Question 1

An IT company uses Scaling policies to maintain an exact number of Amazon EC2 instances in different Availability zones as per application workloads. The developer team has developed a new version of the application for which a new AMI needs to be updated to all the instances. For this, you have been asked to ensure that instances with previous AMI are phased out quickly.

Which termination criteria best suits the requirement?

- A. Specify termination criteria using “ClosestToNextInstanceHour” predefined termination policy
- B. Specify termination criteria using “OldestInstance” predefined termination policy
- C. Specify termination criteria using “AllocationStrategy” predefined termination policy
- D. Specify termination criteria using “OldestLaunchTemplate” predefined termination policyright

Explanation:

Correct Answer: D

Amazon EC2 Auto Scaling uses termination policies that determine which Amazon EC2 instance to be terminated first. Based upon different criteria, it terminates instances. Following are some of the pre-defined termination policies.

1. Default
2. AllocationStrategy
3. OldestLaunchTemplate
4. OldestLaunchConfiguration
5. ClosestToNextInstanceHour
6. NewestInstance
7. OldestInstance

In the above case, the company needs to phase out instances with older versions of AMI. For this, a predefined termination policy with a terminate instance based on OldestLaunchTemplate can be used.

- Option A is incorrect as this policy will terminate the instance closest to the billing cycle. This policy ensures maximizing the use of the instance with an hourly billing cycle.
- Option B is incorrect as this policy will terminate the oldest instance in a group. This policy will be useful for replacing older instances with new instances.
- Option C is incorrect as “AllocationStrategy” termination is useful while rebalancing the number of EC2 instances in an Auto scaling policy to align to the allocation strategy for the terminating instance.

For more information on controlling instance termination using Amazon EC2 Auto Scaling, refer to the following URL,

- https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-termination-policies.html

Question 2

A large engineering company plans to deploy a distributed application with Amazon Aurora as a database. The database should be restored with a Recovery Time objective (RTO) of one minute when there is a service degradation in the primary region. The service restoration should incur the least admin work.

What approach can be initiated to design an Aurora database to meet cross-region disaster recovery requirements?

- A. Use Amazon Aurora Global Database and use the secondary region as a failover for service degradation in the primary regionright
- B. Use Multi-AZ deployments with Aurora Replicas which will go into failover to one of the Replicas for service degradation in the primary region

- C. Create DB Snapshots from the existing Amazon Aurora database and save them in the Amazon S3 bucket. Create a new database instance in a new region using these snapshots when service degradation occurs in the primary region

- D. Use Amazon Aurora point-in-time recovery to automatically store backups in the Amazon S3 bucket. Restore a new database instance in a new region when service degradation occurs in the primary region using these backups

Explanation:

Correct Answer: A
For distributed applications, Global databases can be used. With this, Amazon Aurora spans a single database across multiple regions. This enables fast reads from each region and helps quick cross-region disaster recovery. With the Global database, failover to the secondary region can be completed with an RTO of one minute from the degradation or complete failures in the primary region.

- Option B is incorrect as this will work only in case of service impact with one of the Availability Zones. It won't work for regional outages.
- Option C is incorrect as creating a new DB instance with snapshots will involve manual work in provisioning the instance which will delay service restoration.
- Option D is incorrect as although these backups are automated using Amazon Aurora point-in-time recovery, restoration to another region will result in delay in service restoration.

For more information on Amazon Aurora Global Database, refer to the following URLs,

- https://aws.amazon.com/rds/aurora/global-database/
- https://aws.amazon.com/rds/aurora/features/
- https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database.html

Question 3

A financial company has deployed a business-critical application on an Amazon EC2 instance front-ended by an internet-facing Application Load Balancer. AWS WAF is used with Application Load Balancer for securing this application. The security team is looking to protect the expensive computational resources of the application specifically. The requests to these resources should be limited to a threshold number of sessions beyond which all the requests should be dropped.

Which security policy can be designed to get the required protection for the application?

- A. Create AWS WAF blanket rate-based rules and attach them to the Application Load Balancer

- B. Create AWS WAF URI-specific rate-based rules and attach them to the Application Load Balancer right
- C. Create AWS WAF IP reputation rate-based rules and attach them to the Application Load Balancer

- D. Create AWS WAF Managed rule group statements and attach them to the Application Load Balancer

Explanation:

Correct Answer: B

A rate-based rule tracks the rate of the request from the source IP address and takes action once the limits are crossed. Following are customized rate-based rules which can be used for application protection,

1. Blanket rate-based rule: Prevents source IP address from making excessive requests to entire applications.
2. URI-specific rate-based rule: Prevents IP address from making excessive requests to the URI (Uniform Request Identifier) of the application. These are useful if specific functions of the applications, such as computationally expensive resources need to be protected from excessive requests.
3. IP reputation rate-based rule: Prevents well-known malicious IP addresses from making excessive requests to the application.

All the above three rules can be combined or can be used separately as per need.

In the above scenario, the company is looking to limit the number of requests to the heavy computational resources of the application. This can be achieved by creating URI-specific rate-based rules and attaching them to the Application Load Balancer. This rule would track the number of requests made to the URI (Uniform Request Identifier) of the application such as database query or search function and block the requests once threshold values are crossed.

- Option A is incorrect as blanket rate-based rules will be useful to block source IP addresses that excessively make requests to the entire application. These rules will not be useful for blocking excessive requests to the URI of the application.
- Option C is incorrect as IP Reputation rate-based rules will be more useful for limiting traffic from well-known malicious IP sources.
- Option D is incorrect as Managed rules group would not track the rate of the request and take action.

For more information on AWS WAF rate-based rules, refer to the following URLs,

- https://aws.amazon.com/blogs/security/three-most-important-aws-waf-rate-based-rules/
- https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statements-list.html

Question 4

An IT company has recently deployed highly available resilient web servers on Amazon EC2 instances. Application Load Balancers are used as the front-end to these instances. The company has deployed a lower-capacity web server at the on-premises data center. IT Head wants to have Amazon EC2 instances in AWS Cloud as primary and web servers at the data center as secondary. You will be using Amazon Route 53 to configure this failover.

How can Amazon Route 53 health checks be designed to get the required results?

