AWS Solution Architect

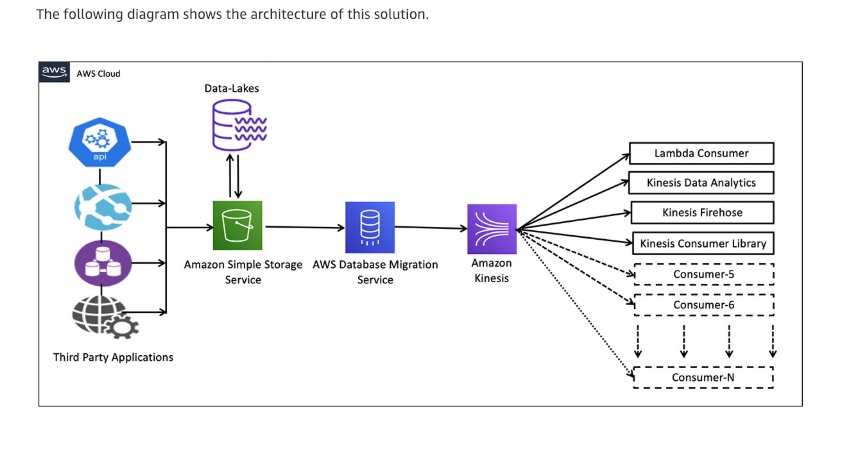
**1->A Big Data Analytics Company writes data and log files in Amazon S3 buckets. The company now wants to stream the existing data files as well as any ongoing file updates from Amazon S3 to Amazon Kinesis Data Streams.**

**As a Solutions Architect, which of the following would you suggest as the fastest possible way of building a solution for this requirement?**

Correct option:

**Leverage AWS Database Migration Service (AWS DMS) as a bridge between Amazon S3 and Amazon Kinesis Data Streams** - You can achieve this by using AWS Database Migration Service (AWS DMS). AWS DMS enables you to seamlessly migrate data from supported sources to relational databases, data warehouses, streaming platforms, and other data stores in AWS cloud.

AWS DMS supports specifying Amazon S3 as the source and streaming services like Kinesis and Amazon Managed Streaming of Kafka (Amazon MSK) as the target.



**2->Your Company runs a website for evaluating coding skills. As a Solutions Architect, you've designed the architecture of the website to follow a server less pattern on the AWS Cloud using API Gateway and AWS Lambda. The backend is using an RDS PostgreSQL database. Caching is implemented using a Redis ElastiCache cluster. You would like to increase the security of your authentication to Redis from the Lambda function, leveraging a username and password combination.**

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

Correct option:

**Use Redis Auth** - Amazon ElastiCache for Redis is a blazing fast in-memory data store that provides sub-millisecond latency to power internet-scale real-time applications

ElastiCache for Redis supports replication, high availability, and cluster sharding right out of the box. IAM Auth is not supported by ElastiCache.

**3->An IT Company has built a custom data warehousing solution for a retail organization by using Amazon Redshift. As part of the cost optimizations, the company wants to move any historical data (any data older than a year) into S3, as the daily analytical reports consume data for just the last one year. However the analysts want to retain the ability to cross-reference this historical data along with the daily reports.**

**The company wants to develop a solution with the LEAST amount of effort and MINIMUM cost. As a solutions architect, which option would you recommend to facilitate this use-case?**

Correct option:

**Use Redshift Spectrum to create Redshift cluster tables pointing to the underlying historical data in S3. The analytics team can then query this historical data to cross-reference with the daily reports from Redshift**

Using Amazon Redshift Spectrum, you can efficiently query and retrieve structured and semi structured data from files in Amazon S3 without having to load the data into Amazon Redshift tables.

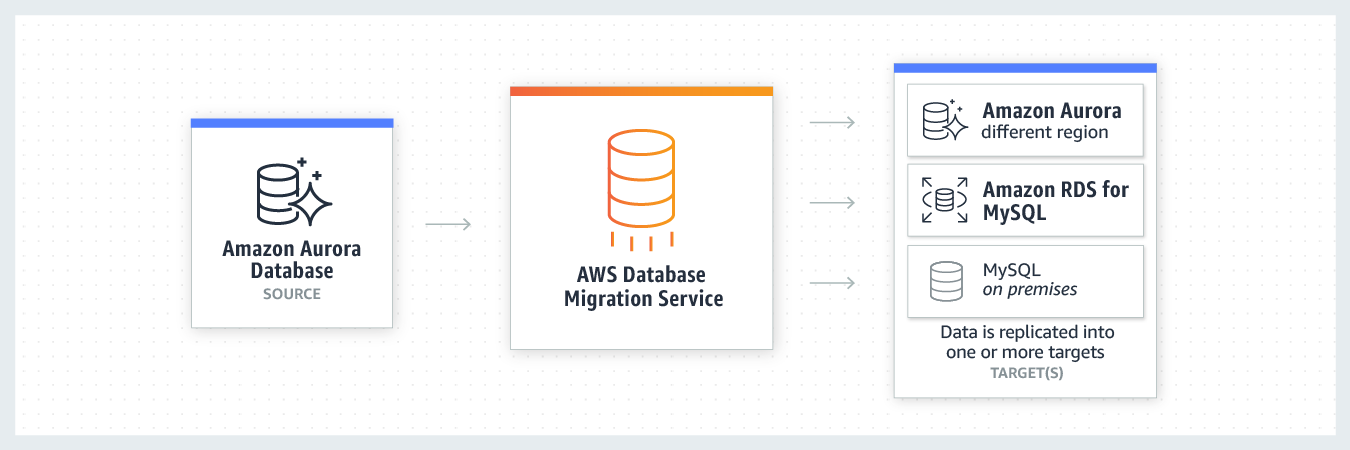
**4->the business analytics team at a company has been running ad-hoc queries on Oracle and PostgreSQL services on Amazon RDS to prepare daily reports for senior management. To facilitate the business analytics reporting, the engineering team now wants to continuously replicate this data and consolidate these databases into a petabyte-scale data warehouse by streaming data to Amazon Redshift.**

**As a solutions architect, which of the following would you recommend as the MOST resource-efficient solution that requires the LEAST amount of development time without the need to manage the underlying infrastructure?**

Correct option:

**Use AWS Database Migration Service to replicate the data from the databases into Amazon Redshift**

AWS Database Migration Service helps you migrate databases to AWS quickly and securely. The source database remains fully operational during the migration, minimizing downtime to applications that rely on the database. With AWS Database Migration Service, you can continuously replicate your data with high availability and consolidate databases into a petabyte-scale data warehouse by streaming data to Amazon Redshift and Amazon S3.



**5-> a retail company uses AWS Cloud to manage its IT infrastructure. The company has set up "AWS Organizations" to manage several departments running their AWS accounts and using resources such as EC2 instances and RDS databases. The company wants to provide shared and centrally-managed VPCs to all departments using applications that need a high degree of interconnectivity.**

**As a solutions architect, which of the following options would you choose to facilitate this use-case?**

Correct option:

**Use VPC sharing to share one or more subnets with other AWS accounts belonging to the same parent organization from AWS Organizations**

VPC sharing (part of Resource Access Manager) allows multiple AWS accounts to create their application resources such as EC2 instances, RDS databases, Redshift clusters, and Lambda functions, into shared and centrally-managed Amazon Virtual Private Clouds (VPCs). To set this up, the account that owns the VPC (owner) shares one or more subnets with other accounts (participants) that belong to the same organization from AWS Organizations

**6-> a start-up’s cloud infrastructure consists of a few Amazon EC2 instances, Amazon RDS instances and Amazon S3 storage. A year into their business operations, the start-up is incurring costs that seem too high for their business requirements.**

**Which of the following options represents a valid cost-optimization solution?**

Correct option:

**Use AWS Cost Explorer Resource Optimization to get a report of EC2 instances that are either idle or have low utilization and use AWS Compute Optimizer to look at instance type recommendations** - AWS Cost Explorer helps you identify under-utilized EC2 instances that may be downsized on an instance by instance basis within the same instance family, and also understand the potential impact on your AWS bill by taking into account your Reserved Instances and Savings Plans.

AWS Compute Optimizer recommends optimal AWS Compute resources for your workloads to reduce costs and improve performance by using machine learning to analyze historical utilization metrics. Compute Optimizer helps you choose the optimal Amazon EC2 instance types, including those that are part of an Amazon EC2 Auto Scaling group, based on your utilization data.

**7-> The DevOps team at an IT company is provisioning a two-tier application in a VPC with a public subnet and a private subnet. The team wants to use either a NAT instance or a NAT gateway in the public subnet to enable instances in the private subnet to initiate outbound IPv4 traffic to the internet but needs some technical assistance in terms of the configuration options available for the NAT instance and the NAT gateway.**

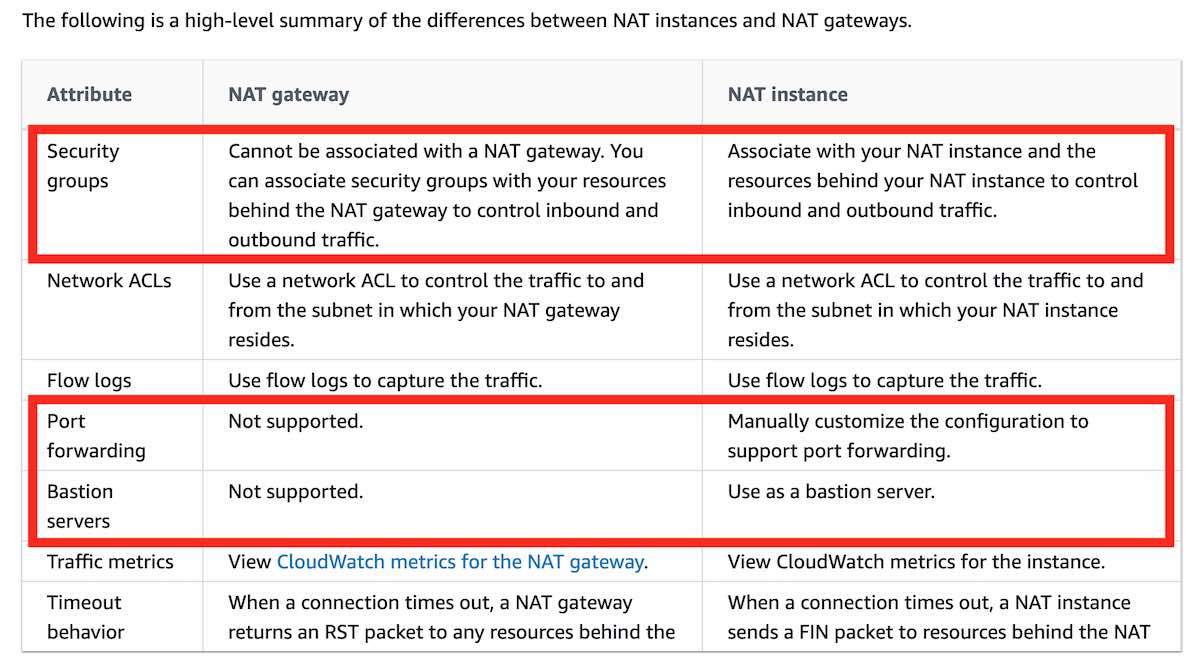
**As a solutions architect, which of the following options would you identify as CORRECT? (Select three)**

Correct options:

NAT instance can be used as a bastion server

Security Groups can be associated with a NAT instance

NAT instance supports port forwarding



**Note-**

**Cluster placement group** - A cluster placement group is a logical grouping of instances within a single Availability Zone. A cluster placement group can span peered VPCs in the same Region. Instances in the same cluster placement group enjoy a higher per-flow throughput limit of up to 10 Gbps for TCP/IP traffic and are placed in the same high-bisection bandwidth segment of the network.

**8-A big data analytics company is using Kinesis Data Streams (KDS) to process IoT data from the field devices of an agricultural sciences company. Multiple consumer applications are using the incoming data streams and the engineers have noticed a performance lag for the data delivery speed between producers and consumers of the data streams.**

**As a solutions architect, which of the following would you recommend for improving the performance for the given use-case?**

Correct option:

**Use Enhanced Fan-out feature of Kinesis Data Streams**

Amazon Kinesis Data Streams (KDS) is a massively scalable and durable real-time data streaming service. KDS can continuously capture gigabytes of data per second from hundreds of thousands of sources such as website clickstreams, database event streams, financial transactions, social media feeds, IT logs, and location-tracking events.

