1. 1. Question

A popular e-commerce application runs on AWS and uses an Amazon Aurora Multi-AZ deployment for its database. When monitoring the performance ,you noticed that the database reads are causing high I/O and adding latency to the write requests against the database.  
What is the best solution to separate the read requests from the write requests?

* + Use Amazon DynamoDB Accelerator (DAX) to provide a caching layer.
  + **Create a read replica and modify the application to use the appropriate endpoint.**
  + Replica DB instances endpoint for Aurora.
  + Create a second Amazon Aurora database and link it to the primary database as a read replica.

**Unattempted**

Exam Tip  
Create read replica and use Reader endpoint for Amazon Aurora.  
Explanation  
Aurora Replicas are independent endpoints in an Aurora DB cluster, best used for scaling read operations and increasing availability. Up to 15 Aurora Replicas can be distributed across the Availability Zones that a DB cluster spans within an AWS Region. The DB cluster volume is made up of multiple copies of the data for the DB cluster. However, the data in the cluster volume is represented as a single, logical volume to the primary instance and to Aurora Replicas in the DB cluster.  
As a result, all Aurora Replicas return the same data for query results with minimal replica lag—usually much less than 100 milliseconds after the primary instance has written an update. Replica lag varies depending on the rate of database change. That is, during periods where a large amount of write operations occur for the database, you might see an increase in replica lag.  
Aurora Replicas work well for read scaling because they are fully dedicated to read operations on your cluster volume. Write operations are managed by the primary instance. Because the cluster volume is shared among all DB instances in your DB cluster, minimal additional work is required to replicate a copy of the data for each Aurora Replica.  
To increase availability, you can use Aurora Replicas as failover targets. That is, if the primary instance fails, an Aurora Replica is promoted to the primary instance. There is a brief interruption during which read and write requests made to the primary instance fail with an exception, and the Aurora Replicas are rebooted. If your Aurora DB cluster doesn’t include any Aurora Replicas, then your DB cluster will be unavailable for the duration it takes your DB instance to recover from the failure event. However, promoting an Aurora Replica is much faster than recreating the primary instance. For high-availability scenarios, we recommend that you create one or more Aurora Replicas. These should be of the same DB instance class as the primary instance and in different Availability Zones for your Aurora DB cluster. For more information on Aurora Replicas as failover targets,  
Reference  
<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html>

1. 2. Question

A three-tier image-sharing application deployed on Amazon EC2 instance for the front-end layer, another for the backend tier, and a third for the MySQL database.  
What is the best solution to design a highly available with minimum impact on the application?

* + **Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers. Move the database to an Amazon RDS instance with a Multi-AZ deployment. Use Amazon S3 to store and serve users' images.**
  + Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers. Move the database to an Amazon RDS instance with multiple read replicas to store and serve users' images.
  + Use Amazon S3 to host the front-end layer and AWS Lambda functions for the backend layer. Move the database to an Amazon DynamoDB table and use Amazon S3 to store and serve users' images.
  + Use Amazon S3 to host the front-end layer and a fleet of Amazon EC2 instances in an Auto Scaling group for the backend layer. Move the database to a memory optimized instance type to store and serve users' images.

**Unattempted**

Exam Tip  
the best answer to address high availability in all three tiers is “Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end and backend layers. Move the database to an Amazon RDS instance with a Multi-AZ deployment. Use Amazon S3 to store and serve users’ images.”  
Explanation  
When you enable load balancing, AWS Elastic Beanstalk creates an Elastic Load Balancing load balancer for your environment. The load balancer distributes traffic among your environment’s instances.  
Elastic Beanstalk supports these load balancer types:  
Classic Load Balancer – The Elastic Load Balancing previous-generation load balancer. Routes HTTP, HTTPS, or TCP request traffic to different ports on environment instances.  
Application Load Balancer – An application layer load balancer. Routes HTTP or HTTPS request traffic to different ports on environment instances based on the request path.  
Network Load Balancer – A network layer load balancer. Routes TCP request traffic to different ports on environment instances. Supports both active and passive health checks.  
By default, Elastic Beanstalk creates an Application Load Balancer for your environment when you enable load balancing with the Elastic Beanstalk console or the EB CLI. It configures the load balancer to listen for HTTP traffic on port 80 and forward this traffic to instances on the same port. You can choose the type of load balancer that your environment uses only during environment creation. Later, you can change settings to manage the behavior of your running environment’s load balancer, but you can’t change its type.  
Reference  
<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.managing.elb.html>

1. 3. Question

A scientific research agency has an application which runs on AWS Fargate, and the connected storage needs to have concurrent access to files and deliver high performance. As solutions Architect you needs to design a managed storage solution for this application that includes high-performance machine learning.  
Which storage option should the solutions architect recommend?

* + Create an Amazon Elastic File System (Amazon EFS) file share and establish an IAM role that allows Fargate to communicate with Amazon EFS.
  + Create an Amazon S3 bucket for the application and establish an IAM role for Fargate to communicate with Amazon S3.
  + **Create an Amazon FSx for Lustre file share and establish an IAM role that allows Fargate to communicate with FSx for Lustre.**
  + Create an Amazon Elastic Block Store (Amazon EBS) volume for the application and establish an IAM role that allows Fargate to communicate with Amazon EBS.

**Unattempted**

Exam Tip  
FSx for Lustre use case is HPC and/or ML. It also supports concurrent access.  
Explanation  
Amazon FSx for Lustre makes it easy and cost effective to launch and run the world’s most popular high-performance file system. Use it for workloads where speed matters, such as machine learning, high performance computing (HPC), video processing, and financial modeling.  
The open source Lustre file system is designed for applications that require fast storage – where you want your storage to keep up with your compute. Lustre was built to quickly and cost effectively process the fastest-growing data sets in the world, and it’s the most widely used file system for the 500 fastest computers in the world. It provides sub-millisecond latencies, up to hundreds of gigabytes per second of throughput, and millions of IOPS.  
Now as a fully managed service, Amazon FSx enables you to use Lustre file systems for any workload where storage speed matters. It eliminates the traditional complexity of setting up and managing Lustre file systems, allowing you to spin up a high-performance file system in minutes. It also provides multiple deployment options to optimize cost.  
FSx for Lustre integrates with Amazon S3, making it easy to process data sets with the Lustre file system. When linked to an S3 bucket, an FSx for Lustre file system transparently presents S3 objects as files and allows you to write changed data back to S3.  
Reference  
<https://aws.amazon.com/fsx/lustre/?nc2=type_a>

1. 4. Question

A Solutions Architect is building a multi-tier web application that runs six front-end web servers in an Amazon EC2 Auto Scaling group in a single Availability Zone behind an Application Load Balancer (ALB).  
Which architecture should the solutions architect choose that provides high availability without modifying the application.?

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

**Unattempted**

Exam Tip  
to achieve high availability , deploy 3 instances in each of the two AZ.

Reference  
<https://aws.amazon.com/marketplace/solutions/infrastructure-software/high-availability>

1. 5. Question

Solution architect is working in designing multimedia application which will stream huge sequential and consistent amount of data from EC2 instance up to 400 MiB/s.  
What is the best cost optimized storage to handle this requirement with high performance?

* + **EBS Throughput Optimized HDD**
  + S3
  + EFS
  + EBS Provisioned IOPS SSD

**Unattempted**

Exam Tip  
huge amount of data + sequential processing + consistent = EBS Throughput Optimized HDD  
Explanation  
Throughput Optimized HDD (st1) volumes provide low-cost magnetic storage that defines performance in terms of throughput rather than IOPS. This volume type is a good fit for large, sequential workloads such as Amazon EMR, ETL, data warehouses, and log processing. Bootable st1 volumes are not supported.  
Reference  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html>

1. 6. Question

As Solution architect in transportation company is designing a new service to receive the location for 5000 cars each hour then stores the data in DynamoDB.  
Which service will process the updates and automatically scale during peak traffic times?

* + Amazon Kinesis Firehouse
  + Amazon ECS.
  + **Amazon API Gateway**
  + Amazon EC2

**Unattempted**

Exam Tip  
Since The data does not come from stream = Use API Gateway.  
since no streaming , no needs for Amazon Kinesis Firehouse  
Explanation  
Amazon API Gateway is an AWS service for creating, publishing, maintaining, monitoring, and securing REST, HTTP, and WebSocket APIs at any scale. API developers can create APIs that access AWS or other web services, as well as data stored in the AWS Cloud. As an API Gateway API developer, you can create APIs for use in your own client applications. Or you can make your APIs available to third-party app developers.  
Reference  
<https://docs.aws.amazon.com/apigateway/latest/developerguide/welcome.html>

1. 7. Question

You are designing a multi-tier online learning site which will write a huge amount of data in form of key value pairs, the course’s exercises data will be accessed frequently and the data objects are required to be stored in inconsistent schemas.  
Which AWS Storage can handles this requirement?

* + Amazon Aurora
  + Amazon Redshift
  + **Amazon DynamoDB**
  + Amazon RDS PostGreSQL

**Unattempted**

Exam Tip  
key-value store + changeable schema = Amazon DynamoDB  
Explanation  
Amazon DynamoDB is a key-value and document database that delivers single-digit millisecond performance at any scale. It’s a fully managed, multiregion, multimaster, durable database with built-in security, backup and restore, and in-memory caching for internet-scale applications. DynamoDB can handle more than 10 trillion requests per day and can support peaks of more than 20 million requests per second.  
Reference  
<https://aws.amazon.com/blogs/aws/amazon-dynamodb-internet-scale-data-storage-the-nosql-way/>

1. 8. Question

A scientific research company has restful API deployed on single EC2 instance and due to scalability and performance issues, the company decided to add two additional EC2 instances with auto scaling group but it does not want to enforce the clients to change the IPs each time it add/remove instances.  
Which AWS service can be used to handle this requirement with high scalability?

* + ASG
  + S3
  + SQS
  + **ELB**

**Unattempted**

Exam Tip  
we must use ELB and share its IP with the clients instead of the instance IP  
Explanation  
Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions. It can handle the varying load of your application traffic in a single Availability Zone or across multiple Availability Zones. Elastic Load Balancing offers three types of load balancers that all feature the high availability, automatic scaling, and robust security necessary to make your applications fault tolerant.  
Application Load Balancer  
Reference  
<https://aws.amazon.com/elasticloadbalancing/>

1. 9. Question

A solution architect working in a news agency ,he is designing a news website inside a VPC with public subnet for web servers and the RDS database servers will be deployed inside the private subnet , the database servers need to access the internet for OS updates.  
Which option satisfies these requirements?

* + Use VPN CloudHub
  + Create a VPC Endpoint for Amazon RDS.
  + **Use a NAT Gateway.**
  + Use AWS Direct Connect

**Unattempted**

Exam Tip  
provide internet to private subnet = use NAT gateway  
Explanation  
You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances.  
Reference  
<https://aws.amazon.com/premiumsupport/knowledge-center/nat-gateway-vpc-private-subnet/>

1. 10. Question

Which AWS feature can be used to capture information about the IP traffic going to and from network interfaces in your VPC?

* + ELB access Logs
  + **VPC Flow Logs**
  + Enable AWS CloudTrail logging
  + Enable AWS CloudWatch logging

**Unattempted**

Exam Tip  
VPC flow logs records the IP traffics in subnet level  
Explanation  
VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs or Amazon S3. After you’ve created a flow log, you can retrieve and view its data in the chosen destination.  
Flow logs can help you with a number of tasks, such as:  
a) Diagnosing overly restrictive security group rules  
b) Monitoring the traffic that is reaching your instance  
c) Determining the direction of the traffic to and from the network interfaces

Reference  
<https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html>

1. 11. Question

A popular mobile game has multiple Amazon EC2 instances in a single Availability Zone for its multiplayer game that communicates with users on Layer 4.  
Which actions should the solutions architect  must take into consideration to make the architecture highly available and cost-effective? (Choose two.)

* + Decrease the number of EC2 instances.
  + Configure an Application Load Balancer in front of the EC2 instances.
  + **Configure a Network Load Balancer in front of the EC2 instances.**
  + **Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically.**
  + increase the number of EC2 instances.