- A. For primary resources in the AWS Cloud, create alias records and set Evaluate Target Health to Yes. For secondary records, create a health check in Route 53 for web servers in the data center. Create a single failover alias record for both primary and secondary resources

- B. For primary resources in the AWS Cloud, create alias records and health checks. For secondary records, create a health check in Route 53 for web servers in the data center. Create a single failover alias record for both primary and secondary resources

- C. For primary resources in the AWS Cloud, create alias records and set Evaluate Target Health to Yes. For secondary records, create a health check in Route 53 for web servers in the data center. Create two failover alias records for each primary and secondary resourceright
- D. For primary resources in the AWS Cloud, create alias records and health checks. For secondary records, create a health check in Route 53 for web servers in the data center. Create two failover alias records for each primary and secondary resource

Explanation:

Correct Answer: C
Amazon Route 53 health checks can be used to configure active-active and active-passive failover configurations.

Active-passive failover configuration can be used when primary resources are available most of the time, and secondary resources are used only in case of primary resources are not available.

For configuring active-passive failover with multiple primary and secondary resources, the following setting can be done.

1. For Primary resources, create an alias record pointing to Application Load Balancer with 'evaluate health check' as yes.
2. For Secondary resources, create health checks for the web servers in the data centers.
3. Create two failover alias records, one for primary and one for secondary resources.

- Option A is incorrect as two failover alias records need to be created and not a single failover alias record.
- Option B is incorrect as for alias records created for the primary resources in the AWS cloud, Evaluate Target Health should be set to Yes. Health checks are not required to be created separately for the primary resources. Also, a single failover alias record is not suitable.
- Option D is incorrect as for alias records created for the primary resources in the AWS cloud, Evaluate Target Health should be set to Yes. Health checks are not required to be created separately for the primary resources.

For more information on health checks for active-passive failover with multiple resources, refer to the following URL,

- https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html

Question 5

A start up firm has a large number of applications servers hosted on VMs (virtual machines) associated with VMware vCenter at the on-premises data center. Each of these VMs has different operating systems. They are planning to host these servers in the AWS Cloud. For estimating Amazon EC2 sizing in the AWS Cloud, the IT Team is looking for the resource utilization from on-premises servers which should include key parameters like CPU, disk, memory, and network. This data should be saved in an encrypted format and shared with the SME (Subject Matter Expert) working on this migration.

Which method is best suited to get these server details?

- A. Use Agentless-discovery method with AWS Application Discovery Serviceright
- B. Use Agentless-discovery method with AWS Server Migration Service
- C. Use Agent-based discovery method with AWS Server Migration Service
- D. Use Agent-based discovery method with AWS Application Discovery Service

Explanation:

Correct Answer: A

AWS Application Discovery Service collects data from existing servers at on-premises which can be used by the customers to understand server configurations, usage, and behavior. It gathers various server parameters such as CPU, disk, memory, and network. This collected data is encrypted in transit as well as at rest. These parameters can be discovered in any of the following two ways.

1. Agentless Discovery: This is suited for VMware hosts. With this method, an OVA (Open Virtual Appliance) needs to be deployed on a VM host associated with VMware vCenter. No additional software is required to discover the required parameters. This agent can collect the required information irrespective of the operating systems installed on the VMs.

2. Agent-based Discovery: Agent-based discovery is suitable for collecting data for hosts other than VMware hosts. With this, agents are deployed on machines having Windows, Linux, Ubuntu, CentOS, and SUSE operating systems.

- Option B is incorrect as AWS Server Migration Service performs migration of the application from on-premises to AWS Cloud. It's not the service to identify server parameters such as CPU, and memory of the on-premises servers. For migrating VMware hosts to the Amazon EC2 instance, AWS Server Migration Service Connector can be used.
- Option C is incorrect as AWS Server Migration Service performs migration of the application from on-premises to AWS Cloud. It's not the service to identify server parameters such as CPU, and memory of the on-premises servers.
- Option D is incorrect as Agent-based discovery with AWS Application Discovery Service is best For more information on AWS Application Discovery Service, refer to the following URL,
- https://aws.amazon.com/application-discovery/faqs/

Question 6

A company has SQL Servers at the on-premises location which they are planning to migrate to AWS Cloud. This migration should be non-disruptive with minimal downtime. Prerequisite tests should be performed, and results should be captured before servers in AWS are elevated as primary servers.

What cost-effective automated tool can be used to perform SQL server migration?

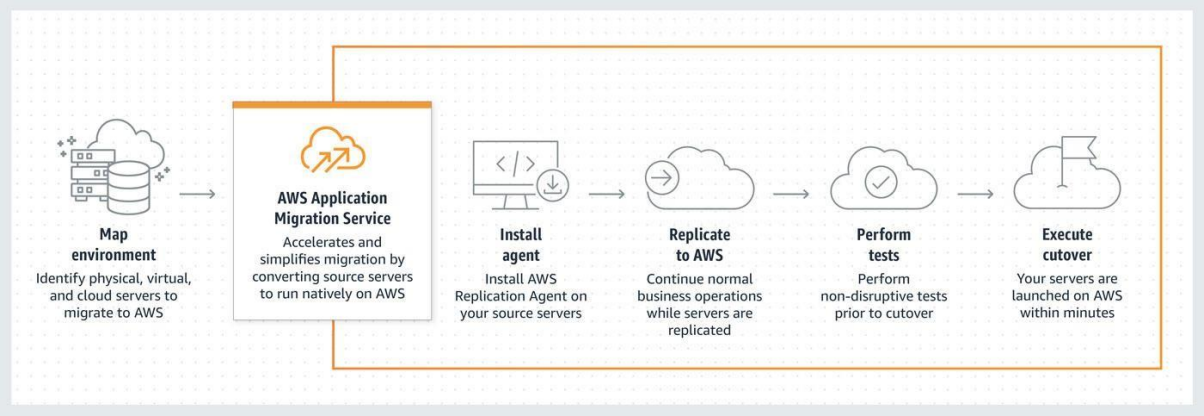
- A. AWS Migration Hub
- B. AWS Application Migration Serviceright
- C. AWS DataSync
- D. AWS Server Migration Service

Explanation:

Correct Answer: B

AWS Application Migration Service can be used to migrate on-premises servers to AWS. It supports applications such as SAP, Oracle, and SQL server migrations to AWS Cloud. While using AWS Application Migration Service, there is no need to have any application-specific experts to perform migration or have multiple migration solutions to be designed.

