**Q1.** An audit department generates and accesses the audit reports only twice in a financial year. The department uses AWS Step Functions to orchestrate the report creating process that has failover and retry scenarios built into the solution. The underlying data to create these audit reports is stored on S3, runs into hundreds of Terabytes and should be available with millisecond latency.

As a solutions architect, which is the MOST cost-effective storage class that you would recommend to be used for this use-case?

**A.** Amazon S3 Glacier (S3 Glacier)

**B.** Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering)

**C.** Amazon S3 Standard

**D.** Amazon S3 Standard-Infrequent Access (S3 Standard-IA)

**Ans D.**

**Explanation**: Since the data is accessed only twice in a financial year but needs rapid access when required, the most cost-effective storage class for this use-case is S3 Standard-IA

**Q2.** The engineering team at a Spanish professional football club has built a notification system for its website using Amazon SNS notifications which are then handled by a Lambda function for end-user delivery. During the off-season, the notification systems need to handle about 100 requests per second. During the peak football season, the rate touches about 5000 requests per second and it is noticed that a significant number of the notifications are not being delivered to the end-users on the website.

As a solutions architect, which of the following would you suggest as the BEST possible solution to this issue?

**A.** Amazon SNS message deliveries to AWS Lambda have crossed the account concurrency quota for Lambda, so the team needs to contact AWS support to raise the account limit  
**B.** Amazon SNS has hit a scalability limit, so the team needs to contact AWS support to raise the account limit  
**C.** The engineering team needs to provision more servers running the Lambda service  
**D.** The engineering team needs to provision more servers running the SNS service

**Ans A.**

**Explanation**:  
Amazon SNS message deliveries to AWS Lambda have crossed the account concurrency quota for Lambda, so the team needs to contact AWS support to raise the account limit  
Amazon Simple Notification Service (SNS) is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications.  
With AWS Lambda, you can run code without provisioning or managing servers. You pay only for the compute time that you consume—there’s no charge when your code isn’t running.  
AWS Lambda currently supports 1000 concurrent executions per AWS account per region. If your Amazon SNS message deliveries to AWS Lambda contribute to crossing these concurrency quotas, your Amazon SNS message deliveries will be throttled. You need to contact AWS support to raise the account limit. Therefore this option is correct.  
Incorrect options:  
Amazon SNS has hit a scalability limit, so the team needs to contact AWS support to raise the account limit – Amazon SNS leverages the proven AWS cloud to dynamically scale with your application. You don’t need to contact AWS support, as SNS is a fully managed service, taking care of the heavy lifting related to capacity planning, provisioning, monitoring, and patching. Therefore, this option is incorrect.  
The engineering team needs to provision more servers running the SNS service  
The engineering team needs to provision more servers running the Lambda service  
As both Lambda and SNS are serverless and fully managed services, the engineering team cannot provision more servers. Both of these options are incorrect.

**Q3.** A retail company has developed a REST API which is deployed in an Auto Scaling group behind an Application Load Balancer. The API stores the user data in DynamoDB and any static content, such as images, are served via S3. On analyzing the usage trends, it is found that 90% of the read requests are for commonly accessed data across all users.

As a Solutions Architect, which of the following would you suggest as the MOST efficient solution to improve the application performance?

**A.** Enable ElastiCache Redis for DynamoDB and CloudFront for S3  
**B.** Enable DAX for DynamoDB and ElastiCache Memcached for S3  
**C.** Enable DynamoDB Accelerator (DAX) for DynamoDB and CloudFront for S3  
**D.** Enable ElastiCache Redis for DynamoDB and ElastiCache Memcached for S3

**Ans: C**

**Explanation**:  
Enable DynamoDB Accelerator (DAX) for DynamoDB and CloudFront for S3  
DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for Amazon DynamoDB that delivers up to a 10 times performance improvement—from milliseconds to microseconds—even at millions of requests per second.  
DAX is tightly integrated with DynamoDB—you simply provision a DAX cluster, use the DAX client SDK to point your existing DynamoDB API calls at the DAX cluster, and let DAX handle the rest. Because DAX is API-compatible with DynamoDB, you don’t have to make any functional application code changes. DAX is used to natively cache DynamoDB reads.  
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.  
When a user requests content that you serve with CloudFront, their request is routed to a nearby Edge Location. If CloudFront has a cached copy of the requested file, CloudFront delivers it to the user, providing a fast (low-latency) response. If the file they’ve requested isn’t yet cached, CloudFront retrieves it from your origin – for example, the S3 bucket where you’ve stored your content.  
So, you can use CloudFront to improve application performance to serve static content from S3.  
**Incorrect options**:  
Enable ElastiCache Redis for DynamoDB and CloudFront for S3  
Amazon ElastiCache for Redis is a blazing fast in-memory data store that provides sub-millisecond latency to power internet-scale real-time applications. Amazon ElastiCache for Redis is a great choice for real-time transactional and analytical processing use cases such as caching, chat/messaging, gaming leaderboards, geospatial, machine learning, media streaming, queues, real-time analytics, and session store.  
Although you can integrate Redis with DynamoDB, it’s much more involved than using DAX which is a much better fit.  
Enable DAX for DynamoDB and ElastiCache Memcached for S3  
Enable ElastiCache Redis for DynamoDB and ElastiCache Memcached for S3  
Amazon ElastiCache for Memcached is a Memcached-compatible in-memory key-value store service that can be used as a cache or a data store. Amazon ElastiCache for Memcached is a great choice for implementing an in-memory cache to decrease access latency, increase throughput, and ease the load off your relational or NoSQL database.  
ElastiCache cannot be used as a cache to serve static content from S3, so both these options are incorrect.

**Q4.** A data analytics company measures what the consumers watch and what advertising they’re exposed to. This real-time data is ingested into its on-premises data center and subsequently, the daily data feed is compressed into a single file and uploaded on Amazon S3 for backup. The typical compressed file size is around 2 GB.

Which of the following is the fastest way to upload the daily compressed file into S3?

**A.** Upload the compressed file using multipart upload with S3 transfer acceleration  
**B.** Upload the compressed file in a single operation  
**C.** Upload the compressed file using multipart upload  
**D.** FTP the compressed file into an EC2 instance that runs in the same region as the S3 bucket. Then transfer the file from the EC2 instance into the S3 bucket

**Ans A.**

**Explanation:**  
Upload the compressed file using multipart upload with S3 transfer acceleration  
Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. Transfer Acceleration takes advantage of Amazon CloudFront’s globally distributed edge locations. As the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path.  
Multipart upload allows you to upload a single object as a set of parts. Each part is a contiguous portion of the object’s data. You can upload these object parts independently and in any order. If transmission of any part fails, you can retransmit that part without affecting other parts. After all parts of your object are uploaded, Amazon S3 assembles these parts and creates the object. If you’re uploading large objects over a stable high-bandwidth network, use multipart uploading to maximize the use of your available bandwidth by uploading object parts in parallel for multi-threaded performance. If you’re uploading over a spotty network, use multipart uploading to increase resiliency to network errors by avoiding upload restarts.  
**Incorrect options:**  
Upload the compressed file in a single operation – In general, when your object size reaches 100 MB, you should consider using multipart uploads instead of uploading the object in a single operation. Multipart upload provides improved throughput – you can upload parts in parallel to improve throughput. Therefore, this option is not correct.  
Upload the compressed file using multipart upload – Although using multipart upload would certainly speed up the process, combining with S3 transfer acceleration would further improve the transfer speed. Therefore just using multipart upload is not the correct option.  
FTP the compressed file into an EC2 instance that runs in the same region as the S3 bucket. Then transfer the file from the EC2 instance into the S3 bucket – This is a roundabout process of getting the file into S3 and added as a distractor. Although it is technically feasible to follow this process, it would involve a lot of scripting and certainly would not be the fastest way to get the file into S3.

**Q 5.** A media company runs a photo-sharing web application that is accessed across three different countries. The application is deployed on several Amazon EC2 instances running behind an Application Load Balancer. With new government regulations, the company has been asked to block access from two countries and allow access only from the home country of the company.

Which configuration should be used to meet this changed requirement?

**A.** Use Geo Restriction feature of Amazon CloudFront in a VPC

**B.** Configure the security group on the Application Load Balancer

**C.** Configure the security group for the EC2 instances

**D.** Configure AWS WAF on the Application Load Balancer in a VPC

**Ans D.**

**Q 6.** A gaming company is looking at improving the availability and performance of its global flagship application which utilizes UDP protocol and needs to support fast regional failover in case an AWS Region goes down. The company wants to continue using its own custom DNS service.

Which of the following AWS services represents the best solution for this use-case?

**A.** Amazon CloudFront

**B.** AWS Global Accelerator

**C.** Amazon Route 53

**D.** AWS Elastic Load Balancing (ELB)

**Ans B**  
**Explanation:**  AWS Global Accelerator utilizes the Amazon global network, allowing you to improve the performance of your applications by lowering first-byte latency (the round trip time for a packet to go from a client to your endpoint and back again) and jitter (the variation of latency), and increasing throughput (the amount of time it takes to transfer data) as compared to the public internet.  
Global Accelerator improves performance for a wide range of applications over TCP or UDP by proxying packets at the edge to applications running in one or more AWS Regions. Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover.

**Q 7**. A new DevOps engineer has just joined a development team and wants to understand the replication capabilities for RDS Multi-AZ as well as RDS Read-replicas.  
Which of the following correctly summarizes these capabilities for the given database?  
Options:  
**A.** Multi-AZ follows asynchronous replication and spans one Availability Zone within a single region. Read replicas follow synchronous replication and can be within an Availability Zone, Cross-AZ, or Cross-Region  
**B.** Multi-AZ follows asynchronous replication and spans at least two Availability Zones within a single region. Read replicas follow synchronous replication and can be within an Availability Zone, Cross-AZ, or Cross-Region  
**C.** Multi-AZ follows synchronous replication and spans at least two Availability Zones within a single region. Read replicas follow asynchronous replication and can be within an Availability Zone, Cross-AZ, or Cross-Region  
**D.** Multi-AZ follows asynchronous replication and spans at least two Availability Zones within a single region. Read replicas follow asynchronous replication and can be within an Availability Zone, Cross-AZ, or Cross-Region

**Ans C.**

**Explanation:** Multi-AZ follows synchronous replication and spans at least two Availability Zones within a single region. Read replicas follow asynchronous replication and can be within an Availability Zone, Cross-AZ, or Cross-Region  
Amazon RDS Multi-AZ deployments provide enhanced availability and durability for RDS database (DB) instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Multi-AZ spans at least two Availability Zones within a single region.  
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. 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.  
Amazon RDS replicates all databases in the source DB instance. Read replicas can be within an Availability Zone, Cross-AZ, or Cross-Region.

**Q8.** An IT security consultancy is working on a solution to protect data stored in S3 from any malicious activity as well as check for any vulnerabilities on EC2 instances.

As a solutions architect, which of the following solutions would you suggest to help address the given requirement?

**A.** Use Amazon GuardDuty to monitor any malicious activity on data stored in S3. Use security assessments provided by Amazon GuardDuty to check for vulnerabilities on EC2 instances  
**B.** Use Amazon GuardDuty to monitor any malicious activity on data stored in S3. Use security assessments provided by Amazon Inspector to check for vulnerabilities on EC2 instances  
**C.** Use Amazon Inspector to monitor any malicious activity on data stored in S3. Use security assessments provided by Amazon Inspector to check for vulnerabilities on EC2 instances  
**D.** Use Amazon Inspector to monitor any malicious activity on data stored in S3. Use security assessments provided by Amazon GuardDuty to check for vulnerabilities on EC2 instances

**Ans B**

**Explanation**:

Q: What is Amazon GuardDuty?

