements?

A. Create an Amazon EFS file system. Configure a mount target in each Availability Zone. Attach each instance to the appropriate mount target.  
B. Create an additional EC2 instance and configure it as a file server. Create a security group that allows communication between the Instances and apply that to the additional instance.  
C. Create an Amazon S3 bucket with the appropriate permissions. Create a role in AWS IAM that grants the correct permissions to the S3 bucket. Attach the role to the EC2 Instances that need access to the data.  
D. Create an Amazon EBS volume with the appropriate permissions. Create a role in AWS IAM that grants the correct permissions to the EBS volume. Attach the role to the EC2 instances that need access to the data.

**Correct Answer:**  
A. Create an Amazon EFS file system. Configure a mount target in each Availability Zone. Attach each instance to the appropriate mount target.

**Exam Question 384**

A company is designing an internet-facing web application. The application runs on Amazon EC2 for Linux-based instances that store sensitive user data in Amazon RDS MySQL Multi-AZ DB instances. The EC2 instances are in public subnets, and the RDS DB instances are in private subnets. The security team has mandated that the DB instances be secured against web-based attacks.

What should a solutions architect recommend?

A. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Configure the EC2 instance iptables rules to drop suspicious web traffic. Create a security group for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the individual EC2 instances.  
B. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Move DB instances to the same subnets that EC2 instances are located in. Create a security group for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the individual EC2 instances.  
C. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Use AWS WAF to monitor inbound web traffic for threats. Create a security group for the web application servers and a security group for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the web application server security group.  
D. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Use AWS WAF to monitor inbound web traffic for threats. Configure the Auto Scaling group to automatically create new DB instances under heavy traffic. Create a security group for the RDS DB instances. Configure the RDS security group to only allow port 3306 inbound.

**Correct Answer:**  
C. Ensure the EC2 instances are part of an Auto Scaling group and are behind an Application Load Balancer. Use AWS WAF to monitor inbound web traffic for threats. Create a security group for the web application servers and a security group for the DB instances. Configure the RDS security group to only allow port 3306 inbound from the web application server security group.

**Exam Question 385**

A company wants a storage option that enables its data science team to analyze its data on-premises and in the AWS Cloud. The team needs to be able to run statistical analyses by using the data on-premises and by using a fleet of Amazon EC2 instances across multiple Availability Zones.

What should a solutions architect do to meet these requirements?

A. Use an AWS Storage Gateway tape gateway to copy the on-premises files into Amazon S3.  
B. Use an AWS Storage Gateway volume gateway to copy the on-premises files into Amazon S3.  
C. Use an AWS Storage Gateway file gateway to copy the on-premises files to Amazon Elastic Block Store (Amazon EBS).  
D. Attach an Amazon Elastic File System (Amazon EFS) file system to the on-premises servers. Copy the files to Amazon EFS.

**Correct Answer:**  
C. Use an AWS Storage Gateway file gateway to copy the on-premises files to Amazon Elastic Block Store (Amazon EBS).

**Exam Question 386**

A company wants to improve the availability and performance of its stateless UDP-based workload. The workload is deployed on Amazon EC2 instances in multiple AWS Regions.

What should a solutions architect recommend to accomplish this?

A. Place the EC2 instances behind Network Load Balancers (NLBs) in each Region. Create an accelerator using AWS Global Accelerator. Use the NLBs as endpoints for the accelerator.  
B. Place the EC2 instances behind Application Load Balancers (ALBs) in each Region. Create an accelerator using AWS Global Accelerator. Use the ALBs as endpoints for the accelerator.  
C. Place the EC2 instances behind Network Load Balancers (NLBs) in each Region. Create an Amazon CloudFront distribution with an origin that uses Amazon Route 53 latency-based routing to route requests to the NLBs.  
D. Place the EC2 instances behind Application Load Balancers (ALBs) in each Region. Create an Amazon CloudFront distribution with an origin that uses Amazon Route 53 latency-based routing to route requests to the ALBs.

**Correct Answer:**  
D. Place the EC2 instances behind Application Load Balancers (ALBs) in each Region. Create an Amazon CloudFront distribution with an origin that uses Amazon Route 53 latency-based routing to route requests to the ALBs.

**Exam Question 387**

A company is creating a three-tier web application consisting of a web server, an application server, and a database server. The application will track GPS coordinates of packages as they are being delivered. The application will update the database every 0-5 seconds.

The tracking will need to read a fast as possible for users to check the status of their packages. Only a few packages might be tracked on some days, whereas millions of package might be tracked on other days.

Tracking will need to be searchable by tracking ID customer ID and order ID. Order than 1 month no longer read to be tracked.

What should a solution architect recommend to accomplish this with minimal cost of ownership?

A. Use Amazon DynamoDB Enable Auto Scaling on the DynamoDB table. Schedule an automatic deletion script for items older than 1 month.  
B. Use Amazon DynamoDB with global secondary indexes. Enable Auto Scaling on the DynamoDB table and the global secondary indexes. Enable TTL on the DynamoDB table.  
C. Use an Amazon RDS On-Demand instance with Provisioned IOPS (PIOPS). Enable Amazon CloudWatch alarms to send notifications when PIOPS are exceeded. Increase and decrease PIOPS as needed.  
D. Use an Amazon RDS Reserved Instance with Provisioned IOPS (PIOPS). Enable Amazon CloudWatch alarms to send notification when PIOPS are exceeded. Increase and decrease PIOPS as needed.

**Correct Answer:**  
B. Use Amazon DynamoDB with global secondary indexes. Enable Auto Scaling on the DynamoDB table and the global secondary indexes. Enable TTL on the DynamoDB table.

**Exam Question 388**

A new employee has joined a company as a deployment engineer. The deployment engineer will be using AWS CloudFormation templates to create multiple AWS resources. A solutions architect wants the deployment engineer to perform job activities while following the principle of least privilege.

Which combination of actions should the solutions architect take to accomplish this goal? (Choose two.)

A. Have the deployment engineer use AWS account root user credentials for performing AWS CloudFormation stack operations.  
B. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the PowerUsers IAM policy attached.  
C. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the Administrate/Access IAM policy attached.  
D. Create a new IAM User for the deployment engineer and add the IAM user to a group that has an IAM policy that allows AWS CloudFormation actions only.  
E. Create an IAM role for the deployment engineer to explicitly define the permissions specific to the AWS CloudFormation stack and launch stacks using Dial IAM role.

**Correct Answer:**  
A. Have the deployment engineer use AWS account root user credentials for performing AWS CloudFormation stack operations.  
E. Create an IAM role for the deployment engineer to explicitly define the permissions specific to the AWS CloudFormation stack and launch stacks using Dial IAM role.

**Exam Question 389**

A company is planning to use an Amazon DynamoDB table for data storage. The company is concerned about cost optimization. The table will not be used on most mornings in the evenings, the read and write traffic will often be unpredictable. When traffic spikes occur they will happen very quickly.

What should a solutions architect recommend?

A. Create a DynamoDB table in on-demand capacity mode.  
B. Create a DynamoDB table with a global secondary index.  
C. Create a DynamoDB table with provisioned capacity and auto scaling.  
D. Create a DynamoDB table in provisioned capacity mode, and configure it as a global table.

**Correct Answer:**  
A. Create a DynamoDB table in on-demand capacity mode.

**Exam Question 390**

A company has NFS servers in an on-premises data center that need to periodically back up small amounts of data to Amazon S3.

Which solution meets these requirements and is MOST cost-effective?

A. Set up AWS Glue to copy the data from the on-premises servers to Amazon S3.  
B. Set up an AWS DataSync agent on the on-premises servers, and sync the data to Amazon S3.  
C. Set up an SFTP sync using AWS Transfer for SFTP to sync data from on-premises to Amazon S3.  
D. Set up an AWS Direct Connect connection between the on-premises data center and a VPC, and copy the data to Amazon S3.

**Correct Answer:**  
C. Set up an SFTP sync using AWS Transfer for SFTP to sync data from on-premises to Amazon S3.

**Exam Question 391**

A company runs its production workload on an Amazon Aurora MySQL DB cluster that includes six Aurora Replicas. The company wants near-real-time reporting queries from one of its departments to be automatically distributed across three of the Aurora Replicas. Those three replicas have a different compute and memory specification from the rest of the DB cluster.  
Which solution meets these requirements?

A. Create and use a custom endpoint for the workload.  
B. Create a three-node cluster clone and use the reader endpoint.  
C. Use any of the instance endpoints for the selected three nodes.  
D. Use the reader endpoint to automatically distribute the read-only workload.

**Correct Answer:**  
B. Create a three-node cluster clone and use the reader endpoint.

**Exam Question 392**

A company wants to move its on-premises network, attached storage (NAS) to AWS. The company wants to make the data available to any Linux instances within its VPC and ensure changes are automatically synchronized across all instances accessing the data store. The majority of the data is accessed very rarely, and some files are accessed by multiple users at the same time.  
Which solution meets these requirements and is MOST cost-effective?

A. Create an Amazon Elastic Block Store (Amazon EBS) snapshot containing the data. Share it with users within the VPC.  
B. Create an Amazon S3 bucket that has a lifecycle policy set to transition the data to S3 Standard Infrequent Access (S3 Standard-IA) after the appropriate number of days.  
C. Create an Amazon Elastic File System (Amazon EFS) file system within the VPC. Set the throughput mode to Provisioned and to the required amount of IOPS to support concurrent usage.  
D. Create an Amazon Elastic File System (Amazon EFS) file system within the VPC. Set the lifecycle policy to transition the data to EFS Infrequent Access (EFS IA) after the appropriate number of days.

**Correct Answer:**  
D. Create an Amazon Elastic File System (Amazon EFS) file system within the VPC. Set the lifecycle policy to transition the data to EFS Infrequent Access (EFS IA) after the appropriate number of days.

**Exam Question 393**

A company that recently started using AWS establishes a Site-to-Site VPN between its on-premises datacenter and AWS. The company’s security mandate states that traffic originating from on-premises should stay within the company’s private IP space when communicating with an Amazon Elastic Container Service (Amazon ECS) cluster that is hosting a sample web application.

Which solution meets this requirement?

A. Configure a gateway endpoint for Amazon ECS. Modify the route table to include an entry pointing to the ECS cluster.  
B. Create a Network Load Balancer and AWS PrivateLink endpoint for Amazon ECS in the same VPC that is hosting the ECS cluster.  
C. Create a Network Load Balancer in one VPC and an AWS PrivateLink endpoint for Amazon ECS in another VPC. Connect the two VPCs by using VPC peering.  
D. Configure an Amazon Route 53 record with Amazon ECS as the target. Apply a server certificate to Route 53 from AWS Certificate Manager (ACM) for SSL offloading.

**Correct Answer:**  
C. Create a Network Load Balancer in one VPC and an AWS PrivateLink endpoint for Amazon ECS in another VPC. Connect the two VPCs by using VPC peering.

**Exam Question 394**

An application allows users at a company’s headquarters to access product data. The product data is stored in an Amazon RDS MySQL DB instance. The operations team has isolated an application performance slowdown and wants to separate read traffic from write traffic. A solutions architect needs to optimize the application’s performance quickly.

What should the solutions architect recommend?

A. Change the existing database to a Multi-AZ deployment. Serve the read requests from the primary Availability Zone.  
B. Change the existing database to a Multi-AZ deployment. Serve the read requests from the secondary Availability Zone.  
C. Create read replicas for the database. Configure the read replicas with half of the compute and storage resources as the source database.  
D. Create read replicas for the database. Configure the read replicas with the same compute and storage resources as the source database.

**Correct Answer:**  
D. Create read replicas for the database. Configure the read replicas with the same compute and storage resources as the source database.

**Exam Question 395**

A company requires that all versions of objects in its Amazon S3 bucket be retained. Current object versions will be frequently accessed during the first 30 days, after which they will be rarely accessed and must be retrievable within 5 minutes. Previous object versions need to be kept forever, will be rarely accessed, and can be retrieved within 1 week. All storage solutions must be highly available and highly durable.

What should a solutions architect recommend to meet these requirements in the MOST cost-effective manner?

A. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Glacier after 30 days and moves previous object versions to S3 Glacier after 1 day.  
B. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Glacier after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day.  
C. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Standard-infrequent Access (S3 Standard-IA) after 30 days and moves previous object versions toS3 Glacier Deep Archive after 1 day.  
D. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days and moves previous object versions to S3 Glacier Deep Archive after 1 day.

**Correct Answer:**  
A. Create an S3 lifecycle policy for the bucket that moves current object versions from S3 Standard storage to S3 Glacier after 30 days and moves previous object versions to S3 Glacier after 1 day.

**Exam Question 396**

A company is developing a video conversion application hosted on AWS. The application will be available in two tiers: a free tier and a paid tier. Users in the paid tier will have their videos converted first and then the tree tier users will have their videos converted.

Which solution meets these requirements and is MOST cost-effective?

A. One FIFO queue for the paid tier and one standard queue for the free tier.  
B. A single FIFO Amazon Simple Queue Service (Amazon SQS) queue for all file types.  
C. A single standard Amazon Simple Queue Service (Amazon SQS) queue for all file types.  
D. Two standard Amazon Simple Queue Service (Amazon SQS) queues with one for the paid tier and one for the free tier.

**Correct Answer:**  
D. Two standard Amazon Simple Queue Service (Amazon SQS) queues with one for the paid tier and one for the free tier.

**Answer Description:**  
In AWS, the queue service is the Simple Queue Service (SQS). Multiple SQS queues may be prepared to prepare queues for individual priority levels (with a priority queue and a secondary queue). Moreover, you may also use the message Delayed Send function to delay process execution.

**Exam Question 397**

An administrator of a large company wants to monitor for and prevent any cryptocurrency-related attacks on the company’s AWS accounts.

Which AWS service can the administrator use to protect the company against attacks?

A. Amazon Cognito  
B. Amazon GuardDuty  
C. Amazon Inspector  
D. Amazon Macie

**Correct Answer:**  
C. Amazon Inspector

**Exam Question 398**

A company wants to host its web application on AWS using multiple Amazon EC2 instances across different AWS Regions. Since the application content will be specific to each geographic region, the client requests need to be routed to the server that hosts the content for that clients Region.

