Q1/218 **A major finance organisation has engaged your company to set up a large data mining application.  
Using AWS you decide the best service for this is Amazon Elastic MapReduce(EMR) which you know uses Hadoop.  
Which of the following statements best describes Hadoop?**

**A.** Hadoop is 3rd Party software which can be installed using AMI

**B.** Hadoop is an open source python web framework

**C.** **Hadoop is an open source Java software framework**

**D.** Hadoop is an open source javascript framework

**Answer: C** Amazon EMR uses Apache Hadoop as its distributed data processing engine.  
Hadoop is an open source, Java software framework that supports data-intensive distributed applications running on large clusters of commodity hardware. Hadoop implements a programming model named  
"MapReduce," where the data is divided into many small fragments of work, each of which may be executed on any node in the cluster.  
This framework has been widely used by developers, enterprises and startups and has proven to be a reliable software platform for processing up to petabytes of data on clusters of thousands of commodity machines.

Q2/218 **What is the charge for the data transfer incurred in replicating data** between your **primary and standby?**

**A.** Double the standard data transfer charge

**B.** **No charge**. It is free.

**C.** Half of the standard data transfer charge

**D.** Same as the standard data transfer charge

Q3/218 **A Solutions Architect must select the storage type for a big data application that requires very high sequential I/O. The data must persist if the instance is stopped.  
Which of the following storage types will provide the best fit at the LOWEST cost for the application?**

**A.** An Amazon EC2 instance store local SSD volume.

**B.** An Amazon EBS provisioned IOPS SSD volume.

**C.** An Amazon EBS throughput optimized HDD volume.

**D.** An Amazon EBS general purpose SSD volume

**Answer: B** Explanation https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html

Q4/218 **You receive a bill from AWS but are confused because you see you are incurring different costs for the exact same storage size in different regions on Amazon S3. You ask AWS why this is so. What response would you expect to receive from AWS?**

**A.** We charge less in different time zones.

**B.** We charge less where our costs are less.

**C.** This will balance out next bill.

**D.** It must be a mistake.

Answer **B** Explanation Here's a more detailed breakdown of the factors involved:

**Infrastructure Costs:**

Building and maintaining data centers in different regions involves varying costs for land, power, cooling, and physical security.

**Local Market Conditions:**

Labor costs, taxes, and other operational expenses can fluctuate between locations, impacting the overall cost of providing the service.

**Demand:**

Regions with higher customer demand for storage might have different pricing structures due to supply and demand dynamics.

**Specific S3 Storage Classes:**

The chosen storage class (e.g., Standard, Glacier) also influences the price, with some classes offering lower storage costs but potentially higher retrieval fees.

**Data Transfer:**

While S3 data transfer within a region is generally free, transferring data in or out of a region can incur costs.

AWS also offers tools to help manage and optimize costs:

**AWS Pricing Calculator:**

Users can estimate costs for different regions and storage classes using the calculator.

**AWS Cost Explorer:**

This tool allows users to visualize and analyze their AWS spending, helping identify areas where costs can be optimized.

**AWS Budgets:**

Users can set up budget alerts to monitor spending and proactively manage costs.

**AWS Cost and Usage Reports (CUR):**

These reports provide detailed cost and usage information, enabling in-depth analysis of spending patterns.

Q5/218 **A solutions architect is designing the architecture for a software demonstration environment. The environment will run on Amazon EC2 instances in an Auto Seating group bel (ALB). The system will experience significant increases in traffic during working hours but is not required to operate on weekends.  
Which combination of actions should the solutions architect take to ensure that the system can scale to meet demand? (Select TWO.)**

**A.** Use AWS Auto Scaling to adjust the ALB capacity based on request rate.

**B.** **Use a** target tracking scaling policy **to scale** the Auto Scaling group **based on** instance CPU utilization.

**C.** **Use** scheduled scaling **to change** the Auto Scaling group minimum, maximum, and desired capacity to zero **for weekends**. Revert to the default values at the start of

**D.** Launch the EC2 instances in multiple AWS Regions to distribute the load across Regions.

**E.** Use AWS Auto Scaling to scale the capacity of the VPC internet gateway.

Answers **B, C** Explanation:

**Target tracking scaling policy (B):**

By **using** a target tracking policy **based on** CPU utilization, the Auto Scaling group will automatically adjust the number of EC2 instances to maintain a desired level of CPU usage, ensuring sufficient resources during peak times.

**Scheduled scaling (C):**

This allows the architect to define a schedule for scaling the Auto Scaling group, specifically scaling down to zero instances during weekends **when** the system is not required to be operational, thus **minimizing** costs.

Q6/218 A company **hosts its web application on AWS using seven Amazon EC2 instances The company requires that the IP addresses of all healthy EC2 instances be returned in response to DNS queries. Which policy should be used to meet this requirement?**

**A.** Simple routing policy

**B.** Latency routing policy

**C.** Geolocation routing policy

**D.** **Multivalue** routing policy

Q7/218 **A company is writing a new service running on Amazon EC2 that must create thumbnail images of thousands of images in a large archive. The system will write scratch data to storage during the process. Which storage service is best suited for this scenario?**

**A.** Amazon CloudSearch

**B.** Amazon EBS Throughput Optimized HDD (st1)

**C.** Amazon EFS

**D.** EC2 instance store

**Correct Answer: C**

Q8/218 **You've been brought in as solutions architect to assist an enterprise customer with their migration of an e-commerce platform to Amazon Virtual Private Cloud (VPC) The previous architect has already deployed a 3-tier VPC.**The configuration is as follows**: VPC vpc-2f8t>C447 IGVV ig-2d8bc445 NACL acl-2080c448  
Subnets** and **Route Tables: Web server's** subnet**-258Dc44d Application server's** suDnet**-248bc44c Database** server's **subnet-9189c6f9  
Route Tables: rrb-218DC449 rtb-238bc44b  
Associations: subnet-258bc44d: rtb-2i8bc449 Subnet-248DC44C rtb-238tX44b subnet-9189c6f9 rtb-238Dc 44b  
You are now ready to begin deploying EC2 instances into the VPC Web servers must have direct access to the internet. Application and database servers cannot have direct access to the internet. Which configuration below will allow you the ability to remotely administer your application and database servers, as well as allow these servers to retrieve updates from the Internet?**

**A.** Add a route from rtD-238bc44D to igw-2d8bc445 and add a bastion and NAT instance within subnet-248bc44c.

**B.** Create a bastion and NAT Instance In subnet-258bc44d. Add a route from rtb-238bc44b to igw-2d8bc445. And a new NACL that allows access between subnet-258bc44d and subnet-248bc44c.

**C.** Create a bastion and NAT instance in suDnet-258Dc44d and add a route from rtD238Dc44D to the mat instance.

**D.** Create a bastion and NAT Instance in subnet-248bc44c and add a route from rtb238bc44b to subnet-258bc44d.

Explanation: To **enable remote administration** and **internet access for** updates **for** application **and** database servers **within a VPC** while **restricting** direct internet access, a NAT Gateway (or NAT Instance) in the public subnet can be used **in conjunction with** a Route Table **that directs** traffic destined for the internet through the NAT. Additionally, VPC Endpoints for S3 can be **created** for secure **and** private access ***to*** S3 ***from*** within the VPC.

Here's a breakdown of the configuration:

|  |  |
| --- | --- |
| A diagram of a network  AI-generated content may be incorrect. | 1. **Internet Gateway (IGW) Configuration:**   * The existing Internet Gateway (ig-2d8bc445) **is correctly attached** to the **VPC** (vpc-2f8t>C447) **and allows** internet traffic **to flow in and out** of the VPC.   2. **Route Tables and Subnet Associations**:   * **Web Server Subnet (subnet-258Dc44d):**   + Keep the current route table (rtb-218DC449) associated with this subnet.   + This route table should have a route that sends all traffic (0.0.0.0/0) to the Internet Gateway (ig-2d8bc445). * **Application Server Subnet (subnet-248bc44c) & Database Server Subnet (subnet-9189c6f9):**   + The current route table (rtb-238bc44b) associated with these subnets needs to be modified.   + This route table should have a route that directs all traffic (0.0.0.0/0) to the NAT Gateway (or NAT Instance) in the public subnet. * **NAT Gateway/Instance:**   + A NAT Gateway (or NAT Instance) should be deployed in the public subnet associated with the web server.   + This component handles the translation of private IP addresses to public IP addresses for outbound traffic from the application and database servers, allowing them to retrieve updates without having a direct public IP address. * **VPC Endpoints for S3:**   + Create VPC Endpoints for S3 in the VPC.   + These endpoints allow the application and database servers to access S3 resources privately and securely, without needing to go through the NAT Gateway or internet. |
| A diagram of a diagram  AI-generated content may be incorrect. | 3**. Security Groups:**   * **Web Servers:**   + **Open** inbound traffic **on** necessary ports (e.g., 80, 443) **from** the internet **for** HTTP and HTTPS traffic.   + Allow outbound traffic to the internet and other tiers as needed. * **Application Servers:**   + **Allow** inbound traffic **from** the web server's security group **on** appropriate ports.   + **Allow** outbound traffic **to** the database server's security group **on** appropriate ports.   + Allow outbound traffic to the internet only through the NAT Gateway. * **Database Servers:**   + **Allow** inbound traffic **from** the application server's security group **on** appropriate ports.   + Allow outbound traffic to the internet only through the NAT Gateway.   4. **Remote Access:**   * **Application and Database Servers:**   + To **administer** these servers remotely, you can **use** SSH (port 22) or RDP (port 3389) if using Windows, **but only** allow access **from** your specific IP address **or a** bastion host's security group for enhanced security.   + Configure the route tables and security groups accordingly to enable this access through the NAT Gateway or a VPN connection.   + If you need to access these servers from outside the VPC, consider using a bastion host or a VPN connection. |

In essence, the **combination** of a NAT Gateway, VPC Endpoints, **and** appropriate route tables **and** security groups **will allow** you to securely and privately manage your application and database servers, while **also** allowing them to retrieve updates from the internet via the NAT.

Q 9/218 **A company runs a static website through its on-premises data center. The company has multiple servers that handle all of its traffic, but on busy days, services are interrupted and the website becomes unavailable. The company wants to expand its presence globally and plans to triple its website traffic.  
What should a solutions architect recommend to meet these requirements?**

**A.** **Use** Amazon Route 53 **to distribute** the loads **across** multiple Amazon CloudFront distributions **for each** AWS Region that **exists globally**.

**B.** Migrate the website content to Amazon EC2 instances and vertically scale as the load increases.

**C.** Migrate the website content to Amazon EC2 instances with public Elastic IP addresses in multiple AWS Regions.

**D.** Migrate the website content to Amazon S3 and host the website on Amazon CloudFront.

**Answer: A This question is similar to 97/218 ! 😊**

Q **~~97~~** 10/113 **A company runs a static website through its on-premises data center. The company has multiple servers mat handle all of its traffic, but on busy days, services are interrupted and the website becomes unavailable. The company wants to expand its presence globally and plans to triple its website traffic.  
What should a solutions architect recommend to meet these requirements?**

**A.** Migrate the website content to **Amazon S3** and **host** the website on Amazon CloudFront.

**B.** Migrate the website content to Amazon EC2 instances with public Elastic IP addresses in multiple AWS Regions.

**C.** Migrate the website content to Amazon EC2 instances and vertically scale as the load increases.

**D.** Use Amazon Route 53 to distribute the loads across multiple Amazon CloudFront distributions for each AWS Region that exists globally.