GuardDuty is an intelligent threat detection service that continuously monitors your AWS accounts, Amazon Elastic Compute Cloud (EC2) instances, Amazon Elastic Kubernetes Service (EKS) clusters, and data stored in Amazon Simple Storage Service (S3) for malicious activity without the use of security software or agents. If potential malicious activity, such as anomalous behaviour, credential exfiltration, or command and control infrastructure (C2) communication is detected, GuardDuty generates detailed security findings that can be used for security visibility and assisting in remediation. Additionally, using the Amazon GuardDuty Malware Protection feature helps to detect malicious files on Amazon Elastic Block Store (EBS) volumes attached to EC2 instance and container workloads.

**Q 9**. An ivy-league university is assisting NASA to find potential landing sites for exploration vehicles of unmanned missions to our neighboring planets. The university uses High Performance Computing (HPC) driven application architecture to identify these landing sites.

Which of the following EC2 instance topologies should this application be deployed on?

**A.** The EC2 instances should be deployed in a partition placement group so that distributed workloads can be handled effectively  
**B.** The EC2 instances should be deployed in a cluster placement group so that the underlying workload can benefit from low network latency and high network throughput  
**C.** The EC2 instances should be deployed in a spread placement group so that there are no correlated failures  
**D.** The EC2 instances should be deployed in an Auto Scaling group so that application meets high availability requirements

**Ans B.**

**Q 10**. The product team at a startup has figured out a market need to support both stateful and stateless client-server communications via the APIs developed using its platform. You have been hired by the startup as a solutions architect to build a solution to fulfill this market need using AWS API Gateway.

Which of the following would you identify as correct?

**A.** API Gateway creates RESTful APIs that enable stateful client-server communication and API Gateway also creates WebSocket APIs that adhere to the WebSocket protocol, which enables stateful, full-duplex communication between client and server  
**B.** API Gateway creates RESTful APIs that enable stateless client-server communication and API Gateway also creates WebSocket APIs that adhere to the WebSocket protocol, which enables stateless, full-duplex communication between client and server  
**C.** API Gateway creates RESTful APIs that enable stateful client-server communication and API Gateway also creates WebSocket APIs that adhere to the WebSocket protocol, which enables stateless, full-duplex communication between client and server  
**D.** API Gateway creates RESTful APIs that enable stateless client-server communication and API Gateway also creates WebSocket APIs that adhere to the WebSocket protocol, which enables stateful, full-duplex communication between client and server

**Ans D.**

**Q 11.** The engineering team at an in-home fitness company is evaluating multiple in-memory data stores with the ability to power its on-demand, live leaderboard. The company’s leaderboard requires high availability, low latency, and real-time processing to deliver customizable user data for the community of users working out together virtually from the comfort of their home.  
As a solutions architect, which of the following solutions would you recommend? (Select two)

**A.** Power the on-demand, live leaderboard using DynamoDB with DynamoDB Accelerator (DAX) as it meets the in-memory, high availability, low latency requirements  
**B.** Power the on-demand, live leaderboard using AWS Neptune as it meets the in-memory, high availability, low latency requirements  
**C.** Power the on-demand, live leaderboard using DynamoDB as it meets the in-memory, high availability, low latency requirements  
**D.** Power the on-demand, live leaderboard using RDS Aurora as it meets the in-memory, high availability, low latency requirements  
**E.** Power the on-demand, live leaderboard using ElastiCache Redis as it meets the in-memory, high availability, low latency requirements

**Ans A and E**.

**Q 12.** A news network uses Amazon S3 to aggregate the raw video footage from its reporting teams across the US. The news network has recently expanded into new geographies in Europe and Asia. The technical teams at the overseas branch offices have reported huge delays in uploading large video files to the destination S3 bucket. Which of the following are the MOST cost-effective options to improve the file upload speed into S3? (Select two)

A. Use multipart uploads for faster file uploads into the destination S3 bucket.  
B. Use Amazon S3 Transfer Acceleration to enable faster file uploads into the destination S3 bucket.  
C. Use AWS Global Accelerator for faster file uploads into the destination S3 bucket.  
D. Create multiple site-to-site VPN connections between the AWS Cloud and branch offices in Europe and Asia. Use these VPN connections for faster file uploads into S3.  
E. Create multiple AWS direct connect connections between the AWS Cloud and branch offices in Europe and Asia. Use the direct connect connections for faster file uploads into S3.

**Ans A and B**

**Q 13.** A retail company has set up a Network Load Balancer (NLB) having a target group that is configured to use an Amazon EC2 Auto Scaling group with multiple EC2 instances (across 3 Availability Zones) that run the web service. The company is getting poor feedback from its customers regarding the application's availability as the NLB is unable to detect HTTP errors for the application. These HTTP errors require a manual restart of the EC2 instances that run the web service.

The company has hired you as an AWS Certified Solutions Architect Associate to build the best-fit solution that does not require custom development/scripting effort. Which of the following will you suggest?

**A.** Set up a cron job on the EC2 instances to inspect the web application’s logs at a regular frequency. When HTTP error are detected, force an application restart.

**B.** Replace the Network Load Balancer(NLB) with an Application Load Balancer(ALB) and config HTTP health checks on the ALB by pointing to the URL of the application. Leverage the Auto Scaling group to replace unhealthy instances.

**C.** Configure HTTP health checks on the Network Load Balancer(NLB) by pointing to URL of the application. Leverage the Auto Scaling group to replace unhealthy instances

**D.** Set up a CloudWatch alarm to monitor the UnhealthyHostCount metric for the NLB. Leverage the Auto Scaling group to unhealthy instances when the alarm is in the ALARM state.

**Ans B.**

**Q 14.** A file-hosting service uses Amazon S3 under the hood to power its storage offerings. Currently all the customer files are uploaded directly under a single S3 bucket. The engineering team has started seeing scalability issues where customer file uploads have started failing during the peak access hours with more than 5000 requests per second.

Which of the following is the MOST resource efficient and cost-optimal way of addressing this issue?

**A.** Change the application architecture to use EFS instead of Amazon S3 for storing the customers' uploaded files

**B.** Change the application architecture to create customer-specific custom prefixes within the single bucket and then upload the daily files into those prefixed locations

**C.** Change the application architecture to create a new S3 bucket for each customer and then upload each customer's files directly under the respective buckets

**D.** Change the application architecture to create a new S3 bucket for each day's data and then upload the daily files directly under that day's bucket

**Ans B.**

**Q 15**. A company uses DynamoDB as a data store for various kinds of customer data, such as user profiles, user events, clicks, and visited links. Some of these use-cases require a high request rate (millions of requests per second), low predictable latency, and reliability. The company now wants to add a caching layer to support high read volumes.

As a solutions architect, which of the following AWS services would you recommend as a caching layer for this use-case? (Select two)

A. DynamoDB Accelerator (DAX)  
B. ElastiCache  
C. Elastisearch  
D. RDS  
E. Redshift

**Ans A and B**

**Explanation**  
**Correct options**:  
**DynamoDB Accelerator** (DAX) – Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for DynamoDB that delivers up to a 10x performance improvement – from milliseconds to microseconds – even at millions of requests per second. DAX does all the heavy lifting required to add in-memory acceleration to your DynamoDB tables, without requiring developers to manage cache invalidation, data population, or cluster management. Therefore, this is a correct option.  
**ElastiCache** – Amazon ElastiCache for Memcached is an ideal front-end for data stores like Amazon RDS or Amazon DynamoDB, providing a high-performance middle tier for applications with extremely high request rates and/or low latency requirements. Therefore, this is also a correct option.  
**Incorrect options**:  
**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. RDS cannot be used as a caching layer for DynamoDB.  
Elasticsearch – Elasticsearch is a search engine based on the Lucene library. It provides a distributed, multitenant-capable full-text search engine with an HTTP web interface and schema-free JSON documents. It cannot be used as a caching layer for DynamoDB.  
Redshift – Amazon Redshift is a fully-managed petabyte-scale cloud-based data warehouse product designed for large scale data set storage and analysis. It cannot be used as a caching layer for DynamoDB.

**Q 16**. A video analytics organization has been acquired by a leading media company. The analytics organization has 10 independent applications with an on-premises data footprint of about 70TB for each application. The CTO of the media company has set a timeline of two weeks to carry out the data migration from on-premises data center to AWS Cloud and establish connectivity.

Which of the following are the MOST cost-effective options for completing the data transfer and establishing connectivity?

**A.** Order 1 Snowmobile to complete the one-time data transfer  
**B.** Setup AWS direct connect to establish connectivity between the on-premises data center and AWS Cloud  
**C.** Order 70 Snowball Edge Storage Optimized devices to complete the one-time data transfer  
**D.** Setup Site-to-Site VPN to establish connectivity between the on-premises data center and AWS Cloud  
**E.** Order 10 Snowball Edge Storage Optimized devices to complete the one-time data transfer

**Ans D and E.**

**Q 17**. A social photo-sharing company uses Amazon S3 to store the images uploaded by the users. These images are kept encrypted in S3 by using AWS-KMS and the company manages its own Customer Master Key (CMK) for encryption. A member of the DevOps team accidentally deleted the CMK a day ago, thereby rendering the user's photo data unrecoverable. You have been contacted by the company to consult them on possible solutions to this crisis.

As a solutions architect, which of the following steps would you recommend to solve this issue?

**A.** Contact AWS support to retrieve the CMK from their backup

**B.** As the CMK was deleted a day ago, it must be in the 'pending deletion' status and hence you can just cancel the CMK deletion and recover the key

**C.** The company should issue a notification on its web application informing the users about the loss of their data

**D.** The CMK can be recovered by the AWS root account user

**Ans B.**

**Q 18.** One of the biggest football leagues in Europe has granted the distribution rights for live streaming its matches in the US to a silicon valley based streaming services company. As per the terms of distribution, the company must make sure that only users from the US are able to live stream the matches on their platform. Users from other countries in the world must be denied access to these live-streamed matches.

Which of the following options would allow the company to enforce these streaming restrictions? (Select two)

**A.** Use Route 53 based weighted routing policy to restrict distribution of content to only the locations in which you have distribution rights

**B.** Use Route 53 based latency routing policy to restrict distribution of content to only the locations in which you have distribution rights

**C.** Use Route 53 based geolocation routing policy to restrict distribution of content to only the locations in which you have distribution rights

**D.** Use Route 53 based failover routing policy to restrict distribution of content to only the locations in which you have distribution rights

**E.** Use georestriction to prevent users in specific geographic locations from accessing content that you're distributing through a CloudFront web distribution

**Ans C and E.**

**Correct options:**  
Use Route 53 based geolocation routing policy to restrict distribution of content to only the locations in which you have distribution rights  
Geolocation routing lets you choose the resources that serve your traffic based on the geographic location of your users, meaning the location that DNS queries originate from. For example, you might want all queries from Europe to be routed to an ELB load balancer in the Frankfurt region. You can also use geolocation routing to restrict the distribution of content to only the locations in which you have distribution rights.  
Use georestriction to prevent users in specific geographic locations from accessing content that you’re distributing through a CloudFront web distribution  
You can use georestriction, 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.