**Unattempted**

Exam Tip  
Layer 4 traffic is handled using Network load balancer.  
to make the architecture highly available = Configure an Auto Scaling group  
Explanation  
A Network Load Balancer functions at the fourth layer of the Open Systems Interconnection (OSI) model. It can handle millions of requests per second. After the load balancer receives a connection request, it selects a target from the target group for the default rule. It attempts to open a TCP connection to the selected target on the port specified in the listener configuration.  
When you enable an Availability Zone for the load balancer, Elastic Load Balancing creates a load balancer node in the Availability Zone. By default, each load balancer node distributes traffic across the registered targets in its Availability Zone only. If you enable cross-zone load balancing, each load balancer node distributes traffic across the registered targets in all enabled Availability Zones.

An Auto Scaling group contains a collection of Amazon EC2 instances that are treated as a logical grouping for the purposes of automatic scaling and management. An Auto Scaling group also enables you to use Amazon EC2 Auto Scaling features such as health check replacements and scaling policies. Both maintaining the number of instances in an Auto Scaling group and automatic scaling are the core functionality of the Amazon EC2 Auto Scaling service.  
The size of an Auto Scaling group depends on the number of instances that you set as the desired capacity. You can adjust its size to meet demand, either manually or by using automatic scaling.  
An Auto Scaling group starts by launching enough instances to meet its desired capacity. It maintains this number of instances by performing periodic health checks on the instances in the group. The Auto Scaling group continues to maintain a fixed number of instances even if an instance becomes unhealthy. If an instance becomes unhealthy, the group terminates the unhealthy instance and launches another instance to replace it.  
Reference  
<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html>  
<https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html>

1. 12. Question

The operation team at a training provider company has an issue that the data manipulation language(DML) queries which come from a web application to the database became slower, and the database become not able to handle all requests specially in the peak times.  
What is the best AWS service can be used to solve this issue?

* + **Amazon SQS**
  + Amazon EFS
  + Amazon S3
  + AWS Lambda

**Unattempted**

Exam Tip  
SQS =  decouple the web application from the database

Explanation  
Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message oriented middleware, and empowers developers to focus on differentiating work. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available. Get started with SQS in minutes using the AWS console, Command Line Interface or SDK of your choice, and three simple commands.

Reference  
<https://aws.amazon.com/sqs/>

1. 13. Question

A stock exchange company has an application that captures user data and stores it for future analysis. The application’s static front end is deployed on an Amazon EC2 instance. The front-end application sends the requests to the backend application running on separate EC2 instance and use Amazon RDS to store the data.  
What should a solutions architect do to decouple the architecture and make it scalable?

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

**Unattempted**

Exam Tip  
Static =Use Amazon S3 , Decouple= Use SQS Queue, Scalable=Use Auto Scaling Group  
Explanation  
Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message oriented middleware, and empowers developers to focus on differentiating work. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available. Get started with SQS in minutes using the AWS console, Command Line Interface or SDK of your choice, and three simple commands.  
SQS offers two types of message queues. Standard queues offer maximum throughput, best-effort ordering, and at-least-once delivery. SQS FIFO queues are designed to guarantee that messages are processed exactly once, in the exact order that they are sent.  
Reference  
<https://aws.amazon.com/sqs/>

1. 14. Question

A Solutions Architect working for a startup is designing a High Performance Computing (HPC) application workload on Amazon EC2. The EC2 instances need to communicate to each other frequently and require network performance with low latency and high throughput.  
Which EC2 configuration meets these requirements?

* + Launch the EC2 instances in an Auto Scaling group in two Regions and peer the VPCs.
  + Use a Spread placement group while launching the EC2 instances in one Availability Zone.
  + Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones.
  + **Use a cluster placement group while launching the EC2 instances in one Availability Zone.**

**Unattempted**

Exam Tip  
low latency and high throughput= Use Cluster placement groups  
Explanation  
Cluster placement groups  
A cluster placement group is a logical grouping of instances within a single Availability Zone. A cluster placement group can span peered VPCs in the same Region. Instances in the same cluster placement group enjoy a higher per-flow throughput limit of up to 10 Gbps for TCP/IP traffic and are placed in the same high-bisection bandwidth segment of the network.  
The following image shows instances that are placed into a cluster placement group.

[A screen shot of a computer

Description automatically generated](https://skillcertpro.com/wp-content/uploads/2020/08/a61.png)  
Cluster placement groups are recommended for applications that benefit from low network latency, high network throughput, or both. They are also recommended when the majority of the network traffic is between the instances in the group. To provide the lowest latency and the highest packet-per-second network performance for your placement group, choose an instance type that supports enhanced networking. For more information, see Enhanced Networking.  
We recommend that you launch your instances in the following way:  
Use a single launch request to launch the number of instances that you need in the placement group.  
Use the same instance type for all instances in the placement group.  
If you try to add more instances to the placement group later, or if you try to launch more than one instance type in the placement group, you increase your chances of getting an insufficient capacity error.  
If you stop an instance in a placement group and then start it again, it still runs in the placement group. However, the start fails if there isn’t enough capacity for the instance.  
If you receive a capacity error when launching an instance in a placement group that already has running instances, stop and start all of the instances in the placement group, and try the launch again. Starting the instances may migrate them to hardware that has capacity for all of the requested instances.  
Partition placement groups  
Partition placement groups help reduce the likelihood of correlated hardware failures for your application. When using partition placement groups, Amazon EC2 divides each group into logical segments called partitions. Amazon EC2 ensures that each partition within a placement group has its own set of racks. Each rack has its own network and power source. No two partitions within a placement group share the same racks, allowing you to isolate the impact of hardware failure within your application.  
The following image is a simple visual representation of a partition placement group in a single Availability Zone. It shows instances that are placed into a partition placement group with three partitions—Partition 1, Partition 2, and Partition 3. Each partition comprises multiple instances. The instances in a partition do not share racks with the instances in the other partitions, allowing you to contain the impact of a single hardware failure to only the associated partition.

[A diagram of several options

Description automatically generated with medium confidence](https://skillcertpro.com/wp-content/uploads/2020/08/a62.png)  
Partition placement groups can be used to deploy large distributed and replicated workloads, such as HDFS, HBase, and Cassandra, across distinct racks. When you launch instances into a partition placement group, Amazon EC2 tries to distribute the instances evenly across the number of partitions that you specify. You can also launch instances into a specific partition to have more control over where the instances are placed.  
A partition placement group can have partitions in multiple Availability Zones in the same Region. A partition placement group can have a maximum of seven partitions per Availability Zone. The number of instances that can be launched into a partition placement group is limited only by the limits of your account.  
In addition, partition placement groups offer visibility into the partitions — you can see which instances are in which partitions. You can share this information with topology-aware applications, such as HDFS, HBase, and Cassandra. These applications use this information to make intelligent data replication decisions for increasing data availability and durability.  
If you start or launch an instance in a partition placement group and there is insufficient unique hardware to fulfill the request, the request fails. Amazon EC2 makes more distinct hardware available over time, so you can try your request again later.  
Spread placement groups  
A spread placement group is a group of instances that are each placed on distinct racks, with each rack having its own network and power source.  
The following image shows seven instances in a single Availability Zone that are placed into a spread placement group. The seven instances are placed on seven different racks.

[A white rectangular object with black squares

Description automatically generated](https://skillcertpro.com/wp-content/uploads/2020/08/a63.png)  
Spread placement groups are recommended for applications that have a small number of critical instances that should be kept separate from each other. Launching instances in a spread placement group reduces the risk of simultaneous failures that might occur when instances share the same racks. Spread placement groups provide access to distinct racks, and are therefore suitable for mixing instance types or launching instances over time.  
A spread placement group can span multiple Availability Zones in the same Region. You can have a maximum of seven running instances per Availability Zone per group.  
If you start or launch an instance in a spread placement group and there is insufficient unique hardware to fulfill the request, the request fails. Amazon EC2 makes more distinct hardware available over time, so you can try your request again later.  
Reference  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

1. 15. Question

You are working as a Solutions Architect for an investment bank and your Chief Technical Officer intends to migrate all of your applications to AWS within a month. Each application has 50 TB of data to be transferred. After the migration is complete, this bank will require secure network connectivity with consistent throughput from their data centers to the applications.  
What is the best solution to meet these requirements?

* + AWS Site-to-Site VPN for both the initial transfer and ongoing connectivity.
  + AWS Direct Connect for both the initial transfer and ongoing connectivity.
  + **AWS Snowball for the initial transfer and AWS Direct Connect for ongoing connectivity.**
  + AWS Snowball for the initial transfer and AWS Site-to-Site VPN for ongoing connectivity.

**Unattempted**

Exam Tip  
To transfer 50 TB of data for each application within a month= Use Snow ball  
secure network connectivity with consistent throughput from their data centers to the applications = Use Direct Connect  
Explanation  
AWS Snowball is a data transport solution that accelerates moving terabytes to petabytes of data into and out of AWS using storage appliances designed to be secure for physical transport. Using Snowball helps to eliminate challenges that can be encountered with large-scale data transfers including high network costs, long transfer times, and security concerns.

AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

Reference  
<https://aws.amazon.com/directconnect/#:~:text=Using%20AWS%20Direct%20Connect%2C%20you,experience%20than%20Internet%2Dbased%20connections>.

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

1. 16. Question

As AWS Solutions architect, you have a requirement from the security team to provide them with a service which continuously monitor, and retain account activity related to actions across AWS multi Regions.  
What is the best approach to handle this task?

* + Enable CloudWatch logging across all regions
  + **Enable CloudTrail logging across all regions**
  + Enable CloudTrail logging in each region
  + Enable CloudWatch logging in each region

**Unattempted**

Exam Tip  
you can use AWS CloudTrail to monitor, and retain account activity related to actions across AWS multi Regions  
Explanation  
AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. In addition, you can use CloudTrail to detect unusual activity in your AWS accounts. These capabilities help simplify operational analysis and troubleshooting.  
Reference  
<https://aws.amazon.com/cloudtrail/>

1. 17. Question

An online stocks trading application use a fleet of EC2 instances with auto scaling group , every day at the beginning of trading session, the application becomes very slow for 10 minutes then works as normal.  
What is the BEST approach to fix this problem ?

* + Add a Scheduled Scaling action based on number of concurrent requests.
  + Add more spot instances before the start of the trading session with 30 minutes.
  + Use EC2 scheduled reserved instances.
  + **Add a Scheduled Scaling action before the start of the trading session with 30 minutes.**

**Unattempted**

Exam Tip  
you have to use Scheduled Scaling to scale the resources with enough time before the trading session.  
Explanation  
Scaling based on a schedule allows you to set your own scaling schedule for predictable load changes. For example, every week the traffic to your web application starts to increase on Wednesday, remains high on Thursday, and starts to decrease on Friday. You can configure Application Auto Scaling to increase capacity on Wednesday and decrease capacity on Friday.  
To use scheduled scaling, create scheduled actions, which tell Application Auto Scaling to perform scaling activities at specific times. When you create a scheduled action, you specify the scalable target, when the scaling activity should occur, and the minimum and maximum capacity. At the specified time, Application Auto Scaling scales based on the new capacity values.  
Reference  
<https://docs.aws.amazon.com/autoscaling/application/userguide/application-auto-scaling-scheduled-scaling.html>

1. 18. Question

You are AWS Chief architect in cloud consultancy company, one of the clients has a difficulty in managing the VPC NAT instances availability which exist in multi availability zone.  
What is the best approach to provide cost-optimized solution to enhance this architecture?

* + Create script to provide high availability to the current NAT instances
  + Use NAT gateway in addition to the current NAT instances in each availability zone.
  + Use ELB Network Load balancer in front of NAT instances.
  + **Remove the NAT instances and use one NAT gateway in each availability zone.**

**Unattempted**

Exam Tip  
You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances.  
You can create a script to handle the availability of NAT instances but it will increase the complexity  
Explanation  
The following diagram illustrates the architecture of a VPC with a NAT gateway. The main route table sends internet traffic from the instances in the private subnet to the NAT gateway. The NAT gateway sends the traffic to the internet gateway using the NAT gateway’s Elastic IP address as the source IP address.

[A diagram of a network

Description automatically generated](https://skillcertpro.com/wp-content/uploads/2020/08/a55.png)  
Reference  
<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>

1. 19. Question

An e-trading company provides highly available clothes tailoring service by providing users the ability to submit requests to customize clothes by sending tailoring parameters in addition to the original clothes image ID in a request to an AWS API Gateway API. The customized image will be generated on demand, and users will receive a link they can click to view or download their customized image.  
What is the MOST cost-effective solution to meet these requirements?

