Attempt 1

All knowledge areas

All questions

Top of Form

Question 1: **Incorrect**

**As a SysOps engineer working at Digital Cloud Training, you are constantly trying to improve your processes for collecting log data. Currently you are collecting logs from across your AWS resources using CloudWatch and a combination of standard and custom metrics. You are currently investigating how you can optimize the storage of log files collected by CloudWatch.**

**Which of the following are valid options for storing CloudWatch log files? (choose 2)**

* ​

EBS

**(Incorrect)**

* ​

RedShift

* ​

EFS

**(Incorrect)**

* ​

CloudWatch Logs

**(Correct)**

* ​

Splunk

**(Correct)**

**Explanation**

* Valid options for storing logs include:
* - CloudWatch Logs
* - Centralized logging system (e.g. Splunk)
* - Custom script and store on S3
* RedShift, EFS and EBS are not valid options for storing CloudWatch log files

**References:**

* <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management-tools/amazon-cloudwatch/>

Bottom of Form

Top of Form

Question 2: **Correct**

**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?**

* ​

Use RedShift in a Multi-AZ configuration

* ​

Install a relational database on EC2 instances in multiple AZs and create a cluster

* ​

Use DynamoDB

* ​

Use RDS in a Multi-AZ configuration

**(Correct)**

**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/>

Bottom of Form

Top of Form

Question 3: **Incorrect**

**Your company has offices in several locations around the world. Each office utilizes resources deployed in the geographically closest AWS region. You would like to implement connectivity between all of the VPCs so that you can provide full access to each other’s resources. As you are security conscious you would like to ensure the traffic is encrypted and does not traverse the public Internet. The topology should be many-to-many to enable all VPCs to access the resources in all other VPCs.**

**How can you successfully implement this connectivity using only AWS services? (choose 2)**

* ​

Implement a fully meshed architecture

**(Correct)**

* ​

Use inter-region VPC peering

**(Correct)**

* ​

Implement a hub and spoke architecture

* ​

Use VPC endpoints between VPCs

**(Incorrect)**

* ​

Use software VPN appliances running on EC2 instances

**Explanation**

* Peering connections can be created with VPCs in different regions (available in most regions now)
* Data sent between VPCs in different regions is encrypted (traffic charges apply)
* You cannot do transitive peering so a hub and spoke architecture would not allow all VPCs to communicate directly with each other. For this you need to establish a mesh topology
* A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services, it does not provide full VPC to VPC connectivity
* Using software VPN appliances to connect VPCs together is not the best solution as it is cumbersome, expensive and would introduce bandwidth and latency constraints (amongst other problems)

**References:**

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

Bottom of Form

Top of Form

Question 4: **Correct**

**You are troubleshooting a connectivity issue where you cannot connect to an EC2 instance in a public subnet in your VPC from the Internet. Which of the configuration items in the list below would you check first? (choose 2)**

* ​

There is a NAT Gateway installed in the subnet

* ​

The subnet has “Auto-assign public IPv4 address” set to “Yes”

**(Correct)**

* ​

The security group attached to the EC2 instance has an inbound rule allowing the traffic

**(Correct)**

* ​

The subnet route table has an attached NAT Gateway

* ​

The EC2 instance has a private IP address associated with it

**Explanation**

* Public subnets are subnets that have:
  + “Auto-assign public IPv4 address” set to “Yes” which will assign a public IP
  + The subnet route table has an attached Internet Gateway
* The instance will also need to a security group with an inbound rule allowing the traffic
* EC2 instances always have a private IP address assigned. When using a public subnet with an Internet Gateway the instance needs a public IP to be addressable from the Internet
* NAT gateways are used to enable **outbound** Internet access for instances in private **subnets**

**References:**

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

Bottom of Form

Top of Form

Question 5: **Incorrect**

**A Solutions Architect has been asked to suggest a solution for analyzing data in S3 using standard SQL queries. The solution should use a serverless technology.**

**Which AWS service can the Architect use?**

* ​

AWS Glue

* ​

AWS Data Pipeline

* ​

Amazon Athena

**(Correct)**

* ​

Amazon RedShift

**(Incorrect)**

**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
* Amazon RedShift is used for analytics but cannot analyze data in S3
* AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics. It is not used for analyzing data in S3
* AWS Data Pipeline is a web service that helps you reliably process and move data between different AWS compute and storage services, as well as on-premises data sources, at specified intervals

**References:**

* <https://aws.amazon.com/athena/>

Bottom of Form

Top of Form

Question 6: **Correct**

**An application you manage stores encrypted data in S3 buckets. You need to be able to query the encrypted data using SQL queries and write the encrypted results back the S3 bucket. As the data is sensitive you need to implement fine-grained control over access to the S3 bucket.**