**Q 19**. Which of the following features of an Amazon S3 bucket can only be suspended once they have been enabled?

**A.** Static Website Hosting  
**B.** Versioning  
**C.** Server Access Logging  
**D.** Requester Pays

**Ans B.**

Once you version-enable a bucket, it can never return to an unversioned state. Versioning can only be suspended once it has been enabled.

Versioning is not enabled by default, however, once you have enabled it, you can't disable it, instead, you can only suspend it on the bucket which will prevent any further versions from being created of your objects, but it will keep all existing versions of objects up to the point of suspension.

**Q 20.** An IT company wants to review its security best-practices after an incident was reported where a new developer on the team was assigned full access to DynamoDB. The developer accidentally deleted a couple of tables from the production environment while building out a new feature.

Which is the MOST effective way to address this issue so that such incidents do not recur?

**A.** Only root user should have full database access in the organization

**B.** Remove full database access for all IAM users in the organization

**C.** The CTO should review the permissions for each new developer's IAM user so that such incidents don't recur

**D.** Use permissions boundary to control the maximum permissions employees can grant to the IAM principals

**And B.**

**Permissions boundaries for IAM entities**

AWS supports *permissions boundaries* for IAM entities (users or roles). A permissions boundary is an advanced feature for using a managed policy to set the maximum permissions that an identity-based policy can grant to an IAM entity. An entity's permissions boundary allows it to perform only the actions that are allowed by both its identity-based policies and its permissions boundaries.

<https://www.youtube.com/watch?v=t8P8ffqWrsY>

Permissions boundaries are additional IAM policies that can be attached to IAM entities (users and roles), and limit the maximum entitlements of the entity. IAM permissions boundaries can only deny entitlements with either an implicit (entitlement is not present in the permissions boundary) or explicit (there is a deny statement in the permissions boundary) deny, and cannot be used to grant an entitlement.

Permissions boundaries are an IAM policy defined in the just same way as other IAM policies, however when used as a permission boundary the policy will apply constraints to the entity to which they are attached.

**Q 21.** A gaming company is developing a mobile game that streams score updates to a backend processor and then publishes results on a leaderboard. The company has hired you as an AWS Certified Solutions Architect Associate to design a solution that can handle major traffic spikes, process the mobile game updates in the order of receipt, and store the processed updates in a highly available database. The company wants to minimize the management overhead required to maintain the solution.

Which of the following will you recommend to meet these requirements?

**A.** Push score updates to Kinesis Data Streams which uses a fleet of EC2 instances (with Auto Scaling) to process the updates in Kinesis Data Streams and then store these processed updates in DynamoDB  
**B.** Push score updates to an SNS topic, subscribe a Lambda function to this SNS topic to process the updates and then store these processed updates in a SQL database running on Amazon EC2  
**C.** Push score updates to Kinesis Data Streams which uses a Lambda function to process these updates and then store these processed updates in DynamoDB  
**D.** Push score updates to an SQS queue which uses a fleet of EC2 instances (with Auto Scaling) to process these updates in the SQS queue and then store these processed updates in an RDS MySQL database

**Ans C.**

To help ingest real-time data or streaming data at large scales, you can use Amazon Kinesis Data Streams (KDS). KDS can continuously capture gigabytes of data per second from hundreds of thousands of sources. The data collected is available in milliseconds, enabling real-time analytics. KDS provides ordering of records, as well as the ability to read and/or replay records in the same order to multiple Amazon Kinesis Applications.  
Lambda integrates natively with Kinesis Data Streams. The polling, checkpointing, and error handling complexities are abstracted when you use this native integration. The processed data can then be configured to be saved in DynamoDB.

**Q 22.** A media agency stores its re-creatable assets on Amazon S3 buckets. The assets are accessed by a large number of users for the first few days and the frequency of access falls down drastically after a week. Although the assets would be accessed occasionally after the first week, but they must continue to be immediately accessible when required. The cost of maintaining all the assets on S3 storage is turning out to be very expensive and the agency is looking at reducing costs as much as possible.

As a Solutions Architect, can you suggest a way to lower the storage costs while fulfilling the business requirements?

**A.** Configure a lifecycle policy to transition the object to Amazon S3 standard-Infrequent Access (S3 Standard-IA) after 30 days

**B.** Configure a lifecycle policy to transition the objects to Amazon S3 Zone-Infrequent Access (S3 Standard-IA) after 7 days

**C.** Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 7 days

**D.** Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.

**Ans B.**

**Explanation**: S3 One Zone-IA is for data that is accessed less frequently, but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ and costs 20% less than S3 Standard-IA. S3 One Zone-IA is ideal for customers who want a lower-cost option for infrequently accessed and re-creatable data but do not require the availability and resilience of S3 Standard or S3 Standard-IA. The minimum storage duration is 30 days before you can transition objects from S3 Standard to S3 One Zone-IA. S3 One Zone-IA offers the same high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval fee. S3 Storage Classes can be configured at the object level, and a single bucket can contain objects stored across S3 Standard, S3 Intelligent-Tiering, S3 Standard-IA, and S3 One Zone-IA. You can also use S3 Lifecycle policies to automatically transition objects between storage classes without any application changes.

**Q 23.** An organization wants to delegate access to a set of users from the development environment so that they can access some resources in the production environment which is managed under another AWS account.

As a solutions architect, which of the following steps would you recommend?

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

**B.** Both IAM roles and IAM users can be used interchangeably for cross-account access

**C.** It is not possible to access cross-account resources

**D.** Create new IAM user credentials for the production environment and share these credentials with the set of users from the development environment

**Ans A.**

**Q 24.** A leading video streaming service delivers billions of hours of content from Amazon S3 to customers around the world. Amazon S3 also serves as the data lake for its big data analytics solution. The data lake has a staging zone where intermediary query results are kept only for 24 hours. These results are also heavily referenced by other parts of the analytics pipeline.

Which of the following is the MOST cost-effective strategy for storing this intermediary query data?

**A.** Store the intermediary query results in S3 Intelligent-Tiering storage class  
**B.** Store the intermediary query results in S3 Standard-Infrequent Access storage class  
**C.** Store the intermediary query results in S3 One Zone-Infrequent Access storage class  
**D.** Store the intermediary query results in S3 Standard storage class

**Explanation**:

Store the intermediary query results in S3 Standard storage class  
S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. Because it delivers low latency and high throughput, S3 Standard is appropriate for a wide variety of use cases, including cloud applications, dynamic websites, content distribution, mobile and gaming applications, and big data analytics. As there is no minimum storage duration charge and no retrieval fee (remember that intermediary query results are heavily referenced by other parts of the analytics pipeline), this is the MOST cost-effective storage class amongst the given options.

**Q 25.** A company has a web application that runs 24\*7 in the production environment. The development team at the company runs a clone of the same application in the dev environment for up to 8 hours every day. The company wants to build the MOST cost-optimal solution by deploying these applications using the best-fit pricing options for EC2 instances.

What would you recommend?

**A.** Use reserved EC2 instances for the production application and spot instances for the dev application.

**B.** Use reserved EC2 instances for the production application and on-demand instances for the dev application

**C.** Use on-demand EC2 instances for the production application and spot instances for the dev application

**D.** Use reserved EC2 instances for the production application and spot block instances for the dev application

**And B.**

**Q 26.** A retail company's dynamic website is hosted using on-premises servers in its data center in the United States. The company is launching its website in Asia, and it wants to optimize the website loading times for new users in Asia. The website's backend must remain in the United States. The website is being launched in a few days, and an immediate solution is needed.

What would you recommend?

**A.** Leverage a Route 53 geo-proximity routing policy pointing to on premises servers

**B.** Use Amazon CloudFront with a custom origin pointing to the on-premises servers

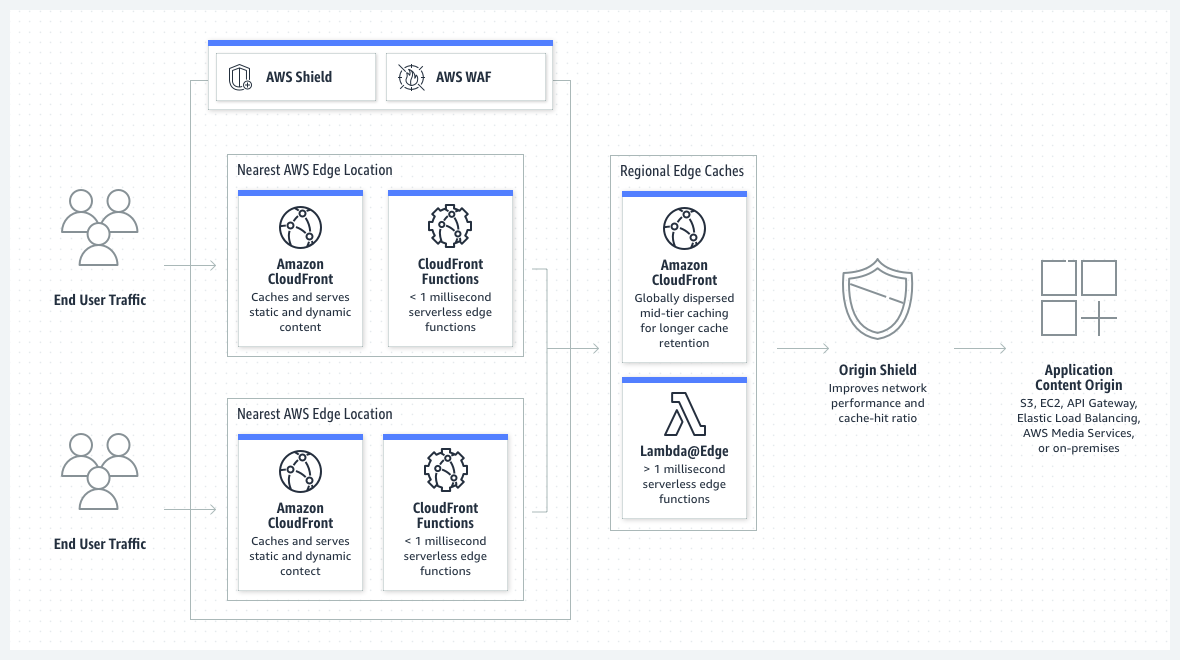
**C.** Use Amazon CloudFront with a custom origin pointing to the DNS record of the website on Route 53

**D.** Migrate the website to Amazon S3. Use cross-Region replication between AWS Regions in the US and Asia.

**And B.**

**Explanation:** Amazon CloudFront is a web service that gives businesses and web application developers an easy and cost-effective way to distribute content with low latency and high data transfer speeds. Amazon CloudFront uses standard cache control headers you set on your files to identify static and dynamic content. You can use different origins for different types of content on a single site – e.g. Amazon S3 for static objects, Amazon EC2 for dynamic content, and custom origins for third-party content.

An origin server stores the original, definitive version of your objects. If you're serving content over HTTP, your origin server is either an Amazon S3 bucket or an HTTP server, such as a web server. Your HTTP server can run on an Amazon Elastic Compute Cloud (Amazon EC2) instance or on a server that you manage; these servers are also known as custom origins.





via - <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>

Amazon CloudFront employs a global network of edge locations and regional edge caches that cache copies of your content close to your viewers. Amazon CloudFront ensures that end-user requests are served by the closest edge location. As a result, viewer requests travel a short distance, improving performance for your viewers. Therefore for the given use case, the users in Asia will enjoy a low latency experience while using the website even though the on-premises servers continue to be in the US.

Incorrect options:

**Use Amazon CloudFront with a custom origin pointing to the DNS record of the website on Route 53** - This option has been added as a distractor. CloudFront cannot have a custom origin pointing to the DNS record of the website on Route 53.

