Question 1Skipped

A Solutions Architect is launching an Amazon EC2 instance with multiple attached volumes by modifying the block device mapping. Which block device can be specified in a block device mapping to be used with an EC2 instance? (choose 2)

Correct selection

Instance store volume

S3 bucket

EFS volume

Correct selection

EBS volume

Snapshot

Overall explanation

Each instance that you launch has an associated root device volume, either an Amazon EBS volume or an instance store volume.

You can use block device mapping to specify additional EBS volumes or instance store volumes to attach to an instance when it's launched. You can also attach additional EBS volumes to a running instance.

You cannot use a block device mapping to specify a snapshot, EFS volume or S3 bucket.

CORRECT: "EBS volume" is a correct answer.

CORRECT: "Instance store volume" is also a correct answer.

INCORRECT: "EFS volume" is incorrect as described above.

INCORRECT: "Snapshot" is incorrect as described above.

INCORRECT: "S3 bucket" is incorrect as described above.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/block-device-mapping-concepts.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-ebs/

Domain

AWS Storage

Question 2Skipped

A company operates multiple AWS accounts under AWS Organizations. To better manage the costs, the company wants to allocate different budgets for each of these accounts. The

company also wants to prevent additional resource provisioning in an AWS account if it reaches its allocated budget before the end of the budget period.

Which combination of solutions will meet these requirements? (Select THREE.)

Use AWS Budgets in the AWS Management Console to set up budgets and specify the cost threshold for each AWS account.

Correct selection

Set up an IAM role with the necessary permissions that allow AWS Budgets to execute budget actions.

Correct selection

Use AWS Budgets to establish different budgets for each AWS account. Configure the budgets in the Billing and Cost Management console.

Correct selection

Configure alerts in AWS Budgets to notify the company when an account is about to reach its budget threshold. Then use a budget action that links to the IAM role to prevent additional resource provisioning.

Set up an alert in AWS Budgets to notify the company when a particular account meets its budget threshold. Enable real-time monitoring for immediate notification.

Create an IAM user with adequate permissions to allow AWS Budgets to enforce budget actions.

Overall explanation

AWS Budgets is a tool that enables you to set custom cost and usage budgets. You can set your budget amount, and AWS provides you with estimated charges and forecasted costs for your AWS usage. Configuring the budgets in the Billing and Cost Management console is a recommended step.

AWS Budgets can execute budget actions (like preventing additional resource provisioning) using an IAM role with the necessary permissions.

Configuring alerts in AWS Budgets and linking a budget action to an IAM role for automatic prevention of additional resource provisioning is a correct and efficient way to manage costs.

CORRECT: "Use AWS Budgets to establish different budgets for each AWS account. Configure the budgets in the Billing and Cost Management console" is a correct answer (as explained above.)

CORRECT: "Set up an IAM role with the necessary permissions that allow AWS Budgets to execute budget actions" is also a correct answer (as explained above.)

CORRECT: "Configure alerts in AWS Budgets to notify the company when an account is about to reach its budget threshold. Then use a budget action that links to the IAM role to prevent additional resource provisioning" is also a correct answer (as explained above.)

INCORRECT: "Use AWS Budgets in the AWS Management Console to set up budgets and specify the cost threshold for each AWS account" is incorrect.

While AWS Budgets can indeed be set up in the AWS Management Console, the budgets aren't set in the context of cost thresholds for each AWS account. This option is not fully accurate.

INCORRECT: "Create an IAM user with adequate permissions to allow AWS Budgets to enforce budget actions" is incorrect.

Although you can create an IAM user with necessary permissions, using an IAM role is generally a better practice. An IAM user is an entity that you create in AWS to represent the person or service that uses it to interact with AWS, while an IAM role is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. A role does not have long-term credentials associated with it like an IAM user does.

INCORRECT: "Set up an alert in AWS Budgets to notify the company when a particular account meets its budget threshold. Enable real-time monitoring for immediate notification" is incorrect.

AWS Budgets doesn't allow for real-time monitoring; the data can be delayed up to 24 hours. The frequency of budget alert notifications is not customizable to the minute or hour; they are typically sent out daily, weekly, or when a certain threshold is crossed.

References:

https://docs.aws.amazon.com/cost-management/latest/userguide/budgets-controls.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/aws-cost-management/

Domain

AWS Management & Governance

Question 3Skipped

An application uses an Amazon RDS database and Amazon EC2 instances in a web tier. The web tier instances must not be directly accessible from the internet to improve security.

How can a Solutions Architect meet these requirements?

Correct answer

Launch the EC2 instances in a private subnet and create an Application Load Balancer in a public subnet

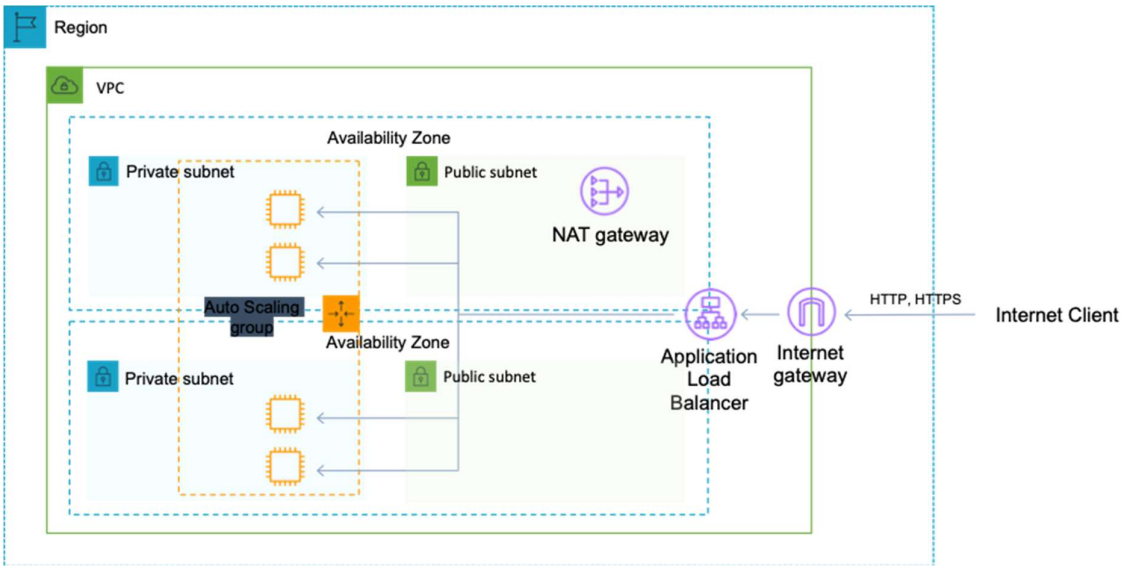
Launch the EC2 instances in a private subnet with a NAT gateway and update the route table

Launch the EC2 instances in a public subnet and create an Application Load Balancer in a public subnet

Launch the EC2 instances in a public subnet and use AWS WAF to protect the instances from internet-based attacks

Overall explanation

To prevent direct connectivity to the EC2 instances from the internet you can deploy your EC2 instances in a private subnet and have the ELB in a public subnet. To configure this you must enable a public subnet in the ELB that is in the same AZ as the private subnet.



CORRECT: "Launch the EC2 instances in a private subnet and create an Application Load Balancer in a public subnet" is the correct answer.

INCORRECT: "Launch the EC2 instances in a private subnet with a NAT gateway and update the route table" is incorrect. This configuration will not allow the application to be accessible from the internet, the aim is to only prevent direct access to the EC2 instances.

INCORRECT: "Launch the EC2 instances in a public subnet and use AWS WAF to protect the instances from internet-based attacks" is incorrect. With the EC2 instances in a public subnet, direct access from the internet is possible. It only takes a security group misconfiguration or software exploit and the instance becomes vulnerable to attack.

INCORRECT: "Launch the EC2 instances in a public subnet and create an Application Load Balancer in a public subnet" is incorrect. The EC2 instances should be launched in a private subnet.

References:

https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-vpc/

Domain

AWS Networking & Content Delivery

Question 4Skipped

A financial institution wants to use machine learning (ML) algorithms to detect potential fraudulent transactions. They need to create ML models based on their vast financial transaction data and integrate these models into their business intelligence system for real-time decision-making. The solution should require minimal operational overhead.

Which solution will best meet these requirements?

1. Use AWS Glue to perform ETL jobs on the transaction data and use Amazon Forecast for predictive analytics.

Use a pre-built ML Amazon Machine Image (AMI) from the AWS Marketplace to build and train models and use AWS Athena for data visualization.

Use Amazon Comprehend for analyzing the transaction data and Amazon Elasticsearch for visualization.

Correct answer

Use Amazon SageMaker to build, train, and deploy ML models, and use Amazon QuickSight for data visualization.

Overall explanation

Amazon SageMaker is a fully managed service that provides every developer and data scientist with the ability to build, train, and deploy machine learning models quickly. It can directly connect with data sources and has built-in algorithms to ease the ML process.

Amazon QuickSight is a business intelligence tool that can be used to create dashboards for data visualization. This combination perfectly suits the requirement.

CORRECT: "Use Amazon SageMaker to build, train, and deploy ML models, and use Amazon QuickSight for data visualization" is the correct answer (as explained above.)

INCORRECT: "Use AWS Glue to perform ETL jobs on the transaction data and use Amazon Forecast for predictive analytics" is incorrect.

AWS Glue is primarily used for ETL jobs - cleaning, preparing, and moving data. Amazon Forecast is a fully managed service for time-series forecasting, which might not be a complete solution for detecting fraudulent transactions.

INCORRECT: "Use a pre-built ML Amazon Machine Image (AMI) from the AWS Marketplace to build and train models and use AWS Athena for data visualization" is incorrect.

AWS Marketplace ML AMIs can be used to create and train models, but this will require manual operational effort in terms of setting up and managing the instances. Athena is a query service and does not provide data visualization capabilities that a business intelligence tool like QuickSight provides.

INCORRECT: "Use Amazon Comprehend for analyzing the transaction data and Amazon Elasticsearch for visualization" is incorrect.

Amazon Comprehend is primarily used for natural language processing (NLP), which isn't suited for detecting fraudulent transactions. Elasticsearch is a search and analytics engine and might not be the best tool for the use case described here.

References:

https://aws.amazon.com/sagemaker/

Save time with our AWS cheat sheets:

https://digitalcloud.training/aws-machine-learning-services/

Domain

AWS Machine Learning

Question 5Skipped

An application receives a high traffic load between 7:30am and 9:30am daily. The application uses an Auto Scaling group to maintain three instances most of the time but during the peak period it requires six instances.

How can a Solutions Architect configure Auto Scaling to perform a daily scale-out event at 7:30am and a scale-in event at 9:30am to account for the peak load?

Use a Step scaling policy

Correct answer

Use a Scheduled scaling policy

Use a Simple scaling policy

Use a Dynamic scaling policy

Overall explanation

The following scaling policy options are available:

Simple – maintains a current number of instances, you can manually change the ASGs min/desired/max and attach/detach instances.

Scheduled – Used for predictable load changes, can be a single event or a recurring schedule

Dynamic (event based) – scale in response to an event/alarm.

Step – configure multiple scaling steps in response to multiple alarms.

CORRECT: "Use a Scheduled scaling policy" is the correct answer.

INCORRECT: "Use a Simple scaling policy" is incorrect. Please refer to the description above.

INCORRECT: "Use a Dynamic scaling policy" is incorrect. Please refer to the description above.

INCORRECT: "Use a Step scaling policy" is incorrect. Please refer to the description above.

References:

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

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-ec2-auto-scaling/

Domain

AWS Compute

Question 6Skipped

A media company hosts several terabytes of multimedia content across multiple AWS accounts. The company uses AWS Lake Formation to manage its data lake. The company's

marketing team needs to securely access and analyze selective data from various accounts for targeted advertisement campaigns.

Which solution will meet these requirements with the LEAST operational overhead?

Use AWS DataSync to synchronize the necessary data to the marketing team accounts.

Correct answer

Utilize Lake Formation tag-based access control to authorize and grant cross-account permissions for the required data to the marketing team accounts.

Replicate the required data to a shared account. Create an IAM access role in that account. Grant access by defining a permission policy that includes users from the marketing team accounts as trusted entities.

Use the Lake Formation permissions Grant command in each account where the data is stored to permit the required marketing team users to access the data.

Overall explanation

With Lake Formation tag-based access control, you can manage permissions using tags and grant cross-account permissions, which would meet the requirements with the least operational overhead.

CORRECT: "Utilize Lake Formation tag-based access control to authorize and grant cross-account permissions for the required data to the marketing team accounts" is the correct answer (as explained above.)

INCORRECT: "Replicate the required data to a shared account. Create an IAM access role in that account. Grant access by defining a permission policy that includes users from the marketing team accounts as trusted entities" is incorrect.

This solution involves the unnecessary replication of data, leading to increased storage costs and operational overhead.

INCORRECT: "Use the Lake Formation permissions Grant command in each account where the data is stored to permit the required marketing team users to access the data" is incorrect.

The Grant command would need to be manually executed in each account where data is stored, which could lead to increased operational overhead, particularly if the data is spread across many accounts.

INCORRECT: "Use AWS DataSync to synchronize the necessary data to the marketing team accounts" is incorrect.

AWS DataSync is designed for online data transfer, not for granting access permissions to data already stored in AWS, so this would not meet the requirement.

References:

https://docs.aws.amazon.com/lake-formation/latest/dg/tag-based-access-control.html

Domain

AWS Storage

Question 7Skipped

An application makes calls to a REST API running on Amazon EC2 instances behind an Application Load Balancer (ALB). Most API calls complete quickly. However, a single endpoint is making API calls that require much longer to complete and this is introducing overall latency into the system. What steps can a Solutions Architect take to minimize the effects of the long-running API calls?

Increase the ALB idle timeout to allow the long-running requests to complete

Correct answer

Create an Amazon SQS queue and decouple the long-running API calls

Change the ALB to a Network Load Balancer (NLB) and use SSL/TLS termination

Change the EC2 instance to one with enhanced networking to reduce latency

Overall explanation

An Amazon Simple Queue Service (SQS) can be used to offload and decouple the long-running requests. They can then be processed asynchronously by separate EC2 instances. This is the best way to reduce the overall latency introduced by the long-running API call.

CORRECT: "Create an Amazon SQS queue and decouple the long-running API calls" is the correct answer.

INCORRECT: "Change the EC2 instance to one with enhanced networking to reduce latency" is incorrect. This will not reduce the latency of the API call as network latency is not the issue here, it is the latency of how long the API call takes to complete.