**What combination of services represent the BEST options support these requirements? (choose 2)**

* ​

Use the AWS KMS API to query the encrypted data, and the S3 API for writing the results

* ​

Use Athena for querying the data and writing the results back to the bucket

**(Correct)**

* ​

Use AWS Glue to extract the data, analyze it, and load it back to the S3 bucket

* ​

Use bucket ACLs to restrict access to the bucket

* ​

Use IAM policies to restrict access to the bucket

**(Correct)**

**Explanation**

* Athena also allows you to easily query encrypted data stored in Amazon S3 and write encrypted results back to your S3 bucket. Both, server-side encryption and client-side encryption are supported
* With IAM policies, you can grant IAM users fine-grained control to your S3 buckets, and is preferable to using bucket ACLs
* AWS Glue is an ETL service and is not used for querying and analyzing data in S3
* The AWS KMS API can be used for encryption purposes, however it cannot perform analytics so is not suitable

**References:**

* <https://aws.amazon.com/athena/>
* <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-iam/>

Bottom of Form

Top of Form

Question 7: **Correct**

**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?**

* ​

Use a Kinesis data stream to store the file, and use Lambda for processing

* ​

Store the file in an EBS volume which can then be accessed by another EC2 instance for processing

* ​

Place the files in an SQS queue, and use a fleet of EC2 instances to extract the metadata

* ​

Upload files into an S3 bucket, and use the Amazon S3 event notification to invoke a Lambda function to extract the metadata

**(Correct)**

**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>

Bottom of Form

Top of Form

Question 8: **Incorrect**

**Your client is looking for a fully managed directory service in the AWS cloud. The service should provide an inexpensive Active Directory-compatible service with common directory features. The client is a medium-sized organization with 4000 users. As the client has a very limited budget it is important to select a cost-effective solution.**

**What would you suggest?**

* ​

Amazon Cognito

* ​

AWS Single Sign-On

* ​

AWS Active Directory Service for Microsoft Active Directory

**(Incorrect)**

* ​

AWS Simple AD

**(Correct)**

**Explanation**

* Simple AD is an inexpensive Active Directory-compatible service with common directory features. It is a standalone, fully managed, directory on the AWS cloud and is generally the least expensive option. It is the best choice for less than 5000 users and when you don’t need advanced AD features
* Active Directory Service for Microsoft Active Directory is the best choice if you have more than 5000 users and/or need a trust relationship set up. It provides advanced AD features that you don't get with SimpleAD
* Amazon Cognito is an authentication service for web and mobile apps
* AWS Single Sign-On (SSO) is a cloud SSO service that makes it easy to centrally manage SSO access to multiple AWS accounts and business applications

**References:**

* <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-directory-service/>

Bottom of Form

Top of Form

Question 9: **Correct**

**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)**

* ​

A workflow service such as Amazon Simple Workflow Service (SWF)

* ​

Sticky sessions on an Elastic Load Balancer (ELB)

**(Correct)**

* ​

A key/value store such as ElastiCache Redis

**(Correct)**

* ​

A block storage service such as Elastic Block Store (EBS)

* ​

A relational data store such as Amazon RDS

**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/>

Bottom of Form

Top of Form

Question 10: **Incorrect**

**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)**

* ​

Lambda for transforming the data

**(Correct)**

* ​

Kinesis Video Streams for capturing the data and loading it into RedShift

* ​

AWS Data Pipeline for transforming the data

* ​

EMR for transforming the data

**(Incorrect)**

* ​

Kinesis Data Firehose for capturing the data and loading it into RedShift

**(Correct)**

**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/>

Bottom of Form

Top of Form

Question 11: **Correct**

**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?**

* ​

AWS KMS API

**(Correct)**

* ​

API Gateway with STS

* ​

AWS Certificate Manager

* ​

IAM Access Key

**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>

Bottom of Form

Top of Form

Question 12: **Incorrect**

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

* ​

Maintain the original snapshot; subsequent snapshots will overwrite one another

* ​

Maintain a single snapshot; the latest snapshot is both incremental and complete

**(Correct)**

* ​

Maintain the most current snapshot; archive the original to Amazon Glacier

**(Incorrect)**

* ​

Maintain two snapshots: the original snapshot and the latest incremental snapshot

**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/>

Bottom of Form

Top of Form

Question 13: **Correct**

**You are a Solutions Architect at Digital Cloud Training. One of your clients runs an application that writes data to a DynamoDB table. The client has asked how they can implement a function that runs code in response to item level changes that take place in the DynamoDB table. What would you suggest to the client?**

* ​

Enable DynamoDB Streams and create an event source mapping between AWS Lambda and the relevant stream

**(Correct)**

* ​

Use Kinesis Data Streams and configure DynamoDB as a producer

* ​

Create a local secondary index that records item level changes and write some custom code that responds to updates to the index

