Set 1: Practice Questions, Answers & Explanations

1. Question

A company has deployed Amazon RedShift for performing analytics on user data. When using Amazon RedShift, which of the following statements are correct in relation to availability and durability? (choose 2)

1. RedShift always keeps three copies of your data
2. Single-node clusters support data replication
3. RedShift provides continuous/incremental backups
4. Manual backups are automatically deleted when you delete a cluster
5. RedShift always keeps five copies of your data

Answer: 1,3

Explanation:

- RedShift always keeps three copies of your data and provides continuous/incremental backups
- Corrections:
- Single-node clusters do not support data replication
- Manual backups are not automatically deleted when you delete a cluster

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-redshift/

2. Question

You are a Solutions Architect at Digital Cloud Training. A client from a large multinational corporation is working on a deployment of a significant amount of resources into AWS. The client would like to be able to deploy resources across multiple AWS accounts and regions

using a single toolset and template. You have been asked to suggest a toolset that can provide this functionality?

1. Use a CloudFormation template that creates a stack and specify the logical IDs of each account and region
2. Use a CloudFormation StackSet and specify the target accounts and regions in which the stacks will be created
3. Use a third-party product such as Terraform that has support for multiple AWS accounts and regions
4. This cannot be done, use separate CloudFormation templates per AWS account and region

Answer: 2
Explanation:

- AWS CloudFormation StackSets extends the functionality of stacks by enabling you to create, update, or delete stacks across multiple accounts and regions with a single operation
- Using an administrator account, you define and manage an AWS CloudFormation template, and use the template as the basis for provisioning stacks into selected target accounts across specified regions. An administrator account is the AWS account in which you create stack sets
- A stack set is managed by signing in to the AWS administrator account in which it was created. A target account is the account into which you create, update, or delete one or more stacks in your stack set
- Before you can use a stack set to create stacks in a target account, you must set up a trust relationship between the administrator and target accounts
- A regular CloudFormation template cannot be used across regions and accounts. You would need to create copies of the template and then manage updates
- You do not need to use a third-party product such as Terraform as this functionality can be delivered through native AWS technology

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-cloudformation/

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stacksets-concepts.html

3. Question

A new Big Data application you are developing will use hundreds of EC2 instances to write data to a shared file system. The file system must be stored redundantly across multiple AZs within a region and allow the EC2 instances to concurrently access the file system. The required throughput is multiple GB per second.

From the options presented which storage solution can deliver these requirements?

1. Amazon EBS using multiple volumes in a RAID 0 configuration
2. Amazon EFS
3. Amazon S3
4. Amazon Storage Gateway

Answer: 2

Explanation:

- Amazon EFS is the best solution as it is the only solution that is a file-level storage solution (not block/object-based), stores data redundantly across multiple AZs within a region and you can concurrently connect up to thousands of EC2 instances to a single filesystem
- Amazon EBS volumes cannot be accessed by concurrently by multiple instances
- Amazon S3 is an object store, not a file system
- Amazon Storage Gateway is a range of products used for on-premises storage management and can be configured to cache data locally, backup data to the cloud and also provides a virtual tape backup solution

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/

4. Question

An application running on an external website is attempting to initiate a request to your company's website on AWS using API calls. A problem has been reported in which the requests are failing with an error that includes the following text:

"Cross-Origin Request Blocked: The Same Origin Policy disallows reading the remote resource"

You have been asked to resolve the problem, what is the most likely solution?

1. Enable CORS on the APIs resources using the selected methods under the API Gateway
2. The ACL on the API needs to be updated
3. The IAM policy does not allow access to the API
4. The request is not secured with SSL/TLS

Answer: 1

Explanation:

- Can enable Cross Origin Resource Sharing (CORS) for multiple domain use with Javascript/AJAX:
  - Can be used to enable requests from domains other the APIs domain
  - Allows the sharing of resources between different domains
  - The method (GET, PUT, POST etc.) for which you will enable CORS must be available in the API Gateway API before you enable CORS
  - If CORS is not enabled and an API resource received requests from another domain the request will be blocked
  - Enable CORS on the APIs resources using the selected methods under the API Gateway
- IAM policies are not used to control CORS and there is no ACL on the API to update

- This error would display whether using SSL/TLS or not

References:
https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-api-gateway/

5. Question

You need to configure an application to retain information about each user session and have decided to implement a layer within the application architecture to store this information.

Which of the options below could be used? (choose 2)

1. A workflow service such as Amazon Simple Workflow Service (SWF)
2. Sticky sessions on an Elastic Load Balancer (ELB)
3. A block storage service such as Elastic Block Store (EBS)
4. A relational data store such as Amazon RDS
5. A key/value store such as ElastiCache Redis

Answer: 2,5

Explanation:

- In order to address scalability and to provide a shared data storage for sessions that can be accessible from any individual web server, you can abstract the HTTP sessions from the web servers themselves. A common solution to for this is to leverage an In-Memory Key/Value store such as Redis and Memcached.
- Sticky sessions, also known as session affinity, allow you to route a site user to the particular web server that is managing that individual user's session. The session's validity can be determined by a number of methods, including a client-side cookie or via configurable duration parameters that can be set at the load balancer which routes requests to the web servers. You can configure sticky sessions on Amazon ELBs.
- Relational databases are not typically used for storing session state data due to their rigid schema that tightly controls the format in which data can be stored.

- Workflow services such as SWF are used for carrying out a series of tasks in a coordinated task flow. They are not suitable for storing session state data.
- In this instance the question states that a caching layer is being implemented and EBS volumes would not be suitable for creating an independent caching layer as they must be attached to EC2 instances.

References:
https://aws.amazon.com/caching/session-management/

6. Question

The data scientists in your company are looking for a service that can process and analyze real-time, streaming data. They would like to use standard SQL queries to query the streaming data.

Which combination of AWS services would deliver these requirements?

1. Kinesis Data Streams and Kinesis Data Analytics
2. Kinesis Data Streams and Kinesis Firehose
3. ElastiCache and EMR
4. DynamoDB and EMR

Answer: 1
Explanation:

- Kinesis Data Streams enables you to build custom applications that process or analyze streaming data for specialized needs
- Amazon Kinesis Data Analytics is the easiest way to process and analyze real-time, streaming data. Kinesis Data Analytics can use standard SQL queries to process Kinesis data streams and can ingest data from Kinesis Streams and Kinesis Firehose but Firehose cannot be used for running SQL queries
- DynamoDB is a NoSQL database that can be used for storing data from a stream but cannot be used to process or analyze the data or to query it with SQL queries. Elastic Map Reduce (EMR)

is a hosted Hadoop framework and is not used for analytics on streaming data

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-kinesis/

7. Question

Which of the following approaches provides the lowest cost for Amazon elastic block store snapshots while giving you the ability to fully restore data?

1. Maintain a single snapshot; the latest snapshot is both incremental and complete
2. Maintain the most current snapshot; archive the original to Amazon Glacier
3. Maintain two snapshots: the original snapshot and the latest incremental snapshot
4. Maintain the original snapshot; subsequent snapshots will overwrite one another

Answer: 1

Explanation:

- You can backup data on an EBS volume by periodically taking snapshots of the volume. The scenario is that you need to reduce storage costs by maintaining as few EBS snapshots as possible whilst ensuring you can restore all data when required.
- If you take periodic snapshots of a volume, the snapshots are incremental which means only the blocks on the device that have changed after your last snapshot are saved in the new snapshot. Even though snapshots are saved incrementally, the snapshot deletion process is designed such that you need to retain only the most recent snapshot in order to restore the volume
- You cannot just keep the original snapshot as it will not be incremental and complete
- You do not need to keep the original and latest snapshot as the latest snapshot is all that is needed

- There is no need to archive the original snapshot to Amazon Glacier. EBS copies your data across multiple servers in an AZ for durability

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/

8. Question

You are undertaking a project to make some audio and video files that your company uses for onboarding new staff members available via a mobile application. You are looking for a cost-effective way to convert the files from their current formats into formats that are compatible with smartphones and tablets. The files are currently stored in an S3 bucket.

What AWS service can help with converting the files?

1. Rekognition
2. Elastic Transcoder
3. Data Pipeline
4. Amazon Personalize

Answer: 2

Explanation:

- Amazon Elastic Transcoder is a highly scalable, easy to use and cost-effective way for developers and businesses to convert (or “transcode”) video and audio files from their source format into versions that will playback on devices like smartphones, tablets and PCs
- Amazon Personalize is a machine learning service that makes it easy for developers to create individualized recommendations for customers using their applications
- Data Pipeline helps you move, integrate, and process data across AWS compute and storage resources, as well as your on-premises resources
- Rekognition is a deep learning-based visual analysis service

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/media-services/amazon-elastic-transcoder/

9. Question

You are a Solutions Architect at Digital Cloud Training. A large multi-national client has requested a design for a multi-region, multi-master database. The client has requested that the database be designed for fast, massively scaled applications for a global user base. The database should be a fully managed service including the replication.

Which AWS service can deliver these requirements?