**Migrate the website to Amazon S3. Use cross-Region replication between AWS Regions in the US and Asia** - The use case states that the company operates a dynamic website. You can use Amazon S3 to host a static website. On a static website, individual web pages include static content. They might also contain client-side scripts. By contrast, a dynamic website relies on server-side processing, including server-side scripts, such as PHP, JSP, or ASP.NET. Amazon S3 does not support server-side scripting, but AWS has other resources for hosting dynamic websites. So this option is incorrect.

**Leverage a Route 53 geo-proximity routing policy pointing to on-premises servers** - Since the on-premises servers continue to be in the US, so even using a Route 53 geo-proximity routing policy that directs the users in Asia to the on-premises servers in the US would not reduce the latency for the users in Asia. So this option is incorrect.

References:

<https://aws.amazon.com/cloudfront/>

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteHosting.html>

**Q 27.** A company runs a data processing workflow that takes about 60 minutes to complete. The workflow can withstand disruptions and it can be started and stopped multiple times.

Which is the most cost-effective solution to build a solution for the workflow?

**A.** Use EC2 spot instances to run the workflow processes

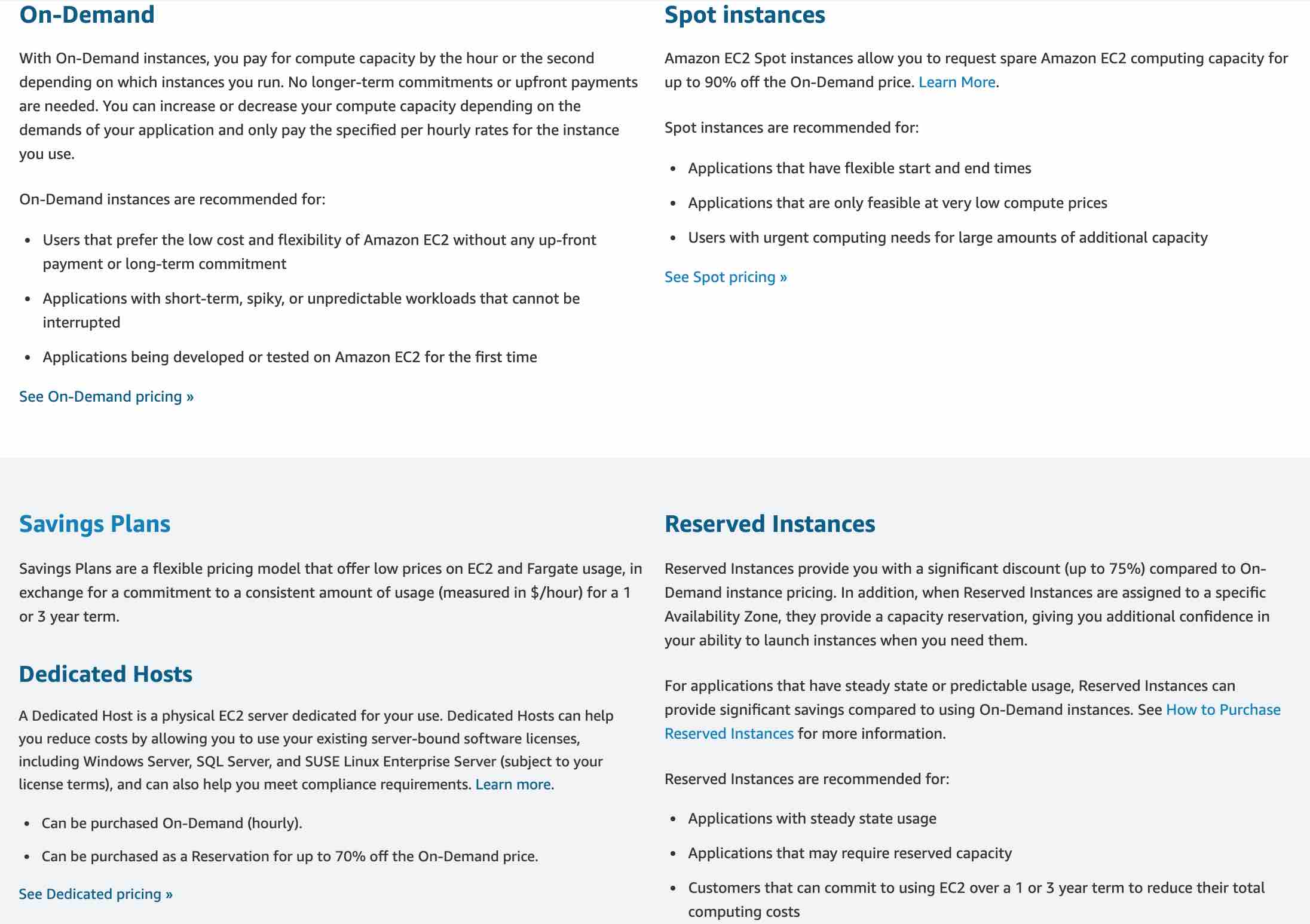
**B.** Use EC2 on-demand instances to run the workflow processes

**C.** Use AWS Lambda function to run the workflow processes

**D.** Use EC2 reserved instances to run the workflow processes

**Ans A.**

**Explanation:**



via - <https://aws.amazon.com/ec2/pricing/>

Amazon EC2 Spot instances allow you to request spare Amazon EC2 computing capacity for up to 90% off the On-Demand price.

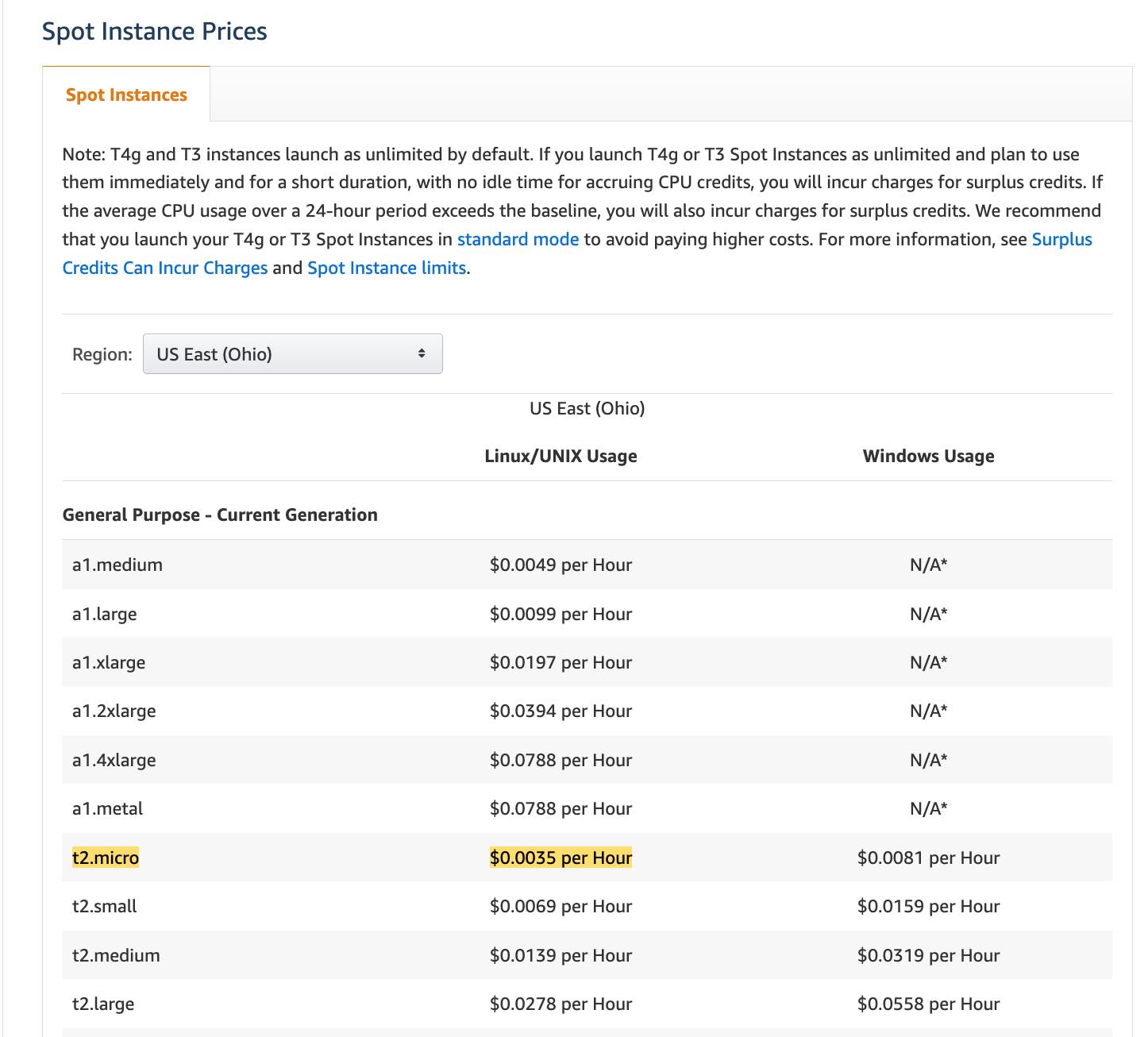
Spot instances are recommended for:

Applications that have flexible start and end times Applications that are feasible only at very low compute prices Users with urgent computing needs for large amounts of additional capacity

For the given use case, spot instances offer the most cost-effective solution as the workflow can withstand disruptions and can be started and stopped multiple times.

For example, considering a process that runs for an hour and needs about 1024 MB of memory, spot instance pricing for a t2.micro instance (having 1024 MB of RAM) is $0.0035 per hour.