INCORRECT: "Increase the ALB idle timeout to allow the long-running requests to complete" is incorrect. The issue is not the connection being interrupted, it is that the API call takes a long time to complete.

INCORRECT: "Change the ALB to a Network Load Balancer (NLB) and use SSL/TLS termination" is incorrect. SSL/TLS termination is not of benefit here as the problem is not encryption or processing of encryption. The issue is API call latency.

References:

https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/aws-application-integration-services/

Domain

AWS Application Integration

Question 8Skipped

A company runs a web-based application that uses Amazon EC2 instances for the web front-end and Amazon RDS for the database back-end. The web application writes transaction log

files to an Amazon S3 bucket and the quantity of files is becoming quite large. It is acceptable to retain the most recent 60 days of log files and permanently delete the rest.

Which action can a Solutions Architect take to enable this to happen automatically?

Use an S3 lifecycle policy to move the log files that are more than 60 days old to the GLACIER storage class

Use an S3 bucket policy that deletes objects that are more than 60 days old

Write a Ruby script that checks the age of objects and deletes any that are more than 60 days old

Correct answer

Use an S3 lifecycle policy with object expiration configured to automatically remove objects that are more than 60 days old

Overall explanation

To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their Amazon S3 Lifecycle. An S3 Lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. There are two types of actions:

- Transition actions—Define when objects transition to another storage class. For example, you might choose to transition objects to the S3 Standard-IA storage class 30 days after you created them, or archive objects to the S3 Glacier storage class one year after creating them.

- Expiration actions—Define when objects expire. Amazon S3 deletes expired objects on your behalf.

CORRECT: "Use an S3 lifecycle policy with object expiration configured to automatically remove objects that are more than 60 days old" is the correct answer.

INCORRECT: "Write a Ruby script that checks the age of objects and deletes any that are more than 60 days old" is incorrect as the automated method is to use object expiration.

INCORRECT: "Use an S3 bucket policy that deletes objects that are more than 60 days old" is incorrect as you cannot do this with bucket policies.

INCORRECT: "Use an S3 lifecycle policy to move the log files that are more than 60 days old to the GLACIER storage class" is incorrect. Moving logs to Glacier may save cost but the question requests that the files are permanently deleted.

References:

https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-s3-and-glacier/

Domain

AWS Storage

Question 9Skipped

A company is in the process of improving its security posture and wants to analyze and rectify a high volume of failed login attempts and unauthorized activities being logged in AWS CloudTrail.

What is the most efficient solution to help the company identify these security events with the LEAST amount of operational effort?

Utilize AWS Data Pipeline to regularly extract CloudTrail logs and use a custom script to identify the required security events.

Leverage AWS Lambda to trigger on CloudTrail log updates and use a custom script to scan for failed logins and unauthorized actions.

Correct answer

Use Amazon Athena to directly query CloudTrail logs for failed logins and unauthorized activities.

Implement Amazon Elasticsearch Service with Kibana to visualize the CloudTrail logs and manually search for these events.

Overall explanation

Amazon Athena can directly query data from S3 (where CloudTrail logs are stored) using standard SQL, making it a powerful and efficient tool for analyzing these logs. You don't need to manage any infrastructure or write custom scripts, and you can quickly write and run queries to identify the required security events.

CORRECT: "Use Amazon Athena to directly query CloudTrail logs for failed logins and unauthorized activities" is the correct answer (as explained above.)

INCORRECT: "Leverage AWS Lambda to trigger on CloudTrail log updates and use a custom script to scan for failed logins and unauthorized actions" is incorrect.

While Lambda functions can be triggered based on CloudTrail log updates and could theoretically be used to scan for security events, this would require substantial setup and ongoing maintenance of the script. It's not the most efficient choice.

INCORRECT: "Utilize AWS Data Pipeline to regularly extract CloudTrail logs and use a custom script to identify the required security events" is incorrect.

This solution could work, but the operational overhead of managing the extraction process and maintaining a custom script for analysis is not minimal.

INCORRECT: "Implement Amazon Elasticsearch Service with Kibana to visualize the CloudTrail logs and manually search for these events" is incorrect.

While Elasticsearch and Kibana provide powerful search and visualization capabilities, respectively, they require a fair amount of setup and management. This option would provide more in-depth analysis and real-time monitoring, but it wouldn't be the most efficient way to simply identify the security events mentioned.

References:

https://docs.aws.amazon.com/athena/latest/ug/cloudtrail-logs.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-athena/

Domain

AWS Analytics

Question 10Skipped

A Solutions Architect has logged into an Amazon EC2 Linux instance using SSH and needs to determine a few pieces of information including what IAM role is assigned, the instance ID and the names of the security groups that are assigned to the instance.

From the options below, what would be the best source of this information?

Correct answer

Metadata

Tags

Parameters

User data

Overall explanation

Instance metadata is data about your instance that you can use to configure or manage the running instance. Instance metadata is divided into categories, for example, host name, events, and security groups.

Instance metadata is available at http://169.254.169.254/latest/meta-data.

CORRECT: "Metadata" is the correct answer.

INCORRECT: "Tags" is incorrect. Tags are used to categorize and label resources.

INCORRECT: "User data" is incorrect. User data is used to configure the system at launch time and specify scripts.

INCORRECT: "Parameters" is incorrect. Parameters are used in databases.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-ec2/

Domain

AWS Compute

Question 11Skipped

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

AWS Config

AWS CodeDeploy

Correct answer

Run Command

AWS OpsWorks

Overall explanation

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

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

CORRECT: "Run Command" is the correct answer.

INCORRECT: "AWS CodeDeploy" is incorrect. AWS CodeDeploy is a deployment service that automates application deployments to Amazon EC2 instances, on-premises instances, serverless Lambda functions, or Amazon ECS services.

INCORRECT: "AWS Config" is incorrect. AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. It is not used for ad-hoc script execution.

INCORRECT: "AWS OpsWorks" is incorrect. AWS OpsWorks provides instances of managed Puppet and Chef.

References:

https://aws.amazon.com/blogs/aws/new-ec2-run-command-remote-instance-management-at-scale/

Domain

AWS Compute

Question 12Skipped

A company runs a streaming media service and the content is stored on Amazon S3. The media catalog server pulls updated content from S3 and can issue over 1 million read operations per second for short periods. Latency must be kept under 5ms for these updates. Which solution will provide the BEST performance for the media catalog updates?

Correct answer

Update the application code to use an Amazon ElastiCache for Redis cluster

Implement an Instance store volume on the media catalog server

Implement Amazon CloudFront and cache the content at Edge Locations

Update the application code to use an Amazon DynamoDB Accelerator cluster

Overall explanation

Some applications, such as media catalog updates require high frequency reads, and consistent throughput. For such applications, customers often complement S3 with an in-memory cache, such as Amazon ElastiCache for Redis, to reduce the S3 retrieval cost and to improve performance.

ElastiCache for Redis is a fully managed, in-memory data store that provides sub-millisecond latency performance with high throughput. ElastiCache for Redis complements S3 in the following ways:

- Redis stores data in-memory, so it provides sub-millisecond latency and supports incredibly high requests per second.

- It supports key/value based operations that map well to S3 operations (for example, GET/SET => GET/PUT), making it easy to write code for both S3 and ElastiCache.

- It can be implemented as an application side cache. This allows you to use S3 as your persistent store and benefit from its durability, availability, and low cost. Your applications decide what objects to cache, when to cache them, and how to cache them.

In this example the media catalog is pulling updates from S3 so the performance between these components is what needs to be improved. Therefore, using ElastiCache to cache the content will dramatically increase the performance.

CORRECT: "Update the application code to use an Amazon ElastiCache for Redis cluster" is the correct answer.

INCORRECT: "Implement Amazon CloudFront and cache the content at Edge Locations" is incorrect. CloudFront is good for getting media closer to users but in this case we're trying to improve performance within the data center moving data from S3 to the media catalog server.

INCORRECT: "Update the application code to use an Amazon DynamoDB Accelerator cluster" is incorrect. DynamoDB Accelerator (DAX) is used with DynamoDB but is unsuitable for use with Amazon S3.

INCORRECT: "Implement an Instance store volume on the media catalog server" is incorrect. This will improve local disk performance but will not improve reads from Amazon S3.

References:

https://aws.amazon.com/blogs/storage/turbocharge-amazon-s3-with-amazon-elasticache-for-redis/

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-elasticache/

Domain

AWS Database

Question 13Skipped

A telecommunication company has an API that allows users to manage their mobile plans and services. The API experiences significant traffic spikes during specific times such as end of the

month and special offer periods. The company needs to ensure low latency response time consistently to ensure a good user experience. The solution should also minimize operational overhead.

Which solution would meet these requirements MOST efficiently?

Use Amazon API Gateway with AWS Fargate tasks to handle the API requests.

Correct answer

Use Amazon API Gateway along with AWS Lambda functions with provisioned concurrency.

Implement the API using AWS Elastic Beanstalk with auto-scaling groups.

Implement the API on an Amazon EC2 instance behind an Application Load Balancer with manual scaling.

Overall explanation

Amazon API Gateway and AWS Lambda together make a highly scalable solution for APIs. Provisioned concurrency in Lambda ensures that there is always a warm pool of functions ready to quickly respond to API requests, thereby guaranteeing low latency even during peak traffic times.

CORRECT: "Use Amazon API Gateway along with AWS Lambda functions with provisioned concurrency" is the correct answer (as explained above.)

INCORRECT: "Implement the API using AWS Elastic Beanstalk with auto-scaling groups" is incorrect.

Elastic Beanstalk is a viable option for deploying applications and auto-scaling and can help handle increased traffic, but it doesn't guarantee the low latency requirement during peak traffic times.

INCORRECT: "Use Amazon API Gateway with AWS Fargate tasks to handle the API requests" is incorrect.

API Gateway with Fargate can provide scalable compute, but this approach can result in higher operational overhead because of the need to manage the container lifecycle.

INCORRECT: "Implement the API on an Amazon EC2 instance behind an Application Load Balancer with manual scaling" is incorrect.

This solution does not scale automatically and would require manual intervention to ensure optimal performance during traffic spikes. Therefore, it doesn't satisfy the requirement of minimizing operational overhead.

References:

https://docs.aws.amazon.com/lambda/latest/dg/provisioned-concurrency.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-api-gateway/

Domain

AWS Networking & Content Delivery

Question 14Skipped

An organization in the agriculture sector is deploying sensors and smart devices around factory plants and fields. The devices will collect information and send it to cloud applications running on AWS.

Which AWS service will securely connect the devices to the cloud applications?

Correct answer

AWS IoT Core

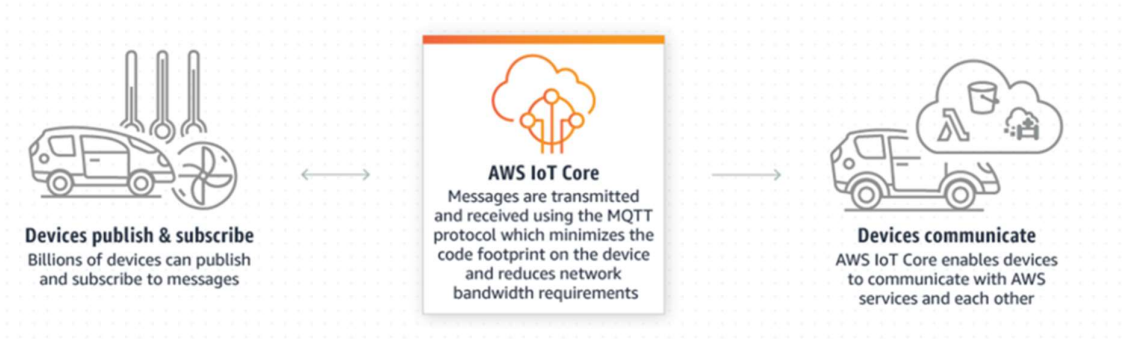
AWS DMS

AWS Glue

AWS Lambda

Overall explanation

AWS IoT Core is a managed cloud service that lets connected devices easily and securely interact with cloud applications and other devices. AWS IoT Core can support billions of devices and trillions of messages, and can process and route those messages to AWS endpoints and to other devices reliably and securely.



CORRECT: "AWS IoT Core" is the correct answer.

INCORRECT: "AWS Glue" is incorrect. 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.

INCORRECT: "AWS DMS" is incorrect. AWS Database Migration Service helps you migrate databases to AWS quickly and securely.

INCORRECT: "AWS Lambda" is incorrect. AWS Lambda lets you run code without provisioning or managing servers.

References:

https://aws.amazon.com/iot-core/

Domain

AWS Internet of Things

Question 15Skipped

A company requires an Elastic Load Balancer (ELB) for an application they are planning to deploy on AWS. The application requires extremely high throughput and extremely low latencies. The connections will be made using the TCP protocol and the ELB must support load balancing to multiple ports on an instance. Which ELB would should the company use?

Classic Load Balancer

Application Load Balancer

Correct answer

Network Load Balancer

Route 53

Overall explanation

The Network Load Balancer operates at the connection level (Layer 4), routing connections to targets – Amazon EC2 instances, containers and IP addresses based on IP protocol data. It is architected to handle millions of requests/sec, sudden volatile traffic patterns and provides extremely low latencies.

The NLB provides high throughput and extremely low latencies and is designed to handle traffic as it grows and can load balance millions of requests/second. NLB also supports load balancing to multiple ports on an instance.

CORRECT: "Network Load Balancer" is the correct answer.

INCORRECT: "Classic Load Balancer" is incorrect. The CLB operates using the TCP, SSL, HTTP and HTTPS protocols. It is not the best choice for requirements of extremely high throughput and low latency and does not support load balancing to multiple ports on an instance.

INCORRECT: "Application Load Balancer" is incorrect. The ALB operates at the HTTP and HTTPS level only (does not support TCP load balancing).

INCORRECT: "Route 53" is incorrect. Route 53 is a DNS service, it is not a type of ELB (though you can do some types of load balancing with it).

References:

https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/aws-elastic-load-balancing-aws-elb/

Domain

AWS Networking & Content Delivery

Question 16Skipped

A security officer has requested that all data associated with a specific customer is encrypted. The data resides on Elastic Block Store (EBS) volumes. Which of the following statements about using EBS encryption are correct? (Select TWO.)

Correct selection

Data in transit between an instance and an encrypted volume is also encrypted

Only current generation instance types are supported.