1. S3 with Cross Region Replication
2. RDS with Multi-AZ
3. DynamoDB with Global Tables and Cross Region Replication
4. EC2 instances with EBS replication

Answer: 3

Explanation:

- Cross-region replication allows you to replicate across regions:
  - Amazon DynamoDB global tables provides a fully managed solution for deploying a multi-region, multi-master database
  - When you create a global table, you specify the AWS regions where you want the table to be available
  - DynamoDB performs all of the necessary tasks to create identical tables in these regions, and propagate ongoing data changes to all of them
- RDS with Multi-AZ is not multi-master (only one DB can be written to at a time), and does not span regions
- S3 is an object store not a multi-master database
- There is no such thing as EBS replication. You could build your own database stack on EC2 with DB-level replication but that is not what is presented in the answer

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/

10. Question

A customer has asked you to recommend the best solution for a highly available database. The database is a relational OLTP type of database and the customer does not want to manage the operating system the database runs on. Failover between AZs must be automatic.

Which of the below options would you suggest to the customer?

1. Use RDS in a Multi-AZ configuration
2. Use DynamoDB
3. Use RedShift in a Multi-AZ configuration
4. Install a relational database on EC2 instances in multiple AZs and create a cluster

Answer: 1

Explanation:

- Amazon Relational Database Service (Amazon RDS) is a managed service that makes it easy to set up, operate, and scale a relational database in the cloud. With RDS you can configure Multi-AZ which creates a replica in another AZ and synchronously replicates to it (DR only)
- RedShift is used for analytics OLAP not OLTP
- If you install a DB on an EC2 instance you will need to manage to OS yourself and the customer wants it to be managed for them
- DynamoDB is a managed database of the NoSQL type. NoSQL DBs are not relational DBs

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

11. Question

An application you manage uses Auto Scaling and a fleet of EC2 instances. You recently noticed that Auto Scaling is scaling the number of instances up and down multiple times in the same hour. You need to implement a remediation to reduce the amount of scaling events. The remediation must be cost-effective and preserve elasticity. What design changes would you implement? (choose 2)

1. Modify the Auto Scaling group termination policy to terminate the newest instance first
2. Modify the Auto Scaling group cool-down timers
3. Modify the CloudWatch alarm period that triggers your Auto Scaling scale down policy
4. Modify the Auto Scaling policy to use scheduled scaling actions
5. Modify the Auto Scaling group termination policy to terminate the oldest instance first

Answer: 2,3
Explanation:

- The cooldown period is a configurable setting for your Auto Scaling group that helps to ensure that it doesn't launch or terminate additional instances before the previous scaling activity takes effect so this would help. After the Auto Scaling group dynamically scales using a simple scaling policy, it waits for the cooldown period to complete before resuming scaling activities
- The CloudWatch Alarm Evaluation Period is the number of the most recent data points to evaluate when determining alarm state. This would help as you can increase the number of datapoints required to trigger an alarm
- The order in which Auto Scaling terminates instances is not the issue here, the problem is that the workload is dynamic and Auto Scaling is constantly reacting to change, and launching or terminating instances
- Using scheduled scaling actions may not be cost-effective and also affects elasticity as it is less dynamic

References:

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html#alarm-evaluation

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

12. Question

One of your EC2 instances runs an application process that saves user data to an attached EBS volume. The EBS volume was attached to the EC2 instance after it was launched and is unencrypted. You would like to encrypt the data that is stored on the volume as it is considered sensitive however you cannot shutdown the instance due to other application processes that are running.

What is the best method of applying encryption to the sensitive data without any downtime?

1. Create an encrypted snapshot of the current EBS volume. Restore the snapshot to the EBS volume
2. Create and mount a new encrypted EBS volume. Move the data to the new volume and then delete the old volume
3. Unmount the volume and enable server-side encryption. Re-mount the EBS volume
4. Leverage the AWS Encryption CLI to encrypt the data on the volume

Answer: 2

Explanation:

- You cannot restore a snapshot of a root volume without downtime
- There is no direct way to change the encryption state of a volume
- Either create an encrypted volume and copy data to it or take a snapshot, encrypt it, and create a new encrypted volume from the snapshot

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/

13. Question

You are planning to launch a RedShift cluster for processing and analyzing a large amount of data. The RedShift cluster will be deployed into a VPC with multiple subnets. Which construct is used when provisioning the cluster to allow you to specify a set of subnets in the VPC that the cluster will be deployed into?

1. Subnet Group
2. Availability Zone (AZ)
3. DB Subnet Group
4. Cluster Subnet Group

Answer: 4

Explanation:

- You create a cluster subnet group if you are provisioning your cluster in your virtual private cloud (VPC)
- A cluster subnet group allows you to specify a set of subnets in your VPC
- When provisioning a cluster, you provide the subnet group and Amazon Redshift creates the cluster on one of the subnets in the group
- A DB Subnet Group is used by RDS
- A Subnet Group is used by ElastiCache
- Availability Zones are part of the AWS global infrastructure, subnets reside within AZs but in RedShift you provision the cluster into Cluster Subnet Groups

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-redshift/

https://docs.aws.amazon.com/redshift/latest/mgmt/working-with-cluster-subnet-groups.html

14. Question

A Solutions Architect is responsible for a web application that runs on EC2 instances that sit behind an Application Load Balancer (ALB). Auto Scaling is used to launch instances across 3 Availability Zones.

The web application serves large image files and these are stored on an Amazon EFS file system. Users have experienced delays in retrieving the files and the Architect has been asked to improve the user experience.

What should the Architect do to improve user experience?

1. Cache static content using CloudFront
2. Reduce the file size of the images
3. Move the digital assets to EBS
4. Use Spot instances

Answer: 1

Explanation:

- CloudFront is ideal for caching static content such as the files in this scenario and would increase performance
- Moving the files to EBS would not make accessing the files easier or improve performance
- Reducing the file size of the images may result in better retrieval times, however CloudFront would still be the preferable option
- Using Spot EC2 instances may reduce EC2 costs but it won't improve user experience

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/

15. Question

A Solutions Architect is deploying an Auto Scaling Group (ASG) and needs to determine what CloudWatch monitoring option to use. Which of the statements below would assist the Architect in making his decision? (choose 2)

1. Basic monitoring is enabled by default if the ASG is created from the CLI
2. Detailed monitoring is chargeable and must always be manually enabled

3. Detailed monitoring is free and can be manually enabled
4. Detailed monitoring is enabled by default if the ASG is created from the CLI
5. Basic monitoring is enabled by default if the ASG is created from the console

Answer: 4,5
Explanation:

- Basic monitoring sends EC2 metrics to CloudWatch about ASG instances every 5 minutes
- Detailed can be enabled and sends metrics every 1 minute (it is always chargeable)
- When the launch configuration is created from the CLI detailed monitoring of EC2 instances is enabled by default
- When you enable Auto Scaling group metrics, Auto Scaling sends sampled data to CloudWatch every minute

References:
https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

16. Question

A Linux instance running in your VPC requires some configuration changes to be implemented locally and you need to run some commands. Which of the following can be used to securely connect to the instance?

1. SSL/TLS certificate
2. Public key
3. Key Pairs
4. EC2 password

Answer: 3
Explanation:

- A key pair consists of a public key that AWS stores, and a private key file that you store

- For Windows AMIs, the private key file is required to obtain the password used to log into your instance
- For Linux AMIs, the private key file allows you to securely SSH into your instance
- The “EC2 password” might refer to the operating system password. By default, you cannot login this way to Linux and must use a key pair. However, this can be enabled by setting a password and updating the /etc/ssh/sshd_config file
- You cannot login to an EC2 instance using certificates/public keys

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ec2/

17. Question

Your company would like to restrict the ability of most users to change their own passwords whilst continuing to allow a select group of users within specific user groups.

What is the best way to achieve this? (choose 2)

1. Under the IAM Password Policy deselect the option to allow users to change their own passwords
2. Create an IAM Policy that grants users the ability to change their own password and attach it to the groups that contain the users
3. Create an IAM Policy that grants users the ability to change their own password and attach it to the individual user accounts
4. Create an IAM Role that grants users the ability to change their own password and attach it to the groups that contain the users
5. Disable the ability for all users to change their own passwords using the AWS Security Token Service

Answer: 1,2

Explanation:

- A password policy can be defined for enforcing password length, complexity etc. (applies to all users)
- You can allow or disallow the ability to change passwords using an IAM policy and you should attach this to the group that contains the users, not to the individual users themselves
- You cannot use an IAM role to perform this function
- The AWS STS is not used for controlling password policies

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/

18. Question

A colleague from your company's IT Security team has notified you of an Internet-based threat that affects a certain port and protocol combination. You have conducted an audit of your VPC and found that this port and protocol combination is allowed on an Inbound Rule with a source of 0.0.0.0/0. You have verified that this rule only exists for maintenance purposes and need to make an urgent change to block the access.

What is the fastest way to block access from the Internet to the specific ports and protocols?

