# Exam #3

Question 2: Correct

Your manager has asked you to deploy a mobile application that can collect votes for a popular singing competition. Millions of users from around the world will submit votes using their mobile phones. These votes must be collected and stored in a highly scalable and highly available data store which will be queried for real-time ranking.

Explanation

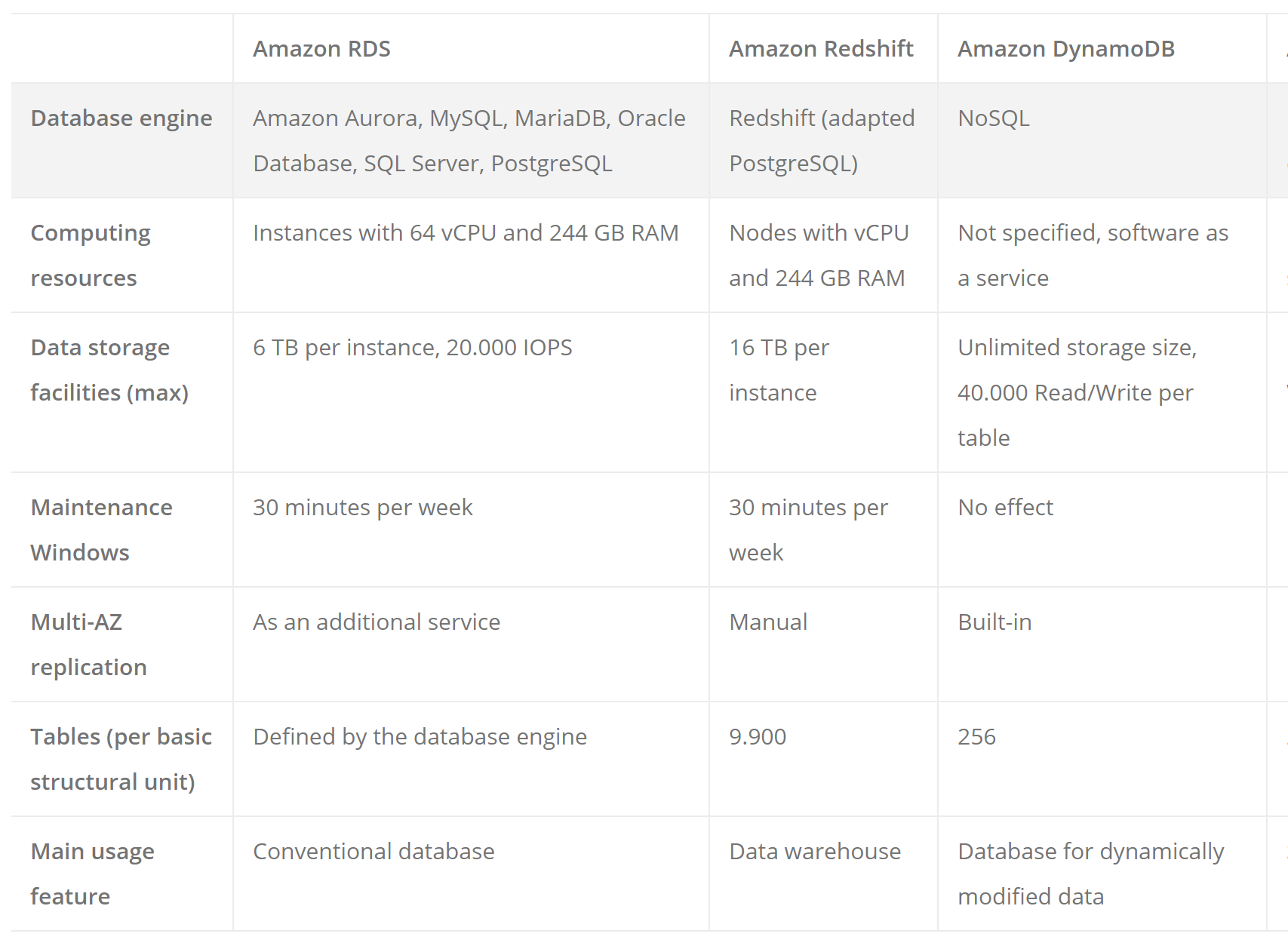
When the word durability pops out, the first service that should come to your mind is Amazon S3. Since this service is not available in the answer options, we can look at the other data store available which is Amazon DynamoDB.

DynamoDB is durable, scalable, and highly available data store which can be used for **real-time tabulation**. You can also use AppSync with DynamoDB to make it easy for you to build collaborative apps that keep shared data updated in real time. You just specify the data for your app with simple code statements and AWS AppSync manages everything needed to keep the app data updated in real time. This will allow your app to access data in Amazon DynamoDB, trigger AWS Lambda functions, or run Amazon Elasticsearch queries and combine data from these services to provide the exact data you need for your app.

RDS vs Redshift vs DynamoDB

<https://www.cloudberrylab.com/resources/blog/aws-database-services-complete-overview-rds-vs-redshift-vs-dynamodb-vs-simpledb/>

* RDS is a good solution for those, who want to run a common database engine with no need for dealing with administration and maintenance. AWS presupposes RDS to be a fully functional alternative to common hardware databases. It is fast, scalable and can be replicated among Availability Zones for greater accessibility.
  + Here are the most typical applications of Amazon RDS:
    - You already have a database with a familiar engine, which needs to be offsite.
    - The platform for an application that requires the database to be fast, durable, scalable or all of these.
    - There is unrationed workflow, which requires a highly scalable database in order to avoid expenses
    - The Data shall be processed quickly without storing too much onsite.
* Redshift is a tool designed to work with data of up to dozens of petabytes. Powered by PostgreSQL, it is mostly applied to any kind of SQL applications with minimum changes. The target feature of the service is creating a data warehouse, where a user may focus on data management without keeping an effortful and complex infrastructure. From the technical point of view, Redshift is a cluster database without such consistency features as a foreign key and the uniqueness of field values. The cluster includes a number of nodes with virtual databases powered by Amazon Elastic Compute Cloud (EC2) instances. Those nodes are basic database units that you can use for your tasks.
  + The most common use cases of Amazon Redshift are as follows:
    - Data warehousing – the name speaks for itself
    - Big corporate or scientific data processing, with loads related to big amounts of data and large computing loads
    - Analytical databases for businesses required to store, analyze and transfer big data within a short time
    - Customer activity monitoring for analysis and statistics
* DynamoDB is a NoSQL database service by AWS designed for fast processing of small data, which dynamically grows and changes. The main non-relative feature of DynamoDB is the unstrict structure of a table – it consists of items (as compared to rows in a traditional table) and attributes (an analog to columns). Carrying over of relational engines, it resembles a table with an individual number of columns in each row. Database mutability and fast I/O rate is powered by an SSD used as the basic (and the only) storage hardware. The multi-AZ feature, which requires an additional fee with RDS, comes from the box here: your data is automatically replicated among 3 Availability Zones (AZ) within the selected region. The total absence of administering activities, data replication, and final-performance scaling models make DynamoDB extremely durable. Meanwhile, DynamoDB doesn’t support such complex functions as advanced querying and transactions. Since data is partitioned for durability, it takes some time to re-write it in each replica after a successful write operation in the main one.
  + In the upshot, the best practices with DynamoDB are the following:
    - Data blocks systematization and processing.
    - Advertising services: the collection of customer data, making trend charts, etc.
    - Messaging and blogging: building message selections, the list of blog entries by author, etc.
    - Gaming: high-scores, world changes, player status, and statistics, etc.
    - Any other case when you have to process data rather than store and the data shall be highly available rather transactable.



Question 3: Correct

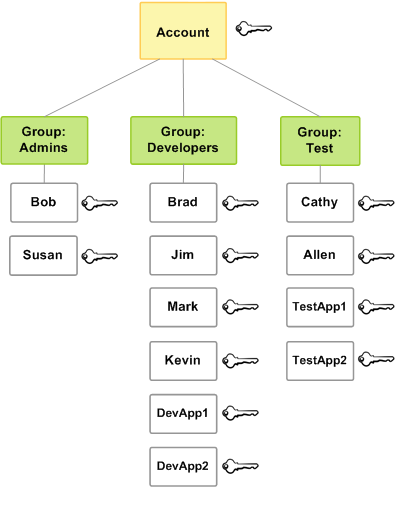
You were recently promoted to a technical lead role in your DevOps team. Your company has an existing VPC which is quite un-utilized for the past few months. The business manager instructed you to integrate your on-premises data center and your VPC. You explained the list of tasks that you'll be doing and mentioned about a Virtual Private Network (VPN) connection. The business manager is not tech-savvy but he is interested to know what a VPN is and its benefits.