* + **Use AWS Lambda to adapt the original image to the requested customization. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.**
  + Use AWS Lambda to adapt the original image to the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Elastic Load Balancer in front of the Amazon EC2 instances.
  + Use ECS to adapt the original image into the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Amazon CloudFront distribution with the S3 bucket as the origin.
  + Configure an ELB in front of the EC2 instances , Amazon EC2 instances will be used to adapt the original image into the requested customization Store the original and manipulated images in Amazon S3.

**Unattempted**

Exam Tip  
1. Use Amazon Lambda for pay-per-use compute instead of EC2.  
2. Use CloudFront infront of S3 to cache images at the nodes. Hence reducing data transfer cost.  
Explanation  
Lambda@Edge lets you run Node.js and Python Lambda functions to customize content that CloudFront delivers, executing the functions in AWS locations closer to the viewer. The functions run in response to CloudFront events, without provisioning or managing servers. You can use Lambda functions to change CloudFront requests and responses at the following points:  
After CloudFront receives a request from a viewer (viewer request)  
Before CloudFront forwards the request to the origin (origin request)  
After CloudFront receives the response from the origin (origin response)  
Before CloudFront forwards the response to the viewer (viewer response)

[A diagram of a cloudfront system

Description automatically generated](https://skillcertpro.com/wp-content/uploads/2020/08/a64.png)  
Reference  
<https://docs.aws.amazon.com/lambda/latest/dg/lambda-edge.html>

1. 20. Question

As Solution architect, you are designing a mobile application which will allow users to upload files directly to Amazon S3 without accessing the web servers.  
What the simplest approach to handle this requirement?

* + Create multiple Docker containers managed by Amazon Elastic Container Service to write the files into Amazon S3 bucket.
  + **Upload the files directly to S3 using a pre-signed URL.**
  + Create Multiple EC2 instances behind Application Load Balancer to write the files into Amazon S3 bucket
  + Use lambda to receive the files from Amazon SQS which then store the files into Amazon S3 bucket

**Unattempted**

Exam Tip  
if you need to bypass web servers and store the files directly into S3 bucket , then use pre-signed URL.  
Explanation  
A presigned URL gives you access to the object identified in the URL, provided that the creator of the presigned URL has permissions to access that object. That is, if you receive a presigned URL to upload an object, you can upload the object only if the creator of the presigned URL has the necessary permissions to upload that object.  
All objects and buckets by default are private. The presigned URLs are useful if you want your user/customer to be able to upload a specific object to your bucket, but you don’t require them to have AWS security credentials or permissions. When you create a presigned URL, you must provide your security credentials and then specify a bucket name, an object key, an HTTP method (PUT for uploading objects), and an expiration date and time. The presigned URLs are valid only for the specified duration.  
Reference  
<https://docs.aws.amazon.com/AmazonS3/latest/dev/PresignedUrlUploadObject.html>

1. 21. Question

A Solutions Architect is designing messaging system between order service and stock service, the expected number of transactions will not be more than 250 transaction per second. the orders must be processed in order without losing any orders.  
Which low-cost AWS service should you recommend to handle this requirement?

* + Amazon SNS
  + Amazon MQ
  + **Amazon SQS**
  + Kinesis Stream

**Unattempted**

Exam Tip  
Low cost messaging system+ number of transactions will not be more than 250 transaction per second + order must be processed in order= Amazon SQS  
Explanation  
Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message oriented middleware, and empowers developers to focus on differentiating work. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available. Get started with SQS in minutes using the AWS console0  
Reference  
<https://aws.amazon.com/sqs/>

1. 22. Question

A company has a monolithic application which performs data processing using two sequential dependable functions. The second function of the process takes longer than the first, so the company has decided to rewrite the application as two microservices running on Amazon ECS that can scale independently.  
How should a solutions architect integrate the microservices?

* + Create microservice 1 to publish data to an Amazon SNS topic. Create microservice 2 to subscribe to this topic.
  + Create microservice 1 to send data to Amazon Kinesis Data Firehose, Create microservice 2 to read from Kinesis Data Firehose.
  + **Create microservice 1 to send data to an Amazon SQS queue. Create microservice 2 to process messages from the queue.**
  + Create microservice 1 to send data to an Amazon S3 bucket. Use S3 event notifications to invoke microservice 2

**Unattempted**

Exam Tip  
SQS is used for decoupling + scaling microservices. Not the best use case for Kinesis.  
Explanation  
Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message oriented middleware, and empowers developers to focus on differentiating work. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available. Get started with SQS in minutes using the AWS console, Command Line Interface or SDK of your choice, and three simple commands.  
SQS offers two types of message queues. Standard queues offer maximum throughput, best-effort ordering, and at-least-once delivery. SQS FIFO queues are designed to guarantee that messages are processed exactly once, in the exact order that they are sent.  
Reference  
<https://aws.amazon.com/sqs/>

1. 23. Question

A public trading company hosts its main web site’s DNS records in Amazon Route 53 where the domain is pointing to an Application Load Balancer. you received a task to direct the user to backup error page if the main website was down.  
What is the SIMPLEST solution to handle this requirement with the minimum changes?

* + Use Amazon CloudFront distribution with Application Load Balancer as origin and point Route 53 alias record to this distribution.
  + Configure Route 53 record to use a latency-based routing policy, host the error page in Amazon S3 bucket and direct the request to the most responsive endpoints.
  + **Configure Route 53 active-passive failover, if the Application load balancer endpoint is unhealthy , redirect the traffic to the error page which is hosted in Amazon S3 bucket.**
  + Configure Route 53 active-active policy with Application load balancer and an Amazon EC2 instance hosting a error page as endpoints,if the Application load balancer endpoint is unhealthy , redirect the traffic to EC2 instance.

**Unattempted**

Exam Tip  
You can use Route 53 health checking to configure active-active and active-passive failover configurations. You configure active-active failover using any routing policy (or combination of routing policies) other than failover, and you configure active-passive failover using the failover routing policy.  
Explanation  
Active-active failover  
Use this failover configuration when you want all of your resources to be available the majority of the time. When a resource becomes unavailable, Route 53 can detect that it’s unhealthy and stop including it when responding to queries.  
In active-active failover, all the records that have the same name, the same type (such as A or AAAA), and the same routing policy (such as weighted or latency) are active unless Route 53 considers them unhealthy. Route 53 can respond to a DNS query using any healthy record.  
Active-passive failover  
Use an active-passive failover configuration when you want a primary resource or group of resources to be available the majority of the time and you want a secondary resource or group of resources to be on standby in case all the primary resources become unavailable. When responding to queries, Route 53 includes only the healthy primary resources. If all the primary resources are unhealthy, Route 53 begins to include only the healthy secondary resources in response to DNS queries.  
Reference  
<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html>

1. 24. Question

An e-commerce company has  a relation database running on-premises which serves high read traffic for users in different locations. The company wants to migrate to AWS with the least amount of effort. The database solution should support disaster recovery and not affect the company’s current traffic flow.  
What is the best solution to handle this requirement?

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

**Unattempted**

Exam Tip  
AWS Read Replica can support multi-region.  
Explanation  
Amazon RDS (Relational Database Service) is a managed service that makes it easier to set up, operate, and scale a relational database. Based on AWS high performance compute and storage, Amazon RDS supports the MySQL, SQL Server, PostgreSQL, MariaDB, and Oracle database engines. It offers a complete set of solutions for provisioning, patching, monitoring, and disaster recovery (DR). This blog presents three features in Amazon RDS that support DR: automated backups, manual backups, and Read Replicas.  
Reference  
<https://aws.amazon.com/blogs/database/implementing-a-disaster-recovery-strategy-with-amazon-rds/>

1. 25. Question

As Solution architect, you want to minimize the CPU utilization of EC2 instance resulted from serving a high amount of requests to access static content in S3 bucket,  
how should you enhance the current architecture to overcome this problem?

* + Use Amazon API Gateway with lambda to retrieve the static contents from S3 buckets
  + **Use Amazon CloudFront with S3 bucket as the origin.**
  + Use a combination from Amazon CloudFront and Amazon API gateway in addition to lambda
  + Add more EC2 instances and use ELB to distribute the workload.

**Unattempted**

Exam Tip  
use CloudFront to serve a static website hosted on Amazon S3  
Explanation  
Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment. CloudFront is integrated with AWS – both physical locations that are directly connected to the AWS global infrastructure, as well as other AWS services. CloudFront works seamlessly with services including AWS Shield for DDoS mitigation, Amazon S3, Elastic Load Balancing or Amazon EC2 as origins for your applications, and Lambda@Edge to run custom code closer to customers’ users and to customize the user experience. Lastly, if you use AWS origins such as Amazon S3, Amazon EC2 or Elastic Load Balancing, you don’t pay for any data transferred between these services and CloudFront.  
Reference  
<https://aws.amazon.com/cloudfront/>

1. 26. Question

A Solutions Architect is re-designing the current multi-tier application to solve scaling and performance issues, the application is running in Amazon VPC which consists of one public subnet and one private subnet , the private subnet hosts multiple EC2 instances and there is ELB classic load balancer as the front end of the public subnet, and reverse proxy to route the traffic between EC2 instances using that content-based routing.  
What the steps should you take to enhance this architecture? (Select Two)

* + Replace ELB classic load balancer and reverse proxy with ELB Network Load Balancer.
  + Replace only ELB classic load balancer with ELB Application Load Balancer.
  + Replace EC2 instances with c4.large instances
  + **Use auto scaling group with EC2 instances**
  + **Replace ELB classic load balancer and reverse proxy with ELB Application Load Balancer.**

**Unattempted**

Exam Tip  
content-based routing = use ELB Application load balancer.  
for scalability , use Auto scaling group.  
Explanation  
AWS Application Load Balancers have been around since the summer of 2016! They support content-based routing, work well for serverless & container-based applications, and are highly scalable. Many AWS customers are using the existing host and path-based routing to power their HTTP and HTTPS applications, while also taking advantage of other ALB features such as port forwarding (great for container-based applications), health checks, service discovery, redirects, fixed responses, and built-in authentication.  
An Auto Scaling group contains a collection of Amazon EC2 instances that are treated as a logical grouping for the purposes of automatic scaling and management. An Auto Scaling group also enables you to use Amazon EC2 Auto Scaling features such as health check replacements and scaling policies. Both maintaining the number of instances in an Auto Scaling group and automatic scaling are the core functionality of the Amazon EC2 Auto Scaling service.  
Reference  
<https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html>  
<https://aws.amazon.com/blogs/aws/new-advanced-request-routing-for-aws-application-load-balancers/>

1. 27. Question

A Solution Architect has a two-tier application with a single Amazon EC2 instance web server and Amazon RDS MySQL Multi-AZ DB instances. The Architect is re-architecting the application for high availability by adding instances in a second Availability Zone.  
Which additional services will improve the availability of the application? (Choose two.)

* + Amazon ElastiCache
  + **Auto Scaling group**
  + **ELB Classic Load Balancer**
  + AWS CloudTrail
  + Amazon DynamoDB

**Unattempted**

Exam Tip  
For HA = Use ELB + Auto Scaling group  
Explanation  
You can take advantage of the safety and reliability of geographic redundancy by spanning your Auto Scaling group across multiple Availability Zones within a Region and then attaching a load balancer to distribute incoming traffic across those zones. Incoming traffic is distributed equally across all Availability Zones enabled for your load balancer.

When one Availability Zone becomes unhealthy or unavailable, Amazon EC2 Auto Scaling launches new instances in an unaffected zone. When the unhealthy Availability Zone returns to a healthy state, Amazon EC2 Auto Scaling automatically redistributes the application instances evenly across all of the zones for your Auto Scaling group. Amazon EC2 Auto Scaling does this by attempting to launch new instances in the Availability Zone with the fewest instances. If the attempt fails, however, Amazon EC2 Auto Scaling attempts to launch in other Availability Zones until it succeeds.  
You can expand the availability of your scaled and load-balanced application by adding an Availability Zone to your Auto Scaling group and then enabling that zone for your load balancer. After you’ve enabled the new Availability Zone, the load balancer begins to route traffic equally among all the enabled zones.  
Reference  
<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-add-availability-zone.html>

1. 28. Question

A Solutions Architect is designing a solution for car tracking application, this application will receive data from more than 5000 cars every 2 minutes, it is expected that number of cars will be 7000 after 2 weeks from the product launching date.  
What is the most scalable solution to handle streaming data?