This allows us to save costs while migrating critical applications to the cloud. With AWS Application Migration Service, data from source servers is first replicated to AWS. Post data is replicated to AWS; tests are performed to ensure application performance from the AWS cloud, and once tests are passed, cutover is performed. This ensures a small cutover window without any disruption to application performance.



- Option A is incorrect as AWS Migration Hub is a suite of tools that simplify migration from on-premises to AWS Cloud. Tools such as AWS Application Migration Service, AWS Server Migration Service, AWS Database Migration Service, and ATADATA ATAmotion are integrated with AWS Migration Hub. AWS Migration Hub can be used to track the migration activity performed by each of these tools.
- Option C is incorrect as AWS DataSync can be used to migrate data from on-premises to one of the AWS storage services. This service cannot be used to migrate SQL Server from on-premises to AWS.
- Option D is incorrect as AWS Server Migration Service uses snapshot-based replication which makes a cutover migration window in hours. AWS Application Service uses block-level replication which makes a cutover migration window in minutes. AWS server migration service is free to use, but it can be used only till March 2023. For AWS Application migration services, there is a cost per server post initial free period. It is recommended to use AWS Server Migration Service only in regions where AWS Application Migration service is unavailable.

For more information on AWS Application Migration Service, refer to the following URLs,

- https://aws.amazon.com/application-migration-service/faqs/
- https://aws.amazon.com/application-migration-service/

Question 7

A finance company is using Amazon S3 to store data for all its customers. During an annual audit, it was observed that sensitive data is stored by some of the customers. Operations Head is looking for an automated tool to scan all data in Amazon S3 buckets and create a report based on the findings from all the buckets with sensitive data.

Which solution can be designed to get the required details?

- A. Enable Amazon GuardDuty on the Amazon S3 buckets
- B. Enable Amazon Detective on the Amazon S3 buckets
- C. Enable Amazon Macie on the Amazon S3 bucketsright
- D. Enable Amazon Inspector on the Amazon S3 buckets

Explanation:

Correct Answer: C

Amazon Macie uses machine learning and pattern matching to discover, monitor, and protect sensitive data stored in Amazon S3 buckets.

Once Amazon Macie is enabled on the Amazon S3, it first generates an inventory of S3 buckets. It automatically discovers and reports any sensitive data stored in an Amazon S3 bucket by creating and

running sensitive data discovery jobs. It further provides a detailed report for any findings with respect to the sensitive data. These jobs can be initiated at periodic intervals or just once on-demand basis.

- Option A is incorrect as Amazon GuardDuty protects against the use of compromised credentials or unusual access to Amazon S3. It does not scan data in Amazon S3 buckets to find any sensitive data stored in it.
- Option B is incorrect as Amazon Detective analyses and visualizes security data from AWS security services such as Amazon GuardDuty, Amazon Macie, and AWS Security Hub to get the root cause of the potential security issues. It does not scan data in Amazon S3 buckets to find any sensitive data stored in it.
- Option D is incorrect as Amazon Inspector evaluates Amazon EC2 instance for any software vulnerability or network exposure. It does not scan data in Amazon S3 buckets to find any sensitive data stored in it.

For more information on Amazon Macie, refer to the following URL,

- https://docs.aws.amazon.com/macie/latest/user/what-is-macie.html

Question 8

An online photo printing company is planning to free up on-premises IT resources by moving all its data to Amazon S3 buckets. This data is around 50 TB in size. All the data must be processed using a customized AWS Lambda function before storing them into the Amazon S3 bucket.

Which design approach is best suited for this data transfer?

- A. Migrate data using AWS Snowball Edgeright
- B. Migrate data using AWS Snowcone
- C. Migrate data using AWS Transfer Family with FTPS
- D. Migrate data using AWS Snowcone SSD

Explanation:

Correct Answer: A

AWS Snowball Edge is a data transfer device having onboard storage and compute capabilities. It supports data processing with AWS compute services like AWS Lambda. AWS Snowball Edge comes in the following flavors:

1. Snowball Edge Storage Optimized (for data transfer): Supports 100 TB (80TB usable) storage capacity.
2. Snowball Edge Storage Optimized (with EC2 compute functionality): 80 TB of usable storage along with 40 vCPUs, and 80 GiB of memory for computing functionality. Additional 1 TB of SSD storage.
3. Snowball Edge Compute Optimized: 42 TB (39.5 TB usable) storage along with 52 vCPUs, and 208 GiB of memory for computing functionality. Additional 7.68 TB of SSD storage.
4. Snowball Edge Compute Optimized with GPU: Same specifications as that of Snowball Edge Compute Optimized with additional GPU (Graphics Processing Unit).

- Option B is incorrect as AWS Snowcone supports data collection and data processing using AWS compute services but supports only 8 TB of HDD-based hard disk. It's not the best option for transferring 50 TB of data, as it will require multiple iterations of offline data transfer. Computing with AWS Lambda is not supported with AWS Snowcone.
- Option C is incorrect as AWS Transfer Family supports the transfer of files over SFTP, FTPS, and FTP from and into Amazon S3 and Amazon EFS.

- Option D is incorrect as AWS Snowcone SSD supports data collection and data processing using AWS compute services but supports only 14 TB of storage. It's not the best option for transferring 50 TB of data, as it will require multiple iterations of offline data transfer. Computing with AWS Lambda is not supported with AWS Snowcone SSD.

For more information on AWS Snowball Edge, refer to the following URLs,

- https://docs.aws.amazon.com/snowball/latest/developer-guide/device-differences.html
- https://aws.amazon.com/snowball/faqs/
- https://aws.amazon.com/aws-transfer-family/faqs/?nc=sn&loc=6

Question 9

Utopia Municipality Corporation runs its application used for the local citizen in EC2 while its database is still in an on-premise data center. The Organization is adamant about not migrating its Database to AWS due to regulatory compliances. However, they are willing to extend the database to the cloud to serve all other AWS services. The organization is looking for a solution by which all AWS services can communicate seamlessly to their on-premises Database without migrating or hosting it in the cloud.