What is one of the major advantages of having a VPN in AWS?

Explanation

Option 2 is correct. One main advantage of having a VPN connection is that you will be able to connect your Amazon VPC to other remote networks.

You can create an IPsec VPN connection between your VPC and your remote network. On the AWS side of the VPN connection, a virtual private gateway provides two VPN endpoints (tunnels) for automatic failover. You configure your **customer gateway** on the remote side of the VPN connection. If you have more than one remote network (for example, multiple branch offices), you can create multiple AWS managed VPN connections via your virtual private gateway to enable communication between these networks.



Question 6

You are working for a data analytics company as a Software Engineer, which has a client that is setting up an innovative checkout-free grocery store. You developed a monitoring application that uses smart sensors to collect the items that your customers are getting from the grocery’s refrigerators and shelves then automatically maps it to their accounts. To know more about the buying behavior of your customers, you want to analyze the items that are constantly being bought and store the results in S3 for durable storage. What service can you use to easily capture, transform, and load streaming data into Amazon S3, Amazon Elasticsearch Service, and Splunk?

Explanation

Amazon Kinesis Data Firehose is the easiest way to load streaming data into data stores and analytics tools. It can capture, transform, and load streaming data into Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk, enabling near real-time analytics with existing business intelligence tools and dashboards you are already using today.

It is a fully managed service that automatically scales to match the throughput of your data and requires no ongoing administration. It can also batch, compress, and encrypt the data before loading it, minimizing the amount of storage used at the destination and increasing security.

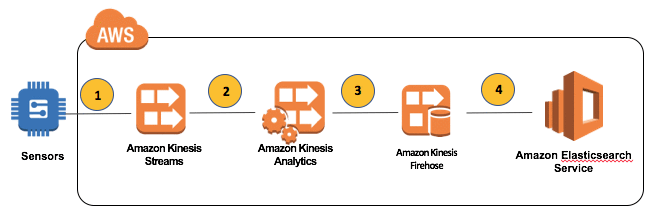
In the diagram below, you gather the data from your smart refrigerators and use Kinesis Data firehouse to prepare and load the data. S3 will be used as a method of durably storing the data for analytics and the eventual ingestion of data for output using analytical tools.



Option 2 is incorrect because Amazon Kinesis is the streaming data platform of AWS and has four distinct services under it: Kinesis Data Firehose, Kinesis Data Streams, Kinesis Video Streams, and Amazon Kinesis Data Analytics. For a specific use case of the requirement by the question, use Kinesis Data Firehose.

Question 13

Kinesis Data Streams supports changes to the data record retention period of your stream. A Kinesis data stream is an ordered sequence of data records meant to be written to and read from in real-time. Data records are therefore stored in shards in your stream temporarily.

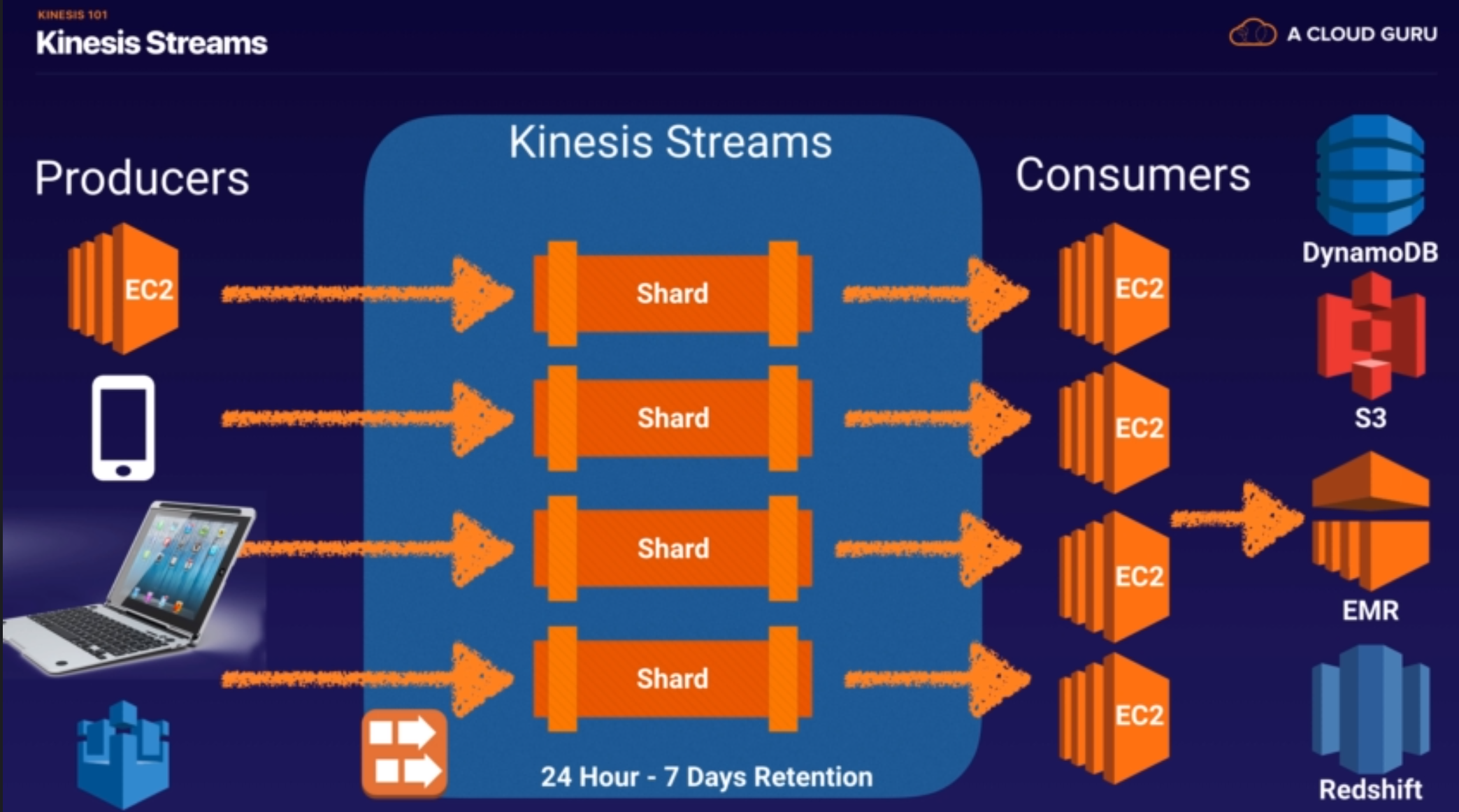


The time period from when a record is added to when it is no longer accessible is called the retention period. A Kinesis data stream stores records from 24 hours by default to a maximum of 168 hours (1 week).