* ​

Enable server access logging and create an event source mapping between AWS Lambda and the S3 bucket to which the logs are written

**Explanation**

* DynamoDB Streams help you to keep a list of item level changes or provide a list of item level changes that have taken place in the last 24hrs. Amazon DynamoDB is integrated with AWS Lambda so that you can create triggers—pieces of code that automatically respond to events in DynamoDB Streams
* If you enable DynamoDB Streams on a table, you can associate the stream ARN with a Lambda function that you write. Immediately after an item in the table is modified, a new record appears in the table's stream. AWS Lambda polls the stream and invokes your Lambda function synchronously when it detects new stream records
* An event source mapping identifies a poll-based event source for a Lambda function. It can be either an Amazon Kinesis or DynamoDB stream. Event sources maintain the mapping configuration except for stream-based services (e.g. DynamoDB, Kinesis) for which the configuration is made on the Lambda side and Lambda performs the polling
* You cannot configure DynamoDB as a Kinesis Data Streams producer
* You can write Lambda functions to process S3 bucket events, such as the object-created or object-deleted events. For example, when a user uploads a photo to a bucket, you might want Amazon S3 to invoke your Lambda function so that it reads the image and creates a thumbnail for the photo . However, the questions asks for a solution that runs code in response to changes in a DynamoDB table, not an S3 bucket
* A local secondary index maintains an alternate sort key for a given partition key value, it does not record item level changes

**References:**

* <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/>
* <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.Lambda.html>
* <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/>

Bottom of Form

Top of Form

Question 14: **Correct**

**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?**

* ​

Kinesis Data Streams and Kinesis Data Analytics

**(Correct)**

* ​

DynamoDB and EMR

* ​

ElastiCache and EMR

* ​

Kinesis Data Streams and Kinesis Firehose

**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/>

Bottom of Form

Top of Form

Question 15: **Incorrect**

**An application hosted in your VPC uses an EC2 instance with a MySQL DB running on it. The database uses a single 1TB General Purpose SSD (GP2) EBS volume. Recently it has been noticed that the database is not performing well and you need to improve the read performance. What are two possible ways this can be achieved? (choose 2)**

* ​

Create an active/passive cluster using MySQL

* ​

Use a provisioned IOPS volume and specify the number of I/O operations required

**(Correct)**

* ​

Add multiple EBS volumes in a RAID 1 array

* ​

Add an RDS read replica in another AZ

**(Incorrect)**

* ​

Add multiple EBS volumes in a RAID 0 array

**(Correct)**

**Explanation**

* RAID 0 = 0 striping – data is written across multiple disks and increases performance but no redundancy
* RAID 1 = 1 mirroring – creates 2 copies of the data but does not increase performance, only redundancy
* SSD, Provisioned IOPS – I01 provides higher performance than General Purpose SSD (GP2) and you can specify the IOPS required up to 50 IOPS per GB and a maximum of 32000 IOPS
* RDS read replicas cannot be created from EC2 instances
* Creating an active/passive cluster doesn't improve read performance as the passive node is not servicing requests. This is use for fault tolerance

**References:**

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

Bottom of Form

Top of Form

Question 16: **Correct**

**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?**

* ​

Permanently keep a steady state of instance that is needed at 9:00am to guarantee available resources, but use Spot Instances

* ​

Change the Auto Scaling group’s scale out event to scale based on network utilization

* ​

Use Reserved Instances to ensure the system has reserved the right amount of capacity for the scaling events

* ​

Create an Auto Scaling scheduled action to scale out the necessary resources at 8:30am each morning

**(Correct)**

**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>

Bottom of Form

Top of Form

Question 17: **Correct**

**Your organization is planning to go serverless in the cloud. Which of the following combinations of services provides a fully serverless architecture?**

* ​

EC2, EBS, Auto Scaling, ELB

* ​

Lambda, API Gateway, DynamoDB, S3, CloudFront

**(Correct)**

* ​

Lambda, SQS, RDS, S3

* ​

API Gateway, EC2, DynamoDB, S3

**Explanation**

* Serverless is the native architecture of the cloud that enables you to shift more of your operational responsibilities to AWS, increasing your agility and innovation. Serverless allows you to build and run applications and services without thinking about servers. It eliminates infrastructure management tasks such as server or cluster provisioning, patching, operating system maintenance, and capacity provisioning
* Serverless services include Lambda, API Gateway, DynamoDB, S3, SQS, and CloudFront
* EC2 and RDS are not serverless as they both rely on EC2 instances which must be provisioned and managed

**References:**

* <https://aws.amazon.com/serverless/>

Bottom of Form

Top of Form

Question 18: **Correct**

**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?**

* ​

Store the files on Amazon S3, and create a lifecycle policy to remove the files after three months