**Correct Answer: A**

Q10/218 **A company is planning to migrate an** application **from** on-premises to AWS**. The** application currently **uses** an Oracle database and the company can **tolerate a brief** downtime of 1 hour **when performing** the switch **to the** new infrastructure. As part of the migration, the database engine **will be changed** to MySQL**. A Solutions Architect needs to determine which AWS services can be used to perform the migration while minimizing the amount of work and time required.  
Which of the following will meet the requirements?**

**A**. Use AWS DMS to begin moving data from the on-premises database to AWS. After the initial copy, continue to use AWS DMS to keep the databases in sync until cutting over to the new database. Use AWS Application Discovery Service to identify what embedded SQL code in the application can be converted and what has to be done manually.

**B.** Use AWS SCT to generate the schema scripts and apply them on the target prior to migration. Use AWS DMS ~~to~~ **~~analyze~~** the current schema and provide a recommendation for the optimal database engine. Then, use AWS DMS to migrate to the recommended engine. Use AWS SCT to identify what embedded SQL code in the application can be converted and what has to be done manually.

**C**. **Use** AWS SCT to **generate** the schema scripts **and apply** them on the target **prior** to migration. **Use** AWS DMS to begin **moving** data **from** the on-premises database **to** AWS. **After** the initial copy, **continue** to **use** AWS DMS to **keep** the databases in sync **until** cutting over to the new database. **Use** AWS SCT to **identify** **what** embedded SQL code in the application **can be** converted and **what has to be done** manually.

**D**. Use AWS DMS to help identify the best target deployment between installing the database engine on Amazon EC2 directly or moving to Amazon RDS. Then, use AWS DMS to migrate to the platform. Use AWS Application Discovery Service to identify what embedded SQL code in the application can be converted and what has to be done manually.

**Correct Answer: C**

Q11/218 A company's application is **increasingly popular** and **experiencing** latency **because of** high volume reads **on the** database server. **The service has the following properties:  
 \*** A highly available **REST API** hosted in one region **using** Application Load Balancer (ALB) **with** auto scaling. **\*** A MySQL database **hosted on** an Amazon EC2 instance **in a single** Availability Zone.The company **wants** to **reduce latency, increase** *in-region* database read **performance,** and **have** multi-region disaster recovery capabilities **that can perform** a live recovery automatically **without any** data or performance loss **(HA/DR). Which deployment strategy will meet these requirements?**

**A**. Use AWS CloudFormation StackSets to deploy the API layer i**n** two regions. Migrate the database to an Amazon Aurora with MySQL database cluster with multiple read replicas in one region **and** a read replica **in** **a** different region **than** the source database cluster. **Use** Amazon Route 53 health checks **to trigger** a DNS failover to the standby region **if the** health checks to the primary load balancer **fails**. In the event of Route 53 failover, **promote the** cross-region database replica **to be** the master and **build out** new read replicas in the standby region.

**B**. Use AWS CloudFormation StackSets to deploy the API layer in two regions. Add the database to an Auto Scaling group. Add a read replica to the database in the second region. Use Amazon Route 53 health checks on the database to trigger a DNS failover to the standby region if the health checks in the primary region fail. Promote the cross-region database replica to be the master and build out new read replicas in the standby region.

**C**. Use Amazon ElastiCache for Redis Multi-AZ with an automatic failover to cache the database read queries.  
Use AWS OpsWorks to deploy the API layer, cache layer, and existing database layer in two regions. In the event of failure, use Amazon Route 53 health checks on the database to trigger a DNS failover to the standby region if the health checks in the primary region fail. Back up the MySQL database frequently, and in the event of a failure in an active region, copy the backup to the standby region and restore the standby database.

**D**. Use Amazon ElastiCache for Redis Multi-AZ with an automatic failover to cache the database read queries.  
Use AWS OpsWorks to deploy the API layer, cache layer, and existing database layer in two regions. Use Amazon Route 53 health checks on the ALB to trigger a DNS failover to the standby region if the health checks in the primary region fail. Back up the MySQL database frequently, and in the event of a failure in an active region, copy the backup to the standby region and restore the standby database.

**Correct Answer: A**

Explanation: AI: **To address** the latency **and** multi-region disaster recovery requirements, a suitable **deployment strategy** would involve migrating the MySQL database to an Amazon Aurora MySQL-compatible read replica cluster, with one replica in the primary region and another in a separate region. This, combined with read-only replicas for high availability, and using Amazon Route 53 for health checks and failover, will meet the requirements.

Here's a breakdown of the recommended strategy:

**1. Migrate to Aurora MySQL:**

Replace the existing single-AZ MySQL instance with an Aurora MySQL-compatible read replica cluster. This cluster provides:

* + **High Availability:** Aurora's architecture allows for automatic failover to a replica in the event of an issue with the primary instance.
  + **Read Scalability:** Multiple read replicas can handle increased read traffic, reducing latency.
  + **Multi-AZ Support:** Aurora distributes replicas across multiple Availability Zones, enhancing fault tolerance within a region.

**2. Multi-Region Replication:**

Configure asynchronous replication between the Aurora cluster in the primary region and a read replica in a separate region. This provides disaster recovery capabilities.

**3. Amazon Route 53 for Routing:**

* + **Health Checks:** Use Route 53 health checks to monitor the primary and replica regions. If the primary region becomes unavailable, Route 53 can automatically redirect traffic to the replica region.
  + **Latency-Based Routing:** Consider using Route 53's latency-based routing policy to direct traffic to the region with the lowest latency, further optimizing performance.

**4. API Layer Deployment:**

Deploy the REST API across multiple regions, possibly using ***AWS CloudFormation StackSets*** for consistent deployments. This allows for:

* + **In-Region Performance:** Serving users from the closest region improves latency and responsiveness.
  + **Resilience:** If one region experiences an issue, the other region can continue serving traffic.

**5. Automated Failover:**

By combining **Aurora'**s automatic failover capabilities **with Route 53's health checks**, a live **recovery** can be **achieved** with **minimal** data loss. This approach combines the benefits of *Aurora's scalability* and *high availability with Route 53's* routing and failover capabilities to meet the company's requirements.

Q12/218 An organization has a **write-intensive** mobile application that **uses** Amazon API Gateway, AWS Lambda, **and** Amazon DynamoDB. The application has scaled well, however, **costs have increased exponentially** because of higher than anticipated Lambda costs. The application's **use is unpredictable**, but there has been a **steady 20% increase** in utilization every month. **While monitoring** the current Lambda functions, the Solutions Architect notices that the execution-time **averages 4.5 minutes**. Most of the wait time **is** the result **of a** high-latency network call **to a** 3-TB MySQL database server **that is** on-premises. A VPN **is used to connect** to the VPC, so the Lambda functions have been configured with a five-minute timeout.  
How can the Solutions Architect **reduce the cost** of the current architecture?

**A**. **Replace the VPN** with **AWS Direct Connect** to reduce **the network latency** to the **on-premises MySQL** database**. Enable** local caching in **the mobile application** to reduce the Lambda function invocation calls. **Monitor the** Lambda function performance; **gradually adjust** the timeout **and** memory properties **to lower values** while **maintaining** an acceptable execution time. **Offload** the frequently accessed records from DynamoDB **to** Amazon ElastiCache.  
 **B.** Replace the VPN with AWS Direct Connect to reduce the network latency to the on-premises MySQL database. Cache the API Gateway results to Amazon CloudFront. Use Amazon EC2 Reserved Instances instead of Lambda. Enable Auto Scaling on EC2, and use Spot Instances during peak times. Enable DynamoDB Auto Scaling to manage target utilization.  
 **C.** Migrate the MySQL database server into a Multi-AZ Amazon RDS for MySQL. Enable caching of the Amazon API Gateway results in Amazon CloudFront to reduce the number of Lambda function invocations. Monitor the Lambda function performance; gradually adjust the timeout and memory properties to lower values while maintaining an acceptable execution time.  
 Enable DynamoDB Accelerator for frequently accessed records, and enable the DynamoDB Auto Scaling feature.  
 **D**. Migrate the MySQL database server into a Multi-AZ Amazon RDS for MySQL. Enable API caching on API Gateway to reduce the number of Lambda function invocations. Continue to monitor the AWS Lambda function performance; gradually adjust the timeout and memory properties to lower values while maintaining an acceptable execution time. Enable Auto Scaling in DynamoDB.

**Correct Answer:** A

Q13/218 A **financial services company** has a **web application** that serves **users** in the **United States** and **Europe** The **application** consists of a **database** tier and a **web** server tier. The database tier consists of a **MySQL database** hosted in **us-east-1.**  Amazon **Route 53** **geoproximity routing** is used to direct **traffic** to **instances** in the closest Region. A **performance review** of the system reveals that **European users** are not receiving the **same level of** query performance as those in the **United States** Which changes should be **made to the database** tier to **improve** performance?

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

**B.** Migrate the database to Amazon DynamoDB Use DynamoDB global tables to enable replication to additional Regions

**C.** Migrate the database to Amazon RDS for MySQL Configure Multi-AZ in one of the European Regions

**D.** Deploy MySQL instances in each Region Deploy an Application Load Balancer in front of MySQL to reduce the load on the primary instance

Q14/218 A company is hosting its website on Amazon S3 and is using Amazon CloudFront to cache content The company has an upcoming product launch An employee accidentally published marketing content to the website before the official release of the product The company **needs to remove the marketing content from the website** **as quickly as** possible Which solution will meet these requirements?

**A**.**Delete** the marketing content **in the** existing S3 bucket **Invalidate** the **file path** in CloudFront

**B**. Deploy the updated version of the website to another S3 bucket Update the origin for CloudFront

**C**. Create a new CloudFront cache policy with a low TTL Associate the new policy with the existing CloudFront distribution

**D**. Delete the marketing content in the existing S3 bucket Update the S3 bucket policy to block requests to the file path

**Correct Answer:** A

**Your company plans to host a large donation website on Amazon Web Services (AWS). You anticipate a large and undetermined amount of traffic that will create many database writes. To be certain that you do not drop any writes to a database hosted on AWS. Which service should you use?**

**A.** Amazon RDS with provisioned lOPS up to the anticipated peak write throughput.

**B.** Amazon **Simple Queue Service** (SOS) for **capturing** the writes **and** draining the queue **to write** to the database.

**C.** Amazon ElastiCache to store the writes until the writes are committed to the database.

**D.** Amazon DynamoDB with provisioned write throughput up to the anticipated peak write throughput.

**Correct Answer: B**

Q16/218 **Once again your customers are concerned about the security of their sensitive data and with their latest enquiry ask about what happens to old storage devices on AWS. What would be the best answer to this question?**

**A.** AWS reformats the disks and uses them again.

**B.** AWS uses the techniques detailed in **DoD 5220.22-M** to **destroy data** as part of the **decommissioning process.**

**C.** AWS uses their own proprietary software to destroy data as part of the decommissioning process.

**D.** AWS uses a 3rd party security organization to destroy data as part of the decommissioning process.

**Correct Answer: B**

When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals.  
AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process.

Q17/218 **You have a video Trans coding application running on Amazon EC2. Each instance pools a queue to find out which video should be Trans coded, and then runs a Trans coding process.** If this process is interrupted, the video will be Trans coded by another instance based on the queuing system. You have a large backlog of videos which need to be Trans coded and would like to reduce this backlog by adding more instances. You will need these instances only until the backlog is reduced. Which type of Amazon EC2 instance should you use to reduce the backlog in the most cost-effective way?