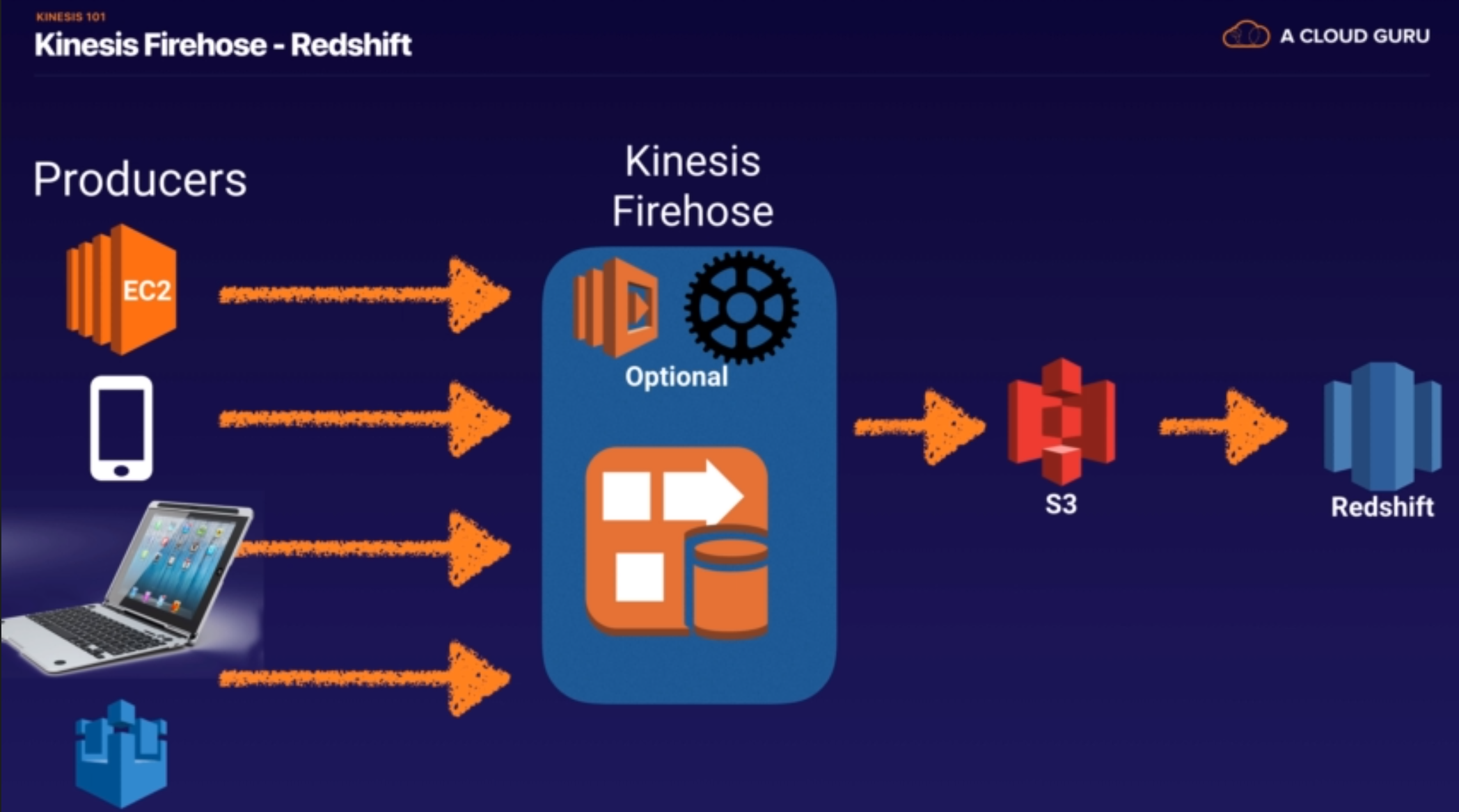
This is the reason why there are missing data in your S3 bucket. To fix this, you can either configure your sensors to send the data everyday instead of every other day or alternatively, you can increase the retention period of your Kinesis data stream.

**Kinesis Data Stream vs Kinesis Data Firehose vs Kinesis Data Analytics:**

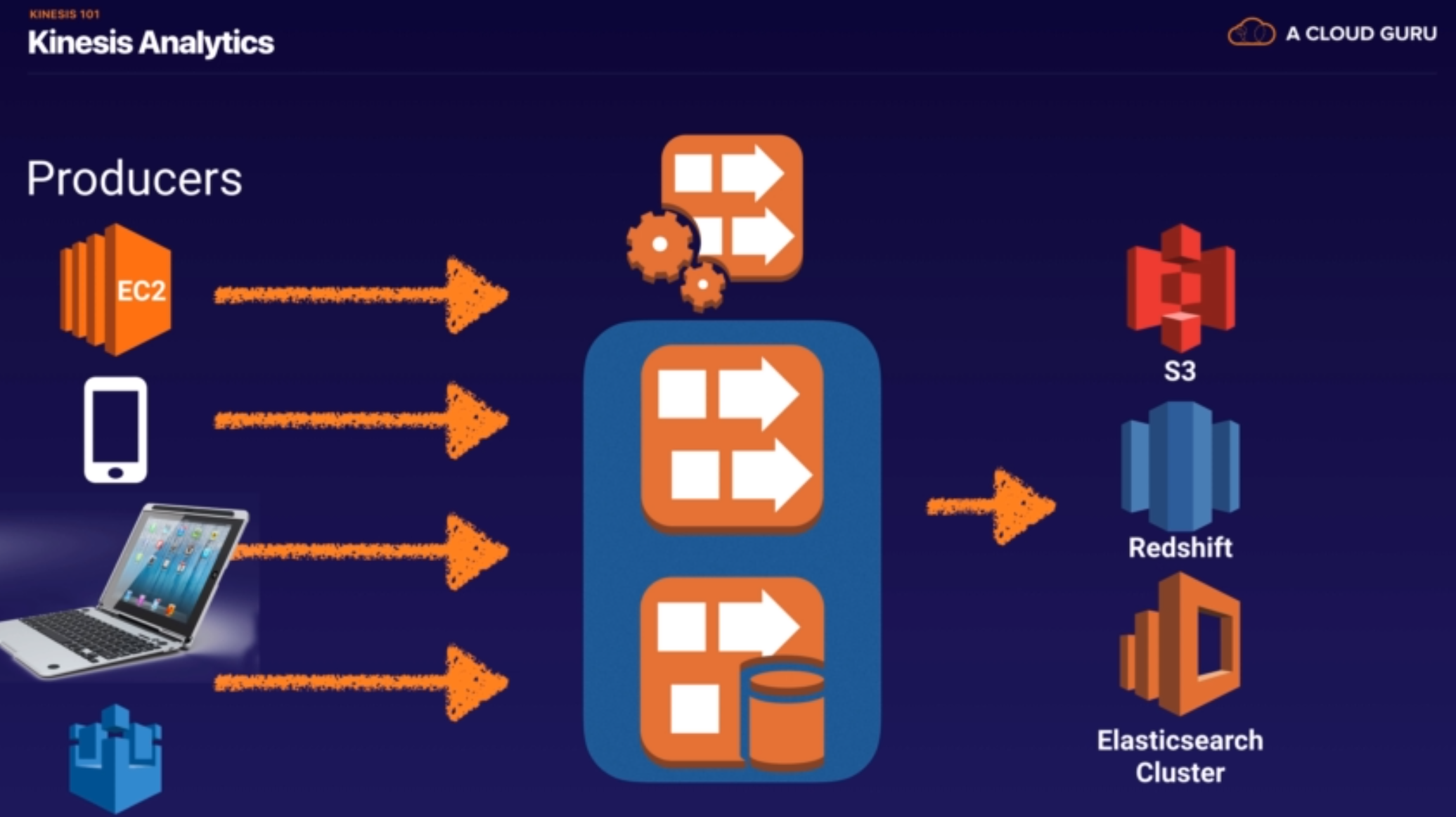
* Kinesis Data Stream: has shards to store the stream data for temporary persistency by default for 24 hours changeable up to 1 week.



* Kinesis Data Firehose: There’s no data persistency; as soon as it receives the data, it has to process by, say Lambda.



* Kinesis Data Analytics: This is to analyze the streaming data as it comes in on the fly. Kinesis Data Analytics can exist inside the Kinesis Data Stream and Kinesis Data Firehose.



Question 10: Incorrect

You are working for a startup as its AWS Chief Architect. You are currently assigned on a project that develops an online registration platform for events, which uses Simple Workflow for complete control of your orchestration logic. A decider ingests the customer name, address, contact number, and email address while the activity workers update the customer with the status of their online application status via email. Recently, you were having problems with your online registration platform which was solved by checking the decision task of your workflow.

In SWF, what is the purpose of a decision task?

Explanation

The decider can be viewed as a special type of worker. Like workers, it can be written in any language and asks Amazon SWF for tasks. However, it handles special tasks called decision tasks.

Amazon SWF issues decision tasks whenever a workflow execution has transitions such as an activity task completing or timing out. A decision task contains information on the inputs, outputs, and current state of previously initiated activity tasks. Your decider uses this data to decide the next steps, including any new activity tasks, and returns those to Amazon SWF. Amazon SWF in turn enacts these decisions, initiating new activity tasks where appropriate and monitoring them.

By responding to decision tasks in an ongoing manner, the decider controls the order, timing, and concurrency of activity tasks and consequently the execution of processing steps in the application. SWF issues the first decision task when an execution starts. From there on, Amazon SWF enacts the decisions made by your decider to drive your execution. The execution continues until your decider makes a decision to complete it.

Check out this Amazon SWF Cheat Sheet:

<https://tutorialsdojo.com/aws-cheat-sheet-amazon-simple-workflow-amazon-swf/>

**Task in SWF:**

* Tasks represent invocations of various processing steps in an application.
* Task is only assigned once, while SQS message can be generated multiple times.