**(Correct)**

* ​

Store the files on Amazon EBS, and create a lifecycle policy to remove the files after three months

* ​

Store the files on Amazon EFS, and create a lifecycle policy to remove the files after three months

* ​

Store the files on Amazon Glacier, and create a lifecycle policy to remove the files after three months

**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/>

Bottom of Form

Top of Form

Question 19: **Incorrect**

**A Solutions Architect is building a complex application with several back-end APIs. The architect is considering using Amazon API Gateway. With Amazon API Gateway what are features that assist with creating and managing APIs? (Choose 2)**

* ​

Executes your code as functions using serverless technology

* ​

You can define plans that meter and restrict third-party developer access to APIs

**(Correct)**

* ​

You can define the maintenance window or AWS will schedule a 30 minute window

* ​

You can operate multiple API versions and multiple stages for each version simultaneously

**(Correct)**

* ​

Flexible message delivery over multiple transport protocols

**(Incorrect)**

**Explanation**

* Metering – define plans that meter and restrict third-party developer access to APIs
* Lifecycle Management – Operate multiple API versions and multiple stages for each version simultaneously so that existing applications can continue to call previous versions after new API versions are published

**References:**

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

Bottom of Form

Top of Form

Question 20: **Incorrect**

**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?**

* ​

AWS Billing Dashboard

* ​

Cost Explorer

* ​

Cost & Usage reports

**(Incorrect)**

* ​

AWS Budgets

**(Correct)**

**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/>

Bottom of Form

Top of Form

Question 21: **Correct**

**For operational access to your AWS environment you are planning to setup a bastion host implementation. Which of the below are AWS best practices for setting up bastion hosts? (choose 2)**

* ​

Bastion hosts are deployed in the private subnets of the VPC

* ​

Ports are unrestricted to allow full operational access to the bastion hosts

* ​

Deploy in 2 AZs and use an Auto Scaling group to ensure that the number of bastion host instances always matches the desired capacity you specify during launch

**(Correct)**

* ​

Access to the bastion hosts is configured to 0.0.0.0/0 for ingress in security groups

* ​

Elastic IP addresses are associated with the bastion instances to make it easier to remember and allow these IP addresses from on-premises firewalls

**(Correct)**

**Explanation**

* You can configure EC2 instances as bastion hosts (aka jump boxes) in order to access your VPC instances for management. Bastion hosts are deployed in public (not private) subnets within your VPC. You can use the SSH or RDP protocols to connect to bastion hosts
* You need to configure a security group with the relevant permissions to allow the SSH or RDP protocols. You can also use security group rules to restrict the IP addresses/CIDRs that can access the bastion host. Bastion hosts can use auto-assigned public IPs or Elastic IPs
* It is a best practice is to deploy Linux bastion hosts in two AZs, use Auto Scaling (set to 1 to just replace)and Elastic IP addresses
* Setting the security rule to allow from the 0.0.0.0/0 source would allow any host on the Internet to access your bastion. It's a security best practice to restrict the sources to known (safe) IP addresses or CIDR blocks. You would not want to allow unrestricted access to ports on the bastion host

**References:**

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

Bottom of Form

Top of Form

Question 22: **Incorrect**

**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?**

* ​

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

**(Correct)**

* ​

Configure CloudFront to require users to access the files using signed cookies, and move the files to an encrypted EBS volume

* ​

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

**(Incorrect)**

* ​

Configure CloudFront to require users to access the files using a signed URL, and configure the S3 bucket as a website endpoint

**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/>

Bottom of Form

Top of Form

Question 23: **Correct**

**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)**

* ​

ElastiCache with the Memcached engine

* ​

Multiple nodes placed in different AZs

* ​

Multi-AZ with Cluster mode and Automatic Failover enabled

**(Correct)**

* ​

Read replica with failover mode enabled

* ​

ElastiCache with the Redis engine

**(Correct)**

**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/>

Bottom of Form

Top of Form

Question 24: **Correct**

**A manufacturing company captures data from machines running at customer sites. Currently, thousands of machines send data every 5 minutes, and this is expected to grow to hundreds of thousands of machines in the near future. The data is logged with the intent to be analyzed in the future as needed.**

**What is the SIMPLEST method to store this streaming data at scale?**

* ​

Create an Auto Scaling Group of Amazon EC2 instances behind ELBs to write data into Amazon RDS

* ​

Create an Amazon EC2 instance farm behind an ELB to store the data in Amazon EBS Cold HDD volumes