What should a solutions architect do to accomplish this?

A. Configure Amazon Route 53 with a latency routing policy.  
B. Configure Amazon Route 53 with a weighted routing policy.  
C. Configure Amazon Route 53 with a geolocation routing policy.  
D. Configure Amazon Route 53 with a multivalue answer routing policy.

**Correct Answer:**  
C. Configure Amazon Route 53 with a geolocation routing policy.

**Exam Question 399**

A company is developing a new machine learning model solution in AWS. The models are developed as independent microservices that fetch about 1 GB of model data from Amazon S3 at startup and load the data into memory. Users access the models through an asynchronous API. Users can send a request or a batch of requests and specify where the results should be sent.

The company provides models to hundreds of users. The usage patterns for the models are irregular Some models could be unused for days or weeks. Other models could receive batches of thousands of requests at a time.

Which solution meets these requirements?

A. The requests from the API are sent to an Application Load Balancer (ALB). Models are deployed as AWS Lambda functions invoked by the ALB.  
B. The requests from the API are sent to the models Amazon Simple Queue Service (Amazon SQS) queue. Models are deployed as AWS Lambda functions triggered by SQS events AWS Auto Scaling is enabled on Lambda to increase the number of vCPUs based on the SQS queue size.  
C. The requests from the API are sent to the model’s Amazon Simple Queue Service (Amazon SQS) queue. Models are deployed as Amazon Elastic Container Service (Amazon ECS) services reading from the queue AWS App Mesh scales the instances of the ECS cluster based on the SQS queue size.  
D. The requests from the API are sent to the models Amazon Simple Queue Service (Amazon SQS) queue. Models are deployed as Amazon Elastic Container Service (Amazon ECS) services reading from the queue AWS Auto Scaling is enabled on Amazon ECS for both the cluster and copies of the service based on the queue size.

**Correct Answer:**  
D. The requests from the API are sent to the models Amazon Simple Queue Service (Amazon SQS) queue. Models are deployed as Amazon Elastic Container Service (Amazon ECS) services reading from the queue AWS Auto Scaling is enabled on Amazon ECS for both the cluster and copies of the service based on the queue size.

**Exam Question 400**

A company is preparing to launch a public-facing web application in the AWS Cloud. The architecture consists of Amazon EC2 instances within a VPC behind an Elastic Load Balancer (ELB). A third party service is used for the DNS. The company’s solutions architect must recommend a solution to detect and protect against largescale DDoS attacks.

Which solution meets these requirements?

A. Enable Amazon GuardDuty on the account.  
B. Enable Amazon Inspector on the EC2 instances.  
C. Enable AWS Shield and assign Amazon Route 53 to it.  
D. Enable AWS Shield Advanced and assign the ELB to it.

**Correct Answer:**  
C. Enable AWS Shield and assign Amazon Route 53 to it.

**AWS Certified Solutions Architect – Associate SAA-C02 Exam Questions and Answers – Page 5**

The latest AWS Certified Solutions Architect – Associate SAA-C02 certification actual real practice exam question and answer (Q&A) dumps are available free, which are helpful for you to pass the AWS Certified Solutions Architect – Associate SAA-C02 exam and earn AWS Certified Solutions Architect – Associate SAA-C02 certification.

**Exam Question 401**

A company is running an online transaction processing (OLTP) workload on AWS. This workload uses an unencrypted Amazon RDS DB instance in a Multi-AZ deployment. Daily database snapshots are taken from this instance.

What should a solutions architect do to ensure the database and snapshots are always encrypted moving forward?

A. Encrypt a copy of the latest DB snapshot. Replace existing DB instance by restoring the encrypted snapshot.  
B. Create a new encrypted Amazon Elastic Block Store (Amazon EBS) volume and copy the snapshots to it. Enable encryption on the DB instance.  
C. Copy the snapshots and enable encryption using AWS Key Management Service (AWS KMS). Restore encrypted snapshot to an existing DB instance.  
D. Copy the snapshots to an Amazon S3 bucket that is encrypted using server-side encryption with AWS Key Management Service (AWS KMS) managed keys (SSE-KMS).

**Correct Answer:**  
A. Encrypt a copy of the latest DB snapshot. Replace existing DB instance by restoring the encrypted snapshot.

**Exam Question 402**

A company previously migrated its data warehouse solution to AWS. The company also has an AWS Direct Connect connection. Corporate office users query the data warehouse using a visualization tool. The average size of a query returned by the data warehouse is 50 MB and each webpage sent by the visualization tool is approximately 500 KB. Result sets returned by the data warehouse are not cached.

Which solution provides the LOWEST data transfer egress cost for the company?

A. Host the visualization tool on-premises and query the data warehouse directly over the internet.  
B. Host the visualization tool in the same AWS Region as the data warehouse. Access it over the internet.  
C. Host the visualization tool on-premises and query the data warehouse directly over a Direct Connect connection at a location in the same AWS Region.  
D. Host the visualization tool in the same AWS Region as the data warehouse and access it over a DirectConnect connection at a location in the same Region.

**Correct Answer:**  
A. Host the visualization tool on premises and query the data warehouse directly over the internet.

**Exam Question 403**

A mobile gaming company runs application servers on Amazon EC2 instances. The servers receive updates from players every 15 minutes. The mobile game creates a JSON object of the progress made in the game since the last update, and sends the JSON object to an Application Load Balancer. As the mobile game is played, game updates are being lost. The company wants to create a durable way to get the updates in older.

What should a solutions architect recommend to decouple the system?

A. Use Amazon Kinesis Data Streams to capture the data and store the JSON object in Amazon S3.  
B. Use Amazon Kinesis Data Firehose to capture the data and store the JSON object in Amazon S3.  
C. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues to capture the data and EC2 instances to process the messages in the queue.  
D. Use Amazon Simple Notification Service (Amazon SNS) to capture the data and EC2 instances to process the messages sent to the Application Load Balancer.

**Correct Answer:**  
C. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues to capture the data and EC2 instances to process the messages in the queue.

**Exam Question 404**

A company has an application that runs on Amazon EC2 instances within a private subnet in a VPC. The instances access data in an Amazon S3 bucket in the same AWS Region. The VPC contains a NAT gateway in a public subnet to access the S3 bucket. The company wants to reduce costs by replacing the NAT gateway without compromising security or redundancy.

Which solution meets these requirements?

A. Replace the NAT gateway with a NAT instance.  
B. Replace the NAT gateway with an internet gateway.  
C. Replace the NAT gateway with a gateway VPC endpoint.  
D. Replace the NAT gateway with an AWS Direct Connect connection.

**Correct Answer:**  
C. Replace the NAT gateway with a gateway VPC endpoint.

**Exam Question 405**

A company has a dynamic web application hosted on two Amazon EC2 instances. The company has its own SSL certificate, which is on each instance to perform SSL termination.

There has been an increase in traffic recently, and the operations team determined that SSL encryption and decryption is causing the compute capacity of the web servers to reach their maximum limit.

What should a solutions architect do to increase the application’s performance?

A. Create a new SSL certificate using AWS Certificate Manager (ACM). Install the ACM certificate on each instance.  
B. Create an Amazon S3 bucket. Migrate the SSL certificate to the S3 bucket. Configure the EC2 instances to reference the bucket for SSL termination.  
C. Create another EC2 instance as a proxy server. Migrate the SSL certificate to the new instance and configure it to direct connections to the existing EC2 instances.  
D. Import the SSL certificate into AWS Certificate Manager (ACM). Create an Application Load Balancer with an HTTPS listener that uses the SSL certificate from ACM.

**Correct Answer:**  
D. Import the SSL certificate into AWS Certificate Manager (ACM). Create an Application Load Balancer with an HTTPS listener that uses the SSL certificate from ACM.

**Exam Question 406**

A company has an application hosted on Amazon EC2 instances in two VPCs across different AWS Regions. To communicate with each other, the instances use the internet for connectivity. The security team wants to ensure that no communication between the instances happens over the internet.

What should a solutions architect do to accomplish this?

A. Create a NAT gateway and update the route table of the EC2 instances’ subnet.  
B. Create a VPC endpoint and update the route table of the EC2 instances’ subnet.  
C. Create a VPN connection and update the route table of the EC2 instances’ subnet.  
D. Create a VPC peering connection and update the route table of the EC2 instances’ subnet.

**Correct Answer:**  
D. Create a VPC peering connection and update the route table of the EC2 instances’ subnet.

**Exam Question 407**

A company is preparing to store confidential data in Amazon S3. For compliance reasons, the data must be encrypted at rest. Encryption key usage must be logged for auditing purposes. Keys must be rotated every year.

Which solution meets these requirements and is the MOST operationally efficient?

A. Server-side encryption with customer-provided keys (SSE-C)  
B. Server-side encryption with Amazon S3 managed keys (SSE-S3)  
C. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with manual rotation  
D. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with automatic rotation

**Correct Answer:**  
D. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with automatic rotation

**Exam Question 408**

A media company has an application that tracks user clicks on its websites and performs analytics to provide near-real-time recommendations. The application has a Heel of Amazon EC2 instances that receive data from the websites and send the data to an Amazon RDS DB instance. Another fleet of EC2 instances hosts the portion of the application that is continuously checking changes in the database and executing SQL queries to provide recommendations. Management has requested a redesign to decouple the infrastructure. The solution must ensure that data analysts are writing SQL to analyze the data only No data can the lost during the deployment.

What should a solutions architect recommend?

A. Use Amazon Kinesis Data Streams to capture the data from the websites Kinesis Data Firehose to persist the data on Amazon S3, and Amazon Athena to query the data.  
B. Use Amazon Kinesis Data Streams to capture the data from the websites. Kinesis Data Analytics to query the data, and Kinesis Data Firehose to persist the data on Amazon S3.  
C. Use Amazon Simple Queue Service (Amazon SQS) to capture the data from the websites, keep the fleet of EC2 instances, and change to a bigger instance type in the Auto Scaling group configuration.  
D. Use Amazon Simple Notification Service (Amazon SNS) to receive data from the websites and proxy the messages to AWS Lambda functions that execute the queries and persist the data. Change Amazon RDS to Amazon Aurora Serverless to persist the data.

**Correct Answer:**  
B. Use Amazon Kinesis Data Streams to capture the data from the websites. Kinesis Data Analytics to query the data, and Kinesis Data Firehose to persist the data on Amazon S3.

**Exam Question 409**

A company has a mobile game that reads most of its metadata from an Amazon RDS DB instance. As the game increased in popularity developers noticed slowdowns related to the game’s metadata load times.

Performance metrics indicate that simply scaling the database will not help. A solutions architect must explore all options that include capabilities for snapshots replication and sub-millisecond response times.

What should the solutions architect recommend to solve these issues?

A. Migrate the database to Amazon Aurora with Aurora Replicas.  
B. Migrate the database to Amazon DyramoDB with global tables.  
C. Add an Amazon ElastiCache for Redis layer in front of the database.  
D. Add an Amazon ElastiCache for Memcached layer in front of the database.

**Correct Answer:**  
B. Migrate the database to Amazon DyramoDB with global tables.

**Exam Question 410**

A company is deploying an application in three AWS Regions using an Application Load Balancer Amazon Route 53 will be used to distribute traffic between these Regions.

Which Route 53 configuration should a solutions architect use to provide the MOST high-performing experience?

A. Create an A record with a latency policy.  
B. Create an A record with a geolocation policy.  
C. Create a CNAME record with a failover policy.  
D. Create a CNAME record with a geoproximity policy.

**Correct Answer:**  
A. Create an A record with a latency policy.

**Exam Question 411**

A company has a multi-tier application deployed on several Amazon EC2 instances in an Auto Scaling group. An Amazon RDS for Oracle instance is the application, data layer that uses Oracle-specific PSQL functions. Traffic to the application has been steadily increasing. This is causing the EC2 instances to become overloaded and RDS instance to run out of storage. The Auto Scaling group does not have any scaling metrics and defines the minimum healthy instance count only. The company predicts that traffic will continue to increase at a steady but unpredictable rate before leveling off.

What should a solutions architect do to ensure the system can automatically scale for the increased traffic? (Choose two.)

A. Configure storage Auto Scaling on the RDS for Oracle instance.  
B. Migrate the database to Amazon Aurora to use Auto Scaling storage.  
C. Configure an alarm on the RDS for Oracle instance for low free storage space.  
D. Configure the Auto Scaling group to use the average CPU as the scaling metric.  
E. Configure the Auto Scaling group to use the average free memory as the scaling metric.

**Correct Answer:**  
A. Configure storage Auto Scaling on the RDS for Oracle instance.  
C. Configure an alarm on the RDS for Oracle instance for low free storage space.

**Exam Question 412**

A company’s application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. On the first day of every month at midnight, the application becomes much slower when the month-end financial calculation batch executes. This causes the CPU utilization of the EC2 instances to immediately peak to 100%, which disrupts the application.

What should a solutions architect recommend to ensure the application is able to handle the workload and avoid downtime?

A. Configure an Amazon CloudFront distribution in front of the ALB.  
B. Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization.  
C. Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule.  
D. Configure Amazon ElastiGache to remove some of the workload from the EC2 instances.

**Correct Answer:**  
C. Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule.

**Exam Question 413**

A company wants to run its critical applications in containers to meet requirements for scalability and availability. The company prefers to focus on maintenance of the critical applications. The company does not want to be responsible for provisioning and managing the underlying infrastructure that runs the containerized workload.

What should a solutions architect do to meet these requirements?

A. Use Amazon EC2 instances, and install Docker on the instances.  
B. Use Amazon Elastic Container Service (Amazon ECS) on Amazon EC2 worker nodes.  
C. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate.  
D. Use Amazon EC2 instances from an Amazon Elastic Container Service (Amazon ECS)-optimized Amazon Machine Image (AMI).

**Correct Answer:**  
C. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate.

**Exam Question 414**

A company is designing a new application that runs in a VPC on Amazon EC2 instances. The application stores data in Amazon S3 and uses Amazon DynamoDB as its database. For compliance reasons, the company prohibits all traffic between the EC2 instances and other AWS services from passing over the public internet.