**Actors in SWF:**

* Workflow Starter: who initiates an application workflow, e.g. e-commerce website following the placement of order.
* Decider: who controls the flow of activity tasks in workflow execution. If something fails, deciders decide what to do.
* Activity Worker: who carries out the workflow.

**SWF vs SQS:**

* SWF could have human interaction, as a good memorable example Amazon’s own storage.
* SWF offers task-oriented API and SQS does message-oriented API.
* SWF execution can last up to 1 year, while SQS’s retention period lasts up to 14 days.
* SWF keeps track of all the tasks and event in the application, while SQS doesn’t and you need to implement your own application-level tracking.

Question 14: Correct

You are automating the creation of EC2 instances in your VPC. Hence, you wrote a python script to trigger the Amazon EC2 API to request 50 EC2 instances in a single Availability Zone. However, you noticed that after 20 successful requests, subsequent requests failed.

What could be a reason for this issue and how would you resolve it?

Explanation

You are limited to running up to a total of 20 On-Demand instances **(per region)** across the instance family, purchasing 20 Reserved Instances and requesting Spot Instances per your dynamic Spot limit per region. If you wish to run more than 20 instances, complete the Amazon EC2 instance request form.

Question 15: Incorrect

You are working as an IT Consultant for a large investment bank that generates large financial datasets with millions of rows. The data must be stored in a columnar fashion to reduce the number of disk I/O requests and reduce the amount of data needed to load from the disk. The bank has an existing third-party business intelligence application which will connect to the storage service and then generate daily and monthly financial reports for its clients around the globe.

In this scenario, which is the best storage service to use to meet the requirement?

Explanation

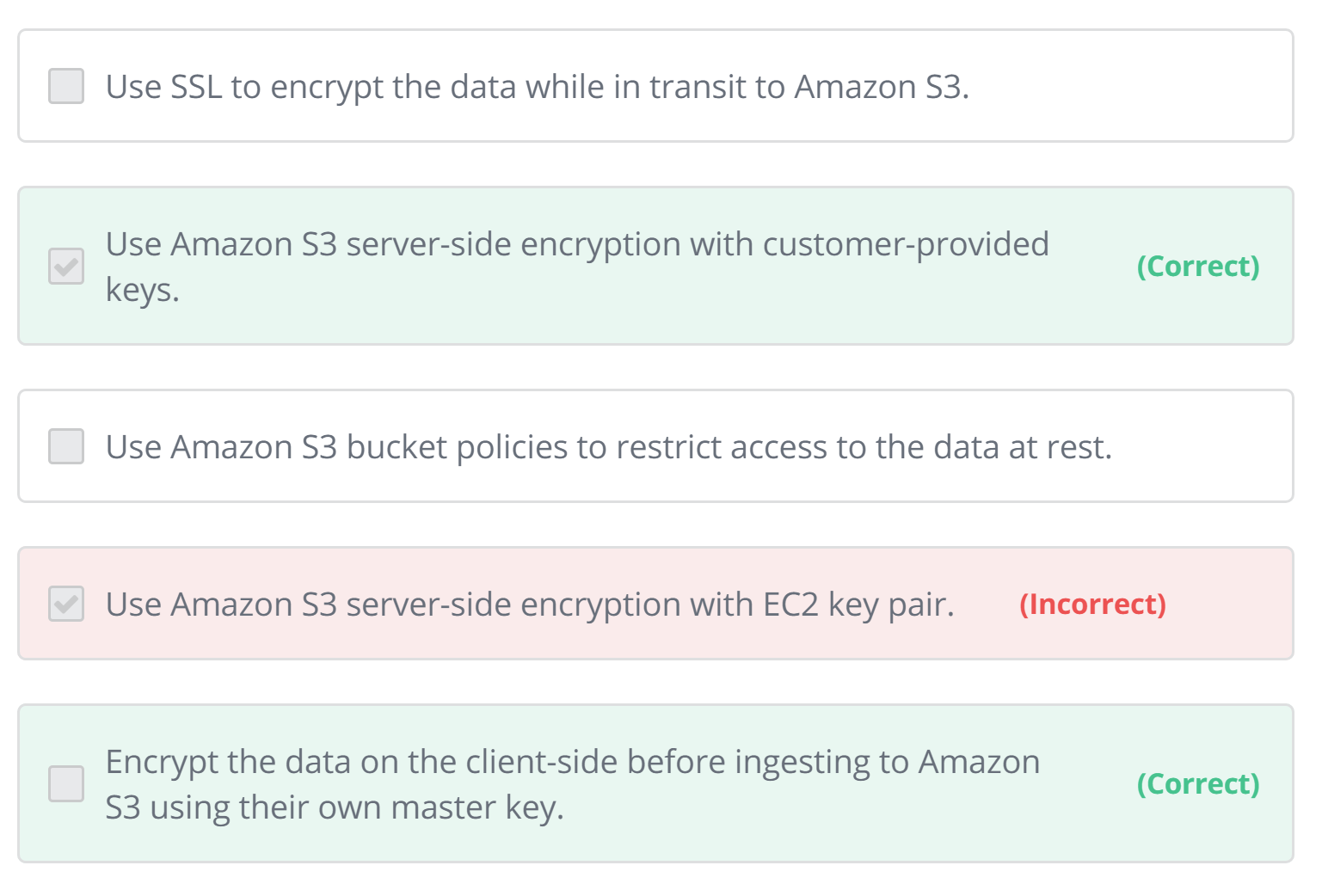
Amazon Redshift is a fast, scalable data warehouse that makes it simple and cost-effective to analyze all your data across your data warehouse and data lake. (Amazon Redshift is a tool designed to work with data of up to dozens of petabytes. Powered by PostgreSQL, it is mostly applied to any kind of SQL applications with minimum changes.) Redshift delivers ten times faster performance than other data warehouses by using machine learning, massively parallel query execution, and columnar storage on high-performance disk.

In this scenario, there is a requirement to have a storage service which will be used by a business intelligence application and where the data must be stored in a columnar fashion. Business Intelligence reporting systems is a type of Online Analytical Processing (OLAP) which Redshift is known to support. In addition, Redshift also provides columnar storage unlike the other options. Hence, the correct answer in this scenario is Option 1: Amazon Redshift.

Selection between RDS vs DynamoDB vs RedShift

Question 19: Incorrect

A music company is storing data on Amazon Simple Storage Service (S3). The company’s security policy requires that data are encrypted at rest. Which of the following methods can achieve this? (Choose 2)

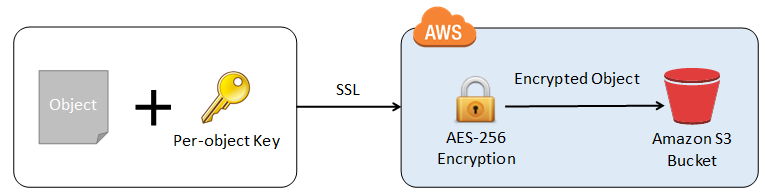


Explanation

Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by using SSL or by using client-side encryption. You have the following options for protecting data at rest in Amazon S3:

Use **Server-Side Encryption** – You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.

1. Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3) – AES-256
   1. Enable SSE on an S3 bucket to make use of AES-256 encryption.
2. Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS) – envelop key + full audit trail
3. Use Server-Side Encryption with Customer-Provided Keys (SSE-C)
   1. Encrypt the data locally using your own encryption keys, then copy the data to Amazon S3 over HTTPS endpoints.



SSE-C means that you provide the encryption keys to Amazon, and they encrypt all data with your public key so that ONLY you can only read the data with your private key. This means nobody at Amazon can ever read your files, but you are totally screwed if you lose or damage your key; Amazon cannot help you recover.

SSE-S3 provides server side encryption, but Amazon manages the keys of the object storage system, This system makes sure uploaded data is encrypted when stored on Amazon's servers. The risk of losing the data due to lost keys is eliminated.

SSE-KMS is most advanced, allowing you to manage and audit the keys and providing a level of advanced control over the SSE-S3 service.

Use **Client-Side Encryption** – You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

1. Use Client-Side Encryption with AWS KMS–Managed Customer Master Key (CMK)
2. Use Client-Side Encryption Using a Client-Side Master Key



Question 21: Correct

A document sharing website is using AWS as its cloud infrastructure. Free users can upload a total of 5 GB data while premium users can upload as much as 5 TB. Their application uploads the user files, which can have a max file size of 1 TB, to an S3 Bucket.