* ​

Create an Amazon SQS queue, and have the machines write to the queue

* ​

Create an Amazon Kinesis Firehose delivery stream to store the data in Amazon S3

**(Correct)**

**Explanation**

* Kinesis Data Firehose is the easiest way to load streaming data into data stores and analytics tools. It captures, transforms, and loads streaming data and you can deliver the data to “destinations” including Amazon S3 buckets for later analysis
* Writing data into RDS via a series of EC2 instances and a load balancer is more complex and more expensive. RDS is also not an ideal data store for this data
* Using an SQS queue to store the data is not possible as the data needs to be stored long-term and SQS queues have a maximum retention time of 14 days
* Storing the data in EBS wold be expensive and as EBS volumes cannot be shared by multiple instances you would have a bottleneck of a single EC2 instance writing the data

**References:**

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

Bottom of Form

Top of Form

Question 25: **Incorrect**

**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)**

* ​

Use AWS Glue to extract, transform and load the data into the target data store

**(Correct)**

* ​

Configure CloudFormation to provision a Kinesis data stream to transform the data and load it into S3

**(Incorrect)**

* ​

Configure CloudFormation to provision AWS Data Pipeline to transform the data

* ​

Configure a CloudWatch alarm to send a notification to CloudFormation when data is uploaded

* ​

Configure S3 event notifications to trigger a Lambda function when data is uploaded and use the Lambda function to trigger the ETL job

**(Correct)**

**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/>

Bottom of Form

Top of Form

Question 26: **Correct**

**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?**

* ​

DynamoDB

**(Correct)**

* ​

RDS with Microsoft SQL

* ​

RDS with MySQL

* ​

RedShift

**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/>

Bottom of Form

Top of Form

Question 27: **Incorrect**

**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)**

* ​

Share the documents using CloudFront and a static website

* ​

Grant public read on all objects using the S3 bucket ACL

**(Incorrect)**

* ​

Share the documents using a bastion host in a public subnet

* ​

Grant public read access to the objects when uploading

**(Correct)**

* ​

Use the AWS Policy Generator to create a bucket policy for your Amazon S3 bucket granting read access to public anonymous users

**(Correct)**

**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/>

Bottom of Form

Top of Form

Question 28: **Incorrect**

**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?**

* ​

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

**(Correct)**

* ​

The Architect will need to instruct the user in the other AWS account to grant him access when uploading objects

* ​

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

**(Incorrect)**

* ​

The Architect will need to take ownership of objects after they have been uploaded

**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 behaviour 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/>

Bottom of Form

Top of Form

Question 29: **Correct**

**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?**

* ​

AWS Workspaces

* ​

AWS Cognito

* ​

AWS Device Farm

**(Correct)**

* ​

Amazon Appstream 2.0

**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/>

Bottom of Form

Top of Form

Question 30: **Correct**

**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?**

* ​

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

**(Correct)**

* ​

Write the data to an S3 bucket, configure RDS to poll the bucket for new messages

* ​

Use RDS Auto Scaling for the database layer which will automatically scale as required

* ​

Use DynamoDB and provision enough write capacity to handle the highest expected load

**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
* 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/>

Bottom of Form

Top of Form

Question 31: **Correct**

**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?**

* ​

Configure a NAT Gateway for each AZ with an Elastic IP address

**(Correct)**

* ​

Use multiple Internet-facing Application Load Balancers with Elastic IP addresses

* ​

Configure redundant Internet Gateways and update the routing tables for each subnet

* ​

Use a Network Load Balancer and configure a static IP for each AZ

**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/>

Bottom of Form

Top of Form

Question 32: **Correct**

**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?**

* ​

RDS with Multi-AZ

* ​

DynamoDB with Global Tables and Cross Region Replication

**(Correct)**

* ​

EC2 instances with EBS replication

* ​

S3 with Cross Region Replication

**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/>

Bottom of Form

Top of Form

Question 33: **Incorrect**

**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)**

* ​

Use CloudFront with an RTMP distribution

**(Incorrect)**

* ​

Use CloudFront with a Web and RTMP distribution

**(Correct)**

* ​

Store the media files on an EC2 instance

* ​

Store the media files in an S3 bucket

**(Correct)**

**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/>

Bottom of Form

Top of Form

Question 34: **Incorrect**

**An application tier of a multi-tier web application currently hosts two web services on the same set of instances. The web services each listen for traffic on different ports. Which AWS service should a Solutions Architect use to route traffic to the service based on the incoming request path?**

* ​

Classic Load Balancer (CLB)

* ​

Application Load Balancer (ALB)