What can a solutions architect do to meet this requirement?

A. Configure gateway VPC endpoints to Amazon S3 and DynamoDB.  
B. Configure interface VPC endpoints to Amazon S3 and DynamoDB.  
C. Configure a gateway VPC endpoint to Amazon S3. Configure an interface VPC endpoint to DynamoDB.  
D. Configure a gateway VPC endpoint to DynamoDB. Configure an interface VPC endpoint to Amazon S3.

**Correct Answer:**  
C. Configure a gateway VPC endpoint to Amazon S3. Configure an interface VPC endpoint to DynamoDB.

**Exam Question 415**

A company’s security team requests that network traffic be captured in VPC Flow Logs. The logs will be frequently accessed for 90 days and then accessed intermittently.

What should a solutions architect do to meet these requirements when configuring the logs?

A. Use Amazon CloudWatch as the target. Set the CloudWatch log group with an expiration of 90 days.  
B. Use Amazon Kinesis as the target. Configure the Kinesis stream to always retain the logs for 90 days.  
C. Use AWS CloudTrail as the target. Configure CloudTrail to save to an Amazon S3 bucket, and enable S3 Intelligent-Tiering.  
D. Use Amazon S3 as the target. Enable an S3 Lifecycle policy to transition the logs to S3 StandardInfrequent Access (S3 Standard-IA) after 90 days.

**Correct Answer:**  
D. Use Amazon S3 as the target. Enable an S3 Lifecycle policy to transition the logs to S3 StandardInfrequent Access (S3 Standard-IA) after 90 days.

**Exam Question 416**

A company needs to provide its employees with secure access to confidential and sensitive files. The company wants to ensure that the files can be accessed only by authorized users. The files must be downloaded securely to the employees’ devices.

The files are stored in an on-premises Windows file server. However, due to an increase in remote usage, the file server is running out of capacity.

Which solution will meet these requirements?

A. Migrate the file server to an Amazon EC2 instance in a public subnet. Configure the security group to limit inbound traffic to the employees’ IP addresses.  
B. Migrate the files to an Amazon FSx for Windows File Server file system. Integrate the Amazon FSx file system with the on-premises Active Directory. Configure AWS Client VPN.  
C. Migrate the files to Amazon S3, and create a private VPC endpoint. Create a signed URL to allow download.  
D. Migrate the files to Amazon S3, and create a public VPC endpoint. Allow employees to sign on with AWS Single Sign-On.

**Correct Answer:**  
C. Migrate the files to Amazon S3, and create a private VPC endpoint. Create a signed URL to allow download.

**Exam Question 417**

A company hosts a multi-tier web application that uses an Amazon Aurora MySQL DB cluster for storage. The application tier is hosted on Amazon EC2 instances. The company’s IT security guidelines mandate that the database credentials be encrypted and rotated every 14 days.

What should a solutions architect do to meet this requirement with the LEAST operational effort?

A. Create a new AWS Key Management Service (AWS KMS) encryption key. Use AWS Secrets Manager to create a new secret that uses the KMS key with the appropriate credentials. Associate the secret with the Aurora DB cluster. Configure a custom rotation period of 14 days.  
B. Create two parameters in AWS Systems Manager Parameter Store: one for the user name as a string parameter and one that uses the SecureString type for the password. Select AWS Key Management Service (AWS KMS) encryption for the password parameter, and load these parameters in the application tier. Implement an AWS Lambda function that rotates the password every 14 days.  
C. Store a file that contains the credentials in an AWS Key Management Service (AWS KMS) encrypted Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system in all EC2 instances of the application tier. Restrict the access to the file on the file system so that the application can read the file and that only super users can modify the file. Implement an AWS Lambda function that rotates the key in Aurora every 14 days and writes new credentials into the file.  
D. Store a file that contains the credentials in an AWS Key Management Service (AWS KMS) encrypted Amazon S3 bucket that the application uses to load the credentials. Download the file to the application regularly to ensure that the correct credentials are used. Implement an AWS Lambda function that rotates the Aurora credentials every 14 days and uploads these credentials to the file in the S3 bucket.

**Correct Answer:**  
B. Create two parameters in AWS Systems Manager Parameter Store: one for the user name as a string parameter and one that uses the SecureString type for the password. Select AWS Key Management Service (AWS KMS) encryption for the password parameter, and load these parameters in the application tier. Implement an AWS Lambda function that rotates the password every 14 days.

**Exam Question 418**

A company is building an application that consists of several microservices. The company has decided to use container technologies to deploy its software on AWS. The company needs a solution that minimizes the amount of ongoing effort for maintenance and scaling. The company cannot manage additional infrastructure.

Which combination of actions should a solutions architect take to meet these requirements? (Choose two.)

A. Deploy an Amazon Elastic Container Service (Amazon ECS) cluster.  
B. Deploy the Kubernetes control plane on Amazon EC2 instances that span multiple Availability Zones.  
C. Deploy an Amazon Elastic Container Service (Amazon ECS) service with an Amazon EC2 launch type. Specify a desired task number level of greater than or equal to 2.  
D. Deploy an Amazon Elastic Container Service (Amazon ECS) service with a Fargate launch type. Specify a desired task number level of greater than or equal to 2.  
E. Deploy Kubernetes worker nodes on Amazon EC2 instances that span multiple Availability Zones. Create a deployment that specifies two or more replicas for each microservice.

**Correct Answer:**  
A. Deploy an Amazon Elastic Container Service (Amazon ECS) cluster.  
B. Deploy the Kubernetes control plane on Amazon EC2 instances that span multiple Availability Zones.

**Exam Question 419**

A company recently launched a new service that involves medical images. The company scans the images and sends them from its on-premises data center through an AWS Direct Connect connection to Amazon EC2 instances. After processing is complete, the images are stored in an Amazon S3 bucket.

A company requirement states that the EC2 instances cannot be accessible through the internet. The EC2 instances run in a private subnet, which has a default route back to the on-premises data center for outbound internet access.

Usage of the new service is increasing rapidly. A solutions architect must recommend a solution that meets the company’s requirements and reduces the Direct Connect charges.

Which solution accomplishes these goals MOST cost-effectively?

A. Configure a VPC endpoint for Amazon S3. Add an entry to the private subnet’s route table for the S3 endpoint.  
B. Configure a NAT gateway in a public subnet. Configure the private subnet’s route table to use the NAT gateway.  
C. Configure Amazon S3 as a file system mount point on the EC2 instances. Access Amazon S3 through the mount.  
D. Move the EC2 instances into a public subnet. Configure the public subnet route table to point to an internet gateway.

**Correct Answer:**  
B. Configure a NAT gateway in a public subnet. Configure the private subnet’s route table to use the NAT gateway.

**Exam Question 420**

A company is building an online multiplayer game. The game communicates by using UDP, and low latency between the client and the backend is important. The backend is hosted on Amazon EC2 instances that can be deployed to multiple AWS Regions to meet demand. The company needs the game to be highly available so that users around the world can access the game at all times.

What should a solutions architect do to meet these requirements?

A. Deploy Amazon CloudFront to support the global traffic. Configure CloudFront with an origin group to allow access to EC2 instances in multiple Regions.  
B. Deploy an Application Load Balancer in one Region to distribute traffic to EC2 instances in each Region that hosts the game’s backend instances.  
C. Deploy Amazon CloudFront to support an origin access identity (OAI). Associate the OAI with EC2 instances in each Region to support global traffic.  
D. Deploy a Network Load Balancer in each Region to distribute the traffic. Use AWS Global Accelerator to route traffic to the correct Regional endpoint.

**Correct Answer:**  
C. Deploy Amazon CloudFront to support an origin access identity (OAI). Associate the OAI with EC2 instances in each Region to support global traffic.

**Exam Question 421**

A company runs its two-tier eCommerce website on AWS. The web tier consists of a load balancer that sends traffic to Amazon EC2 instances. The database tier uses an Amazon RDS DB instance. The EC2 instances and the RDS DB instance should not be exposed to the public internet. The EC2 instances require internet access to complete payment processing of orders through a third-party web service. The application must be highly available.

Which combination of configuration options will meet these requirements? (Choose two.)

A. Use an Auto Scaling group to launch the EC2 instances in private subnets. Deploy an RDS Multi-AZ DB instance in private subnets.  
B. Configure a VPC with two private subnets and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the private subnets.  
C. Use an Auto Scaling group to launch the EC2 instances in public subnets across two Availability Zones. Deploy an RDS Multi-AZ DB instance in private subnets.  
D. Configure a VPC with one public subnet, one private subnet, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnet.  
E. Configure a VPC with two public subnets, two private subnets, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnets.

**Correct Answer:**  
A. Use an Auto Scaling group to launch the EC2 instances in private subnets. Deploy an RDS Multi-AZ DB instance in private subnets.  
B. Configure a VPC with two private subnets and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the private subnets.

**Exam Question 422**

A security team needs to enforce the rotation of all IAM users’ access keys every 90 days. If an access key is found to be older, the key must be made inactive and removed. A solutions architect must create a solution that will check for and remediate any keys older than 90 days.

Which solution meets these requirements with the LEAST operational effort?

A. Create an AWS Config rule to check for the key age. Configure the AWS Config rule to run an AWS Batch job to remove the key.  
B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to check for the key age. Configure the rule to run an AWS Batch job to remove the key.  
C. Create an AWS Config rule to check for the key age. Define an Amazon EventBridge (Amazon CloudWatch Events) rule to schedule an AWS Lambda function to remove the key.  
D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to check for the key age. Define an EventBridge (CloudWatch Events) rule to run an AWS Batch job to remove the key.

**Correct Answer:**  
A. Create an AWS Config rule to check for the key age. Configure the AWS Config rule to run an AWS Batch job to remove the key.

**Exam Question 423**

A solutions architect must provide an automated solution for a company’s compliance policy that states security groups cannot include a rule that allows SSH from 0.0.0.0/0. The company needs to be notified if there is any breach in the policy. A solution is needed as soon as possible.

What should the solutions architect do to meet these requirements with the LEAST operational overhead?

A. Write an AWS Lambda script that monitors security groups for SSH being open to 0.0.0.0/0 addresses and creates a notification every time it finds one.  
B. Enable the restricted-ssh AWS Config managed rule and generate an Amazon Simple Notification Service (Amazon SNS) notification when a noncompliant rule is created.  
C. Create an IAM role with permissions to globally open security groups and network ACLs. Create an Amazon Simple Notification Service (Amazon SNS) topic to generate a notification every time the role is assumed by a user.  
D. Configure a service control policy (SCP) that prevents non-administrative users from creating or editing security groups. Create a notification in the ticketing system when a user requests a rule that needs administrator permissions.

**Correct Answer:**  
B. Enable the restricted-ssh AWS Config managed rule and generate an Amazon Simple Notification Service (Amazon SNS) notification when a noncompliant rule is created.

**Exam Question 424**

A media company is using two video conversion tools that run on Amazon EC2 instances. One tool runs on Windows instances, and the other tool runs on Linux instances. Each video file is large in size and must be processed by both tools.

The company needs a storage solution that can provide a centralized file system that can be mounted on all the EC2 instances that are used in this process.

Which solution meets these requirements?

A. Use Amazon FSx for Windows File Server for the Windows instances. Use Amazon Elastic File System (Amazon EFS) with Max I/O performance mode for the Linux instances.  
B. Use Amazon FSx for Windows File Server for the Windows instances. Use Amazon FSx for Lustre for the Linux instances. Link both Amazon FSx file systems to the same Amazon S3 bucket.  
C. Use Amazon Elastic File System (Amazon EFS) with General Purpose performance mode for the Windows instances and the Linux instances  
D. Use Amazon FSx for Windows File Server for the Windows instances and the Linux instances.

**Correct Answer:**  
C. Use Amazon Elastic File System (Amazon EFS) with General Purpose performance mode for the Windows instances and the Linux instances

**Exam Question 425**

A company operates a two-tier application for image processing. The application uses two Availability Zones, each with one public subnet and one private subnet. An Application Load Balancer (ALB) for the web tier uses the public subnets.

Amazon EC2 instances for the application tier use the private subnets.

Users report that the application is running more slowly than expected. A security audit of the web server log files shows that the application is receiving millions of illegitimate requests from a small number of IP addresses. A solutions architect needs to resolve the immediate performance problem while the company investigates a more permanent solution.

What should the solutions architect recommend to meet this requirement?

A. Modify the inbound security group for the web tier. Add a deny rule for the IP addresses that are consuming resources.  
B. Modify the network ACL for the web tier subnets. Add an inbound deny rule for the IP addresses that are consuming resources.  
C. Modify the inbound security group for the application tier. Add a deny rule for the IP addresses that are consuming resources.  
D. Modify the network ACL for the application tier subnets. Add an inbound deny rule for the IP addresses that are consuming resources.

**Correct Answer:**  
A. Modify the inbound security group for the web tier. Add a deny rule for the IP addresses that are consuming resources.

**Exam Question 426**

A company is planning to migrate a TCP-based application into the company’s VPC. The application is publicly accessible on a nonstandard TCP port through a hardware appliance in the company’s data center. This public endpoint can process up to 3 million requests per second with low latency. The company requires the same level of performance for the new public endpoint in AWS.

What should a solutions architect recommend to meet this requirement?

A. Deploy a Network Load Balancer (NLB). Configure the NLB to be publicly accessible over the TCP port that the application requires.  
B. Deploy an Application Load Balancer (ALB). Configure the ALB to be publicly accessible over the TCP port that the application requires.  
C. Deploy an Amazon CloudFront distribution that listens on the TCP port that the application requires. Use an Application Load Balancer as the origin.  
D. Deploy an Amazon API Gateway API that is configured with the TCP port that the application requires. Configure AWS Lambda functions with provisioned concurrency to process the requests.

**Correct Answer:**  
C. Deploy an Amazon CloudFront distribution that listens on the TCP port that the application requires. Use an Application Load Balancer as the origin.

**Exam Question 427**

An eCommerce company is creating an application that requires a connection to a third-party payment service to process payments. The payment service needs to explicitly allow the public IP address of the server that is making the payment request. However, the company’s security policies do not allow any server to be exposed directly to the public internet.