**A.** Reserved instances

**B.** Dedicated instances

**C.** **Spot** instances

**D.** On-demand instances

Answer **C:**

Q17/218 **A company has a three-tier application image sharing. The application uses an Amazon EC2 instance for the front-end layer, another EC2 instance tor the application layer, and a third EC2 instance for a MySQL database A solutions architect must design a scalable and highly available solution that requires the least amount** of **change to the application. Which solution meets these requirements?**

**A.** Use toad-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end layer and the application layer. Move the database to an Amazon RDS DB instance with multiple read replicas to serve users' images.

**B.** Use Amazon S3 to host the front-end layer. Use a fleet of EC2 instances in an Auto Scaling group for the application layer. Move the database to a memory optimized instance type to store and serve users' images.

**C.** Use Amazon S3 to host the front-end layer. Use AWS Lambda functions for the application layer. Move the database to an Amazon DynamoDB table Use Amazon S3 to store and service users' images.

**D.** Use toad-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end layer and the application layer. Move the database to an Amazon RDS Multi-AZ DB instance Use Amazon S3 to store and serve users' images.

Explanation: **The correct solution is D.** Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end layer and the application layer. Move the database to an Amazon RDS Multi-AZ DB instance. Use Amazon S3 to store and serve users' images. Here's why:

* **Least amount of change to the application:**
  + Elastic Beanstalk: This service abstracts away the underlying EC2 instances, load balancers, and Auto Scaling, making it easy to deploy and manage web applications without significant code changes. It supports various platforms, including those commonly used for front-end and application layers on EC2.
  + Amazon RDS: Moving from an EC2-based MySQL database to Amazon RDS for MySQL requires minimal to no application code changes, as RDS provides a fully managed, compatible MySQL endpoint.
  + Amazon S3: If the application is currently serving images directly from the EC2 instances, migrating image storage to S3 is a common and relatively straightforward change. Applications typically use S3 SDKs or pre-signed URLs to interact with S3, which is a small and localized change compared to re-architecting the entire application logic.
* **Scalable and Highly Available:**
  + Load-balanced Multi-AZ Elastic Beanstalk: This configuration automatically distributes incoming traffic across multiple instances in different Availability Zones (AZs) and scales the number of instances up or down based on demand. This provides both scalability and high availability.
  + Amazon RDS Multi-AZ DB instance: This ensures high availability for the database. In a Multi-AZ deployment, Amazon RDS **automatically provisions** and **maintains** a synchronous standby replica **in a different** Availability Zone**. In case of an outage** in the primary AZ, RDS a**utomatically fails** over to the standby.
  + Amazon S3: S3 is inherently scalable and highly available. It's designed for 99.999999999% (11 nines) durability and 99.99% availability over a given year.

Why other options **are not ideal:**

* **A**. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end layer and the application layer. Move the database to an Amazon RDS DB instance with multiple read replicas to serve users' images.
  + While Elastic Beanstalk and **RDS** are **good choices**, **read replicas** **are for** scaling read operations, **not for** high availability **in case of a** primary database failure. They also **don't replace** the need for **a separate** image storage solution **like** S3 **if images are** currently stored **on** EC2.
* **B.** Use Amazon S3 to host the front-end layer. Use a fleet of EC2 instances in an Auto Scaling group for the application layer. Move the database to a memory optimized instance type to store and serve users' images.
  + Amazon S3 for front-end: While S3 can host static websites, if the front-end is a dynamic application running on EC2, this would require **a significant re-architecture** (e.g., converting it to a Single Page Application).
  + Memory-optimized instance for database and images: This doesn't inherently provide high availability or the scalability needed for images. Storing and serving images directly from a database instance is **generally not** a scalable **or efficient** solution **for a** large number of images; **dedicated** object storage **like** S3 **is preferred**.
* **C**. Use Amazon S3 to host the front-end layer. Use AWS Lambda functions for the application layer. Move the database to an Amazon DynamoDB table. Use Amazon S3 to store and service users' images.
  + This is **a significant re-architecture** to a serverless model. **While** highly scalable **and** available, it would **require** substantial changes **to the** existing application code for **both** the front-end (if dynamic), application layer (moving to Lambda), **and** database (migrating from MySQL to DynamoDB), which goes against the "least amount of change" requirement.

Q19/218 A web company is looking to implement an external payment service into their highly available application deployed in a VPC. Their application EC2 instances are behind a public facing ELB. Auto scaling is used to add additional instances as traffic increases. Under normal load the application runs 2 instances in the Auto Scaling group but at peak it can scale 3x in size. The application instances need to communicate with the payment service over the Internet which requires whitelisting of all public IP addresses used to communicate with it. A maximum of 4 whitelisting IP addresses are allowed at a time and can be added through an API.  
How should they architect their solution?

**A.** Whitelist the VPC Internet Gateway Public IP and route payment requests through the Internet Gateway.

**B.** Whitelist the ELB IP addresses and route payment requests from the Application servers through the ELB.

**C.** Automatically assign public IP addresses to the application instances in the Auto Scaling group and run a script on boot that adds each instances public IP address to the payment validation whitelist API.

**D.** Route payment requests through two NAT instances setup for High Availability and whitelist the Elastic IP addresses attached to the MAT instances.

Explanation (**withou**t giving the 4 options to choose from) To meet the requirements of **external payment service communication** with a **highly available application** in a VPC, given the IP whitelisting constraints, the company should **route outbound traffic from the application instances through a set of fixed, public IP addresses**.

Here's how to architect the solution:

**Solution Architecture**

The most effective way to manage outbound public IP addresses for an auto-scaling group while adhering to a strict whitelisting limit is to use **NAT Gateways**.

1. **Private Subnets for Application EC2 Instances**: Deploy the application EC2 instances in **private subnets** within the VPC. This is a best practice for security as it prevents direct internet access to the instances.
2. **Public Subnets for NAT Gateways**: Create **public subnets** in each Availability Zone (AZ) where the application instances might launch.
3. **NAT Gateways for Outbound Internet Access**:
   * Deploy **one NAT Gateway in each public subnet** of the Availability Zones where your application instances reside. If your application spans two AZs, deploy two NAT Gateways (one in each AZ). If it spans three, deploy three.
   * Associate an **Elastic IP (EIP)** with each NAT Gateway. Elastic IPs are static public IP addresses. Since you're allowed a maximum of 4 whitelisting IP addresses, and your Auto Scaling group can scale up to 6 instances (2 normal \* 3x peak), having 2-4 NAT Gateways (each with a unique EIP) would keep you within the whitelisting limit.
   * Configure the **route tables** for the private subnets to route all internet-bound traffic (0.0.0.0/0) through the NAT Gateway in the same Availability Zone.
4. **Public-facing ELB**: Keep the existing public-facing Elastic Load Balancer (ELB) in public subnets to distribute incoming traffic to the application instances.

**Why This Works**

* **Fixed Outbound IPs**: All instances in the private subnets will route their internet-bound traffic through their respective NAT Gateways. Since each NAT Gateway has a **static Elastic IP**, these are the only public IP addresses that the external payment service will see. This effectively provides a fixed set of public IP addresses for whitelisting, regardless of how many instances are running in the Auto Scaling group.
* **High Availability**: Deploying NAT Gateways across multiple Availability Zones ensures high availability for outbound connectivity. If one AZ experiences an issue, instances in other AZs can continue to communicate.
* **Scalability**: The Auto Scaling group can scale up and down without impacting the whitelisted IP addresses. The NAT Gateways handle the increased outbound traffic from the growing number of instances.
* **Security**: Keeping application instances in private subnets enhances security by preventing direct inbound internet access to them, except via the ELB.
* **Minimal Application Changes**: This solution primarily involves network configuration changes within the VPC and does not require modifications to the application code itself for outbound communication.

**API Whitelisting**

The company will need to whitelist the **Elastic IP addresses associated with each NAT Gateway** with the external payment service via their API. If they deploy 2 NAT Gateways, they will whitelist 2 EIPs. If they deploy 3, they whitelist 3 EIPs. This remains within the maximum of 4 allowed whitelisted IP addresses.

**Considerations**

* **Cost**: NAT Gateways incur costs based on usage (data processed and per-hour charges).
* **Availability Zone Strategy**: Ensure that the NAT Gateways are deployed in all the Availability Zones where the Auto Scaling Group is configured to launch instances.
* **Security Groups and Network ACLs**: Ensure that the security groups on the application EC2 instances allow outbound traffic to the payment service, and that Network Access Control Lists (NACLs) on the subnets also permit this traffic.

Now, asked for an explanation **to choose between the 4 options**, it gives the following Explanation,

The best choice is **D. Route payment requests through two NAT instances setup for High Availability and whitelist the Elastic IP addresses attached to the NAT instances.**

Let's break down why and why the other options aren't suitable:

**Why Option D is the Best Choice**

Option D, which involves using **NAT instances (or preferably, NAT Gateways for a managed service)** with whitelisted Elastic IP addresses, is the most robust and practical solution for this scenario.

**Fixed Public IP Addresses:** NAT instances/Gateways provide **static Elastic IP addresses**. This means that regardless of how many application instances are launched or terminated by the Auto Scaling group, the outbound public IP addresses seen by the external payment service remain constant. This directly addresses the requirement of whitelisting a maximum of 4 IP addresses.

**Scalability:** The application instances can scale up to 3x their normal size (from 2 to 6 instances) without impacting the number of whitelisted IPs. All outbound traffic from these instances will be routed through the NAT instances/Gateways.

**High Availability:** Setting up two NAT instances for High Availability (ideally across different Availability Zones) ensures that if one NAT instance fails, the other can take over, maintaining continuous communication with the payment service. This aligns with the "highly available application" requirement.

**Minimal Application Changes:** This solution primarily involves network configuration (routing traffic through NAT instances/Gateways) and does not require changes to the application code itself for outbound communication.

**Why the Other Options Are Not Suitable:**

**A. Whitelist the VPC Internet Gateway Public IP and route payment requests through the Internet Gateway.**

**Internet Gateways (IGW) do not have public IP addresses that can be whitelisted.** An Internet Gateway is a logical construct that provides a target for routes to the internet from your VPC. It enables communication, but it doesn't have a specific, static public IP address that can be used for whitelisting purposes in the way an EC2 instance or a NAT Gateway does. Therefore, this option is fundamentally flawed.

**B. Whitelist the ELB IP addresses and route payment requests from the Application servers through the ELB.**

**ELBs are for inbound traffic, not outbound.** An Elastic Load Balancer (ELB) distributes incoming application traffic across multiple targets, such as EC2 instances. It is designed to handle **inbound** requests to your application. It does not act as a proxy or gateway for **outbound** requests originating from your application instances. Application servers send outbound requests directly to the internet (if in public subnets) or through a NAT device (if in private subnets). Attempting to route outbound requests *through* an ELB is not a supported or functional architecture.

**ELB IP addresses are dynamic.** Even if it were possible to use an ELB for outbound traffic, the public IP addresses of an ELB are dynamic and can change. This would violate the whitelisting requirement.

**C. Automatically assign public IP addresses to the application instances in the Auto Scaling group and run a script on boot that adds each instance's public IP address to the payment validation whitelist API.**

**Violates IP Whitelisting Limit:** The Auto Scaling group can scale up to 6 instances (2 normal \* 3x peak). Each of these instances would get a unique public IP address. This means at peak, you would be attempting to whitelist 6 different IP addresses, exceeding the "maximum of 4 whitelisting IP addresses" allowed by the payment service API.