In this scenario, what is the best way for the application to upload the large files in S3?

Explanation

The total volume of data and number of objects you can store are unlimited (by default, you can create up to 100 buckets in each of your AWS accounts.) Individual Amazon S3 objects can range in size from a minimum of 0 bytes to a maximum of 5 terabytes. The largest object that can be uploaded **in a single PUT** is 5 gigabytes. For objects larger than 100 megabytes, customers should consider using the **Multipart Upload** capability. <https://aws.amazon.com/about-aws/whats-new/2010/11/10/Amazon-S3-Introducing-Multipart-Upload/>

The Multipart upload API enables you to upload large objects in parts. You can use this API to upload new large objects or make a copy of an existing object. Multipart uploading is a three-step process: you initiate the upload, you upload the object parts, and after you have uploaded all the parts, you complete the multipart upload. Upon receiving the complete multipart upload request, Amazon S3 constructs the object from the uploaded parts and you can then access the object just as you would any other object in your bucket.

Option 1 is incorrect because the largest file size you can upload using a single PUT request is 5 GB. Files larger than this will fail to be uploaded.

Option 2 is incorrect because Snowball is a migration tool that lets you transfer large amounts of data from your on-premises data center to AWS S3 and vice versa. This tool is not suitable for the given scenario. And when you provision Snowball, the device gets transported to you, and not to your customers. Therefore, you bear the responsibility of securing the device.

Option 3 is incorrect because Import/Export is similar to AWS Snowball in such a way that it is meant to be used as a migration tool, and not for multiple customer consumption such as in the given scenario.

<https://aws.amazon.com/about-aws/whats-new/2009/05/20/AWS-Import-Export/>

Question 22: Correct

One of your clients wants to leverage on Amazon S3 and Amazon Glacier as part of their backup and archive infrastructure. They created a new S3 bucket called “tutorialsdojobackup”. To support this integration between AWS and their on-premises network, they decided to use a third-party software.

Which approach will limit the access of the third party software to the Amazon S3 bucket only and not to other AWS resources?

Explanation

In this scenario, you have to provide access to your VPC to the third party software by creating a new IAM user. Since you want to limit the access of the third party software, you can simply manage the available AWS resources that it can communicate with by setting up a custom user policy, which will only allow access to a specific S3 bucket.

Question 25: Incorrect

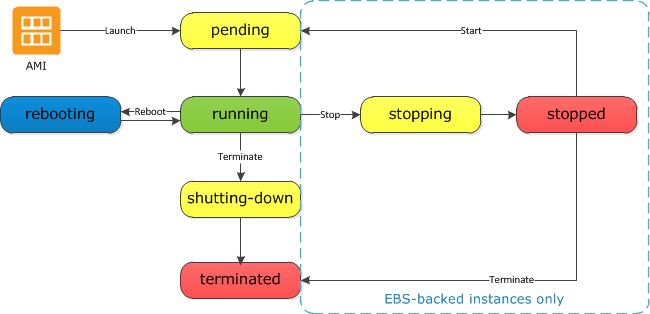
You are working for a FinTech startup as their AWS Solutions Architect. You deployed an application on different EC2 instances with Elastic IP addresses attached for easy DNS resolution and configuration. These servers are only accessed from 8 AM to 6 PM and can be stopped from 6 PM to 8 AM for cost efficiency using Lambda with the script that automates this based on tags.

Which of the following will occur when an EC2-VPC instance with an associated Elastic IP is stopped and started? (Choose 2)

Explanation

This question did not mention the specific type of EC2 instance however, it says that it will be stopped and started. Since only EBS-backed instances can be stopped and restarted, it is implied that the instance is EBS-backed. Remember that an instance store-backed instance can only be rebooted or terminated and its data will be erased if the EC2 instance is terminated.

If you stopped an EBS-backed EC2 instance, the volume is preserved but the data in any attached Instance store volumes will be erased. Keep in mind that an EC2 instance has an underlying physical host computer. If the instance is stopped, AWS usually moves the instance to a new host computer. Your instance may stay on the same host computer if there are no problems with the host computer. In addition, its Elastic IP address is disassociated from the instance if it is an EC2-Classic instance. Otherwise, if it is an EC2-VPC instance, the Elastic IP address remains associated. (Any instances launched after 201302014 are EC2-VPC only.)



Question 26



Question 28: Correct

You are working as an IT Consultant for a large media company where you are tasked to design a web application that stores static assets in an Amazon Simple Storage Service (S3) bucket. You expect this S3 bucket to immediately receive over 2000 PUT requests and 3500 GET requests per second at peak hour.

What should you do to ensure optimal performance?

Explanation

Amazon S3 now provides increased performance to support at least 3,500 requests per second to add data and 5,500 requests per second to retrieve data, which can save significant processing time for no additional charge. Each S3 prefix can support these request rates, making it simple to increase performance significantly.

Applications running on Amazon S3 today will enjoy this performance improvement with no changes, and customers building new applications on S3 do not have to make any application customizations to achieve this performance. Amazon S3's support for parallel requests means you can scale your S3 performance by the factor of your compute cluster, without making any customizations to your application. Performance scales per prefix, so you can use as many prefixes as you need in parallel to achieve the required throughput (retrieving by ‘bucket/1/file’ and ‘bucket/2/file’ will attain 11,000 requests per second). There are no limits to the number of prefixes.

This S3 request rate performance increase removes any previous guidance to randomize object prefixes to achieve faster performance. That means you can now use logical or sequential naming patterns in S3 object naming without any performance implications. This improvement is now available in all AWS Regions.

Question 29: Correct

You are working as a Solutions Architect for a multinational financial firm. They have a global online trading platform in which the users from all over the world regularly upload terabytes of transactional data to a centralized S3 bucket. What AWS feature should you use in your present system to improve throughput and ensure consistently fast data transfer to the Amazon S3 bucket, regardless of your user's location?

Explanation

Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and your Amazon S3 bucket. Transfer Acceleration leverages Amazon CloudFront’s globally distributed AWS Edge Locations. As data arrives at an AWS Edge Location, data is routed to your Amazon S3 bucket over an optimized network path.

An Origin Access Identity (OAI) is used for sharing private content via CloudFront (-> Question 65). The OAI is a virtual user identity that will be used to give your CF distribution permission to fetch a private object from your origin server (e.g. S3 bucket). This is a feature which ensures that only CloudFront can serve S3 content. It does not increase throughput and ensure fast delivery of content to your customers.

Question 31: Incorrect

You are designing a social media website for a startup company and the founders want to know the ways to mitigate distributed denial-of-service (DDoS) attacks to their website.

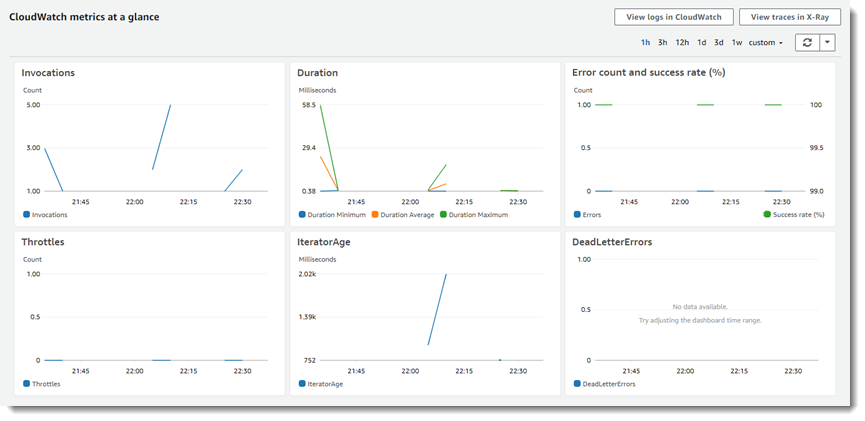
Which of the following are not viable mitigation techniques? (Choose 2)

Explanation

(xxxxxxxxxx) To protect your system from SoS attack, you can do the following:

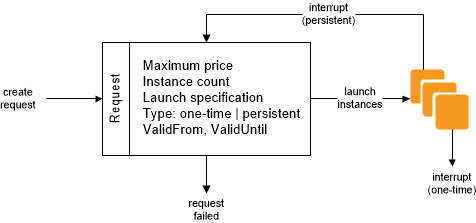
* Use an Amazon CloudFront service for distributing both static and dynamic content.
* Use an Application Load Balancer with Auto Scaling groups for your EC2 instances then restrict direct Internet traffic to your Amazon RDS database by deploying to a private subnet.
* Setup alerts in Amazon CloudWatch to look for high ‘Network In’ and CPU utilization metrics.
* Use AWS Shield and AWS WAF to fortify your cloud network. AWS Shield is a managed DDoS protection service that is available in two tiers: Standard and Advanced. AWS Shield Standard applies always-on detection and inline mitigation techniques, such as deterministic packet filtering and priority-based traffic shaping, to minimize application downtime and latency.