Which solution will meet these requirements?

A. Provision an Elastic IP address. Host the application servers on Amazon EC2 instances in a private subnet. Assign the public IP address to the application servers.  
B. Create a NAT gateway in a public subnet. Host the application servers on Amazon EC2 instances in a private subnet. Route payment requests through the NAT gateway.  
C. Deploy an Application Load Balancer (ALB). Host the application servers on Amazon EC2 instances in a private subnet. Route the payment requests through the ALB.  
D. Set up an AWS Client VPN connection to the payment service. Host the application servers on Amazon EC2 instances in a private subnet. Route the payment requests through the VPN.

**Correct Answer:**  
B. Create a NAT gateway in a public subnet. Host the application servers on Amazon EC2 instances in a private subnet. Route payment requests through the NAT gateway.

**Exam Question 428**

A company is running an ASP.NET MVC application on a single Amazon EC2 instance. A recent increase in application traffic is causing slow response times for users during lunch hours. The company needs to resolve this concern with the least amount of configuration.

What should a solutions architect recommend to meet these requirements?

A. Move the application to AWS Elastic Beanstalk. Configure load-based auto scaling and time-based scaling to handle scaling during lunch hours.  
B. Move the application to Amazon Elastic Container Service (Amazon ECS). Create an AWS Lambda function to handle scaling during lunch hours.  
C. Move the application to Amazon Elastic Container Service (Amazon ECS). Configure scheduled scaling for AWS Application Auto Scaling during lunch hours.  
D. Move the application to AWS Elastic Beanstalk. Configure load-based auto scaling, and create an AWS Lambda function to handle scaling during lunch hours.

**Correct Answer:**  
A. Move the application to AWS Elastic Beanstalk. Configure load-based auto scaling and time-based scaling to handle scaling during lunch hours.

**Exam Question 429**

An online gaming company is designing a game that is expected to be popular all over the world. A solutions architect needs to define an AWS Cloud architecture that supports near-real-time recording and displaying of current game statistics for each player, along with the names of the top 25 players in the world, at any given time.

Which AWS database solution and configuration should the solutions architect use to meet these requirements?

A. Use Amazon RDS for MySQL as the data store for player activity. Configure the RDS DB instance for Multi-AZ support.  
B. Use Amazon DynamoDB as the data store for player activity. Configure DynamoDB Accelerator (DAX) for the player data.  
C. Use Amazon DynamoDB as the data store for player activity. Configure global tables in each required AWS Region for the player data.  
D. Use Amazon RDS for MySQL as the data store for player activity. Configure cross-region read replicas in each required AWS Region based on player proximity.

**Correct Answer:**  
D. Use Amazon RDS for MySQL as the data store for player activity. Configure cross-region read replicas in each required AWS Region based on player proximity.

**Exam Question 430**

A company uses Amazon RDS for PostgreSQL databases for its data tier. The company must implement password rotation for the databases.

Which solution meets this requirement with the LEAST operational overhead?

A. Store the password in AWS Secrets Manager. Enable automatic rotation on the secret.  
B. Store the password in AWS Systems Manager Parameter Store. Enable automatic rotation on the parameter.  
C. Store the password in AWS Systems Manager Parameter Store. Write an AWS Lambda function that rotates the password.  
D. Store the password in AWS Key Management Service (AWS KMS). Enable automatic rotation on the customer master key (CMK).

**Correct Answer:**  
A. Store the password in AWS Secrets Manager. Enable automatic rotation on the secret.

**Exam Question 431**

A company’s facility has badge readers at every entrance throughout the building. When badges are scanned, the readers send a message over HTTPS to indicate who attempted to access that particular entrance.

A solutions architect must design a system to process these messages from the sensors. The solution must be highly available, and the results must be made available for the company’s security team to analyze.

Which system architecture should the solutions architect recommend?

A. Launch an Amazon EC2 instance to serve as the HTTPS endpoint and to process the messages. Configure the EC2 instance to save the results to an Amazon S3 bucket.  
B. Create an HTTPS endpoint in Amazon API Gateway. Configure the API Gateway endpoint to invoke an AWS Lambda function to process the messages and save the results to an Amazon DynamoDB table.  
C. Use Amazon Route 53 to direct incoming sensor messages to an AWS Lambda function. Configure the Lambda function to process the messages and save the results to an Amazon DynamoDB table.  
D. Create a gateway VPC endpoint for Amazon S3. Configure a Site-to-Site VPN connection from the facility network to the VPC so that sensor data can be written directly to an S3 bucket by way of the VPC endpoint.

**Correct Answer:**  
B. Create an HTTPS endpoint in Amazon API Gateway. Configure the API Gateway endpoint to invoke an AWS Lambda function to process the messages and save the results to an Amazon DynamoDB table.

**Exam Question 432**

An Amazon EC2 instance is located in a private subnet in a new VPC. This subnet does not have outbound internet access, but the EC2 instance needs the ability to download monthly security updates from an outside vendor.

What should a solutions architect do to meet these requirements?

A. Create an internet gateway, and attach it to the VPC. Configure the private subnet route table to use the internet gateway as the default route.  
B. Create a NAT gateway, and place it in a public subnet. Configure the private subnet route table to use the NAT gateway as the default route.  
C. Create a NAT instance, and place it in the same subnet where the EC2 instance is located. Configure the private subnet route table to use the NAT instance as the default route.  
D. Create an internet gateway, and attach it to the VPC. Create a NAT instance, and place it in the same subnet where the EC2 instance is located. Configure the private subnet route table to use the internet gateway as the default route.

**Correct Answer:**  
A. Create an internet gateway, and attach it to the VPC. Configure the private subnet route table to use the internet gateway as the default route.

**Exam Question 433**

A company has been running a web application with an Oracle relational database in an on-premises data center for the past 15 years. The company must migrate the database to AWS. The company needs to reduce operational overhead without having to modify the application’s code.

Which solution meets these requirements?

A. Use AWS Database Migration Service (AWS DMS) to migrate the database servers to Amazon RDS.  
B. Use Amazon EC2 instances to migrate and operate the database servers.  
C. Use AWS Database Migration Service (AWS DMS) to migrate the database servers to Amazon DynamoDB.  
D. Use an AWS Snowball Edge Storage Optimized device to migrate the data from Oracle to Amazon Aurora.

**Correct Answer:**  
A. Use AWS Database Migration Service (AWS DMS) to migrate the database servers to Amazon RDS.

**Exam Question 434**

A company is running an application on Amazon EC2 instances. Traffic to the workload increases substantially during business hours and decreases afterward. The CPU utilization of an EC2 instance is a strong indicator of end-user demand on the application.

The company has configured an Auto Scaling group to have a minimum group size of 2 EC2 instances and a maximum group size of 10 EC2 instances.

The company is concerned that the current scaling policy that is associated with the Auto Scaling group might not be correct. The company must avoid over-provisioning EC2 instances and incurring unnecessary costs.

What should a solutions architect recommend to meet these requirements?

A. Configure Amazon EC2 Auto Scaling to use a scheduled scaling plan and launch an additional 8 EC2 instances during business hours.  
B. Configure AWS Auto Scaling to use a scaling plan that enables predictive scaling. Configure predictive scaling with a scaling mode of forecast and scale, and to enforce the maximum capacity setting during scaling.  
C. Configure a step scaling policy to add 4 EC2 instances at 50% CPU utilization and add another 4 EC2 instances at 90% CPU utilization. Configure scale-in policies to perform the reverse and remove EC2 instances based on the two values.  
D. Configure AWS Auto Scaling to have a desired capacity of 5 EC2 instances, and disable any existing scaling policies. Monitor the CPU utilization metric for 1 week. Then create dynamic scaling policies that are based on the observed values.

**Correct Answer:**  
D. Configure AWS Auto Scaling to have a desired capacity of 5 EC2 instances, and disable any existing scaling policies. Monitor the CPU utilization metric for 1 week. Then create dynamic scaling policies that are based on the observed values.

**Exam Question 435**

A company runs a web application that is backed by Amazon RDS. A new database administrator caused data loss by accidentally editing information in a database table. To help recover from this type of incident, the company wants the ability to restore the database to its state from 5 minutes before any change within the last 30 days.

Which feature should the solutions architect include in the design to meet this requirement?

A. Read replicas  
B. Manual snapshots  
C. Automated backups  
D. Multi-AZ deployments

**Correct Answer:**  
C. Automated backups

**Exam Question 436**

A company wants to use a custom distributed application that calculates various profit and loss scenarios. To achieve this goal, the company needs to provide a network connection between its Amazon EC2 instances. The connection must minimize latency and must maximize throughput

Which solution will meet these requirements?

A. Provision the application to use EC2 Dedicated Hosts of the same instance type.  
B. Configure a placement group for EC2 instances that have the same instance type.  
C. Use multiple AWS elastic network interfaces and link aggregation.  
D. Configure AWS PrivateLink for the EC2 instances.

**Correct Answer:**  
B. Configure a placement group for EC2 instances that have the same instance type.

**Exam Question 437**

A company designed a stateless two-tier application that uses Amazon EC2 in a single Availability Zone and an Amazon RDS Multi-AZ DB instance. New company management wants to ensure the application is highly available.

What should a solutions architect do to meet this requirement?

A. Configure the application to use Multi-AZ EC2 Auto Scaling and create an Application Load Balancer.  
B. Configure the application to take snapshots of the EC2 instances and send them to a different AWS Region.  
C. Configure the application to use Amazon Route 53 latency-based routing to feed requests to the application.  
D. Configure Amazon Route 53 rules to handle incoming requests and create a Multi-AZ Application Load Balancer.

**Correct Answer:**  
A. Configure the application to use Multi-AZ EC2 Auto Scaling and create an Application Load Balancer.

**Exam Question 438**

A company is developing a mobile game that streams score updates to a backend processor and then posts results on a leaderboard A solutions architect needs to design a solution that can handle large traffic spikes process the mobile game updates in order of receipt and store the processed updates in a highly available database. The company also wants to minimize the management overhead required to maintain the solution

What should the solutions architect do to meet these requirements?

A. Push score updates to Amazon Kinesis Data Streams Process the updates in Kinesis Data Streams with AWS Lambda Store the processed updates in Amazon DynamoDB  
B. Push score updates to Amazon Kinesis Data Streams Process the updates with a fleet of Amazon EC2 instances set up for Auto Scaling Store the processed updates in Amazon Redshift  
C. Push score updates to an Amazon Simple Notification Service (Amazon SNS) topic Subscribe an AWS Lambda function to the SNS topic to process the updates Store the processed updates in a SQL database running on Amazon EC2  
D. Push score updates to an Amazon Simple Queue Service (Amazon SQS) queue Use a fleet of Amazon EC2 instances with Auto Scaling to process the updates in the SQS queue Store the processed updates in an Amazon RDS Multi-AZ DB instance

**Correct Answer:**  
A. Push score updates to Amazon Kinesis Data Streams Process the updates in Kinesis Data Streams with AWS Lambda Store the processed updates in Amazon DynamoDB

**Exam Question 439**

A company maintains about 300 TB in Amazon S3 Standard storage month after month. The S3 objects are each typically around 50 GB in size and are frequently replaced with multipart uploads by their global application. The number and size of S3 objects remain constant but the company’s S3 storage costs are increasing each month.

How should a solutions architect reduce costs in this situation?

A. Switch from multipart uploads to Amazon S3 Transfer Acceleration  
B. Enable an S3 Lifecycle policy that deletes incomplete multipart uploads  
C. Configure S3 inventory to prevent objects from being archived too quickly  
D. Configure Amazon CloudFront to reduce the number of objects stored in Amazon S3

**Correct Answer:**  
B. Enable an S3 Lifecycle policy that deletes incomplete multipart uploads

**Exam Question 440**

A computer is reviewing a recent migration of a three-tier application to a VPC. The security team discover that the principle of least privilege is not being applied to Amazon EC2 security group ingress and egress rules between the application tiers.

What should a solution architect do to connect issue?

A. Create security group rules using the instance ID as the source destination.  
B. Create security group rules using the security ID as the source or destination.  
C. Create security group rules using the VPC CDR blocks as the source or destination  
D. Create security group rules using the subnet CDR blocks as the source or destination

**Correct Answer:**  
A. Create security group rules using the instance ID as the source destination.

**Exam Question 441**

A company processes large amounts of data. The output data is stored in Amazon S3 Standard storage in an S3 bucket, where it is analyzed for 1 month. The data must remain immediately accessible after the 1-month analysis period.

Which storage solution meets these requirements MOST cost-effectively?

A. Configure an S3 Lifecycle policy to transition the objects to S3 Glacier after 30 days.  
B. Configure S3 Intelligent-Tiering to transition the objects to S3 Glacier after 30 days.  
C. Configure an S3 Lifecycle policy to transition the objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.  
D. Configure an S3 Lifecycle policy to delete the objects after 30 days. Enable versioning on the S3 bucket so that deleted objects can still be immediately restored as needed.

**Correct Answer:**  
B. Configure S3 Intelligent-Tiering to transition the objects to S3 Glacier after 30 days.

**Exam Question 442**

A social media company is building a feature for its website. The feature will give users the ability to upload photos. The company expects significant increases in demand during large events and must ensure that the website can handle the upload traffic from users.

Which solution meets these requirements with the MOST scalability?

A. Upload files from the user’s browser to the application servers Transfer the files to an Amazon S3 bucket.  
B. Provision an AWS Storage Gateway file gateway. Upload files directly from the user’s browser to the file gateway.  
C. Generate Amazon S3 presigned URLs in the application. Upload files directly from the user’s browser into an S3 bucket  
D. Provision an Amazon Elastic File System (Amazon EFS) file system. Upload files directly from the user’s browser to the file system.

**Correct Answer:**  
C. Generate Amazon S3 presigned URLs in the application. Upload files directly from the user’s browser into an S3 bucket

**Exam Question 443**

A development team needs to host a website that will be accessed by other teams. The website contents consist of HTML. CSS, client-side JavaScript, and images.

Which method is the MOST cost-effective for hosting the website?