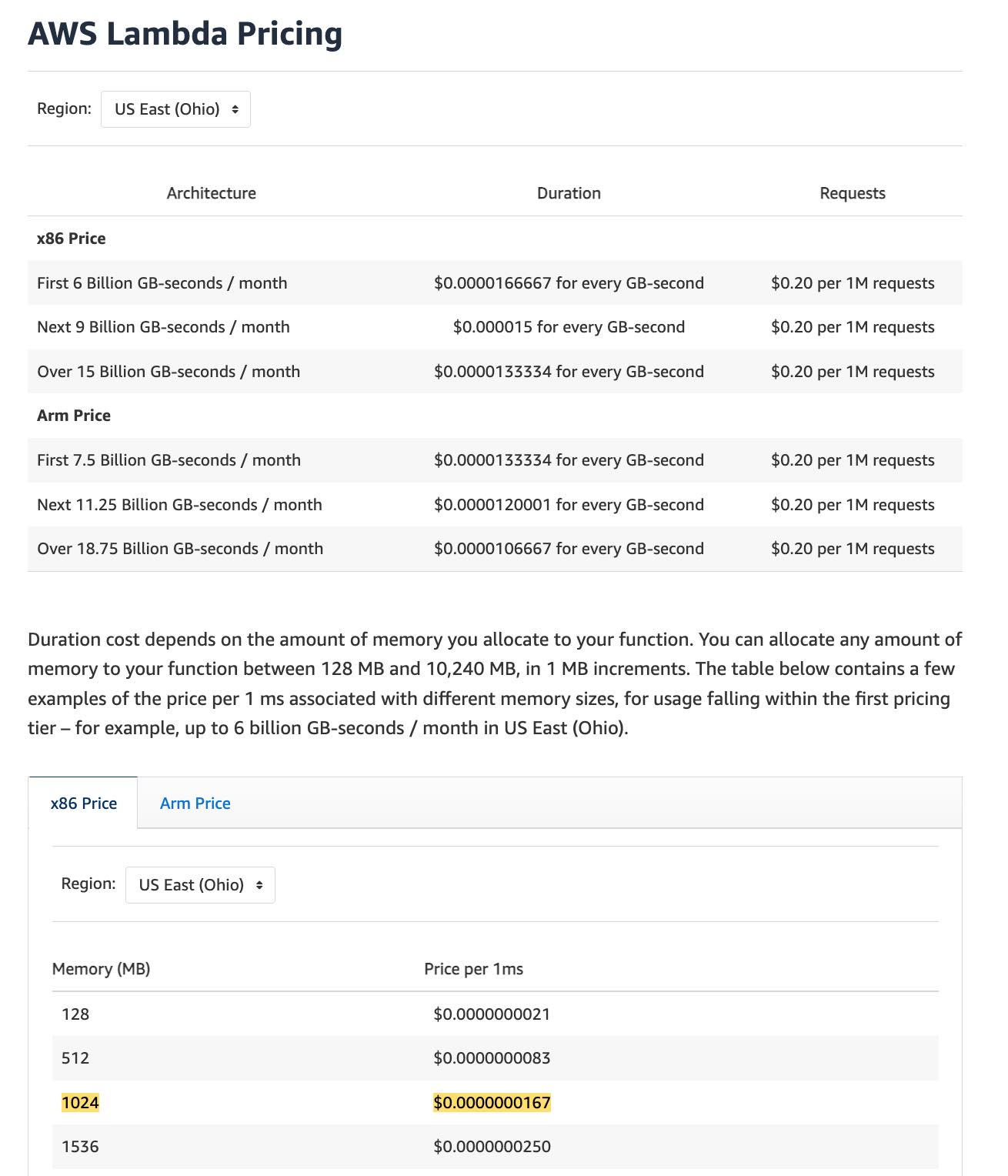
Spot instance pricing:



via - <https://aws.amazon.com/ec2/spot/pricing/>

Contrast this with the pricing of a Lambda function (having 1024 MB of allocated memory), which comes out to $0.0000000167 per 1ms or $0.06 per hour ($0.0000000167 \* 1000 \* 60 \* 60 per hour).

Lambda function pricing:



via - <https://aws.amazon.com/lambda/pricing/>

Thus, a spot instance turns out to be about 20 times cost effective than a Lambda function to meet the requirements of the given use case.

Incorrect options:

**Use AWS Lambda function to run the workflow processes** - As mentioned in the explanation above, a Lambda function turns out to be 20 times more expensive than a spot instance to meet the workflow requirements of the given use case, so this option is incorrect. You should also note that the maximum execution time of a Lambda function is 15 minutes, so the workflow process would be disrupted for sure. On the other hand, it is certainly possible that the workflow process can be completed in a single run on the spot instance (the average frequency of stop instance interruption across all Regions and instance types is <10%).

**Use EC2 on-demand instances to run the workflow processes**

**Use EC2 reserved instances to run the workflow processes**

You should note that both on-demand and reserved instances are more expensive than spot instances. In addition, reserved instances have a term of 1 year or 3 years, so they are not suited for the given workflow. Therefore, both these options are incorrect.

**Q 28.** A Big Data analytics company wants to set up an AWS cloud architecture that throttles requests in case of sudden traffic spikes. The company is looking for AWS services that can be used for buffering or throttling to handle such traffic variations.

Which of the following services can be used to support this requirement?

**A.** Amazon Gateway Endpoints, Amazon SQS and Amazon Kinesis  
**B.** Amazon API Gateway, Amazon SQS and Amazon Kinesis  
**C.** Elastic Load Balancer, Amazon SQS, AWS Lambda  
**D.** Amazon SQS, Amazon SNS and AWS Lambda

**Ans B.**

**Explanation**

Throttling is the process of limiting the number of requests an authorized program can submit to a given operation in a given amount of time.  
Amazon API Gateway, Amazon SQS and Amazon Kinesis – To prevent your API from being overwhelmed by too many requests, Amazon API Gateway throttles requests to your API using the token bucket algorithm, where a token counts for a request. Specifically, API Gateway sets a limit on a steady-state rate and a burst of request submissions against all APIs in your account. In the token bucket algorithm, the burst is the maximum bucket size.  
Amazon SQS – 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. Amazon SQS offers buffer capabilities to smooth out temporary volume spikes without losing messages or increasing latency.  
Amazon Kinesis – Amazon Kinesis is a fully managed, scalable service that can ingest, buffer, and process streaming data in real-time.

**Q 29.** A leading social media analytics company is contemplating moving its dockerized application stack into AWS Cloud. The company is not sure about the pricing for using Elastic Container Service (ECS) with the EC2 launch type compared to the Elastic Container Service (ECS) with the Fargate launch type.  
Which of the following is correct regarding the pricing for these two services?

**A.** Both ECS with EC2 launch type and ECS with Fargate launch type are charged based on vCPU and memory resources that the containerized application requests  
**B.** Both ECS with EC2 launch type and ECS with Fargate launch type are charged based on EC2 instances and EBS volumes used  
**C.** ECS with EC2 launch type is charged based on EC2 instances and EBS volumes used. ECS with Fargate launch type is charged based on vCPU and memory resources that the containerized application requests  
**D.** Both ECS with EC2 launch type and ECS with Fargate launch type are just charged based on Elastic Container Service used per hour

**Ans C.**

**Explanation**  
ECS with EC2 launch type is charged based on EC2 instances and EBS volumes used. ECS with Fargate launch type is charged based on vCPU and memory resources that the containerized application requests  
Amazon Elastic Container Service (Amazon ECS) is a fully managed container orchestration service. ECS allows you to easily run, scale, and secure Docker container applications on AWS.  
With the Fargate launch type, you pay for the amount of vCPU and memory resources that your containerized application requests. vCPU and memory resources are calculated from the time your container images are pulled until the Amazon ECS Task\* terminates, rounded up to the nearest second. With the EC2 launch type, there is no additional charge for the EC2 launch type. You pay for AWS resources (e.g. EC2 instances or EBS volumes) you create to store and run your application.

**Q 30.** A company is in the process of migrating its on-premises SMB file shares to AWS so the company can get out of the business of managing multiple file servers across dozens of offices. The company has 200TB of data in its file servers. The existing on-premises applications and native Windows workloads should continue to have low latency access to this data without any disruptions after the migration. The company also wants any new applications deployed on AWS to have access to this migrated data.

Which of the following is the best solution to meet this requirement?

**A.** Use Amazon Storage Gateway’s File Gateway to provide low latency, on-premises access to fully managed file shares in Amazon S3. The applications deployed on AWS can access this data directly from Amazon S3

**B.** Use Amazon FSx File Gateway to provide low-latency,on-premises access to fully managed file shares in Amazon EFS. The applications deployed on AWS can access this data directly from Amazon EFS.

**C.** Use Amazon storage Gateway’s File Gateway to provide low-latency,on-premises access to fully managed file shares in Amazon FSx for Window File Server. The application deployed on AWS can access this data directly from Amazon FSx in AWS

**D.** Use Amazon FSx File Gateway to provide low-latency, on-premises access to fully managed file shares in Amazon FSx for Windows File Server. The applications deployed on AWS can access this data directly from Amazon FSx in AWS

**Ans D.**

**Q 31**. A gaming company uses Amazon Aurora as its primary database service. The company has now deployed 5 multi-AZ read replicas to increase the read throughput and for use as failover target. The replicas have been assigned the following failover priority tiers and corresponding sizes are given in parentheses: tier-1 (16TB), tier-1 (32TB), tier-10 (16TB), tier-15 (16TB), tier-15 (32TB).  
In the event of a failover, Amazon RDS will promote which of the following read replicas?  
  
**A.** Tier-1 (32TB)  
**B.** Tier-1 (16TB)  
**C.** Tier-15 (32TB)  
**D.** Tier-10 (16TB)

**Ans A.**

**Explanation:** Amazon Aurora features a distributed, fault-tolerant, self-healing storage system that auto-scales up to 64TB per database instance. It delivers high performance and availability with up to 15 low-latency read replicas, point-in-time recovery, continuous backup to Amazon S3, and replication across three Availability Zones (AZs).  
For Amazon Aurora, each Read Replica is associated with a priority tier (0-15). In the event of a failover, Amazon Aurora will promote the Read Replica that has the highest priority (the lowest numbered tier). If two or more Aurora Replicas share the same priority, then Amazon RDS promotes the replica that is largest in size. If two or more Aurora Replicas share the same priority and size, then Amazon Aurora promotes an arbitrary replica in the same promotion tier.  
Therefore, for this problem statement, the Tier-1 (32TB) replica will be promoted.

**Q 32**. A retail company uses Amazon EC2 instances, API Gateway, Amazon RDS, Elastic Load Balancer and CloudFront services. To improve the security of these services, the Risk Advisory group has suggested a feasibility check for using the Amazon GuardDuty service.

Which of the following would you identify as data sources supported by GuardDuty?

**A.** VPC Flow Logs, API Gateway logs, S3 access logs  
**B.** ELB logs, DNS logs, CloudTrail events  
**C.** VPC Flow Logs, DNS logs, CloudTrail events  
**D.** CloudFront logs, API Gateway logs, CloudTrail events

**Ans C.**

**Explanation**:  
VPC Flow Logs, DNS logs, CloudTrail events – Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts, workloads, and data stored in Amazon S3. With the cloud, the collection and aggregation of account and network activities is simplified, but it can be time-consuming for security teams to continuously analyze event log data for potential threats. With GuardDuty, you now have an intelligent and cost-effective option for continuous threat detection in AWS. The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats.  
GuardDuty analyzes tens of billions of events across multiple AWS data sources, such as AWS CloudTrail events, Amazon VPC Flow Logs, and DNS logs.  
With a few clicks in the AWS Management Console, GuardDuty can be enabled with no software or hardware to deploy or maintain. By integrating with Amazon CloudWatch Events, GuardDuty alerts are actionable, easy to aggregate across multiple accounts, and straightforward to push into existing event management and workflow systems.

**Q 33.** A large financial institution operates an on-premises data center with hundreds of PB of data managed on Microsoft’s Distributed File System (DFS). The CTO wants the organization to transition into a hybrid cloud environment and run data-intensive analytics workloads that support DFS.

Which of the following AWS services can facilitate the migration of these workloads?

**A.** Amazon FSx for Lustre  
**B.** Amazon FSx for Windows File Server  
**C.** AWS Managed Microsoft AD  
**D.** Microsoft SQL Server on Amazon

**Ans B.**

**Explanation**: Amazon FSx supports the use of Microsoft’s Distributed File System (DFS) to organize shares into a single folder structure up to hundreds of PB in size.

**Q 34.** A junior scientist working with the Deep Space Research Laboratory at NASA is trying to upload a high-resolution image of a nebula into Amazon S3. The image size is approximately 3GB. The junior scientist is using S3 Transfer Acceleration (S3TA) for faster image upload. It turns out that S3TA did not result in an accelerated transfer. Given this scenario, which of the following is correct regarding the charges for this image transfer?

**A.** The junior scientist needs to pay both S3 transfer charges and S3TA transfer charges for the image upload.  
**B.** The junior scientist does not need to pay any transfer charges for the image upload.  
**C.** The junior scientist only needs to pay S3 transfer charges for the image upload.  
**D.** The junior scientist only needs to pay S3TA transfer charges for the image upload.