You are hired as a Solutions Architect to help the customer achieve this and also ensure a region-specific, friction-less, low-latency fully managed environment for a truly consistent hybrid experience.

Which of the following would you recommend?

- A. AWS Outposts right
- B. Use AWS Snowball Edge to copy the data and upload to AWS
- C. AWS DataSync
- D. AWS Storage Gateway

Explanation:

Correct Answer: A

- Option A is CORRECT. AWS Outposts delivers AWS infrastructure and services to virtually any on-premises or edge location that provides a truly consistent hybrid experience. It is a fully managed solution.

With AWS Outposts, you can run some AWS services locally and connect to a broad range of services available in the local AWS Region requiring low latency access to on-premises systems, local data processing, data residency, and application migration with local system interdependencies.

- Option B is incorrect because AWS Snowball Edge is a data migration service that copies on-premises data to AWS S3, and the organization is against data migration to AWS. In addition, the requirement will not be served through the static data in S3 as this will miss the latest data update in the on-prem database.
- Option C is incorrect because AWS DataSync is an online data transfer service that simplifies, automates, and accelerates moving data rapidly over the network into Amazon S3, Amazon EFS, FSx for Windows File Server, FSx for Lustre, or FSx for OpenZFS. This will also go against customer requirements of not having the data migrated to AWS.
- Option D is incorrect because AWS Storage Gateway is fast and easy to deploy, enabling you to integrate it with your existing environments and access AWS Storage in a frictionless manner. Storage Gateway is mainly used for moving backups to the cloud, using on-premises file shares backed by cloud storage, and providing low-latency access to data in AWS for on-premises applications. So, again, it is not suitable as per the customer requirement.

References:

- https://aws.amazon.com/storagegateway/features/
- https://aws.amazon.com/outposts/

Question 10

A drug research company is receiving sensitive scientific data from multiple sources in different formats. The organization wants to create a Data Lake in AWS to analyze the data thoroughly. Data cleansing is a critical step before the data lands in Date Lake, and all the matching data need to be removed. The solution should also enable secure access to sensitive data using granular controls at the column, row, and cell levels.

You are hired as a Solutions Architect to help them achieve this in real quick time.

Which of the following do you think would resolve the problem?

- A. Amazon Redshift Spectrum
- B. Amazon Redshift
- C. AWS Glue Data Catalog
- D. AWS Lake Formationright

Explanation:

Correct Answer: D

- Option A is incorrect because Amazon Redshift Spectrum is used to query data directly from files in S3. This cannot be used to create Data Lake.
- Option B is incorrect because Amazon Redshift is a Data warehouse service and does not satisfy all the conditions above.
- Option C is incorrect because AWS Glue Data Catalog contains references to data used as sources and targets of your extract, transform, and load (ETL) jobs in AWS Glue. The information in the Glue Data Catalog is used to create and monitor your ETL jobs. This cannot be used to create a Data Lake.
- Option D is CORRECT because using AWS Lake Formation one can easily set up Data Lakes in days satisfying all the above conditions. Lake Formation collects and catalogs data from databases and object storage, moves the data into your new Amazon Simple Storage Service (S3) data lake, uses ML algorithms to clean and classify the data, and secures access to the sensitive data using granular controls at the column, row, and cell-levels.

Reference:

- https://aws.amazon.com/lake-formation/

Question 11

To comply with industry regulations, a Healthcare Institute wants to keep their large volume of lab records in some durable, secure, lowest-cost storage class for an extended period of time (say about five years). The data will be rarely accessed but requires immediate retrieval (in milliseconds) when required. As a Solutions Architect, the Institute wants your suggestion to select a suitable storage class here. Which of the following would you recommend for the given requirement?

- A. Amazon S3 Standard
- B. Amazon S3 Standard-Infrequent Access
- C. Amazon S3 Glacier Instant Retrievalright
- D. AWS S3 One Zone-Infrequent Access

Explanation:

Correct Answer: C

- Option A is incorrect because S3 Standard is not a preferred choice of storage for long-term or archived data. It is costlier among all its S3 storage classes. So, it does not qualify on the cost and time.
- Option B is incorrect because Amazon S3 Standard-IA is also not a preferred choice of storage for long-term or archived data.
- Option C is CORRECT because the Amazon S3 Glacier Instant Retrieval storage class is the lowest-cost storage for long-lived data that is rarely accessed that still needs immediate access like online file-sharing applications, image hosting, etc.

It can save up to 68% if the data is retrieved once in a quarter, compared to S3 Infrequent Access (IA).

- Option D is incorrect because S3 One Zone-IA is a cheaper one, but not quite durable and also not fit for data archival.

Reference:

- https://aws.amazon.com/s3/storage-classes/glacier/instant-retrieval/

Question 12

A media company is planning to host its relational database in AWS. They want a self-managed, low-cost, on-demand auto-scaling database from the RDS family that can handle variable and unpredictable workloads and scales compute capacity up and down based on your application's needs.

Which of the following RDS types will fulfill this requirement?

- A. Amazon Aurora
- B. Amazon RDS for MySQL
- C. Amazon Aurora Serverlessright
- D. Amazon RDS for PostgreSQL

Explanation:

Correct Answer: C

- Option A is incorrect because Amazon Aurora is an advanced RDS offering from AWS to have as a relational DB, but does not have the capability of on-demand auto-scaling as and when load increases or decreases. In this case, Aurora Serverless should be the best choice.
- Option B is incorrect. MySQL with Amazon RDS is widely popular because of its higher performance and reliability, greater security and identity services, more migration support, the broadest and deepest capabilities, lower total cost of ownership, and flexible licensing options. But again, it misses the on-demand auto-scaling capability like the one in Aurora Serverless.
- Option C is CORRECT because Amazon Aurora Serverless is an on-demand, auto-scaling configuration for Amazon Aurora. It automatically starts up, shuts down, and scales capacity up or down based on your application's needs. You can run your database on AWS without managing database capacity.
- Option D is incorrect. PostgreSQL has become the preferred open-source relational database for many enterprise developers and start-ups, powering leading business and mobile applications. But it misses the customer requirement of on-demand auto-scaling capability like the one in Aurora Serverless.