A. Containerize the website and host it in AWS Fargate.  
B. Create an Amazon S3 bucket and host the website there  
C. Deploy a web server on an Amazon EC2 instance to host the website.  
D. Configure an Application Load Balancer with an AWS Lambda target that uses the Express js framework.

**Correct Answer:**  
B. Create an Amazon S3 bucket and host the website there

**Exam Question 444**

A company hosts an application on multiple Amazon EC2 instances. The application processes messages from an Amazon SQS queue writes to an Amazon RDS table and deletes the message from the queue Occasional duplicate records are found in the RDS table. The SQS queue does not contain any duplicate messages.

What should a solutions architect do to ensure messages are being processed once only?

A. Use the CreateQueue API call to create a new queue  
B. Use the Add Permission API call to add appropriate permissions  
C. Use the ReceiveMessage API call to set an appropriate wail time  
D. Use the ChangeMessageVisibility API call to increase the visibility timeout

**Correct Answer:**  
D. Use the ChangeMessageVisibility APi call to increase the visibility timeout

**Exam Question 445**

An application runs on Amazon EC2 instances in private subnets. The application needs to access an Amazon DynamoDB table.

What is me MOST secure way to access the table while ensuring that the traffic does not leave the AWS network?

A. Use a VPC endpoint for DynamoDB  
B. Use a NAT gateway in a public subnet  
C. Use a NAT instance in a private subnet  
D. Use the internet gateway attached to the VPC

**Correct Answer:**  
A. Use a VPC endpoint for DynamoDB

**Exam Question 446**

A social media company allows users to upload images to its website. The website runs on Amazon EC2 instances. During upload requests, the website resizes the images to a standard size and stores the resized images in Amazon S3. Users are experiencing slow upload requests to the website.

The company needs to reduce coupling within the application and improve website performance A solutions architect must design the most operationally efficient process for image uploads.

Which combination of actions should the solutions architect take to meet these requirements? (Select TWO.)

A. Configure the application to upload images to S3 Glacier.  
B. Configure the web server to upload the original images to Amazon S3.  
C. Configure the application to upload images directly from each user’s browser to Amazon S3 through the use of a presigned UR  
D. Configure S3 Event Notifications to invoke an AWS Lambda function when an image is uploaded. Use the function to resize the image  
E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function on a schedule to resize uploaded images.

**Correct Answer:**  
D. Configure S3 Event Notifications to invoke an AWS Lambda function when an image is uploaded. Use the function to resize the image

**Exam Question 447**

A company’s security team requests that network traffic be captured in VPC Flow Logs. The logs will be frequently accessed for 90 days and then accessed intermittently.

What should a solutions architect do to meet these requirements when configuring the logs?

A. Use Amazon CloudWatch as the target. Set the CloudWatch log group with an expiration of 90 days.  
B. Use Amazon Kinesis as the target Configure the Kinesis stream to always retain the logs for 90 days  
C. Use AWS CloudTrail as the target. Configure CloudTrail to save to an Amazon S3 bucket, and enable S3 Intelligent-Tiering  
D. Use Amazon S3 as the target Enable an S3 Lifecycle policy to transition the logs to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days

**Correct Answer:**  
D. Use Amazon S3 as the target Enable an S3 Lifecycle policy to transition the logs to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days

**Exam Question 448**

A company needs to provide its employees with secure access to confidential and sensitive files. The company wants to ensure that the tiles can be accessed only by authorized users. The files must be downloaded securely to the employees’ devices.

The tiles are stored in an on-premises Windows file server. However, due to an increase in remote usage, the file server is running out of capacity.

Which solution will meet these requirements?

A. Migrate the file server to an Amazon EC2 instance in a public subnet. Configure the security group to limit inbound traffic to the employees’ IP addresses.  
B. Migrate the files to an Amazon FSx for Windows File Server file system. Integrate the Amazon FSx file system with the on-premises Active Directory. Configure AWS Client VP  
C. Migrate the tiles to Amazon S3, and create a private VPC endpoint. Create a signed URL to allow download.  
D. Migrate the tiles to Amazon S3, and create a public VPC endpoint. Allow employees to sign on with AWS Single Sign-On.

**Correct Answer:**  
D. Migrate the tiles to Amazon S3, and create a public VPC endpoint. Allow employees to sign on with AWS Single Sign-On.

**Exam Question 449**

A company uses a payment processing system that requires messages for a particular payment ID to be received in the same order that they were sent Otherwise, the payments might be processed incorrectly.

Which actions should a solutions architect take to meet this requirement? (Select TWO.)

A. Write the messages to an Amazon DynamoDB table with the payment ID as the partition key  
B. Write the messages to an Amazon Kinesis data stream with the payment ID as the partition key.  
C. Write the messages to an Amazon ElastiCache for Memcached cluster with the payment ID as the key  
D. Write the messages to an Amazon Simple Queue Service (Amazon SQS) queue Set the message attribute to use the payment ID  
E. Write the messages to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the message group to use the payment ID

**Correct Answer:**  
A. Write the messages to an Amazon DynamoDB table with the payment ID as the partition key  
E. Write the messages to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the message group to use the payment ID

**Exam Question 450**

A company is concerned about the security of its public web application due to recent web attacks. The application uses an Application Load Balancer (ALB). A solutions architect must reduce the risk of DDoS attacks against the application

What should the solutions architect do to meet this requirement?

A. Add an Amazon Inspector agent to the ALB  
B. Configure Amazon Made to prevent attacks.  
C. Enable AWS Shield Advanced to prevent attacks.  
D. Configure Amazon GuardDuty to monitor the ALB

**Correct Answer:**  
C. Enable AWS Shield Advanced to prevent attacks.

#### Exam Question 451

A company is launching a new application that will be hosted on Amazon EC2 instances. A solutions architect needs to design a solution that does not allow public IPv4 access that originates from the internet. However, the solution must allow the EC2 instances to make outbound IPv4 internet requests.

The initial design proposal shows that the EC2 instances would be located in two private subnets across two Availability Zones.

The entire architecture must be highly available.

How should the solutions architect change the architecture to meet these requirements?

A. Deploy a NAT gateway in public subnets in both Availability Zones. Create and configure one route table for each private subnet.  
B. Deploy an internet gateway in public subnets in both Availability Zones. Create and configure a shared route table for the private subnets.  
C. Deploy a NAT gateway in public subnets in both Availability Zones. Create and configure a shared route table for the private subnets.  
D. Deploy an egress-only internet gateway in public subnets in both Availability Zones. Create and configure one route table for each private subnet.

**Correct Answer:**  
C. Deploy a NAT gateway in public subnets in both Availability Zones. Create and configure a shared route table for the private subnets.

#### Exam Question 452

A company has deployed a multiplayer game for mobile devices. The game requires live location tracking of players based on latitude and longitude. The data store for the game must support rapid updates and retrieval of locations.

The game uses an Amazon RDS for PostgreSQL DB instance with read replicas to store the location data. During peak usage periods, the database is unable to maintain the performance that is needed for reading and writing updates. The game’s user base is increasing rapidly.

What should a solutions architect do to improve the performance of the data tier?

A. Take a snapshot of the existing DB instance. Restore the snapshot with Multi-AZ enabled.  
B. Migrate from Amazon RDS to Amazon Elasticsearch Service (Amazon ES) with Kibana.  
C. Deploy Amazon DynamoDB Accelerator (DAX) in front of the existing DB instance. Modify the game to use DA  
D. Deploy an Amazon ElastiCache for Redis cluster in front of the existing DB instance. Modify the game to use Redis.

**Correct Answer:**  
D. Deploy an Amazon ElastiCache for Redis cluster in front of the existing DB instance. Modify the game to use Redis.

#### Exam Question 453

A company is automating an order management application. The company’s development team has decided to use SFTP to transfer and store the business-critical information files. The files must be encrypted and must be highly available. The files also must be automatically deleted a month after they are created.

Which solution meets these requirements with the LEAST operational overhead?

A. Configure an Amazon S3 bucket with encryption enabled. Use AWS transfer for SFTP to securely transfer the files to the S3 bucket Apply an AWS Transfer for SFTP file retention policy to delete the files after a month  
B. Install an SFTP service on an Amazon EC2 instance Mount an Amazon Elastic File System (Amazon EFS) file share on the EC2 instance. Enable cron to delete the files after a month  
C. Configure an Amazon Elastic File System (Amazon EFS) file system with encryption enabled. Use AWS Transfer for SFTP to securely transfer the files to the EFS file system. Apply an EFS lifecycle policy to automatically delete the files after a month.  
D. Configure an Amazon S3 bucket with encryption enabled. Use AWS Transfer for SFTP to securely transfer the files to the S3 bucket. Apply S3 Lifecycle rules to automatically delete the files after a month.

**Correct Answer:**  
D. Configure an Amazon S3 bucket with encryption enabled. Use AWS Transfer for SFTP to securely transfer the files to the S3 bucket. Apply S3 Lifecycle rules to automatically delete the files after a month.

#### Exam Question 454

Organizers for a global event want to put daily reports online as static HTML pages. The pages are expected to generate millions of views from users around the work. 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?

A. Generate presigned URLs for the files  
B. Use cross-Region replication to all Regions  
C. Use the geoproximity feature of Amazon Route 53  
D. Use Amazon CloudFront with the S3 bucket as its origin

**Correct Answer:**  
D. Use Amazon CloudFront with the S3 bucket as its ongin

#### Exam Question 455

A company needs a storage solution for an application that runs on a high performance computing (HPC) cluster. The cluster is hosted on AWS Fargate for Amazon Elastic Container Service (Amazon ECS). The company needs a mountable file system that provides concurrent access to files while delivering hundreds of Gbps of throughput at sub-millisecond latencies

Which solution meets these requirements?

A. Create an Amazon FSx for Lustre file share for the application data Create an IAM role that allows Fargate to access the FSx for Lustre file share  
B. Create an Amazon Elastic File System (Amazon EFS) file share for the application data. Create an IAM role that allows Fargate to access the EFS file share.  
C. Create an Amazon S3 bucket for the application data. Create an S3 bucket policy that allows Fargate to access the S3 bucket  
D. Create an Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS SSD (io2) volume for the application data Create an IAM role that allows Fargate to access the volume.

**Correct Answer:**  
A. Create an Amazon FSx for Lustre file share for the application data Create an IAM role that allows Fargate to access the FSx for Lustre file share

#### Exam Question 456

A company hosts historical weather records in Amazon S3. The records are downloaded from the company’s website by way of a URL that resolves to a domain name Users all over the world access this content through subscriptions A third-party provider hosts the company’s root domain name, but the company recently migrated some of its services to Amazon Route 53. The company wants to consolidate contracts, reduce latency for users, and reduce costs related to serving the application to subscribers

Which solution meets these requirements?

A. Create a web distribution on Amazon CloudFront to serve the S3 content for the application Create a CNAME record in a Route 53 hosted zone that points to the CloudFront distribution, resolving to the application’s URL domain name.  
B. Create a web distribution on Amazon CloudFront to serve the S3 content for the application. Create an ALIAS record in the Amazon Route 53 hosted zone that points to the CloudFront distribution, resolving to the application’s URL domain name.  
C. Create an A record in a Route 53 hosted zone for the application. Create a Route 53 traffic policy for the web application, and configure a geolocation rule Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.  
D. Create an A record in a Route 53 hosted zone for the application Create a Route 53 traffic policy for the web application, and configure a geoproximity rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.

**Correct Answer:**  
C. Create an A record in a Route 53 hosted zone for the application. Create a Route 53 traffic policy for the web application, and configure a geolocation rule Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.

#### Exam Question 457

A solutions architect is optimizing a website for an upcoming musical event Videos of the performances will be streamed in real-time and then will be available on demand. The event is expected to attract a global online audience

Which service will improve the performance of both real-time and on-demand streaming?

A. Amazon CloudFront  
B. AWS Global Accelerator  
C. Amazon Route 53  
D. Amazon S3 Transfer Acceleration

**Correct Answer:**  
A. Amazon CloudFront

**Answer Description:**  
Amazon CloudFront can be used to stream video to users across the globe using a wide variety of protocols that are layered on top of HTTP. This can include both on-demand video as well as real-time streaming video.

CORRECT: “Amazon CloudFront” is the correct answer.

INCORRECT: “AWS Global Accelerator” is incorrect as this would be an expensive way of getting the content closer to users compared to using CloudFront. As this is a use case for CloudFront and there are so many edge locations it is the better option.

INCORRECT: “Amazon Route 53” is incorrect as you still need a solution for getting the content closer to users.

INCORRECT: “Amazon S3 Transfer Acceleration” is incorrect as this is used to accelerate uploads of data to Amazon S3 buckets.

**References:**

* [Amazon CloudFront media streaming tutorials](https://aws.amazon.com/cloudfront/streaming/)
* Amazon CloudFront > Developer Guide > [Video on Demand and Live Streaming Video with CloudFront](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/on-demand-streaming-video.html)

#### Exam Question 458

A company wants to build an online marketplace application on AWS as a set of loosely coupled microservices For this application, when a customer submits a new order two microservices should handle the event simultaneously. The Email microservice will send a confirmation email and the order processing microservice will start the order delivery process If a customer cancels an order, the order cancellation and Email microservices should handle the event simultaneously.

A solutions architect wants to use Amazon Simple Queue Service (Amazon SQS) and Amazon Simple Notification Service (Amazon SNS) to design the messaging between the microservices.

How should the solutions architect design the solution?

A. Create a single SOS queue and publish order events to it. The Email, OrderProcessing and OrderCancellation microservices can then consume messages off the queue  
B. Create three SNS topics for each microservice Publish order events to the three topics Subscribe each of the Email OrderProcessmg, and OrderCancellation microservices to its own topic  
C. Create an SNS topic and publish order events to it Create three SQS queues for the Email OrderProcessing and OrderCancellation microservices Subscribe all SQS queues to the SNS topic with message filtering  
D. Create two SQS queues and publish order events to both queues simultaneously One queue is for the Email and OrderProcessmg microservices. The second queue is for the Email and Order Cancellation microservices

**Correct Answer:**  
C. Create an SNS topic and publish order events to it Create three SQS queues for the Email OrderProcessing and OrderCancellation microservices Subscribe all SQS queues to the SNS topic with message filtering

#### Exam Question 459

A company is developing a mobile game that streams score updates to a backend processor and then posts results on a leaderboard A solutions architect needs to design a solution that can handle large traffic spikes process the mobile game updates in order of receipt and store the processed updates in a highly available database. The company also wants to minimize the management overhead required to maintain the solution

What should the solutions architect do to meet these requirements?