**Dynamic and Ephemeral IPs:** The public IP addresses assigned to EC2 instances in an Auto Scaling group are dynamic. When an instance is terminated, its IP is released. When a new instance is launched, it gets a new IP. This would lead to constant additions and removals from the whitelist, potentially causing race conditions, failures, and administrative overhead.

**Security Concerns:** Exposing application instances directly to the internet with public IPs for outbound connectivity can increase the attack surface if not properly secured with strict Security Group rules. Best practice is to place application servers in private subnets.

In summary, **Option D** provides the **necessary combination** of fixed outbound IP addresses, high availability, and scalability, making **it the most suitable** solution for this scenario.

Q 20/218 A company is running a multi-tier web application on AWS. The application runs its database on Amazon Aurora MySQL. The application and database tiers are in the us-easily Region. A database administrator who monitors the Aurora DB cluster finds that an intermittent increase in read traffic is creating high CPU utilization on the read replica. The result is increased read latency for the application. The memory and disk utilization of the DB instance are stable throughout the event of increased latency.  
What should a solutions architect do to improve the read scalability?

A. Reboot the DB cluster

B. Create a cross-Region read replica

C. Configure Aurora Auto Scaling for the read replica

D. Increase the provisioned read IOPS for the DB instance

To improve read scalability for an Amazon Aurora MySQL database experiencing high CPU utilization on read replicas due to intermittent read traffic spikes, a solutions architect should **add more Aurora Replicas to the DB cluster**.

Explanation (W/O 4 options)

Amazon Aurora MySQL is designed with a decoupled storage and compute layer, allowing for highly scalable read operations. Aurora Replicas share the same underlying storage volume as the primary instance, which means all replicas are always up-to-date and ready to serve reads.

* **Aurora Replicas:** Adding more Aurora Replicas distributes the read workload across multiple instances. When read traffic increases, the load is shared among all available read replicas, reducing the CPU utilization on individual replicas and consequently decreasing read latency for the application.
* **CPU Utilization:** The problem explicitly states that high **CPU utilization** on the read replica is causing increased read latency. This indicates that the existing replica(s) are becoming a bottleneck for processing read queries due to computational strain, not I/O or memory issues (as memory and disk utilization are stable).
* **Memory and Disk Utilization Stability:** The fact that memory and disk utilization are stable rules out issues like insufficient memory for caching or I/O bottlenecks to the storage layer. This further supports the conclusion that the bottleneck is CPU-bound read processing.

**Why Other Solutions Are Not Ideal (or Less Direct)**

* **Scaling Up the Existing Read Replica:** While increasing the instance size (scaling up) of the existing read replica could provide more CPU, it's a vertical scaling approach. It might temporarily alleviate the issue for a single replica, but for intermittent and potentially unpredictable spikes, adding more instances (horizontal scaling) offers better long-term scalability and resilience. If the traffic continues to grow, you'll hit the limits of a single larger instance.
* **Implementing Read/Write Splitting at the Application Layer:** While good practice for optimizing database interactions, read/write splitting primarily ensures that read queries go to replicas and write queries go to the primary. It doesn't inherently solve a CPU bottleneck on the *existing* read replica if the volume of read queries is simply too high for its current capacity. You'd still need more read capacity (more replicas or larger replicas) after implementing splitting.
* **Using Amazon ElastiCache:** ElastiCache (Redis or Memcached) is an excellent solution for caching frequently accessed data to reduce database load. However, the problem specifies "intermittent increase in read traffic" causing high CPU on the read replica, with stable memory and disk. If the reads are diverse or not highly repetitive, caching might have limited impact. More importantly, it's a change to the application's data access pattern, whereas adding replicas is a direct scaling solution for the database tier itself, requiring minimal to no application changes.
* **Migrating to a Different Database Engine:** This would be a drastic and complex change. Aurora MySQL is already a highly scalable and performant database. The issue is a capacity problem within the existing architecture, not an inherent limitation of Aurora for this workload.

Therefore, adding more Aurora Replicas is the most direct, effective, and operationally simplest solution to improve read scalability in this scenario.

Explanation (**When 4 options** were given)

The best choice for improving read scalability for an Amazon Aurora MySQL database experiencing high CPU utilization on a read replica due to intermittent read traffic is C. Configure Aurora Auto Scaling for the read replica.

Let's break down why and why the others are not ideal:

Why Option C is the Best Choice

C. **Configure Aurora Auto Scaling for the read replica.**

* Addresses Intermittent Spikes: The problem explicitly states "intermittent increase in read traffic." Aurora Auto Scaling is designed precisely for this scenario. It automatically adds or removes Aurora Replicas based on predefined metrics (like CPU utilization), ensuring that you have enough read capacity when demand is high and scale down to save costs when demand is low.
* Targets the Root Cause (CPU): The problem states "high CPU utilization on the read replica" is causing the latency. Aurora Auto Scaling will add more replicas, distributing the CPU load across multiple instances and alleviating the bottleneck.
* Scalability and Elasticity: Aurora Auto Scaling provides horizontal scalability. Instead of relying on a single, larger replica, it allows for dynamically adding more replicas. This is a more resilient and cost-effective approach for fluctuating workloads.
* Minimal Manual Intervention: Once configured, Auto Scaling handles the scaling operations automatically, reducing the need for manual intervention during traffic spikes.
* Cost-Effective: You only pay for the additional replicas when they are needed. When traffic subsides, Auto Scaling can remove them, optimizing costs.

Why the Other Options **Are Not Suitable**

A. **Reboot the DB cluster**

* Temporary Fix, Not a Scalability Solution: Rebooting the DB cluster (or just the read replica) might temporarily clear any transient issues, but it does not address the underlying problem of insufficient read capacity for intermittent traffic spikes. The high CPU utilization will simply return with the next surge in read traffic. It also introduces downtime or a brief interruption for connections.

B. **Create a cross-Region read replica**

* Wrong Problem Solved: A cross-Region read replica is primarily used for disaster recovery (providing a geographically separate backup) or for serving users in different geographic regions to reduce read latency for them. It does not directly address a CPU bottleneck on a read replica within the same Region due to high read traffic. While it adds a read replica, it's generally more expensive and has higher replication lag than in-Region replicas, making it less suitable for solving an immediate performance bottleneck in the same region.

D. **Increase the provisioned read IOPS for the DB instance**

* Misdiagnosis of the Problem: The problem states that "The memory and disk utilization of the DB instance are stable throughout the event of increased latency." This explicitly rules out an I/O bottleneck. Increasing provisioned IOPS would only help if the database was limited by how quickly it could read or write data to storage. Since CPU utilization is high and I/O is stable, this option would not resolve the issue. Aurora's storage is also shared across instances, and IOPS are typically handled by the distributed storage layer, not directly provisioned per instance in the same way as traditional RDS.

Q 21/218 **A company recently started using Amazon Aurora as the data store for its global ecommerce application. When large reports are run, developers report that the ecommerce application is performing poorly. After reviewing metrics in Amazon CloudWatch, a solutions architect finds that the ReadIOPS and CPU Utilization metrics are spiking when monthly reports run. What is the MOST cost-effective solution?**

A. Migrate the Aurora database to a larger instance class.

B. Migrate the monthly reporting to Amazon Redshift.

C. **Increase the Provisioned IOPS** on the **Aurora instance**.

D. Migrate the monthly reporting to an Aurora Replica.

Q 22/218 **Making your snapshot public shares all snapshot data with everyone. Can the snapshots with AWS Market place product codes be made public?**

A. No

B. Yes

No, **snapshots with AWS Marketplace** product codes **cannot** be made public.

Here's why:

* Licensing and Billing: AWS Marketplace products (including AMIs) often come with specific licensing agreements **and** associated billing models. When you make a snapshot public, you are essentially making the underlying data, which includes the Marketplace product, **available to anyone**. This would circumvent the billing and licensing mechanisms of AWS Marketplace, ***as anyone could then*** launch instances **from your** public snapshot **without going through** the proper subscription **and** payment process.
* Security and Control: AWS maintains strict control over the distribution and usage of Marketplace products to ensure compliance with seller agreements and intellectual property rights. Allowing public snapshots of these products would undermine this control.
* Documentation Confirmation: AWS documentation explicitly states this restriction. For example, when modifying snapshot permissions, you'll find notes indicating that "This is not a valid option for encrypted snapshots or snapshots with AWS Marketplace product codes."

**Instead** of making such snapshots public, **if you** need **to share an AMI** (which is built from a snapshot) that you've purchased from AWS Marketplace **with another** AWS account, you typically **need to**:

1. Share the AMI privately with specific AWS accounts.
2. The target account **must also subscribe** to the same AWS Marketplace product in order **to launch instances** from the shared AMI. This **ensures** that the licensing and billing are correctly applied for **both** the seller **and** AWS

Q23/218 **A solutions architect needs to convert potential single points of failure to a highly-available configuration. The currently architecture contains amazon EC2 instances with databases running in one availability zone. Web-tier resources have not been given public addresses, but still require internet access. Which solution should the architect use to maintain high availability?**

A. Use ELB Classic Load Balancer with the web tier Deploy EC2 instances in two Availability Zones and enable Multi-AZ RDS Deploy a NAT gateway in ~~one~~ Availability Zone

B. Use ELB Classic Load Balancer with the web tier Deploy EC2 instances in two Availability Zones and enable Multi-AZ RDS Deploy NAT gateways in **both** Availability Zones

C. Use ELB Classic Load Balancer with the database tier Deploy Amazon EC2 instances in two Availability Zones and enable Multi-AZ RDS Deploy NAT gateways in both Availability Zones

D. Use ELB Classic Load Balancer with the database tier Deploy Amazon EC2 instances in two Available Zones and enable Multi-AZ RDS Deploy a NAT gateway in one Availability Zone

**Correct Answer: B**

Explanation "**If** you **have** EC2 instances in **multiple** Availability Zones and these **share one** NAT gateway, **in the event of AZ** failure the **NAT g**ateway **becomes unavailable** and the resources **within other** Availability Zones **lose** internet access. To create a fault-tolerant architecture, make sure that your AWS NAT gateways are deployed in **at least two Availability Zones** (AZs)"

Q24/218 **A company hosts its enterprise content management platform in one AWS Region but needs to operate the platform across multiple Regions. The company has an Amazon Elastic Kubernetes Service (Amazon EKS) cluster that runs its microservices in the EKS cluster stores and retrieves objects from Amazon S3. The EKS cluster also stores and retrieves metadata from Amazon DynamoDB. Which combination of steps should a solutions architect take to deploy the platform across multiple Regions?  
(Select TWO.)**

**A.** Replicate the EKS cluster with cross-Region replication.

**B.** Deploy an EKS cluster and an S3 bucket in another Region. Configure cross-Region replication on **both** S3 buckets. **Turn on** global tables for DynamoDB

**C.** Use Amazon API Gateway to create a global endpoint to the EKS cluster

**D.** Use AWS Global Accelerator endpoints to distribute the traffic to multiple Regions

**E.** Use Amazon S3 access points to give access to the objects across multiple Regions Configure DynamoDB Accelerator (DAX) Connect DAX to the relevant tables.

**Correct Answer: ~~B,C~~**

Explanation: The **correct combination of steps** to deploy the platform across multiple Regions is B and D

**B. Deploy an EKS cluster and an S3 bucket in another Region. Configure cross-Region replication on both S3 buckets. Turn on global tables for DynamoDB.**

This option **addresses** the core components of the multi-region deployment **for the** application **and** its data.