References:

- https://aws.amazon.com/rds/aurora/serverless/
- https://aws.amazon.com/rds/mysql/
- https://aws.amazon.com/rds/postgresql/

Question 13

A popular media company delivers content on News, Sports and Entertainment to the audiences across the globe. The company uses AWS Redshift to analyze petabytes of structured and semi-structured data across their data warehouse, operational database, and Amazon S3 files to activate data-driven decisions and powerful insights. As their petabyte-scale data continues to grow rapidly, the company starts facing bottlenecks around network bandwidth and memory processing (CPU) that result in slow query performance.

As a solution architect in the company, you have to find a solution that will improvise the query performance without increasing the operational overhead and cost. What would you recommend?

- A. Use Amazon S3 Transfer Acceleration to copy the data to a central S3 bucket and then use Redshift Spectrum for the query purpose
- B. Use Amazon Redshift Spectrum to enhance query performance
- C. Use AQUA (Advanced Query Accelerator) for Amazon Redshiftright
- D. Enable and configure caching solutions to expedite query performance using Amazon ElastiCache Memcached

Explanation:

Correct Answer: C

- Option A is incorrect because Amazon S3 Transfer Acceleration is a bucket-level feature that enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. Transfer Acceleration is designed to optimize transfer speeds from across the world into S3 buckets. The objective is to improve the query performance in the existing solution that the customer is already using, which is Redshift.
- Option B is incorrect because Redshift Spectrum is not a query performance enhancer for data stored in Redshift. It is used for querying data directly in S3 files.
- Option C is CORRECT because Advanced Query Accelerator or AQUA for Redshift meets all the above requirements.

Using AQUA, customers can boost the query performance by 10X. It resolves network bandwidth and memory processing (CPU) bottleneck, low cost, and is easy to deploy.

- Option D is incorrect because in-memory caching can boost the query performance and query results can be retrieved from low latency and high throughput in-memory data stores. It does not satisfy the cost and low operational overload factor here.

Reference:

- https://aws.amazon.com/redshift/features/aqua/

Question 14

An organization runs nearly 500 EC2 instances in several accounts across regions.

These EC2 instances are built on custom Amazon Machine Images (AMIs). The organization is concerned about the accidental deletions of AMIs used for production EC2 instances. They want a solution that can help them recover from accidental deletions as soon as they know about it.

Which of the following can be used for the above scenario?

- A. Use Recycle Binright
- B. Use Cloudformation StackSets
- C. Use Elastic Beanstalk

- D. Take a snapshot of the EBS volume attached to all EC2 and later use it to restore the AMIs

Explanation:

Correct Answer: A

- Option A is CORRECT. Recycle Bin, a data recovery feature, is a new feature introduced by AWS that enables one to restore accidentally deleted Amazon EBS snapshots and EBS-backed AMIs. If your resources are deleted, they are retained in the Recycle Bin for a time period that you specify before being permanently deleted.
- Option B is incorrect because AWS CloudFormation StackSets extends the capability of stacks by enabling you to create, update, or delete stacks across multiple accounts and AWS Regions with a single operation. It is never meant to be used to recover a lost asset/service.
- Option C is incorrect because AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS. It is not any feature of EC2 which will be used to recover deleted AMIs.
- A snapshot of the EBS volume may be a possible solution, but it involves a good amount of operational steps of backup and restore. Hence, option D is incorrect.

Reference:

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/recycle-bin-working-with-amis.html

Question 15

An application needs to access resources from another AWS account of another VPC in the same region. Which of the following ensure that the resources can be accessed as required?

- A. Establish a NAT instance between both accounts.
- B. Use a VPN between both accounts.
- C. Use a NAT Gateway between both accounts.
- D. Use VPC Peering between both accounts.right

Explanation:

Correct Answer – D

- Options A and C are incorrect because these are used when private resources are required to access the Internet.
- Option B is incorrect because it's used to create a connection between the On-premises and AWS resources.

AWS Documentation mentions the following about VPC Peering:

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC Peering connection between your own VPCs, with a VPC in another AWS account, or with a VPC in a different AWS Region.

For more information on VPC Peering, please visit the following URL:

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html

Question 16

You are a solutions architect working for a regional bank that is moving its data center to the AWS cloud. You need to migrate your data center storage to a new S3 and EFS data store in AWS. Since your data includes Personally Identifiable Information (PII), you have been asked to transfer data from your data center to AWS without traveling over the public internet. Which option gives you the most efficient solution that meets your requirements?

- A. Migrate your on-prem data to AWS using the DataSync agent using NAT Gateway.

- B. Create a public VPC endpoint, and configure the DataSync agent to communicate to the DataSync public service endpoints via the VPC endpoint using Direct Connect.

- C. Migrate your on-prem data to AWS using the DataSync agent using Internet Gateway.

- D. Create a private VPC endpoint, and configure the DataSync agent to communicate to the DataSync private service endpoints via the VPC endpoint using VPN.right

Explanation:

Correct Answer: D
AWs documentation mentions the following:

While configuring this setup, you'll place a private VPC endpoint in your VPC that connects to the DataSync service. This endpoint will be used for communication between your agent and the DataSync service.
In addition, for each transfer task, four elastic network interfaces (ENIs) will automatically get placed in your VPC. DataSync agent will send traffic through these ENIs in order to transfer data from your on-premises shares into AWS.
"When you use DataSync with a private VPC endpoint, the DataSync agent can communicate directly with AWS without the need to cross the public internet."

- Option A is incorrect. To ensure your data isn't sent over the public internet, you need to use a VPC endpoint to connect the DataSync agent to the DataSync service endpoints.
- Option B is incorrect. You need to use a private VPC endpoint, not the public VPC endpoint to keep your data away from traveling over the public internet.
- Option C is incorrect. Using the Internet Gateway by definition sends your traffic over the public internet, which is the solution as per the requirement.
- Option D is correct. Using a private VPC endpoint and the DataSync private service endpoints to communicate over your VPN will give you the non-internet transfer you require.