1. You don't need to do anything; this rule will only allow access to VPC based resources
2. Update the security group by removing the rule
3. Delete the security group
4. Add a deny rule to the security group with a higher priority

Answer: 2

Explanation:

- Security group membership can be changed whilst instances are running
- Any changes to security groups will take effect immediately
- You can only assign permit rules in a security group, you cannot assign deny rules

- If you delete the security you will remove all rules and potentially cause other problems
- You do need to make the update, as it's the VPC based resources you're concerned about

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

19. Question

You are an entrepreneur building a small company with some resources running on AWS. As you have limited funding, you're extremely cost conscious. Which AWS service can send you alerts via email or SNS topic when you are forecast to exceed your funding capacity so you can take action?

1. Cost & Usage reports
2. AWS Billing Dashboard
3. AWS Budgets
4. Cost Explorer

Answer: 3

Explanation:

- AWS Budgets gives you the ability to set custom budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount. Budget alerts can be sent via email and/or Amazon Simple Notification Service (SNS) topic
- The AWS Cost Explorer is a free tool that allows you to view charts of your costs
- The AWS Billing Dashboard can send alerts when you're bill reaches certain thresholds but you must use AWS Budgets to created custom budgets that notify you when you are forecast to exceed a budget
- The AWS Cost and Usage report tracks your AWS usage and provides estimated charges associated with your AWS account but does not send alerts

References:
https://aws.amazon.com/aws-cost-management/aws-budgets/

20. Question

Your company is starting to use AWS to host new web-based applications. A new two-tier application will be deployed that provides customers with access to data records. It is important that the application is highly responsive and retrieval times are optimized. You're looking for a persistent data store that can provide the required performance. From the list below what AWS service would you recommend for this requirement?

1. Kinesis Data Streams
2. ElastiCache with the Memcached engine
3. ElastiCache with the Redis engine
4. RDS in a multi-AZ configuration

Answer: 3

Explanation:

ElastiCache is a web service that makes it easy to deploy and run Memcached or Redis protocol-compliant server nodes in the cloud. The in-memory caching provided by ElastiCache can be used to significantly improve latency and throughput for many read-heavy application workloads or compute-intensive workloads

There are two different database engines with different characteristics as per below:

Memcached

- Not persistent
- Cannot be used as a data store
- Supports large nodes with multiple cores or threads
- Scales out and in, by adding and removing nodes

Redis

- Data is persistent
- Can be used as a datastore
- Not multi-threaded

- Scales by adding shards, not nodes

Kinesis Data Streams is used for processing streams of data, it is not a persistent data store

RDS is not the optimum solution due to the requirement to optimize retrieval times which is a better fit for an in-memory data store such as ElastiCache

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-elasticache/

21. Question

A Solutions Architect is developing an encryption solution. The solution requires that data keys are encrypted using envelope protection before they are written to disk.

Which solution option can assist with this requirement?

1. AWS Certificate Manager
2. AWS KMS API
3. IAM Access Key
4. API Gateway with STS

Answer: 2

Explanation:

- The AWS KMS API can be used for encrypting data keys (envelope encryption)
- AWS Certificate Manager is a service that lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources
- The AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for AWS Identity and Access Management (IAM) users or for users that you authenticate (federated users)
- IAM access keys are used for signing programmatic requests you make to AWS

References:
https://docs.aws.amazon.com/kms/latest/APIReference/Welcome.html

22. Question

A solutions Architect is designing a new workload where an AWS Lambda function will access an Amazon DynamoDB table.

What is the MOST secure means of granting the Lambda function access to the DynamoDB table?

1. Create an identity and access management (IAM) role with the necessary permissions to access the DynamoDB table, and assign the role to the Lambda function
2. Create a DynamoDB username and password and give them to the Developer to use in the Lambda function
3. Create an identity and access management (IAM) user and create access and secret keys for the user. Give the user the necessary permissions to access the DynamoDB table. Have the Developer use these keys to access the resources
4. Create an identity and access management (IAM) role allowing access from AWS Lambda and assign the role to the DynamoDB table

Answer: 1

Explanation:

- The most secure method is to use an IAM role so you don't need to embed any credentials in code and can tightly control the services that your Lambda function can access. You need to assign the role to the Lambda function, NOT to the DynamoDB table
- You should not provide a username and password to the Developer to use with the function. This is insecure – always avoid using credentials in code!
- You should not use an access key and secret ID to access DynamoDB. Again, this means embedding credentials in code which should be avoided.

References:

https://aws.amazon.com/blogs/security/how-to-create-an-aws-iam-policy-to-grant-aws-lambda-access-to-an-amazon-dynamodb-table/

23. Question

An e-commerce application is hosted in AWS. The last time a new product was launched, the application experienced a performance issue due to an enormous spike in traffic. Management decided that capacity must be doubled this week after the product is launched.

What is the MOST efficient way for management to ensure that capacity requirements are met?

1. Add Amazon EC2 Spot instances
2. Add a Step Scaling policy
3. Add a Simple Scaling policy
4. Add a Scheduled Scaling action

Answer: 4

Explanation:

- Scheduled scaling: Scaling based on a schedule allows you to set your own scaling schedule for predictable load changes. To configure your Auto Scaling group to scale based on a schedule, you create a scheduled action. This is ideal for situations where you know when and for how long you are going to need the additional capacity
- Step scaling: step scaling policies increase or decrease the current capacity of your Auto Scaling group based on a set of scaling adjustments, known as step adjustments. The adjustments vary based on the size of the alarm breach. This is more suitable to situations where the load unpredictable
- Simple scaling: AWS recommend using step over simple scaling in most cases. With simple scaling, after a scaling activity is started, the policy must wait for the scaling activity or health check replacement to complete and the cooldown period to expire before responding to additional alarms (in contrast to step scaling). Again, this is more suitable to unpredictable workloads
- EC2 Spot Instances: adding spot instances may decrease EC2 costs but you still need to ensure they are available. The main

requirement of the question is that the performance issues are resolved rather than the cost being minimized

References:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scale-based-on-demand.html

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

24. Question

A colleague has asked you some questions about how AWS charge for DynamoDB. He is interested in knowing what type of workload DynamoDB is best suited for in relation to cost and how AWS charges for DynamoDB? (choose 2)

1. DynamoDB is more cost effective for read heavy workloads
2. DynamoDB is more cost effective for write heavy workloads
3. Priced based on provisioned throughput (read/write) regardless of whether you use it or not
4. You provision for expected throughput but are only charged for what you use
5. DynamoDB scales vertically by adding additional nodes

Answer: 1,3

Explanation:

- DynamoDB is more cost effective for read heavy workloads. This is due to the read capacity units (RCU) being half the price of the write capacity units (WCU).
- With DynamoDB you are charged based on the provisioned throughput you assign (RCUs/WCUs) regardless of whether you use it or not. With the DynamoDB Auto Scaling feature you can now have DynamoDB dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns. However, this is not provided as an answer option.
- DynamoDB scales horizontally and the mechanism by which this happens is transparent to consumers. It does not scale vertically by adding nodes.

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AutoScaling.html

25. Question

A user is testing a new service that receives location updates from 5,000 rental cars every hour. Which service will collect data and automatically scale to accommodate production workload?

1. Amazon API Gateway
2. Amazon EBS
3. Amazon Kinesis Firehose
4. Amazon EC2

Answer: 3

Explanation:

- What we need here is a service that can streaming collect streaming data. The only option available is Kinesis Firehose which captures, transforms, and loads streaming data into "destinations" such as S3, RedShift, Elasticsearch and Splunk
- Amazon EC2 is not suitable for collecting streaming data
- EBS is a block-storage service in which you attach volumes to EC2 instances, this does not assist with collecting streaming data (see previous point)
- Amazon API Gateway is used for hosting and managing APIs not for receiving streaming data

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-kinesis/

26. Question

A research company is developing a data lake solution in Amazon S3 to analyze huge datasets. The solution makes infrequent SQL

queries only. In addition, the company wants to minimize infrastructure costs.

Which AWS service should be used to meet these requirements?

1. Amazon Redshift Spectrum
2. Amazon Aurora
3. Amazon Athena
4. Amazon RDS for MySQL

Answer: 3

Explanation:

- Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run – this satisfies the requirement to minimize infrastructure costs for infrequent queries.
- Amazon RedShift Spectrum is a feature of Amazon Redshift that enables you to run queries against exabytes of unstructured data in Amazon S3, with no loading or ETL required. However, RedShift nodes run on EC2 instances, so for infrequent queries this will not minimize infrastructure costs.
- Amazon RDS and Aurora are not suitable solutions for analyzing datasets on S3 – these are both relational databases typically used for transactional (not analytical) workloads.

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-athena/

https://docs.aws.amazon.com/athena/latest/ug/what-is.html

27. Question

An application runs on two EC2 instances in private subnets split between two AZs. The application needs to connect to a CRM SaaS application running on the Internet. The vendor of the SaaS application restricts authentication to a whitelist of source IP addresses and only 2 IP addresses can be configured per customer.