**Ans B.**

**Explanation**: No S3 data transfer charges when data is transferred in from the internet. Also with S3TA, pay only for transfers that are accelerated. Since S3TA did not result in an accelerated transfer so no transfer charges.

**Q 35.** The solo founder at a tech startup has just created a brand new AWS account. The founder has provisioned an EC2 instance 1A which is running in region A. Later, he takes a snapshot of the instance 1A and then creates a new AMI in region A from this snapshot. This AMI is then copied into another region B. The founder provisions an instance 1B in region B using this new AMI in region B.

At this point in time, what entities exist in region B?

A. 1 EC2 instance and 1 snapshot exist in region B  
B. 1 EC2 instance, 1 AMI and 1 snapshot exist in region B  
C. 1 EC2 instance and 1 AMI exist in region B  
D. 1 EC2 instance and 2 AMIs exist in region B

**Ans B**

**Explanation:** An Amazon Machine Image (AMI) provides the information required to launch an instance. You must specify an AMI when you launch an instance. When the new AMI is copied from region A into region B, it automatically creates a snapshot in region B because AMIs are based on the underlying snapshots. Further, an instance is created from this AMI in region B. Hence, we have 1 EC2 instance, 1 AMI and 1 snapshot in region B.

**Q 36**. The DevOps team at an e-commerce company wants to perform some maintenance work on a specific EC2 instance that is part of an Auto Scaling group using a step scaling policy. The team is facing a maintenance challenge - every time the team deploys a maintenance patch, the instance health check status shows as out of service for a few minutes. This causes the Auto Scaling group to provision another replacement instance immediately.

As a solutions architect, which are the MOST time/resource efficient steps that you would recommend so that the maintenance work can be completed at the earliest? (Select two)

**A.** Put the instance into the Standby state and then update the instance by applying the maintenance patch. Once the instance is ready, you can exit the Standby state and then return the instance to service

**B.** Delete the Auto Scaling group and apply the maintenance fix to the given instance. Create a new Auto Scaling group and add all the instances again using the manual scaling policy

**C.** Suspend the ReplaceUnhealthy process type for the Auto Scaling group and apply the maintenance patch to the instance. Once the instance is ready, you can manually set the instance's health status back to healthy and activate the ReplaceUnhealthy process type again

**D.** Take a snapshot of the instance, create a new AMI and then launch a new instance using this AMI. Apply the maintenance patch to this new instance and then add it back to the Auto Scaling Group by using the manual scaling policy. Terminate the earlier instance that had the maintenance issue

**E.** Suspend the ScheduledActions process type for the Auto Scaling group and apply the maintenance patch to the instance. Once the instance is ready, you can you can manually set the instance's health status back to healthy and activate the ScheduledActions process type again

**Ans A and C.**

**Q 37.** As part of a pilot program, a biotechnology company wants to integrate data files from its on-premises analytical application with AWS Cloud via an NFS interface.

Which of the following AWS service is the MOST efficient solution for the given use-case?

**A.** AWS Storage Gateway - File Gateway

**B.** AWS Storage Gateway - Volume Gateway

**C.** AWS Storage Gateway - Tape Gateway

**D.** AWS Site-to-Site VPN

**Ans A.**

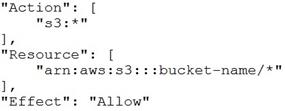
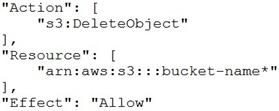
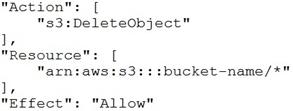
**Q 38.** A new DevOps engineer has joined a large financial services company recently. As part of his onboarding, the IT department is conducting a review of the checklist for tasks related to AWS Identity and Access Management.  
As a solutions architect, which best practices would you recommend (Select two)?  
  
**A.** Create a minimum number of accounts and share these account credentials among employees  
**B.** Configure AWS CloudTrail to record all account activity  
**C.** Enable MFA for privileged users  
**D.** Grant maximum privileges to avoid assigning privileges again  
**E.** Use user credentials to provide access specific permissions for Amazon EC2 instances

**Ans B and C.**

**Explanation**: Enable MFA for privileged users – As per the AWS best practices, it is better to enable Multi Factor Authentication (MFA) for privileged users via an MFA-enabled mobile device or hardware MFA token.  
Configure AWS CloudTrail to record all account activity – AWS recommends to turn on CloudTrail to log all IAM actions for monitoring and audit purposes.

**Q 39.** A development team requires permissions to list an S3 bucket and delete objects from that bucket. A systems administrator has created the following IAM policy to provide access to the bucket and applied that policy to the group. The group is not able to delete objects in the bucket. The company follows the principle of least privilege.

“Version”: “2021-10-17”,  
“Statement”: [  
{  
“Action”: [  
“s3:ListBucket”,  
“s3:DeleteObject”  
],  
“Resource”: [  
“arn:aws:s3:::example-bucket”  
],  
“Effect”: “Allow”  
}  
]  
Which statement should a solutions architect add to the policy to address this issue?

**A.**  
  
**B.**  
  
**C.**  
  
**D.**  


**Ans D**.

**Explanation:**

The main elements of a policy statement are:  
Effect: Specifies whether the statement will Allow or Deny an action (Allow is the effect defined here).  
Action: Describes a specific action or actions that will either be allowed or denied to run based on the Effect entered. API actions are unique to each service (DeleteObject is the action defined here).  
Resource: Specifies the resources—for example, an S3 bucket or objects—that the policy applies to in Amazon Resource Name (ARN) format ( example-bucket/\* is the resource defined here).  
This policy provides the necessary delete permissions on the resources of the S3 bucket to the group.

**Q 40.** The engineering team at an e-commerce company wants to establish a dedicated, encrypted, low latency, and high throughput connection between its data center and AWS Cloud. The engineering team has set aside sufficient time to account for the operational overhead of establishing this connection.

As a solutions architect, which of the following solutions would you recommend to the company?

**A.** Use AWS Direct Connect plus VPN to establish a connection between the data center and AWS Cloud  
**B.** Use site-to-site VPN to establish a connection between the data center and AWS Cloud  
**C.** Use VPC transit gateway to establish a connection between the data center and AWS Cloud  
**D.** Use AWS Direct Connect to establish a connection between the data center and AWS Cloud

**Ans A.**

**Explanation:**  
AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. AWS Direct Connect lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations.  
With AWS Direct Connect plus VPN, you can combine one or more AWS Direct Connect dedicated network connections with the Amazon VPC VPN. This combination provides an IPsec-encrypted private connection that also reduces network costs, increases bandwidth throughput, and provides a more consistent network experience than internet-based VPN connections.  
This solution combines the AWS managed benefits of the VPN solution with low latency, increased bandwidth, more consistent benefits of the AWS Direct Connect solution, and an end-to-end, secure IPsec connection. Therefore, AWS Direct Connect plus VPN is the correct solution for this use-case.

**Q 41**. A research group needs a fleet of EC2 instances for a specialized task that must deliver high random I/O performance. Each instance in the fleet would have access to a dataset that is replicated across the instances. Because of the resilient application architecture, the specialized task would continue to be processed even if any instance goes down, as the underlying application architecture would ensure the replacement instance has access to the required dataset.  
Which of the following options is the MOST cost-optimal and resource-efficient solution to build this fleet of EC2 instances?  
Options  
A. Use EBS based EC2 instances  
B. Use EC2 instances with EFS mount points  
C. Use EC2 instances with access to S3 based storage  
D. Use Instance Store based EC2 instances

**Ans D.**

**Explanation**: An instance store provides temporary block-level storage for your instance. This storage is located on disks that are physically attached to the host computer. Instance store is ideal for the temporary storage of information that changes frequently such as buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as a load-balanced pool of web servers. Instance store volumes are included as part of the instance’s usage cost.  
As Instance Store based volumes provide high random I/O performance at low cost (as the storage is part of the instance’s usage cost) and the resilient architecture can adjust for the loss of any instance, therefore you should use Instance Store based EC2 instances for this use-case.

**Q 42.** The sourcing team at the US headquarters of a global e-commerce company is preparing a spreadsheet of the new product catalog. The spreadsheet is saved on an EFS file system created in us-east-1 region. The sourcing team counterparts from other AWS regions such as Asia Pacific and Europe also want to collaborate on this spreadsheet.

As a solutions architect, what is your recommendation to enable this collaboration with the LEAST amount of operational overhead?

**A.** The spreadsheet will have to be copied in Amazon S3 which can then be accessed from any AWS region.  
**B.** The spreadsheet will have to be copied into EFS file systems of other AWS regions as EFS is a regional service and it does not allow access from other AWS regions.  
**C.** The spreadsheet on the EFS file system can be accessed from EC2 instances running in other AWS regions by using an inter-region VPC peering connection.  
**D.** The spreadsheet data will have to be moved into an RDS MySQL database which can then be accessed from any AWS region.

**Ans C.**

**Announcing Support for Inter-Region VPC Peering**

Amazon EC2 now allows peering relationships to be established between Virtual Private Clouds (VPCs) across different AWS regions. Inter-Region VPC Peering allows VPC resources like EC2 instances, RDS databases and Lambda functions running in different AWS regions to communicate with each other using private IP addresses, without requiring gateways, VPN connections or separate network appliances.

Inter-Region VPC Peering provides a simple and cost-effective way to share resources between regions or replicate data for geographic redundancy. Built on the same horizontally scaled, redundant, and highly available technology that powers VPC today, Inter-Region VPC Peering encrypts inter-region traffic with no single point of failure or bandwidth bottleneck. Traffic using Inter-Region VPC Peering always stays on the global AWS backbone and never traverses the public internet, thereby reducing threat vectors, such as common exploits and DDoS attacks.

**Q 43.** An e-commerce company is looking for a solution with high availability, as it plans to migrate its flagship application to a fleet of Amazon EC2 instances. The solution should allow for content-based routing as part of the architecture.

As a Solutions Architect, which of the following will you suggest for the company?

**A.** Use a Network Load Balancer for distributing traffic to the EC2 instances spread across different Availability Zones. Configure a Private IP address to mask any failure of an instance  
**B.** Use an Application Load Balancer for distributing traffic to the EC2 instances spread across different Availability Zones. Configure Auto Scaling group to mask any failure of an instance  
**C.** Use an Auto Scaling group for distributing traffic to the EC2 instances spread across different Availability Zones. Configure an Elastic IP address to mask any failure of an instance  
**D.** Use an Auto Scaling group for distributing traffic to the EC2 instances spread across different Availability Zones. Configure a Public IP address to mask any failure of an instance

**Ans B.**

**Routing:** NLB just forward requests whereas ALB examines the contents of the HTTP request header to determine where to route the request. So, an ALB support advanced request (content-based) routing.

**Q 44.** A company manages a multi-tier social media application that runs on 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. As a solutions architect, you have been tasked to make the application more resilient to periodic spikes in request rates.

Which of the following solutions would you recommend for the given use-case? (Select two)

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

**Ans D and E.**

**Q 45.** The payroll department at a company initiates several computationally intensive workloads on EC2 instances at a designated hour on the last day of every month. The payroll department has noticed a trend of severe performance lag during this hour. The engineering team has figured out a solution by using Auto Scaling Group for these EC2 instances and making sure that 10 EC2 instances are available during this peak usage hour. For normal operations only 2 EC2 instances are enough to cater to the workload.

As a solutions architect, which of the following steps would you recommend to implement the solution?