Question 34



Question 35

Stop instance request.



Question 38: Correct

You currently have an Augment Reality (AR) mobile game which has a serverless backend. It is using a DynamoDB table which was launched using the AWS CLI to store all the user data and information gathered from the players and a Lambda function to pull the data from DynamoDB. The game is being used by millions of users each day to read and store data.

How would you design the application to improve its overall performance and make it more scalable while keeping the costs low? (Choose 2)

Explanation

Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for DynamoDB that delivers up to a 10x performance improvement – from milliseconds to microseconds – even at millions of requests per second. DAX does all the heavy lifting required to add in-memory acceleration to your DynamoDB tables, without requiring developers to manage cache invalidation, data population, or cluster management.

Amazon API Gateway lets you create an API that acts as a "front door" for applications to access data, business logic, or functionality from your back-end services, such as code running on AWS Lambda. Amazon API Gateway handles all of the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls, including traffic management, authorization and access control, monitoring, and API version management. Amazon API Gateway has no minimum fees or startup costs. (API Gateway + enabling caching makes the entire performance improved)

AWS Lambda scales your functions automatically on your behalf. Every time an event notification is received for your function, AWS Lambda quickly locates free capacity within its compute fleet and runs your code. Since your code is stateless, AWS Lambda can start as many copies of your function as needed without lengthy deployment and configuration delays. (ref Question 56)

Question 39

Question 39: Incorrect

An online job site is using NGINX for its application servers hosted in EC2 instances and MongoDB Atlas for its database-tier. MongoDB Atlas is a fully automated third-party cloud service which is not provided by AWS, but supports VPC peering to connect to your VPC.

Which of the following items are invalid VPC peering configurations? (Choose 2)

Explanation

The following VPC peering connection configurations are **not supported**.

* Overlapping CIDR Blocks. If the VPCs have multiple IPv4 CIDR blocks, you cannot create a VPC peering connection if any of the CIDR blocks overlap.
* Transitive Peering
* Edge to Edge Routing Through a Gateway or Private Connection (edge-to-edge routing in a cloud provider context means essentially using a "virtual cloud" as a transit between another cloud and some other network)

Question 42: Correct

A company is using a custom shell script to automate the deployment and management of their EC2 instances. The script is using various AWS CLI commands such as revoke-security-group-ingress, revoke-security-group-egress, run-scheduled-instances and many others.

In the shell script, what does the revoke-security-group-ingress command do?

The revoke-security-group-ingress command removes one or more ingress rules from a security group.

Ingress vs Egress

Ingress traffic is composed of all the data communications and network traffic originating from external networks and destined for a node in the host network. The following picture illustrates ingress and egress when you are the router…



Question 43: Incorrect

You are unable to connect to your new EC2 instance via SSH from your home computer, which you have recently deployed. However, you were able to successfully access other existing instances in your VPC without any issues.

Which of the following should you check and possibly correct to restore connectivity?

Explanation

Network ACL is much suitable to control the traffic that goes in and out of your entire VPC and not just on one EC2 instance (Security Group will do better job when it comes to a single EC2 instance).

Security Group vs NACL

* Security group is the firewall of EC2 Instances whereas Network ACL Is the firewall of the Subnet. Security group support allow rules only (by default all rules are denied).
* Network ACL support allow and deny rules. By deny rules, you could explicitly deny a certain IP address.
* Security groups evaluate all the rules in them before allowing a traffic whereas NACLs do it in the number order, from top to bottom.
* Security group first layer of defense, whereas Network ACL is second layer of the defense.

Question 44: Correct

A leading media company has an application hosted in an EBS-backed EC2 instance which uses Simple Workflow Service (SWF) to handle its sequential background jobs. The application works well in production and your manager asked you to also implement the same solution to other areas of their business.

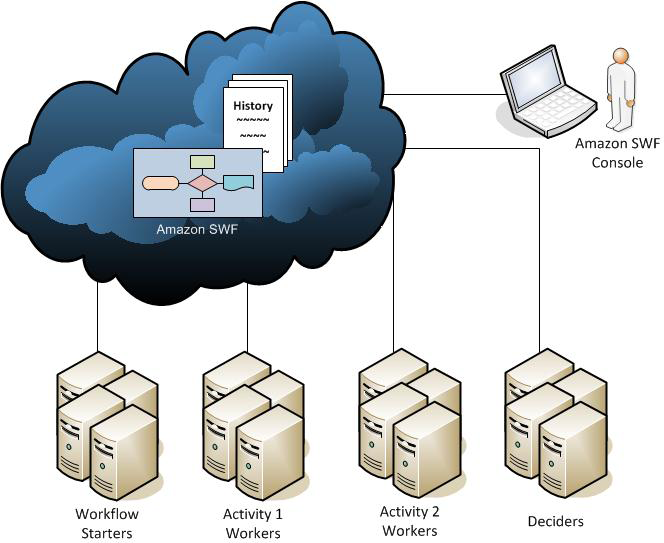
In which other scenarios can you use both Simple Workflow Service (SWF) and Amazon EC2 as a solution? (Choose 2)

Explanation

You can use a combination of EC2 and SWF for the following scenarios:

* Managing a multi-step and multi-decision checkout process of an e-commerce mobile app.
* Orchestrating the execution of distributed business processes

**Elasticache is the best option for distributed session management.**



Question 46: Incorrect

A tech company is currently using Auto Scaling for their web application. A new AMI now needs to be used for launching a fleet of EC2 instances.

Which of the following changes needs to be done?

Explanation

For this scenario, you have to create a new launch configuration. Remember that you can't modify a launch configuration after you've created it.

A launch configuration is a template that an Auto Scaling group uses to launch EC2 instances. When you create a launch configuration, you specify information for the instances such as the ID of the Amazon Machine Image (AMI), the instance type, a key pair, one or more security groups, and a block device mapping. If you've launched an EC2 instance before, you specified the same information in order to launch the instance.

you only want to change the AMI being used by your instances, and not the instances themselves. Therefore, you should be updating your launch configuration, not the target group.

Question 48: Incorrect

You are setting up the cloud architecture for an international money transfer service to be deployed in AWS which will have thousands of users around the globe. The service should be available 24/7 to avoid any business disruption and should be resilient enough to handle the outage of an entire AWS region. To meet this requirement, you have deployed your AWS resources to multiple AWS Regions. You need to use Route 53 and configure it to set all of your resources to be available all the time as much as possible. When a resource becomes unavailable, your Route 53 should detect that it's unhealthy and stop including it when responding to queries.

Which of the following is the most fault tolerant routing configuration that you should use in this scenario?

Explanation

You can use Route 53 health checking to configure active-active and active-passive failover configurations. You configure active-active failover using any routing policy (or combination of routing policies) other than failover, and you configure active-passive failover using the failover routing policy.

**Active-Active Failover**

Use this failover configuration when you want all of your resources to be available the majority of the time. When a resource becomes unavailable, Route 53 can detect that it's unhealthy and stop including it when responding to queries.

In active-active failover, all the records that have the same name, the same type (such as A or AAAA), and the same routing policy (such as weighted or latency) are active unless Route 53 considers them unhealthy. Route 53 can respond to a DNS query using any healthy record.