* **Deploy an EKS cluster in another Region:** To operate the platform across multiple Regions, you need a replicated compute environment. Deploying another EKS cluster provides the necessary compute capacity for your microservices in the new region.
* **Deploy an S3 bucket in another Region. Configure cross-Region replication on both S3 buckets:** For content management, objects stored in S3 need to be available in both regions. S3 Cross-Region Replication automatically copies objects between buckets in different AWS Regions, ensuring data availability and low-latency access for users in each respective region.
* **Turn on global tables for DynamoDB:** DynamoDB Global Tables provide a fully managed, multi-Region, multi-master database. They enable applications to access data locally in multiple regions, providing fast read and write performance and disaster recovery capabilities.

**D. Use AWS Global Accelerator endpoints to distribute the traffic to multiple Regions.**

* **AWS Global Accelerator** improves the availability and performance of your applications by directing user traffic to the closest healthy endpoint across multiple AWS Regions. **It uses the AWS global network** to route traffic, which can **significantly reduce latency** compared to traditional internet routing. **This is crucial** for distributing user traffic **effectively to** the EKS clusters in different regions.

**Why other options are not suitable:**

* **A. Replicate the EKS cluster with cross-Region replication.**
  + AWS EKS does not have a native "cross-Region replication" feature like S3 or DynamoDB. Replicating an EKS cluster involves deploying a new cluster, configuring networking, and deploying applications and their configurations separately in the target region. You cannot simply "replicate" the cluster in the same way you replicate data.
* **C. Use Amazon API Gateway to create a global endpoint to the EKS cluster.**
  + **While** API Gateway **can** provide global endpoints**, its primary role** is to create, publish, maintain, monitor, **and** secure APIs**. It routes API requests**. **For** distributing *general application traffic* (not just API calls**) to an** EKS cluster across regions **for** performance **and** availability**, AWS Global Accelerator** **is a more direct** and **efficient service** designed **for this purpose**, as it **operates at the** network layer, o**ptimizing** routing.
* **E. Use Amazon S3 access points to give access to the objects across multiple Regions. Configure DynamoDB Accelerator (DAX) Connect DAX to the relevant tables.**
  + **Amazon S3 Access Points** are used to simplify data access for applications and specific users **within a single** AWS account, **but they don't inherently provide** cross-Region replication for high availability across regions. While you can create access points for buckets in different regions, they don't automatically replicate data. S3 Cross-Region Replication is the correct service for data replication.
  + **DynamoDB Accelerator (DAX)** **is an** in-memory cache for DynamoDB that **improves read** performance for ***eventual consistency*** reads **within a single region**. It **does not provide** multi-region replication or global distribution of data. **Global Tables** is the service for **multi-region DynamoDB**.

Q25/218 **A corporate web application is deployed within an Amazon Virtual Private Cloud (VPC) and is connected to the corporate data center via an iPsec VPN. The application must authenticate against the on-premises LDAP server. After authentication, each logged-in user can only access an Amazon Simple Storage Space (S3) keyspace specific to that user.  
Which two approaches can satisfy these objectives? (Choose 2 answers)**

**A.** Develop an identity broker that authenticates against LDAP and then calls IAM Security Token Service to get IAM federated user credentials The application calls the identity broker to get IAM federated user credentials with access to the appropriate S3 bucket.

**B.** The application authenticates against LOAP and retrieves the name of an IAM role associated with the user. The application then cails the IAM Security Token Service to assume that IAM role The application can use the temporary credentials to access the appropriate S3 bucket.

**C.** Develop an identity broker that authenticates against IAM security Token service to assume a IAM role in order to get temporary AWS security credentials The application calls the identity broker to get AWS temporary security credentials with access to the appropriate S3 bucket.

**D.** The application authenticates against LDAP the application then calls the AWS identity and Access Management (IAM) Security service to log in to IAM using the LDAP credentials the application can use the IAM temporary credentials to access the appropriate S3 bucket.

**E.** The application authenticates against IAM Security Token Service using the LDAP credentials the application uses those temporary AWS security credentials to access the appropriate S3 bucket.

**Correct Answer: ~~C,E~~**

Explanation(W/O the options): To satisfy the objectives of authenticating against an on-premises LDAP server and granting user-specific access to Amazon S3 keyspaces, a solutions architect should implement a combination of **identity federation** and **fine-grained S3 access control**.

Here are the approaches:

**1. Authentication against On-Premises LDAP Server**

The primary approach here is to leverage **Identity Federation** using a custom identity broker or AWS Directory Service.

* **AWS Identity and Access Management (IAM) Federation with LDAP (Custom Identity Broker):**
  + The corporate web application, when a user attempts to log in, would first **authenticate the user against the on-premises LDAP server**.
  + Upon successful LDAP authentication, the application's backend (running on EC2 instances within the VPC) **would then** call the AWS Security Token Service (STS) **AssumeRoleWithWebIdentity** or **AssumeRole** API operation.
  + Crucially, the application would **generate temporary AWS security credentials** (access key ID, secret access key, and session token) for the authenticated user. To do this, it needs to map the LDAP user's attributes (e.g., username, groups) to an **IAM Role**.
  + This requires a **custom identity broker** application logic that handles the interaction between LDAP, the web application, and AWS STS.
* **AWS Directory Service (AD Connector or Managed Microsoft AD) (Alternative/Enhancement):**
  + While the existing setup has an IPsec VPN, for a more robust and integrated solution, consider using **AWS Directory Service AD Connector**.
  + **AD Connector** acts as a proxy, redirecting directory requests from AWS services (like IAM Identity Center, formerly AWS SSO) to your on-premises LDAP (Active Directory). This allows your AWS resources and users to authenticate against your on-premises directory without replicating your directory data to the cloud.
  + Once integrated, **AWS IAM Identity Center** can be used to manage access to AWS accounts and applications, federating identities from your on-premises LDAP. This simplifies user access management and provides a unified login experience.

**2. User-Specific S3 Keyspace Access**

After a user is authenticated and temporary AWS credentials are obtained, **fine-grained access control** with **IAM Policies and S3 Bucket Policies** is key to restricting access to user-specific S3 keyspaces.

* **S3 Bucket Structure:**
  + Design your S3 bucket to have a **folder (prefix)** for each user, e.g., s3://your-bucket/users/<username>/.
* **Dynamic IAM Policy Generation (via Assumed Role):**
  + The **IAM Role** assumed by the federated user (or the role granted to the web application itself which then vends temporary credentials) would have an IAM policy that uses **policy variables** to grant access only to the user's specific S3 keyspace.
  + For example, the IAM policy attached to the assumed role could look like this:

JSON

**{**

**"Version": "2012-10-17",**

**"Statement": [**

**{**

**"Effect": "Allow",**

**"Action": [**

**"s3:GetObject",**

**"s3:PutObject",**

**"s3:DeleteObject",**

**"s3:ListBucket"**

**],**

**"Resource": [**

**"arn:aws:s3:::your-bucket/users/${aws:username}/\*",**

**"arn:aws:s3:::your-bucket/users/${aws:username}/"**

**],**

**"Condition": {**

**"StringLike": {**

**"s3:prefix": [**

**"users/${aws:username}/\*"**

**]**

**}**

**}**

**},**

**{**

**"Effect": "Allow",**

**"Action": "s3:ListBucket",**

**"Resource": "arn:aws:s3:::your-bucket",**

**"Condition": {**

**"StringEquals": {**

**"s3:prefix": [**

**"",**

**"users/",**

**"users/${aws:username}/"**

**]**

**}**

**}**

**}**

**]**

**}**

* + In this policy:
    - ${aws:username} is a **policy variable** that resolves to the friendly name **of the current** IAM user, **or** in the case of federated users, the RoleSessionName provided during AssumeRole (which you can set to the LDAP username).
    - This **ensures** that a **user can only** list, get, put, or delete objects **within** their designated folder **(s3://your-bucket/users/<username>/).**
* **S3 Bucket Policy (Optional but Recommended for Defense-in-Depth):**
  + You can add an **S3 Bucket Policy** to the bucket (your-bucket) for an additional layer of security. This policy can **explicitly deny access** to prefixes **not matching t**he RoleSessionName or specific ARN, **ensuring** that **only** correctly authenticated **and** authorized requests can access their specific folders.
  + For example:

JSON

**{**

**"Version": "2012-10-17",**

**"Statement": [**

**{**

**"Effect": "Deny",**

**"Principal": "\*",**

**"Action": "s3:\*",**

**"Resource": "**arn:aws:s3:::your-bucket/users**/\*",**

**"Condition": {**

**"StringNotLike": {**

**"aws:PrincipalArn": "arn:aws:iam::\*:role/YourAssumedRoleName-\*"**

**},**

**"StringNotEquals": {**

**"s3:prefix": [**

**"",**

**"users/",**

**"users/${aws:username}/\*"**

**]**

**}**

**}**

**}**

**]**

**}**

*This example is illustrative and requires careful crafting to ensure it doesn't inadvertently block legitimate access.*

**Architecture Flow**

1. **User Access:** A user accesses the corporate web application deployed in the AWS VPC.
2. **Authentication Request:** The web application sends the user's credentials to the on-premises LDAP server via the existing IPsec VPN tunnel.
3. **LDAP Authentication:** The LDAP server authenticates the user.
4. **Identity Broker/Application Logic:**
   * If authentication is successful, the web application's backend (your custom identity broker) receives confirmation.
   * The identity broker then makes an AWS STS API call (e.g., AssumeRole) to obtain **temporary AWS credentials**. The RoleSessionName in this call should be set to a value derived from the authenticated LDAP username (e.g., ldap-user-<username>).
   * This AssumeRole call targets an IAM Role specifically designed for this application, which has an IAM Policy with the ${aws:username} variable for S3 access.
5. **Temporary Credentials:** AWS STS returns temporary credentials.
6. **S3 Access:** The web application uses these temporary credentials to interact with Amazon S3. Due to the IAM policy attached to the assumed role (and potentially the S3 bucket policy), the credentials will **only allow access to the S3 keyspace corresponding to that specific user's folder**.

**Considerations**

* **VPN Bandwidth and Latency:** An IPsec VPN might introduce **latency** for LDAP authentication. For mission-critical applications or very frequent authentications, consider **AWS Direct Connect** for a dedicated, more consistent, and lower-latency connection to your data center.
* **Security of Temporary Credentials:** Ensure that the web application handles temporary credentials securely, storing them in memory for the duration of the user's session and revoking them (or allowing them to expire) appropriately.
* **Error Handling:** Implement robust error handling for authentication failures and S3 access issues.
* **Audit Logging:** Enable AWS CloudTrail for API activity logging and S3 server access logging to monitor and audit S3 access, providing visibility into who accessed what and when.
* **Scalability of LDAP:** Ensure your on-premises LDAP infrastructure can handle the authentication load from the web application.

Explanation(With the options):

The two approaches that can satisfy these **objectives are A and B.**

Here's why:

**Why Options A and B are Correct.**

Both A and B describe valid approaches to federate on-premises LDAP users with AWS IAM and grant them specific S3 access. They leverage the **core concept of** Identity Federation **and** temporary AWS security credentials **from** AWS Security Token Service (STS).

**A**. **Develop** an identity broker that **authenticates** against LDAP and **then calls** IAM Security Token Service **to get** IAM federated user credentials. The application **calls** the identity broker **to get** IAM federated user credentials **with access** to the appropriate S3 bucket.