By default, the 2MB/second/shard output is shared between all of the applications consuming data from the stream. You should use enhanced fan-out if you have multiple consumers retrieving data from a stream in parallel. With enhanced fan-out developers can register stream consumers to use enhanced fan-out and receive their own 2MB/second pipe of read throughput per shard, and this throughput automatically scales with the number of shards in a stream.

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

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

Correct option:

**Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days** - S3 One Zone-IA is for data that is accessed less frequently, but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ and costs 20% less than S3 Standard-IA. S3 One Zone-IA is ideal for customers who want a lower-cost option for infrequently accessed and re-creatable data but do not require the availability and resilience of S3 Standard or S3 Standard-IA. The minimum storage duration is 30 days before you can transition objects from S3 Standard to S3 One Zone-IA.

**10-A multi-national retail company has multiple business divisions, with each division having its own AWS account. The engineering team at the company would like to debug and trace data across these AWS accounts and visualize it in a centralized account.**

**As a Solutions Architect, which of the following solutions would you suggest for the given use-case?**

**X-Ray**

AWS X-Ray helps developers analyse and debug production, distributed applications, such as those built using a micro services architecture. With X-Ray, you can understand how your application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors. X-Ray provides an end-to-end view of requests as they travel through your application, and shows a map of your application’s underlying components.

**11- A leading online gaming company is migrating its flagship application to AWS Cloud for delivering its online games to users across the world. The company would like to use a Network Load Balancer (NLB) to handle millions of requests per second. The engineering team has provisioned multiple instances in a public subnet and specified these instance IDs as the targets for the NLB.**

**As a solutions architect, can you help the engineering team understand the correct routing mechanism for these target instances?**

Correct option:

**Traffic is routed to instances using the primary private IP address specified in the primary network interface for the instance**

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

Request Routing and IP Addresses -

If you specify targets using an instance ID, traffic is routed to instances using the primary private IP address specified in the primary network interface for the instance. The load balancer rewrites the destination IP address from the data packet before forwarding it to the target instance.

If you specify targets using IP addresses, you can route traffic to an instance using any private IP address from one or more network interfaces. This enables multiple applications on an instance to use the same port. Note that each network interface can have its security group. The load balancer rewrites the destination IP address before forwarding it to the target.

**12 - A company has moved its business critical data to Amazon EFS file system which will be accessed by multiple EC2 instances.**

**As an AWS Certified Solutions Architect Associate, which of the following would you recommend to exercise access control such that only the permitted EC2 instances can read from the EFS file system? (Select three)**

Correct options:

**Use VPC security groups to control the network traffic to and from your file system**

**Attach an IAM policy to your file system to control clients who can mount your file system with the required permissions**

**Use EFS Access Points to manage application access**

You control which EC2 instances can access your EFS file system by using VPC security group rules and AWS Identity and Access Management (IAM) policies. Use VPC security groups to control the network traffic to and from your file system. Attach an IAM policy to your file system to control which clients can mount your file system and with what permissions, and use EFS Access Points to manage application access. Control access to files and directories with POSIX-compliant user and group-level permissions.

Files and directories in an Amazon EFS file system support standard Unix-style read, write, and execute permissions based on the user ID and group IDs. When an NFS client mounts an EFS file system without using an access point, the user ID and group ID provided by the client is trusted. You can use EFS access points to override user ID and group IDs used by the NFS client. When users attempt to access files and directories, Amazon EFS checks their user IDs and group IDs to verify that each user has permission to access the objects

**13 - A leading social media analytics company is contemplating moving its dockerized application stack into AWS Cloud. The company is not sure about the pricing for using Elastic Container Service (ECS) with the EC2 launch type compared to the Elastic Container Service (ECS) with the Fargate launch type.**

**Which of the following is correct regarding the pricing for these two services?**

Correct option:

**ECS with EC2 launch type is charged based on EC2 instances and EBS volumes used. ECS with Fargate launch type is charged based on vCPU and memory resources that the containerized application requests**

**14 - A company runs its EC2 servers behind an Application Load Balancer along with an Auto Scaling group. The engineers at the company want to be able to install proprietary tools on each instance and perform a pre-activation status check of these tools whenever an instance is provisioned because of a scale-out event from an auto-scaling policy.**

**Which of the following options can be used to enable this custom action?**

Correct option:

**Use the Auto Scaling group lifecycle hook to put the instance in a wait state and launch a custom script that installs the proprietary forensic tools and performs a pre-activation status check**

An Auto Scaling group contains a collection of Amazon EC2 instances that are treated as a logical grouping for automatic scaling and management.

Auto scaling group lifecycle hooks enable you to perform custom actions as the Auto Scaling group launches or terminates instances. Lifecycle hooks enable you to perform custom actions by pausing instances as an Auto Scaling group launches or terminates them. When an instance is paused, it remains in a wait state either until you complete the lifecycle action using the complete-lifecycle-action command or the CompleteLifecycleAction operation, or until the timeout period ends (one hour by default). For example, you could install or configure software on newly launched instances, or download log files from an instance before it terminates.

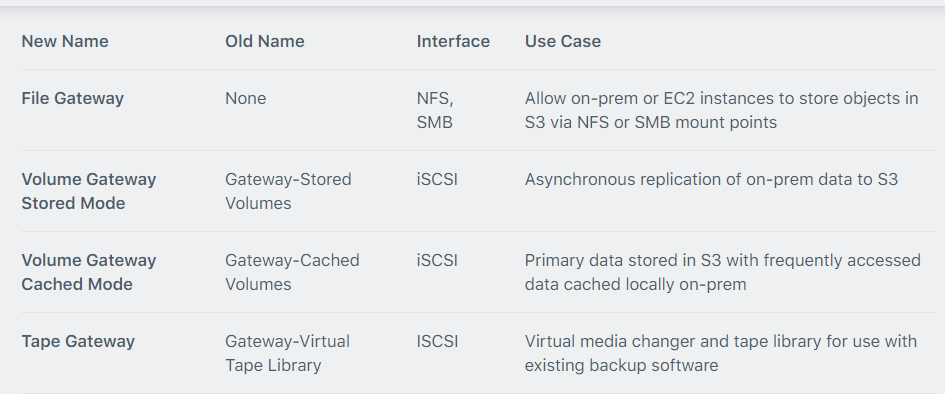
**15 - A company runs an application in a factory that has a small rack of physical compute resources. The application stores data on a network attached storage (NAS) device using the NFS protocol. The company requires a daily offsite backup of the application data.**

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

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

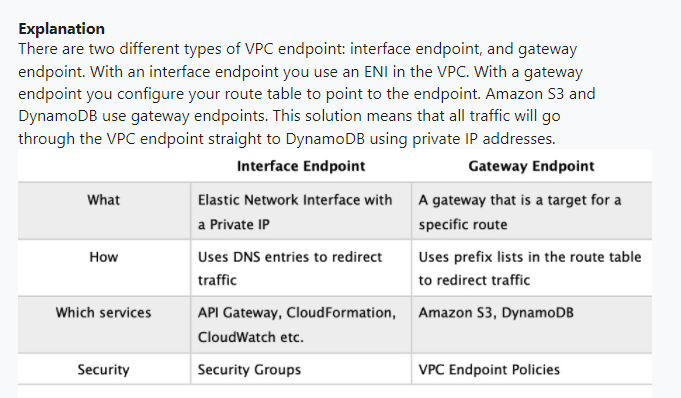
A file gateway is the correct type of appliance to use for this use case as it is suitable for mounting via the NFS and SMB protocols.

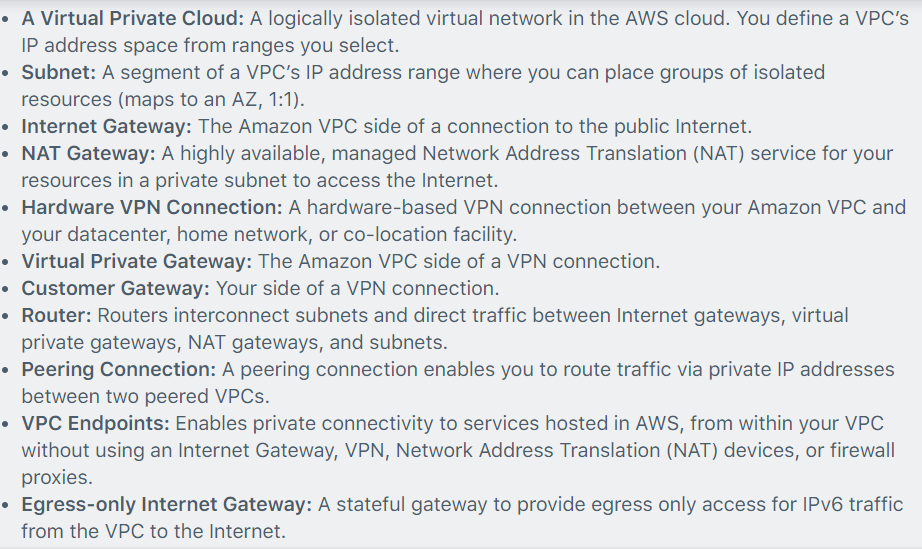
**CORRECT:**"Use an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3" is the correct answer.



**16 -> A company wishes to restrict access to their Amazon Dynamo DB table to specific, private source IP addresses from their VPC. What should be done to secure access to the table?**

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

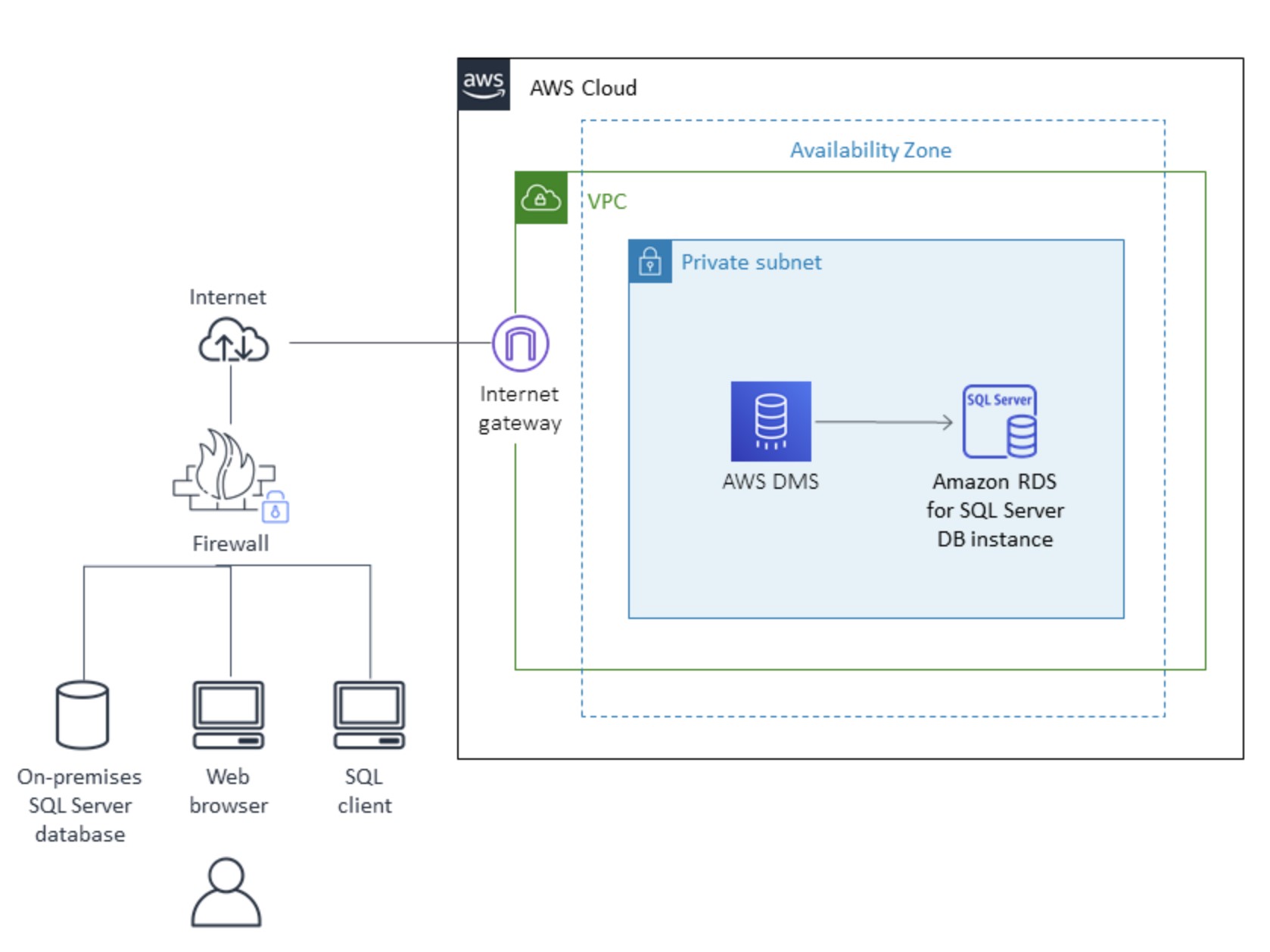




**17-> the database tier of a web application is running on a Windows server on-premises. The database is a Microsoft SQL Server database. The application owner would like to migrate the database to an Amazon RDS instance.**

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

**CORRECT:**"Use the AWS Database Migration Service (DMS) to directly migrate the database to RDS" is the correct answer.