A. Push score updates to Amazon Kinesis Data Streams Process the updates in Kinesis Data Streams with AWS Lambda Store the processed updates in Amazon DynamoDB  
B. Push score updates to Amazon Kinesis Data Streams Process the updates with a fleet of Amazon EC2 instances set up for Auto Scaling Store the processed updates in Amazon Redshift  
C. Push score updates to an Amazon Simple Notification Service (Amazon SNS) topic Subscribe an AWS Lambda function to the SNS topic to process the updates Store the processed updates in a SQL database running on Amazon EC2  
D. Push score updates to an Amazon Simple Queue Service (Amazon SQS) queue Use a fleet of Amazon EC2 instances with Auto Scaling to process the updates in the SQS queue Store the processed updates in an Amazon RDS Multi-AZ DB instance

**Correct Answer:**  
A. Push score updates to Amazon Kinesis Data Streams Process the updates in Kinesis Data Streams with AWS Lambda Store the processed updates in Amazon DynamoDB

**Answer Description:**  
You can use Amazon Kinesis Data Streams to collect and process large streams of data records in real-time. You can use Kinesis Data Streams for rapid and continuous data intake and aggregation. The type of data used can include IT infrastructure log data, application logs, social media, market data feeds, and web clickstream data. Because the response time for the data intake and processing is in real-time, the processing is typically lightweight.

#### Exam Question 460

A company has two VPCs that are located in the us-west-2 Region within the same AWS account. The company needs to allow network traffic between these VPCs. Approximately 500 GB of data transfer will occur between the VPCs each month.

What is the MOST cost-effective solution to connect these VPCs?

A. Implement AWS Transit Gateway to connect the VPCs Update the route tables of each VPC to use the transit gateway for inter-VPC communication  
B. Implement an AWS Site-to-Site VPN tunnel between the VPCs. Update the route tables of each VPC to use the VPN tunnel for inter-VPC communication  
C. Set up a VPC peering connection between the VPCs. Update the route tables of each VPC to use the VPC peering connection for inter-VPC communication.  
D. Set up a 1 GB AWS Direct Connect connection between the VPCs. Update the route tables of each VPC to use the Direct Connect connection for inter-VPC communication.

**Correct Answer:**  
C. Set up a VPC peering connection between the VPCs. Update the route tables of each VPC to use the VPC peering connection for inter-VPC communication.

**Exam Question 461**

A company has three AWS accounts Management Development and Production. These accounts use AWS services only in the us-east-1 Region All accounts have a VPC with VPC Flow Logs configured to publish data to an Amazon S3 bucket in each separate account For compliance reasons the company needs an ongoing method to aggregate all the VPC flow logs across all accounts into one destination S3 bucket in the Management account.

What should a solutions architect do to meet these requirements with the LEAST operational overhead?

A. Add S3 Same-Region Replication rules in each S3 bucket that stores VPC flow logs to replicate objects to the destination S3 bucket Configure the destination S3 bucket to allow objects to be received from the S3 buckets in other accounts  
B. Set up an 1AM user in the Management account Grant permissions to the 1AM user to access the S3 buckets that contain the VPC flow logs Run the aws s3 sync command in the AWS CLI to copy the objects to the destination S3 bucket  
C. Use an S3 inventory report to specify which objects in the S3 buckets to copy Perform an S3 batch operation to copy the objects into the destination S3 bucket in the Management account with a single request.  
D. Create an AWS Lambda function in the Management account Grant S3 GET permissions on the source S3 buckets Grant S3 PUT permissions on the destination S3 bucket Configure the function to invoke when objects are loaded in the source S3 buckets

**Correct Answer:**  
A. Add S3 Same-Region Replication rules in each S3 bucket that stores VPC flow logs to replicate objects to the destination S3 bucket Configure the destination S3 bucket to allow objects to be received from the S3 buckets in other accounts

**Exam Question 462**

A company is building a web application that serves a content management system. The content management system runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The EC2 instances run in an Auto Scaling group across multiple Availability Zones Users are constantly adding and updating files blogs and other website assets in the content management system.

A solutions architect must implement a solution in which all the EC2 instances share up-to-date website content with the least possible lag time.

Which solution meets these requirements?

A. Update the EC2 user data in the Auto Scaling group lifecycle policy to copy the website assets from the EC2 instance that was launched most recently Configure the ALB to make changes to the website assets only m the newest EC2 instance  
B. Copy the website assets to an Amazon Elastic File System (Amazon EFS) file system Configure each EC2 instance to mount the EPS file system locally Configure the website hosting application to reference the website assets that are stored in the EFS file system  
C. Copy the website assets to an Amazon S3 bucket Ensure that each EC2 instance downloads the website assets from the S3 bucket to the attached Amazon Elastic Block Store (Amazon EBS) volume Run the S3 sync command once each hour to keep files up to date  
D. Restore an Amazon Elastic Block Store (Amazon EBS) snapshot with the website assets Attach the EBS snapshot as a secondary EBS volume when a new EC2 instance is launched Configure the website hosting application to reference the website assets that are stored in the secondary EBS volume

**Correct Answer:**  
A. Update the EC2 user data in the Auto Scaling group lifecycle policy to copy the website assets from the EC2 instance that was launched most recently Configure the ALB to make changes to the website assets only m the newest EC2 instance

**Exam Question 463**

A solutions architect is designing the architecture for a new web application. The application will run on AWS Fargate containers with an Application Load Balancer (ALB) and an Amazon Aurora PostgreSQL database. The web application will perform primarily read queries against the database.

What should the solutions architect do to ensure that the website can scale with increasing traffic? (Select TWO.)

A. Enable auto scaling on the ALB to scale the load balancer horizontally.  
B. Configure Aurora Auto Scaling to adjust the number of Aurora Replicas in the Aurora cluster dynamically.  
C. Enable cross-zone load balancing on the ALB to distribute the load evenly across containers in all Availability Zones.  
D. Configure an Amazon Elastic Container Service (Amazon ECS) cluster in each Availability Zone to distribute the load across multiple Availability Zones.  
E. Configure Amazon Elastic Container Service (Amazon ECS) Service Auto Scaling with a target tracking scaling policy that is based on CPU utilization.

**Correct Answer:**  
A. Enable auto scaling on the ALB to scale the load balancer horizontally.  
B. Configure Aurora Auto Scaling to adjust the number of Aurora Replicas in the Aurora cluster dynamically.

**Exam Question 464**

The application’s traffic is often low. but it occasionally grows significantly. During these sudden increases in traffic, DynamoDB returns throttling errors. The result is that error pages are displayed to end users.

What should a solutions architect do to reduce these errors?

A. Change the DynamoDB table to use on-demand capacity mode.  
B. Create a DynamoDB read replica to scale the read traffic horizontally.  
C. Purchase DynamoDB reserved capacity of 1,000 RCUs and 500 WCUs.  
D. Configure the application to use strongly consistent reads for DynamoDB queries.

**Correct Answer:**  
D. Configure the application to use strongly consistent reads for DynamoDB queries.

**Exam Question 465**

A company wants to build an immutable infrastructure for its software applications. The company wants to test the software applications before sending traffic to them. The company seeks an efficient solution that limits the effects of application bugs

Which combination of steps should a solutions architect recommend? {Select TWO)

A. Use AWS Cloud Formation to update the production infrastructure and roll back the stack if the update fails  
B. Apply Amazon Route 53 weighted routing to test the staging environment and gradually increase the traffic as the tests pass  
C. Apply Amazon Route 53 failover routing to test the staging environment and fail over to the production environment if the tests pass  
D. Use AWS Cloud Formation with a parameter set to the staging value in a separate environment other than the production environment  
E. Use AWS Cloud Formation to deploy the staging environment with a snapshot deletion policy and reuse the resources in the production environment if the tests pass

**Correct Answer:**  
A. Use AWS Cloud Formation to update the production infrastructure and roll back the stack if the update fails  
B. Apply Amazon Route 53 weighted routing to test the staging environment and gradually increase the traffic as the tests pass

**Exam Question 466**

A company stores project information in a shared spreadsheet. The company wants to create a web application to replace the spreadsheet. The company has chosen Amazon DynamoDB to store the spreadsheet’s data and is designing the web application to display the project information that is obtained from DynamoDB.

A solutions architect must design the web application’s backend by using managed services that require minimal operational maintenance.

Which architectures meet these requirements? (Select TWO.)

A. An Amazon API Gateway REST API accesses the project information that is in DynamoD  
B. An Elastic Load Balancer forwards requests to a target group with DynamoDB set up as the target.  
C. An Amazon API Gateway REST API invokes an AWS Lambda function. The Lambda function accesses DynamoD  
D. An Amazon Route 53 hosted zone routes requests to an AWS Lambda endpoint to invoke a Lambda function that accesses DynamoD  
E. An Elastic Load Balancer forwards requests to a target group of Amazon EC2 instances. The EC2 instances run an application that accesses DynamoD

**Correct Answer:**  
A. An Amazon API Gateway REST API accesses the project information that is in DynamoD  
E. An Elastic Load Balancer forwards requests to a target group of Amazon EC2 instances. The EC2 instances run an application that accesses DynamoD

**Exam Question 467**

A solution architect at a company is designing the architecture for a two-tiered web application. The web application is composed of an internet facing application load balancer that forwards traffic to an auto scaling group of Amazon EC2 instances. The EC2 instances must be able to access a database that runs on Amazon RDS.

The company has requested a defense-in-depth approach to the network layout. The company does not want to rely solely on security groups or network ACLs. Only the minimum resources that are necessary should be routable from the internet.

Which network design should the solutions architect recommend to meet these requirements?

A. Place the ALB, EC2 instances and RDS database in private subnets.  
B. Place the ALB in public subnets. Place the EC2 instances and RDS database in private subnets  
C. Place the ALB and EC2 instances in public subnets. Place the RDS database in private subnets  
D. Place the ALB outside the VP  
E. Place the EC2 instances and RDS database in private subnets.

**Correct Answer:**  
B. Place the ALB in public subnets. Place the EC2 instances and RDS database in private subnets

**Exam Question 468**

A company has thousands of edge devices that collectively generate 1 TB of status averts each day Each alert s approximately 2 KB in size. A solutions architect needs to implement a solution to ingest and store the alerts for future analysis.

The company wants a highly available solution However the company needs to minimize costs and does not want to manage additional infrastructure Additionally, the company wants to keep 14 days of data available for immediate analysis and archive any data older than 14 days.

What is the MOST operationally efficient solution that meets these requirements?

A. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon S3 bucket Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days  
B. Launch Amazon EC2 instances across two Availability Zones and place them behind an Elastic Load Balancer to ingest the alerts Create a script on the EC2 instances that will store the alerts m an Amazon S3 bucket Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days  
C. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon Elasticsearch Service (Amazon ES) duster Set up the Amazon ES cluster to take manual snapshots every day and delete data from the duster that is older than 14 days  
D. Create an Amazon Simple Queue Service (Amazon SQS I standard queue to ingest the alerts and set the message retention period to 14 days Configure consumers to poll the SQS queue check the age of the message and analyze the message data as needed If the message is 14 days old the consumer should copy the message to an Amazon S3 bucket and delete the message from the SQS queue

**Correct Answer:**  
A. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon S3 bucket Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days

**Exam Question 469**

A company has a customer relationship management (CRM) application that stores data in an Amazon RDS DB instance that runs Microsoft SQL Server. The company’s IT staff has administrative access to the database. The database contains sensitive data. The company wants to ensure that the data is not accessible to the IT staff and that only authorized personnel can view the data.

What should a solutions architect do to secure the data?

A. Use client-side encryption with an Amazon RDS managed key.  
B. Use client-side encryption with an AWS Key Management Service (AWS KMS) customer managed key.  
C. Use Amazon RDS encryption with an AWS Key Management Service (AWS KMS) default encryption key.  
D. Use Amazon RDS encryption with an AWS Key Management Service (AWS KMS) customer managed key.

**Correct Answer:**  
D. Use Amazon RDS encryption with an AWS Key Management Service (AWS KMS) customer managed key.

**Exam Question 470**

A company is developing a serverless web application that gives users the ability to interact with real-time analytics from online games. The data from the games must be streamed in real time. The company needs a durable, low-latency database option for user data. The company does not know how many users will use the application Any design considerations must provide response times of single-digit milliseconds as the application scales.

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

A. Amazon CloudFront  
B. Amazon DynamoDB  
C. Amazon Kinesis  
D. Amazon RDS  
E. AWS Global Accelerator

**Correct Answer:**  
A. Amazon CloudFront  
B. Amazon DynamoDB

**Exam Question 471**

A medical records company is hosting an application on Amazon EC2 instances. The application processes customer data files that are stored on Amazon S3. The EC2 instances are hosted in public subnets. The EC2 instances access Amazon S3 over the internet, but they do not require any other network access.

A new requirement mandates that the network traffic for file transfers take a private route and not be sent over the internet.

Which change to the network architecture should a solutions architect recommend to meet this requirement?

A. Create a NAT gateway. Configure the route table for the public subnets to send traffic to Amazon S3 through the NAT gateway.  
B. Configure the security group for the EC2 instances to restrict outbound traffic so that only traffic to the S3 prefix list is permitted.  
C. Move the EC2 instances to private subnets. Create a VPC endpoint for Amazon S3, and link the endpoint to the route table for the private subnets  
D. Remove the internet gateway from the VP  
E. Set up an AWS Direct Connect connection, and route traffic to Amazon S3 over the Direct Connect connection.

**Correct Answer:**  
C. Move the EC2 instances to private subnets. Create a VPC endpoint for Amazon S3, and link the endpoint to the route table for the private subnets

**Exam Question 472**

A company is implementing new data retention policies for all databases that run on Amazon RDS DB instances. The company must retain daily backups for a minimum period of 2 years. The backups must be consistent and restorable.