References:

- Please see the AWS DataSync user guide titled Using AWS DataSync in a virtual private cloud (https://docs.aws.amazon.com/datasync/latest/userguide/datasync-in-vpc.html), and the AWS Storage Blog titled Transferring files from on-premises to AWS and back without leaving your VPC using AWS DataSync (https://aws.amazon.com/blogs/storage/transferring-files-from-on-premises-to-aws-and-back-without-leaving-your-vpc-using-aws-datasync/)

Question 17

You are a solutions architect working for a financial services firm that operates applications in the hybrid cloud model. You have applications running on EC2 instances in your VPC that communicate with resources in your on-prem data center. You have a workload on an EC2 instance in one subnet and a transit gateway association in a different subnet. Also, these two subnets are associated with different NACLs. You have set up Network Access Control List (NACL) rules to control the traffic to and from your EC2 instances and transit gateway.

Which of the following is true about the NACL rules for traffic from your EC2 instances to the transit gateway?

- A. Outbound rules use the source IP address to evaluate traffic from the instances to the transit gateway.

- B. Outbound rules use the destination IP address to evaluate traffic from the instances to the transit gateway.right

- C. Outbound rules are not evaluated for the transit gateway subnet

- D. Inbound rules use the destination IP address to evaluate traffic from the transit gateway to the instances.

Explanation:

Correct Answer: B
The question asks for the NACL rule when the instances and transit gateway are in different subnets and traffic flows from EC2 instance to transit gateway.

- Option A is incorrect. For traffic outbound from your EC2 instance subnet, the source IP address is not valid, the destination IP address is used to evaluate the rule.
- Option B is correct. This is the required rule NACLs should follow when the instances and transit gateway are in different subnets and the traffic flows from instances to the transit gateway. Network ACL Outbound rules use the destination IP address to evaluate traffic from the instances to the transit gateway.
- Option C is incorrect because when the instances and transit gateway are in different subnets, outbound rules are evaluated and provide the flow of traffic as required.
- Option D is incorrect. For traffic inbound from your transit gateway, the source IP address is used to evaluate the rule.

Different subnets for EC2 instances and transit gateway association

Consider a configuration where you have EC2 instances in one subnet and the transit gateway association in a different subnet, and each subnet is associated with a different network ACL.

Network ACL rules are applied as follows for the EC2 instance subnet:

- Outbound rules use the destination IP address to evaluate traffic from the instances to the transit gateway.
- Inbound rules use the source IP address to evaluate traffic from the transit gateway to the instances.

NACL rules are applied as follows for the transit gateway subnet:

- Outbound rules use the destination IP address to evaluate traffic from the transit gateway to the instances.
- Outbound rules are not used to evaluate traffic from the instances to the transit gateway.
- Inbound rules use the source IP address to evaluate traffic from the instances to the transit gateway.
- Inbound rules are not used to evaluate traffic from the transit gateway to the instances.

References:

- Please see the Amazon Virtual Private Cloud Transit Gateways page titled How Network ACLs work with transit gateways (https://docs.aws.amazon.com/vpc/latest/tgw/tgw-nacls.html), and the Amazon Virtual Private Cloud Transit Gateways page titled How transit gateways work (https://docs.aws.amazon.com/vpc/latest/tgw/how-transit-gateways-work.html)

Question 18

You are a solutions architect working for a media company that produces stock images and videos for sale via a mobile app and website. Your app and website allow users to gain access only to stock content they have purchased. Your content is stored in S3 buckets. You need to restrict access to multiple files that your users have purchased. Also, due to the nature of the stock content (purchasable by multiple users), you don't want to change the URLs of each stock item.

Which access control option best fits your scenario?

- A. Use CloudFront signed URLs

- B. Use S3 Presigned URLs

- C. Use CloudFront Signed Cookiesright
- D. Use S3 Signed Cookies

Explanation:

Correct Answer: C

- Option A is incorrect. CloudFront signed URLs allow you to restrict access to individual files. Signed URLs require you to change your content URLs for each customer access.
- Option B is incorrect. S3 Presigned URLs require you to change your content URLs. The presigned URL expires after its defined expiration date.
- Option C is correct. CloudFront Signed Cookies allow you to control access to multiple content files and you don't have to change your URL for each customer access.
- Option D is incorrect. There is no S3 Signed Cookies feature.

References:

- Please see the Amazon CloudFront developer guide titled Using signed cookies (https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-cookies.html), the Amazon Simple Storage Service user guide titled Sharing an object with a presigned URL (https://docs.aws.amazon.com/AmazonS3/latest/userguide/ShareObjectPreSignedURL.html), the Amazon Simple Storage Service user guide titled Using presigned URLs (https://docs.aws.amazon.com/AmazonS3/latest/userguide/using-presigned-url.html#PresignedUrlUploadObject-LimitCapabilities), and the Amazon CloudFront developer guide titled Choosing between signed URLs and signed cookies (https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-choosing-signed-urls-cookies.html)

Question 19

You are a solutions architect working as a consultant where you build web applications for clients. One of your clients' needs a static website hosted on AWS. The website will predominantly host content files owned by the AWS account used to create the S3 bucket that will host the website. However, some of the objects in the bucket are owned by a parent company's AWS account.

How should you configure the S3 bucket access controls to achieve the most secure website that is accessible to the public? (Choose TWO)

- A. Create a bucket policy that grants s3:GetObject access to the objects owned by the parent company account.
- B. Create a bucket policy that grants s3:GetObject access to the objects in the bucket owned by the account used to create the S3 bucket that will host the website.right
- C. Create an object access control list to grant read permissions on objects owned by the account used to create the S3 bucket that will host the website.
- D. Create an object access control list to grant read permissions on objects owned by the parent company account.right
- E. Create a bucket policy that grants s3:GetObject access to the objects owned by the parent company account and the objects owned by the account used to create the S3 bucket that will host the website.

Explanation:

Correct Answers: B and D

- Option A is incorrect. The objects owned by the parent company account need an access control list that grants read permission to all users. This is because these objects are not controlled by

the bucket policy, since they are not owned by the account used to create the bucket that will host the website.

- Option B is correct. If you create a bucket policy that grants s3:GetObject access to the objects in the bucket owned by the account used to create the bucket, they will become publicly readable.
- Option C is incorrect. You use a bucket policy to control access to objects in the bucket that are owned by the account used to create the bucket. You don't use an ACL for this access control.
- Option D is correct. Since the account used to create the S3 bucket used to host the website is different from the parent company account, you need to use an ACL to control access to the objects owned by the parent company account.

- Option E is incorrect. The bucket policy will control access to objects owned by the account used to create the S3 bucket that will host the website. Your bucket policy can't control access to objects owned by the parent company account. You need to use an ACL to control access to objects owned by the parent company account.