What is the most appropriate and cost-effective solution to enable authentication to the SaaS application?

1. Configure redundant Internet Gateways and update the routing tables for each subnet
2. Configure a NAT Gateway for each AZ with an Elastic IP address
3. Use multiple Internet-facing Application Load Balancers with Elastic IP addresses
4. Use a Network Load Balancer and configure a static IP for each AZ

Answer: 2
Explanation:

- In this scenario you need to connect the EC2 instances to the SaaS application with a source address of one of two whitelisted public IP addresses to ensure authentication works.
- A NAT Gateway is created in a specific AZ and can have a single Elastic IP address associated with it. NAT Gateways are deployed in public subnets and the route tables of the private subnets where the EC2 instances reside are configured to forward Internet-bound traffic to the NAT Gateway. You do pay for using a NAT Gateway based on hourly usage and data processing, however this is still a cost-effective solution
- A Network Load Balancer can be configured with a single static IP address (the other types of ELB cannot) for each AZ. However, using a NLB is not an appropriate solution as the connections are being made outbound from the EC2 instances to the SaaS app and ELBs are used for distributing inbound connection requests to EC2 instances (only return traffic goes back through the ELB)
- An ALB does not support static IP addresses and is not suitable for a proxy function
- AWS Route 53 is a DNS service and is not used as an outbound proxy server so is not suitable for this scenario

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

28. Question

A recent security audit uncovered some poor deployment and configuration practices within your VPC. You need to ensure that applications are deployed in secure configurations.

How can this be achieved in the most operationally efficient manner?

1. Remove the ability for staff to deploy applications
2. Use AWS Inspector to apply secure configurations
3. Manually check all application configurations before deployment
4. Use CloudFormation with securely configured templates

Answer: 4

Explanation:

- CloudFormation helps users to deploy resources in a consistent and orderly way. By ensuring the CloudFormation templates are created and administered with the right security configurations for your resources, you can then repeatedly deploy resources with secure settings and reduce the risk of human error
- Removing the ability of staff to deploy resources does not help you to deploy applications securely as it does not solve the problem of how to do this in an operationally efficient manner
- Manual checking of all application configurations before deployment is not operationally efficient
- Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. It is not used to secure the actual deployment of resources, only to assess the deployed state of the resources

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-cloudformation/

29. Question

The application development team in your company has a new requirement for the deployment of a container solution. You plan to use the AWS Elastic Container Service (ECS). The solution should include load balancing of incoming requests across the ECS containers and allow the containers to use dynamic host port mapping so that multiple tasks from the same service can run on the same container host.

Which AWS load balancing configuration will support this?

1. You cannot run multiple copies of a task on the same instance, because the ports would conflict
2. Use a Network Load Balancer (NLB) and host-based routing
3. Use a Classic Load Balancer (CLB) and create a static mapping of the ports
4. Use an Application Load Balancer (ALB) and map the ECS service to the ALB

Answer: 4

Explanation:

- It is possible to associate a service on Amazon ECS to an Application Load Balancer (ALB) for the Elastic Load Balancing (ELB) service
- An Application Load Balancer allows dynamic port mapping. You can have multiple tasks from a single service on the same container instance.
- The Classic Load Balancer requires that you statically map port numbers on a container instance. You cannot run multiple copies of a task on the same instance, because the ports would conflict
- An NLB does not support host-based routing (ALB only), and this would not help anyway

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ecs/

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

30. Question

To improve security in your AWS account you have decided to enable multi-factor authentication (MFA). You can authenticate using an MFA device in which two ways? (choose 2)

1. Using biometrics
2. Locally to EC2 instances
3. Through the AWS Management Console
4. Using the AWS API
5. Using a key pair

Answer: 3,4

Explanation:

You can authenticate using an MFA device in the following ways:

- Through the AWS Management Console – the user is prompted for a user name, password and authentication code
- Using the AWS API – restrictions are added to IAM policies and developers can request temporary security credentials and pass MFA parameters in their AWS STS API requests
- Using the AWS CLI by obtaining temporary security credentials from STS (aws sts get-session-token)

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/

31. Question

The company you work for has a presence across multiple AWS regions. As part of disaster recovery planning you are formulating a solution to provide a regional DR capability for an application running on a fleet of Amazon EC2 instances that are provisioned by an Auto Scaling Group (ASG). The applications are stateless and read and write data to an S3 bucket. You would like to utilize the current AMI used by the ASG as it has some customizations made to it.

What are the steps you might take to enable a regional DR capability for this application? (choose 2)

1. Enable cross region replication on the S3 bucket and specify a destination bucket in the DR region
2. Modify the launch configuration for the ASG in the DR region and specify the AMI
3. Copy the AMI to the DR region and create a new launch configuration for the ASG that uses the AMI
4. Enable multi-AZ for the S3 bucket to enable synchronous replication to the DR region
5. Modify the permissions of the AMI so it can be used across multiple regions

Answer: 1,3
Explanation:

- There are two parts to this solution. First you need to copy the S3 data to each region (as the instances are stateless), then you need to be able to deploy instances from an ASG using the same AMI in each regions.

  – CRR is an Amazon S3 feature that automatically replicates data across AWS Regions. With CRR, every object uploaded to an S3 bucket is automatically replicated to a destination bucket in a different AWS Region that you choose, this enables you to copy the existing data across to each region
  – AMIs of both Amazon EBS-backed AMIs and instance store-backed AMIs can be copied between regions. You can then use the copied AMI to create a new launch configuration (remember that you cannot modify an ASG launch configuration, you must create a new launch configuration)

- There's no such thing as Multi-AZ for an S3 bucket (it's an RDS concept)
- Changing permissions on an AMI doesn't make it usable from another region, the AMI needs to be present within each region to be used

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/

32. Question

A Solutions Architect needs to improve performance for a web application running on EC2 instances launched by an Auto Scaling group. The instances run behind an ELB Application Load Balancer. During heavy use periods the ASG doubles in size and analysis has shown that static content stored on the EC2 instances is being requested by users in a specific geographic location.

How can the Solutions Architect reduce the need to scale and improve the application performance?

1. Re-deploy the application in a new VPC that is closer to the users making the requests
2. Create an Amazon CloudFront distribution for the site and redirect user traffic to the distribution
3. Store the contents on Amazon EFS instead of the EC2 root volume
4. Implement Amazon Redshift to create a repository of the content closer to the users

Answer: 2

Explanation:

- This is a good use case for CloudFront. CloudFront is a content delivery network (CDN) that caches content closer to users. You can cache the static content on CloudFront using the EC2 instances as origins for the content. This will improve performance (as the content is closer to the users) and reduce the need for the ASG to scale (as you don't need the processing power of the EC2 instances to serve the static content).
- Re-deploying the application in a VPC closer to the users may reduce latency (and therefore improve performance), but it doesn't solve the problem of reducing the need for the ASG to scale.

- Using EFS instead of the EC2 root volume does not solve either problem.
- RedShift cannot be used to create content repositories to get content closer to users, it's a data warehouse used for analytics.

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/

https://aws.amazon.com/caching/cdn/

33. Question

You are a Solutions Architect at Digital Cloud Training. One of your clients has requested that you design a solution for distributing load across a number of EC2 instances across multiple AZs within a region. Customers will connect to several different applications running on the client's servers through their browser using multiple domain names and SSL certificates. The certificates are stored in AWS Certificate Manager (ACM).

What is the optimal architecture to ensure high availability, cost effectiveness, and performance?

1. Launch a single ALB, configure host-based routing for the domain names and bind an SSL certificate to each routing rule
2. Launch a single ALB and bind multiple SSL certificates to the same secure listener. Clients will use the Server Name Indication (SNI) extension
3. Launch a single ALB and bind multiple SSL certificates to multiple secure listeners
4. Launch multiple ALBs and bind separate SSL certificates to each ELB

Answer: 2

Explanation:

- You can use a single ALB and bind multiple SSL certificates to the same listener
- With Server Name Indication (SNI) a client indicates the hostname to connect to. SNI supports multiple secure websites

using a single secure listener

- You cannot have the same port in multiple listeners so adding multiple listeners would not work. Also, when using standard HTTP/HTTPS the port will always be 80/443 so you must be able to receive traffic on the same ports for multiple applications and still be able to forward to the correct instances. This is where host-based routing comes in
- With host-based routing you can route client requests based on the Host field (domain name) of the HTTP header allowing you to route to multiple domains from the same load balancer (and share the same listener)
- You do not need multiple ALBs and it would not be cost-effective

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

34. Question

The website for a new application received around 50,000 requests each second and the company wants to use multiple applications to analyze the navigation patterns of the users on their website so they can personalize the user experience.

What can a Solutions Architect use to collect page clicks for the website and process them sequentially for each user?