All attached EBS volumes must share the same encryption state

Correct selection

There is no direct way to change the encryption state of a volume

Not all EBS types support encryption

Overall explanation

Amazon EBS encryption uses AWS KMS keys when creating encrypted volumes and snapshots. Encryption operations occur on the servers that host EC2 instances, ensuring the security of both data-at-rest and data-in-transit between an instance and its attached EBS storage.

Encryption is supported by all EBS volume types. Amazon EBS encryption is available on all current generation and previous generation instance types.

CORRECT: "Data in transit between an instance and an encrypted volume is also encrypted" is the correct answer.

CORRECT: "There is no direct way to change the encryption state of a volume" is the correct answer.

INCORRECT: "Not all EBS types support encryption" is incorrect as all EBS volume types support encryption.

INCORRECT: "All attached EBS volumes must share the same encryption state" is incorrect. You can have encrypted and non-encrypted EBS volumes on a single instance.

INCORRECT: "Only current generation instance types are supported" is incorrect. Amazon EBS encryption is available on all current generation and previous generation instance types.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-ebs/

Domain

AWS Storage

Question 17Skipped

A web application runs on a series of Amazon EC2 instances behind an Application Load Balancer (ALB). A Solutions Architect is updating the configuration with a health check and needs to select the protocol to use. What options are available? (choose 2)

Correct selection

HTTP

ICMP

Correct selection

HTTPS

TCP

SSL

Overall explanation

An Application Load Balancer periodically sends requests to its registered targets to test their status. These tests are called *health checks*.

Each load balancer node routes requests only to the healthy targets in the enabled Availability Zones for the load balancer. Each load balancer node checks the health of each target, using the health check settings for the target groups with which the target is registered. After your target is registered, it must pass one health check to be considered healthy. After each health check is completed, the load balancer node closes the connection that was established for the health check.

If a target group contains only unhealthy registered targets, the load balancer nodes route requests across its unhealthy targets.

For an ALB the possible protocols are HTTP and HTTPS. The default is the HTTP protocol.

CORRECT: "HTTP" is the correct answer.

CORRECT: "HTTPS" is the correct answer.

INCORRECT: "SSL" is incorrect as this is not supported by the ALB.

INCORRECT: "TCP" is incorrect as this is not supported by the ALB.

INCORRECT: "ICMP" is incorrect as this is not supported by the ALB.

References:

https://docs.aws.amazon.com/elasticloadbalancing/latest/network/target-group-health-checks.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/aws-elastic-load-balancing-aws-elb/

Domain

AWS Networking & Content Delivery

Question 18Skipped

A web application receives order processing information from customers and places the messages on an Amazon SQS queue. A fleet of Amazon EC2 instances are configured to pick up the messages, process them, and store the results in a DynamoDB table. The current

configuration has been resulting in a large number of empty responses to ReceiveMessage API requests.

A Solutions Architect needs to eliminate empty responses to reduce operational overhead. How can this be done?

Use a Standard queue to provide at-least-once delivery, which means that each message is delivered at least once

Configure Short Polling to eliminate empty responses by reducing the length of time a connection request remains open

Use a FIFO (first-in-first-out) queue to preserve the exact order in which messages are sent and received

Correct answer

Configure Long Polling to eliminate empty responses by allowing Amazon SQS to wait until a message is available in a queue before sending a response

Overall explanation

The correct answer is to use Long Polling which will eliminate empty responses by allowing Amazon SQS to wait until a message is available in a queue before sending a response.

The problem does not relate to the order in which the messages are processed in and there are no concerns over messages being delivered more than once so it doesn't matter whether you use a FIFO or standard queue.

Long Polling:

– Uses fewer requests and reduces cost.

– Eliminates false empty responses by querying all servers.

– SQS waits until a message is available in the queue before sending a response.

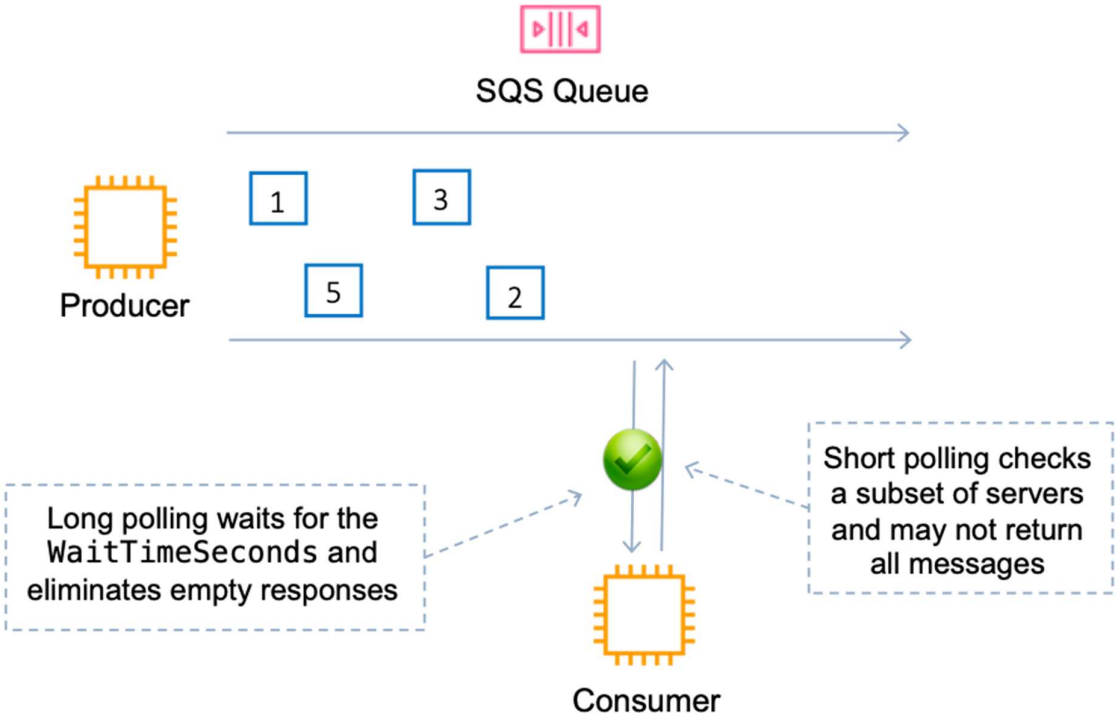
Short Polling:

– Does not wait for messages to appear in the queue.

– It queries only a subset of the available servers for messages (based on weighted random execution).

– Short polling is the default.

– ReceiveMessageWaitTime is set to 0.



CORRECT: "Configure Long Polling to eliminate empty responses by allowing Amazon SQS to wait until a message is available in a queue before sending a response" is the correct answer.

INCORRECT: "Use a Standard queue to provide at-least-once delivery, which means that each message is delivered at least once" is incorrect as explained above.

INCORRECT: "Use a FIFO (first-in-first-out) queue to preserve the exact order in which messages are sent and received" is incorrect as explained above.

INCORRECT: "Configure Short Polling to eliminate empty responses by reducing the length of time a connection request remains open" is incorrect as explained above.

References:

https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-short-and-long-polling.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/aws-application-integration-services/

Domain

AWS Application Integration

Question 19Skipped

A company is developing a web-based application that will be used for real-time chat functionality. The application should use WebSocket APIs to maintain a persistent connection with the client. The backend services of the application, hosted in containers within private subnets of a VPC, need to be accessed securely.

Which solution will meet these requirements?

Develop a REST API using Amazon API Gateway. Host the application in Amazon Elastic Kubernetes Service (EKS) in a private subnet. Establish a private VPC link for the API Gateway to securely access the Amazon EKS cluster.

Develop a WebSocket API using Amazon API Gateway. Host the application in Amazon Elastic Kubernetes Service (EKS) in a private subnet. Create a security group that allows API Gateway to access the Amazon EKS cluster.

Correct answer

Develop a WebSocket API using Amazon API Gateway. Host the application in Amazon Elastic Kubernetes Service (EKS) in a private subnet. Establish a private VPC link for the API Gateway to securely access the Amazon EKS cluster.

Develop a REST API using Amazon API Gateway. Host the application in Amazon Elastic Kubernetes Service (EKS) in a private subnet. Create a security group that allows API Gateway to access the Amazon EKS cluster.

Overall explanation

The requirement is for a real-time chat application, which makes the use of WebSocket APIs more suitable. Hosting the application in Amazon EKS within a private subnet allows secure and scalable management of the application. Creating a VPC link provides secure, private connectivity between API Gateway and the Amazon EKS service hosted inside the VPC.

CORRECT: "Develop a WebSocket API using Amazon API Gateway. Host the application in Amazon Elastic Kubernetes Service (EKS) in a private subnet. Establish a private VPC link for the API Gateway to securely access the Amazon EKS cluster" is the correct answer (as explained above.)

INCORRECT: "Develop a REST API using Amazon API Gateway. Host the application in Amazon Elastic Kubernetes Service (EKS) in a private subnet. Establish a private VPC link for the API Gateway to securely access the Amazon EKS cluster" is incorrect.

This solution does provide the secure hosting environment and private connectivity between API Gateway and the Amazon EKS cluster, but REST APIs are not suitable for real-time applications like a chat service. This is because REST APIs use request-response model which doesn't provide the continuous connection needed for real-time communication.

INCORRECT: "Develop a WebSocket API using Amazon API Gateway. Host the application in Amazon Elastic Kubernetes Service (EKS) in a private subnet. Create a security group that allows API Gateway to access the Amazon EKS cluster" is incorrect.

This option, while correctly suggesting the use of WebSocket APIs and Amazon EKS, proposes the use of a security group for connectivity. However, security groups act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level, while access to services within VPCs is more securely managed through VPC links.

INCORRECT: "Develop a REST API using Amazon API Gateway. Host the application in Amazon Elastic Kubernetes Service (EKS) in a private subnet. Create a security group that allows API Gateway to access the Amazon EKS cluster" is incorrect.

REST APIs are not suitable for a real-time chat application. Also, managing access via a security group is not the most secure method for accessing services hosted within private subnets in a VPC.

References:

https://docs.aws.amazon.com/whitepapers/latest/best-practices-api-gateway-private-apis-integration/websocket-api.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-api-gateway/

Domain

AWS Networking & Content Delivery

Question 20Skipped

A Solutions Architect needs to capture information about the traffic that reaches an Amazon Elastic Load Balancer. The information should include the source, destination, and protocol.

What is the most secure and reliable method for gathering this data?

Use Amazon CloudWatch Logs to review detailed logging information

Create a VPC flow log for the subnets in which the ELB is running

Enable Amazon CloudTrail logging and configure packet capturing

Correct answer

Create a VPC flow log for each network interface associated with the ELB

Overall explanation

You can use VPC Flow Logs to capture detailed information about the traffic going to and from your Elastic Load Balancer. Create a flow log for each network interface for your load balancer. There is one network interface per load balancer subnet.

CORRECT: "Create a VPC flow log for each network interface associated with the ELB" is the correct answer.

INCORRECT: "Enable Amazon CloudTrail logging and configure packet capturing" is incorrect. CloudTrail performs auditing of API actions, it does not do packet capturing.

INCORRECT: "Use Amazon CloudWatch Logs to review detailed logging information" is incorrect as this service does not record this information in CloudWatch logs.

INCORRECT: "Create a VPC flow log for the subnets in which the ELB is running" is incorrect as the more secure option is to use the ELB network interfaces.

References:

https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html
https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-monitoring.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/aws-elastic-load-balancing-aws-elb/

Domain

AWS Networking & Content Delivery

Question 21Skipped

A tool needs to analyze data stored in an Amazon S3 bucket. Processing the data takes a few seconds and results are then written to another S3 bucket. Less than 256 MB of memory is needed to run the process. What would be the MOST cost-effective compute solutions for this use case?

Amazon EC2 spot instances

Correct answer

AWS Lambda functions

AWS Fargate tasks

Amazon Elastic Beanstalk

Overall explanation

AWS Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume. Lambda has a maximum execution time of 900 seconds and memory can be allocated up to 3008 MB. Therefore, the most cost-effective solution will be AWS Lambda.

CORRECT: "AWS Lambda functions" is the correct answer.

INCORRECT: "AWS Fargate tasks" is incorrect. Fargate runs Docker containers and is serverless. However, you do pay for the running time of the tasks so it will not be as cost-effective.

INCORRECT: "Amazon EC2 spot instances" is incorrect. EC2 instances must run continually waiting for jobs to process so even with spot this would be less cost-effective (and subject to termination).

INCORRECT: "Amazon Elastic Beanstalk" is incorrect. This services also relies on Amazon EC2 instances so would not be as cost-effective.

References:

https://aws.amazon.com/lambda/

Save time with our AWS cheat sheets:

https://digitalcloud.training/aws-lambda/

Domain

AWS Compute

Question 22Skipped

A company needs to capture detailed information about all HTTP requests that are processed by their Internet facing Application Load Balancer (ALB). The company requires information on the requester, IP address, and request type for analyzing traffic patterns to better understand their customer base.

Which actions should a Solutions Architect recommend?

Correct answer

Enable Access Logs and store the data on S3

Enable EC2 detailed monitoring

Configure metrics in CloudWatch for the ALB

Use CloudTrail to capture all API calls made to the ALB

Overall explanation

You can enable access logs on the ALB and this will provide the information required including requester, IP, and request type. Access logs are not enabled by default. You can optionally store and retain the log files on S3.

CORRECT: "Enable Access Logs and store the data on S3" is the correct answer.

INCORRECT: "Configure metrics in CloudWatch for the ALB" is incorrect. CloudWatch is used for performance monitoring and CloudTrail is used for auditing API access..

INCORRECT: "Enable EC2 detailed monitoring" is incorrect. Enabling EC2 detailed monitoring will not capture the information requested.

INCORRECT: Use CloudTrail to capture all API calls made to the ALB"" is incorrect. CloudTrail captures API activity and would not include the requested information.

References:

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/aws-elastic-load-balancing-aws-elb/

Domain

AWS Networking & Content Delivery

Question 23Skipped

A company has launched a multi-tier application architecture. The web tier and database tier run on Amazon EC2 instances in private subnets within the same Availability Zone.

Which combination of steps should a Solutions Architect take to add high availability to this architecture? (Select TWO.)

Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer (ALB)

Create new private subnets in the same VPC but in a different AZ. Create a database using Amazon EC2 in one AZ

Create new public subnets in the same AZ for high availability and move the web tier to the public subnets

Correct selection

Create an Amazon EC2 Auto Scaling group and Application Load Balancer (ALB) spanning multiple AZs

Correct selection

Create new private subnets in the same VPC but in a different AZ. Migrate the database to an Amazon RDS multi-AZ deployment

Overall explanation

The Solutions Architect can use Auto Scaling group across multiple AZs with an ALB in front to create an elastic and highly available architecture. Then, migrate the database to an Amazon RDS multi-AZ deployment to create HA for the database tier. This results in a fully redundant architecture that can withstand the failure of an availability zone.

CORRECT: "Create an Amazon EC2 Auto Scaling group and Application Load Balancer (ALB) spanning multiple AZs" is a correct answer.

CORRECT: "Create new private subnets in the same VPC but in a different AZ. Migrate the database to an Amazon RDS multi-AZ deployment" is also a correct answer.

INCORRECT: "Create new public subnets in the same AZ for high availability and move the web tier to the public subnets" is incorrect. If subnets share the same AZ they are not suitable for splitting your tier across them for HA as the failure of a an AZ will take out both subnets.

INCORRECT: "Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer (ALB)" is incorrect. The instances are in a single AZ so the Solutions Architect should create a new auto scaling group and launch instances across multiple AZs.

INCORRECT: "Create new private subnets in the same VPC but in a different AZ. Create a database using Amazon EC2 in one AZ" is incorrect. A database in a single AZ will not be highly available.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-increase-availability.html

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-ec2/

https://digitalcloud.training/amazon-rds/

Domain

AWS Compute

Question 24Skipped

An application uses a MySQL database running on an Amazon EC2 instance. The application generates high I/O and constant writes to a single table on the database. Which Amazon EBS volume type will provide the MOST consistent performance and low latency?

General Purpose SSD (gp2)

Correct answer

Provisioned IOPS SSD (io1)

Throughput Optimized HDD (st1)

Cold HDD (sc1)

Overall explanation

The Provisioned IOPS SSD (io1) volume type will offer the most consistent performance and can be configured with the amount of IOPS required by the application. It will also provide the lowest latency of the options presented.

	Solid-state drives (SSD)		Hard disk drives (HDD)	
Volume type	General Purpose SSD (gp2)	Provisioned IOPS SSD (io1)	Throughput Optimized HDD (st1)	Cold HDD (sc1)
Description	General purpose SSD volume that balances price and performance for a wide variety of workloads	Highest-performance SSD volume for mission-critical low-latency or high-throughput workloads	Low-cost HDD volume designed for frequently accessed, throughput-intensive workloads	Lowest cost HDD volume designed for less frequently accessed workloads

CORRECT: "Provisioned IOPS SSD (io1)" is the correct answer.

INCORRECT: "General Purpose SSD (gp2)" is incorrect. This is not the best solution for when you require high I/O, consistent performance and low latency.

INCORRECT: "Throughput Optimized HDD (st1)" is incorrect. This is a HDD type of disk and not suitable for low latency workloads that require consistent performance.

INCORRECT: "Cold HDD (sc1)" is incorrect. This is the lowest cost option and not suitable for frequently accessed workloads.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-ebs/

Domain

AWS Compute

Question 25Skipped

A company runs an application on premises that stores a large quantity of semi-structured data using key-value pairs. The application code will be migrated to AWS Lambda and a highly scalable solution is required for storing the data.

Which datastore will be the best fit for these requirements?

Amazon EFS

Amazon EBS

Amazon RDS MySQL

Correct answer

Amazon DynamoDB

Overall explanation

Amazon DynamoDB is a no-SQL database that stores data using key-value pairs. It is ideal for storing large amounts of semi-structured data and is also highly scalable. This is the best solution for storing this data based on the requirements in the scenario.

CORRECT: "Amazon DynamoDB" is the correct answer.

INCORRECT: "Amazon EFS" is incorrect. The Amazon Elastic File System (EFS) is not suitable for storing key-value pairs.

INCORRECT: "Amazon RDS MySQL" is incorrect. Amazon Relational Database Service (RDS) is used for structured data as it is an SQL type of database.

INCORRECT: "Amazon EBS" is incorrect. Amazon Elastic Block Store (EBS) is a block-based storage system. You attach volumes to EC2 instances. It is not used for key-value pairs or to be used by Lambda functions.

References:

https://aws.amazon.com/dynamodb/features/

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-dynamodb/

Domain

AWS Database

Question 26Skipped

An Amazon EC2 instance behind an Elastic Load Balancer (ELB) is in the process of being de-registered. Which ELB feature is used to allow existing connections to close cleanly?

Proxy Protocol

Sticky Sessions

Correct answer

Connection Draining

Deletion Protection

Overall explanation

Connection draining is enabled by default and provides a period of time for existing connections to close cleanly. When connection draining is in action an CLB will be in the status “InService: Instance deregistration currently in progress”.

CORRECT: "Connection Draining" is the correct answer.

INCORRECT: "Sticky Sessions" is incorrect. Session stickiness uses cookies and ensures a client is bound to an individual back-end instance for the duration of the cookie lifetime.

INCORRECT: "Proxy Protocol" is incorrect. The Proxy Protocol header helps you identify the IP address of a client when you have a load balancer that uses TCP for back-end connections.

INCORRECT: "Deletion Protection" is incorrect. Deletion protection is used to protect the ELB from deletion.

References:

https://aws.amazon.com/about-aws/whats-new/2014/03/20/elastic-load-balancing-supports-connection-draining/

Save time with our AWS cheat sheets:

https://digitalcloud.training/aws-elastic-load-balancing-aws-elb/

Domain

AWS Networking & Content Delivery

Question 27Skipped

A multinational organization has a distributed application that runs on Amazon EC2 instances, which are behind an Application Load Balancer in an Auto Scaling group. The application utilizes a MySQL database hosted on Amazon Aurora. The database cluster spans across multiple Availability Zones in a single region.

The organization plans to launch its services in a new geographical area and wants to ensure maximum availability with minimal service interruption.

Which strategy should the organization adopt?

Replicate the application layer in the new region. Implement an Aurora MySQL Read Replica in the new region using Route 53 health checks and a failover routing policy. In case of primary failure, promote the Read Replica to primary.

Correct answer

Establish the application layer in the new region. Use Amazon Aurora Global Database for deploying the database in the primary and new regions. Apply Amazon Route 53 health checks with a failover routing policy to the new region. Promote the secondary to primary as needed.

Expand the existing Auto Scaling group into the new Region. Utilize Amazon Aurora Global Database to extend the database across the primary and new regions. Implement Amazon Route 53 health checks with a failover routing policy directed towards the new region.

Create a similar application layer in the new region. Establish a new Aurora MySQL database in this region. Use AWS Database Migration Service (AWS DMS) for ongoing replication from the primary database to the new region. Implement Amazon Route 53 health checks with a failover routing policy to the new region.

Overall explanation

This solution involves creating an application layer in the new region and using Amazon Aurora Global Database, which supports replicating your databases across multiple regions with minimal impact on performance.

This configuration can enhance disaster recovery capabilities and can reduce the impact of planned maintenance. Amazon Route 53 health checks with a failover routing policy can automatically route traffic to the new region in the event of a failure in the primary region, thereby ensuring high availability.

With an Aurora global database, there are two different approaches to failover depending on the scenario. You can use manual unplanned failover (detach and promote) or managed planned failover.

CORRECT: "Establish the application layer in the new region. Use Amazon Aurora Global Database for deploying the database in the primary and new regions. Apply Amazon Route 53 health checks with a failover routing policy to the new region. Perform a manual failover as required" is the correct answer (as explained above.)

INCORRECT: "Replicate the application layer in the new region. Implement an Aurora MySQL Read Replica in the new region using Route 53 health checks and a failover routing policy. In case of primary failure, promote the Read Replica to primary" is incorrect.

This solution involves creating a Read Replica in the new region, which would indeed allow for the promotion of the Read Replica to a primary instance if necessary. However, this process isn't instantaneous and could lead to service interruption, which is not what the question asked for. Aurora Global Database provides a lower RTO/RPO.

INCORRECT: "Create a similar application layer in the new region. Establish a new Aurora MySQL database in this region. Use AWS Database Migration Service (AWS DMS) for ongoing replication from the primary database to the new region. Implement Amazon Route 53 health checks with a failover routing policy to the new region" is incorrect.

AWS Database Migration Service (AWS DMS) is primarily used for migrating databases to AWS from on-premises environments or for replicating databases for data warehousing and other use cases. It isn't as suitable for ongoing high-availability or failover scenarios as Amazon Aurora Global Database, which is specifically designed for these situations.

INCORRECT: "Expand the existing Auto Scaling group into the new Region. Utilize Amazon Aurora Global Database to extend the database across the primary and new regions. Implement Amazon Route 53 health checks with a failover routing policy directed towards the new region" is incorrect.

It is not possible to expand an Auto Scaling group across multiple Regions. ASGs operate within a Region only.

References:

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

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database-disaster-recovery.html#aurora-global-database-failover

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-aurora/

Domain

AWS Compute

Question 28Skipped

A Solutions Architect has created an AWS account and selected the Asia Pacific (Sydney) region. Within the default VPC there is a default security group. What settings are configured within this security group by default? (choose 2)

Correct selection

There is an outbound rule that allows all traffic to all addresses

Correct selection

There is an inbound rule that allows all traffic from the security group itself

There is an inbound rule that allows all traffic from any address

There is an outbound rule that allows all traffic to the security group itself

There is an outbound rule that allows traffic to the VPC router

Overall explanation

Default security groups have inbound allow rules (allowing traffic from within the group) whereas custom security groups do not have inbound allow rules (all inbound traffic is denied by default). All outbound traffic is allowed by default in custom and default security groups.

CORRECT: "There is an inbound rule that allows all traffic from the security group itself" is a correct answer.

CORRECT: "There is an outbound rule that allows all traffic to all addresses" is also a correct answer.

INCORRECT: "There is an inbound rule that allows all traffic from any address" is incorrect as explained above.

INCORRECT: "There is an outbound rule that allows all traffic to the security group itself" is incorrect as explained above.

INCORRECT: "There is an outbound rule that allows traffic to the VPC router" is incorrect as explained above.

References:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-vpc/

Domain

AWS Networking & Content Delivery

Question 29Skipped

A company needs to ensure that they can failover between AWS Regions in the event of a disaster seamlessly with minimal downtime and data loss. The applications will run in an active-active configuration.

Which DR strategy should a Solutions Architect recommend?

Correct answer

Multi-site

Pilot light

Warm standby

Backup and restore

Overall explanation

A multi-site solution runs on AWS as well as on your existing on-site infrastructure in an active-active configuration. The data replication method that you employ will be determined by the recovery point that you choose. This is either Recovery Time Objective (the maximum allowable downtime before degraded operations are restored) or Recovery Point Objective (the maximum allowable time window whereby you will accept the loss of transactions during the DR process).

CORRECT: "Multi-site" is the correct answer.

INCORRECT: "Backup and restore" is incorrect. This is the lowest cost DR approach that simply entails creating online backups of all data and applications.

INCORRECT: "Pilot light" is incorrect. With a pilot light strategy a core minimum of services are running and the remainder are only brought online during a disaster recovery situation.

INCORRECT: "Warm standby" is incorrect. The term warm standby is used to describe a DR scenario in which a scaled-down version of a fully functional environment is always running in the cloud.

References:

https://aws.amazon.com/blogs/publicsector/rapidly-recover-mission-critical-systems-in-a-disaster/

Domain

AWS Cloud Architecture & Design

Question 30Skipped

An international software firm provides its clients with custom solutions and tools designed for efficient data collection and analysis on AWS. The firm intends to centrally manage and distribute a standard set of solutions and tools for its clients' self-service needs.

Which solution would best satisfy these requirements?

Create AWS Config rules for the clients.

Correct answer

Create AWS Service Catalog portfolios for the clients.

Create AWS Systems Manager documents for the clients.

Create AWS CloudFormation stacks for the clients.

Overall explanation

AWS Service Catalog enables organizations to create and manage catalogs of IT services that are approved for use on AWS. It allows centrally managed service portfolios, which clients can use on a self-service basis.

AWS Service Catalog provides a single location where organizations can centrally manage catalogs of IT services, which simplifies the organizational process and helps ensure compliance.

CORRECT: "Create AWS Service Catalog portfolios for the clients" is the correct answer (as explained above.)

INCORRECT: "Create AWS CloudFormation stacks for the clients" is incorrect.

While AWS CloudFormation is a powerful service for infrastructure as code (IaC), it doesn't provide a straightforward way for clients to discover and use shared tools or solutions for self-service needs. It lacks the management features and access control mechanisms necessary for this scenario.

INCORRECT: "Create AWS Systems Manager documents for the clients" is incorrect.

AWS Systems Manager documents define the actions that Systems Manager performs on your managed instances. Although Systems Manager allows the central management of resources and applications, it doesn't provide an effective means for clients to self-discover and use shared tools or solutions.

INCORRECT: "Create AWS Config rules for the clients" is incorrect.

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. It isn't designed to centrally manage and distribute software tools or solutions.

References:

https://aws.amazon.com/servicecatalog/

Save time with our AWS cheat sheets:

https://digitalcloud.training/aws-service-catalog/

Domain

AWS Management & Governance

Question 31Skipped

Three AWS accounts are owned by the same company but in different regions. Account Z has two AWS Direct Connect connections to two separate company offices. Accounts A and B require the ability to route across account Z's Direct Connect connections to each company office. A Solutions Architect has created an AWS Direct Connect gateway in account Z.

How can the required connectivity be configured?