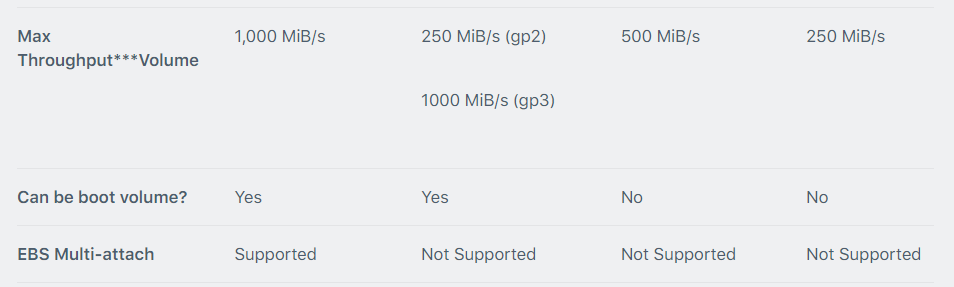


**18-> A persistent database must be migrated from an on-premises server to an Amazon EC2 instances. The database requires 64,000 IOPS and, if possible, should be stored on a single Amazon EBS volume.**

**Which solution should a Solutions Architect recommend?**

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





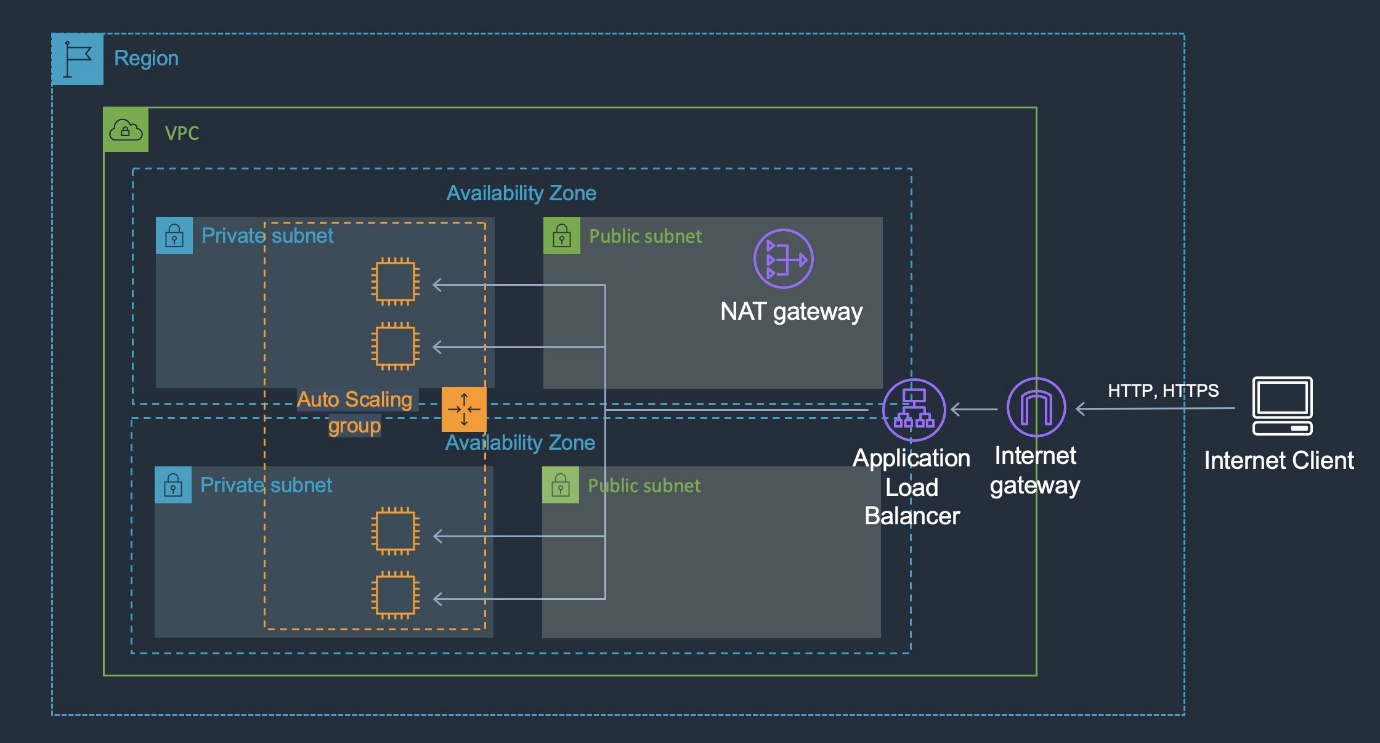
**18-> A Solutions Architect has deployed an application on several Amazon EC2 instances across three private subnets. The application must be made accessible to internet-based clients with the least amount of administrative effort.**

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

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

**Explanation**

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



**19 -> A gaming company uses Amazon Aurora as its primary database service. The company has now deployed 5 multi-AZ read replicas to increase the read throughput and for use as failover target. The replicas have been assigned the following failover priority tiers and corresponding sizes are given in parentheses: tier-1 (16TB), tier-1 (32TB), tier-10 (16TB), tier-15 (16TB), tier-15 (32TB).**

**In the event of a failover, Amazon RDS will promote which of the following read replicas?**

Correct option:

**Tier-1 (32TB)**

Amazon Aurora features a distributed, fault-tolerant, self-healing storage system that auto-scales up to 64TB per database instance. It delivers high performance and availability with up to 15 low-latency read replicas, point-in-time recovery, and continuous backup to Amazon S3, and replication across three Availability Zones (AZs).

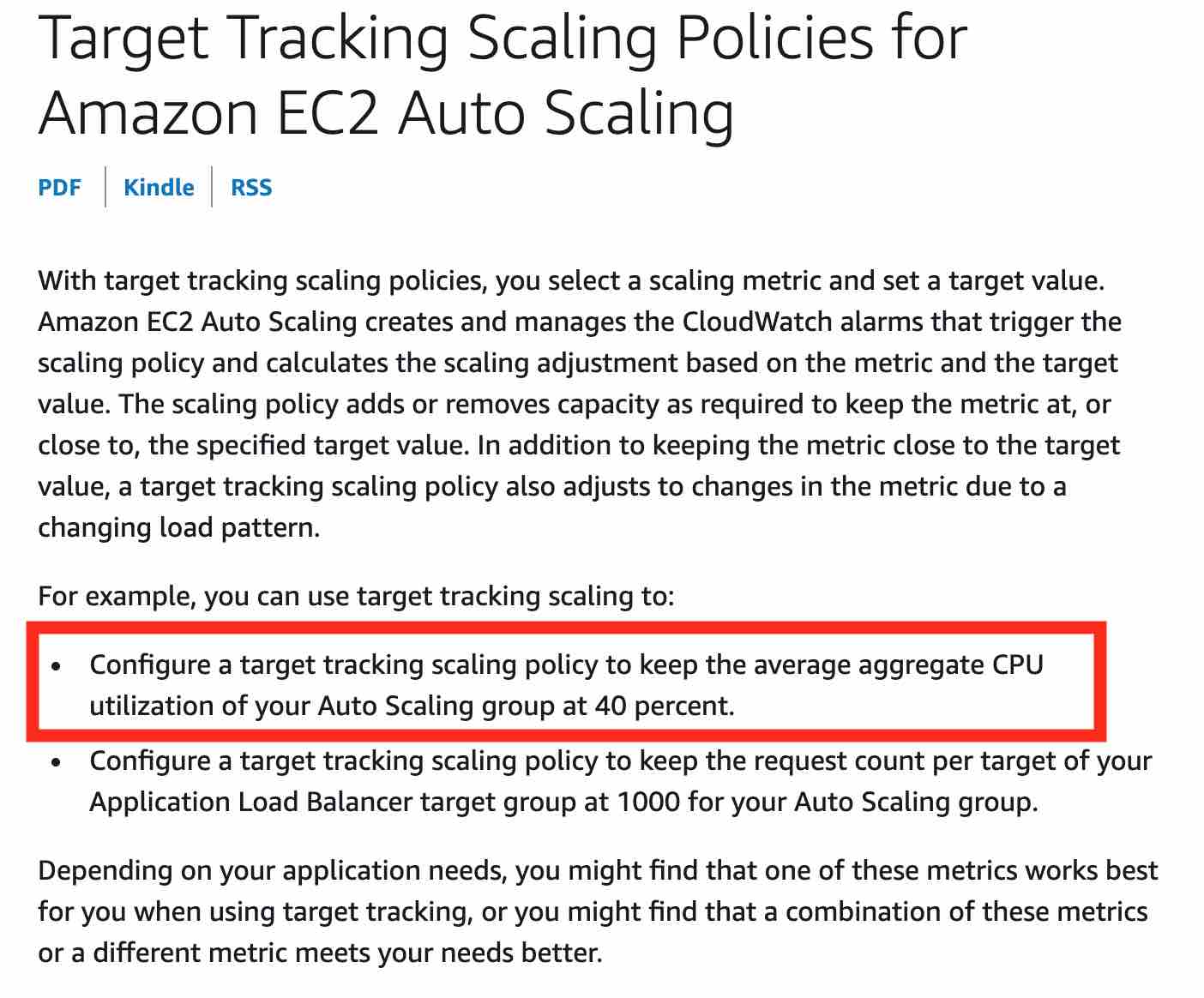
For Amazon Aurora, each Read Replica is associated with a priority tier (0-15). In the event of a failover, Amazon Aurora will promote the Read Replica that has the highest priority (the lowest numbered tier). If two or more Aurora Replicas share the same priority, then Amazon RDS promotes the replica that is largest in size. If two or more Aurora Replicas share the same priority and size, then Amazon Aurora promotes an arbitrary replica in the same promotion tier.

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

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

Correct option:

**Configure the Auto Scaling group to use target tracking policy and set the CPU utilization as the target metric with a target value of 50%**



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

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

Correct option:

**AWS Global Accelerator** - AWS Global Accelerator utilizes the Amazon global network, allowing you to improve the performance of your applications by lowering first-byte latency (the round trip time for a packet to go from a client to your endpoint and back again) and jitter (the variation of latency), and increasing throughput (the amount of time it takes to transfer data) as compared to the public internet.

Global Accelerator improves performance for a wide range of applications over TCP or UDP by proxying packets at the edge to applications running in one or more AWS Regions. Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover.

**Diff Btw Cloudfront and Global Accelerator ->** AWS Global Accelerator and Amazon CloudFront are separate services that use the AWS global network and its edge locations around the world. CloudFront improves performance for both cacheable content (such as images and videos) and dynamic content (such as API acceleration and dynamic site delivery), while Global Accelerator improves performance for a wide range of applications over TCP or UDP.