* + Use ELB in front of EC2 instances to receive the data then store in Amazon S3
  + Create lambda function to receive and process the data then store it in DynamoDB.
  + **Store the data in Amazon S3 bucking using Amazon Kinesis Firehouse delivery stream.**
  + Store the data in Amazon S3 bucking using Amazon SQS.

**Unattempted**

Exam Tip  
streaming data +scalable+ store in S3 = Kinesis Firehouse streams  
Explanation  
Amazon Kinesis Data Firehose is the easiest way to reliably load streaming data into data lakes, data stores and analytics tools. It can capture, transform, and load streaming data into Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk, enabling near real-time analytics with existing business intelligence tools and dashboards you’re already using today. It is a fully managed service that automatically scales to match the throughput of your data and requires no ongoing administration. It can also batch, compress, transform, and encrypt the data before loading it, minimizing the amount of storage used at the destination and increasing security.  
Reference  
<https://aws.amazon.com/kinesis/data-firehose/>

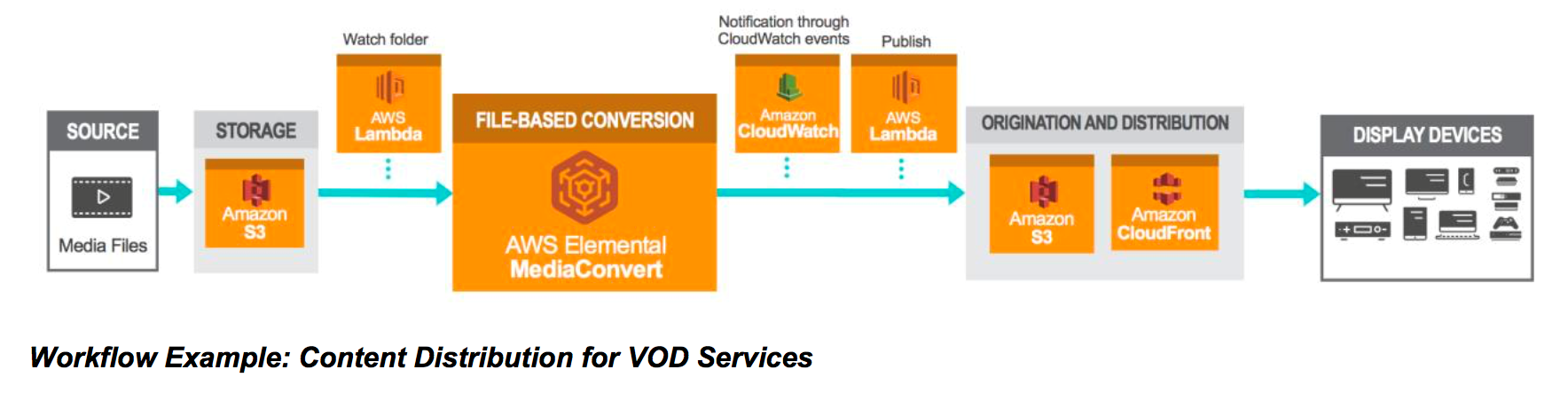
1. 29. Question

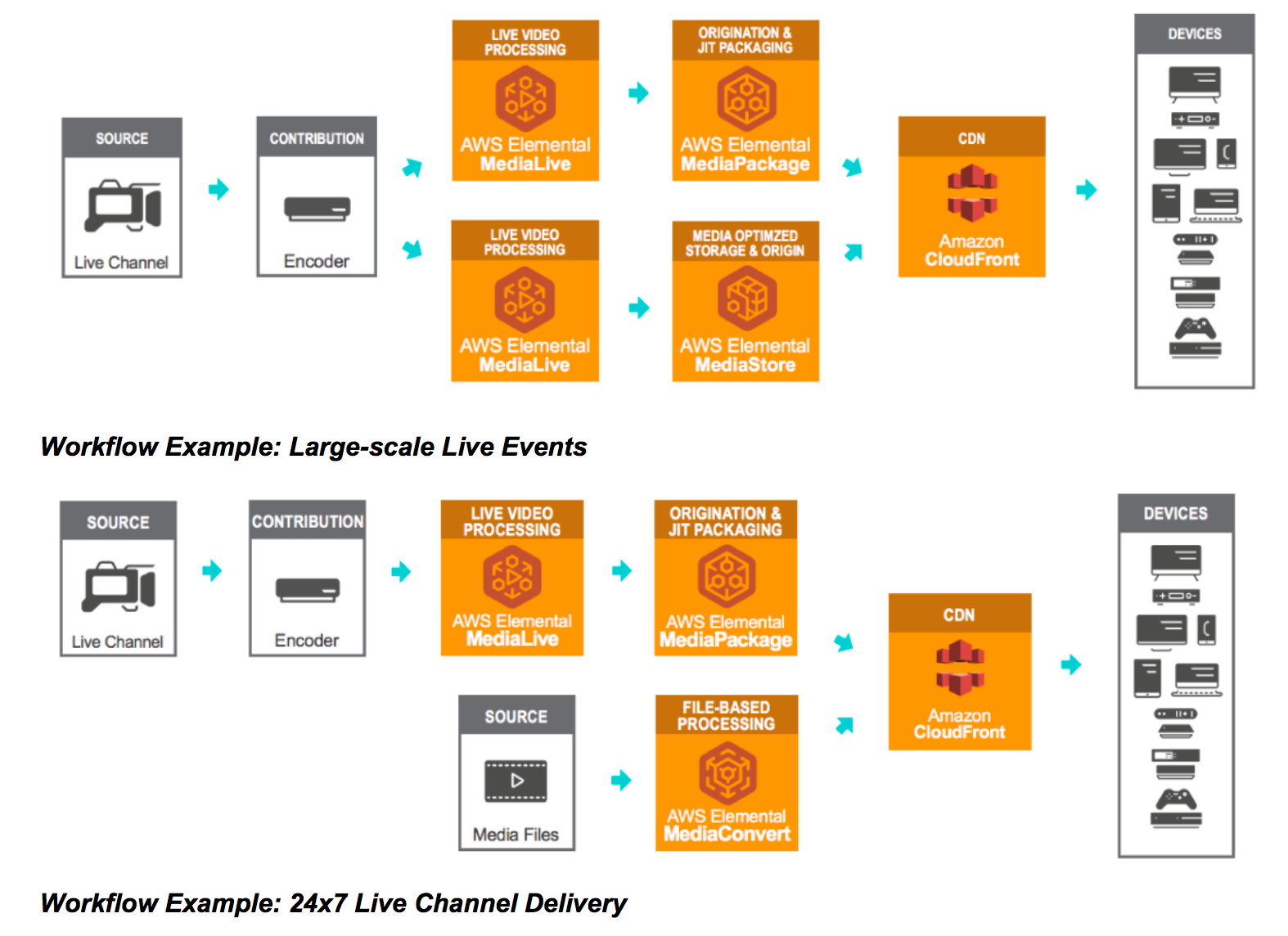
A solutions architect is designing multimedia application to publish live events. Videos of the performances will be streamed in real time and then will be available on demand. The event is expected to attract a global online audience.  
Which service will improve the performance of both the real-time and on-demand steaming?

* + AWS Global Accelerator
  + Amazon Route S3
  + Amazon S3 Transfer Acceleration
  + **Amazon CloudFront**

**Unattempted**

Exam Tip  
You can use CloudFront to deliver video on demand (VOD) or live streaming video using any HTTP origin. One way you can set up video workflows in the cloud is by using CloudFront together with AWS Media Services.  
Explanation  
On-Demand streaming

[](https://skillcertpro.com/wp-content/uploads/2020/08/a65.png)  
In the on demand streaming case, your video content is stored in Amazon S3. Your viewers can choose to watch it at any desired time, hence the name on-demand. A complete on-demand streaming solution typically makes use of Amazon S3 for storage, AWS Elemental MediaConvert for file-based video processing, and Amazon CloudFront for delivery.  
Amazon S3 is an excellent storage facility for your video assets. It is infinitely scalable, has built-in redundancy, and is available to you on a pay-as-you-go basis. You can upload your content to S3 in a number of different ways. You can start by using the AWS Management Console when your volume is low, and then move to a more automated system as your volume increases. It is very easy to use S3 from the console. After you create your AWS account, you simply log in, create an S3 bucket, and then upload your content. If you want to implement an automated system, you can use the AWS Command Line Interface in your own scripts or the Amazon S3 APIs in your own code.  
Once uploaded, you may need to convert your video into the size, resolution, or format needed by a particular television or connected device. AWS Elemental MediaConvert will take care of this for you. MediaConvert takes content from S3, transcodes it per your request, and stores the result back in S3. Transcoding processes video files, creating compressed versions of the original content to reduce its size, change its format, or increase playback device compatibility. Again, you can manage this process from the AWS Management Console, the command line, or via the MediaConvert APIs.  
With your content safely stored and available in the formats required by your users, the next step is global delivery with Amazon CloudFront. The Amazon Content Delivery Network caches content at the edges for low latency and high throughput video delivery. Its scalability means that you can serve up as much or as little video as you want. You can handle unexpected spikes in demand with ease on a pay-as-you-go basis (see the CloudFront pricing to learn more).  
At this point our story line forks, and you have two options. You can deliver the entire video file to the device before playing it, or you can stream it to the device.  
The first option is very easy to implement and is supported by just about every mobile device and desktop. All you need to do is to put your content in an S3 bucket and create a CloudFront distribution that points to the bucket. Your user’s video player will use CloudFront URLs (accessible as part of the distribution) to request the video file. The request will be directed to the best edge location, based on the user’s location. The CDN will serve the video from its cache, fetching it from the S3 bucket if it is not already cached. This option has a couple of downsides. It makes inefficient use of your viewer’s bandwidth. If the user doesn’t bother to watch the entire video, content that would never be seen is still downloaded and you are paying for it.  
The second option is almost always preferred. A family of video streaming protocols including Apple’s HTTP Live Streaming (HLS), Dynamic Adaptive Streaming over HTTP (DASH), Microsoft’s Smooth Streaming (MSS), and Adobe’s HTTP Dynamic Streaming (HDS) improve the user experience by delivering video as it is being watched, generally fetching content a few seconds ahead of when it will be needed. Playback starts more quickly, fast-forwarding is more efficient, and the overall user experience is smoother. With this option, you only pay for what the viewer watches, you don’t waste user’s bandwidth, and users get to see the desired content more quickly.  
You will need to do a little more work in order to implement the second option. First, you use MediaConvert to convert your video files to HLS format (the most widely supported streaming protocol). This will split the video into short segments and will also create a manifest file. Then, you point the CloudFront distribution at the manifest. Finally, to play the live stream, embed the manifest URL in the players that your users will play your live stream with. For example, to play a live stream for which the manifest file is myStream/playlist.m3u8 and the CloudFront distribution is d111111abcdef8.cloudfront.net, you embed the following URL in players: <http://d111111abcdef8.cloudfront.net/myStream/playlist.m3u8>  
The “Video on Demand on AWS” page provides best practices and guidance to consider when implementing a video on demand workflow on the AWS Cloud, and introduces an AWS solution that automatically provisions the services necessary to build a scalable, distributed architecture that ingests, stores, processes, and delivers video content.  
Live streaming

[](https://skillcertpro.com/wp-content/uploads/2020/08/a66.png)  
In the live streaming case, your content represents either live events or 24×7 live channel delivery. Examples of the first include broadcasters and content aggregators streaming sports tournaments, awards ceremonies, keynote addresses and other highly viewed live events. Examples of the latter include studios, broadcasters and pay TV service operators looking to package and deliver live linear channels over the Internet directly to their audiences, without a third-party distribution platform.  
You can use AWS to cost-effectively broadcast live content to a global audience by following a few simple steps.  
The first step is live video processing. For this you can use AWS Elemental MediaLive, which encodes your live video streams in real-time, taking a larger-sized live video source – for example, coming from an on-premises encoder like AWS Elemental Live – and compressing it into smaller versions for distribution to your viewers. For the second step, you have two options depending on your use case. You can use a just-in-time packaging origin like AWS Elemental MediaPackage to convert video content from a single format to multiple formats and securely package it for different device types. MediaPackage makes it easy to implement popular video features for viewers (start-over, pause, rewind, etc.), like those commonly found on DVRs. It can also protect your content using Digital Rights Management (DRM). Alternatively, if the encoder is already putting the content in the format required by all of your end viewer targeted devices, you can use a high performance scalable origin like AWS Elemental MediaStore. MediaPackage and MediaStore deliver the content to Amazon CloudFront, which will route it to the audience that’s viewing the live event.  
Once your solution is up and running, the live event can be broadcast around the global in a scalable, cost-effective fashion. The CDN can accommodate an audience that varies in size and can handle “flash crowds”.  
The “Live Video Streaming” page provides best practices and guidance to consider when choosing a live video streaming workflow on the AWS Cloud, and introduces an AWS solution that automatically provisions the services necessary to build a highly available and cost-effective architecture that delivers an exceptional real-time viewing experience.  
Reference  
<https://aws.amazon.com/cloudfront/streaming/>

1. 30. Question

You are working as a Solutions Architect for a multinational financial firm which has application running on Amazon EC2 instances in a  single region. the business continuity plan asked you to ensure that the resources can also be deployed to a second Region.  
Which combination of actions should the solutions architect take to accomplish this? (Choose two.)