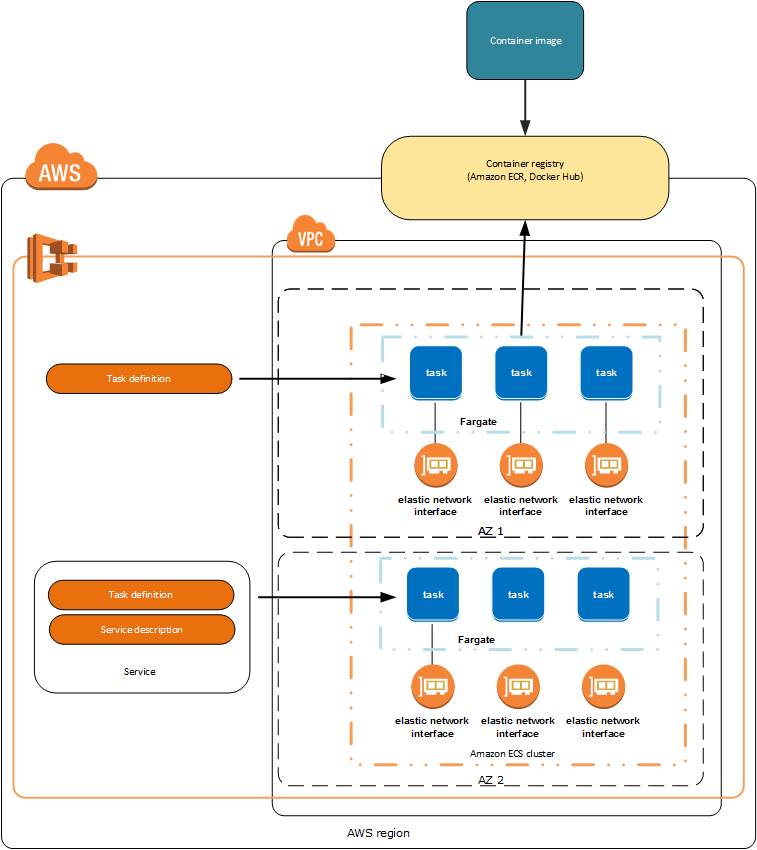
**Active-Passive Failover**

Use an active-passive failover configuration when you want a primary resource or group of resources to be available the majority of the time and you want a secondary resource or group of resources to be on standby in case all the primary resources become unavailable. When responding to queries, Route 53 includes only the healthy primary resources. If all the primary resources are unhealthy, Route 53 begins to include only the healthy secondary resources in response to DNS queries.

Question 50

A new online banking platform has been re-designed to have a microservices architecture in which complex applications are decomposed into smaller, independent services. The new platform is using Docker considering that application containers are optimal for running small, decoupled services.

Which service can you use to migrate this new platform to AWS?



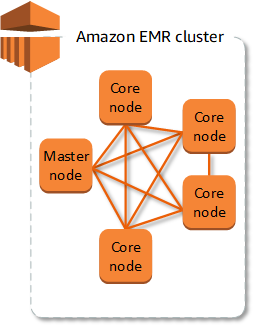
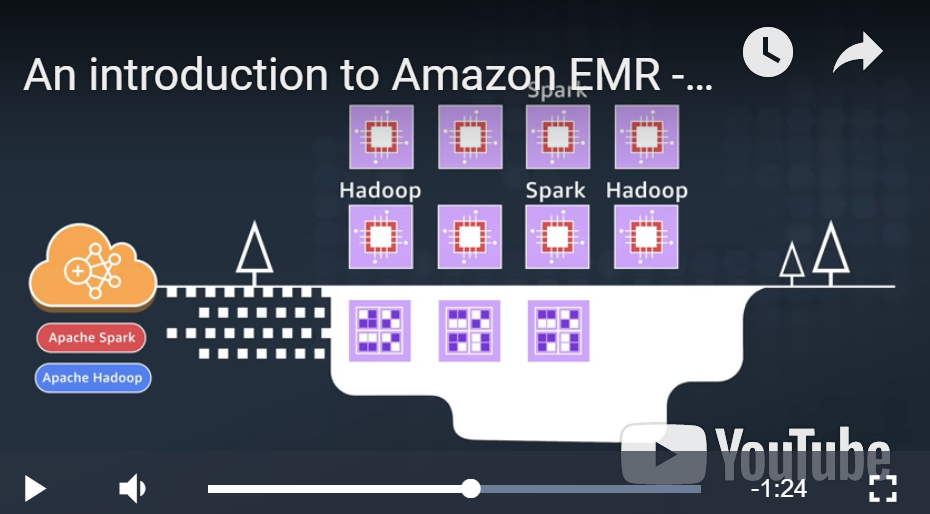
Question 51: Correct

You are working for a large telecommunications company where you need to run analytics against all combined log files from your Application Load Balancer as part of the regulatory requirements.

Which AWS services can be used together to collect logs and then easily perform log analysis?

Explanation

Amazon EMR is the industry leading cloud-native big data platform, allowing teams to process vast amounts of data quickly, and cost-effectively at scale. Using open source tools such as Apache Spark, Apache Hive, Apache HBase, Apache Flink, and Presto, coupled with the dynamic scalability of Amazon EC2 and scalable storage of Amazon S3.

Question 52: Correct

Your company is in a hurry of deploying their new web application written in NodeJS to AWS. As the Solutions Architect of the company, you were assigned to do the deployment without worrying about the underlying infrastructure that runs the application. Which service will you use to easily deploy and manage your new web application in AWS?

Explanation

CloudFormation vs Elastic Beanstalk

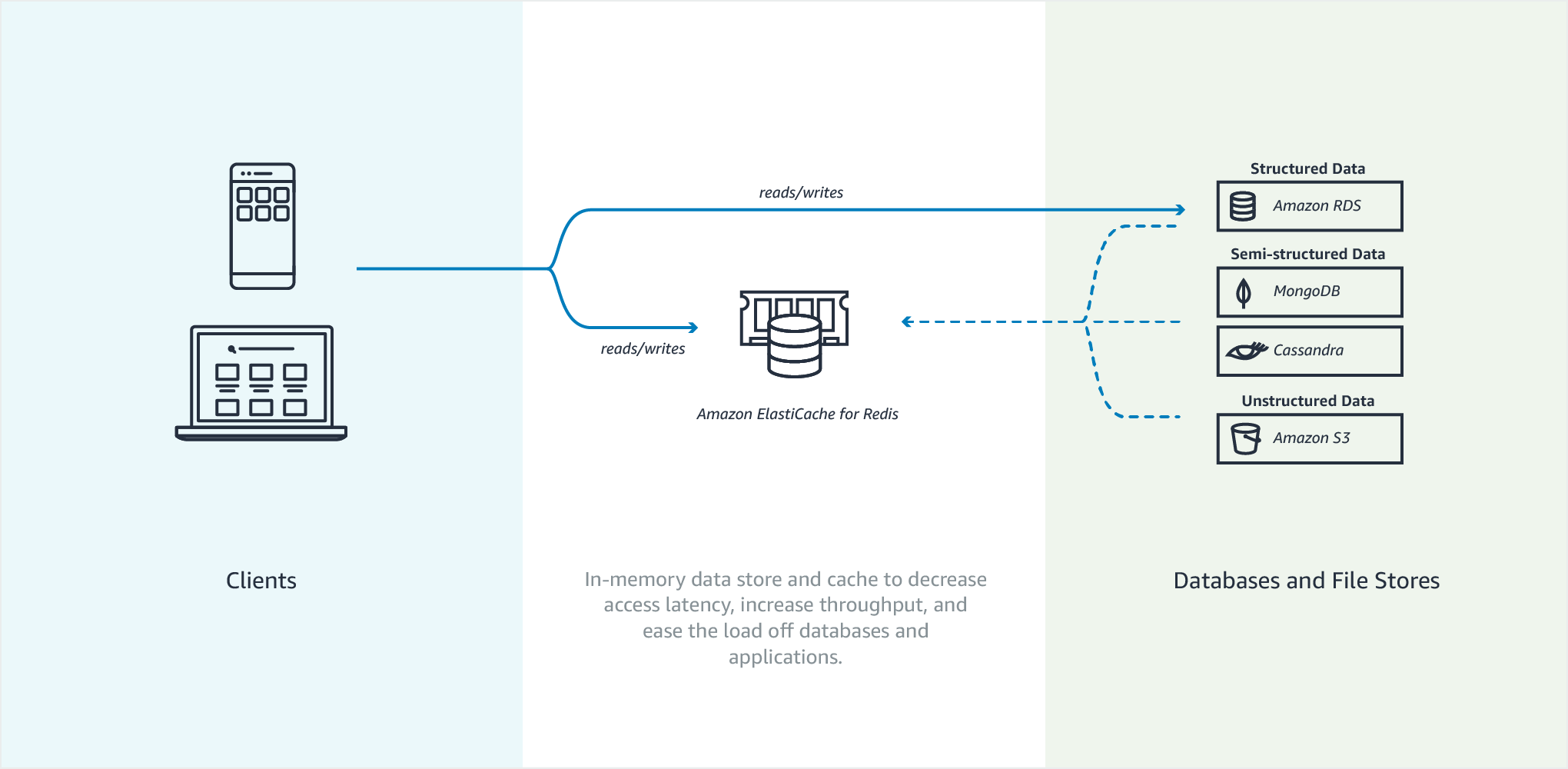
CloudFormation is based on your template in JSON and requires you to understand how AWS works in some extent of details. Beanstalk is more for people who have almost no idea what they are.