1. Amazon SQS standard queue
2. AWS CloudTrail trail
3. Amazon Kinesis Streams
4. Amazon SQS FIFO queue

Answer: 3

Explanation:

- This is a good use case for Amazon Kinesis streams as it is able to scale to the required load, allow multiple applications to access the records and process them sequentially

- Amazon Kinesis Data Streams enables real-time processing of streaming big data. It provides ordering of records, as well as the ability to read and/or replay records in the same order to multiple Amazon Kinesis Applications
- Amazon Kinesis streams allows up to 1 MiB of data per second or 1,000 records per second for writes per shard. There is no limit on the number of shards so you can easily scale Kinesis Streams to accept 50,000 per second
- The Amazon Kinesis Client Library (KCL) delivers all records for a given partition key to the same record processor, making it easier to build multiple applications reading from the same Amazon Kinesis data stream
- Standard SQS queues do not ensure that messages are processed sequentially and FIFO SQS queues do not scale to the required number of transactions a second
- CloudTrail is used for auditing and is not useful here

References:

https://docs.aws.amazon.com/streams/latest/dev/service-sizes-and-limits.html

https://aws.amazon.com/kinesis/data-streams/faqs/

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-kinesis/

35. Question

A retail organization is deploying a new application that will read and write data to a database. The company wants to deploy the application in three different AWS Regions in an active-active configuration. The databases need to replicate to keep information in sync.

Which solution best meets these requirements?

1. Amazon DynamoDB with global tables
2. Amazon Athena with Amazon S3 cross-region replication
3. AWS Database Migration Service with change data capture
4. Amazon Aurora Global Database

Answer: 1

Explanation:

- Amazon DynamoDB global tables provide a fully managed solution for deploying a multi-region, multi-master database. This is the only solution presented that provides an active-active configuration where reads and writes can take place in multiple regions with full bi-directional synchronization.
- Amazon Athena with S3 cross-region replication is not suitable. This is not a solution that provides a transactional database solution (Athena is used for analytics), or active-active synchronization.
- Amazon Aurora Global Database provides read access to a database in multiple regions – it does not provide active-active configuration with bi-directional synchronization (though you can failover to your read-only DBs and promote them to writable).

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/

https://aws.amazon.com/blogs/database/how-to-use-amazon-dynamodb-global-tables-to-power-multiregion-architectures/

36. Question

You are building an application that will collect information about user behavior. The application will rapidly ingest large amounts of dynamic data and requires very low latency. The database must be scalable without incurring downtime. Which database would you recommend for this scenario?

1. RedShift
2. DynamoDB
3. RDS with MySQL
4. RDS with Microsoft SQL

Answer: 2

Explanation:

- Amazon Dynamo DB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability
- Push button scaling means that you can scale the DB at any time without incurring downtime
- DynamoDB provides low read and write latency
- RDS uses EC2 instances so you have to change your instance type/size in order to scale compute vertically
- RedShift uses EC2 instances as well, so you need to choose your instance type/size for scaling compute vertically, but you can also scale horizontally by adding more nodes to the cluster
- Rapid ingestion of dynamic data is not an ideal use case for RDS or RedShift

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/

37. Question

You have been asked to implement a solution for capturing, transforming and loading streaming data into an Amazon RedShift cluster. The solution will capture data from Amazon Kinesis Data Streams. Which AWS services would you utilize in this scenario? (choose 2)

1. Kinesis Data Firehose for capturing the data and loading it into RedShift
2. Kinesis Video Streams for capturing the data and loading it into RedShift
3. Lambda for transforming the data
4. EMR for transforming the data
5. AWS Data Pipeline for transforming the data

Answer: 1,3

Explanation:

- For this solution Kinesis Data Firehose can be used as it can use Kinesis Data Streams as a source and can capture, transform,

and load streaming data into a RedShift cluster. Kinesis Data Firehose can invoke a Lambda function to transform data before delivering it to destinations

- Kinesis Video Streams makes it easy to securely stream video from connected devices to AWS for analytics, machine learning (ML), and other processing, this solution does not involve video streams
- AWS Data Pipeline is used for processing and moving data between compute and storage services. It does not work with streaming data as Kinesis does
- Elastic Map Reduce (EMR) is used for processing and analyzing data using the Hadoop framework. It is not used for transforming streaming data

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/analytics/amazon-kinesis/

38. Question

A company is deploying a big data and analytics workload. The analytics will be run from a fleet of thousands of EC2 instances across multiple AZs. Data needs to be stored on a shared storage layer that can be mounted and accessed concurrently by all EC2 instances. Latency is not a concern however extremely high throughput is required.

What storage layer would be most suitable for this requirement?

1. Amazon EFS in Max I/O mode
2. Amazon EFS in General Purpose mode
3. Amazon EBS PIOPS
4. Amazon S3

Answer: 1

Explanation:

- Amazon EFS file systems in the Max I/O mode can scale to higher levels of aggregate throughput and operations per second with a tradeoff of slightly higher latencies for file operations

- Amazon S3 is not a storage layer that can be mounted and accessed concurrently
- Amazon EBS volumes cannot be shared between instances

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/

https://docs.aws.amazon.com/efs/latest/ug/performance.html

39. Question

Your company is reviewing their information security processes. One of the items that came out of a recent audit is that there is insufficient data recorded about requests made to a few S3 buckets. The security team requires an audit trail for operations on the S3 buckets that includes the requester, bucket name, request time, request action, and response status.

Which action would you take to enable this logging?

1. Create a CloudWatch metric that monitors the S3 bucket operations and triggers an alarm
2. Enable server access logging for the S3 buckets to save access logs to a specified destination bucket
3. Create a CloudTrail trail that audits S3 bucket operations
4. Enable S3 event notifications for the specific actions and setup an SNS notification

Answer: 2

Explanation:

- Server access logging provides detailed records for the requests that are made to a bucket. To track requests for access to your bucket, you can enable server access logging. Each access log record provides details about a single access request, such as the requester, bucket name, request time, request action, response status, and an error code, if relevant
- For capturing IAM/user identity information in logs you would need to configure AWS CloudTrail Data Events (however this does not audit the bucket operations required in the question)

- Amazon S3 event notifications can be sent in response to actions in Amazon S3 like PUTs, POSTs, COPYs, or DELETEs.S3 event notifications records the request action but not the other requirements of the security team
- CloudWatch metrics do not include the bucket operations specified in the question

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html

40. Question

A Solutions Architect is designing a new architecture that will use an Amazon EC2 Auto Scaling group.

Which of the following factors determine the health check grace period? (choose 2)

1. How long the bootstrap script takes to run
2. How long it takes for the Auto Scaling group to detect a failure
3. How much of the application code is embedded in the AMI
4. How many Amazon CloudWatch alarms are configured for status checks
5. How frequently the Auto Scaling group scales up or down

Answer: 1,3

Explanation:

- Amazon EC2 Auto Scaling waits until the health check grace period ends before checking the health status of the instance. The length of the health check grace period needs to consider the warm-up time for your instances. This includes the time to start the application. Application code in the AMI as well as bootstrap scripts could delay application start-up, so you'd want to consider these factors when determining the health check grace period.
- How many times the Auto Scaling group scales up or down is not relevant to the health check grace period, every instance will

need to go through this when launched and you need to ensure the instances start before the period ends.

- It's not relevant how many CloudWatch alarms are configured for status checks as status checks are not acted on until the health check grace period ends.
- Detecting a failure is related to how quickly Auto Scaling can react and terminate and replace an instance, it's not relevant to the health check grace period.

References:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/healthcheck.html

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

41. Question

A call center application consists of a three-tier application using Auto Scaling groups to automatically scale resources as needed. Users report that every morning at 9:00am the system becomes very slow for about 15 minutes. A Solutions Architect determines that a large percentage of the call center staff starts work at 9:00am, so Auto Scaling does not have enough time to scale to meet demand.

How can the Architect fix the problem?

1. Permanently keep a steady state of instance that is needed at 9:00am to guarantee available resources, but use Spot Instances
2. Use Reserved Instances to ensure the system has reserved the right amount of capacity for the scaling events
3. Create an Auto Scaling scheduled action to scale out the necessary resources at 8:30am each morning
4. Change the Auto Scaling group's scale out event to scale based on network utilization

Answer: 3

Explanation:

- Scheduled scaling: Scaling based on a schedule allows you to set your own scaling schedule for predictable load changes. To

configure your Auto Scaling group to scale based on a schedule, you create a scheduled action. This is ideal for situations where you know when and for how long you are going to need the additional capacity

- Changing the scale-out events to scale based on network utilization may not assist here. We're not certain the network utilization will increase sufficiently to trigger an Auto Scaling scale out action as the load may be more CPU/memory or number of connections. The main problem however is that we need to ensure the EC2 instances are provisioned ahead of demand not in response to demand (which would incur a delay whilst the EC2 instances "warm up")
- Using reserved instances ensures capacity is available within an AZ, however the issue here is not that the AZ does not have capacity for more instances, it is that the instances are not being launched by Auto Scaling ahead of the peak demand
- Keeping a steady state of Spot instances is not a good solution. Spot instances may be cheaper, but this is not guaranteed and keeping them online 24hrs a day is wasteful and could prove more expensive

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-auto-scaling/

https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html

42. Question

Your company keeps unstructured data on a filesystem. You need to provide access to employees via EC2 instances in your VPC. Which storage solution should you choose?