* + Copy an Amazon Elastic Block Store (Amazon EBS) volume from Amazon S3 and launch an EC2 instance in the destination Region using that EBS volume.
  + Detach a volume on an EC2 instance and copy it to Amazon S3.
  + **Copy an Amazon Machine Image (AMI) of an EC2 instance and specify a different Region for the destination.**
  + Launch a new EC2 instance in a new Region and copy a volume from Amazon S3 to the new instance.
  + **Launch a new EC2 instance from an Amazon Machine Image (AMI) in a new Region.**

**Unattempted**

Exam Tip  
To create a copy of your AMI in another AWS Region, follow these steps:  
1- Create an AMI of your EC2 instance:  
2- Copy the AMI of your EC2 instance to another AWS Region:  
3-After the copy operation completes, launch a new EC2 instance from your AMI in the new AWS Region.  
Reference  
<https://aws.amazon.com/premiumsupport/knowledge-center/copy-ami-region/>

1. 31. Question

A Solutions Architect is designing multi-tier application consists of ELB application load balancer in the public subnet, multiple EC2 Instances with auto scaling group and Amazon DynamoDB.  
What is the best architecture to secure the application servers and DynamoDB ?

* + **Create private subnet for EC2 Instances and private subnet for DynamoDB**
  + Create private subnet for EC2 Instances and public subnet for DynamoDB
  + Create public subnet for EC2 Instances and private subnet for DynamoDB
  + Create public subnet for EC2 Instances and public subnet for DynamoDB

**Unattempted**

Exam Tip  
application servers and database must be secured so they must be added to the private subnet(s).  
Explanation  
Public subnet  
If a subnet’s default traffic is routed to an internet gateway, the subnet is known as a public subnet. For example, an instance launched in this subnet is publicly accessible if it has an Elastic IP address or a public IP address associated with it.  
Private subnet  
If a subnet’s default traffic is routed to a NAT instance/gateway or completely lacks a default route, the subnet is known as a private subnet. For example, an instance launched in this subnet is not publicly accessible even if it has an Elastic IP address or a public IP address associated with it.  
Reference  
<https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/>

1. 32. Question

A Solutions Architect is designing a new application which uses an Amazon S3 bucket to store files with sensitive data , the files must be encrypted and the encryption keys must be automatically rotated every month also the security team needs to track the usage of encryption key.  
What is the Simplest solution to handle this requirement?

* + Use Server-Side Encryption with Customer-Provided Keys (SSE-C)
  + Use AWS Trusted Advisor
  + Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3).
  + **Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS).**

**Unattempted**

Exam Tip  
automated rotation of the encryption keys+  track the usage of encryption key = use SSE-KMS  
Explanation  
You can choose to have AWS KMS automatically rotate CMKs every year, provided that those keys were generated within AWS KMS HSMs. Automatic key rotation is not supported for imported keys, asymmetric keys, or keys generated in an AWS CloudHSM cluster using the AWS KMS custom key store feature. If you choose to import keys to AWS KMS or asymmetric keys or use a custom key store, you can manually rotate them by creating a new CMK and mapping an existing key alias from the old CMK to the new CMK.  
Reference  
<https://aws.amazon.com/kms/faqs/>

1. 33. Question

A Solutions Architect is designing multi-tier application, the database tier in the private subnet needs to access the internet for periodically OS updates, he must ensures that the database will not be accessed from the internet?  
What is the simplest approach to achieve this requirement?

* + Add NAT Gateway in the private subnet and add rout to it from the public subnet
  + Configure the database subnet network ACL to allow outbound traffic and deny the inbound traffic.
  + Enable inbound rule in the Security Group for HTTP port only.
  + **Add NAT Gateway in the public subnet and add route to it from the private subnet**

**Unattempted**

Exam Tip  
You can create a NAT gateway for EC2 instances in a private VPC subnet to connect securely over the Internet. Because the subnet is private, the IP addresses assigned to the instances cannot be used in public. Instead, it is necessary to use network address translation (NAT) to map the private IP addresses to a public address for requests, and then map the public IP address back to private addresses for the response.  
Explanation  
you have to follow these steps to create a NAT gateway:  
Prerequisites:  
a) Create a public VPC subnet to host the NAT gateway. The route table for the subnet should contain a route to the Internet through an Internet gateway.  
b) Provision an unattached Elastic IP address (EIP) to your account. You’ll need to associate this IP address with the NAT gateway.  
c) Update the route table of the private subnet hosting the EC2 instances that need Internet access. The route table should be updated to direct Internet-bound traffic to the NAT gateway.  
After ensuring that prerequisites are met, follow these steps:  
1. Sign in to the AWS Management Console.  
2. Open the Amazon VPC console.  
3. Choose NAT Gateway from the navigation bar on the left.  
4. Choose Create NAT Gateway and then select the public subnet and EIP that you have provisioned for the NAT gateway.  
5. After you create the NAT gateway, make note of the associated ID, which will resemble “nat-xxxxxxx”.  
6. Choose the Route Tables link on the left hand side, and then choose the route table associated with your NAT gateway. Update this route table so that 0.0.0.0/0 points to the ID of the NAT gateway that you created.

Reference  
<https://aws.amazon.com/premiumsupport/knowledge-center/nat-gateway-vpc-private-subnet/>

1. 34. Question

A client has unencrypted data in Amazon Redshift cluster and asked you about the best technique to encrypt data at rest.  
What is your recommendation ?

* + Move the Redshift cluster from public subnet to private subnet.
  + **Use the AWS KMS.**
  + Use SSL/TLS
  + Use Amazon EBS volumes.

**Unattempted**

Exam Tip  
AWS KMS is best option encrypt the data at rest in Amazon Redshift cluster  
Explanation  
In Amazon Redshift, you can enable database encryption for your clusters to help protect data at rest. When you enable encryption for a cluster, the data blocks and system metadata are encrypted for the cluster and its snapshots.  
You can enable encryption when you launch your cluster, or you can modify an unencrypted cluster to use AWS Key Management Service (AWS KMS) encryption. To do so, you can use either an AWS-managed key or a customer-managed key (CMK). When you modify your cluster to enable KMS encryption, Amazon Redshift automatically migrates your data to a new encrypted cluster. Snapshots created from the encrypted cluster are also encrypted. You can also migrate an encrypted cluster to an unencrypted cluster by modifying the cluster and changing the Encrypt database option  
Reference  
<https://docs.aws.amazon.com/redshift/latest/mgmt/working-with-db-encryption.html>

1. 35. Question

You are working in Insurance company ,the company has an web application used by patients to upload they prescriptions into Amazon S3,the customer support team received a lot of complains from the patients that sometimes they see the old prescriptions especially in the peak times.  
Which option may be the root cause for this issue?

* + Communication issue between the application and S3
  + **Same keys are overwritten while executing updating queries by the application.**
  + S3 use randomized object naming
  + Duplication of same S3 buckets

**Unattempted**

Exam Tip  
due to S3 is eventually Consistent  , reading after writing may return old data.  
Explanation  
mazon S3 provides read-after-write consistency for PUTS of new objects in your S3 bucket in all Regions with one caveat. The caveat is that if you make a HEAD or GET request to a key name before the object is created, then create the object shortly after that, a subsequent GET might not return the object due to eventual consistency.  
Amazon S3 offers eventual consistency for overwrite PUTS and DELETES in all Regions.  
Updates to a single key are atomic. For example, if you PUT to an existing key, a subsequent read might return the old data or the updated data, but it never returns corrupted or partial data.  
Reference  
<https://docs.aws.amazon.com/AmazonS3/latest/dev/Introduction.html>

1. 36. Question

What is the best solution to recover static website within an Amazon S3 bucket case of accidental deletion ?

* + Enable Amazon S3 cross-Region replication.
  + **Enable Amazon S3 versioning.**
  + Enable an Amazon S3 lifecycle policy.
  + Enable Amazon S3 Intelligent-Tiering.

**Unattempted**

Exam Tip  
to recover deleted object from Amazon S3 bucket , you have to enable versioning.  
Explanation  
When you delete an object from a version-enabled bucket, Amazon S3 creates a delete marker for the object. The delete marker becomes the current version of the object, and the actual object becomes the previous version. With a delete marker, Amazon S3 responds to requests for the object as though the object was deleted. For example, if you send a GET request for the object, Amazon S3 returns an error.  
Reference  
<https://aws.amazon.com/premiumsupport/knowledge-center/s3-undelete-configuration/>

1. 37. Question

A solutions architect in a Multimedia company is designing application which will use Amazon S3 to store images uploaded by its users. these images must be encrypted at rest in Amazon S3.  the security team does not want to spend time managing and rotating the keys, but it does want to control who can access those keys.  
What should a solutions architect use to accomplish this?

* + **Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)**
  + Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
  + Server-Side Encryption with Customer-Provided Keys (SSE-C)
  + Server-Side Encryption with keys stored in an S3 bucket

**Unattempted**

Exam Tip  
AWS Key Management Service (AWS KMS) is a service that combines secure, highly available hardware and software to provide a key management system scaled for the cloud. When you use server-side encryption with AWS KMS (SSE-KMS), you can specify a customer managed CMK that you have already created. SSE-KMS provides you with an audit trail that shows when your CMK was used and by whom. Therefore SSE-KMS is the correct solution for this use-case.  
Explanation  
AWS Key Management Service (KMS) makes it easy for you to create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect your keys. AWS KMS is integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.  
Reference  
<https://aws.amazon.com/kms/>

1. 38. Question

A Chief Architect is designing a system to analyze the performance of financial markets while the markets are closed. The system will run a series of compute- intensive jobs for 5 hours every night. The time to complete the compute jobs is expected to remain constant, and jobs cannot be interrupted once started. Once completed, the system is expected to run for a minimum of 1 year.  
Which type of Amazon EC2 instances should be used to reduce the cost of the system?

* + Spot instances
  + On-Demand instances
  + Standard Reserved Instances
  + **Scheduled Reserved Instances**

**Unattempted**

Exam Tip  
The answer is between “Standard Reserved Instances” and “Scheduled Reserved Instances”. Schedule reserved instances have some limitations: The following are the only supported instance types: C3, C4, M4, and R3. The required term is 365 days (one year). The minimum required utilization is 1,200 hours per year. You can purchase a Scheduled Instance up to three months in advance. They are available in the following Regions: US East (N. Virginia), US West (Oregon), and Europe (Ireland). So if you go with “Scheduled Reserved Instances” our options are pretty narrow down by region, even if the question doesn’t specify this. It doesn’t say for what period it will run for 4 hours every day. Even if some limitations are met for scheduled reserved instances, make more sense to use on-demand instances.  
With Reserved Instances, you can now choose the type of capacity reservation that best fits your needs:  
Standard Reserved Instances: The instances you reserved are available to launch any time, 24 hours/day x 7 days/week. This option provides the most flexibility to run instances whenever you need them, including steady state workloads.  
Scheduled Reserved Instances: Instances are available to launch within the time windows you reserved. This option allows you to match your capacity reservation to a predictable recurring schedule.  
Reference: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html>

1. 39. Question

A cat tracking application is running on multiple Amazon EC2 instances. The application processes messages from an Amazon SQS queue, writes for an Amazon RDS table, and deletes the message from the queue. Occasional duplicate records are found in the RDS table. The SQS queue does not contain any duplicate messages.  
What should a solutions architect do to ensure messages are being processed once only?