References:

- Please see the Amazon Simple Storage Service user guide titled Setting permissions for website access (https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteAccessPermissionsReqd.html), the Service Authorization reference page titled Actions, resources, and condition keys for Amazon S3 (https://docs.aws.amazon.com/service-authorization/latest/reference/list_amazons3.html)

Question 20

You are a solutions architect working for a media company that produces and stores image and video content that is sold as stock content to other companies that wish to use your stock content in their web and mobile apps. You are storing your stock content in S3 and you need to optimize for cost. Some of your images are small, less than 128 KB in size. However, most of your stock content is much larger. The amount of content you manage is very large, with over 1 million objects in S3. These objects have varying access patterns. Some are accessed frequently, while others are accessed very infrequently. Also, the access patterns for the stock objects change over time.

Which S3 storage class should you choose for your stock content to optimize your costs while also providing the best overall performance?

- A. S3 Standard
- B. S3 Standard-IA
- C. S3 Intelligent-Tieringright
- D. S3 One Zone-IA

Explanation:

Correct Answer: C

- Option A is incorrect. S3 Standard tiering is not a cost-optimized solution. You have a lot of objects and many of them are accessed very infrequently. With S3 Standard, all objects are charged at the same rate, regardless of how often they are accessed.
- Option B is incorrect. S3 Standard-IA, or Infrequent Access, would be a cost-optimized solution for less frequently accessed objects. However, retrieval latency will not be optimal for frequently accessed objects.
- Option C is correct. S3 Intelligent-Tiering gives you the ability to have S3 monitor the access patterns of your objects and move objects across the various storage tiers based on the relevant access patterns. This will give you both cost and performance optimization. Also,

smaller files (less than 128 KB) can be stored in S3 Intelligent-Tiering but they will always remain in the S3 Standard storage class.

- Option D is incorrect. S3 One Zone-IA is used for files that are easily recreated if the one AZ becomes unavailable. Also, an infrequent access tier such as S3 One Zone-IA would be a cost-optimized solution for less frequently accessed objects. However, retrieval latency will not be optimal for frequently accessed objects.

Reference:

- Please see the Amazon Simple Storage Service user guide titled Using Amazon S3 storage classes (https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html)

Question 21

You create several SQS queues to store different types of customer requests. Each SQS queue has a backend node that pulls messages for processing. Now you need a service to collect messages from the frontend and push them to the related queues using the publish/subscribe model. Which service would you choose?

- A. Amazon MQ
- B. Amazon Simple Notification Service (SNS)right
- C. Amazon Simple Queue Service (SQS)
- D. AWS Step Functions

Explanation:

Correct Answer – B

AWS SNS can push notifications to the related SQS endpoints. SNS uses a publish/subscribe model that provides instant event notifications for applications.

- Option A is incorrect: Amazon MQ is a managed message broker service, which is not suitable for this scenario.
- Option B is CORRECT: Because SNS uses Pub/Sub messaging to provide asynchronous event notifications. Please check the link-https://aws.amazon.com/pub-sub-messaging/.
- Option C is incorrect: Because SQS does not use the publish/subscribe model.
- Option D is incorrect: AWS Step Functions coordinate application components using visual workflows. The service should not be used in this scenario.

Question 22

E-Learning platform hosted on AWS provides various online courses to a global audience. They have video lessons and quiz questions for every lesson. They are more customer-centric and always work to improve their services based on the feedback received from their customers. Recently they have seen a surge in the responses where their customers are demanding a feature where they can listen to the questions in the quiz instead of just reading it because they understand it better by listening. It will help the visually impaired learners as well.

Krish, the solutions architect is looking for a solution to introduce this feature to their platform. Which of the following options can fulfil the given requirement?

- A. Use Amazon Rekognition to identify the text from the quiz page and convert it from Text to Speech
- B. Use Amazon Textract to extract the text from the quiz questions and convert it from Text to Speech
- C. Use Amazon Comprehend to use its NLP-based functionality to implement this feature

- D. Use Amazon Polly to implement this feature in the platformright

Explanation:

Correct Answer: D

- Option A is incorrect because Amazon Rekognition is a service with which you can identify objects, people, text, scenes, and activities in images and videos, etc. and also provides highly accurate facial analysis and facial search capabilities that you can use to detect, analyze, and compare faces for various use cases. It can't do the Text to Speech Conversion.
- Option B is incorrect because Amazon Textract is a fully managed machine learning service that automatically extracts printed text, handwriting, and other data from scanned documents. It is for the use cases that go beyond simple optical character recognition (OCR) to identify, understand, and extract data from forms and tables. It can't do the Text to Speech Conversion.
- Option C is incorrect because Amazon Comprehend is a natural-language processing (NLP) service that uses machine learning to uncover valuable insights and connections in text. It is used mainly for sentiment analysis from the given text, but not for text-to-speech conversions.
- Option D is CORRECT because Amazon Polly is a service that turns text into lifelike speech, allowing you to create applications that talk and build entirely new categories of speech-enabled products. So, Krish can easily use Amazon Polly to build the required feature in the platform without any hassle.

References:

- https://aws.amazon.com/polly/
- https://aws.amazon.com/textract/
- https://aws.amazon.com/comprehend/
- https://aws.amazon.com/rekognition/

Question 23

Kayne is instructed by his manager to build a solution to detect whether the visitors entering their office building are wearing a face mask or not. The building has two entrances with CCTVs installed on both. The data needs to be captured from them and sent to AWS for detection and analysis.

He is exploring AWS Services to build this solution efficiently. After some research, he has found that Amazon Kinesis with a combination of Amazon Rekognition can serve the purpose. But he is not aware of what capability in Kinesis will help in this case.
Which of the following Kinesis capabilities is MOST appropriate for the given scenario?