1. Amazon EBS
2. Amazon Snowball
3. Amazon EFS
4. Amazon S3

Answer: 3

Explanation:

- EFS is the only storage system presented that provides a file system. EFS is accessed by mounting filesystems using the NFS v4.1 protocol from your EC2 instances. You can concurrently connect up to thousands of instances to a single EFS filesystem
- Amazon S3 is an object-based storage system that is accessed over a REST API
- Amazon EBS is a block-based storage system that provides volumes that are mounted to EC2 instances but cannot be shared between EC2 instances
- Amazon Snowball is a device used for migrating very large amounts of data into or out of AWS

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-efs/

43. Question

You are a Solutions Architect at a media company and you need to build an application stack that can receive customer comments from sporting events. The application is expected to receive significant load that could scale to millions of messages within a short space of time following high-profile matches. As you are unsure of the load required for the database layer what is the most cost-effective way to ensure that the messages are not dropped?

1. Use RDS Auto Scaling for the database layer which will automatically scale as required
2. Create an SQS queue and modify the application to write to the SQS queue. Launch another application instance the polls the queue and writes messages to the database
3. Use DynamoDB and provision enough write capacity to handle the highest expected load
4. Write the data to an S3 bucket, configure RDS to poll the bucket for new messages

Answer: 2

Explanation:

- Amazon Simple Queue Service (Amazon SQS) is a web service that gives you access to message queues that store messages waiting to be processed. SQS offers a reliable, highly-scalable, hosted queue for storing messages in transit between computers and is used for distributed/decoupled applications.
- This is a great use case for SQS as the messages you don't have to over-provision the database layer or worry about messages being dropped
- RDS Auto Scaling does not exist. With RDS you have to select the underlying EC2 instance type to use and pay for that regardless of the actual load on the DB. Note that a new feature released in June 2019 does allow Auto Scaling for the RDS storage, but not the compute layer.

With DynamoDB there are now 2 pricing options:

- Provisioned capacity has been around forever and is one of the incorrect answers to this question. With provisioned capacity you have to specify the number of read/write capacity units to provision and pay for these regardless of the load on the database.
- With the the new On-demand capacity mode DynamoDB is charged based on the data reads and writes your application performs on your tables. You do not need to specify how much read and write throughput you expect your application to perform because DynamoDB instantly accommodates your workloads as they ramp up or down. it might be a good solution to this question but is not an available option.

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application-integration/amazon-sqs/

44. Question

A company needs to store data for 5 years. The company will need to have immediate and highly available access to the data at any point in time but will not require frequent access.

Which lifecycle action should be taken to meet the requirements while reducing costs?

1. Transition objects from Amazon S3 Standard to the GLACIER storage class
2. Transition objects from Amazon S3 Standard to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)
3. Transition objects to expire after 5 years
4. Transition objects from Amazon S3 Standard to Amazon S3 Standard-Infrequent Access (S3 Standard-IA)

Answer: 4
Explanation:

- This is a good use case for S3 Standard-IA which provides immediate access and 99.9% availability.
- Expiring the objects after 5 years is going to delete them at the end of the 5-year period, but you still need to work out the best storage solution to use before then, and this answer does not provide a solution.
- The S3 One Zone-IA tier provides immediate access, but the availability is lower at 99.5% so this is not the best option.
- The Glacier storage class does not provide immediate access. You can retrieve within hours or minutes, but you do need to submit a job to retrieve the data.

References:
https://aws.amazon.com/s3/storage-classes/
https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

45. Question

A Solutions Architect is designing an application that will run on Amazon ECS behind an Application Load Balancer (ALB). For security reasons, the Amazon EC2 host instances for the ECS cluster are in a private subnet.

What should be done to ensure that the incoming traffic to the host instances is from the ALB only?

1. Update the EC2 cluster security group to allow incoming access from the IP address of the ALB only
2. Modify the security group used by the EC2 cluster to allow incoming traffic from the security group used by the ALB only
3. Create network ACL rules for the private subnet to allow incoming traffic on ports 32768 through 61000 from the IP address of the ALB only
4. Enable AWS WAF on the ALB and enable the ECS rule

Answer: 2
Explanation:

- The best way to accomplish this requirement is to restrict incoming traffic to the Security Group used by the ALB. This will ensure that only the ALB (and its nodes) will be able to connect to the EC2 instances in the ECS cluster.
- You should not use the IP address of the ALB in the Security Group rules as an ALB has multiple nodes in each AZ in which it has subnets defined. Always use security groups whenever you can.
- Network ACLs work at the subnet level. It is preferable to use Security Groups which work at the instance level. Also, you should not use the IP of the ALB as it will have multiple nodes / IPs and it would be cumbersome to setup and administer.
- Enabling a WAF is useful when you need to protect against malicious code. However, this is not a requirement for this solution, you just need to restrict incoming traffic to the ALB.

References:
https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

46. Question

A Solutions Architect is designing a highly-scalable system to track records. Records must remain available for immediate download for three months, and then the records must be deleted.

What's the most appropriate decision for this use case?

1. Store the files on Amazon EFS, and create a lifecycle policy to remove the files after three months
2. Store the files on Amazon S3, and create a lifecycle policy to remove the files after three months
3. Store the files on Amazon EBS, and create a lifecycle policy to remove the files after three months
4. Store the files on Amazon Glacier, and create a lifecycle policy to remove the files after three months

Answer: 2
Explanation:

- With S3 you can create a lifecycle action using the "expiration action element" which expires objects (deletes them) at the specified time
- S3 lifecycle actions apply to any storage class, including Glacier, however Glacier would not allow immediate download
- There is no lifecycle policy available for deleting files on EBS and EFS
- NOTE: The new Amazon Data Lifecycle Manager (DLM) feature automates the creation, retention, and deletion of EBS snapshots but not the individual files within an EBS volume. This is a new feature that may not yet feature on the exam

References:
https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

47. Question

A Solutions Architect needs to allow another AWS account programmatic access to upload objects to his bucket. The Solutions Architect needs to ensure that he retains full control of the objects uploaded to the bucket. How can this be done?

1. The Architect will need to instruct the user in the other AWS account to grant him access when uploading objects
2. The Architect will need to take ownership of objects after they have been uploaded

3. The Architect can use a resource-based bucket policy that grants cross-account access and include a conditional statement that only allows uploads if full control access is granted to the Architect
4. The Architect can use a resource-based ACL with an IAM policy that grants cross-account access and include a conditional statement that only allows uploads if full control access is granted to the Architect

Answer: 3
Explanation:

- You can use a resource-based bucket policy to allow another AWS account to upload objects to your bucket and use a conditional statement to ensure that full control permissions are granted to a specific account identified by an ID (e.g. email address)
- You cannot use a resource-based ACL with IAM policy as this configuration does not support conditional statements
- Taking ownership of objects is not a concept that is valid in Amazon S3 and asking the user in the other AWS account to grant access when uploading is not a good method as technical controls to enforce this behavior are preferred

References:
https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html
https://aws.amazon.com/premiumsupport/knowledge-center/cross-account-access-s3/
https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

48. Question

You are creating a design for a web-based application that will be based on a web front-end using EC2 instances and a database back-end. This application is a low priority and you do not want to incur costs in general day to day management. Which AWS database service can you use that will require the least operational overhead?

1. DynamoDB
2. EMR
3. RedShift
4. RDS

Answer: 1
Explanation:

- Out of the options in the list, DynamoDB requires the least operational overhead as there are no backups, maintenance periods, software updates etc. to deal with
- RDS, RedShift and EMR all require some operational overhead to deal with backups, software updates and maintenance periods

References:
https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/

49. Question

A company's Amazon RDS MySQL DB instance may be rebooted for maintenance and to apply patches. This database is critical and potential user disruption must be minimized.

What should the Solution Architect do in this scenario?

1. Set up an Amazon RDS MySQL cluster
2. Create an RDS MySQL Read Replica
3. Set the Amazon RDS MySQL to Multi-AZ
4. Create an Amazon EC2 instance MySQL cluster

Answer: 3
Explanation:

- With RDS in multi-AZ configuration system upgrades like OS patching, DB Instance scaling and system upgrades, are applied first on the standby, before failing over and modifying the other DB Instance. This means the database is always available with minimal disruption.

- You cannot create a “RDS MySQL cluster” with Amazon RDS. If you want to create a MySQL cluster you need to install on EC2 (which is another option presented). If you install in EC2 you must manage the whole process of patching and failover yourself as it’s not a managed solution.
- Amazon RDS MySQL Read Replicas can serve reads but not writes so there would be a disruption if the application is writing to the DB while the system updates are taking place.