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

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

Correct options:

**When you apply a retention period to an object version explicitly, you specify a Retain Until Date for the object version** - You can place a retention period on an object version either explicitly or through a bucket default setting. When you apply a retention period to an object version explicitly, you specify a Retain Until Date for the object version. Amazon S3 stores the Retain Until Date setting in the object version's metadata and protects the object version until the retention period expires.

**Different versions of a single object can have different retention modes and periods** - Like all other Object Lock settings, retention periods apply to individual object versions. Different versions of a single object can have different retention modes and periods.

For example, suppose that you have an object that is 15 days into a 30-day retention period, and you PUT an object into Amazon S3 with the same name and a 60-day retention period. In this case, your PUT succeeds, and Amazon S3 creates a new version of the object with a 60-day retention period. The older version maintains its original retention period and becomes deletable in 15 days.

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

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

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

AWS Key Management Service (KMS) makes it easy for you to create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2.

Deleting a customer master key (CMK) in AWS Key Management Service (AWS KMS) is destructive and potentially dangerous. Therefore, AWS KMS enforces a waiting period. To delete a CMK in AWS KMS you schedule key deletion. You can set the waiting period from a minimum of 7 days up to a maximum of 30 days. The default waiting period is 30 days. During the waiting period, the CMK status and key state is Pending deletion. To recover the CMK, you can cancel key deletion before the waiting period ends. After the waiting period ends you cannot cancel key deletion, and AWS KMS deletes the CMK.

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

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

Correct option:

**Use SSE-KMS to encrypt the user data on S3**

AWS Key Management Service (AWS KMS) is a service that combines secure, highly available hardware and software to provide a key management system scaled for the cloud. When you use server-side encryption with AWS KMS (SSE-KMS), you can specify a customer-managed CMK that you have already created. SSE-KMS provides you with an audit trail that shows when your CMK was used and by whom. Therefore SSE-KMS is the correct solution for this use-case.

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

**How would you implement this with minimal application refactoring?**

Correct option:

**Use an Amazon Aurora Global Database for the games table and use Amazon Aurora for the users and games\_played tables**

Amazon Aurora is a MySQL and PostgreSQL-compatible relational database built for the cloud, that combines the performance and availability of traditional enterprise databases with the simplicity and cost-effectiveness of open source databases. Amazon Aurora features a distributed, fault-tolerant, self-healing storage system that auto-scales up to 64TB per database instance. Aurora is not an in-memory database.

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

For the given use-case, we, therefore, need to have two Aurora clusters, one for the global table (games table) and the other one for the local tables (users and games\_played tables).

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

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

Correct option:

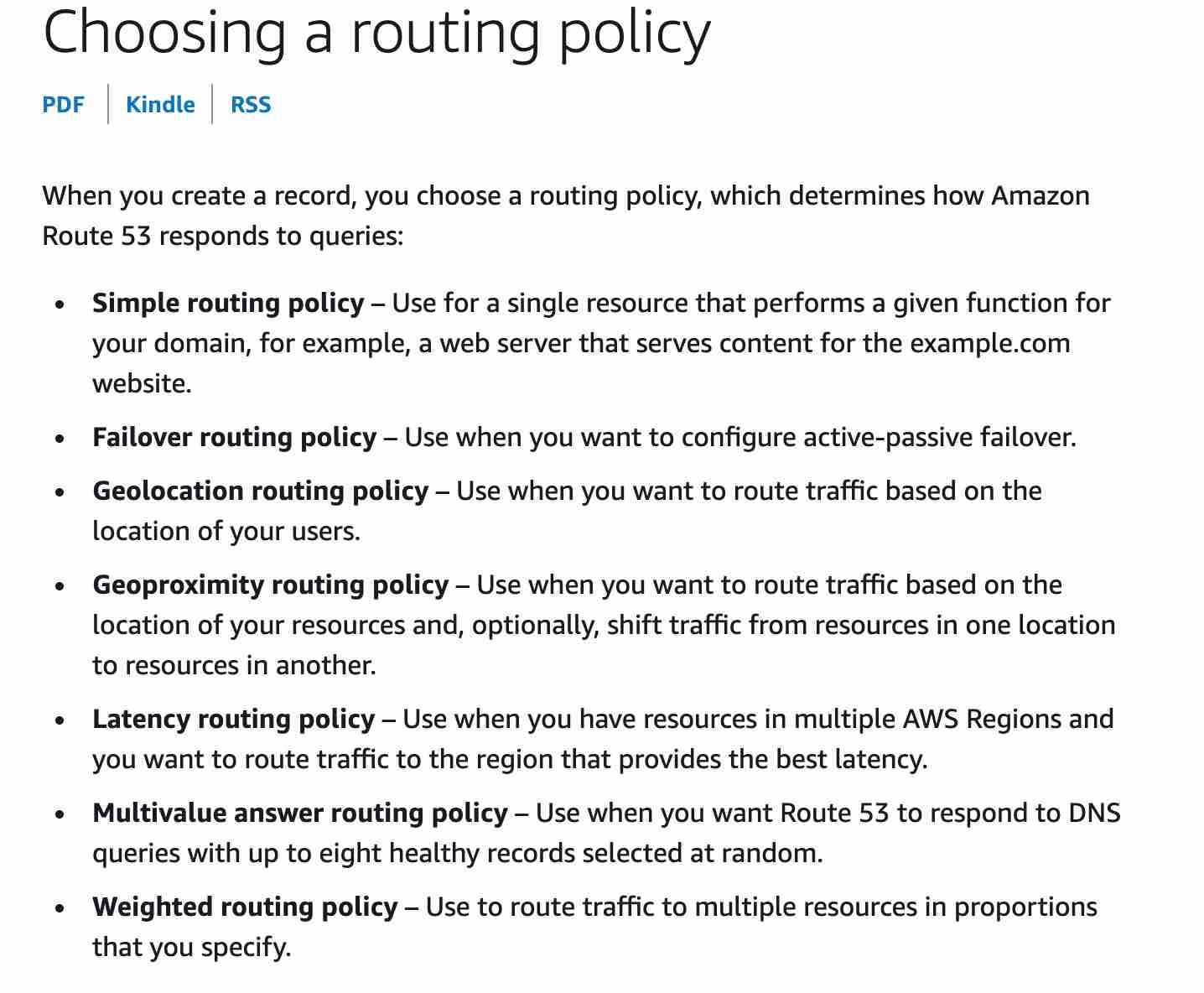
**Amazon SNS message deliveries to AWS Lambda have crossed the account concurrency quota for Lambda, so the team needs to contact AWS support to raise the account limit**

Amazon Simple Notification Service (SNS) is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple micro services, distributed systems, and server less applications.

With AWS Lambda, you can run code without provisioning or managing servers. You pay only for the compute time that you consume—there’s no charge when your code isn’t running.

AWS Lambda currently supports 1000 concurrent executions per AWS account per region. If your Amazon SNS message deliveries to AWS Lambda contribute to crossing these concurrency quotas, your Amazon SNS message deliveries will be throttled. You need to contact AWS support to raise the account limit. Therefore this option is correct.

**Note->**



27 -> a company runs a number of core enterprise applications in an on-premises data center. The data centre is connected to an Amazon VPC using AWS Direct Connect. The company will be creating additional AWS accounts and these accounts will also need to be quickly, and cost-effectively connected to the on-premises data centre in order to access the core applications.

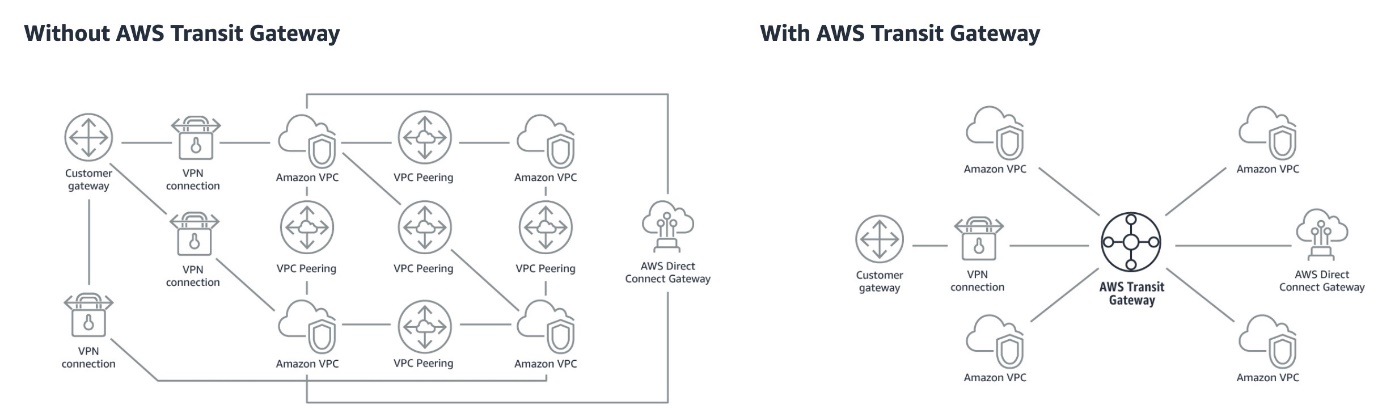
What deployment changes should a Solutions Architect implement to meet these requirements with the LEAST operational overhead?

***CORRECT:* "**Configure AWS Transit Gateway between the accounts. Assign Direct Connect to the transit gateway and route network traffic to the on-premises servers" is the correct answer.

Explanation

AWS Transit Gateway connects VPCs and on-premises networks through a central hub. With AWS Transit Gateway, you can quickly add Amazon VPCs, AWS accounts, VPN capacity, or AWS Direct Connect gateways to meet unexpected demand, without having to wrestle with complex connections or massive routing tables. This is the operationally least complex solution and is also cost-effective.

The image below depicts how transit gateway can assist with simplifying network deployments:



28 –> A web application has recently been launched on AWS. The architecture includes two tier with a web layer and a database layer. It has been identified that the web server layer may be vulnerable to cross-site scripting (XSS) attacks.

What should a solutions architect do to remediate the vulnerability?

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

Explanation

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

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

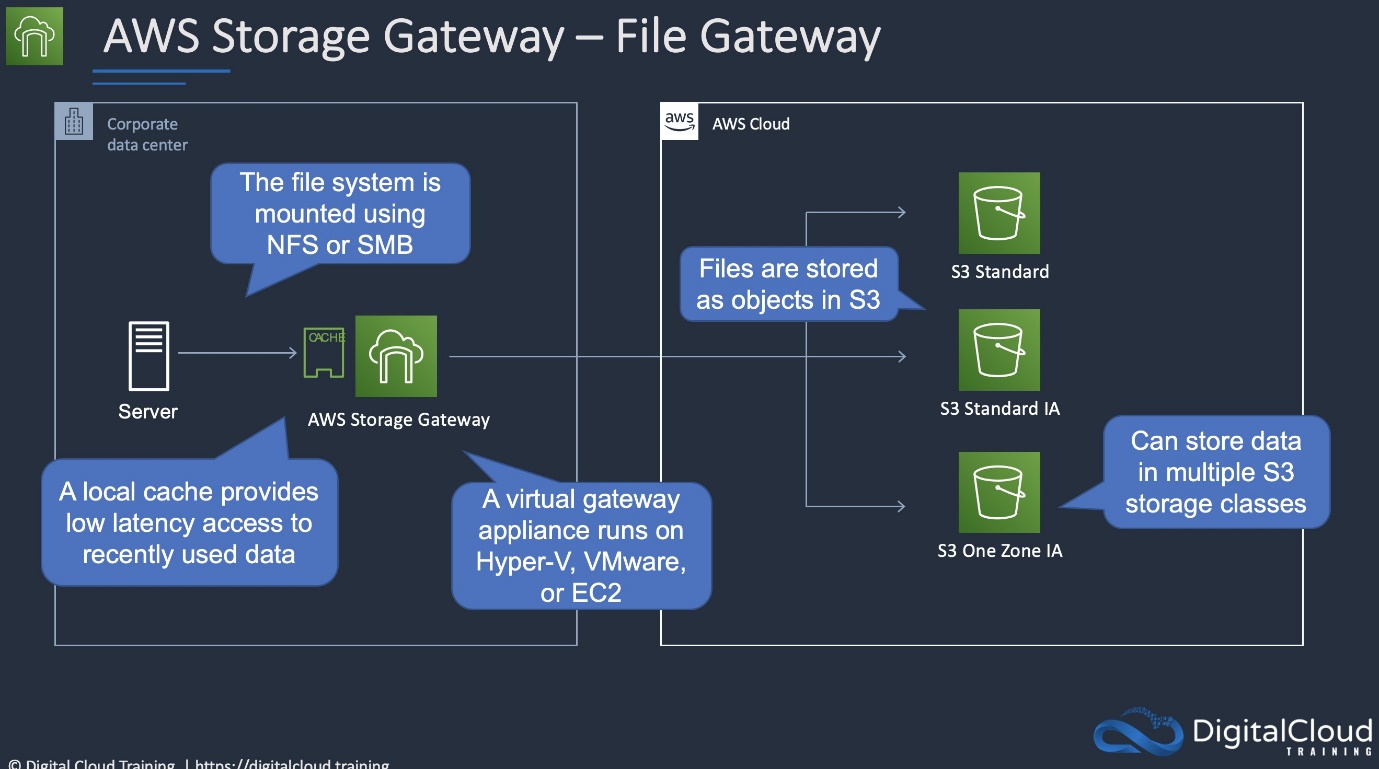
29 -> a company has a file share on a Microsoft Windows Server in an on-premises data centre. The server uses a local network attached storage (NAS) device to store several terabytes of files. The management team require a reduction in the data centre footprint and to minimize storage costs by moving on-premises storage to AWS.