Associate the Direct Connect gateway to a transit gateway in each region

Correct answer

Associate the Direct Connect gateway to a virtual private gateway in account A and B

Create a VPC Endpoint to the Direct Connect gateway in account A and B

Create a PrivateLink connection in Account Z and ENIs in accounts A and B

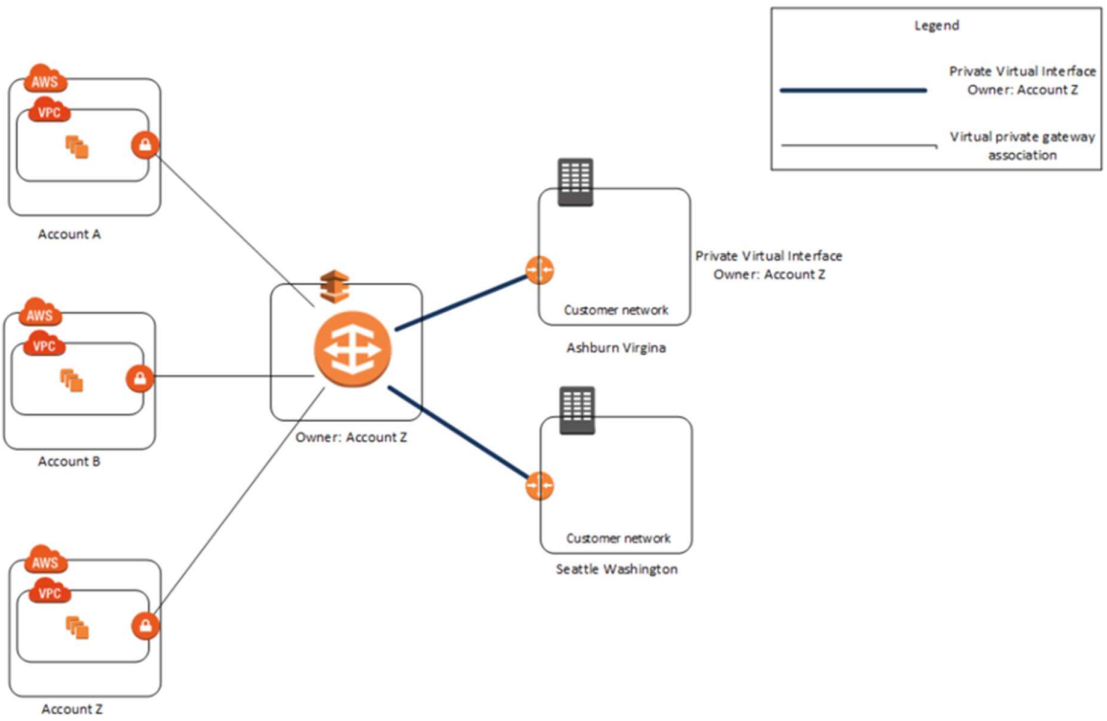
Overall explanation

You can associate an *AWS Direct Connect gateway* with either of the following gateways:

- A transit gateway when you have multiple VPCs in the same Region.

- A virtual private gateway.

In this case account Z owns the Direct Connect gateway so a VPG in accounts A and B must be associated with it to enable this configuration to work. After Account Z accepts the proposals, Account A and Account B can route traffic from their virtual private gateway to the Direct Connect gateway.



CORRECT: "Associate the Direct Connect gateway to a virtual private gateway in account A and B" is the correct answer.

INCORRECT: "Associate the Direct Connect gateway to a transit gateway in each region" is incorrect. This would be a good solution if the accounts were in VPCs within a region rather than across regions.

INCORRECT: "Create a VPC Endpoint to the Direct Connect gateway in account A and B" is incorrect. You cannot create a VPC endpoint for Direct Connect gateways.

INCORRECT: "Create a PrivateLink connection in Account Z and ENIs in accounts A and B" is incorrect. You cannot use PrivateLink connections to publish a Direct Connect gateway.

References:

https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/aws-direct-connect/

Domain

AWS Networking & Content Delivery

Question 32Skipped

A Solutions Architect has created a VPC and is in the process of formulating the subnet design. The VPC will be used to host a two-tier application that will include Internet facing web servers, and internal-only DB servers. Zonal redundancy is required.

How many subnets are required to support this requirement?

2 subnets

1 subnet

6 subnets

Correct answer

4 subnets

Overall explanation

Zonal redundancy indicates that the architecture should be split across multiple Availability Zones. Subnets are mapped 1:1 to AZs.

A public subnet should be used for the Internet-facing web servers and a separate private subnet should be used for the internal-only DB servers. Therefore you need 4 subnets – 2 (for redundancy) per public/private subnet.

CORRECT: "4 subnets" is the correct answer.

INCORRECT: "2 subnets" is incorrect as explained above.

INCORRECT: "6 subnets" is incorrect as explained above.

INCORRECT: "2 subnet" is incorrect as explained above.

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-vpc/

Domain

AWS Networking & Content Delivery

Question 33Skipped

An Amazon EBS-backed EC2 instance has been launched. A requirement has come up for some high-performance ephemeral storage.

How can a Solutions Architect add a new instance store volume?

Correct answer

You can specify the instance store volumes for your instance only when you launch an instance

You must use an Elastic Network Adapter (ENA) to add instance store volumes. First, attach an ENA, and then attach the instance store volume

You can use a block device mapping to specify additional instance store volumes when you launch your instance, or you can attach additional instance store volumes after your instance is running

You must shutdown the instance in order to be able to add the instance store volume

Overall explanation

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

CORRECT: "You can specify the instance store volumes for your instance only when you launch an instance" is the correct answer.

INCORRECT: "You must shutdown the instance in order to be able to add the instance store volume" is incorrect. You can use a block device mapping to specify additional EBS volumes when you launch your instance, or you can attach additional EBS volumes after your instance is running.

INCORRECT: "You must use an Elastic Network Adapter (ENA) to add instance store volumes. First, attach an ENA, and then attach the instance store volume" is incorrect. An Elastic Network Adapter has nothing to do with adding instance store volumes.

INCORRECT: "You can use a block device mapping to specify additional instance store volumes when you launch your instance, or you can attach additional instance store volumes after your instance is running" is incorrect. You can't attach instance store volumes to an instance after you've launched it.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/add-instance-store-volumes.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-ebs/

Domain

AWS Storage

Question 34Skipped

The Solutions Architect in charge of a critical application must ensure the Amazon EC2 instances are able to be launched in another AWS Region in the event of a disaster.

What steps should the Solutions Architect take? (Select TWO.)

Correct selection

Create AMIs of the instances and copy them to another Region

Enable cross-region snapshots for the Amazon EC2 instances

Launch instances in the second Region using the S3 API

Correct selection

Launch instances in the second Region from the AMIs

Copy the snapshots using Amazon S3 cross-region replication

Overall explanation

You can create AMIs of the EC2 instances and then copy them across Regions. This provides a point-in-time copy of the state of the EC2 instance in the remote Region.

Once you've created AMIs of EC2 instances and copied them to the second Region, you can then launch the EC2 instances from the AMIs in that Region.

This is a good DR strategy as you have moved stateful EC2 instances to another Region.

CORRECT: "Create AMIs of the instances and copy them to another Region" is the correct answer.

CORRECT: "Launch instances in the second Region from the AMIs" is also a correct answer.

INCORRECT: "Launch instances in the second Region using the S3 API" is incorrect. Though snapshots (and EBS-backed AMIs) are stored on Amazon S3, you cannot actually access them using the S3 API. You must use the EC2 API.

INCORRECT: "Enable cross-region snapshots for the Amazon EC2 instances" is incorrect. You cannot enable "cross-region snapshots" as this is not a feature that currently exists.

INCORRECT: "Copy the snapshots using Amazon S3 cross-region replication" is incorrect. You cannot work with snapshots using Amazon S3 at all including leveraging the cross-region replication feature.

References:

https://aws.amazon.com/blogs/aws/ebs-snapshot-copy/

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-ec2/

Domain

AWS Compute

Question 35Skipped

A Solutions Architect enabled Access Logs on an Application Load Balancer (ALB) and needs to process the log files using a hosted Hadoop service. What configuration changes and services can be leveraged to deliver this requirement?

Configure Access Logs to be delivered to S3 and use Kinesis for processing the log files

Correct answer

Configure Access Logs to be delivered to S3 and use EMR for processing the log files

Configure Access Logs to be delivered to EC2 and install Hadoop for processing the log files

Configure Access Logs to be delivered to DynamoDB and use EMR for processing the log files

Overall explanation

Access Logs can be enabled on ALB and configured to store data in an S3 bucket. Amazon EMR is a web service that enables businesses, researchers, data analysts, and developers to easily and cost-effectively process vast amounts of data. EMR utilizes a hosted Hadoop framework running on Amazon EC2 and Amazon S3.

CORRECT: "Configure Access Logs to be delivered to S3 and use EMR for processing the log files" is the correct answer.

INCORRECT: "Configure Access Logs to be delivered to EC2 and install Hadoop for processing the log files" is incorrect. EC2 does not provide a hosted Hadoop service.

INCORRECT: "Configure Access Logs to be delivered to DynamoDB and use EMR for processing the log files" is incorrect. You cannot configure access logs to be delivered to DynamoDB.

INCORRECT: "Configure Access Logs to be delivered to S3 and use Kinesis for processing the log files" is incorrect. Kinesis does not provide a hosted Hadoop service.

References:

https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-what-is-emr.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-emr/

https://digitalcloud.training/aws-elastic-load-balancing-aws-elb/

Domain

AWS Analytics

Question 36Skipped

An Amazon EC2 instance is generating very high packets-per-second and performance of the application stack is being impacted. A Solutions Architect needs to determine a resolution to the issue that results in improved performance.

Which action should the Architect take?

Create a placement group and put the EC2 instance in it

Configure a RAID 1 array from multiple EBS volumes

Add multiple Elastic IP addresses to the instance

Correct answer

Use enhanced networking

Overall explanation

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

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

CORRECT: "Use enhanced networking" is the correct answer.

INCORRECT: "Configure a RAID 1 array from multiple EBS volumes" is incorrect. You do not need to create a RAID 1 array (which is more for redundancy than performance anyway).

INCORRECT: "Create a placement group and put the EC2 instance in it" is incorrect. A placement group is used to increase network performance between instances. In this case there is only a single instance so it won't help.

INCORRECT: "Add multiple Elastic IP addresses to the instance" is incorrect. Adding multiple IP addresses is not a way to increase performance of the instance as the same amount of bandwidth is available to the Elastic Network Interface (ENI).

References:

https://aws.amazon.com/premiumsupport/knowledge-center/enable-configure-enhanced-networking/

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-ec2/

Domain

AWS Compute

Question 37Skipped

A healthcare company is migrating its patient record system to AWS. The company receives thousands of encrypted patient data files every day through FTP. An on-premises server processes the data files twice a day. However, the processing job takes hours to finish.

The company wants the AWS solution to process incoming data files as soon as they arrive with minimal changes to the FTP clients that send the files. The solution must delete the incoming data files after the files have been processed successfully. Processing for each file needs to take around 10 minutes.

Which solution will meet these requirements in the MOST operationally efficient way?

Correct answer

Use AWS Transfer Family to create an SFTP server to store incoming files in Amazon S3 Standard. Create an AWS Lambda function to process the files and to delete the files after they are processed. Use an S3 event notification to invoke the Lambda function when the files arrive.

Use an Amazon EC2 instance that runs an SFTP server to store incoming files in Amazon S3 Standard. Configure a job queue in AWS Batch. Use Amazon EventBridge rules to invoke the job to process the files twice a day. Delete the files after the job has processed the files.

Use AWS Transfer Family to create an SFTP server to store incoming files in Amazon S3 Glacier. Configure an Amazon EC2 instance to process the files. Use Amazon EventBridge rules to invoke the EC2 instance to process the files twice a day from S3 Glacier. Delete the objects after the job has processed the objects.

Use AWS Transfer Family to create an SFTP server to store incoming files in Amazon S3 Standard. Use Amazon EC2 instances managed by an Auto Scaling group to process the files. Set an S3 event notification to trigger an AWS Lambda function that launches the EC2 instances when the files arrive. Delete the files after they are processed.

Overall explanation

AWS Transfer Family provides fully managed support for file transfers directly into and out of Amazon S3 using SFTP. Storing incoming files in S3 Standard offers high durability, availability, and performance object storage for frequently accessed data.

AWS Lambda can respond immediately to S3 events, which allows processing of files as soon as they arrive. Lambda can also delete the files after processing. This meets all requirements and is operationally efficient, as it requires minimal management and has low costs.

CORRECT: "Use AWS Transfer Family to create an SFTP server to store incoming files in Amazon S3 Standard. Create an AWS Lambda function to process the files and to delete the files after they are processed. Use an S3 event notification to invoke the Lambda function when the files arrive" is the correct answer (as explained above.)

INCORRECT: "Use AWS Transfer Family to create an SFTP server to store incoming files in Amazon S3 Glacier. Configure an Amazon EC2 instance to process the files. Use Amazon EventBridge rules to invoke the EC2 instance to process the files twice a day from S3 Glacier. Delete the objects after the job has processed the objects" is incorrect.

This option involves using Amazon S3 Glacier, which is primarily used for long-term archival storage. Accessing data for processing could take longer and be more expensive than using S3 Standard. In addition, EC2 instances need to be managed and are less efficient for this scenario compared to AWS Lambda.

INCORRECT: "Use AWS Transfer Family to create an SFTP server to store incoming files in Amazon S3 Standard. Use Amazon EC2 instances managed by an Auto Scaling group to process the files. Set an S3 event notification to trigger an AWS Lambda function that launches the EC2 instances when the files arrive. Delete the files after they are processed" is incorrect.

While this solution will work, it is less efficient operationally because managing EC2 instances and an Auto Scaling group is more complex and likely more expensive than simply using AWS Lambda for processing.

INCORRECT: "Use an Amazon EC2 instance that runs an SFTP server to store incoming files in Amazon S3 Standard. Configure a job queue in AWS Batch. Use Amazon EventBridge rules to invoke the job to process the files twice a day. Delete the files after the job has processed the files" is incorrect.

This option does not meet the requirement of processing incoming data files as soon as they arrive, as EventBridge rules would invoke the job only twice a day. It also involves managing an EC2 instance, which is less operationally efficient than the AWS Transfer Family and AWS Lambda option.

References:

https://aws.amazon.com/aws-transfer-family/

Save time with our AWS cheat sheets:

https://digitalcloud.training/aws-migration-services/

Domain

AWS Migration & Transfer

Question 38Skipped

A development team needs to run up a few lab servers on a weekend for a new project. The servers will need to run uninterrupted for a few hours. Which EC2 pricing option would be most suitable?

Correct answer

On-Demand

Reserved

Spot

Dedicated instances

Overall explanation

On-Demand pricing ensures that instances will not be terminated and is the most economical option. Use on-demand for ad-hoc requirements where you cannot tolerate interruption.

CORRECT: "On-Demand" is the correct answer.

INCORRECT: "Spot" is incorrect. Spot pricing may be the most economical option for a short duration over a weekend but you may have the instances terminated by AWS and there is a requirement that the servers run uninterrupted.

INCORRECT: "Reserved" is incorrect. Reserved pricing provides a reduced cost for a contracted period (1 or 3 years), and is not suitable for ad hoc requirements.

INCORRECT: "Dedicated instances" is incorrect. Dedicated instances run on hardware that's dedicated to a single customer and are more expensive than regular On-Demand instances.