**A.** Configure your Auto Scaling group by creating a scheduled action that kicks-off at the designated hour on the last day of the month. Set the desired capacity of instances to 10. This causes the scale-out to happen before peak traffic kicks in at the designated hour .  
**B.** Configure your Auto Scaling group by creating a scheduled action that kicks-off at the designated hour on the last day of the month. Set the min count as well as the max count of instances to 10. This causes the scale-out to happen before peak traffic kicks in at the designated hour.  
**C.** Configure your Auto Scaling group by creating a target tracking policy and setting the instance count to 10 at the designated hour. This causes the scale-out to happen before peak traffic kicks in at the designated hour.  
**D.** Configure your Auto Scaling group by creating a simple tracking policy and setting the instance count to 10 at the designated hour. This causes the scale-out to happen before peak traffic kicks in at the designated hour.

**Ans A.**

**Q 46.** A US-based healthcare startup is building an interactive diagnostic tool for COVID-19 related assessments. The users would be required to capture their personal health records via this tool. As this is sensitive health information, the backup of the user data must be kept encrypted in S3. The startup does not want to provide its own encryption keys but still wants to maintain an audit trail of when an encryption key was used and by whom.

Which of the following is the BEST solution for this use-case?

A. Use SSE-KMS to encrypt the user data on S3  
B. Use SSE-S3 to encrypt the user data on S3  
C. Use SSE-C to encrypt the user data on S3  
D. Use client-side encryption with client provided keys and then upload the encrypted user data to S3

**Ans A.**

**Q 47.** The flagship application for a gaming company connects to an Amazon Aurora database and the entire technology stack is currently deployed in the United States. Now, the company has plans to expand to Europe and Asia for its operations. It needs the games table to be accessible globally but needs the users and games\_played tables to be regional only.

How would you implement this with minimal application refactoring?

**A.** Use a DynamoDB global table for the games table and use Amazon Aurora for the users and games\_played tables  
**B.** Use an Amazon Aurora Global Database for the games table and use DynamoDB tables for the users and games\_played tables  
**C.** Use an Amazon Aurora Global Database for the games table and use Amazon Aurora for the users and games\_played tables  
**D.** Use a DynamoDB global table for the games table and use DynamoDB tables for the users and games\_played tables

**Ans C.**

**Explanation:**Amazon Aurora global databases span multiple AWS Regions, enabling low latency global reads and providing fast recovery from the rare outage that might affect an entire AWS Region. An Aurora global database has a primary DB cluster in one Region, and up to five secondary DB clusters in different Regions.

Amazon Aurora is a MySQL and PostgreSQL-compatible relational database built for the cloud, that combines the performance and availability of traditional enterprise databases with the simplicity and cost-effectiveness of open source databases. Amazon Aurora features a distributed, fault-tolerant, self-healing storage system that auto-scales up to 64TB per database instance. Aurora is not an in-memory database.  
Amazon Aurora Global Database is designed for globally distributed applications, allowing a single Amazon Aurora database to span multiple AWS regions. It replicates your data with no impact on database performance, enables fast local reads with low latency in each region, and provides disaster recovery from region-wide outages. Amazon Aurora Global Database is the correct choice for the given use-case.  
For the given use-case, we, therefore, need to have two Aurora clusters, one for the global table (games table) and the other one for the local tables (users and games\_played tables).

**Q 48.** A financial services company uses Amazon GuardDuty for analyzing its AWS account metadata to meet the compliance guidelines. However, the company has now decided to stop using GuardDuty service. All the existing findings have to be deleted and cannot persist anywhere on AWS Cloud.  
Which of the following techniques will help the company meet this requirement?  
  
**A.** Suspend the service in the general settings  
**B.** De-register the service under services tab  
**C.** Disable the service in the general settings  
**D.** Raise a service request with Amazon to completely delete the data from all their backups

**Ans C.**

**Explanation**: Amazon GuardDuty offers threat detection that enables you to continuously monitor and protect your AWS accounts, workloads, and data stored in Amazon S3. GuardDuty analyzes continuous streams of meta-data generated from your account and network activity found in AWS CloudTrail Events, Amazon VPC Flow Logs, and DNS Logs. It also uses integrated threat intelligence such as known malicious IP addresses, anomaly detection, and machine learning to identify threats more accurately.  
Disable the service in the general settings – Disabling the service will delete all remaining data, including your findings and configurations before relinquishing the service permissions and resetting the service. So, this is the correct option for our use case.

**Q 49.** An IT consultant is helping the owner of a medium-sized business set up an AWS account. What are the security recommendations he must follow while creating the AWS account root user? (Select two)

**A.** Encrypt the access keys and save them on Amazon S3  
**B.** Create AWS account root user access keys and share those keys only with the business owner  
**C.** Enable Multi Factor Authentication (MFA) for the AWS account root user account  
**D.** Send an email to the business owner with details of the login username and password for the AWS root user. This will help the business owner to troubleshoot any login issues in future  
**E.** Create a strong password for the AWS account root user

**Ans C and E.**

**Q 50.** A financial services company recently launched an initiative to improve the security of its AWS resources and it had enabled AWS Shield Advanced across multiple AWS accounts owned by the company. Upon analysis, the company has found that the costs incurred are much higher than expected.

Which of the following would you attribute as the underlying reason for the unexpectedly high costs for AWS Shield Advanced service?

**A.** AWS Shield Advanced also covers AWS Shield Standard plan, thereby resulting in increased costs  
**B.** Savings Plans has not been enabled for the AWS Shield Advanced service across all the AWS accounts  
**C.** Consolidated billing has not been enabled. All the AWS accounts should fall under a single consolidated billing for the monthly fee to be charged only once  
**D.** AWS Shield Advanced is being used for custom servers, that are not part of AWS Cloud, thereby resulting in increased costs

**Ans C.**

**Explanation:** If your organization has multiple AWS accounts, then you can subscribe multiple AWS Accounts to AWS Shield Advanced by individually enabling it on each account using the AWS Management Console or API. You will pay the monthly fee once as long as the AWS accounts are all under a single consolidated billing, and you own all the AWS accounts and resources in those accounts.

**Q 51.** The IT department at a consulting firm is conducting a training workshop for new developers. As part of an evaluation exercise on Amazon S3, the new developers were asked to identify the invalid storage class lifecycle transitions for objects stored on S3.

Can you spot the INVALID lifecycle transitions from the options below? (Select two)

**A.** S3 Intelligent-Tiering => S3 Standard  
**B.** S3 One Zone-IA => S3 Standard-IA  
**C.** S3 Standard => S3 Intelligent-Tiering  
**D.** S3 Standard-IA => S3 Intelligent-Tiering  
**E.** S3 Standard-IA => S3 One Zone-IA

**Ans A and B.**

**Explanation:** As the question wants to know about the INVALID lifecycle transitions, the following options are the correct answers –  
S3 Intelligent-Tiering => S3 Standard  
S3 One Zone-IA(Infrequent Access) => S3 Standard-IA  
Following are the unsupported life cycle transitions for S3 storage classes – Any storage class to the S3 Standard storage class. Any storage class to the Reduced Redundancy storage class.

The S3 Intelligent-Tiering storage class to the S3 Standard-IA storage class.

The S3 One Zone-IA storage class to the S3 Standard-IA or S3 Intelligent-Tiering storage classes.

Incorrect options:  
S3 Standard => S3 Intelligent-Tiering  
S3 Standard-IA => S3 Intelligent-Tiering  
S3 Standard-IA => S3 One Zone-IA  
Here are the supported life cycle transitions for S3 storage classes –

The S3 Standard storage class to any other storage class.

Any storage class to the S3 Glacier or S3 Glacier Deep Archive storage classes.

The S3 Standard-IA storage class to the S3 Intelligent-Tiering or S3 One Zone-IA storage classes.

The S3 Intelligent-Tiering storage class to the S3 One Zone-IA storage class.

The S3 Glacier storage class to the S3 Glacier Deep Archive storage class.


                    Amazon S3 storage class waterfall graphic.
                

**Q 52.** A healthcare startup needs to enforce compliance and regulatory guidelines for objects stored in Amazon S3. One of the key requirements is to provide adequate protection against accidental deletion of objects.

As a solutions architect, what are your recommendations to address these guidelines? (Select two)

**A.** Establish a process to get managerial approval for deleting S3 objects  
**B.** Create an event trigger on deleting any S3 object. The event invokes an SNS notification via email to the IT manager  
**C.** Enable versioning on the bucket  
**D.** Change the configuration on AWS S3 console so that the user needs to provide additional confirmation while deleting any S3 object  
**E.** Enable MFA delete on the bucket

**Ans C and E.**

**Q 53.** A leading carmaker would like to build a new car-as-a-sensor service by leveraging fully serverless components that are provisioned and managed automatically by AWS. The development team at the carmaker does not want an option that requires the capacity to be manually provisioned, as it does not want to respond manually to changing volumes of sensor data.

Given these constraints, which of the following solutions is the BEST fit to develop this car-as-a-sensor service?

**A.** Ingest the sensor data in a Kinesis Data Stream, which is polled by a Lambda function in batches, and the data is written into an auto-scaled DynamoDB table for downstream processing  
**B.** Ingest the sensor data in an Amazon SQS standard queue, which is polled by a Lambda function in batches and the data is written into an auto-scaled DynamoDB table for downstream processing  
**C.** Ingest the sensor data in an Amazon SQS standard queue, which is polled by an application running on an EC2 instance and the data is written into an auto-scaled DynamoDB table for downstream processing  
**D.** Ingest the sensor data in a Kinesis Data Stream, which is polled by an application running on an EC2 instance and the data is written into an auto-scaled DynamoDB table for downstream processing

**Ans B.**

**Q 54.** A major bank is using SQS to migrate several core banking applications to the cloud to ensure high availability and cost efficiency while simplifying administrative complexity and overhead. The development team at the bank expects a peak rate of about 1000 messages per second to be processed via SQS. It is important that the messages are processed in order.

Which of the following options can be used to implement this system?

**A.** Use Amazon SQS FIFO queue in batch mode of 4 messages per operation to process the messages at the peak rate  
**B.** Use Amazon SQS FIFO queue to process the messages  
**C.** Use Amazon SQS standard queue to process the messages  
**D.** Use Amazon SQS FIFO queue in batch mode of 2 messages per operation to process the messages at the peak rate

**Ans A.**

**Explanation**: Use Amazon SQS FIFO queue in batch mode of 4 messages per operation to process the messages at the peak rate  
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 offers two types of message queues – Standard queues vs FIFO queues.  
For FIFO queues, the order in which messages are sent and received is strictly preserved (i.e. First-In-First-Out). On the other hand, the standard SQS queues offer best-effort ordering. This means that occasionally, messages might be delivered in an order different from which they were sent.  
By default, FIFO queues support up to 300 messages per second (300 send, receive, or delete operations per second). When you batch 10 messages per operation (maximum), FIFO queues can support up to 3,000 messages per second. Therefore you need to process 4 messages per operation so that the FIFO queue can support up to 1200 messages per second, which is well within the peak rate.

**Q 56**. An Electronic Design Automation (EDA) application produces massive volumes of data that can be divided into two categories. The ‘hot data’ needs to be both processed and stored quickly in a parallel and distributed fashion. The ‘cold data’ needs to be kept for reference with quick access for reads and updates at a low cost.  
Which of the following AWS services is BEST suited to accelerate the aforementioned chip design process?

A. AWS Glue  
B. Amazon EMR  
C. Amazon FSx for Windows File Server  
D. Amazon FSx for Lustre

Ans D.