What should a Solutions Architect do to meet these requirements?

**CORRECT:**"Configure an AWS Storage Gateway file gateway" is the correct answer.

Explanation

An AWS Storage Gateway File Gateway provides your applications a file interface to seamlessly store files as objects in Amazon S3, and access them using industry standard file protocols. This removes the files from the on-premises NAS device and provides a method of directly mounting the file share for on-premises servers and clients.



**INCORRECT:** "Configure an AWS Storage Gateway as a volume gateway" is incorrect. A volume gateway uses block-based protocols. In this case we are replacing a NAS device which uses file-level protocols so the best option is a file gateway

**SQS / SNS ->**

Amazon SNS is inexpensive and based on a pay-as-you-go model with no upfront costs.

**SNS Topics**

Multiple recipients can be grouped using Topics.

A topic is an “access point” for allowing recipients to dynamically subscribe for identical copies of the same notification.

One topic can support deliveries to multiple endpoint types.

**30 -** A company has some statistical data stored in an Amazon RDS database. The company wants to allow users to access this information using an API. A solutions architect must create a solution that allows sporadic access to the data, ranging from no requests to large bursts of traffic.

Which solution should the solutions architect suggest?

Explanation

This question is simply asking you to work out the best compute service for the stated requirements. The key requirements are that the compute service should be suitable for a workload that can range quite broadly in demand from no requests to large bursts of traffic.

AWS Lambda is an ideal solution as you pay only when requests are made and it can easily scale to accommodate the large bursts in traffic. Lambda works well with both API Gateway and Amazon RDS.

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

**31-** A company has deployed an application that consists of several micro services running on Amazon EC2 instances behind an Amazon API Gateway API. A Solutions Architect is concerned that the microservices are not designed to elastically scale when large increases in demand occur.

Which solution addresses this concern?

Explanation

The individual microservices are not designed to scale. Therefore, the best way to ensure they are not overwhelmed by requests is to decouple the requests from the microservices. An Amazon SQS queue can be created, and the API Gateway can be configured to add incoming requests to the queue. The microservices can then pick up the requests from the queue when they are ready to process them.

**CORRECT:**"Create an Amazon SQS queue to store incoming requests. Configure the microservices to retrieve the requests from the queue for processing" is the correct answer.

32->A company needs to migrate a large quantity of data from an on-premises environment to Amazon S3. The company is connected via an AWS Direct Connect (DX) connection. The company requires a fully managed solution that will keep the data private and automate and accelerate the replication of the data to AWS storage services.

Which solution should a Solutions Architect recommend?

Explanation

AWS DataSync can be used to automate and accelerate the replication of data to AWS storage services. Note that Storage Gateway is used for hybrid scenarios where servers need local access to data with various options for storing and synchronizing the data to AWS storage services. Storage Gateway does not accelerate replication of data.

To deploy DataSync an agent must be installed. Then a task must be configured to replicated data to AWS. The task requires a connection to a service endpoint. To keep the data private and send it across the DX connection, a VPC endpoint should be used.

**CORRECT:**"Deploy an AWS DataSync agent for the on-premises environment. Configure a task to replicate the data and connect it to a VPC endpoint" is the correct answer.

33->A company runs a containerized application on an Amazon Elastic Kubernetes Service (EKS) using a microservices architecture. The company requires a solution to collect, aggregate, and summarize metrics and logs. The solution should provide a centralized dashboard for viewing information including CPU and memory utilization for EKS namespaces, services, and pods.

Which solution meets these requirements?

Explanation

Use CloudWatch Container Insights to collect, aggregate, and summarize metrics and logs from your containerized applications and microservices. Container Insights is available for Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS), and Kubernetes platforms on Amazon EC2.

With Container Insights for EKS you can see the top contributors by memory or CPU, or the most recently active resources. This is available when you select any of the following dashboards in the drop-down box near the top of the page:

  •  ECS Services

  •  ECS Tasks

  •  EKS Namespaces

  •  EKS Services

  •  EKS Pods

**CORRECT:**"Configure Amazon CloudWatch Container Insights in the existing EKS cluster. View the metrics and logs in the CloudWatch console" is the correct answer.

34->An organization is extending a secure development environment into AWS. They have already secured the VPC including removing the Internet Gateway and setting up a Direct Connect connection. What else needs to be done to add encryption?

Explanation

A VPG is used to setup an AWS VPN which you can use in combination with Direct Connect to encrypt all data that traverses the Direct Connect link. This combination provides an IPsec-encrypted private connection that also reduces network costs, increases bandwidth throughput, and provides a more consistent network experience than internet-based VPN connections.

**CORRECT:**"Setup a Virtual Private Gateway (VPG)" is the correct answer.

35->A Kinesis consumer application is reading at a slower rate than expected. It has been identified that multiple consumer applications have total reads exceeding the per-shard limits. How can this situation be resolved?

Explanation

One shard provides a capacity of 1MB/sec data input and 2MB/sec data output. One shard can support up to 1000 PUT records per second. The total capacity of the stream is the sum of the capacities of its shards.

In a case where multiple consumer applications have total reads exceeding the per-shard limits, you need to increase the number of shards in the Kinesis data stream.

**CORRECT:**"Increase the number of shards in the Kinesis data stream" is the correct answer.

\*\*\*Global Accelerator directs traffic to optimal endpoints over the AWS global network.

36 - > When using throttling controls with API Gateway what happens when request submissions exceed the steady-state request rate and burst limits?

Explanation

You can throttle and monitor requests to protect your backend. Resiliency through throttling rules based on the number of requests per second for each HTTP method (GET, PUT). Throttling can be configured at multiple levels including Global and Service Call.

When request submissions exceed the steady-state request rate and burst limits, API Gateway fails the limit-exceeding requests and returns 429 Too Many Requests error responses to the client.

**CORRECT:**"API Gateway fails the limit-exceeding requests and returns “429 Too Many Requests” error responses to the client" is the correct answer.

37-> A website uses web servers behind an Internet-facing Elastic Load Balancer. What record set should be created to point the customer’s DNS zone apex record at the ELB?

Explanation

An Alias record can be used for resolving apex or naked domain names (e.g. example.com). You can create an A record that is an Alias that uses the customer’s website zone apex domain name and map it to the ELB DNS name.

**CORRECT:**"Create an A record that is an Alias, and select the ELB DNS as a target" is the correct answer.

38->A Solutions Architect would like to implement a method of automating the creation, retention, and deletion of backups for the Amazon EBS volumes in an Amazon VPC. What is the easiest way to automate these tasks using AWS tools?

Explanation

You backup EBS volumes by taking snapshots. This can be automated via the AWS CLI command “create-snapshot”. However the question is asking for a way to automate not just the creation of the snapshot but the retention and deletion too.

The EBS Data Lifecycle Manager (DLM) can automate all of these actions for you and this can be performed centrally from within the management console.

**CORRECT:**"Use the EBS Data Lifecycle Manager (DLM) to manage snapshots of the volumes" is the correct answer.

**\*\*\*\*\*\*When you're using an Edge device, the data migration process has the following stages:**

**1. You use the AWS Schema Conversion Tool (AWS SCT) to extract the data locally and move it to an Edge device.**

**2. You ship the Edge device or devices back to AWS.**

**3. After AWS receives your shipment, the Edge device automatically loads its data into an Amazon S3 bucket.**

**4. AWS DMS takes the files and migrates the data to the target data store. If you are using change data capture (CDC), those updates are written to the Amazon S3 bucket and then applied to the target data store.**

38->Every time an item in an Amazon DynamoDB table is modified a record must be retained for compliance reasons. What is the most efficient solution to recording this information?

Explanation

Amazon DynamoDB Streams captures a time-ordered sequence of item-level modifications in any DynamoDB table and stores this information in a log for up to 24 hours. Applications can access this log and view the data items as they appeared before and after they were modified, in near-real time.

For example, in the diagram below a DynamoDB stream is being consumed by a Lambda function which processes the item data and records a record in CloudWatch Logs:

**CORRECT:**"Enable DynamoDB Streams. Configure an AWS Lambda function to poll the stream and record the modified item data to an Amazon S3 bucket" is the correct answer

39->A Solutions Architect must design a solution for providing single sign-on to existing staff in a company. The staff manage on-premise web applications and also need access to the AWS management console to manage resources in the AWS cloud.

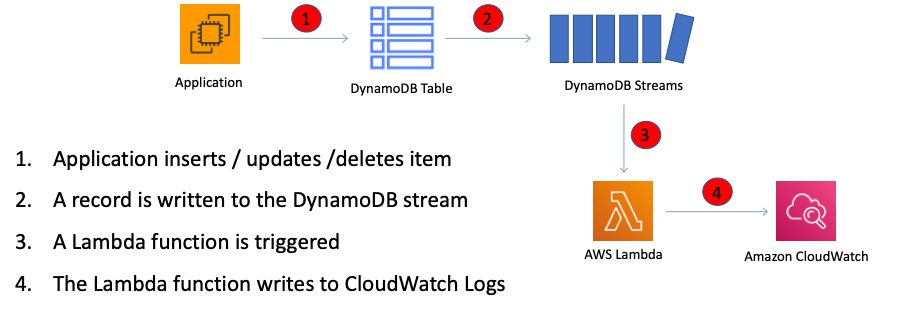
Which combination of services are BEST suited to delivering these requirements?

Explanation

Single sign-on using federation allows users to login to the AWS console without assigning IAM credentials. The AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for IAM users or for users that you authenticate (such as federated users from an on-premise directory).

Federation (typically Active Directory) uses SAML 2.0 for authentication and grants temporary access based on the users AD credentials. The user does not need to be a user in IAM.

**CORRECT:**"Use the AWS Secure Token Service (STS) and SAML" is the correct answer.

.

40->A company has two accounts in an AWS Organization. The accounts are: Prod1 and Prod2. An Amazon RDS database runs in the Prod1 account. Amazon EC2 instances run in the Prod2 account. The EC2 instances in the Prod2 account must access the RDS database.

How can a Solutions Architect meet this requirement MOST cost-effectively?

Explanation

VPC sharing makes use of the AWS Resource Access Manager (AWS RAM) service. It enables the sharing of VPCs across accounts. In this model, the account that owns the VPC (owner) shares one or more subnets with other accounts (participants) that belong to the same organization from AWS Organizations.

This scenario could be implemented with Prod1 account as the VPC owner and the Prod2 account as a VPC participant. This would allow the central control of the shared resource whilst enabling the EC2 instances in Prod2 to access the database.

**CORRECT:**"Set up VPC sharing with the Prod1 account as the owner and the Prod2 account as the participant to transfer the data" is the correct answer.

41->An Amazon S3 bucket is going to be used by a company to store sensitive data. A Solutions Architect needs to ensure that all objects uploaded to an Amazon S3 bucket are encrypted. How can this be achieved?