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-rds/

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_UpgradeDBInstance.Maintenance.html

50. Question

You would like to share some documents with public users accessing an S3 bucket over the Internet. What are two valid methods of granting public read permissions so you can share the documents? (choose 2)

1. Grant public read access to the objects when uploading
2. Grant public read on all objects using the S3 bucket ACL
3. Share the documents using CloudFront and a static website
4. Use the AWS Policy Generator to create a bucket policy for your Amazon S3 bucket granting read access to public anonymous users
5. Share the documents using a bastion host in a public subnet

Answer: 1,4

Explanation:

- Access policies define access to resources and can be associated with resources (buckets and objects) and users
- You can use the AWS Policy Generator to create a bucket policy for your Amazon S3 bucket. Bucket policies can be used to grant permissions to objects
- You can define permissions on objects when uploading and at any time afterwards using the AWS Management Console.

- You cannot use a bucket ACL to grant permissions to objects within the bucket. You must explicitly assign the permissions to each object through an ACL attached as a subresource to that object
- Using an EC2 instance as a bastion host to share the documents is not a feasible or scalable solution
- You can configure an S3 bucket as a static website and use CloudFront as a front-end however this is not necessary just to share the documents and imposes some constraints on the solution

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

51. Question

You have created a private Amazon CloudFront distribution that serves files from an Amazon S3 bucket and is accessed using signed URLs. You need to ensure that users cannot bypass the controls provided by Amazon CloudFront and access content directly.

How can this be achieved? (choose 2)

1. Create an origin access identity and associate it with your distribution
2. Modify the Edge Location to restrict direct access to Amazon S3 buckets
3. Modify the permissions on the origin access identity to restrict read access to the Amazon S3 bucket
4. Create a new signed URL that requires users to access the Amazon S3 bucket through Amazon CloudFront
5. Modify the permissions on the Amazon S3 bucket so that only the origin access identity has read and download permissions

Answer: 1,5

Explanation:

- If you're using an Amazon S3 bucket as the origin for a CloudFront distribution, you can either allow everyone to have access to the files there, or you can restrict access. If you limit

access by using CloudFront signed URLs or signed cookies you also won't want people to be able to view files by simply using the direct URL for the file. Instead, you want them to only access the files by using the CloudFront URL, so your protections work. This can be achieved by creating an OAI and associating it with your distribution and then modifying the permissions on the S3 bucket to only allow the OAI to access the files

- You do not modify permissions on the OAI – you do this on the S3 bucket
- If users are accessing the S3 files directly, a new signed URL is not going to stop them
- You cannot modify edge locations to restrict access to S3 buckets

References:

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html

52. Question

Your company shares some HR videos stored in an Amazon S3 bucket via CloudFront. You need to restrict access to the private content so users coming from specific IP addresses can access the videos and ensure direct access via the Amazon S3 bucket is not possible.

How can this be achieved?

1. Configure CloudFront to require users to access the files using a signed URL, and configure the S3 bucket as a website endpoint
2. Configure CloudFront to require users to access the files using signed cookies, and move the files to an encrypted EBS volume
3. Configure CloudFront to require users to access the files using signed cookies, create an origin access identity (OAI) and instruct users to login with the OAI
4. Configure CloudFront to require users to access the files using a signed URL, create an origin access identity (OAI) and restrict access to the files in the Amazon S3 bucket to the OAI

Answer: 4

Explanation:

- A signed URL includes additional information, for example, an expiration date and time, that gives you more control over access to your content. You can also specify the IP address or range of IP addresses of the users who can access your content
- If you use CloudFront signed URLs (or signed cookies) to limit access to files in your Amazon S3 bucket, you may also want to prevent users from directly accessing your S3 files by using Amazon S3 URLs. To achieve this, you can create an origin access identity (OAI), which is a special CloudFront user, and associate the OAI with your distribution. You can then change the permissions either on your Amazon S3 bucket or on the files in your bucket so that only the origin access identity has read permission (or read and download permission)
- Users cannot login with an OAI
- You cannot use CloudFront and an OAI when you're S3 bucket is configured as a website endpoint
- You cannot use CloudFront to pull data directly from an EBS volume

References:

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

53. Question

There is a temporary need to share some video files that are stored in a private S3 bucket. The consumers do not have AWS accounts and you need to ensure that only authorized consumers can access the files. What is the best way to enable this access?

1. Enable public read access for the S3 bucket
2. Use CloudFront to distribute the files using authorization hash tags
3. Generate a pre-signed URL and distribute it to the consumers

4. Configure an allow rule in the Security Group for the IP addresses of the consumers

Answer: 3
Explanation:

- S3 pre-signed URLs can be used to provide temporary access to a specific object to those who do not have AWS credentials. This is the best option
- Enabling public read access does not restrict the content to authorized consumers
- You cannot use CloudFront as hash tags are not a CloudFront authentication mechanism
- Security Groups do not apply to S3 buckets

References:
https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

54. Question

You would like to provide some on-demand and live streaming video to your customers. The plan is to provide the users with both the media player and the media files from the AWS cloud. One of the features you need is for the content of the media files to begin playing while the file is still being downloaded.

What AWS services can deliver these requirements? (choose 2)

1. Store the media files in an S3 bucket
2. Use CloudFront with a Web and RTMP distribution
3. Store the media files on an EBS volume
4. Use CloudFront with an RTMP distribution
5. Store the media files on an EC2 instance

Answer: 1,2
Explanation:

- For serving both the media player and media files you need two types of distributions:

- A web distribution for the media player
- An RTMP distribution for the media files

- RTMP:

  - Distribute streaming media files using Adobe Flash Media Server's RTMP protocol
  - Allows an end user to begin playing a media file before the file has finished downloading from a CloudFront edge location
  - Files must be stored in an S3 bucket (not an EBS volume or EC2 instance)

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/

55. Question

The company you work for is currently transitioning their infrastructure and applications into the AWS cloud. You are planning to deploy an Elastic Load Balancer (ELB) that distributes traffic for a web application running on EC2 instances. You still have some application servers running on-premise and you would like to distribute application traffic across both your AWS and on-premises resources.

How can this be achieved?

1. Provision a Direct Connect connection between your on-premises location and AWS and create a target group on an ALB to use IP based targets for both your EC2 instances and on-premises servers
2. Provision a Direct Connect connection between your on-premises location and AWS and create a target group on an ALB to use Instance ID based targets for both your EC2 instances and on-premises servers
3. Provision an IPSec VPN connection between your on-premises location and AWS and create a CLB that uses cross-zone load balancing to distributed traffic across EC2 instances and on-premises servers

4. This cannot be done, ELBs are an AWS service and can only distributed traffic within the AWS cloud

Answer: 1
Explanation:

- The ALB (and NLB) supports IP addresses as targets
- Using IP addresses as targets allows load balancing any application hosted in AWS or on-premises using IP addresses of the application back-ends as targets
- You must have a VPN or Direct Connect connection to enable this configuration to work
- You cannot use instance ID based targets for on-premises servers and you cannot mix instance ID and IP address target types in a single target group
- The CLB does not support IP addresses as targets

References:
https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/
https://aws.amazon.com/blogs/aws/new-application-load-balancing-via-ip-address-to-aws-on-premises-resources/

56. Question

A Solutions Architect is developing a mobile web app that will provide access to health-related data. The web apps will be tested on Android and iOS devices. The Architect needs to run tests on multiple devices simultaneously and to be able to reproduce issues, and record logs and performance data to ensure quality before release.

What AWS service can be used for these requirements?

1. AWS Cognito
2. AWS Device Farm
3. AWS Workspaces
4. Amazon Appstream 2.0

Answer: 2
Explanation:

- AWS Device Farm is an app testing service that lets you test and interact with your Android, iOS, and web apps on many devices at once, or reproduce issues on a device in real time
- Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily. It is not used for testing
- Amazon WorkSpaces is a managed, secure cloud desktop service
- Amazon AppStream 2.0 is a fully managed application streaming service

References:
https://aws.amazon.com/device-farm/

57. Question

There is a new requirement to implement in-memory caching for a Financial Services application due to increasing read-heavy load. The data must be stored persistently. Automatic failover across AZs is also required.

Which two items from the list below are required to deliver these requirements? (choose 2)

1. ElastiCache with the Memcached engine
2. Multi-AZ with Cluster mode and Automatic Failover enabled
3. ElastiCache with the Redis engine
4. Multiple nodes placed in different AZs
5. Read replica with failover mode enabled

Answer: 2,3

Explanation:

- Redis engine stores data persistently
- Memached engine does not store data persistently
- Redis engine supports Multi-AZ using read replicas in another AZ in the same region
- You can have a fully automated, fault tolerant ElastiCache-Redis implementation by enabling both cluster mode and multi-AZ failover

- Memcached engine does not support Multi-AZ failover or replication

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-elasticache/

58. Question

An application you are designing receives and processes files. The files are typically around 4GB in size and the application extracts metadata from the files which typically takes a few seconds for each file. The pattern of updates is highly dynamic with times of little activity and then multiple uploads within a short period of time.

What architecture will address this workload the most cost efficiently?