Question 53: Incorrect

Your web application is relying entirely on slower disk-based databases, causing it to perform slowly. To improve its performance, you integrated an in-memory data store to your web application using ElastiCache. How does Amazon ElastiCache improve database performance?

Explanation

ElastiCache improves the performance of your database through caching query results.



Question 54: Correct

In your VPC, you have a Classic Load Balancer distributing traffic to 2 running EC2 instances in ap-southeast-1a AZ and 8 EC2 instances in ap-southeast-1b AZ. However, you noticed that half of your incoming traffic goes to ap-southeast-1a AZ which over-utilize its 2 instances but underutilize the other 8 instances in the other AZ.

Explanation

Cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled Availability Zone, and improves your application's ability to handle the loss of one or more instances.

When you create a Classic Load Balancer, the default for cross-zone load balancing depends on how you create the load balancer. With the API or CLI, cross-zone load balancing is disabled by default. With the AWS Management Console, the option to enable cross-zone load balancing is selected by default.

Question 56: Correct

You have a VPC that has a CIDR block of 10.31.0.0/27 which is connected to your on-premises data center. There was a requirement to create a Lambda function that will process massive amounts of cryptocurrency transactions every minute and then store the results to EFS. After you set up the serverless architecture and connected Lambda function to your VPC, you noticed that there is an increase in invocation errors with EC2 error types such as EC2ThrottledException on certain times of the day.

Which of the following are the possible causes of this issue? (Choose 2)

Explanation

You can configure a function to connect to a virtual private cloud (VPC) in your account. Use Amazon Virtual Private Cloud (Amazon VPC) to create a private network for resources such as databases, cache instances, or internal services. Connect your function to the VPC to access private resources during execution.

AWS Lambda runs your function code securely within a VPC by default. However, 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 to connect securely to other resources within your private VPC.

Lambda functions cannot connect directly to a VPC with dedicated instance tenancy. To connect to resources in a dedicated VPC, peer it to a second VPC with default tenancy.

Your Lambda function automatically scales based on the number of events it processes. If your Lambda function accesses a VPC, you must make sure that your VPC has sufficient ENI capacity to support the scale requirements of your Lambda function. It is also recommended that you specify at least one subnet in each Availability Zone in your Lambda function configuration.

By specifying subnets in each of the Availability Zones, your Lambda function can run in another Availability Zone if one goes down or runs out of IP addresses. If your VPC does not have sufficient ENIs or subnet IPs, your Lambda function will not scale as requests increase, and you will see an increase in invocation errors with EC2 error types like EC2ThrottledException. For asynchronous invocation, if you see an increase in errors without corresponding CloudWatch Logs, invoke the Lambda function synchronously in the console to get the error responses.

Question 57

* -Each subnet maps to a single Availability Zone.
* -Every subnet that you create is automatically associated with the main route table for the VPC.
* -If a subnet's traffic is routed to an Internet gateway, the subnet is known as a public subnet.

Question 58: Correct

You are working as a Solutions Architect for a tech company where you are instructed to build a web architecture using On-Demand EC2 instances and a database in AWS. However, due to budget constraints, the company instructed you to choose a database service in which they no longer need to worry about database management tasks such as hardware or software provisioning, setup, configuration, scaling and backups.

Which database service in AWS is best to use in this scenario?

Explanation

Basically, a database service in which you no longer need to worry about database management tasks such as hardware or software provisioning, setup and configuration is called a fully managed database. This means that AWS fully manages all of the database management tasks and the underlying host server. The main differentiator here is the keyword "scaling" in the question. In RDS, you still have to manually scale up your resources and create Read Replicas to improve scalability while in DynamoDB, this is automatically done. DynamoDB also lets you backup and restore all your tables for data archival, helping you meet your corporate and governmental regulatory requirements.

Question 61: Incorrect

In Amazon EC2, you can manage your instances from the moment you launch them up to their termination. You can flexibly control your computing costs by changing the EC2 instance state. Which of the following statements is true regarding EC2 billing? (Choose 2)

Explanation

pending – Not billed.

stopping - You will not billed if it is preparing to stop however, you will still be billed if it is just preparing to hibernate.

stopped – Not billed. Hibernate??

shutting-down – Not billed, but except the case your instance is reserved which is billed until the end of your contract end.

terminated – Dido.

Hibernation for EC2 Instances: The hibernation process stores the in-memory state of the instance, along with its **private** and elastic IP addresses (\*instance store and **public** IP (non EIP) are NOT preserved) , allowing it to pick up exactly where it left off.

Question 64: Incorrect

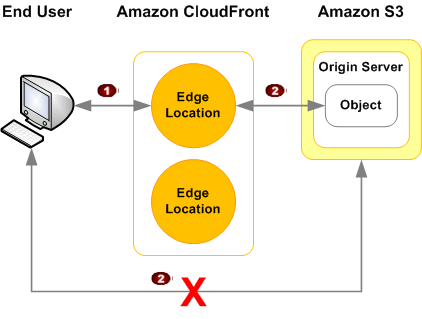
Your customer has clients all across the globe that access product files stored in several S3 buckets, which are behind each of their own CloudFront web distributions. They currently want to deliver their content to a specific client, and they need to make sure that only that client can access the data. Currently, all of their clients can access their S3 buckets directly using an S3 URL or through their CloudFront distribution.

Which of the following are possible solutions that you could implement to meet the above requirements?

Explanation

Many companies that distribute content over the Internet want to restrict access to documents, business data, media streams, or content that is intended for selected users, for example, users who have paid a fee. To securely serve this private content by using CloudFront, you can do the following:

* Require that your users access your private content by using special CloudFront signed URLs or signed cookies. Then you create a special CloudFront user called an origin access identity (OAI).
* Require that your users access your Amazon S3 content by using CloudFront URLs, not Amazon S3 URLs. Requiring CloudFront URLs isn't necessary, but it is recommended to prevent users from bypassing the restrictions that you specify in signed URLs or signed cookies.



The presigned URLs are useful if you want your user/customer to be able to access a specific object to your S3 bucket.

Three (+ one) options to allow S3 bucket object access from outside of AWS:

* Make the object publicly-readable: This can be done via the console or CLI/API. However, anyone with that URL will be able to download it.
* Create an Amazon S3 Bucket Policy that grants read access for the desired file/directory/bucket. But, again, anyone with the URL will be able to access those objects.
* Keep the object private, but use a pre-signed URL that adds parameters to the URL to prove that you are permitted to download the object. This pre-signed URL is time-limited and can be generated with a few lines of code using current AWS credentials.
* + signed URL or signed cookies through CloudFront to specific privileged user (called OAI)

Question 65: Incorrect

A travel company has a suite of web applications hosted in an Auto Scaling group of On-Demand EC2 instances behind an Application Load Balancer that handles traffic from various web domains such as i-love-manila.com, i-love-boracay.com, i-love-cebu.com and many others. To improve security and lessen the overall cost, you are instructed to secure the system by allowing multiple domains to serve SSL traffic without the need to reauthenticate and reprovision your certificate everytime you add a new domain. This migration from HTTP to HTTPS will help improve their SEO and Google search ranking.

Which of the following is the most cost-effective solution to meet the above requirement?

Explanation

SNI (Server Name Indication) Custom SSL relies on the SNI extension of the Transport Layer Security protocol, which allows multiple domains to serve SSL traffic over the same IP address by including the hostname which the viewers are trying to connect to.

You can host multiple TLS secured applications, each with its own TLS certificate, behind a single load balancer. In order to use SNI, all you need to do is bind multiple certificates to the same secure listener on your load balancer. ALB will automatically choose the optimal TLS certificate for each client. These features are provided at no additional charge.

To meet the requirements in the scenario, you can upload all SSL certificates of the domains in the ALB using the console and bind multiple certificates to the same secure listener on your load balancer. ALB will automatically choose the optimal TLS certificate for each client using Server Name Indication (SNI).