Explanation

To encrypt an object at the time of upload, you need to add a header called x-amz-server-side-encryption to the request to tell S3 to encrypt the object using SSE-C, SSE-S3, or SSE-KMS.

To enforce object encryption, create an S3 bucket policy that denies any S3 Put request that does not include the x-amz-server-side-encryption header. There are two possible values for the x-amz-server-side-encryption header: AES256, which tells S3 to use S3-managed keys, and aws:kms, which tells S3 to use AWS KMS–managed keys.

**CORRECT:**"Create a bucket policy that denies Put requests that do not have an x-amz-server-side-encryption header set" is the correct answer.

**42->**A Solutions Architect needs to work programmatically with IAM. Which feature of IAM allows direct access to the IAM web service using HTTPS to call service actions and what is the method of authentication that must be used? (Choose 2)

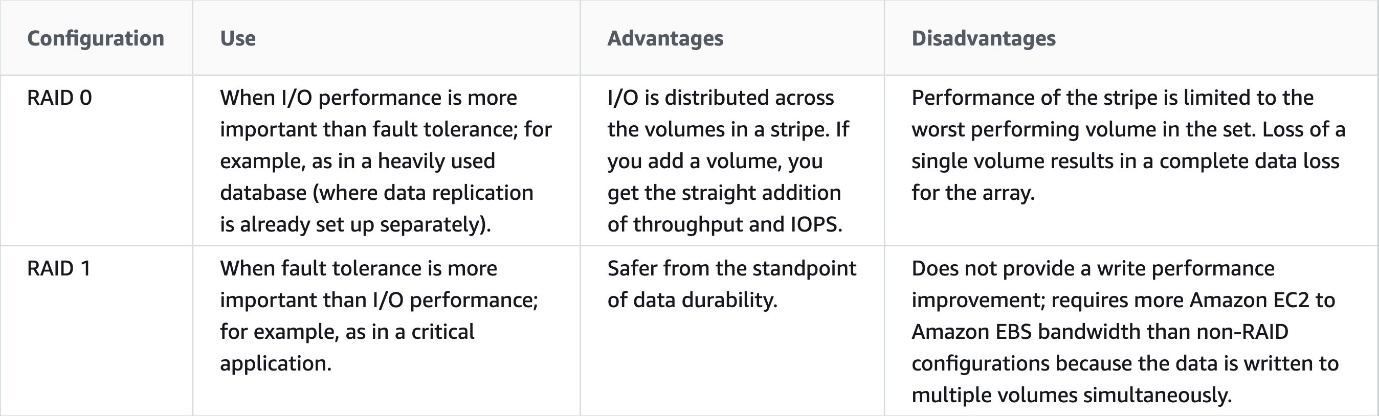
Explanation

AWS recommend that you use the AWS SDKs to make programmatic API calls to IAM. However, you can also use the IAM Query API to make direct calls to the IAM web service. An access key ID and secret access key must be used for authentication when using the Query API.

**CORRECT:**"Query API" is a correct answer.

**CORRECT:**"Access key ID and secret access key" is also a correct answer.

**\*\*\*\*\*\*RAID->**



**43->**An application you manage runs a number of components using a micro-services architecture. Several ECS container instances in your ECS cluster are displaying as disconnected. The ECS instances were created from the Amazon ECS-Optimized AMI. What steps might you take to troubleshoot the issue? (choose 2)

Explanation

The ECS container agent is included in the Amazon ECS optimized AMI and can also be installed on any EC2 instance that supports the ECS specification (only supported on EC2 instances). Therefore, you don’t need to verify that the agent is installed.

You need to verify that the installed agent is running and that the IAM instance profile has the necessary permissions applied.

Troubleshooting steps for containers include:

- Verify that the Docker daemon is running on the container instance.

- Verify that the Docker Container daemon is running on the container instance.

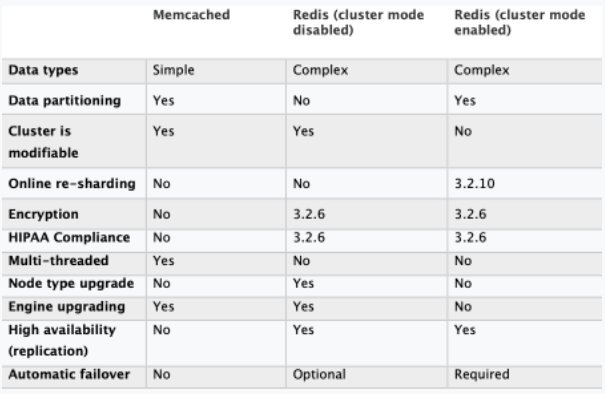
- Verify that the container agent is running on the container instance.

- Verify that the IAM instance profile has the necessary permissions.

**CORRECT:**"Verify that the IAM instance profile has the necessary permissions" is the correct answer.

**CORRECT:**"Verify that the container agent is running on the container instances" is the correct answer.

**Memcached Vs Redis ->**



**44->**An application is running on EC2 instances in a private subnet of an Amazon VPC. A Solutions Architect would like to connect the application to Amazon API Gateway. For security reasons, it is necessary to ensure that no traffic traverses the Internet and to ensure all traffic uses private IP addresses only.

Explanation

An Interface endpoint uses AWS PrivateLink and is an elastic network interface (ENI) with a private IP address that serves as an entry point for traffic destined to a supported service. Using PrivateLink you can connect your VPC to supported AWS services, services hosted by other AWS accounts (VPC endpoint services), and supported AWS Marketplace partner services.

**CORRECT:**"Create a private API using an interface VPC endpoint" is the correct answer.

**\*\*\*\*\*\*\*columnar storage = RedShift**

**\*\*\*\*\*\*The requirements are to avoid the internet and use private IP addresses only = VPC endpoint for Amazon API Gateway can be created and this will provide access to API Gateway using private IP addresses and avoids the internet completely.**

**\*\*\*\*\*DynamoDB best practices include:**

- Keep item sizes small.

- If you are storing serial data in DynamoDB that will require actions based on data/time use separate tables for days, weeks, months.

- Store more frequently and less frequently accessed data in separate tables.

- If possible compress larger attribute values.

- Store objects larger than 400KB in S3 and use pointers (S3 Object ID) in DynamoDB.

45->A Solutions Architect is creating a multi-tier application that includes loosely-coupled, distributed application components and needs to determine a method of sending notifications instantaneously. Using Amazon SNS which transport protocols are supported? (Choose 2)

Amazon SNS supports notifications over multiple transport protocols:

- HTTP/HTTPS – subscribers specify a URL as part of the subscription registration.

- Email/Email-JSON – messages are sent to registered addresses as email (text-based or JSON-object).

- SQS – users can specify an SQS standard queue as the endpoint.

- SMS – messages are sent to registered phone numbers as SMS text messages.

**CORRECT:**"HTTPS" is the correct answer.

**CORRECT:**"Email-JSON" is the correct answer

**46->**An application stack is being created which needs a message bus to decouple the application components from each other. The application will generate up to 300 messages per second without using batching. A Solutions Architect needs to ensure that a message is delivered only once and duplicates are not introduced into the queue. It is not necessary to maintain the order of the messages.

Which SQS queue type should be used?

Explanation

The key fact you need to consider here is that duplicate messages cannot be introduced into the queue. For this reason alone you must use a FIFO queue. The statement about it not being necessary to maintain the order of the messages is meant to confuse you, as that might lead you to think you can use a standard queue, but standard queues don’t guarantee that duplicates are not introduced into the queue.

FIFO (first-in-first-out) queues preserve the exact order in which messages are sent and received – note that this is not required in the question but exactly once processing is. FIFO queues provide exactly-once processing, which means that each message is delivered once and remains available until a consumer processes it and deletes it.

**CORRECT:**"FIFO queues" is the correct answer.

**\*\*\*\*\*\*\*\*\***To enable your Lambda function to access resources inside your private VPC, you must provide additional VPC-specific configuration information that includes VPC subnet IDs and security group IDs. AWS Lambda uses this information to set up elastic network interfaces (ENIs) that enable your function.

**47->**A Solutions Architect manages multiple Amazon RDS MySQL databases. To improve security, the Solutions Architect wants to enable secure user access with short-lived credentials. How can these requirements be met?

**Explanation**

With MySQL, authentication is handled by AWSAuthenticationPlugin—an AWS-provided plugin that works seamlessly with IAM to authenticate your IAM users. Connect to the DB instance and issue the CREATE USER statement, as shown in the following example.

CREATE USER jane\_doe IDENTIFIED WITH AWSAuthenticationPlugin AS 'RDS';

The IDENTIFIED WITH clause allows MySQL to use the AWSAuthenticationPlugin to authenticate the database account (jane\_doe). The AS 'RDS' clause refers to the authentication method, and the specified database account should have the same name as the IAM user or role. In this example, both the database account and the IAM user or role are named jane\_doe.

**CORRECT:**"Create the MySQL user accounts to use the AWSAuthenticationPlugin with IAM" is the correct answer.

**\*\*\*\*\*\*\*\*\*\*CloudFormation provides two methods for updating-**

Explanation

AWS CloudFormation provides two methods for updating stacks: direct update or creating and executing change sets. When you directly update a stack, you submit changes and AWS CloudFormation immediately deploys them.

Use direct updates when you want to quickly deploy your updates. With change sets, you can preview the changes AWS CloudFormation will make to your stack, and then decide whether to apply those changes.

**\*\*\*\*\*\*\*Trails can be configured to log Data events and management events:**

**Data events:** These events provide insight into the resource operations performed on or within a resource. These are also known as data plane operations

**Management events:** Management events provide insight into management operations that are performed on resources in your AWS account. These are also known as control plane operations. Management events can also include non-API events that occur in your account

**\*\*\*\*\*\*\*\*\*\*Some facts about Amazon EBS encrypted volumes and snapshots:\*\***

- All **EBS** types support encryption and all instance **families** now support encryption.

- Not all **instance** types support encryption.

- Data in transit between an instance and an encrypted volume is also encrypted (data is encrypted in trans.

- You can have encrypted an unencrypted EBS volumes attached to an instance at the same time.

- Snapshots of encrypted volumes are encrypted automatically.

- EBS volumes restored from encrypted snapshots are encrypted automatically.

- EBS volumes created from encrypted snapshots are also encrypted.

48->A company has deployed an API using Amazon API Gateway. There are many repeat requests and a solutions architect has been asked to implement measures to reduce request latency and the number of calls to the Amazon EC2 endpoint.

How can this be most easily achieved?

Explanation

You can enable API caching in Amazon API Gateway to cache your endpoint's responses. With caching, you can reduce the number of calls made to your endpoint and also improve the latency of requests to your API.

When you enable caching for a stage, API Gateway caches responses from your endpoint for a specified time-to-live (TTL) period, in seconds. API Gateway then responds to the request by looking up the endpoint response from the cache instead of making a request to your endpoint. The default TTL value for API caching is 300 seconds. The maximum TTL value is 3600 seconds. TTL=0 means caching is disabled.

**CORRECT:**"Create a cache for a stage and configure a TTL" is the correct answer.

**\*\*\*\*Enhanced networking->**

Enhanced networking provides higher bandwidth, higher packet-per-second (PPS) performance, and consistently lower inter-instance latencies. If your packets-per-second rate appears to have reached its ceiling, you should consider moving to enhanced networking because you have likely reached the upper thresholds of the VIF driver. It is only available for certain instance types and only supported in VPC. You must also launch an HVM AMI with the appropriate drivers.

AWS currently supports enhanced networking capabilities using SR-IOV. SR-IOV provides direct access to network adapters, provides higher performance (packets-per-second) and lower latency.

**\*\*\*\*AWS Server less Application Model (AWS SAM) ->**

Explanation

AWS Server less Application Model (AWS SAM) is an extension of AWS CloudFormation that is used to package, test, and deploy serverless applications.

With Amazon CloudWatch, you can access system metrics on all the AWS services you use, consolidate system and application level logs, and create business key performance indicators (KPIs) as custom metrics for your specific needs.