* + **Use the ChangeMessageVisibility API call to increase the visibility timeout.**
  + Use the CreateQueue API call to create a new queue.
  + Use the CreateQueue API call to create a new queue.
  + Use the ReceiveMessage API call to set an appropriate wait time.

**Unattempted**

Exam Tip  
The visibility timeout begins when Amazon SQS returns a message. During this time, the consumer processes and deletes the message. However, if the consumer fails before deleting the message and your system doesn’t call the DeleteMessage action for that message before the visibility timeout expires, the message becomes visible to other consumers and the message is received again. If a message must be received only once, your consumer should delete it within the duration of the visibility timeout.  
Reference  
<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html>

1. 40. Question

You are working as solution architect in a research company which currently has legacy application used to download scientific PDFs from internet then store it in a local storage,the company wants to migrate its storage to AWS S3 buckets using the existing VPN connection between company network and AWS.  
What is the simplest solution to open the firewall to access S3 bucket from company network ?

* + Create Lambda function with an IAM role with permissions to access S3 bucket and call the Lambda function from the application
  + Use Amazon CloudFront with S3 buckets as the origin and configure the CloudFront IP in the company network
  + **Create an IAM role with S3 bucket access permissions to allow accessing from company network.**
  + Configure IP whitelisting in Amazon API Gateway.

**Unattempted**

Exam Tip  
Company Network + VPN + S3 Bucket = Create an IAM role with S3 bucket access permissions  
Explanation  
Both individuals and companies can use bucket policies. When companies register with Amazon S3, they create an account. Thereafter, the company becomes synonymous with the account. Accounts are financially responsible for the AWS resources that they (and their employees) create. Accounts have the power to grant bucket policy permissions and assign employees permissions based on a variety of conditions. For example, an account could create a policy that gives a user write access To a particular S3 bucket and /OR from from an account’s corporate network

Reference  
<https://docs.aws.amazon.com/AmazonS3/latest/dev/Introduction.html>

1. 41. Question

A Solutions Architect is designing a static website which will use the zone apex of a DNS domain (e.g. yourcompany.com).  
Which AWS service should you recommend to handle this requirement?

* + **Store the static content in S3 Bucket and map a Route 53 alias record to website endpoint then create a Route 53 hosted zone.**
  + Store the static content in Amazon CloudFront and map a Route 53 alias record to CloudFront IP
  + Store the static content in docker container and map a Route 53 alias record to container IP.
  + Store the static content in Amazon EC2 instance, and map a Route 53 alias record to the public IP address of the Amazon EC2 instance.

**Unattempted**

Exam Tip  
the best solution is to host the static website in S3 (no EC2 needed). Map a Route 53 endpoint to the website endpoint gives you everything you need in terms of cost effective and scalable solution.  
Explanation  
you have to follow the following steps :-  
Step 1: Register a custom domain with Route 53  
Step 2: Create two buckets  
Step 3: Configure your root domain bucket for website hosting  
Step 4: Configure your subdomain bucket for website redirect  
Step 5: Configure logging for website traffic  
Step 6: Upload index and website content  
Step 7: Edit block public access settings  
Step 8: Attach a bucket policy  
Step 9: Test your domain endpoint  
Step 10: Add alias records for your domain and subdomain  
Step 11: Test the website  
Reference  
<https://docs.aws.amazon.com/AmazonS3/latest/dev/website-hosting-custom-domain-walkthrough.html>

1. 42. Question

A training provider has a web application which stores educational videos in Amazon S3 bucket in eu-east-1 to serve customer around the world, during the peak hours, some customers in Asia report receiving HTTP 500 errors,  
As AWS Solutions Architect, how to solve this issue?

* + **Use Amazon CloudFront to cache the web content and use edge locations to deliver the content.**
  + Replicate the bucket policy into another Region.
  + Use Amazon S3 with failover routing policy in front of Amazon S3 Bucket
  + Create Classic Load Balancer in front of Amazon S3 bucket

**Unattempted**

Exam Tip  
Keyword deliver content around the world so CloudFront is the content delivery feature.  
Explanation  
To deliver video on demand (VOD) streaming with CloudFront, use the following services:  
a) Amazon S3 to store the content in its original format and to store the transcoded video.  
b) An encoder (such as AWS Elemental MediaConvert) to transcode the video into streaming formats.  
c) CloudFront to deliver the transcoded video to viewers.  
To create a VOD solution with CloudFront:  
a) Upload your content to an Amazon S3 bucket.  
b) Transcode your content by using a MediaConvert job. The job converts your video into the formats required by the players that your viewers use. You can also use the job to create assets that vary in resolution and bitrate. These assets are used for adaptive bitrate (ABR) streaming, which adjusts the viewing quality depending on the viewer’s available bandwidth. MediaConvert stores the transcoded video in an S3 bucket.  
c) Deliver your converted content by using a CloudFront distribution. Viewers can watch the content on any device, at any time.

Reference  
<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/on-demand-video.html>

1. 43. Question

As Solutions architect, you have a task to enhance the current architecture of dynamic web site which is deployed on multiple EC2 instances inside same subnet behind ELB Application Load balancer to support High availability.  
What is the SIMPLEST solution to provide HA to the current architecture?

* + Replace the current architecture with Amazon API Gateway and Lambda function
  + Move some Amazon EC2 instances to another subnet in the same Availability Zone.
  + **Move some Amazon EC2 instances to another subnet in the different Availability Zone.**
  + Replace the ELB Application load balancer with ELB Network load balancer

**Unattempted**

Exam Tip  
High Availability = Multi AZ  
Explanation  
When you add a subnet to your load balancer, Elastic Load Balancing creates a load balancer node in the Availability Zone. Load balancer nodes accept traffic from clients and forward requests to the healthy registered instances in one or more Availability Zones. For load balancers in a VPC, we recommend that you add one subnet per Availability Zone for at least two Availability Zones. This improves the availability of your load balancer. Note that you can modify the subnets for your load balancer at any time.  
Select subnets from the same Availability Zones as your instances. If your load balancer is an Internet-facing load balancer, you must select public subnets in order for your back-end instances to receive traffic from the load balancer (even if the back-end instances are in private subnets). If your load balancer is an internal load balancer, we recommend that you select private subnets.

Reference  
<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-manage-subnets.html>

1. 44. Question

What is the MOST secure way to allow public user for a limited time from accessing a file stored on Amazon S3 and is 10 GB in size?

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

**Unattempted**

Exam Tip  
The presigned URLs are valid only for the specified duration.  
Explanation  
All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a presigned URL, using their own security credentials, to grant time-limited permission to download the objects.  
When you create a presigned URL for your object, you must provide your security credentials, specify a bucket name, an object key, specify the HTTP method (GET to download the object) and expiration date and time. The presigned URLs are valid only for the specified duration.  
Anyone who receives the presigned URL can then access the object. For example, if you have a video in your bucket and both the bucket and the object are private, you can share the video with others by generating a presigned URL.  
Reference  
<https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html>

1. 45. Question

A training provider hosts a website which consists of dynamic and static content, this website runs on Amazon EC2 instances behind an Application Load Balancer (ALB) , some of users around the world are suffering from the slowness of the website.  
Which action can be done to improve website performance for users worldwide?

* + **Create an Amazon CloudFront distribution and configure the ALB as an origin. Then update the Amazon Route 53 record to point to the CloudFront distribution.**
  + Launch new EC2 instances hosting the same web application in different Regions closer to the users. Then register instances with the same ALB using cross- Region VPC peering.
  + Create a latency-based Amazon Route 53 record for the ALB. Then launch new EC2 instances with larger instance sizes and register the instances with the ALB.
  + Host the website in an Amazon S3 bucket in the Regions closest to the users and delete the ALB and EC2 instances. Then update an Amazon Route 53 record to point to the S3 buckets.

**Unattempted**

Exam Tip  
Amazon CloudFront is used to serve dynamic and/or static assets from Amazon EC2  
Explanation  
t’s common practice to use Amazon CloudFront to accelerate the delivery of static web assets stored in Amazon Simple Storage Service (Amazon S3) to end users. CloudFront can cache content at edge locations closer to your viewers giving them greater performance, instant global reach, and higher platform availability. For Amazon Elastic Compute Cloud (Amazon EC2) origins serving dynamic and/or static content, you should also consider using CloudFront because it offers a number of additional benefits. In this blog post, we will provide an overview of the performance, security, and cost benefits you get when using CloudFront to serve dynamic and/or static assets from Amazon EC2. We will also walk through the exercise of configuring CloudFront for Amazon EC2 origins.  
Performance  
– Cacheable Content. While most applications serve static content from Amazon S3, origins in Amazon EC2 that serve static content can also benefit from caching content at the edge. By leveraging the CloudFront edge locations and regional edge caches, applications can reduce the origin’s workload and bandwidth utilization while bringing content closer to viewers. This reduces the latency of serving static content.  
– Global Reach. The CloudFront global network, which consists of over 100 points of presence (POP), reduces the time to establish viewer-facing connections because the physical distance to the viewer is shortened. This reduces overall latency for serving both static and dynamic content.  
– Persistent Connections. CloudFront maintains a pool of persistent connections to the origin, thus reducing the overhead of repeatedly establishing new connections to the origin. Over these connections, traffic between CloudFront and AWS origins are routed over a private backbone network for reliability and performance. This reduces overall latency for serving both static and dynamic content.  
– Collapsed Forwarding. During traffic spikes, CloudFront collapses simultaneous requests for cache misses before forwarding the request to your origin reducing unnecessary load to your origin.  
Reference  
<https://aws.amazon.com/blogs/networking-and-content-delivery/dynamic-whole-site-delivery-with-amazon-cloudfront/>

1. 46. Question

You are working in popular company as Solutions architect, your company has DynamoDB database running inside private subnet and it was requested from you to create lambda function in same VPC to insert some records in DynamoDB.  
What is the best solution to give Lambda an access to DynamoDB ?

* + Update the inbound security rules of Lambda to allow the DynamoDB Security Group
  + Move the lambda outside DynamoDB VPC
  + Create VPC Endpoint for DynamoDb VPC
  + **Update the inbound security rules of DynamoDB to allow the Lambda Security Group**

**Unattempted**

Exam Tip  
First you will need to enable VPC access for the Lambda function, during which you will assign it a Security Group. Then, within the Security Group assigned to the DynamoDB instance you will enable access for the Security Group assigned to the Lambda function.  
Explanation  
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC can be assigned to a different set of security groups.  
If you launch an instance using the Amazon EC2 API or a command line tool and you don’t specify a security group, the instance is automatically assigned to the default security group for the VPC. If you launch an instance using the Amazon EC2 console, you have an option to create a new security group for the instance.  
For each security group, you add rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic. This section describes the basic things that you need to know about security groups for your VPC and their rules.  
Reference  
<https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html>

1. 47. Question

A research company has been storing analytics data in an Amazon RDS instance for the past few years. the company decide to expose the data to be accessed to external users via  an API. The expectation is that the application will experience periods of inactivity but could receive bursts of traffic within seconds.  
Which solution should the solutions architect suggest?

* + Set up an Amazon API Gateway and use AWS Elastic Beanstalk.
  + Set up an Amazon API Gateway and use Amazon ECS.
  + Set up an Amazon API Gateway and use Amazon EC2 with Auto Scaling.
  + **Set up an Amazon API Gateway and use AWS Lambda functions.**

**Unattempted**

Exam Tip  
Quickest way to handle sudden increase in traffic = Use Amazon API Gateway and AWS Lambda functions.  
Explanation  
You can create a web API with an HTTP endpoint for your Lambda function by using Amazon API Gateway. API Gateway provides tools for creating and documenting web APIs that route HTTP requests to Lambda functions. You can secure access to your API with authentication and authorization controls. Your APIs can serve traffic over the internet or can be accessible only within your VPC.  
To add a public endpoint to your Lambda function  
1. Open the Lambda console Functions page.  
2. Choose a function.  
3. Under Designer, choose Add trigger.  
4. Choose API Gateway.  
5. For API, choose Create an API.  
6. For Security, choose Open.  
7. Choose Add.  
With the API Gateway trigger selected in the designer, choose the endpoint to invoke the function with API Gateway.