- A. Kinesis Data Firehose
- B. Kinesis Data Analytics
- C. Kinesis Video Streamsright
- D. Kinesis Data Streams

Explanation:

Correct Answer: C

- OPTION A is incorrect because Kinesis Data Firehose is fully managed and used to capture, transform and load the data from various sources into AWS data stores like Amazon S3, Amazon Redshift, etc., data lakes or analytical services. But it doesn't capture the data from the video streaming devices like CCTVs as mentioned in the given scenario.
- OPTION B is incorrect because Kinesis Data Analytics is used to gather streaming data from sources like Kinesis data streams, Amazon S3, IoT devices, etc. It analyzes the data by performing the queries and sends the output to other AWS services or analytical tools. This output can be utilized for creating alerts or responding in real-time. It doesn't capture the video streams as required in the current scenario.

- OPTION C is CORRECT because Kinesis Video Streams is explicitly built for the use cases like video playback, face detection, security monitoring, etc. It can serve the purpose mentioned in the given scenario. The CCTVs will stream the video to Kinesis Video Streams in real-time. It will then ingest and index those streams used for Face detection. After that, you can use Amazon Rekognition Video to perform face detection for mask checking in the streaming video.
- OPTION D is incorrect because Kinesis Data Streams is useful for capturing GBs of real-time data every second from various sources. This data can be further consumed by Kinesis data analytics, Amazon EMR, etc. to query and perform analytics on it. It neither captures the data from Video Streaming devices nor sends it to Amazon Rekognition which was the main requirement in the given scenario.

References:

- https://aws.amazon.com/kinesis/video-streams/
- https://aws.amazon.com/kinesis/

Question 24

A stock broking company has deployed a stock trading web application on the Amazon EC2 instance. The company is looking for virtual agents to be integrated with this application to provide conversational channels to its premium customers. Real-time personalized stock recommendations should be provided for premium customers during market hours.

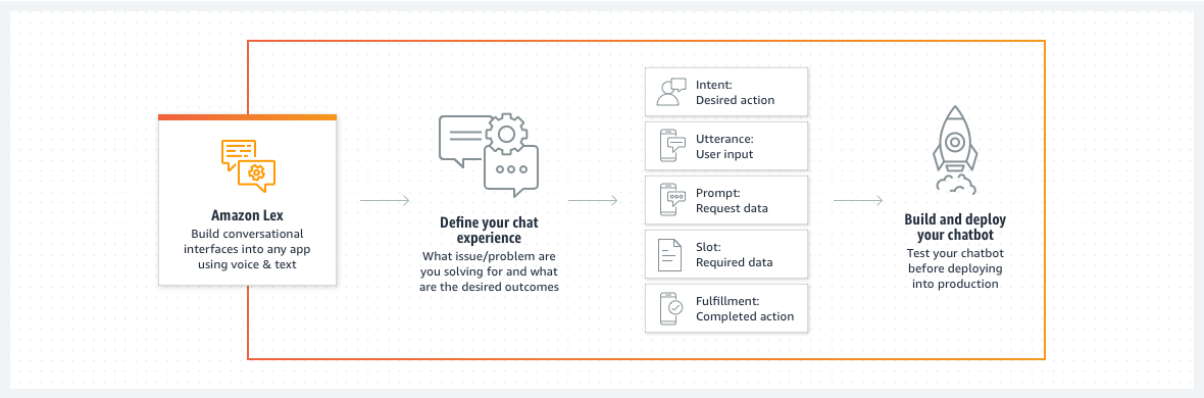
Which service is best suited to integrate with this application?

- A. Amazon Lexright
- B. Amazon Translate
- C. Amazon Transcribe
- D. Amazon Personalize

Explanation:

Correct Answer: A

Amazon Lex is a fully managed AI (Artificial Intelligence) service for creating a conversational interface to the applications. With the prebuilt chatbots integrated with the application, customers can interact with this virtual chat box for queries and personalized recommendations from the capital market.



- Option B is incorrect as Amazon Translate can be used to translate the web application into a language preferred by the users. This service cannot be for creating virtual chat agents with the applications.
- Option C is incorrect as Amazon Transcribe can be used to enhance applications with automated speech recognition. This service cannot be used for creating virtual chat agents with the applications.

- Option D is incorrect as Amazon Personalize can be used to customize applications for each of the users using machine learning but cannot be used for creating virtual chat agents with the applications.

For more information on Amazon Lex, refer to the following URLs,

- https://aws.amazon.com/lex/financial-services/?nc=sn&loc=3&dn=1
- https://aws.amazon.com/machine-learning/ai-services/

Question 25

A large manufacturing company is looking to track IoT sensor data collected from thousands of equipment across multiple factory units. This is extremely high-volume traffic that needs to be collected in real time and should be efficiently visualized. The company is looking for a suitable database in the AWS cloud for storing these sensor data.

Which of the following cost-effective databases can be selected for this purpose?

- A. Send sensor data to Amazon RDS (Relational Database Service) using Amazon Kinesis and visualize data using Amazon QuickSight
- B. Send sensor data to Amazon Neptune using Amazon Kinesis and visualize data using Amazon QuickSight
- C. Send sensor data to Amazon DynamoDB using Amazon Kinesis and visualize data using Amazon QuickSight
- D. Send sensor data to Amazon Timestream using Amazon Kinesis and visualize data using Amazon QuickSightright

Explanation:

Correct Answer: D

Amazon Timestream is the most suitable serverless time series database for IoT and operational services. It can store trillions of events from these sources. Storing this time series data in Amazon Timestream ensures faster processing and is more cost-effective than storing such data in a regular relational database.

Amazon Timestream is integrated with data collection services in AWS such as Amazon Kinesis, and Amazon MSK, and open-source tools such as Telegraf. Data stored in Amazon Timestream can be further visualized using Amazon QuickSight. It can also be integrated with Amazon Sagemaker for machine learning.

- Option A is incorrect as Amazon RDS (Relational Database Service) is best suited for traditional applications such as CRM (customer relationship management) and ERP (Enterprise resource planning). Using Amazon RDS for storing IoT sensor data will be costly and slow as compared to the Amazon Timestream.
- Option B is incorrect as Amazon Neptune is suitable for creating graph databases querying large amounts of data. Amazon Neptune is not a suitable option for storing IoT sensor data.
- Option C is incorrect as Amazon DynamoDB is suitable for web applications supporting key-value NoSQL databases. Using Amazon DynamoDB for storing IoT sensor data will be costly.

For more information on Amazon Timestream, refer to the following URLs,

- https://aws.amazon.com/products/databases/
- https://aws.amazon.com/timestream/features/?nc=sn&loc=2