References:

https://aws.amazon.com/ec2/pricing/

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-ec2/

Domain

AWS Compute

Question 39Skipped

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

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

AWS CloudFormation

AWS CodeDeploy

AWS OpsWorks

Correct answer

AWS Elastic Beanstalk

Overall explanation

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

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

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

INCORRECT: "AWS CodeDeploy" is incorrect. AWS CodeDeploy is a deployment service that automates application deployments to Amazon EC2 instances, on-premises instances, serverless Lambda functions, or Amazon ECS services.

INCORRECT: "AWS CloudFormation" is incorrect. AWS CloudFormation uses templates to deploy infrastructure as code. It is not a PaaS service like Elastic Beanstalk and is more focused on infrastructure than applications and management of applications.

INCORRECT: "AWS OpsWorks" is incorrect. AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet.

References:

https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/aws-elastic-beanstalk/

Domain

AWS Compute

Question 40Skipped

The database layer of an on-premises web application is being migrated to AWS. The database currently uses an in-memory cache. A Solutions Architect must deliver a solution that supports high availability and replication for the caching layer.

Which service should the Solutions Architect recommend?

Amazon RDS Multi-AZ

Amazon ElastiCache Memcached

Amazon DynamoDB

Correct answer

Amazon ElastiCache Redis

Overall explanation

Amazon ElastiCache Redis is an in-memory database cache and supports high availability through replicas and multi-AZ. The table below compares ElastiCache Redis with Memcached:

	Memcached	Redis (cluster mode disabled)	Redis (cluster mode enabled)
Data types	Simple	Complex	Complex
Data partitioning	Yes	No	Yes
Cluster is modifiable	Yes	Yes	No
Online re-sharding	No	No	3.2.10
Encryption	No	3.2.6	3.2.6
HIPAA Compliance	No	3.2.6	3.2.6
Multi-threaded	Yes	No	No
Node type upgrade	No	Yes	No
Engine upgrading	Yes	Yes	No
High availability (replication)	No	Yes	Yes
Automatic failover	No	Optional	Required

CORRECT: "Amazon ElastiCache Redis" is the correct answer.

INCORRECT: "Amazon ElastiCache Memcached" is incorrect as it does not support high availability or multi-AZ.

INCORRECT: "Amazon RDS Multi-AZ" is incorrect. This is not an in-memory database and it not suitable for use as a caching layer.

INCORRECT: "Amazon DynamoDB" is incorrect. DynamoDB is a non-relational database. You would not use it for a caching layer. Also, the in-memory, low-latency caching for DynamoDB is implemented using DynamoDB Accelerator (DAX).

References:

https://aws.amazon.com/elasticache/redis-vs-memcached/

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-elasticache/

Domain

AWS Database

Question 41Skipped

The load on a MySQL database running on Amazon EC2 is increasing and performance has been impacted. Which of the options below would help to increase storage performance? (choose 2)

Correct selection

Use Provisioned IOPS (I01) EBS volumes

Create a RAID 1 array from multiple EBS volumes

Use HDD, Cold (SC1) EBS volumes

Use a larger instance size within the instance family

Correct selection

Use EBS optimized instances

Overall explanation

EBS optimized instances provide dedicated capacity for Amazon EBS I/O. EBS optimized instances are designed for use with all EBS volume types.

Provisioned IOPS EBS volumes allow you to specify the amount of IOPS you require up to 50 IOPS per GB. Within this limitation you can therefore choose to select the IOPS required to improve the performance of your volume.

RAID can be used to increase IOPS, however RAID 1 does not. For example:

– 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.

HDD, Cold – (SC1) provides the lowest cost storage and low performance

CORRECT: "Use Provisioned IOPS (I01) EBS volumes" is a correct answer.

CORRECT: "Use EBS optimized instances" is also a correct answer.

INCORRECT: "Use a larger instance size within the instance family" is incorrect as this may not increase storage performance.

INCORRECT: "Use HDD, Cold (SC1) EBS volumes" is incorrect. As this will likely decrease storage performance.

INCORRECT: "Create a RAID 1 array from multiple EBS volumes" is incorrect. As explained above, mirroring does not increase performance.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-ebs/

Domain

AWS Storage

Question 42Skipped

A Solutions Architect has created a new security group in an Amazon VPC. No rules have been created. Which of the statements below are correct regarding the default state of the security group? (choose 2)

Correct selection

There are no inbound rules and traffic will be implicitly denied

There is an inbound rule allowing traffic from the Internet to port 22 for management

There is an outbound rule allowing traffic to the Internet Gateway

There are is an inbound rule that allows traffic from the Internet Gateway

Correct selection

There is an outbound rule that allows all traffic to all IP addresses

Overall explanation

Custom security groups do not have inbound allow rules (all inbound traffic is denied by default) whereas default security groups do have inbound allow rules (allowing traffic from within the group). All outbound traffic is allowed by default in both custom and default security groups.

Security groups act like a stateful firewall at the instance level. Specifically security groups operate at the network interface level of an EC2 instance. You can only assign permit rules in a security group, you cannot assign deny rules and there is an implicit deny rule at the end of the security group. All rules are evaluated until a permit is encountered or continues until the implicit deny. You can create ingress and egress rules.

CORRECT: "There is an outbound rule that allows all traffic to all IP addresses" is the correct answer.

CORRECT: "There are no inbound rules and traffic will be implicitly denied" is the correct answer.

INCORRECT: "There is an inbound rule allowing traffic from the Internet to port 22 for management" is incorrect. This is not true.

INCORRECT: "There are is an inbound rule that allows traffic from the Internet Gateway" is incorrect. There are no inbound allow rules by default.

INCORRECT: "There is an outbound rule allowing traffic to the Internet Gateway" is incorrect. There is an outbound allow rule but it allows traffic to anywhere, it does not specify the internet gateway.

References:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-vpc/

Domain

AWS Networking & Content Delivery

Question 43Skipped

A software development company is deploying a microservices-based application on Amazon Elastic Kubernetes Service (Amazon EKS). The application's traffic fluctuates significantly throughout the day and the company wants to ensure that the EKS cluster scales up and down according to these traffic patterns.

Which combination of steps would satisfy these requirements with MINIMAL operational overhead? (Select TWO.)

Implement the Kubernetes Vertical Pod Autoscaler to adjust the CPU and memory allocation for the pods.

Leverage AWS X-Ray to track and analyze the application's network activity.

Correct selection

Employ the Kubernetes Cluster Autoscaler for dynamically managing the quantity of nodes in the EKS cluster.

Integrate Amazon SQS and connect it to Amazon EKS for workload management.

Correct selection

Utilize the Kubernetes Metrics Server to enable horizontal pod autoscaling based on resource utilization.

Overall explanation

The Metrics Server collects resource metrics like CPU and memory usage from each node and its pods and provides these metrics to the Kubernetes API server for use by the Horizontal Pod Autoscaler, which automatically scales the number of pods in a deployment, replication controller, replica set, or stateful set based on observed CPU utilization.

The Kubernetes Cluster Autoscaler automatically adjusts the size of the Kubernetes cluster when there are pods that failed to run in the cluster due to insufficient resources or when there are nodes in the cluster that have been underutilized for an extended period and their pods can be placed on other existing nodes.

CORRECT: "Utilize the Kubernetes Metrics Server to enable horizontal pod autoscaling based on resource utilization" is a correct answer (as explained above.)

CORRECT: "Employ the Kubernetes Cluster Autoscaler for dynamically managing the quantity of nodes in the EKS cluster" is also a correct answer (as explained above.)

INCORRECT: "Implement the Kubernetes Vertical Pod Autoscaler to adjust the CPU and memory allocation for the pods" is incorrect.

The Vertical Pod Autoscaler adjusts the resources of the pods and not the number of pods or nodes, which won't directly help with scaling according to traffic patterns.

INCORRECT: "Integrate Amazon SQS and connect it to Amazon EKS for workload management" is incorrect.

Amazon SQS is a message queuing service, and while it can be used to manage workloads by decoupling microservices, it doesn't directly help with autoscaling an EKS cluster based on traffic patterns.

INCORRECT: "Leverage AWS X-Ray to track and analyze the application's network activity" is incorrect.

AWS X-Ray provides insights into the behavior of your applications, but it doesn't directly help with autoscaling an EKS cluster.

References:

https://kubernetes.io/docs/tasks/debug/debug-cluster/resource-metrics-pipeline/#metrics-server

https://docs.aws.amazon.com/eks/latest/userguide/autoscaling.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-ecs-and-eks/

Domain

AWS Compute

Question 44Skipped

A financial services company is migrating its sensitive customer data and applications to AWS. They want to ensure that the data is securely stored and managed while reducing the overall maintenance and operational overhead associated with managing databases.

Which solution will meet these requirements?

Correct answer

Migrate the data and applications to Amazon RDS instances. Enable encryption at rest using AWS Key Management Service (AWS KMS).

Store the data in Amazon S3. Utilize Amazon Macie for ongoing data security and threat detection.

Migrate the data to Amazon RDS instances. Enable Amazon GuardDuty for data protection and threat detection.

Migrate the applications and data to Amazon EC2 instances. Utilize the AWS Key Management Service (AWS KMS) customer managed keys for encryption.

Overall explanation

Amazon RDS makes it easy to go from project conception to deployment by managing time-consuming database administration tasks including backups, software patching, monitoring, scaling, and replication.

Amazon RDS supports encryption at rest, which ensures the security of sensitive data and meets regulatory compliance requirements. AWS Key Management Service (AWS KMS) is integrated with Amazon RDS to make it easier to create, control, and manage keys for encryption.

CORRECT: "Migrate the data and applications to Amazon RDS instances. Enable encryption at rest using AWS Key Management Service (AWS KMS)" is the correct answer (as explained above.)

INCORRECT: "Migrate the applications and data to Amazon EC2 instances. Utilize the AWS Key Management Service (AWS KMS) customer managed keys for encryption" is incorrect.

While this solution offers data encryption, it does not meet the requirement to reduce operational overhead. Managing databases on EC2 instances requires additional administrative tasks, such as managing backups and applying software patches, which Amazon RDS handles automatically.

INCORRECT: "Store the data in Amazon S3. Utilize Amazon Macie for ongoing data security and threat detection" is incorrect.

Amazon S3 and Macie are suitable for data storage and security analysis, respectively. However, Amazon S3 is not designed to serve as a transactional database for applications, which is a key requirement in this scenario.

INCORRECT: "Migrate the data to Amazon RDS instances. Enable Amazon GuardDuty for data protection and threat detection" is incorrect.

While Amazon RDS is a correct choice for database management and Amazon GuardDuty offers threat detection, GuardDuty is not specifically designed for data protection within databases. It's a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads.

References:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-rds/

https://digitalcloud.training/aws-kms/

Domain

AWS Database

Question 45Skipped

A digital media company uses an Amazon RDS MySQL instance for its content management system. Recently, the company has observed that their RDS instance is nearing its storage

capacity due to the constant influx of new data. The company wants to ensure there's always sufficient storage without any operational interruption or manual intervention.

Which solution should the company use to address this situation with the LEAST operational overhead?

Correct answer

Enable automatic storage scaling for the MySQL instance.

Utilize Amazon ElastiCache to offload some read traffic and reduce database load.

Migrate the database to a larger Amazon RDS MySQL instance.

Implement a lifecycle policy to delete older data from the MySQL instance.

Overall explanation

Amazon RDS's automatic storage scaling allows the database to automatically increase its storage capacity when the available storage is low. This feature helps to prevent out-of-storage situations and requires no operational overhead.

CORRECT: "Enable automatic storage scaling for the MySQL instance" is the correct answer (as explained above.)

INCORRECT: "Migrate the database to a larger Amazon RDS MySQL instance" is incorrect.

While this would provide more storage, it does not address the issue of potential future storage shortages and requires significant operational effort for the migration.

INCORRECT: "Implement a lifecycle policy to delete older data from the MySQL instance" is incorrect.

While this might help free up some storage, it might not be suitable if all data is essential for business operations. Also, this does not provide a long-term solution if data growth continues.

INCORRECT: "Utilize Amazon ElastiCache to offload some read traffic and reduce database load" is incorrect.

While ElastiCache can help to improve the database's read efficiency, it doesn't directly address the disk space concern for the RDS instance.

References:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PIOPS.StorageTypes.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-rds/

Domain

AWS Database

Question 46Skipped

A legacy application is being migrated into AWS. The application has a large amount of data that is rarely accessed. When files are accessed they are retrieved sequentially. The application will be migrated onto an Amazon EC2 instance.

What is the LEAST expensive EBS volume type for this use case?

Throughput Optimized HDD (st1)

Provisioned IOPS SSD (io1)

Correct answer

Cold HDD (sc1)

General Purpose SSD (gp2)

Overall explanation

The cold HDD (sc1) EBS volume type is the lowest cost option that is suitable for this use case. The sc1 volume type is suitable for infrequently accessed data and use cases that are oriented towards throughput like sequential data access.

	Solid-state drives (SSD)		Hard disk drives (HDD)	
Volume type	General Purpose SSD (gp2)	Provisioned IOPS SSD (io1)	Throughput Optimized HDD (st1)	Cold HDD (sc1)
Description	General purpose SSD volume that balances price and performance for a wide variety of workloads	Highest-performance SSD volume for mission-critical low-latency or high-throughput workloads	Low-cost HDD volume designed for frequently accessed, throughput-intensive workloads	Lowest cost HDD volume designed for less frequently accessed workloads
Use cases	• Recommended for most workloads • System boot volumes • Virtual desktops	• Critical business applications that require sustained IOPS performance, or more than 16,000 IOPS or 250 MiB/s of throughput per volume • Large database workloads,	• Streaming workloads requiring consistent, fast throughput at a low price • Big data	• Throughput-oriented storage for large volumes of data that is infrequently accessed

CORRECT: "Cold HDD (sc1)" is the correct answer.

INCORRECT: "Provisioned IOPS SSD (io1)" is incorrect. This is the most expensive option and used for use cases that demand high IOPS.

INCORRECT: "General Purpose SSD (gp2)" is incorrect. This is a more expensive SSD volume type that is used for general use cases.

INCORRECT: "Throughput Optimized HDD (st1)" is incorrect. This is also used for throughput-oriented use cases however it is higher cost than sc1 and better for frequently accessed data.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-ec2/

Domain

AWS Compute

Question 47Skipped

An application runs on EC2 instances in a private subnet behind an Application Load Balancer in a public subnet. The application is highly available and distributed across multiple AZs. The EC2 instances must make API calls to an internet-based service. How can the Solutions Architect enable highly available internet connectivity?