The keyword here is “parallel.” Based on this AWS FAQS, Amazon FSx for Lustre provides a parallel file system. Since the scenario also stated that the application consumes thousands of data sets to train its machine learning model. We can take a look at this part of the Amazon FSx for Lustre

**Q 57.** A company uses Amazon S3 buckets for storing sensitive customer data. The company has defined different retention periods for different objects present in the Amazon S3 buckets, based on the compliance requirements. But, the retention rules do not seem to work as expected.

Which of the following options represent a valid configuration for setting up retention periods for objects in Amazon S3 buckets? (Select two)

**A.** When you apply a retention period to an object version explicitly, you specify a Retain Until Date for the object version  
**B.** You cannot place a retention period on an object version through a bucket default setting  
**C.** When you use bucket default settings, you specify a Retain Until Date for the object version  
**D.** Different versions of a single object can have different retention modes and periods  
**E.** The bucket default settings will override any explicit retention mode or period you request on an object version

**And A and D.**

**Q 58.** A logistics company is building a multi-tier application to track the location of its trucks during peak operating hours. The company wants these data points to be accessible in real-time in its analytics platform via a REST API. The company has hired you as an AWS Certified Solutions Architect Associate to build a multi-tier solution to store and retrieve this location data for analysis.

Which of the following options addresses the given use case?

**A.** Leverage Amazon Athena with S3

**B.** Leverage QuickSight with Redshift

**C.** Leverage Amazon API Gateway with Kinesis Data Analytics

**D.** Leverage Amazon API Gateway with AWS Lambda

**Ans C**

**Q 59**. CloudFront offers a multi-tier cache in the form of regional edge caches that improve latency. However, there are certain content types that bypass the regional edge cache, and go directly to the origin.

Which of the following content types skip the regional edge cache? (Select two)

**A.** Static content such as style sheets, JavaScript files  
**B.** E-commerce assets such as product photos  
**C.** Proxy methods PUT/POST/PATCH/OPTIONS/DELETE go directly to the origin  
**D.** User-generated videos  
**E.** Dynamic content, as determined at request time (cache-behavior configured to forward all headers)

**And C and E.**

**Q 60.** A software engineering intern at an e-commerce company is documenting the process flow to provision EC2 instances via the Amazon EC2 API. These instances are to be used for an internal application that processes HR payroll data. He wants to highlight those volume types that cannot be used as a boot volume.

Can you help the intern by identifying those storage volume types that CANNOT be used as boot volumes while creating the instances? (Select two)

**A.** Throughput Optimized HDD (st1)  
**B.** Cold HDD (sc1)  
**C.** General Purpose SSD (gp2)  
**D.** Provisioned IOPS SSD (io1)  
**E.** Instance Store

**Ans A and B.**

**Q 61.** The development team at an e-commerce startup has set up multiple microservices running on EC2 instances under an Application Load Balancer. The team wants to route traffic to multiple back-end services based on the URL path of the HTTP header. So it wants requests for https://www.example.com/orders to go to a specific microservice and requests for https://www.example.com/products to go to another microservice.

Which of the following features of Application Load Balancers can be used for this use-case?

**A.** Path-based Routing  
**B.** HTTP header-based routing  
**C.** Query string parameter-based routing  
**D.** Host-based routing

**Ans A.**

**Explanation:**  
**Path-based Routing**  
Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions.  
If your application is composed of several individual services, an Application Load Balancer can route a request to a service based on the content of the request. Here are the different types –  
**Host-based Routing:**  
You can route a client request based on the Host field of the HTTP header allowing you to route to multiple domains from the same load balancer.  
**Path-based Routing:**  
You can route a client request based on the URL path of the HTTP header.  
**HTTP header-based routing:**  
You can route a client request based on the value of any standard or custom HTTP header.  
**HTTP method-based routing:**  
You can route a client request based on any standard or custom HTTP method.  
**Query string parameter-based routing:**  
You can route a client request based on the query string or query parameters.  
**Source IP address CIDR-based routing:**  
You can route a client request based on source IP address CIDR from where the request originates.  
**Path-based Routing Overview:**  
You can use path conditions to define rules that route requests based on the URL in the request (also known as path-based routing).  
The path pattern is applied only to the path of the URL, not to its query parameters.

**Q 61.** A telecom company operates thousands of hardware devices like switches, routers, cables, etc. The real-time status data for these devices must be fed into a communications application for notifications. Simultaneously, another analytics application needs to read the same real-time status data and analyze all the connecting lines that may go down because of any device failures.

As a Solutions Architect, which of the following solutions would you suggest, so that both the applications can consume the real-time status data concurrently?

**A.** Amazon Kinesis Data Streams  
**B.** Amazon Simple Notification Service (SNS)  
**C.** Amazon Simple Queue Service (SQS) with Amazon Simple Notification Service (SNS)  
**D.** Amazon Simple Queue Service (SQS) with Amazon Simple Email Service (Amazon SES)

**Ans A.**

**Explanation:**

**Amazon Kinesis Data Streams –** Amazon Kinesis Data Streams enables real-time processing of streaming big data. It provides ordering of records, as well as the ability to read and/or replay records in the same order to multiple Amazon Kinesis Applications. The Amazon Kinesis Client Library (KCL) delivers all records for a given partition key to the same record processor, making it easier to build multiple applications reading from the same Amazon Kinesis data stream (for example, to perform counting, aggregation, and filtering).

AWS recommends Amazon Kinesis Data Streams for use cases with requirements that are similar to the following:

Routing related records to the same record processor (as in streaming MapReduce). For example, counting and aggregation are simpler when all records for a given key are routed to the same record processor.

Ordering of records. For example, you want to transfer log data from the application host to the processing/archival host while maintaining the order of log statements.

Ability for multiple applications to consume the same stream concurrently. For example, you have one application that updates a real-time dashboard and another that archives data to Amazon Redshift. You want both applications to consume data from the same stream concurrently and independently.

Ability to consume records in the same order a few hours later. For example, you have a billing application and an audit application that runs a few hours behind the billing application. Because Amazon Kinesis Data Streams stores data for up to 7 days, you can run the audit application up to 7 days behind the billing application.

**Incorrect options:**

**Amazon Simple Notification Service (SNS) –** Amazon Simple Notification Service (SNS) is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications. Amazon SNS provides topics for high-throughput, push-based, many-to-many messaging. SNS is a notification service and cannot be used for real-time processing of data.

Amazon Simple Queue Service (SQS) with Amazon Simple Notification Service (SNS) – Amazon Simple Queue Service (Amazon SQS) offers a reliable, highly scalable hosted queue for storing messages as they travel between computers. Amazon SQS lets you easily move data between distributed application components and helps you build applications in which messages are processed independently (with message-level ack/fail semantics), such as automated workflows. Since multiple applications need to consume the same data stream concurrently, Kinesis is a better choice when compared to the combination of SQS with SNS.

Amazon Simple Queue Service (SQS) with Amazon Simple Email Service (Amazon SES) – As discussed above, Kinesis is a better option for this use case in comparison to SQS. Also, SES does not fit this use-cas**e**. Hence, this option is an incorrect answer.

**Q 62.** A technology blogger wants to write a review on the comparative pricing for various storage types available on AWS Cloud. The blogger has created a test file of size 1GB with some random data. Next he copies this test file into AWS S3 Standard storage class, provisions an EBS volume (General Purpose SSD (gp2)) with 100GB of provisioned storage and copies the test file into the EBS volume, and lastly copies the test file into an EFS Standard Storage filesystem. At the end of the month, he analyses the bill for costs incurred on the respective storage types for the test file.

What is the correct order of the storage charges incurred for the test file on these three storage types?

A. Cost of test file storage on S3 Standard < Cost of test file storage on EBS < Cost of test file storage on EFS  
B. Cost of test file storage on S3 Standard < Cost of test file storage on EFS < Cost of test file storage on EBS  
C. Cost of test file storage on EFS < Cost of test file storage on S3 Standard < Cost of test file storage on EBS  
D. Cost of test file storage on EBS < Cost of test file storage on S3 Standard < Cost of test file storage on EFS

**Ans B.**

**Explanation:**   
**For Amazon EFS**, you pay only for the resources that you use. The EFS Standard Storage pricing is $0.30 per GB per month. Therefore the cost for storing the test file on EFS is $0.30 for the month.  
**For EBS** General Purpose SSD (gp2) volumes, the charges are $0.10 per GB-month of provisioned storage. Therefore, for a provisioned storage of 100GB for this use-case, the monthly cost on EBS is $0.10\*100 = $10. This cost is irrespective of how much storage is actually consumed by the test file.  
**For S3 Standard storage**, the pricing is $0.023 per GB per month. Therefore, the monthly storage cost on S3 for the test file is $0.023.  
Therefore this is the correct option.

**Q 63.** The engineering team at a data analytics company has observed that its flagship application functions at its peak performance when the underlying EC2 instances have a CPU utilization of about 50%. The application is built on a fleet of EC2 instances managed under an Auto Scaling group. The workflow requests are handled by an internal Application Load Balancer that routes the requests to the instances.

As a solutions architect, what would you recommend so that the application runs near its peak performance state?

**A.** Configure the Auto Scaling group to use step scaling policy and set the CPU utilization as the target metric with a target value of 50%  
**B.** Configure the Auto Scaling group to use simple scaling policy and set the CPU utilization as the target metric with a target value of 50%  
**C.** Configure the Auto Scaling group to use target tracking policy and set the CPU utilization as the target metric with a target value of 50%  
**D.** Configure the Auto Scaling group to use a Cloudwatch alarm triggered on a CPU utilization threshold of 50%

**Ans C.**

**Explanation:** Configure the Auto Scaling group to use target tracking policy and set the CPU utilization as the target metric with a target value of 50%  
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.  
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.  
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 50 percent. This meets the requirements specified in the given use-case and therefore, this is the correct option.

**Q 64.** A geological research agency maintains the seismological data for the last 100 years. The data has a velocity of 1GB per minute. You would like to store the data with only the most relevant attributes to build a predictive model for earthquakes.

What AWS services would you use to build the most cost-effective solution with the LEAST amount of infrastructure maintenance?

**A.** Ingest the data in a Spark Streaming Cluster on EMR use Spark Streaming transformations before writing to S3  
**B.** Ingest the data in AWS Glue job and use Spark transformations before writing to S3  
**C.** Ingest the data in Kinesis Data Firehose and use a Lambda function to filter and transform the incoming stream before the output is dumped on S3  
**D.** Ingest the data in Kinesis Data Analytics and use SQL queries to filter and transform the data before writing to S3

**Ans C.**

**Q 65.** A healthcare company uses its on-premises infrastructure to run legacy applications that require specialized customizations to the underlying Oracle database as well as its host operating system (OS). The company also wants to improve the availability of the Oracle database layer. The company has hired you as an AWS Certified Solutions Architect Associate to build a solution on AWS that meets these requirements while minimizing the underlying infrastructure maintenance effort.

Which of the following options represents the best solution for this use case?

**A.** Leverage multi-AZ configuration of RDS for Oracle that allows the database administrators to access and customize the database environment and the underlying operating system  
**B.** Leverage cross AZ read-replica configuration of RDS for Oracle that allows the database administrators to access and customize the database environment and the underlying operating system  
**C.** RDS for Oracle does not allow you to access and customize your database server host and operating system. Therefore, both these options are incorrect.

**D.** Leverage multi-AZ configuration of RDS Custom for Oracle that allows the database administrators to access and customize the database environment and the underlying operating system

**Ans D.**