**(Correct)**

* ​

Amazon CloudFront

* ​

Amazon Route 53

**(Incorrect)**

**Explanation**

* An Application Load Balancer is a type of Elastic Load Balancer that can use layer 7 (HTTP/HTTPS) protocol data to make forwarding decisions. An ALB supports both path-based (e.g. /images or /orders) and host-based routing (e.g. example.com)
* In this scenario a single EC2 instance is listening for traffic for each application on a different port. You can use a target group that listens on a single port (HTTP or HTTPS) and then uses listener rules to selectively route to a different port on the EC2 instance based on the information in the URL path. So you might have example.com/images going to one back-end port and example.com/orders going to a different back0end port
* You cannot use host-based or path-based routing with a CLB
* Amazon CloudFront is used for caching content. It can route based on request path to custom origins however the question is not requesting a content caching service so it's not the best fit for this use case
* Amazon Route 53 is a DNS service. It can be used to load balance however it does not have the ability to route based on information in the incoming request path

**References:**

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

Bottom of Form

Top of Form

Question 35: **Incorrect**

**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)**

* ​

DynamoDB is more cost effective for read heavy workloads

**(Correct)**

* ​

DynamoDB is more cost effective for write heavy workloads

* ​

DynamoDB scales automatically and you are charged for what you use

**(Incorrect)**

* ​

Priced based on provisioned throughput (read/write) regardless of whether you use it or not

**(Correct)**

* ​

You provision for expected throughput but are only charged for what you use

**Explanation**

* DynamoDB charges:
* - DynamoDB is more cost effective for read heavy workloads
* - It is priced based on provisioned throughput (read/write) regardless of whether you use it or not
* **NOTE:** 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 relatively new and may not yet feature on the exam. See the link below for more details

**References:**

* <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/database/amazon-dynamodb/>
* <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AutoScaling.html>

Bottom of Form

Top of Form

Question 36: **Correct**

**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)**

* ​

Using biometrics

* ​

Through the AWS Management Console

**(Correct)**

* ​

Using the AWS API

**(Correct)**

* ​

Using a key pair

* ​

Locally to EC2 instances

**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/>

Bottom of Form

Top of Form

Question 37: **Incorrect**

**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)**

* ​

Create an IAM Policy that grants users the ability to change their own password and attach it to the groups that contain the users

**(Correct)**

* ​

Under the IAM Password Policy deselect the option to allow users to change their own passwords

**(Correct)**

* ​

Create an IAM Role that grants users the ability to change their own password and attach it to the groups that contain the users

**(Incorrect)**

* ​

Create an IAM Policy that grants users the ability to change their own password and attach it to the individual user accounts

* ​

Disable the ability for all users to change their own passwords using the AWS Security Token Service

**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/>

Bottom of Form

Top of Form

Question 38: **Incorrect**

**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?**

* ​

ElastiCache with the Memcached engine

* ​

Kinesis Data Streams

* ​

RDS in a multi-AZ configuration

**(Incorrect)**

* ​

ElastiCache with the Redis engine

**(Correct)**

**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/>

Bottom of Form

Top of Form

Question 39: **Correct**

**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?**

* ​

EC2 password

* ​

Public key

* ​

SSL/TLS certificate

* ​

Key pairs

**(Correct)**

**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/>

Bottom of Form

Top of Form

Question 40: **Incorrect**

**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)**

* ​

Detailed monitoring is free and can be manually enabled

* ​

Basic monitoring is enabled by default if the ASG is created from the CLI

* ​

Detailed monitoring is enabled by default if the ASG is created from the CLI

**(Correct)**

* ​

Detailed monitoring is chargeable and must always be manually enabled

**(Incorrect)**

* ​

Basic monitoring is enabled by default if the ASG is created from the console

**(Correct)**

**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/>

Bottom of Form

Top of Form

Question 41: **Correct**

**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)**

* ​

Enable cross region replication on the S3 bucket and specify a destination bucket in the DR region

**(Correct)**

* ​

Modify the permissions of the AMI so it can be used across multiple regions

* ​

Enable multi-AZ for the S3 bucket to enable synchronous replication to the DR region

* ​

Copy the AMI to the DR region and create a new launch configuration for the ASG that uses the AMI

**(Correct)**

* ​

Modify the launch configuration for the ASG in the DR region and specify the AMI

**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/>

Bottom of Form

Top of Form

Question 42: **Correct**

**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?**

* ​

Launch a single ALB, configure host-based routing for the domain names and bind an SSL certificate to each routing rule

* ​

Launch a single ALB and bind multiple SSL certificates to the same secure listener. Clients will use the Server Name Indication (SNI) extension

**(Correct)**

* ​

Launch a single ALB and bind multiple SSL certificates to multiple secure listeners