Reference  
<https://docs.aws.amazon.com/lambda/latest/dg/services-apigateway.html>

1. 48. Question

An e-commerce application consists of two-step order process to process orders exactly once and in the order in which they are received . The first step is synchronous and must return to the user with little latency. The second step takes longer  
How should the solutions architect integrate these components?

* + Use an AWS Lambda function along with Amazon SQS standard queues.
  + **Use Amazon SQS FIFO queues.**
  + Create an SNS topic and subscribe an Amazon SQS FIFO queue to that topic.
  + Create an SNS topic and subscribe an Amazon SQS Standard queue to that topic.

**Unattempted**

Exam Tip  
this is a trick question. the question never ask to select two or two components. pay attention to the part that says “The second step takes longer, so it will be implemented in a separate component.” its telling you to dont worry about the second part. The answer is A, address the first part of the questions.  
Explanation  
FIFO (First-In-First-Out) queues are designed to enhance messaging between applications when the order of operations and events is critical, or where duplicates can’t be tolerated, for example:  
a – Ensure that user-entered commands are executed in the right order.  
b – Display the correct product price by sending price modifications in the right order.  
c – Prevent a student from enrolling in a course before registering for an account.  
FIFO queues also provide exactly-once processing but have a limited number of transactions per second (TPS):  
Reference  
<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html>

1. 49. Question

As Solution Architect, you have a requirement to design online stock trading system which will heavily use transactional and scalable database with high write consistency, each order  will be saved in multiple linked tables.  
Which AWS database should be used to handle this requirement?

* + Amazon DynamoDB
  + Amazon S3
  + Amazon Redshift
  + **Amazon Aurora**

**Unattempted**

Exam Tip  
transactional + scalable database + high write consistency + linked tables = Amazon Aurora  
Explanation  
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 is up to five times faster than standard MySQL databases and three times faster than standard PostgreSQL databases. It provides the security, availability, and reliability of commercial databases at 1/10th the cost. Amazon Aurora is fully managed by Amazon Relational Database Service (RDS), which automates time-consuming administration tasks like hardware provisioning, database setup, patching, and backups.  
Reference  
<https://aws.amazon.com/rds/aurora/>

1. 50. Question

A company needs to ensure that all files created in an Amazon S3 are not eligible for accidental deletion and ensure that all versions of the documents are available in addition to allowing users to download, modify, and upload documents.

Which action in addition to enable versioning is needed to meet these requirements?

* + Encrypt the bucket using AWS KMS.
  + **Enable MFA Delete on the bucket.**
  + Enable a read-only bucket ACL.
  + Attach an IAM policy to the bucket.
  + Enable versioning on the bucket.

**Unattempted**

Exam Tip  
Enable MFA Delete is to require multi-factor authentication (MFA) when deleting an object version.  
Explanation  
If a bucket’s versioning configuration is MFA Delete–enabled, the bucket owner must include the x-amz-mfa request header in requests to permanently delete an object version or change the versioning state of the bucket. Requests that include x-amz-mfa must use HTTPS. The header’s value is the concatenation of your authentication device’s serial number, a space, and the authentication code displayed on it. If you do not include this request header, the request fails.  
For more information about authentication devices, see  
Reference  
<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMFADelete.html>

1. 51. Question

A company is evaluating Amazon S3 as a data storage solution to migrate a critical dataset. The current solution design uses a single S3 bucket in a single Region with versioning enabled to store the dataset. The business continuity team states that all data multiple AWS Regions.  
How should a solutions architect design the S3 solution?

* + Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS).
  + **Create an additional S3 bucket with versioning in another Region and configure Cross-Region Replication (CRR)**
  + Create an additional S3 bucket in another Region and configure Cross-Region Replication (CRR).
  + Create an additional S3 bucket with versioning in another Region and configure cross-origin resource (CORS).

**Unattempted**

Exam Tip  
for Cross-Region Replication (CRR), we must create addition S3 bucket with version enabled.  
Explanation  
Amazon S3 Cross-Region Replication (CRR)  
With S3 Cross-Region Replication (CRR), you can replicate objects (and their respective metadata and object tags) into other AWS Regions for reduced latency, compliance, security, disaster recovery, and other use cases. S3 CRR is configured to a source S3 bucket and replicates objects into a destination bucket in another AWS Region.  
Amazon S3 CRR automatically replicates data between buckets across different AWS Regions. With CRR, you can set up replication at a bucket level, a shared prefix level, or an object level using S3 object tags. You can use CRR to provide lower-latency data access in different geographic regions. CRR can also help if you have a compliance requirement to store copies of data hundreds of miles apart. You can use CRR to change account ownership for the replicated objects to protect data from accidental deletion. To learn more about CRR,  
Reference  
<https://aws.amazon.com/s3/features/replication/>

1. 52. Question

A Solutions Architect is designing three tiers web site which will be highly available. he needs to ensure that the database tier will accept requests only from the application servers.  
What is the best solution to handle this requirement?

* + **Configure the inbound rule of the database security group to accept only requests from application server security Group.**
  + Configure the network ACL for database subnet to accept requests only from application server subnet.
  + Configure the inbound rule of the database security group to accept only requests from application server IP.
  + Configure the inbound rule of the database security group to deny requests from all IPs other than application server IP.

**Unattempted**

Exam Tip  
The most secure way for this case is to configure the inbound rule of the target AWS resource to allow the security group of the source AWS resource.  
Explanation :-  
You can update the inbound or outbound rules for your VPC security groups to reference security groups in the peered VPC. Doing so allows traffic to flow to and from instances that are associated with the referenced security group in the peered VPC.  
Requirements  
a) The peer VPC can be a VPC in your account, or a VPC in another AWS account. To reference a security group in another AWS account, include the account number in Source or Destination field; for example, 123456789012/sg-1a2b3c4d.  
b) cannot reference the security group of a peer VPC that’s in a different region. Instead, use the CIDR block of the peer VPC.  
c) To reference a security group in a peer VPC, the VPC peering connection must be in the active state.

Reference  
<https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-security-groups.html>

1. 53. Question

A multinational scientific company has a scientific web application which is hosted on a single Amazon EC2 instance and use Amazon EBS volume to stored used uploaded documents. the company decide to create same architecture on a second EC2 instance and EBS volume in another Availability Zone. both EC2 instances are behind application load balancer to provide highly available and scalable application. recently , the operation team  received a lot of complains from users that each time they refreshed the website, they could see one subset of their documents or the other, but never all of the documents at the same time.  
What should a solutions architect propose to ensure users see all of their documents at once?

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

**Unattempted**

Exam Tip  
shared storage between multiple EC2 instances = Use Amazon EFS  
Explanation  
Amazon EFS is designed to provide massively parallel shared access to thousands of Amazon EC2 instances, enabling your applications to achieve high levels of aggregate throughput and IOPS with consistent low latencies.  
Amazon EFS is well suited to support a broad spectrum of use cases from home directories to business-critical applications. Customers can use EFS to lift-and-shift existing enterprise applications to the AWS Cloud. Other use cases include: big data analytics, web serving and content management, application development and testing, media and entertainment workflows, database backups, and container storage.  
Reference  
<https://aws.amazon.com/efs/>

1. 54. Question

A Solution Architect is working in events Agency which currently has a ticketing system, the application currently require more than 16,000 IOPS on a particular volume to handle tickets booking. after ending of the event ,no needs for IOPS. your manager asked you to re-architect this application to enhance its performance without any downtime.  
What is the best Solution to achieve this requirement?

* + **Replace the EBS volume type with Provisioned IOPS.**
  + Use Amazon SQS .
  + Use multiple c4.2xlarge Amazon EC2 instances behind ELB
  + Use EFS instead of EBS.

**Unattempted**

Exam Tip  
update EBS + no downtime = Replace the EBS volume type with Provisioned IOPS.  
Explanation  
With Elastic Volumes, you can dynamically modify the size, performance, and volume type of your Amazon EBS volumes without detaching them.  
Reference  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/requesting-ebs-volume-modifications.html>

1. 55. Question

A Solutions Architect is designing a static pages. The pages are expected to generate millions of views from users around the world. these pages are stored in an Amazon S3 bucket.  
What is the efficient solution to handle this requirement?

* + Use Amazon EFS to store and server static files
  + Enable Amazon ElastiCache in the web server subnet.
  + Generate presigned URLs for the files.
  + **Use Amazon CloudFront with the S3 bucket as its origin.**

**Unattempted**

Exam Tip  
Static content on S3 = Use Cloudfront  
Explanation  
When you use Amazon S3 as an origin for your distribution, you place any objects that you want CloudFront to deliver in an Amazon S3 bucket. You can use any method that is supported by Amazon S3 to get your objects into Amazon S3, for example, the Amazon S3 console or API, or a third-party tool. You can create a hierarchy in your bucket to store the objects, just as you would with any other Amazon S3 bucket.  
Using an existing Amazon S3 bucket as your CloudFront origin server doesn’t change the bucket in any way; you can still use it as you normally would to store and access Amazon S3 objects at the standard Amazon S3 price. You incur regular Amazon S3 charges for storing the objects in the bucket. For more information about the charges to use CloudFront  
Reference  
<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/DownloadDistS3AndCustomOrigins.html#concept_S3Origin>

1. 56. Question

A multi-national bank uses an Amazon RDS PostgreSQL DB instance to store its application data. at End of each Month EOM , the financial team needs to generate some reports.  
What should a solutions architect do to reduce the impact on the database with the LEAST amount of effort?

* + Create a cross-Region read replica and direct reporting traffic to the replica.
  + Create a Multi-AZ database and direct reporting traffic to the standby.
  + Create an Amazon Redshift database and direct reporting traffic to the Amazon Redshift database.
  + **Create a read replica and direct reporting traffic to the replica.**

**Unattempted**

Exam Tip  
to generate reports without affecting the database performance = Use Read Replicas.  
Explanation  
Amazon RDS Read Replicas provide enhanced performance and durability for RDS database (DB) instances. They make it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances. Read replicas are available in Amazon RDS for MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server as well as Amazon Aurora.  
Reference  
<https://aws.amazon.com/rds/features/read-replicas/>

1. 57. Question

A Solutions Architect is designing a multi-tier web application architecture using multiple Linux Amazon EC2 instances and storing data on Amazon EBS volumes.  
What is the best solution to increase the resiliency of the application in case of a failure and to provide storage that complies with atomicity, consistency, isolation, and durability ?

* + Launch the application on EC2 instances in each Availability Zone. Attach EBS volumes to each EC2 instance.
  + Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Mount an instance store on each EC2 instance.
  + **Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data on Amazon EFS and mount a target on each instance.**
  + Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data using Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).

**Unattempted**

Exam Tip  
Application Load balancer+ Auto scaling group are used for resiliency, EFS for storage.  
Explanation  
Elastic Load Balancing is used to automatically distribute your incoming application traffic across all the EC2 instances that you are running. You can use Elastic Load Balancing to manage incoming requests by optimally routing traffic so that no one instance is overwhelmed.

To use Elastic Load Balancing with your Auto Scaling group, you set up a load balancer and then you attach the load balancer to your Auto Scaling group to register the group with the load balancer.

Your load balancer acts as a single point of contact for all incoming web traffic to your Auto Scaling group. When an instance is added to your group, it needs to register with the load balancer or no traffic is routed to it. When an instance is removed from your group, it must deregister from the load balancer or traffic continues to be routed to it.

When you use Elastic Load Balancing with your Auto Scaling group, it’s not necessary to register your EC2 instances with the load balancer. Instances that are launched by your Auto Scaling group are automatically registered with the load balancer. Likewise, instances that are terminated by your Auto Scaling group are automatically deregistered from the load balancer.

After registering a load balancer with your Auto Scaling group, you can configure your Auto Scaling group to use Elastic Load Balancing metrics such as the request count per target (or other metrics) to scale the number of instances in the group as the demand on your instances changes.

You can also optionally enable Elastic Load Balancing health checks to check the health of instances in your Auto Scaling group based on health checks provided by Elastic Load Balancing.  
Reference  
<https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html>

1. 58. Question

A Solutions Architect is designing a highly-scalable application to upload and download scientific researches, these files will be accessed from millions of users from around the world, the size of the files can reach to gigabytes in size.  
What is the best solution to minimize upload and download latency and maximize performance ?