Configure an internet gateway. Add a route to the gateway to each private subnet route table

Correct answer

Create a NAT gateway in the public subnet of each AZ. Update the route tables for each private subnet to direct internet-bound traffic to the NAT gateway

Create a NAT instance in the private subnet of each AZ. Update the route tables for each private subnet to direct internet-bound traffic to the NAT instance

Create a NAT gateway and attach it to the VPC. Add a route to the gateway to each private subnet route table

Overall explanation

The only solution presented that actually works is to create a NAT gateway in the public subnet of each AZ. They must be created in the public subnet as they gain public IP addresses and use an internet gateway for internet access.

The route tables in the private subnets must then be configured with a route to the NAT gateway and then the EC2 instances will be able to access the internet (subject to security group configuration).

CORRECT: "Create a NAT gateway in the public subnet of each AZ. Update the route tables for each private subnet to direct internet-bound traffic to the NAT gateway" is the correct answer.

INCORRECT: "Create a NAT gateway and attach it to the VPC. Add a route to the gateway to each private subnet route table" is incorrect. You do not attach NAT gateways to VPCs, you add them to public subnets.

INCORRECT: "Configure an internet gateway. Add a route to the gateway to each private subnet route table" is incorrect. You cannot add a route to an internet gateway to a private subnet route table (private EC2 instances don’t even have public IP addresses).

INCORRECT: "Create a NAT instance in the private subnet of each AZ. Update the route tables for each private subnet to direct internet-bound traffic to the NAT instance" is incorrect. You do not create NAT instances in private subnets, they must be created in public subnets.

References:

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-vpc/

Domain

AWS Compute

Question 48Skipped

A data analytics company is building a high-performance application that requires concurrent writes to a shared block storage volume from multiple Amazon EC2 instances.

The EC2 instances are Nitro-based and reside within the same Availability Zone. The company needs a storage solution that supports simultaneous connections to facilitate data resilience and high availability.

Which solution will meet these requirements?

Use Amazon S3 with S3 Transfer Acceleration to enhance speed.

Correct answer

Use Provisioned IOPS SSD (io2) EBS volumes with Amazon EBS Multi-Attach.

Use General Purpose SSD (gp2) EBS volumes with Amazon EBS Multi-Attach.

Use Amazon EFS with NFSv4.1 protocol across multiple EC2 instances.

Overall explanation

io2 volumes are designed for I/O-intensive workloads, particularly database workloads, that require high performance and low latency. io1 and io2 volumes support Multi-Attach, which enables you to attach a single volume to multiple EC2 instances in the same Availability Zone.

CORRECT: "Use Provisioned IOPS SSD (io2) EBS volumes with Amazon EBS Multi-Attach" is the correct answer (as explained above.)

INCORRECT: "Use Amazon EFS with NFSv4.1 protocol across multiple EC2 instances" is incorrect.

Amazon Elastic File System (EFS) is a scalable file storage for use with Amazon EC2. You can use an Amazon EFS file system as a common data source for workloads and applications running on multiple instances, but it does not provide the block-level storage required for high IOPS operations.

INCORRECT: "Use Amazon S3 with S3 Transfer Acceleration to enhance speed" is incorrect.

Amazon S3 is an object storage service. While S3 Transfer Acceleration does enhance the speed of in-transit file transfers, it is not a block storage solution, it is an object storage solution and is not suitable for this use case.

INCORRECT: "Use General Purpose SSD (gp2) EBS volumes with Amazon EBS Multi-Attach" is incorrect.

Amazon EBS Multi-Attach only supports io1 and io2 volumes, and it is not supported on gp2 volumes.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes-multi.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-ebs/

Domain

AWS Compute

Question 49Skipped

A company is deploying a new two-tier web application that uses EC2 web servers and a DynamoDB database backend. An Internet facing ELB distributes connections between the web servers.

The Solutions Architect has created a security group for the web servers and needs to create a security group for the ELB. What rules should be added? (choose 2)

Add an Outbound rule that allows HTTP/HTTPS, and specify the destination as VPC CIDR

Correct selection

Add an Outbound rule that allows HTTP/HTTPS, and specify the destination as the web server security group

Add an Outbound rule that allows ALL TCP, and specify the destination as the Internet Gateway

Correct selection

Add an Inbound rule that allows HTTP/HTTPS, and specify the source as 0.0.0.0/0

Add an Inbound rule that allows HTTP/HTTPS, and specify the source as 0.0.0.0/32

Overall explanation

An inbound rule should be created for the relevant protocols (HTTP/HTTPS) and the source should be set to any address (0.0.0.0/0).

The outbound rule should forward the relevant protocols (HTTP/HTTPS) and the destination should be set to the web server security group.

Note that on the web server security group you'd want to add an Inbound rule allowing HTTP/HTTPS from the ELB security group.

CORRECT: "Add an Outbound rule that allows HTTP/HTTPS, and specify the destination as the web server security group" is a correct answer.

CORRECT: "Add an Inbound rule that allows HTTP/HTTPS, and specify the source as 0.0.0.0/0" is also a correct answer.

INCORRECT: "Add an Outbound rule that allows ALL TCP, and specify the destination as the Internet Gateway" is incorrect as the relevant protocol should be specified and the destination should be the web server security group.

INCORRECT: "Add an Outbound rule that allows HTTP/HTTPS, and specify the destination as VPC CIDR" is incorrect. Using the VPC CIDR would not be secure and you cannot specify an Internet Gateway in a security group (not that you'd want to anyway).

INCORRECT: "Add an Inbound rule that allows HTTP/HTTPS, and specify the source as 0.0.0.0/32" is incorrect. The address 0.0.0.0/32 is incorrect as the 32 mask means an exact match is required (0.0.0.0).

References:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/aws-elastic-load-balancing-aws-elb/

Domain

AWS Networking & Content Delivery

Question 50Skipped

A corporation has a web-based multiplayer gaming service that operates using both TCP and UDP protocols. Amazon Route 53 is currently employed to direct application traffic to a set of Network Load Balancers (NLBs) in various AWS Regions. To prepare for an increase in user activity, the company must enhance application performance and reduce latency.

Which approach will best meet these requirements?

Incorporate Amazon CloudFront in front of the NLBs and extend the duration of the Cache-Control max-age directive.

Insert an Amazon API Gateway endpoint behind the NLBs, enable API caching, and customize method caching across different stages.

Substitute the NLBs with Application Load Balancers (ALBs) and set Route 53 to utilize latency-based routing.

Correct answer

Implement AWS Global Accelerator ahead of the NLBs and align the Global Accelerator endpoint to use the appropriate listener ports.

Overall explanation

AWS Global Accelerator is designed to improve the availability and performance of your applications for local and global users. It directs traffic to optimal endpoints over the AWS global network, thus enhancing the performance of your TCP and UDP traffic by routing packets through the AWS global network infrastructure, reducing jitter, and improving overall game performance.

CORRECT: "Implement AWS Global Accelerator ahead of the NLBs and align the Global Accelerator endpoint to use the appropriate listener ports" is the correct answer (as explained above.)

INCORRECT: "Incorporate Amazon CloudFront in front of the NLBs and extend the duration of the Cache-Control max-age directive" is incorrect.

Amazon CloudFront is a content delivery network (CDN) that speeds up the delivery of your static and dynamic web content. While it could potentially help with application performance, it doesn't directly improve TCP/UDP performance, which is the specific requirement in this case.

INCORRECT: "Substitute the NLBs with Application Load Balancers (ALBs) and set Route 53 to utilize latency-based routing" is incorrect.

Application Load Balancers (ALBs) are layer 7 load balancers and they do not support the handling of raw TCP and UDP traffic, which is a requirement for the gaming application in the question. NLBs, on the other hand, are suitable for extreme performance needs and for TCP/UDP traffic.

INCORRECT: "Insert an Amazon API Gateway endpoint behind the NLBs, enable API caching, and customize method caching across different stages" is incorrect.

While the API Gateway would add more control and security to the application, the caching feature is not necessarily beneficial for this real-time gaming scenario where the content is likely to change frequently and unpredictably.

References:

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

Save time with our AWS cheat sheets:

https://digitalcloud.training/aws-global-accelerator/

Domain

AWS Networking & Content Delivery

Question 51Skipped

A cloud architect is assessing the resilience of a web application deployed on AWS. It was observed that the application experienced a downtime of about 3 minutes when a scheduled failover was performed on the application's Amazon RDS MySQL database as part of a scaling operation.

The organization wants to mitigate such downtime in future scaling exercises while minimizing operational overhead.

Which solution will be the MOST effective in achieving this?

Correct answer

Configure an Amazon RDS Proxy for the database and modify the application to connect to the proxy endpoint.

Establish a secondary RDS MySQL cluster within the same AWS Region. During any future failover, modify the application to connect to the secondary cluster's writer endpoint.

Implement an Amazon ElastiCache for Redis cluster to manage the load during the failover.

Implement more RDS MySQL read replicas in the cluster to manage the load during the failover.

Overall explanation

Amazon RDS Proxy is a fully managed, highly available database proxy for Amazon RDS that makes applications more scalable, more resilient to database failures, and more secure.

During a failover, RDS Proxy automatically connects to a standby database instance while preserving connections from your application and reducing failover times for RDS and Aurora multi-AZ databases. So, there is minimal downtime for the application.

CORRECT: "Configure an Amazon RDS Proxy for the database and modify the application to connect to the proxy endpoint" is the correct answer (as explained above.)

INCORRECT: "Implement more RDS MySQL read replicas in the cluster to manage the load during the failover" is incorrect.

Adding more read replicas to the cluster does not decrease the downtime during a failover. It only improves the database's ability to handle read-heavy workloads. Read replicas do not contribute to a faster failover process.

INCORRECT: "Establish a secondary RDS MySQL cluster within the same AWS Region. During any future failover, modify the application to connect to the secondary cluster's writer endpoint" is incorrect.

This approach is operationally heavy as it involves managing two separate RDS clusters and manually updating the application's database endpoint during a failover. Moreover, it does not necessarily reduce the downtime during a failover as there might be data inconsistency issues between the primary and secondary clusters, depending on the replication latency.

INCORRECT: "Implement an Amazon ElastiCache for Redis cluster to manage the load during the failover" is incorrect.

ElastiCache is an in-memory cache and not a relational database service. It is typically used to cache frequently accessed data to reduce latency and improve application performance, not for managing failovers.

References:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/rds-proxy.html

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-rds/

Domain

AWS Compute

Question 52Skipped

A Solutions Architect needs to upload a large (2GB) file to an S3 bucket. What is the recommended way to upload a single large file to an S3 bucket?

Use AWS Import/Export

Use a single PUT request to upload the large file

Correct answer

Use Multipart Upload

Use Amazon Snowball

Overall explanation

In general, when your object size reaches 100 MB, you should consider using multipart uploads instead of uploading the object in a single operation.

CORRECT: "Use Multipart Upload" is the correct answer.

INCORRECT: "Use AWS Import/Export" is incorrect. AWS Import/Export is a service in which you send in HDDs with data on to AWS and they import your data into S3. It is not used for single files.

INCORRECT: "Use a single PUT request to upload the large file" is incorrect. The largest object that can be uploaded in a single PUT is 5 gigabytes.

INCORRECT: "Use Amazon Snowball" is incorrect. Snowball is used for migrating large quantities (TB/PB) of data into AWS, it is overkill for this requirement.

References:

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

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-s3-and-glacier/

Domain

AWS Storage

Question 53Skipped

A company is transitioning their web presence into the AWS cloud. As part of the migration the company will be running a web application both on-premises and in AWS for a period of time. During the period of co-existence the client would like 80% of the traffic to hit the AWS-based web servers and 20% to be directed to the on-premises web servers.

What method can a Solutions Architect use to distribute traffic as requested?

Use an Application Load Balancer to distribute traffic based on IP address

Use Route 53 with a simple routing policy

Use a Network Load Balancer to distribute traffic based on Instance ID

Correct answer

Use Route 53 with a weighted routing policy and configure the respective weights

Overall explanation

Route 53 weighted routing policy is similar to simple but you can specify a weight per IP address. You create records that have the same name and type and assign each record a relative weight which is a numerical value that favours one IP over another (values must total 100). To stop sending traffic to a resource you can change the weight of the record to 0.

CORRECT: "Use Route 53 with a weighted routing policy and configure the respective weights" is the correct answer.

INCORRECT: "Use Route 53 with a simple routing policy" is incorrect as this will not split traffic based on weights as required.

INCORRECT: "Use an Application Load Balancer to distribute traffic based on IP address" is incorrect. Application Load Balancer can distribute traffic to AWS and on-premise resources using IP addresses but cannot be used to distribute traffic in a weighted manner.

INCORRECT: "Use a Network Load Balancer to distribute traffic based on Instance ID" is incorrect. Network Load Balancer can distribute traffic to AWS and on-premise resources using IP addresses (not Instance IDs).

References:

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/aws-elastic-load-balancing-aws-elb/

https://digitalcloud.training/amazon-route-53/

Domain

AWS Networking & Content Delivery

Question 54Skipped

An Amazon DynamoDB table has a variable load, ranging from sustained heavy usage some days, to only having small spikes on others. The load is 80% read and 20% write. The provisioned throughput capacity has been configured to account for the heavy load to ensure throttling does not occur.

What would be the most efficient solution to optimize cost?

Create a CloudWatch alarm that triggers an AWS Lambda function that adjusts the provisioned throughput

Create a CloudWatch alarm that notifies you of increased/decreased load, and manually adjust the provisioned throughput

Correct answer

Create a DynamoDB Auto Scaling scaling policy

Use DynamoDB DAX to increase the performance of the database

Overall explanation

Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to dynamically adjust provisioned throughput capacity on your behalf, in response to actual traffic patterns. This is the most efficient and cost-effective solution to optimizing for cost.

CORRECT: "Create a DynamoDB Auto Scaling scaling policy" is the correct answer.

INCORRECT: "Create a CloudWatch alarm that triggers an AWS Lambda function that adjusts the provisioned throughput" is incorrect. Using AWS Lambda to modify the provisioned throughput is possible but it would be more cost-effective to use DynamoDB Auto Scaling as there is no cost to using it.

INCORRECT: "Create a CloudWatch alarm that notifies you of increased/decreased load, and manually adjust the provisioned throughput" is incorrect. Manually adjusting the provisioned throughput is not efficient.