* ​

Launch multiple ALBs and bind separate SSL certificates to each ELB

**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/>

Bottom of Form

Top of Form

Question 43: **Correct**

**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?**

* ​

Amazon EFS

**(Correct)**

* ​

Amazon Storage Gateway

* ​

Amazon EBS using multiple volumes in a RAID 0 configuration

* ​

Amazon S3

**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/>

Bottom of Form

Top of Form

Question 44: **Correct**

**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?**

* ​

Reduce the file size of the images

* ​

Move the digital assets to EBS

* ​

Use Spot instances

* ​

Cache static content using CloudFront

**(Correct)**

**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/>

Bottom of Form

Top of Form

Question 45: **Correct**

**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?**

* ​

DynamoDB

**(Correct)**

* ​

RDS

* ​

EMR

* ​

RedShift

**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/>

Bottom of Form

Top of Form

Question 46: **Correct**

**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?**

* ​

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

* ​

Enable public read access for the S3 bucket

* ​

Generate a pre-signed URL and distribute it to the consumers

**(Correct)**

* ​

Use CloudFront to distribute the files using authorization hash tags

**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/>

Bottom of Form

Top of Form

Question 47: **Correct**

**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?**

* ​

Use an Application Load Balancer (ALB) and map the ECS service to the ALB

**(Correct)**

* ​

Use a Classic Load Balancer (CLB) and create a static mapping of the ports

* ​

You cannot run multiple copies of a task on the same instance, because the ports would conflict

* ​

Use a Network Load Balancer (NLB) and host-based routing

**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/>

Bottom of Form

Top of Form

Question 48: **Correct**

**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?**

* ​

Add a Simple Scaling policy

* ​

Add Amazon EC2 Spot instances

* ​

Add a Step Scaling policy

* ​

Add a Scheduled Scaling action

**(Correct)**

**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/>

Bottom of Form

Top of Form

Question 49: **Correct**

**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?**

* ​

You don’t need to do anything; this rule will only allow access to VPC based resources

* ​

Update the security group by removing the rule

**(Correct)**

* ​

Add a deny rule to the security group with a higher priority

* ​

Delete the security group

**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/>

Bottom of Form

Top of Form

Question 50: **Incorrect**

**Several websites you run on AWS use multiple Internet-facing Elastic Load Balancers (ELB) to distribute incoming connections to EC2 instances running web applications. The ELBs are configured to forward using either TCP (layer 4) or HTTP (layer 7) protocols. You would like to start recording the IP addresses of the clients that connect to your web applications.**

**Which ELB features will you implement with which protocols? (choose 2)**

* ​

X-Forwarded-For request header and TCP

**(Incorrect)**

* ​

X-Forwarded-For request header for TCP and HTTP

* ​

Proxy Protocol and TCP

**(Correct)**

* ​

X-Forwarded-For request header and HTTP

**(Correct)**

* ​

Proxy Protocol and HTTP

**Explanation**

* Proxy protocol for TCP/SSL carries the source (client) IP/port information
* X-forwarded-for for HTTP/HTTPS carries the source IP/port information
* In both cases the protocol carries the source IP/port information right through to the web server. If you were happy to just record the source connections on the load balancer you could use access logs

**References:**

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

Bottom of Form

Top of Form

Question 51: **Incorrect**

**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?**

* ​

Unmount the volume and enable server-side encryption. Re-mount the EBS volume

* ​

Create an encrypted snapshot of the current EBS volume. Restore the snapshot to the EBS volume

* ​

Create and mount a new encrypted EBS volume. Move the data to the new volume and then delete the old volume

**(Correct)**

* ​

Leverage the AWS Encryption CLI to encrypt the data on the volume

**(Incorrect)**

**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/>

Bottom of Form

Top of Form

Question 52: **Correct**

**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?**

* ​

The request is not secured with SSL/TLS

* ​

The IAM policy does not allow access to the API

* ​

The ACL on the API needs to be updated

* ​

Enable CORS on the APIs resources using the selected methods under the API Gateway

**(Correct)**

**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/>

Bottom of Form

Top of Form

Question 53: **Correct**

**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?**

* ​

Amazon Snowball

* ​

Amazon S3

* ​

Amazon EBS

* ​

Amazon EFS

**(Correct)**

**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/>

Bottom of Form

Top of Form

Question 54: **Correct**

**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)**

* ​

Create an origin access identity and associate it with your distribution

**(Correct)**

* ​

Modify the Edge Location to restrict direct access to Amazon S3 buckets

* ​

Modify the permissions on the Amazon S3 bucket so that only the origin access identity has read and download permissions

**(Correct)**

* ​

Create a new signed URL that requires users to access the Amazon S3 bucket through Amazon CloudFront

* ​

Modify the permissions on the origin access identity to restrict read access to the Amazon S3 bucket

**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>

Bottom of Form

Top of Form

Question 55: **Incorrect**

**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?**

* ​

Use a CloudFormation StackSet and specify the target accounts and regions in which the stacks will be created

**(Correct)**

* ​

Use a CloudFormation template that creates a stack and specify the logical IDs of each account and region

* ​

This cannot be done, use separate CloudFormation templates per AWS account and region