**\*\*\*\*\*Which AWS services would allow the company to query the data in place?-**

Amazon S3 Select is designed to help analyze and process data within an object in Amazon S3 buckets, faster and cheaper. It works by providing the ability to retrieve a subset of data from an object in Amazon S3 using simple SQL expressions

Amazon Redshift Spectrum allows you to directly run SQL queries against exabytes of unstructured data in Amazon S3. No loading or transformation is required.

**CORRECT:**"Amazon S3 Select" is a correct answer.

**CORRECT:**"Amazon RedShift Spectrum" is also a correct answer.

**\*\*\*\*You can specify the instance store volumes for your instance only when you launch an instance. You can’t attach instance store volumes to an instance after you’ve launched it.**

49->A Solutions Architect needs to run a PowerShell script on a fleet of Amazon EC2 instances running Microsoft Windows. The instances have already been launched in an Amazon VPC. What tool can be run from the AWS Management Console that to execute the script on all target EC2 instances?

Explanation

Run Command is designed to support a wide range of enterprise scenarios including installing software, running ad hoc scripts or Microsoft PowerShell commands, configuring Windows Update settings, and more.

Run Command can be used to implement configuration changes across Windows instances on a consistent yet ad hoc basis and is accessible from the AWS Management Console, the AWS Command Line Interface (CLI), the AWS Tools for Windows PowerShell, and the AWS SDKs.

**CORRECT:**"Run Command" is the correct answer.

**50->**The application development team in a company have developed a Java application and saved the source code in a .war file. They would like to run the application on AWS resources and are looking for a service that can handle the provisioning and management of the underlying resources it will run on.

Which AWS service should a Solutions Architect recommend the Developers use to upload the Java source code file?

AWS Elastic Beanstalk can be used to quickly deploy and manage applications in the AWS Cloud. Developers upload applications and Elastic Beanstalk handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring

Elastic Beanstalk supports applications developed in Go, Java, .NET, Node.js, PHP, Python, and Ruby, as well as different platform configurations for each language. To use Elastic Beanstalk, you create an application, upload an application version in the form of an application source bundle (for example, a Java .war file) to Elastic Beanstalk, and then provide some information about the application.

**CORRECT:**"AWS Elastic Beanstalk" is the correct answer.

51->An IT Company is looking to move its on-premises infrastructure to AWS Cloud. The company has a portfolio of applications with a few of them using server bound licenses that are valid for the next year. To utilize the licenses, the CTO wants to use dedicated hosts for a one year term and then migrate the given instances to default tenancy thereafter.

As a solutions architect, which of the following options would you identify as CORRECT for changing the tenancy of an instance after you have launched it? (Select two)

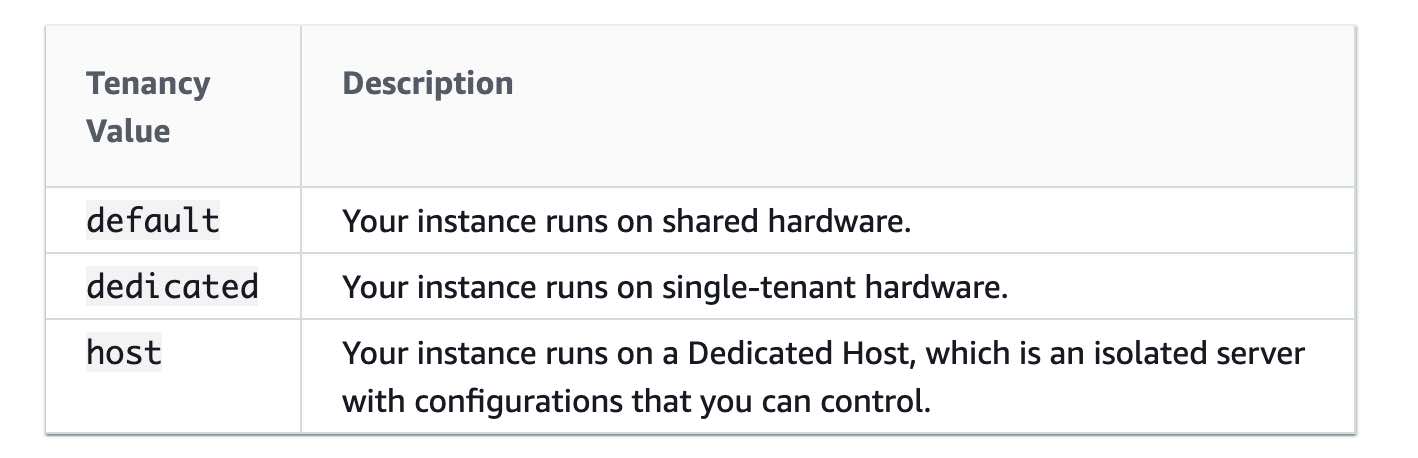
#### Explanation

Correct options:

**You can change the tenancy of an instance from dedicated to host**

**You can change the tenancy of an instance from host to dedicated**

Each EC2 instance that you launch into a VPC has a tenancy attribute. This attribute has the following values.



**FAQs -** [**https://aws.amazon.com/ec2/faqs/**](https://aws.amazon.com/ec2/faqs/)

[**https://aws.amazon.com/kinesis/data-streams/faqs/**](https://aws.amazon.com/kinesis/data-streams/faqs/)

[**https://aws.amazon.com/kinesis/data-firehose/faqs/**](https://aws.amazon.com/kinesis/data-firehose/faqs/)

[**https://aws.amazon.com/kinesis/data-analytics/faqs/**](https://aws.amazon.com/kinesis/data-analytics/faqs/)

[**https://aws.amazon.com/ebs/faqs/**](https://aws.amazon.com/ebs/faqs/)

**52->**the development team at a retail company wants to optimize the cost of EC2 instances. The team wants to move certain nightly batch jobs to spot instances. The team has hired you as a solutions architect to provide the initial guidance.

Which of the following would you identify as CORRECT regarding the capabilities of spot instances? (Select three)

#### Explanation

Correct options:

**If a spot request is persistent, then it is opened again after your Spot Instance is interrupted**

**Spot blocks are designed not to be interrupted**

**When you cancel an active spot request, it does not terminate the associated instance**

53 ->An AWS Organization is using Service Control Policies (SCP) for central control over the maximum available permissions for all accounts in their organization. This allows the organization to ensure that all accounts stay within the organization’s access control guidelines.

Which of the given scenarios are correct regarding the permissions described below? (Select three)

#### Explanation

Correct options:

**If a user or role has an IAM permission policy that grants access to an action that is either not allowed or explicitly denied by the applicable SCPs, the user or role can't perform that action**

**SCPs affect all users and roles in attached accounts, including the root user**

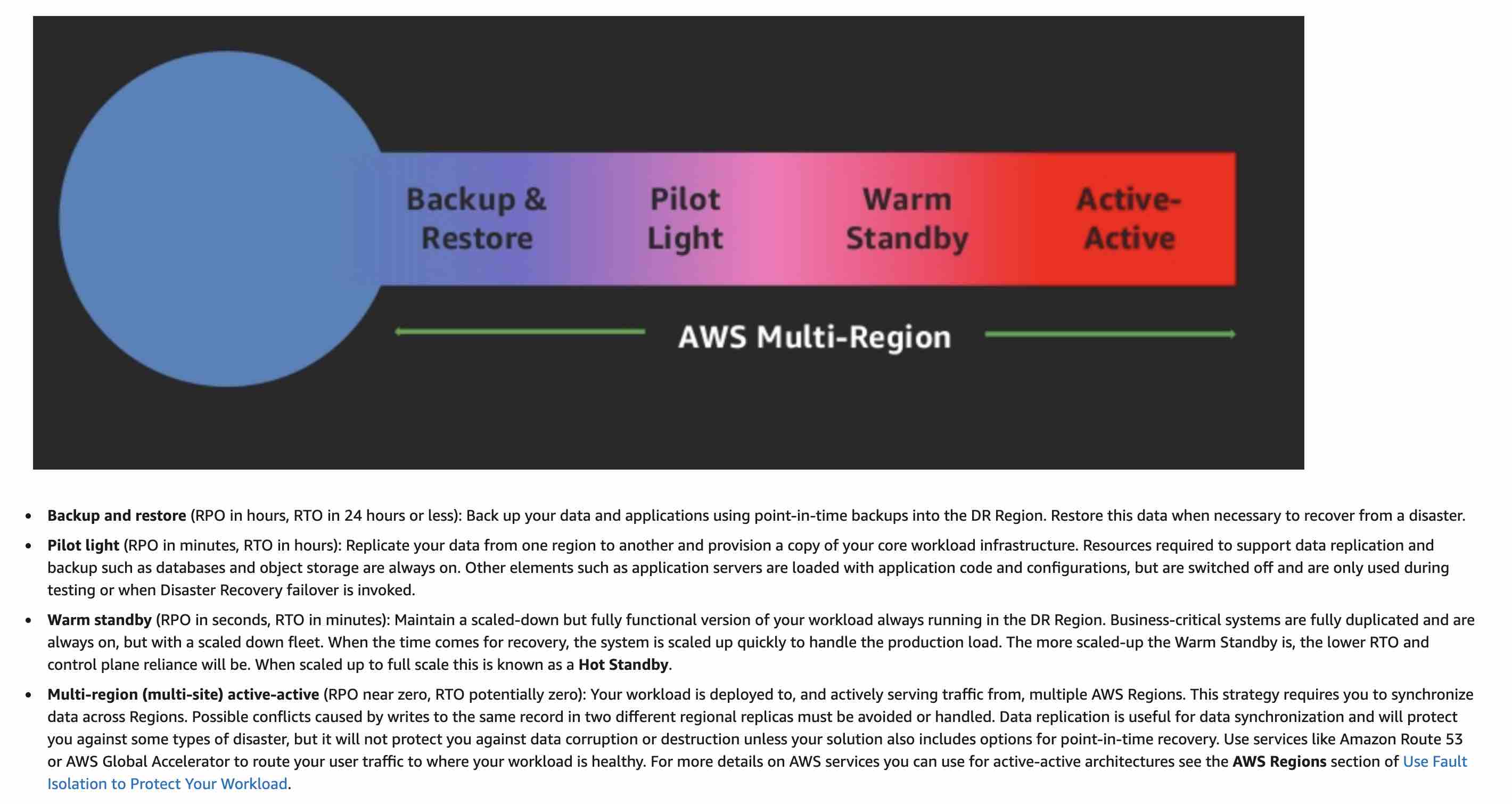
**SCPs do not affect service-linked role**

 Whitelist up to two public IPs = Network load balancer

Which is the only resource-based policy that the IAM service supports? –

**Trust policy** - Trust policies define which principal entities (accounts, users, roles, and federated users) can assume the role. An IAM role is both an identity and a resource that supports resource-based policies. For this reason, you must attach both a trust policy and an identity-based policy to an IAM role. The IAM service supports only one type of resource-based policy called a role trust policy, which is attached to an IAM role.

DR –



**Point to Remember for Lambda Function –**

**If you intend to reuse code in more than one Lambda function, you should consider creating a Lambda Layer for the reusable code** –

**Since Lambda functions can scale extremely quickly, it’s a good idea to deploy a CloudWatch Alarm that notifies your team when function metrics such as ConcurrentExecutions or Invocations exceeds the expected threshold**

**By default, Lambda functions always operate from an AWS-owned VPC and hence have access to any public internet address or public AWS APIs. Once a Lambda function is VPC-enabled, it will need a route through a NAT gateway in a public subnet to access public resources**

54.240.143.188/32 - /32 means only 1 ip

Amazon FSx –

1 - Amazon FSx for Windows File Server does not use Amazon S3 buckets

2 - Amazon FSx works with Microsoft Active Directory (AD) to integrate with your existing Microsoft Windows environments.

\*\*\*\*If you need a shared file system which can integrate with AD that is Amazon FSx for Windows File system

***Amazon Arora -***

**Amazon Aurora Serverless** is an on-demand, auto-scaling configuration for Amazon Aurora. The database automatically starts up, shuts down, and scales capacity up or down based on application needs. This is an ideal database solution for infrequently-used applications.

relational database that can support a Recovery Point Objective (RPO) of 1 second and a Recovery Time Objective (RTO) of 1 minute.- Aurora Global Database

**Q -** A customer has a public-facing web application hosted on a single Amazon Elastic Compute Cloud (EC2) instance serving videos directly from an Amazon S3 bucket. Which of the following will restrict third parties from directly accessing the video assets in the bucket?