1. Upload files into an S3 bucket, and use the Amazon S3 event notification to invoke a Lambda function to extract the metadata
2. Store the file in an EBS volume which can then be accessed by another EC2 instance for processing
3. Place the files in an SQS queue, and use a fleet of EC2 instances to extract the metadata
4. Use a Kinesis data stream to store the file, and use Lambda for processing

Answer: 1

Explanation:

- Storing the file in an S3 bucket is the most cost-efficient solution, and using S3 event notifications to invoke a Lambda function works well for this unpredictable workload
- Kinesis data streams runs on EC2 instances and you must therefore provision some capacity even when the application is not receiving files. This is not as cost-efficient as storing them in an S3 bucket prior to using Lambda for the processing
- SQS queues have a maximum message size of 256KB. You can use the extended client library for Java to use pointers to a payload on S3 but the maximum payload size is 2GB

- Storing the file in an EBS volume and using EC2 instances for processing is not cost efficient

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/amazon-s3/

https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html

59. Question

A Solutions Architect needs to transform data that is being uploaded into S3. The uploads happen sporadically and the transformation should be triggered by an event. The transformed data should then be loaded into a target data store.

What services would be used to deliver this solution in the MOST cost-effective manner? (choose 2)

1. Use AWS Glue to extract, transform and load the data into the target data store
2. Configure CloudFormation to provision a Kinesis data stream to transform the data and load it into S3
3. Configure S3 event notifications to trigger a Lambda function when data is uploaded and use the Lambda function to trigger the ETL job
4. Configure CloudFormation to provision AWS Data Pipeline to transform the data
5. Configure a CloudWatch alarm to send a notification to CloudFormation when data is uploaded

Answer: 1,3

Explanation:

- S3 event notifications triggering a Lambda function is completely serverless and cost-effective
- AWS Glue can trigger ETL jobs that will transform that data and load it into a data store such as S3
- Kinesis Data Streams is used for processing data, rather than extracting and transforming it. The Kinesis consumers are EC2

instances which are not as cost-effective as serverless solutions

- AWS Data Pipeline can be used to automate the movement and transformation of data, it relies on other services to actually transform the data

References:

https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html

https://aws.amazon.com/glue/

60. Question

A company has divested a single business unit and needs to move the AWS account owned by the business unit to another AWS Organization. How can this be achieved?

1. Migrate the account using the AWS Organizations console
2. Create a new account in the destination AWS Organization and migrate resources
3. Create a new account in the destination AWS Organization and share the original resources using AWS Resource Access Manager
4. Migrate the account using AWS CloudFormation

Answer: 1

Explanation:

- Accounts can be migrated between organizations. To do this you must have root or IAM access to both the member and master accounts. Resources will remain under the control of the migrated account.
- You do not need to use AWS CloudFormation. You can use the Organizations API or AWS CLI for when there are many accounts to migrate and therefore you could use CloudFormation for any additional automation but it is not necessary for this scenario.
- You do not need to create a new account in the destination AWS Organization as you can just migrate the existing account.

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-organizations/

https://aws.amazon.com/premiumsupport/knowledge-center/organizations-move-accounts/

61. Question

A new application is to be published in multiple regions around the world. The Architect needs to ensure only 2 IP addresses need to be whitelisted. The solution should intelligently route traffic for lowest latency and provide fast regional failover.

How can this be achieved?

1. Launch EC2 instances into multiple regions behind an ALB and use Amazon CloudFront with a pair of static IP addresses
2. Launch EC2 instances into multiple regions behind an NLB and use AWS Global Accelerator
3. Launch EC2 instances into multiple regions behind an ALB and use a Route 53 failover routing policy
4. Launch EC2 instances into multiple regions behind an NLB with a static IP address

Answer: 2

Explanation:

- AWS Global Accelerator uses the vast, congestion-free AWS global network to route TCP and UDP traffic to a healthy application endpoint in the closest AWS Region to the user. This means it will intelligently route traffic to the closest point of presence (reducing latency). Seamless failover is ensured as AWS Global Accelerator uses anycast IP address which means the IP does not change when failing over between regions so there are no issues with client caches having incorrect entries that need to expire. This is the only solution that provides deterministic failover.
- An NLB with a static IP is a workable solution as you could configure a primary and secondary address in applications.

However, this solution does not intelligently route traffic for lowest latency.

- A Route 53 failover routing policy uses a primary and standby configuration. Therefore, it sends all traffic to the primary until it fails a health check at which time it sends traffic to the secondary. This solution does not intelligently route traffic for lowest latency.
- Amazon CloudFront cannot be configured with "a pair of static IP addresses".

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/aws-global-accelerator/

https://aws.amazon.com/global-accelerator/

https://aws.amazon.com/global-accelerator/faqs/

https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global-accelerator.html

62. Question

An e-commerce web application needs a highly scalable key-value database. Which AWS database service should be used?

1. Amazon DynamoDB
2. Amazon ElastiCache
3. Amazon RedShift
4. Amazon RDS

Answer: 1

Explanation:

- A key-value database is a type of nonrelational (NoSQL) database that uses a simple key-value method to store data. A key-value database stores data as a collection of key-value pairs in which a key serves as a unique identifier. Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability – this is the best database for these requirements.

- Amazon RDS is a relational (SQL) type of database, not a key-value / nonrelational database.
- Amazon RedShift is a data warehouse service used for online analytics processing (OLAP) workloads.
- Amazon ElastiCache is an in-memory caching database. This is not a nonrelational key-value database.

References:

https://aws.amazon.com/nosql/key-value/

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/

63. Question

An Architect needs to find a way to automatically and repeatably create many member accounts within an AWS Organization. The accounts also need to be moved into an OU and have VPCs and subnets created.

What is the best way to achieve this?

1. Use the AWS Management Console
2. Use CloudFormation with scripts
3. Use the AWS Organizations API
4. Use the AWS CLI

Answer: 2

Explanation:

- The best solution is to use a combination of scripts and AWS CloudFormation. You will also leverage the AWS Organizations API. This solution can provide all of the requirements.
- You can create member accounts with the AWS Organizations API. However, you cannot use that API to configure the account and create VPCs and subnets.
- Using the AWS Management Console is not a method of automatically creating the resources.
- You can do all tasks using the AWS CLI but it is better to automate the process using AWS CloudFormation.

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/aws-organizations/

https://aws.amazon.com/blogs/security/how-to-use-aws-organizations-to-automate-end-to-end-account-creation/

64. Question

A company has acquired another business and needs to migrate their 50TB of data into AWS within 1 month. They also require a secure, reliable and private connection to the AWS cloud.

How are these requirements best accomplished?

1. Provision an AWS Direct Connect connection and migrate the data over the link
2. Launch a Virtual Private Gateway (VPG) and migrate the data over the AWS VPN
3. Migrate data using AWS Snowball. Provision an AWS VPN initially and order a Direct Connect link
4. Provision an AWS VPN CloudHub connection and migrate the data over redundant links

Answer: 3

Explanation:

- AWS Direct Connect provides a secure, reliable and private connection. However, lead times are often longer than 1 month so it cannot be used to migrate data within the timeframes. Therefore, it is better to use AWS Snowball to move the data and order a Direct Connect connection to satisfy the other requirement later on. In the meantime, the organization can use an AWS VPN for secure, private access to their VPC.
- A VPG is the AWS-side of an AWS VPN. A VPN does not provide a private connection and is not reliable as you can never guarantee the latency over the Internet.
- AWS VPN CloudHub is a service for connecting multiple sites into your VPC over VPN connections. It is not used for aggregating links and the limitations of Internet bandwidth from

the company where the data is stored will still be an issue. It also uses the public Internet so is not a private or reliable connection.

References:

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/aws-direct-connect/

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/migration/aws-snowball/

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

https://aws.amazon.com/directconnect/

65. Question

An organization in the health industry needs to create an application that will transmit protected health data to thousands of service consumers in different AWS accounts. The application servers run on EC2 instances in private VPC subnets. The routing for the application must be fault tolerant.

What should be done to meet these requirements?

1. Create a proxy server in the service provider VPC to route requests from service consumers to the application servers
2. Create an internal Application Load Balancer in the service provider VPC and put application servers behind it
3. Create a virtual private gateway connection between each pair of service provider VPCs and service consumer VPCs
4. Create a VPC endpoint service and grant permissions to specific service consumers to create a connection

Answer: 4

Explanation:

- What you need to do here is offer the service through a service provider offering. This is a great use case for a VPC endpoint service using AWS PrivateLink (referred to as an endpoint service). Other AWS principals can then create a connection from their VPC to your endpoint service using an interface VPC endpoint. You are acting as the service provider and offering the service to service consumers. This configuration

uses a Network Load Balancer and can be fault tolerant by configuring multiple subnets in which the EC2 instances are running.

- Creating a virtual private gateway connection between each pair of service provider VPCs and service consumer VPCs would be extremely cumbersome and is not the best option.
- Creating an internal ALB would not work as you need consumers from outside your VPC to be able to connect.
- Using a proxy service is possible but would not scale as well and would present a single point of failure unless there is some load balancing to multiple proxies (not mentioned).

References:

https://docs.aws.amazon.com/vpc/latest/userguide/endpoint-service.html

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/