Which solution should a solutions architect recommend to meet these requirements?

A. Create a backup vault in AWS Backup to retain RDS backups. Create a new backup plan with a daily schedule and an expiration period of 2 years after creation. Assign the RDS DB instances to the backup plan. Configure a backup window for the RDS DB Instances for daily snapshots. Assign a snapshot retention policy of 2 years to each RDS DB instance. Use Amazon Data Lifecycle Manager (Amazon DLM)  
B. to schedule snapshot deletions.  
C. Configure database transaction logs to be automatically backed up to Amazon CloudWatch Logs with an expiration period of 2 years  
D. Configure an AWS Database Migration Service (AWS DMS) replication task. Deploy a replication instance, and configure a change data capture (CDC) task to stream database changes to Amazon S3 as the target Configure S3 Lifecycle policies to delete the snapshots after 2 years.

**Correct Answer:**  
A. Create a backup vault in AWS Backup to retain RDS backups. Create a new backup plan with a daily schedule and an expiration period of 2 years after creation. Assign the RDS DB instances to the backup plan. Configure a backup window for the RDS DB Instances for daily snapshots. Assign a snapshot retention policy of 2 years to each RDS DB instance. Use Amazon Data Lifecycle Manager (Amazon DLM)

**Exam Question 473**

The following IAM policy is attached to an IAM group.  
  
This is the only policy applied to the group.

What are the effective IAM permissions of this policy for group members?

A. Group members are permitted any Amazon EC2 action within the us-east-1 Region. Statements after the Allow permission are not applied.  
B. Group members are denied any Amazon EC2 permissions in the us-east-1 Region unless they are logged in with multi-factor authentication (MFA).  
C. Group members are allowed the ec2 Stoplnstances and ec2. TerminateInstances permissions for all Regions when logged in with multi-factor authentication (MFA) Group members are permitted any other Amazon EC2 action.  
D. Group members are allowed the ec2 Stoplnstances and ec2. Terminate instances permissions for the us-east-1 Region only when logged in with multi-factor authentication (MFA) Group members are permitted any other Amazon EC2 action within the us-east-1 Region.

**Correct Answer:**  
D. Group members are allowed the ec2 Stoplnstances and ec2. Terminate instances permissions for the us-east-1 Region only when logged in with multi-factor authentication (MFA) Group members are permitted any other Amazon EC2 action within the us-east-1 Region.

**Exam Question 474**

A company runs an AWS Lambda function in private subnets in a VPC. The subnets have a default route to the internet through an Amazon EC2 NAT instance. The Lambda function processes input data and saves its output as an object to Amazon S3 intermittently the Lambda function times out while trying to upload the object because of saturated traffic on the NAT instance’s network. The company wants to access Amazon S3 without traversing the internet

Which solution will meet these requirements?

A. Replace the fcC2 NAT instance with an AWS managed NAT gateway  
B. Increase the size of the EC2 NAT instance in the VPC to a network optimized instance type  
C. Provision a gateway endpoint for Amazon S3 in the VPC Update the route tables of the subnets accordingly  
D. Provision a transit gateway Place transit gateway attachments in the private subnets where the Lambda function is running

**Correct Answer:**  
B. Increase the size of the EC2 NAT instance in the VPC to a network optimized instance type

**Exam Question 475**

A solution architect is creating a new Amazon CloudFront distribution for an application Some of Ine information submitted by users is sensitive. The application uses HTTPS but needs another layer” of security. The sensitive information should be protected throughout the entire application stack end access to the information should be restricted to certain applications

Which action should the solutions architect take?

A. Configure a CloudFront signed URL  
B. Configure a CloudFront signed cookie.  
C. Configure a CloudFront field-level encryption profile  
D. Configure CloudFront and set the Origin Protocol Policy setting to HTTPS Only for the Viewer Protocol Policy

**Correct Answer:**  
C. Configure a CloudFront field-level encryption profile

**Exam Question 476**

A company is deploying a two-tier web application in a VPC. The web tier is using an Amazon EC2 Auto Scaling group with public subnets that span multiple Availability Zones. The database tier consists of an Amazon RDS for MySQL DB instance in separate private subnets. The web tier requires access to the database to retrieve product information.

The web application is not working as intended. The web application reports that it cannot connect to the database. The database is confirmed to be up and running. All configurations for the network ACLs. security groups, and route tables are still in their default states.

What should a solutions architect recommend to fix the application?

A. Add an explicit rule to the private subnet’s network ACL to allow traffic from the web tier’s EC2 instances.  
B. Add a route in the VPC route table to allow traffic between the web tier’s EC2 instances and The database tier.  
C. Deploy the web tier’s EC2 instances and the database tier’s RDS instance into two separate VPCs. and configure VPC peering.  
D. Add an inbound rule to the security group of the database tier’s RDS instance to allow traffic from the web tier’s security group.

**Correct Answer:**  
D. Add an inbound rule to the security group of the database tier’s RDS instance to allow traffic from the web tier’s security group.

**Exam Question 477**

A company runs a photo processing application mat needs to frequently upload and download pictures from Amazon S3 buckets that are located in the same AWS Region A solutions architect has noticed an increased cost in data transfer lees and needs to implement a solution to reduce these costs

How can the solutions architect meet this requirement?

A. Deploy Amazon API Gateway into a public subnet and adjust the route table to route S3 calls through it  
B. Deploy a NAT gateway into a public subnet and attach an endpoint policy that allows access to the S3 buckets  
C. Deploy the application into a public subnet and allow it to route through an internet gateway to access the S3 buckets  
D. Deploy an S3 VPC gateway endpoint into the VPC and attach an endpoint policy that allows access to the S3 buckets

**Correct Answer:**  
C. Deploy the application into a public subnet and allow it to route through an internet gateway to access the S3 buckets

**Exam Question 478**

A company needs to store 160TB of data for an indefinite of time. The company must be able to use standard SQL and business intelligence tools to query all of the data. The data will be queried no more than twice each month.

What is the MOST cost-effective solution that meets these requirements?

A. Store the data in Amazon Aurora Serverless with MySQL  
B. Use an SQL client to query the data.  
C. Store the data in Amazon S3. Use AWS Glue. Amazon Athena. IDBC and COBC drivers to query the data.  
D. Store the data in an Amazon EMR cluster with EMR File System (EMRFS) as the storage layer use Apache Presto to query the data.  
E. Store a subnet of the data in Amazon Redshift, and store the remaining data in Amazon S3. Use Amazon Redshift Spectrum to query the S3 data.

**Correct Answer:**  
D. Store the data in an Amazon EMR cluster with EMR File System (EMRFS) as the storage layer use Apache Presto to query the data.

**Exam Question 479**

A company needs to connect its on-premises data center network to a new VPC. The data center network has a 100 Mbps symmetrical Internet connection. An application that is running on-premises will transfer multiple gigabytes of data each day. The application will use an Amazon Kinesis Data Firehose delivery stream for processing.

What should a solutions architect recommend for maximum performance?

A. Create a VPC peering connection between the on-premises network and the VPC Configure routing for the on-premises network to use the VPC peering connection.  
B. Procure an AWS Snowball Edge Storage Optimized device. After several days’ worth of data has accumulated, copy the data to the device and ship the device to AWS for expedited transfer to Kinesis Data Firehose Repeat as needed  
C. Create an AWS Site-to-Site VPN connection between the on-premises network and the VPC Configure BGP routing between the customer gateway and the virtual private gateway. Use the VPN connection to send the data from on-premises to Kinesis Data Firehose.  
D. Use AWS PrivateLink to create an interface VPC endpoint for Kinesis Data Firehose in the VP  
E. Set up a 1 Gbps AWS Direct Connect connection between the on-premises network and AWS Use the PrivateLink endpoint to send the data from on-premises to Kinesis Data Firehose.

**Correct Answer:**  
D. Use AWS PrivateLink to create an interface VPC endpoint for Kinesis Data Firehose in the VP

**Exam Question 480**

A company operates a website on Amazon EC2 Linux instances Some of the instances are failing. Troubleshooting points to insufficient swap space on the failed instances. The operations team lead needs a solution to monitor this

What should a solutions architect recommend?

A. Configure an Amazon CloudWatch SwapUsage metric dimension Monitor the SwapUsage dimension in the EC2 metrics in CloudWatch.  
B. Use EC2 metadata to collect information, then publish it to Amazon CloudWatch custom metrics Monitor SwapUsage metrics in CloudWatch  
C. Install an Amazon CloudWatch agent on the instances. Run an appropriate script on a set schedule. Monitor SwapUtilization metrics in CloudWatch  
D. Enable detailed monitoring in the EC2 console Create an Amazon CloudWatch SwapUtilization custom metric Monitor SwapUtilization metrics in CloudWatch

**Correct Answer:**  
A. Configure an Amazon CloudWatch SwapUsage metric dimension Monitor the SwapUsage dimension in the EC2 metrics in CloudWatch.

#### Exam Question 481

A company is designing a shared storage solution for a gaming application that is hosted in the AWS Cloud. The company needs the ability to use SMB clients to access data solution must be fully managed.

Which AWS solution meets these requirements?

A. Create an AWS DataSync task that shares the data as a mountable file system Mount the file system to the application server  
B. Create an Amazon EC2 Windows instance Install and configure a Windows file share role on the instance Connect the application server to the file share  
C. Create an Amazon FSx for Windows File Server file system Attach the file system to the origin server Connect the application server to the Me system  
D. Create an Amazon S3 bucket Assign an 1AM role to the application to grant access to the S3 bucket Mount the S3 bucket to the application server

**Correct Answer:**  
C. Create an Amazon FSx for Windows File Server file system Attach the file system to the origin server Connect the application server to the Me system

#### Exam Question 482

A company is Re-architecting a strongly coupled application to be loosely coupled Previously the application used a request/response pattern to communicate between tiers. The company plans to use Amazon Simple Queue Service (Amazon SQS) to achieve decoupling requirements. The initial design contains one queue for requests and one for responses However, this approach is not processing all the messages as the application scales.

What should a solutions architect do to resolve this issue?

A. Configure a dead-letter queue on the ReceiveMessage API action of the SQS queue.  
B. Configure a FIFO queue, and use the message deduplication ID and message group I  
C. Create a temporary queue, with the Temporary Queue Client to receive each response message.  
D. Create a queue for each request and response on startup for each producer, and use a correlation ID message attribute.

**Correct Answer:**  
A. Configure a dead-letter queue on the ReceiveMessage API action of the SQS queue.

#### Exam Question 483

A solutions architect is creating a new Amazon CloudFront distribution for an application Some of the information submitted by users is sensitive. The application uses HTTPS but needs another layer of security. The sensitive information should be protected throughout the entire application stack, and access to the information should be restricted to certain applications.

Which action should the solutions architect take?

A. Configure a CloudFront signed URL  
B. Configure a CloudFront signed cookie.  
C. Configure a CloudFront field-level encryption profile.  
D. Configure CloudFront and set the Origin Protocol Policy setting to HTTPS Only for the Viewer Protocol Pokey

**Correct Answer:**  
A. Configure a CloudFront signed URL

#### Exam Question 484

A solutions architect needs to design a resilient solution for Windows users’ home directories. The solution must provide fault tolerance, file-level backup and recovery, and access control, based upon the company’s Active Directory.

Which storage solution meets these requirements?

A. Configure Amazon S3 to store the users’ home directories. Join Amazon S3 to Active Directory.  
B. Configure a Multi-AZ file system with Amazon FSx for Windows File Server Join Amazon FSx to Active Directory.  
C. Configure Amazon Elastic File System (Amazon EFS) for the users’ home directories. Configure AWS Single Sign-On with Active Directory.  
D. Configure Amazon Elastic Block Store (Amazon EBS) to store the users’ home directories Configure AWS Single Sign-On with Active Directory.

**Correct Answer:**  
C. Configure Amazon Elastic File System (Amazon EFS) for the users’ home directories. Configure AWS Single Sign-On with Active Directory.

#### Exam Question 485

A solutions architect is creating a data processing job that runs once daily and can take up to 2 hours to complete If the job is interrupted, it has to restart from the beginning

How should the solutions architect address this issue in the MOST cost-effective manner?

A. Create a script that runs locally on an Amazon EC2 Reserved Instance that is triggered by a cron job.  
B. Create an AWS Lambda function triggered by an Amazon EventBridge (Amazon CloudWatch Events} scheduled event  
C. Use an Amazon Elastic Container Service (Amazon ECS) Fargate task triggered by an Amazon EventBridge (Amazon CloudWatch Events) scheduled event.  
D. Use an Amazon Elastic Container Service (Amazon ECS) task running on Amazon EC2 triggered by an Amazon EventBridge (Amazon CloudWatch Events) scheduled event.

**Correct Answer:**  
C. Use an Amazon Elastic Container Service (Amazon ECS) Fargate task triggered by an Amazon EventBridge (Amazon CloudWatch Events) scheduled event.

#### Exam Question 486

A company hosts its multi-tier public web application in the AWS Cloud. The web application runs on Amazon EC2 instances and its database runs on Amazon RDS. The company is anticipating a large increase in sales during an upcoming holiday weekend A solutions architect needs to build a solution to analyze the performance of the web application with a granularity of no more than 2 minutes.

What should the solutions architect do to meet this requirement?

A. Send Amazon CloudWatch logs to Amazon Redshift Use Amazon QuickSight to perform further analysis  
B. Enable detailed monitoring on all EC2 instances Use Amazon CloudWatch metrics to perform further analysis  
C. Create an AWS Lambda function to fetch EC2 logs from Amazon CloudWatch Logs Use Amazon CloudWatch metrics to perform further analysis  
D. Send EC2 logs to Amazon S3 Use Amazon Redshift to fetch logs from the S3 bucket to process raw data for further analysis with Amazon QuickSight.

**Correct Answer:**  
B. Enable detailed monitoring on all EC2 instances Use Amazon CloudWatch metrics to perform further analysis

#### Exam Question 487

A company is creating a three-tier web application consisting of a web server, an application server, and a database server. The application will track GPS coordinates of packages as they are being delivered. The application will update the database every 0-5 seconds.