#### Explanation

To allow read access to the S3 video assets from the public-facing web application, you can add a bucket policy that allows s3:GetObject permission with a condition, using the aws:referer key, that the get request must originate from specific webpages. This is a good answer as it fully satisfies the objective of ensuring the that EC2 instance can access the videos but direct access to the videos from other sources is prevented.

**CORRECT:**"Use a bucket policy to only allow referrals from the main website URL" is the correct answer.

***Temporary AWS credentials –***

1 – Amazon Cognito identity pools- With an identity pool, users can obtain temporary AWS credentials to access AWS services, such as Amazon S3 and DynamoDB.

2 – STS

***EBS Volume Type –***

This is simply about understanding the performance characteristics of the different EBS volume types. The only EBS volume type that supports over 16,000 IOPS per volume is Provisioned IOPS SSD.

**SSD, General Purpose – gp2**

– Volume size 1 GiB – 16 TiB.

– Max IOPS/volume 16,000.

**SSD, Provisioned IOPS – i01**

– Volume size 4 GiB – 16 TiB.

– Max IOPS/volume 64,000.

– **HDD, Throughput Optimized – (st1)**

– Volume size 500 GiB – 16 TiB.

Throughput measured in MB/s, and includes the ability to burst up to 250 MB/s per TB, with a baseline throughput of 40 MB/s per TB and a maximum throughput of 500 MB/s per volume.

**HDD, Cold – (sc1)**

– Volume size 500 GiB – 16 TiB.

Lowest cost storage – cannot be a boot volume.

– These volumes can burst up to 80 MB/s per TB, with a baseline throughput of 12 MB/s per TB and a maximum throughput of 250 MB/s per volume

HDD, Magnetic – Standard – cheap, infrequently accessed storage – lowest cost storage that can be a boot volume.

SSD, General Purpose (GP2) – 3 IOPS / GB

Provisioned IOPS (Io1)  - 50 IOPS per GiB

Throughput Optimized HDD (ST1) - 500 IOPS per volume

 Cold HDD (SC1)-  250 IOPS per volume

***Programmatic API calls to IAM ->***

AWS recommend that you use the AWS SDKs to make programmatic API calls to IAM. However, you can also use the IAM Query API to make direct calls to the IAM web service. An access key ID and secret access key must be used for authentication when using the Query API.

\*\* (AWS SDK, API Query, access key ID and secrete access key these three things is needed)

***How to assign Limited-privilege credentials for IAM users or for users that you authenticate (such as federated users from an on-premise directory). - >***

*STS SAML*

\*\*\*For monitoring the instance in one in 1-minute period – Enable detailed monitoring

CloudTrail trail in the management account with the organization trails option enabled -> this will create the trail in all AWS accounts within the organization.

Member accounts can see the organization trail but can't modify or delete it. By default, member accounts don't have access to the log files for the organization trail in the Amazon S3 bucket.

\*\*\* If any processing related question for AWS lambda – lambda execution time is 15 min. if in question execution time is more than 15 min that means lambda is not right choice

**\*\*\*\* Apex or naked domain names = Alias record**

**\*\*\*\*Message Passing Interface (MPI) protocol= AWS Batch**

***Q -*** A company has deployed an API using Amazon API Gateway. There are many repeat requests and a solutions architect has been asked to implement measures to reduce request latency and the number of calls to the Amazon EC2 endpoint.

How can this be most easily achieved?

**CORRECT:**"Create a cache for a stage and configure a TTL" is the correct answer.

**INCORRECT:** "Create a cache for a method and configure a TTL" is incorrect. An API cache is not enabled for a method, it is enabled for a stage.

***\*\*\* Catching is configured with stage not for method***

1. [**Backup and restore**](https://aws.amazon.com/backup-recovery/)**.** This simple and low cost DR approach backs up your data and applications from anywhere to the AWS cloud for use during recovery from a disaster. Unlike conventional backup methods, data is not backed up to tape. [Amazon Elastic Compute Cloud](https://aws.amazon.com/ec2/)(Amazon EC2) computing instances are only used as needed for testing. With [Amazon Simple Storage Service](https://aws.amazon.com/s3/) (Amazon S3), storage costs are as low as $0.015/GB stored for infrequent access. [Learn more about backup and restore](https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-ii-backup-and-restore-with-rapid-recovery/).
2. **Pilot light.** The idea of the pilot light is an analogy that comes from gas heating. In that scenario, a small flame that’s always on can quickly ignite the entire furnace to heat up a house. In this DR approach, you simply replicate part of your IT structure for a limited set of core services so that the AWS cloud environment seamlessly takes over in the event of a disaster. A small part of your infrastructure is always running simultaneously syncing mutable data (as databases or documents), while other parts of your infrastructure are switched off and used only during testing. Unlike a backup and recovery approach, you must ensure that your most critical core elements are already configured and running in AWS (the pilot light). When the time comes for recovery, you can rapidly provision a full-scale production environment around the critical core. [Learn more about pilot light](https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-iii-pilot-light-and-warm-standby/).
3. **Warm standby.** The term warm standby is used to describe a DR scenario in which a scaled-down version of a fully functional environment is always running in the cloud. A warm standby solution extends the pilot light elements and preparation. It further decreases the recovery time because some services are always running. By identifying your business-critical systems, you can fully duplicate these systems on AWS and have them always on. [Learn more about warm standby](https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-iii-pilot-light-and-warm-standby/).
4. **Multi-site.** A multi-site solution runs on AWS as well as on your existing on-site infrastructure in an active- active configuration. The data replication method that you employ will be determined by the recovery point that you choose, either Recovery Time Objective (the maximum allowable downtime before degraded operations are restored) or Recovery Point Objective (the maximum allowable time window whereby you will accept the loss of transactions during the DR process).

\*\*\*\*Two methods are available for accessing and querying the properties of an EC2 instance such as instance ID, public keys and network interfaces -

**CORRECT:**"Run the command “curl http://169.254.169.254/latest/meta-data/”" is a correct answer.

**CORRECT:**"Download and run the Instance Metadata Query Tool" is also a correct answer.

**"Dedicated Instance" = Billing per Instance**

**“Dedicated Host” = Billing per host**

***Q -*** The application causes the instance to freeze regularly. Then, the instance has to be manually restarted via the AWS management console.

Which of the following is the MOST cost-optimal and resource-efficient way to implement an automated solution until a permanent fix is delivered by the development team?

Correct option:

**Setup a CloudWatch alarm to monitor the health status of the instance. In case of an Instance Health Check failure, an EC2 Reboot CloudWatch Alarm Action can be used to reboot the instance**

***IMP \*\*\*\*\*\*\*\*\*\*\*\*\*\**** an IAM user with full administrator access can perform almost all AWS tasks except a few tasks designated only for the root account user. Some of the AWS tasks that only a root account user can do are as follows: change account name or root password or root email address, change AWS support plan, close AWS account, enable MFA on S3 bucket delete, create Cloudfront key pair, register for GovCloud.

**\*\*\*\*\*\*\*\*\* Create an Application Load Balancer**

Application Load Balancer can automatically distribute incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions. It can handle the varying load of your application traffic in a single Availability Zone or across multiple Availability Zones.

If your application is composed of several individual services, an Application Load Balancer can route a request to a service based on the content of the request.

Here are the different types -

Host-based Routing: You can route a client request based on the Host field of the HTTP header allowing you to route to multiple domains from the same load balancer. You can use host conditions to define rules that route requests based on the hostname in the host header (also known as host-based routing). This enables you to support multiple domains using a single load balancer. Example hostnames: example.com test.example.com \*.example.com The rule \*.example.com matches test.example.com but doesn't match example.com.

Path-based Routing: You can route a client request based on the URL path of the HTTP header. You can use path conditions to define rules that route requests based on the URL in the request (also known as path-based routing). Example path patterns: /img/\* /img//pics The path pattern is used to route requests but does not alter them. For example, if a rule has a path pattern of /img/, the rule would forward a request for /img/picture.jpg to the specified target group as a request for /img/picture.jpg. The path pattern is applied only to the path of the URL, not to its query parameters.

HTTP header-based routing: You can route a client request based on the value of any standard or custom HTTP header.

HTTP method-based routing: You can route a client request based on any standard or custom HTTP method.

Query string parameter-based routing: You can route a client request based on query string or query parameters.

Source IP address CIDR-based routing: You can route a client request based on source IP address CIDR from where the request originates.

Path based routing and host based routing are only available for the Application Load Balancer (ALB). Therefore this is the correct option for the given use-case

**Create a Network Load Balancer** - Network Load Balancer is best suited for use-cases involving low latency and high throughput workloads that involve scaling to millions of requests per second. Network Load Balancer operates at the connection level (Layer 4), routing connections to targets - Amazon EC2 instances, microservices, and containers – within Amazon Virtual Private Cloud (Amazon VPC) based on IP protocol data.

**Q - While troubleshooting, a cloud architect realized that the Amazon EC2 instance is unable to connect to the internet using the Internet Gateway.**

**Which conditions should be met for internet connectivity to be established?**

**1 - The network ACLs associated with the subnet must have rules to allow inbound and outbound traffic**

**2- The route table in the instance’s subnet should have a route to an Internet Gateway**

***\*\*\*\*\*\*\*\*\**By default, cross-zone load balancing is enabled for Application Load Balancer and disabled for Network Load Balancer**

Q - Which of the following AWS database engines can be configured with IAM Database Authentication?

**RDS MySQL**

**RDS PostGreSQL**

IAM database authentication works with MySQL and PostgreSQL engines for Aurora as well as MySQL, MariaDB and RDS PostgreSQL engines for RDS.

ProvisionedThroughputExceededException on KDS = **Use batch messages**

Which of the following is a custom metric in CloudWatch which you have to manually set up? ->

You need to prepare a custom metric using CloudWatch Monitoring Scripts which is written in Perl. You can also install CloudWatch Agent to collect more system-level metrics from Amazon EC2 instances. Here's the list of custom metrics that you can set up:

- Memory utilization  
- Disk swap utilization  
- Disk space utilization  
- Page file utilization  
- Log collection

**Message broker service OR industry-standard APIs and protocols = MQ**

New relational database is needed that autoscales capacity to meet the needs of the application's peak load and scales back down when the surge of activity is over. -?

**Launch an Amazon Aurora Serverless DB cluster then set the minimum and maximum capacity for the cluster.**

**Temporary credentials are useful in scenarios that involve identity federation, delegation, cross-account access, and IAM roles = Temporary credentials = STS**

Amazon API Gateway and increase in site visitors or increase in traffic = Think about

**Enabling throttling limits and result caching in API Gateway**

Authenticate to your instance where database is running = AWS Identity and Access Management (IAM) database authentication (enabling **IAM DB Authentication)**

Whenever there is a schema change in the database = DynamoDB

 Whenever you see "analytics" or OLAP, always consider Redshift.

Ideal for large, sequential cold-data workloads OR require infrequent access to your data and are looking to save costs = **Cold HDD**

Q - An accounting application uses an RDS database configured with Multi-AZ deployments to improve availability. What would happen to RDS if the primary database instance fails?

 (CNAME) will be switched from primary to Standby

Open-source platform in Containerised service = EKS, its open sourced

-> Prerequisites for routing traffic to a website that is hosted in an Amazon S3 Bucket:

**1-** An S3 bucket that is configured to host a static website. The bucket must have the same name as your domain or subdomain. For example, if you want to use the subdomain portal.tutorialsdojo.com, the name of the bucket must be portal.tutorialsdojo.com.

**2-** A registered domain name. You can use Route 53 as your domain registrar, or you can use a different registrar.

IP addresses whitelisted **OR** clients can only access trusted IP addresses **OR** One IP address only = Think About

**Elastic IP address and Network Load Balancer.**

**IMP Point on EBS -** EBS volumes support live configuration changes while in production which means that you can modify the volume type, volume size, and IOPS capacity without service interruptions.

**IMP Point on SQS –** we can use SQS to decouple both on-premise and cloud infrastructure

**Capture, transform, and load** streaming data =**Amazon Kinesis Data Firehose**

**Account password policy or forcing password policy to AWS Account = AWS Config**