* + Use Amazon EC2 with Auto Scaling and Amazon ElastiCache to host the application.
  + Use Amazon EC2 with Auto Scaling and Amazon CloudFront to host the application.
  + Use Amazon S3 with CacheControl headers to host the application.
  + **Use Amazon S3 with Transfer Acceleration to host the application.**

**Unattempted**

Exam Tip  
Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket.  
Explanation

Amazon S3 Transfer Acceleration can speed up content transfers to and from Amazon S3 by as much as 50-500% for long-distance transfer of larger objects. Customers who have either web or mobile applications with widespread users or applications hosted far away from their S3 bucket can experience long and variable upload and download speeds over the Internet. S3 Transfer Acceleration (S3TA) reduces the variability in Internet routing, congestion and speeds that can affect transfers, and logically shortens the distance to S3 for remote applications. S3TA improves transfer performance by routing traffic through Amazon CloudFront’s globally distributed Edge Locations and over AWS backbone networks, and by using network protocol optimizations. You can turn on S3TA with a few clicks in the S3 console, and test its benefits from your location with a speed comparison tool. With S3TA, you pay only for transfers that are accelerated.

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.  
When using Transfer Acceleration, additional data transfer charges may apply.  
Why Use Amazon S3 Transfer Acceleration?  
You might want to use Transfer Acceleration on a bucket for various reasons, including the following:  
a – You have customers that upload to a centralized bucket from all over the world.  
b – You transfer gigabytes to terabytes of data on a regular basis across continents.  
c – You are unable to utilize all of your available bandwidth over the Internet when uploading to Amazon S3.

Reference  
<https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html>

1. 59. Question

A company provides electronic data info via a web application which hosted on a multiple Amazon C2 instances behind an Application Load Balancer in an Auto Scaling group. The website also uses a custom DNS name and communicates with HTTPS only using a dedicated SSL certificate. The company is planning a new product launch and wants to be sure that users from around the world have the best possible experience on the new website.  
What should a solutions architect do to meet these requirements?

* + Redesign the application to use AWS Elastic Beanstalk.
  + Redesign the application to use Amazon S3 static website hosting.
  + **Redesign the application to use Amazon CloudFront.**
  + Redesign the application to use a Network Load Balancer.

**Unattempted**

Exam Tip  
the best solution is to use CloudFront to cache contents, Application load balancer as Origin + Can expose external HTTPS and can talk to internal HTTPS backends

Explanation  
or Amazon S3 origins, CloudFront accepts requests in both HTTP and HTTPS protocols for objects in a CloudFront distribution by default. CloudFront then forwards the requests to your Amazon S3 bucket using the same protocol in which the requests were made.  
For custom origins, when you create your distribution, you can specify how CloudFront accesses your origin: HTTP only, or matching the protocol that is used by the viewer. For more information about how CloudFront handles HTTP and HTTPS requests for custom origins, i.e Application Load Balancer

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

1. 60. Question

You are working as a Solutions Architect for an investment bank and your Chief Technical Officer intends to migrate all of your applications to AWS. One of the company’s applications stores files on a Windows file server farm that uses Distributed File System Replication (DFSR) to keep data in sync. A solutions architect needs to replace the file server farm.  
Which service should the solutions architect use?

* + Amazon EFS
  + **Amazon FSx**
  + AWS Storage Gateway
  + Amazon EBS

**Unattempted**

Exam Tip  
Amazon FSx for windows  
Explanation  
Amazon FSx makes it easy and cost effective to launch and run popular file systems. With Amazon FSx, you can leverage the rich feature sets and fast performance of widely-used open source and commercially-licensed file systems, while avoiding time-consuming administrative tasks like hardware provisioning, software configuration, patching, and backups. It provides cost-efficient capacity and high levels of reliability, and it integrates with other AWS services so that you can manage and use the file systems in cloud-native ways.  
Amazon FSx provides you with two file systems to choose from: Amazon FSx for Windows File Server for business applications and Amazon FSx for Lustre for high-performance workloads.  
Reference  
<https://aws.amazon.com/fsx/>  
<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/migrate-files-to-fsx-datasync.html>

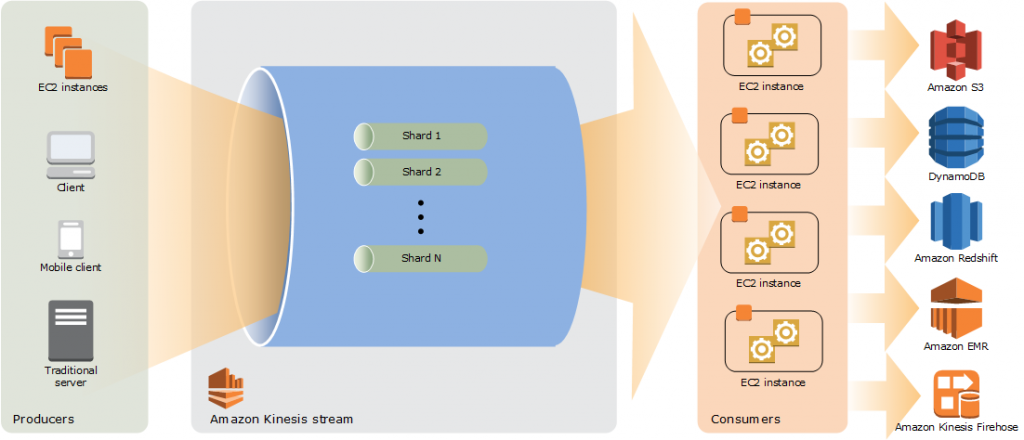
1. 61. Question

A Retail company wants to implement predictive maintenance on its machinery equipment. The company will install thousands of IoT sensors that will send data to AWS in real time.  
As Solutions Architect, what is the best solution to receive events in an ordered manner for each machinery asset and ensure that data is saved for further processing at a later time

* + Use an Amazon SQS FIFO queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function for the SQS queue to save data to Amazon EFS.
  + **Use Amazon Kinesis Data Streams for real-time events with a partition for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon S3.**
  + Use an Amazon SQS standard queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3.
  + Use Amazon Kinesis Data Streams for real-time events with a shard for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon EBS.

**Unattempted**

Exam Tip  
IOT data +  streams+ Partition by equipment + s3 =Use Amazon Kinesis Data Streams for real-time events with a partition for each equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon S3.

[](https://skillcertpro.com/wp-content/uploads/2020/08/a67.png)  
Explanation  
The following diagram illustrates the high-level architecture of Kinesis Data Streams. The producers continually push data to Kinesis Data Streams, and the consumers process the data in real time. Consumers (such as a custom application running on Amazon EC2 or an Amazon Kinesis Data Firehose delivery stream) can store their results using an AWS service such as Amazon DynamoDB, Amazon Redshift, or Amazon S3.

Reference  
<https://docs.aws.amazon.com/streams/latest/dev/key-concepts.html>

1. 62. Question

A solutions architect at a corporate bank and wants to back up application log data to Amazon S3.  
the logs access pattern are unpredictable. The bank wants to keep costs as low as possible by using the appropriate S3 storage class.  
Which S3 storage class should be implemented to meet these requirements?

* + S3 Standard-Infrequent Access (S3 Standard-IA)
  + S3 One Zone-Infrequent Access (S3 One Zone-IA)
  + S3 Glacier
  + **S3 Intelligent-Tiering**

**Unattempted**

Exam Tip  
Intelligent Tiering is designed for three use cases:  
  a – Unpredictable workloads  
  b – Changing access patterns  
  c – Lack of experience with storage optimization  
Explanation  
The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead. It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. For a small monthly monitoring and automation fee per object, Amazon S3 monitors access patterns of the objects in S3 Intelligent-Tiering, and moves the ones that have not been accessed for 30 consecutive days to the infrequent access tier. If an object in the infrequent access tier is accessed, it is automatically moved back to the frequent access tier. There are no retrieval fees when using the S3 Intelligent-Tiering storage class, and no additional tiering fees when objects are moved between access tiers. It is the ideal storage class for long-lived data with access patterns that are unknown or unpredictable. S3 Storage Classes can be configured at the object level and a single bucket can contain objects stored in S3 Standard, S3 Intelligent-Tiering, S3 Standard-IA, and S3 One Zone-IA. You can upload objects directly to S3 Intelligent-Tiering, or use S3 Lifecycle policies to transfer objects from S3 Standard and S3 Standard-IA to S3 Intelligent-Tiering. You can also archive objects from S3 Intelligent-Tiering to S3 Glacier.

Reference  
<https://aws.amazon.com/s3/storage-classes/>

1. 63. Question

An online retailer application runs on Amazon EC2 instances behind an Application Load Balancer with Auto Scaling group across multiple Availability Zones. at day 25 of each month, the application becomes much slower when the month-end financial calculation batch executes. This causes the CPU utilization of the EC2 instances to immediately peak to 100%, which disrupts the application.  
What is the best solution to handle this issue without downtime?

* + Configure an Amazon CloudFront distribution in front of the ALB.
  + Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization.
  + Configure Amazon ElastiGache to remove some of the workload from the EC2 instances.
  + **Configure an EC2 Auto Scaling scheduled scaling policy.**

**Unattempted**

Exam Tip  
Scheduled workloads  = use schedule scaling.  
Explanation  
Scheduled Scaling is a Scaling based on a schedule allows you to scale your application ahead of known load changes. For example, every week the traffic to your web application starts to increase on Wednesday, remains high on Thursday, and starts to decrease on Friday. You can plan your scaling activities based on the known traffic patterns of your web application.  
Reference  
<https://aws.amazon.com/ec2/autoscaling/>

1. 64. Question

A shipping company has online web application which uses Amazon Redshift as main data warehouse ,business continuity plan team recommended to have a disaster recovery for this storage to another recovery site with taking into consideration that the distance between both sites to be more than 2000 kilometres .  
What is the SIMPLEST solution to meet this requirement?

* + Manually move the data using AWS Snowball storage then enable replication.
  + Enable cross-region snapshot to a different Availability Zone.
  + **Enable cross-region snapshot to a different region.**
  + Use AWS Elastic Beanstalk to deploy the cluster in a second region.

**Unattempted**

Tip & Trick  
Simple solution for DR+ distance 2000 kilometres  = Enable cross-region snapshot to a different region.

Explanation  
Snapshots are point-in-time backups of a cluster. There are two types of snapshots: automated and manual. Amazon Redshift stores these snapshots internally in Amazon S3 by using an encrypted Secure Sockets Layer (SSL) connection.  
Amazon Redshift automatically takes incremental snapshots that track changes to the cluster since the previous automated snapshot. Automated snapshots retain all of the data required to restore a cluster from a snapshot. You can create a snapshot schedule to control when automated snapshots are taken, or you can take a manual snapshot any time.  
Reference  
<https://aws.amazon.com/blogs/aws/automated-cross-region-snapshot-copy-for-amazon-redshift/>  
<https://docs.aws.amazon.com/redshift/latest/mgmt/working-with-snapshots.html>

1. 65. Question

A Solutions Architect is working in migrating High Performance Computing (HPC) application with its data to AWS. The application uses tiered storage on premises which consists of high-performance parallel storage to hold data during periodic runs , and economical cold storage to hold the data when the application is not actively running.  
Which services can handle these requirements? (Choose two.)

* + Amazon S3 for high-performance parallel storage
  + **Amazon FSx for Lustre for high-performance parallel storage**
  + Amazon FSx for Windows for high-performance parallel storage
  + Amazon EFS for cold data storage
  + **Amazon S3 for cold data storage**

**Unattempted**

Exam Tip  
Cold data storage refers to the storage of inactive data that is rarely used or accessed  = Use Amazon S3  
Amazon FSx for Lustre for high-performance parallel storage  
Explanation  
Amazon FSx for Lustre makes it easy and cost effective to launch and run the world’s most popular high-performance file system. Use it for workloads where speed matters, such as machine learning, high performance computing (HPC), video processing, and financial modeling.  
The open source Lustre file system is designed for applications that require fast storage – where you want your storage to keep up with your compute. Lustre was built to quickly and cost effectively process the fastest-growing data sets in the world, and it’s the most widely used file system for the 500 fastest computers in the world. It provides sub-millisecond latencies, up to hundreds of gigabytes per second of throughput, and millions of IOPS.  
Reference  
<https://aws.amazon.com/fsx/lustre/>