The tracking will need to read a fast as possible for users to check the status of their packages. Only a few packages might be tracked on some days, whereas millions of package might be tracked on other days. Tracking will need to be searchable by tracking ID customer ID and order ID Order than 1 month no longer read to be tracked.

What should a solution architect recommend to accomplish this with minimal cost of ownership?

A. Use Amazon DynamoDB Enable Auto Scaling on the DynamoDB table. Schedule an automatic deletion script for items older than 1 month.  
B. Use Amazon DynamoDB with global secondary indexes. Enable Auto Scaling on the DynamoDB table and the global secondary indexes. Enable TTL on the DynamoDB table.  
C. Use an Amazon RDS On-Demand instance with Provisioned IOPS (PIOPS). Enable Amazon CloudWatch alarms to send notifications when PIOPS are exceeded. Increase and decrease PIOPS as needed.  
D. Use a Amazon RDS Reserved Instance with Provisioned IOPS (PIOPS). Enable Amazon CloudWatch alarms to send notification when PIOPS are exceeded. Increase and decrease PIOPS as needed.

**Correct Answer:**  
B. Use Amazon DynamoDB with global secondary indexes. Enable Auto Scaling on the DynamoDB table and the global secondary indexes. Enable TTL on the DynamoDB table.

#### Exam Question 488

A start-up company has a web application based in the us-east-1 Region with multiple Amazon EC2 instances running behind an Application Load Balancer across multiple Availability Zones As the company’s user base grows in the us-west-1 Region, it needs 3 solution with low latency and high availability.

What should a solutions architect do to accomplish this?

A. Provision EC2 instances in us-west-1. Switch my Application Load Balancer to a Network Load Balancer to achieve cross-Region load balancing.  
B. Provision EC2 instances and an Application Load Balancer in us-west-1 Make the load balancer distribute the traffic based on the location of the request  
C. Provision EC2 instances and configure an Application Load Balancer in us-west-1. Create an accelerator in AWS Global Accelerator that uses an endpoint group that includes the load balancer endpoints in both Regions.  
D. Provision EC2 Instances and configure an Application Load Balancer in us-west-1 Configure Amazon Route 53 with a weighted routing policy. Create alias records in Route 53 that point to the Application Load Balancer

**Correct Answer:**  
C. Provision EC2 instances and configure an Application Load Balancer in us-west-1. Create an accelerator in AWS Global Accelerator that uses an endpoint group that includes the load balancer endpoints in both Regions.

**Answer Description:**  
ELB provides load balancing within one Region, AWS Global Accelerator provides traffic management across multiple Regions […] AWS Global Accelerator complements ELB by extending these capabilities beyond a single AWS Region, allowing you to provision a global interface for your applications in any number of Regions. If you have workloads that cater to a global client base, we recommend that you use AWS Global Accelerator. If you have workloads hosted in a single AWS Region and used by clients in and around the same Region, you can use an Application Load Balancer or Network Load Balancer to manage your resources.

**References:**  
[AWS Global Accelerator FAQs](https://aws.amazon.com/global-accelerator/faqs/)

#### Exam Question 489

A company has a service that produces event data. The company wants to use AWS to process the event data as it is received. The data is written in a specific order that must be maintained throughout processing. The company wants to implement a solution that minimizes operational overhead.

How should a solution architect accomplish this”

A. Create an Amazon Simple Queue Service (Amazon SOS) FIFO queue to hold messages. Set up an AWS Lambda function to process messages from the queue.  
B. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an AWS Lambda function as a subscriber  
C. Create an Amazon Simple Queue Service (Amazon SOS) standard queue to hold messages Set up an AWS Lambda function 😮 process messages from the queue independently  
D. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process Configure an Amazon Simple Queue Service (Amazon SQS) queue as a subscriber.

**Correct Answer:**  
A. Create an Amazon Simple Queue Service (Amazon SOS) FIFO queue to hold messages. Set up an AWS Lambda function to process messages from the queue.

#### Exam Question 490

The following IAM policy is attached to an IAM group. This is the only policy applied to the group.  
  
What are the effective IAM permissions of this policy for group members?

A. Group members are permitted any Amazon EC2 action within the us-east-1 Region. Statements after. The Allow permission are not applied  
B. Group member are denied any Amazon EC2 permissions in the us-east-1 Region unless they are tagged in with multi-factor authentication (MFA).  
C. Group members are allowed the ec2:StopInstances and ec2:Terminatelnstances permissions for all Regions when logged in with multi-factor authentication (MFA). Group members authorized any other Amazon EC2 action.  
D. Group members are allowed the ec2:Stoplnstances and ec2:Terminatelnstances permissions for the us-east-1 Region only when logged in with multi-factor authentication (MFA). Groups are permitted any other Amazon EC2 action within the us-east-1 Region

**Correct Answer:**  
D. Group members are allowed the ec2:Stoplnstances and ec2:Terminatelnstances permissions for the us-east-1 Region only when logged in with multi-factor authentication (MFA). Groups are permitted any other Amazon EC2 action within the us-east-1 Region

**Exam Question 491**

A company is running a highly sensitive application on Amazon EC2 backed by an Amazon RDS database Compliance regulations mandate that all personally identifiable information (Pll) be encrypted at rest.

Which solution should a solutions architect recommend to meet this requirement with the LEAST amount of changes to the infrastructure”

A. Deploy AWS Certificate Manager to generate certificates Use the certificates to encrypt the database volume  
B. Deploy AWS CloudHS  
C. generate encryption keys, and use the customer master key (CMK) to encrypt database volumes.  
D. Configure SSL encryption using AWS Key Management Service customer master keys (AWS KMS CMKs) to encrypt database volumes  
E. Configure Amazon Elastic Block Store {Amazon EBS) encryption and Amazon RDS encryption with AWS Key Management Service (AWS KMS) keys to encrypt instance and database volumes.

**Correct Answer:**  
D. Configure SSL encryption using AWS Key Management Service customer master keys (AWS KMS CMKs) to encrypt database volumes

**Exam Question 492**

A company recently migrated a message processing system to AWS. The system receives messages into an ActiveMQ queue running on an Amazon EC2 instance. Messages are processed by a consumer application running on Amazon EC2. The consumer application processes the messages and writes results to a MySQL database running on Amazon EC2. The company wants this application to be highly available with low operational complexity

Which architecture offers the HIGHEST availability?

A. Add a second ActiveMQ server to another Availability Zone Add an additional consumer EC2 instance in another Availability Zone Replicate the MySQL database to another Availability Zone.  
B. Use Amazon MQ with active/standby brokers configured across two Availability Zones Add an additional consumer EC2 instance in another Availability Zone. Replicate the MySQL database to another Availability Zone  
C. Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an additional consumer EC2 instance in another Availability Zone. Use Amazon RDS for MySQL with Multi-AZ enabled  
D. Use Amazon MQ with active/standby brokers configured across two Availability Zones Add an Auto Scaling group for the consumer EC2 instances across two Availability Zones Use Amazon RDS for MySQL with Multi-AZ enabled.

**Correct Answer:**  
D. Use Amazon MQ with active/standby brokers configured across two Availability Zones Add an Auto Scaling group for the consumer EC2 instances across two Availability Zones Use Amazon RDS for MySQL with Multi-AZ enabled.

**Exam Question 493**

A meteorological startup company has a custom web application to sell weather data to its users online. The company uses Amazon DynamoDB to store its data and wants to build a new service that sends an alert to the managers of four internal teams every time a new weather event is recorded. The company does not want this new service to affect the performance of the current application

What should a solutions architect do to meet these requirements with the LEAST amount of operational overhead?

A. Use DynamoDB transactions to write new event data to the table Configure the transactions to notify internal teams.  
B. Have the current application publish a message to four Amazon Simple Notification Service (Amazon SNS) topics. Have each team subscribe to one topic.  
C. Enable Amazon DynamoDB Streams on the table Use triggers to write to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe  
D. Add a custom attribute to each record to flag new items Write a cron job that scans the table every minute for items that are new and notifies an Amazon Simple Queue Service (Amazon SQS) queue to which the teams can subscribe

**Correct Answer:**  
A. Use DynamoDB transactions to write new event data to the table Configure the transactions to notify internal teams.

**Exam Question 494**

A company needs guaranteed Amazon EC2 capacity in three specific Availability Zones in a specific AWS Region for an upcoming event that will last 1 week.

What should the company do to guarantee the EC2 capacity?

A. Purchase Reserved Instances that specify the Region needed.  
B. Create an On-Demand Capacity Reservation that specifies the Region needed.  
C. Purchase Reserved Instances that specify the Region and three Availability Zones needed.  
D. Create an On-Demand Capacity Reservation that specifies the Region and three Availability Zones needed.

**Correct Answer:**  
A. Purchase Reserved Instances that specify the Region needed.

**Exam Question 495**

A company receives data from millions of users totaling about 1 TB each flay. The company provides its user’s with usage reports gang back 12 months Al usage data must be stored for at least 5 years to comply with regulatory and auditing requirements

Which storage solution is MOST cost-effective?

A. Store the data in Amazon S3 Standard. Set a lifecycle -rule to transition the data to S3 Glacier Deep Archive after 1 year. Set a Recycle rule to delete the data after5 years.  
B. Store. The data in Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA). Set a lifecycle rule to transition the data to S3 Glacier after 1 year Set the lifecycle rule to delete the data after 5 years.  
C. Store the data in Amazon S3 Standard Set a lifecycle rule to transition the data to S3 Standard-infrequent Access (S3 Standard-IA) after 1 year Sol a lifecycle rule to delete the data after 5 years.  
D. Store the data in Amazon S3 Standard Set a lifecycle -rule to transition the data to S3 One Zone-infrequent Access (S3 One Zone-IA) after 1 year, Set a Lifecycle rule to delete the data after 5 years.

**Correct Answer:**  
A. Store the data in Amazon S3 Standard. Set a lifecycle -rule to transition the data to S3 Glacier Deep Archive after 1 year. Set a Recycle rule to delete the data after5 years.

**Exam Question 496**

A three-tier web application processes orders from customers. The web tier consists of Amazon EC2 instances behind an Application Load Balancer, a middle tier of three EC2 instances decoupled from the web tier using Amazon SQS. and an Amazon DynamoDB backend. At peak times, customers who submit orders using the site have to wait much longer than normal to receive confirmations due to lengthy processing times. A solutions architect needs to reduce these processing times.

Which action will be MOST effective in accomplishing this?

A. Replace the SQS queue with Amazon Kinesis Data Firehose.  
B. Use Amazon ElastiCache for Redis in front of the DynamoDB backend tier.  
C. Add an Amazon CloudFront distribution to cache the responses for the web tier.  
D. Use Amazon EC2 Auto Scaling to scale out the middle tier instances based on the SOS queue depth.

**Correct Answer:**  
D. Use Amazon EC2 Auto Scaling to scale out the middle tier instances based on the SOS queue depth.

**Exam Question 497**

A company has hired a new cloud engineer who should not have access to an Amazon S3 bucket named Company Confidential. the cloud engineer must be able to read from and write to an S3 bucket called AdminTools.

Which IAM policy will meet these requirements?

A.  
B.  
C.  
D.  
**Correct Answer:**  
A.

**Exam Question 498**

A company needs to store data in Amazon S3 A compliance requirement states that when any changes are made to objects the previous state of the object with any changes must be preserved Additionally files older than 5 years should not be accessed but need to be archived for auditing

What should a solutions architect recommend that is MOST cost-effective?

A. Enable object-level versioning and S3 Object Lock in governance mode  
B. Enable object-level versioning and S3 Object Lock in compliance mode  
C. Enable object-level versioning Enable a lifecycle policy to move data older than 5 years to S3 Glacier Deep Archive  
D. Enable object-level versioning Enable a lifecycle policy to move data older than 5 years to S3 Standard-Infrequent Access (S3 Standard-IA)

**Correct Answer:**  
C. Enable object-level versioning Enable a lifecycle policy to move data older than 5 years to S3 Glacier Deep Archive

**Exam Question 499**

A company recently migrated a message processing system to AWS. The system receives messages into an ActiveMQ queue running on an Amazon EC2 instance. Messages are processed by a consumer application running on Amazon EC2. The consumer application processes the messages and writes results to a MySQL database running on Amazon EC2. The company wants this application to be highly available with low operational complexity

Which architecture offers the HIGHEST availability?

A. Add a second ActiveMQ server to another Availability Zone Add an additional consumer EC2 instance in another Availability Zone Replicate the MySQL database to another Availability Zone.  
B. Use Amazon MQ with active/standby brokers configured across two Availability Zones Add an additional consumer EC2 instance in another Availability Zone. Replicate the MySQL database to another Availability Zone  
C. Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an additional consumer EC2 instance in another Availability Zone. Use Amazon RDS for MySQL with Multi-AZ enabled  
D. Use Amazon MQ with active/standby brokers configured across two Availability Zones Add an Auto Scaling group for the consumer EC2 instances across two Availability Zones Use Amazon RDS for MySQL with Multi-AZ enabled.

**Correct Answer:**  
D. Use Amazon MQ with active/standby brokers configured across two Availability Zones Add an Auto Scaling group for the consumer EC2 instances across two Availability Zones Use Amazon RDS for MySQL with Multi-AZ enabled.

**Exam Question 500**

A company hosts its core network services, including directory services and DNS. in its on-premises data center. The data center is connected to the AWS Cloud using AWS Direct Connect (DX) Additional AWS accounts are planned that will require quick, cost-effective, and consistent access to these network services.

What should a solutions architect implement to meet these requirements with the LEAST amount of operational overhead?

A. Create a DX connection in each new account Route the network traffic to the on-premises servers  
B. Configure VPC endpoints in the DX VPC for all required services Route the network traffic to the on-premises servers.  
C. Create a VPN connection between each new account and the DX VPC, Route the network traffic to the on-premises servers  
D. Configure AWS Transit Gateway between the accounts Assign DX to the transit gateway and route network traffic to the on-premises servers

**Correct Answer:**  
D. Configure AWS Transit Gateway between the accounts Assign DX to the transit gateway and route network traffic to the on-premises servers