* **Authentication Flow: This approach correctly outlines the fundamental flow for federating LDAP users**.
  1. The web application sends user credentials to a custom identity broker.
  2. The identity broker validates these credentials against the on-premises LDAP server.
  3. Upon successful LDAP authentication, the identity broker calls AWS Security Token Service (STS), typically using AssumeRole or AssumeRoleWithWebIdentity (though AssumeRoleWithWebIdentity is usually for external IdPs like Google/Facebook, AssumeRole is used for custom identity brokers mapping to IAM roles).
  4. STS returns temporary AWS security credentials associated with a specific IAM Role.
  5. The identity broker provides these temporary credentials back to the application.
* **S3 Access Control:** The IAM role assumed by the federated user would have an IAM policy that uses policy variables (like ${aws:username} or a custom session tag) to restrict S3 access to s3://your-bucket/users/<username>/\*. This ensures that each user can only access their specific S3 keyspace.
* **Decoupling**: By having a separate identity broker, the web application doesn't directly interact with LDAP or manage IAM complexities, leading to cleaner architecture and improved security.

**B.** The application **authenticates** against LDAP and **retrieves** the name of an IAM role associated **with the** user. The application then calls the IAM Security Token Service **to assume** that IAM role. The application **can use** the temporary credentials **to access** the appropriate S3 bucket.

* **Authentication Flow:** This option is very similar to A but implies that ***the application itself contains*** the logic of the identity broker.
  1. The application directly authenticates against the on-premises LDAP server.
  2. After successful authentication, the application retrieves a specific IAM role ARN that is associated with that authenticated user (this mapping would need to be stored somewhere, e.g., in a local database, or derived from LDAP attributes).
  3. The application then calls AWS STS AssumeRole using the retrieved IAM role ARN.
  4. STS returns temporary credentials for that assumed role.
* **S3 Access Control**: Similar to option A, the IAM role assumed by the user would have an IAM policy with policy variables to grant user-specific access to S3.
* **Viability**: While viable, this approach puts more responsibility on the application directly to handle LDAP interaction, role mapping, and STS calls, which can make the application more complex and potentially less secure if not implemented carefully. However, it still meets the requirements.

Why the Other Options **Are Not Suitable**

**C**. Develop an identity broker that authenticates against IAM security Token service to assume a IAM role in order to get temporary AWS security credentials. The application calls the identity broker to get AWS temporary security credentials with access to the appropriate S3 bucket.

* **Incorrect** Authentication Flow: **This option** describes the identity broker **authenticating** against IAM STS. The *primary authentication* source **is LDAP**, **not IAM STS**. IAM STS **is used after** initial authentication (e.g., against LDAP **or** another identity provider) **to get** temporary AWS credentials. This breaks the specified requirement of authenticating against the "**on-premises LDAP server**."

**D.** The application authenticates against LDAP. The application then calls the AWS Identity and Access Management (IAM) Security service to log in to IAM using the LDAP credentials. The application can use the IAM temporary credentials to access the appropriate S3 bucket.

* Direct LDAP to IAM Login is Not Standard: AWS IAM itself **does not have** a native direct integration or API to "log in to IAM using LDAP credentials" in the way described. You **cannot** simply pass LDAP username/password **directly to an** IAM API call **to get** temporary credentials **for an** IAM user or role. *Federation (via SAML, OIDC, or a custom broker with AssumeRole*) is the standard way to **integrate** external directories.

**E**. The application **authenticates** against **IAM Security Token Service** using the LDAP credentials. The application **uses** those temporary AWS security credentials **to access** the appropriate S3 bucket.

* **Incorrect** Authentication Source: Similar to option C, **this option** implies that **AWS STS** is the *primary authentication* source using LDAP credentials. AWS STS **is for** getting temporary credentials **after** authentication **with a** trusted identity source, **not for** performing the initial authentication against an external directory like LDAP. **You cannot pass raw** LDAP credentials **to** STS to authenticate.

Q 26/218 **Making your snapshot public shares all snapshot data with everyone. Can the snapshots with AWS Marketplace product codes be made public?**

**A.** Yes

**B.** No

**Correct Answer: B**

Q 27/218 **A company hosts its multi-tier, public web application in the AWS Cloud. The web application runs on Amazon EC2 instances and its database runs on Amazon RDS. The company is anticipating a large increase in sales during an upcoming holiday weekend. A solutions architect needs to build a solution to analyze the performance of the web application with a granularity of no more than 2 minutes.  
What should the solutions architect do to meet this requirement?**

**A. Create an AWS Lambda function to fetch EC2 logs from Amazon CloudWatch Logs. Use Amazon CloudWatch metrics to perform further analysis.**

**B. Send EC2 logs to Amazon S3. Use Amazon Redshift to fetch logs from the S3 bucket to process raw data for further analysis with Amazon QuickSight.**

**C. Enable detailed monitoring on all EC2 instances. Use Amazon CloudWatch metrics to perform further analysis.**

**D. Send Amazon CloudWatch logs to Amazon Redshift. Use Amazon QuickSight to perform further analysis.**

**Correct Answer: C** Explanation:

**The core requirement is to analyze the performance of the web application with a granularity of no more than 2 minutes.**

**Let's evaluate each option:**

* **A. Create an AWS Lambda function to fetch EC2 logs from Amazon CloudWatch Logs. Use Amazon CloudWatch metrics to perform further analysis.**
  + **While you *can* create custom metrics from CloudWatch Logs using Metric Filters or Lambda, fetching logs and then creating metrics from them introduces latency. The standard processing time for logs to become available and then converted to metrics might exceed the "no more than 2 minutes" granularity requirement, especially if the Lambda function has to parse and process a large volume of logs. This adds complexity and potential delay.**
* **B. Send EC2 logs to Amazon S3. Use Amazon Redshift to fetch logs from the S3 bucket to process raw data for further analysis with Amazon QuickSight.**
  + **This is a solution for batch analysis and long-term historical data warehousing. Sending logs to S3, then ingesting into Redshift, and finally querying with QuickSight involves significant latency. This approach is not suitable for near real-time analysis with a 2-minute granularity.**
* **C. Enable detailed monitoring on all EC2 instances. Use Amazon CloudWatch metrics to perform further analysis.**
  + **This is the most direct and efficient solution.**
  + **Detailed Monitoring for EC2 instances collects metric data at *1-minute intervals.* This directly meets the requirement of "no more than 2 minutes" granularity.**
  + **Amazon CloudWatch Metrics are inherently designed for performance analysis, visualization, and setting alarms based on these metrics. This is a built-in feature of AWS, requiring minimal operational overhead to configure.**
  + **For performance analysis, metrics (like CPU Utilization, Network I/O, Disk I/O) are typically what you want to monitor in near real-time. Logs are more for debugging and detailed troubleshooting *after* a performance deviation is detected.**
* **D. Send Amazon CloudWatch logs to Amazon Redshift. Use Amazon QuickSight to perform further analysis.**
  + **Similar to option B, this is geared towards historical analysis and business intelligence on log data, not real-time performance monitoring with a 2-minute granularity. The latency involved in moving logs from CloudWatch Logs to Redshift and then visualizing with QuickSight would far exceed the 2-minute requirement.**

**Why Option C is the best:**

* **Directly meets granularity: Detailed monitoring** provides 1-minute resolution, which is **well within** the "no more than 2 minutes**" requirement.**
* **Low Operational Overhead:** It's a simple configuration change within the EC2 console or API/CLI to enable detailed monitoring. CloudWatch automatically collects and stores these metrics.
* **Purpose-built for Performance Analysis:** CloudWatch metrics are designed for this exact purpose, allowing for immediate visualization, alarming, and trend analysis.

**The final answer is C​**

Q 28/218 **A company is running an Apache Hadoop cluster on Amazon EC2 instances. The Hadoop cluster stores approximately 100 TB of data for weekly operational reports and allows occasional access for data scientists to retrieve data. The company needs to reduce the cost and operational complexity for storing and serving this data.  
Which solution meets these requirements in the MOST cost-effective manner?**

**A.** Migrate the data to Amazon DynamoDB and modify the reports to fetch data from DynamoDB. Allow the data scientists to access the data directly in DynamoDB.

**B.** Write a script that resizes the EC2 instances to a smaller instance type during downtime and resizes the instances to a larger instance type before the reports are created.

**C.** Move the Hadoop cluster from EC2 instances to Amazon EMR. Allow data access patterns to remain the same.

**D.** Move the data to Amazon S3 and use Amazon Athena to query the data for reports. Allow the data scientists to access the data directly in Amazon S3.

**Correct Answer: D**

Q 29/218 **A meteorological startup company has a custom web application to sell weather data to its users online. The company uses Amazon DynamoDB to store its data and wants to build a new service that sends an alert to the managers of four internal teams every time a new weather event is recorded. The company does not want this new service to affect the performance of the current application.  
What should a solutions architect do to meet these requirements with the LEAST amount of operational overhead?**

**A.** Have the current application publish a message to four Amazon Simple Notification Service (Amazon SNS) topics. Have each team subscribe to one topic.

**B.** Add a custom attribute to each record to flag new items. Write a cron job that scans the table every minute for items that are new and notifies an Amazon Simple Queue Service (Amazon SQS) queue to which the teams can subscribe.

**C.** Use DynamoDB transactions to write new event data to the table. Configure the transactions to notify internal teams.

**D.** Enable Amazon DynamoDB Streams on the table. Use triggers to write to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe.

**Correct Answer: C**

Q 30/218 **AWS CloudFormation \_\_\_\_\_\_ are special actions** you use in your template **to assign values to** properties **that are not** available **until runtime.**

**A.** intrinsic functions

**B.** properties declarations

**C.** output functions

**D.** conditions declarations

**Correct Answer: A**

AWS **CloudFormation** ***intrinsic functions*** are special actions you use in your template to assign values to properties not available until runtime. Each function is declared with a name enclosed in quotation marks (""), a single colon, and its parameters.  
Reference:  
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/intrinsic-fuctions-structure.html

Q 31/218 **A development team needs to host a website that will be accessed by other teams. The website contents.consist of HTML. CSS, client side JavaScript, and images.  
Which method is the MOST cost-effective for hosting the website?**

**A.** Create an Amazon S3 bucket and host the website there.

**B.** Deploy a web server on an Amazon EC2 instance to host the website.

**C.** Containerize the website and host it in AWS Fargate

**D.** Configure an Application Load Balancer with an AWS Lambda target that uses the Express is framework

**Correct Answer: A**

Q 32/218 **An AWS workload in a VPC is running a legacy database on an Amazon EC2 instance. Data is stored on a  
200GB Amazon EBS (gp2) volume. At peak load times, logs show excessive wait time.  
What solution should be implemented to improve database performance using persistent storage?**

**A**. Change the EC2 instance type to one with burstable performance.

**B**. Migrate the data on the EBS volume to provisioned IOPS SSD (io1).

**C**. Change the EC2 instance type to one with EC2 instance store volumes.

**D**. Migrate the data on the Amazon EBS volume to an SSD-backed volume.

**Correct Answer: B**

Q33/218 **A company runs an application in the AWS Cloud and uses Amazon DynamoDB as the database The company deploys Amazon EC2 instances to a private network to process data from the database The company uses two NAT instances to provide connectivity to DynamoDB.  
The company wants to retire the NAT instances A solutions architect must implement a solution that provides connectivity to DynamoDB and that does not require ongoing management.  
What is the MOST cost-effective solution that meets these requirements?**