* ​

Use a third-party product such as Terraform that has support for multiple AWS accounts and regions

**(Incorrect)**

**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>

Bottom of Form

Top of Form

Question 56: **Incorrect**

**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?**

* ​

Create a CloudTrail trail that audits S3 bucket operations

**(Incorrect)**

* ​

Enable server access logging for the S3 buckets to save access logs to a specified destination bucket

**(Correct)**

* ​

Create a CloudWatch metric that monitors the S3 bucket operations and triggers an alarm

* ​

Enable S3 event notifications for the specific actions and setup an SNS notification

**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>

Bottom of Form

Top of Form

Question 57: **Correct**

**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)**

* ​

Single-node clusters support data replication

* ​

Manual backups are automatically deleted when you delete a cluster

* ​

RedShift provides continuous/incremental backups

**(Correct)**

* ​

RedShift always keeps five copies of your data

* ​

RedShift always keeps three copies of your data

**(Correct)**

**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/>

Bottom of Form

Top of Form

Question 58: **Correct**

**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?**

* ​

Elastic Transcoder

**(Correct)**

* ​

Data Pipeline

* ​

Rekognition

* ​

MediaConvert

**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
* MediaConvert converts file-based content for broadcast and multi-screen delivery
* 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/>

Bottom of Form

Top of Form

Question 59: **Correct**

**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?**

* ​

Amazon API Gateway

* ​

Amazon EC2

* ​

Amazon Kinesis Firehose

**(Correct)**

* ​

Amazon EBS

**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/>

Bottom of Form

Top of Form

Question 60: **Incorrect**

**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?**

* ​

Manually check all application configurations before deployment

* ​

Remove the ability for staff to deploy applications

* ​

Use CloudFormation with securely configured templates

**(Correct)**

* ​

Use AWS Inspector to apply secure configurations

**(Incorrect)**

**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/>

Bottom of Form

Top of Form

Question 61: **Correct**

**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 would like to distribute application traffic across both your AWS and on-premises resources.**

**How can this be achieved?**

* ​

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

* ​

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

* ​

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

**(Correct)**

* ​

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 server

**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/>

Bottom of Form

Top of Form

Question 62: **Incorrect**

**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?**

* ​

Amazon SQS FIFO queue

**(Incorrect)**

* ​

Amazon Kinesis Streams

**(Correct)**

* ​

Amazon SQS standard queue

* ​

AWS CloudTrail trail

**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 an 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/>

Bottom of Form

Top of Form

Question 63: **Correct**

**A company has an on-premises data warehouse that they would like to move to AWS where they will analyze large quantities of data. What is the most cost-efficient EBS storage volume type that is recommended for this use case?**

* ​

Cold HDD (sc1)

* ​

EBS General Purpose SSD (gp2)

* ​

EBS Provisioned IOPS SSD (io1)

* ​

Throughput Optimized HDD (st1)

**(Correct)**

**Explanation**

* Throughput Optimized HDD (st1) volumes are recommended for streaming workloads requiring consistent, fast throughput at a low price. Examples include Big Data warehouses and Log Processing. You cannot use these volumes as a boot volume
* EBS Provisioned IOPS SSD (io1) volumes are recommended for critical business applications that require sustained IOPS performance, or more than 16,000 IOPS or 250 MiB/s of throughput per volume
* EBS General Purpose SSD (gp2) volumes are recommended for most workloads including use as system boot volumes, virtual desktops, low-latency interactive apps, and development and test environments
* Cold HDD (sc1) volumes are recommended for throughput-oriented storage for large volumes of data that is infrequently accessed. This is the lowest cost HDD volume type. You cannot use these volumes as a boot volume.

**References:**

* <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html>
* <https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/amazon-ebs/>

Bottom of Form

Top of Form

Question 64: **Incorrect**

**An AWS user has created a Provisioned IOPS EBS volume which is attached to an EBS optimized instance and configured 1000 IOPS. Based on the EC2 SLA, what is the average IOPS the user will achieve for most of the year?**

* ​

1000

* ​

990

**(Incorrect)**

* ​

900

**(Correct)**

* ​

950

**Explanation**

* Unlike gp2, which uses a bucket and credit model to calculate performance, an io1 volume allows you to specify a consistent IOPS rate when you create the volume, and Amazon EBS delivers within 10 percent of the provisioned IOPS performance 99.9 percent of the time over a given year. Therefore you should expect to get 900 IOPS most of the year

**References:**

* <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html>

Bottom of Form

Top of Form

Question 65: **Correct**

**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?**

* ​

Availability Zone (AZ)

* ​

Cluster Subnet Group

**(Correct)**

* ​

DB Subnet Group

* ​

Subnet Group

**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>

Bottom of Form