**A.** Configure a managed NAT gateway to provide connectivity to DynamoDB

**B.** Deploy an AWS PrivateLink endpoint service between the private network and DynamoDB

**C.** Establish an AWS Direct Connect connection between the private network and DynamoDB

**D.** Create a gateway VPC endpoint to provide connectivity to DynamoDB

**Correct Answer: D**

Q 34/218 **Management has decided to deploy all AWS VPCs with IPv6 enabled After some time a solutions architect tries to launch a new instance and receives an error stating that there is not enough IP address space available in the subnet What should the solutions architect do to fix this?**

**A.** Create a new IPv6-only subnet with a larger range, and then launch the instance

**B.** Disable the IPv4 subnet and migrate all instances to IPv6 only Once that is complete launch the instance

**C.** Create a new IPv4 subnet with a larger range, and then launch the instance

**D.** Check to make sure that only IPv6 was used during the VPC creation.

**Correct Answer: C**

Q 35/218 **A company has multiple AWS accounts, for various departments. One of the departments wants to share an Amazon S3 bucket with all other department.  
Which solution will require the LEAST amount of effort?**

**A.** Enable cross-account S3 replication for the bucket

**B.** Set the S3 bucket policy to allow cross-account access to other departments

**C.** Create a pre signed URL tor the bucket and share it with other departments

**D.** Create IAM users for each of the departments and configure a read-only IAM policy

**Correct Answer: D**

Q36/218 **A solutions architect is designing an architecture that includes web application and database tiers The web tier must be capable of auto scaling. The solutions architect has decided to separate each tier into its own subnets. The design includes two public subnets and four private subnets.  
The security team requires that tiers be able to communicate with each other only when there is a business need and that all other network traffic be blocked What should the solutions architect do to meet these requirements?**

**A.** Create specific security groups for each tier to limit traffic to only the required source and destinations

**B.** Create an Amazon GuardDuty source'destmation rule set to control communication

**C.** Create one security group for all tiers to limit traffic to only the required source and destinations

**D.** Create network ACLs in all six subnets to limit traffic to the sources and destinations required for the application to function

**Correct Answer: D**

Q 37/218 **You are setting up some EBS volumes for a customer who has requested a setup which includes a RAID (redundant array of inexpensive disks). AWS has some recommendations for RAID setups. Which RAID setup is not recommended for Amazon EBS?**

**A.** RAID 1 only

**B.** RAID 5 only

**C.** RAID 5 and RAID 6

**D.** RAID 0 only

**Correct Answer: C**

Q 38/218 **A company uses an Amazon S3 bucket to store static images for its website. The company configured permissions to allow access to Amazon S3 objects by privileged users only. What should a solutions architect do to protect against data loss? (Select TWO.)**

**A.** Enable versioning on the S3 bucket

**B.** Configure an S3 lifecycle rule to transition objects to Amazon S3 Glacier.

**C.** Enable access togging on the S3 bucket.

**D.** Use MFA Delete to require multi-factor authentication to delete an object.

**E.** Enable server-side encryption on the S3 bucket.

**Correct Answer: A,D**

Q 39/218 **Amazon Elastic File System (EFS) provides information about the space used for an object by using the space  
\_ used attribute of the Network File System Version 4.1 (NFSv4.1). The attribute includes the object's current metered data size and not the metadata size. Which of the following utilities will you use to measure the amount of disk that is used of a file?**

**A.** blkid utility

**B.** du utility

**C.** sfdisk utility

**D.** pydf utility

**Correct Answer: B** Amazon EFS reports file system sizes and sizes of objects within a file system. Using the NFSv4.1 space \_ used attribute for measuring the space used for an object, it reports only the object's current metered data size and not the metadata size. There are **two utilities** available for measuring disk usage of a file, the **du** and **stat** utilities.  
https://docs.aws.amazon.com/efs/latest/ug/metered-sizes.html

Q 40/218 **A company has an application with a REST-based Interface that allows data to be received in near-real time from a third-party vendor Once received, the application processes and stores the data for further analysis. The application Is running on Amazon EC2 instances.  
The third-party vendor has received many 503 Service Unavailable Errors when sending data to the application. When the data volume spikes, the compute capacity reaches its maximum limit and the application is unable to process all requests.  
Which design should a solutions architect recommend to provide a more scalable solution?**

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

**B.** Use Amazon Simple Notification Service (Amazon SNS) to ingest the data Put the EC2 instances in an Auto Scaling group behind an Application Load Balancer.

**C.** Repackage the application as a container. Deploy the application using Amazon Elastic Container Service (Amazon ECS) using the EC2 launch type with an Auto Scaling group.

**D.** Use Amazon API Gateway on top of the existing application. Create a usage plan with a quota Iimit for the third-party vendor.

**Correct Answer: A**

Q 41/218 **A company runs a highly available image-processing application on Amazon EC2 instances in a single VPC The EC2 instances run inside several subnets across multiple Availability Zones. The EC2 instances do not communicate with each other However, the EC2 instances download images from Amazon S3 and upload images to Amazon S3 through a single NAT gateway The company is concerned about data transfer charges What is the MOST cost-effective way for the company to avoid Regional data transfer charges?**

**A.** Provision an EC2 Dedicated Host to run the EC2 instances

**B.** Launch the NAT gateway in each Availability Zone

**C.** Replace the NAT gateway with a NAT instance

**D.** Deploy a gateway VPC endpoint for Amazon S3

**Correct Answer: B**

Q  42/218 **A company is moving Its on-premises Oracle database to Amazon Aurora PostgreSQL. The database has several applications that write to the same tables. The applications need to be migrated one by one with a month in between each migration Management has expressed concerns that the database has a high number of reads and writes. The data must be kept in sync across both databases throughout tie migration.  
What should a solutions architect recommend?**

**A.** Use AWS DataSync tor the initial migration. Use AWS Database Migration Service (AWS DMS] to create a change data capture (CDC) replication task and a table mapping to select all cables.

**B.** Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a compute optimized implication instance Create a full load plus change data capture (CDC) replication task and a table mapping to select the largest tables.

**C.** Use the AWS Schema Conversion led with AWS DataBase Migration Service (AWS DMS) using a memory optimized replication instance Create a tui load plus change data capture (CDC) replication task and a table mapping lo select all tables.

**D.** UseAVVS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a full load plus change data capture (CDC) replication task and a table mapping to select ail tables.

**Correct Answer: D**

Q 43/218 **What is the maximum response time for a Business level Premium Support case?**

**A.** You always get instant responses (within a few seconds).

**B.** 1 hour

**C.** 30 minutes

**D.** 10 minutes

**Correct Answer: B**

Q 44/218

**A company is developing an ecommerce application that will consist of a load-balanced front end. a container-based application and a relational database A solutions architect needs to create a highly available solution that operates with as little manual intervention as possible Which solutions meet these requirements? (Select TWO.)**

**A.** Create an Amazon RDS DB instance in Multi-AZ mode

**B.** Create an Amazon RDS DB instance and one or more replicas in another Availability Zone

**C.** Create an Amazon Elastic Container Service (Amazon ECS) cluster with an Amazon EC2 launch type to handle the dynamic application load

**D.** Create an Amazon EC2 instance-based Docker cluster to handle the dynamic application load

**E.** Create an Amazon Elastic Container Service (Amazon ECS) cluster with a Fargate launch type to handle the dynamic application load

**Correct Answer: A,E**

Q 45/218 **Your company runs a customer facing event registration site This site is built with a 3-tier architecture with web and application tier servers and a MySQL database The application requires 6 web tier servers and 6 application tier servers for normal operation, but can run on a minimum of 65% server capacity and a single MySQL database. When deploying this application in a region with three availability zones (AZs) which architecture provides high availability?**

**A.** A web tier deployed across 3 AZs with 2 EC2 (Elastic Compute Cloud) instances in each AZ Inside an Auto Scaling Group behind an ELB (elastic load balancer). And an application tier deployed across 3 AZs with 2 EC2 instances In each AZ inside an Auto Scaling Group behind an ELB. And a Multi-AZ RDS (Relational Database services) deployment.

**B.** d A web tier deployed across 2 AZs with 3 EC2 (Elastic Compute Cloud) instances in each AZ inside an Auto Scaling Group behind an ELB (elastic load balancer) and an application tier deployed across 2 AZs with 3 EC2 instances m each AZ inside an Auto Scaling Group behind an ELS and a Multi-AZ RDS (Relational Database Service) deployment.

**C.** A web tier deployed across 3 AZs with 2 EC2 (Elastic Compute Cloud) instances in each A2 inside an Auto Scaling Group behind an ELB (elastic load balancer) and an application tier deployed across 3 AZs with 2 EC2 instances in each AZ inside an Auto Scaling Group behind an ELB and one RDS (Relational Database Service) Instance deployed with read replicas in the two other AZs.

**D.** A web tier deployed across 2 AZs with 3 EC2 (Elastic Compute Cloud) instances in each AZ inside an Auto Scaling Group behind an ELB (elastic load balancer), and an application tier deployed across 2 AZs with 3 EC2 instances in each AZ inside an Auto Scaling Group behind an ELB. and one RDS (Relational Database Service) instance deployed with read replicas in the other AZ.

**Correct Answer: A**

Q 46/218 **A company wants to migrate a highly transactional database to AWS. Requirements state that the database has more than 6 TB of data and will grow exponentially.  
Which solution should a Solutions Architect recommend?**

**A.** Amazon Aurora

**B.** Amazon Redshift

**C.** Amazon DynamoDB

**D.** Amazon RDS MySQL

**Correct Answer: A**

https://aws.amazon.com/dms/

Q  47/218 **In Amazon Cognito, your mobile app authenticates with the Identity Provider (IdP) using the provider's SDK.  
Once the end user is authenticated with the IdP, the OAuth or OpenID Connect token returned from the IdP is passed by your app to Amazon Cognito, which returns a new \_\_\_\_\_ for the user and a set of temporary, limited-privilege AWS credentials.**

**A.** Cognito Key Pair

**B.** Cognito API

**C.** Cognito ID

**D.** Cognito SDK

**Correct Answer: C**

Your mobile app authenticates with the identity provider (IdP) using the provider's SDK. Once the end user is authenticated with the IdP, the OAuth or OpenID Connect token returned from the IdP is passed by your app to Amazon Cognito, which returns a new Cognito ID for the user and a set of temporary, limited- privilege AWS credentials.  
Reference:  
http://aws.amazon.com/cognito/faqs/

Q 48/218 **An insurance company stores all documents related to annual policies for the duration of the policies. The documents are created once and then stored until they are required typically at Ute end of the policy. A document must be capable of being retrieved immediately. The company is now moving their document management to the AWS Cloud.  
Which service should a Solutions Architect recommend as a cost-effective solution that meets the company's requirements?**

**A.** Amazon RDS MySQL

**B.** Amazon S3 Standard

**C.** Amazon Glacier

**D.** Amazon S3 Standard-infrequent Access

**Correct Answer: D**

Q  49/218

**A company needs to use its on-premises LDAP directory service to authenticate its users to the AWS Management Console. The directory service is not compatible with Security Assertion Markup Language (SAML) Which solution meets these requirements?**

**A.** Create an 1AM policy mat uses AWS credentials and integrate the policy into LDAP

**B.** Set up a process that rotates the IAM credentials whenever LDAP credentials are updated.

**C.** Develop an on-premises custom identity broker application of process mat uses AWS Security Token Service (AWS STS) to get short-lived credentials

**D.** Enable AWS Single Sign-On between AWS and the on-premises LDAP

**Correct Answer: D**

Q  50/218 **Can the string value of 'Key' be prefixed with laws?**

**A.** No

**B.** Yes

**C.** Only for EC2 not S3

**D.** Only for S3 not EC

**Correct Answer: A**

Q 51/218

**What is the type of monitoring data (for Amazon EBS volumes) which is available automatically in 5-minute periods at no charge called?**

**A.** Primary

**B.** Basic

**C.** Detailed

**D.** Local

**Correct Answer: B**

Q 52/218

**Amazon S3 doesn't automatically give a user who creates \_\_\_\_\_ permission to perform other actions on that bucket or object.**

**A.** a object or file

**B.** a bucket or object

**C.** a file

**D.** a bucket or file

**Correct Answer: B**

Q 53/218

**Can you move a Reserved Instance from one Availability Zone to another?**

**A.** Yes, but each Reserved Instance is associated with a specific Region that cannot be changed.

**B.** Yes, only in US-West-2.

**C.** Yes, only in US-East-1.

**D.** No

**Correct Answer: A**

Each Reserved Instance is associated with a specific Region, which is fixed for the lifetime of the reservation and cannot be changed. Each reservation can, however, be used in any of the available AZs within the associated Region.  
Reference: https://aws.amazon.com/rds/faqs/

Q 54/218 **An organization is setting a website on the AWS VPC. The organization has blocked a few IPs to avoid a D-DOS attack.  
How can the organization configure that a request from the above mentioned IPs does not access the application instances?**

**A.** Create an IAM policy for VPC which has a condition to disallow traffic from that IP address.

**B.** Configure a security group at the subnet level which denies traffic from the selected IP.

**C.** Configure the security group with the EC2 instance which denies access from that IP address.

**D.** Configure an ACL at the subnet which denies the traffic from that IP address.

**Correct Answer: D**

Explanation/Reference:   
A Virtual Private Cloud (VPC) is a virtual network dedicated to the user's AWS account. It enables the user to launch AWS resources into a virtual network that the user has defined. AWS provides two features that the user can use to increase security in VPC: security groups and network ACLs. Security group works at the instance level while ACL works at the subnet level. ACL allows both allow and deny rules. Thus, when the user wants to reject traffic from the selected IPs it is recommended to use ACL with subnets.  
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\_ACLs.html

Q 55/218 **A company operates a website on Amazon EC2 Linux instances. Some of the instances are faring Troubleshooting points to insufficient swap space on the failed instances. The operations team lead needs a solution to monitor this.  
What should a solutions architect recommend?**

**A.** Configure an Amazon CloudWatch SwapUsage metric dimension. Monitor the SwapUsage dimension in the EC2 metrics in CloudWatch.

**B.** Use EC2 metadata to collect information, then publish it to Amazon CloudWatch custom metrics.  
Monitor SwapUsage metrics in CloudWatch.

**C.** Install an Amazon CloudWatch agent on the instances. Run an appropriate script on a set schedule.  
Monitor SwapUtilizalion metrics in CloudWatch.

**D.** Enable detailed monitoring in the EC2 console. Create an Amazon CloudWatch SwapUtilizalion custom metric. Monitor SwapUtilization metrics in CloudWatch.

**Correct Answer: A**

Q  56/218 **A solutions architect is designing the cloud architecture for a company that needs to host hundreds of machine learning models for its users Dunng startup, the models need to load up to 10 GB of data from Amazon S3 into memory, out they do not need disk access Most of the models are used sporadically but the users expect all of them to be highly available and accessible with low latency.  
Which solution meets the requirements and is MOST cost-effective1?**

**A.** Deploy models as Amazon Elastic Container Service (Amazon ECS) services behind a single Application Load Balancer with path-based routing where one path corresponds to each model

**B.** Deploy models as Amazon Elastic Container Service (Amazon ECS) services behind an Application Load Balancer for each model

**C.** Deploy models as AWS Lambda functions behind an Amazon API Gateway for each model

**D.** Deploy models as AWS Lambda functions behind a single Amazon API Gateway with path-based routing where one path corresponds to each model

**Correct Answer: A**

Q 57/218 **A solutions architect is designing a security solution for a company that wants to provide developers with individual AWS accounts through AWS Organizations, while also maintaining standard security controls.  
Because the individual developers will have AWS account root user-level access to their own accounts, the solutions architect wants to ensure that the mandatory AWS CloudTrail configuration that is applied to new developer accounts is not modified.  
Which action meets these requirements?**

**A.** Create an IAM policy that prohibits changes to CloudTrail, and attach it to the root user.

**B.** Create a new trail in CloudTrail from within the developer accounts with the organization trails option enabled.

**C.** Create a service control policy (SCP) the prohibits changes to CloudTrail, and attach it the developer accounts.

**D.** Create a service-linked role for CloudTrail with a policy condition that allows changes only from an Amazon Resource Name (ARN) in the master account.

**Correct Answer: C**

Explanation/Reference: https://docs.aws.amazon.com/organizations/latest/userguide/ orgs\_manage\_policies\_scps\_examples.html

Q 58/218 **A company's service for video game recommendations has just gone viral. The company has new users from all over the world. The website for the service is hosted on a set of Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). The website consists of static content with different resources being loaded depending on the device type.  
Users recently reported that the load time for the website has increased. Administrators are reporting high loads on the EC2 instances that host the service.  
Which set actions should a solutions architect take to improve response times?**

**A.** Move content to Amazon S3. Create an Amazon CloudFront distribution to serve content out of the S3 bucket. Use Lambda@Edge to load different resources based on the User-Agent HTTP header.

**B.** Move content to Amazon S3. Create an Amazon CloudFront distribution to serve content out of the S3 bucket. Use the User-Agent HTTP header to load different content.

**C.** Create separate Auto Scaling groups based on device types. Switch to Network Load Balancer (NLB).  
Use the User-Agent HTTP header in the NLB to route to a different set of EC2 instances.

**D.** Create a separate ALB for each device type. Create one Auto Scaling group behind each ALB. Use Amazon Route 53 to route to different ALBs depending on the User-Agent HTTP header.

**Correct Answer: C**

Q 59/218 **A company has thousands of edge devices that collectively generate 1 TB of status alerts each day Each alert is approximately 2 KB in size A solutions architect needs to implement a solution to ingest and store the alerts for future analysis.  
The company wants a highly available solution However the company needs to minimize costs and does not want to manage additional infrastructure Additionally, the company wants to keep 14 days of data available for immediate analysis and archive any data older than 14 days What is the MOST operationally efficient solution that meets these requirements?**

**A.** Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon Elasticsearch Service (Amazon ES) cluster Set up the Amazon ES cluster to take manual snapshots every day and delete data from the cluster that is older than  
14 days

**B.** Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon S3 bucket Set up an S3 LifecycJe configuration to transition data to Amazon S3 Glacier after 14 days

**C.** Launch Amazon EC2 instances across two Availability Zones and place them behind an Elastic Load Balancer to ingest the alerts Create a script on the EC2 instances that will store the alerts in an Amazon S3 bucket Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days

**D.** Create an Amazon Simple Queue Service (Amazon SQS) standard queue to ingest the alerts and set the message retention penod to 14 days Configure consumers to poll the SQS queue check the age of the message and analyze the message data as needed if the message is 14 days old, the consumer should copy the message to an Amazon S3 bucket and delete the message from the SQS queue

**Correct Answer: D**

Q 60/218 **Do the system resources on the Micro instance meet the recommended configuration for Oracle?**

**A.** Yes completely

**B.** Yes but only for certain situations

**C.** Not in any circumstance

**Correct Answer: B**

Q  61/218 **Company is designing a website that uses an Amazon S3 bucket to store static images. The company wants ail future requests have taster response times while reducing both latency and cost.  
Which service configuration should a solutions architect recommend?**

**A.** Deploy a NAT server in front of Amazon S3.

**B.** Deploy a Network Load Balancer in front of Amazon S3.

**C.** Configure Auto Scaling to automatically adjust the capacity of the website.

**D.** Deploy Amazon CloudFront in front of Amazon S3.

**Correct Answer: D**

Q 62/218 **A company wants to use a custom distributed application that calculates various profit and loss scenarios To achieve this goal, the company needs to provide a network connection between its Amazon EC2 instances.  
The connection must minimize latency and must maximize throughput  
Which solution will meet these requirements?**

**A.** Provision the application to use EC2 Dedicated Hosts of the same instance type.

**B.** Configure AWS PrivateLink for the EC2 instances

**C.** Configure a placement group for EC2 instances that have the same instance type

**D.** Use multiple AWS elastic network interfaces and link aggregation

**Correct Answer: A**

Q  63/218 **Which EC2 functionality allows the user to place the Cluster Compute instances in clusters?**

**A.** Cluster group

**B.** Cluster security group

**C.** GPU units

**D.** Cluster placement group

**Correct Answer: D**

The Amazon EC2 cluster placement group functionality allows users to group cluster compute instances in clusters.  
Reference https://aws.amazon.com/ec2/faqs/

Q 64/218 **True or False: When you perform a restore operation to a point in time or from a DB Snapshot, a new DB Instance is created with a new endpoint.**

**A.** FALSE

**B.** TRUE

**Correct Answer: B**

Q 65/218 **A company runs an IoT platform on AWS. IoT sensors in various locations send data to the company's Node.js API servers on Amazon EC2 instances running behind an Application Load Balancer. The data is stored in an Amazon RDS MySQL DB instance that uses a 4 TB General Purpose SSD volume.  
The number of sensors the company has deployed in the field has increased over time, and is expected to grow significantly. The API servers are consistently overloaded and RDS metrics show high write latency.  
Which of the following steps together will resolve the issues permanently and enable growth as new sensors are provisioned, while keeping this platform cost-efficient? (Choose two.)**

**A.** Re-architect the database tier to use Amazon Aurora instead of an RDS MySQL DB instance and add read replicas

**B.** Leverage Amazon Kinesis Data Streams and AWS Lambda to ingest and process the raw data

**C.** Re-architect the database tier to use Amazon DynamoDB instead of an RDS MySQL DB instance

**D.** Resize the MySQL General Purpose SSD storage to 6 TB to improve the volume's IOPS

**E.** Use AWS-X-Ray to analyze and debug application issues and add more API servers to match the load

**Correct Answer: B,C**

Q 66/218 **A company runs a public three-Tier web application in a VPC The application runs on Amazon EC2 instances across multiple Availability Zones. The EC2 instances that run in private subnets need to communicate with a license server over the internet The company needs a managed solution that minimizes operational maintenance Which solution meets these requirements''**

**A.** Provision a NAT instance in a public subnet Modify each private subnets route table with a default route that points to the NAT instance

**B.** Provision a NAT instance in a private subnet Modify each private subnet's route table with a default route that points to the NAT instance

**C.** Provision a NAT gateway in a private subnet Modify each private subnet's route table with a default route that points to the NAT gateway .

**D.** Provision a NAT gateway in a public subnet Modify each private subnet's route table with a default route that points to the NAT gateway

**Correct Answer: D**

Q  67/218

**A company has an API-based inventory reporting application running on Amazon EC2 instances The application stores information in an Amazon DynamoDB table The company's distribution centers have an on-premises shipping application that calls an API to update the inventory before printing shipping labels The company has been experiencing application interruptions several times each day, resulting in lost transactions What should a solutions architect recommend to improve application resiliency?**

**A.** Modify the shipping application to write to a local database

**B.** Modify the application APIs to run serverless using AWS Lambda

**C.** Modify the application to send inventory updates using Amazon Simple Queue Service (Amazon SQS)

**D.** Configure Amazon API Gateway to call the EC2 inventory application APIs.

**Correct Answer: A**