INCORRECT: "Use DynamoDB DAX to increase the performance of the database" is incorrect. DynamoDB DAX is an in-memory cache that increases the performance of DynamoDB. However, it costs money and there is no requirement to increase performance.

References:

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

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-dynamodb/

Domain

AWS Database

Question 55Skipped

Several Amazon EC2 Spot instances are being used to process messages from an Amazon SQS queue and store results in an Amazon DynamoDB table. Shortly after picking up a message from the queue AWS terminated the Spot instance. The Spot instance had not finished processing the message. What will happen to the message?

The message will remain in the queue and be immediately picked up by another instance

The message will be lost as it would have been deleted from the queue when processed

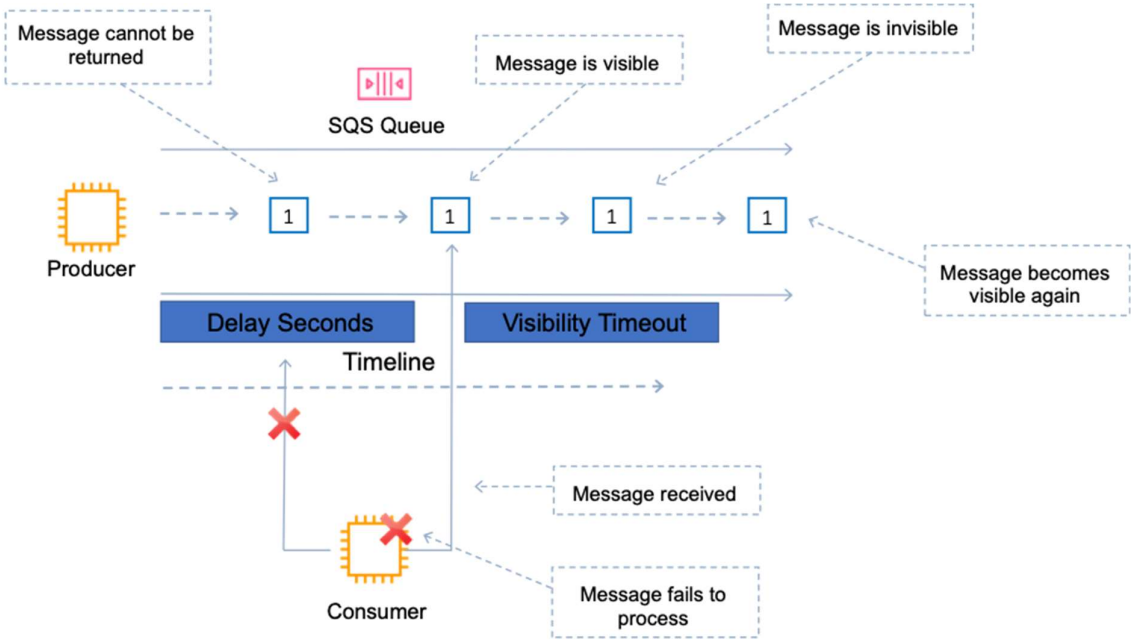
The results may be duplicated in DynamoDB as the message will likely be processed multiple times

Correct answer

The message will become available for processing again after the visibility timeout expires

Overall explanation

The visibility timeout is the amount of time a message is invisible in the queue after a reader picks up the message. If a job is processed within the visibility timeout the message will be deleted. If a job is not processed within the visibility timeout the message will become visible again (could be delivered twice). The maximum visibility timeout for an Amazon SQS message is 12 hours.



CORRECT: "The message will become available for processing again after the visibility timeout expires" is the correct answer.

INCORRECT: "The message will be lost as it would have been deleted from the queue when processed" is incorrect. The message will not be lost and will not be immediately picked up by another instance.

INCORRECT: "The message will remain in the queue and be immediately picked up by another instance" is incorrect. As mentioned above it will be available for processing in the queue again after the timeout expires.

INCORRECT: "The results may be duplicated in DynamoDB as the message will likely be processed multiple times" is incorrect. As the instance had not finished processing the message it should only be fully processed once. Depending on your application process however it is possible some data was written to DynamoDB.

References:

https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/aws-application-integration-services/

Domain

AWS Application Integration

Question 56Skipped

An e-commerce company operates a serverless web application that must interact with numerous Amazon DynamoDB tables to fulfill user requests. It is critical that the application's performance remains consistent and unaffected while interacting with these tables.

Which method provides the MOST operationally efficient way to fulfill these requirements?

AWS Lambda with Step Functions.

AWS Glue with a DynamoDB connector.

Correct answer

AWS AppSync with multiple data sources and resolvers.

Amazon S3 with Lambda triggers.

Overall explanation

AWS AppSync simplifies application development by letting you create a flexible API to securely access, manipulate, and combine data from one or more data sources. AppSync is a managed service that uses GraphQL to make it easy for applications to get exactly the data they need, including from multiple DynamoDB tables.

AWS AppSync is designed for real-time and offline data access which makes it an ideal solution for this scenario.

CORRECT: "AWS AppSync with multiple data sources and resolvers" is the correct answer (as explained above.)

INCORRECT: "AWS Lambda with Step Functions" is incorrect.

AWS Step Functions make it easy to coordinate the components of distributed applications and microservices using visual workflows. However, while you could theoretically build a flow to retrieve data from multiple tables, it's not the most efficient solution as it introduces additional complexity and potential latency.

INCORRECT: "Amazon S3 with Lambda triggers" is incorrect.

While you can use AWS Lambda to execute code in response to triggers like changes to data in an Amazon S3 bucket, this doesn't directly allow the application to retrieve data from multiple DynamoDB tables. This approach would also involve unnecessary data transfers and added latency.

INCORRECT: "AWS Glue with a DynamoDB connector" is incorrect.

AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy to prepare and load your data for analytics. However, AWS Glue isn't meant for real-time data retrieval in an application. Using it for real-time data retrieval would likely be overcomplicated and inefficient.

References:

https://aws.amazon.com/appsync/product-details/

Domain

AWS Compute

Question 57Skipped

One of the departments in a company has been generating a large amount of data on Amazon S3 and costs are increasing. Data older than 90 days is rarely accessed but must be retained for several years. If this data does need to be accessed at least 24 hours notice is provided.

How can a Solutions Architect optimize the costs associated with storage of this data whilst ensuring it is accessible if required?

Implement archival software that automatically moves the data to tape

Use S3 lifecycle policies to move data to the STANDARD_IA storage class

Select the older data and manually migrate it to GLACIER

Correct answer

Use S3 lifecycle policies to move data to GLACIER after 90 days

Overall explanation

To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle. A lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. Transition actions define when objects transition to another storage class.

For example, you might choose to transition objects to the STANDARD_IA storage class 30 days after you created them, or archive objects to the GLACIER storage class one year after creating them.

GLACIER retrieval times:

- Standard retrieval is 3-5 hours which is well within the requirements here.

- You can use Expedited retrievals to access data in 1 – 5 minutes.

- You can use Bulk retrievals to access up to petabytes of data in approximately 5 – 12 hours.

CORRECT: "Use S3 lifecycle policies to move data to GLACIER after 90 days" is the correct answer.

INCORRECT: "Implement archival software that automatically moves the data to tape" is incorrect as this solution can be fully automated using lifecycle policies.

INCORRECT: "Use S3 lifecycle policies to move data to the STANDARD_IA storage class" is incorrect. STANDARD_IA is good for infrequently accessed data and provides faster access times than GLACIER but is more expensive so not the best option here.

INCORRECT: "Select the older data and manually migrate it to GLACIER" is incorrect as a lifecycle policy can automate the process.

References:

https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html

https://aws.amazon.com/about-aws/whats-new/2016/11/access-your-amazon-glacier-data-in-minutes-with-new-retrieval-options/

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-s3-and-glacier/

Domain

AWS Storage

Question 58Skipped

An on-premises server runs a MySQL database and will be migrated to the AWS Cloud. The company require a managed solution that supports high availability and automatic failover in the event of the outage of an Availability Zone (AZ).

Which solution is the BEST fit for these requirements?

Correct answer

Use the AWS Database Migration Service (DMS) to directly migrate the database to an Amazon RDS MySQL Multi-AZ deployment

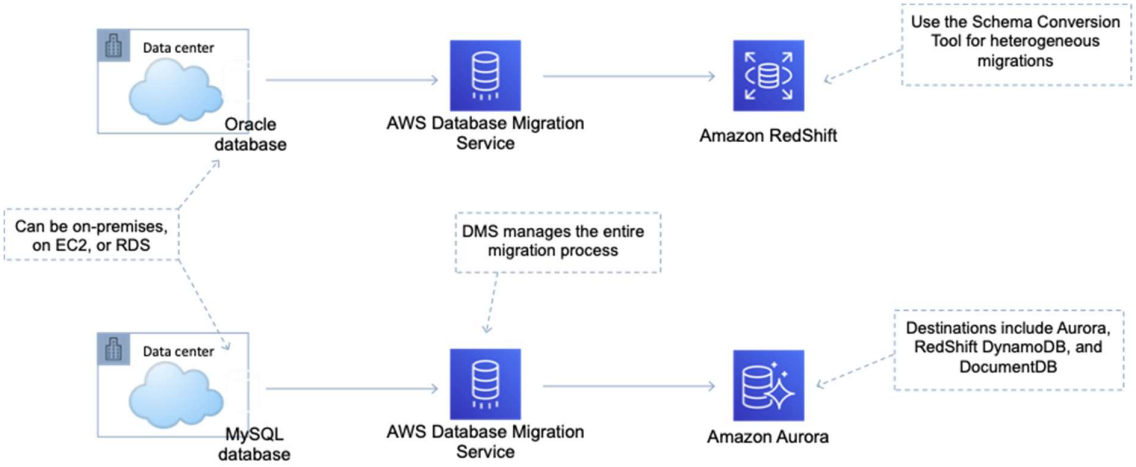
Use the AWS Database Migration Service (DMS) to directly migrate the database to an Amazon EC2 MySQL Multi-AZ deployment

Create a snapshot of the MySQL database server and use AWS DataSync to migrate the data Amazon S3. Launch a new Amazon RDS MySQL Multi-AZ deployment from the snapshot

Use the AWS Database Migration Service (DMS) to directly migrate the database to Amazon RDS MySQL. Use the Schema Conversion Tool (SCT) to enable conversion from MySQL to Amazon RDS

Overall explanation

The AWS DMS service can be used to directly migrate the MySQL database to an Amazon RDS Multi-AZ deployment. The entire process can be online and is managed for you. There is no need to perform schema translation between MySQL and RDS (assuming you choose the MySQL RDS engine).



CORRECT: "Use the AWS Database Migration Service (DMS) to directly migrate the database to an Amazon RDS MySQL Multi-AZ deployment" is the correct answer.

INCORRECT: "Use the AWS Database Migration Service (DMS) to directly migrate the database to an Amazon EC2 MySQL Multi-AZ deployment" is incorrect as there is no such thing as “multi-AZ” on Amazon EC2 with MySQL, you must use RDS.

INCORRECT: "Create a snapshot of the MySQL database server and use AWS DataSync to migrate the data Amazon S3. Launch a new Amazon RDS MySQL Multi-AZ deployment from the snapshot" is incorrect. You cannot create a snapshot of a MySQL database server running on-premises.

INCORRECT: "Use the AWS Database Migration Service (DMS) to directly migrate the database to Amazon RDS MySQL. Use the Schema Conversion Tool (SCT) to enable conversion from MySQL to Amazon RDS" is incorrect. There is no need to convert the schema when migrating from MySQL to Amazon RDS (MySQL engine).

References:

https://aws.amazon.com/rds/features/multi-az/

https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Introduction.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-rds/

https://digitalcloud.training/aws-migration-services/

Domain

AWS Migration & Transfer

Question 59Skipped

A company is looking for ways to incorporate its current AWS usage expenditure into its operational expense tracking dashboard. A solutions architect has been tasked with proposing a method that enables the company to fetch its current year's cost data and project the costs for the forthcoming 12 months programmatically.

Which approach would fulfill these needs with the MINIMUM operational burden?

Correct answer

Leverage the AWS Cost Explorer API to retrieve usage cost-related data, using pagination for larger data sets.

Make use of downloadable AWS Cost Explorer report files in the .csv format to access usage cost-related data.

Set up AWS Budgets actions to transmit usage cost data to the corporation via FTP.

Generate AWS Budgets reports on usage cost data and dispatch the data to the corporation through SMTP.

Overall explanation

AWS Cost Explorer API provides programmatic access to AWS cost and usage information. The user can query for aggregated data such as total monthly costs or total daily usage with this API.

Also, the Cost Explorer API supports pagination for managing larger data sets, making it efficient for larger queries.

CORRECT: "Leverage the AWS Cost Explorer API to retrieve usage cost-related data, using pagination for larger data sets" is the correct answer (as explained above.)

INCORRECT: "Make use of downloadable AWS Cost Explorer report files in the .csv format to access usage cost-related data" is incorrect.

While AWS Cost Explorer does allow you to download .csv reports of your cost data, this method would not be programmatically accessible and would involve manual steps to download and process the data.

INCORRECT: "Set up AWS Budgets actions to transmit usage cost data to the corporation via FTP" is incorrect.

AWS Budgets actions allow you to set custom cost and usage budgets that trigger actions (such as turning off EC2 instances) when the budget thresholds you set are breached. However, AWS Budgets does not support transmitting data via FTP.

INCORRECT: "Generate AWS Budgets reports on usage cost data and dispatch the data to the corporation through SMTP" is incorrect.

AWS Budgets does not support the dispatching of data through SMTP. AWS Budgets is primarily a tool for setting up alerts on your AWS costs or usage to control your costs, rather than a tool for exporting or transmitting cost data.

References:

https://docs.aws.amazon.com/aws-cost-management/latest/APIReference/API_Operations_AWS_Cost_Explorer_Service.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/aws-cost-management/

Domain

AWS Management & Governance

Question 60Skipped

A Solutions Architect has created a new Network ACL in an Amazon VPC. No rules have been created. Which of the statements below are correct regarding the default state of the Network ACL? (choose 2)

There is a default outbound rule allowing all traffic

Correct selection

There is a default inbound rule denying all traffic

Correct selection

There is a default outbound rule denying all traffic

There is a default outbound rule allowing traffic to the Internet Gateway

There is a default inbound rule allowing traffic from the VPC CIDR block

Overall explanation

A VPC automatically comes with a default network ACL which allows all inbound/outbound traffic. A custom NACL denies all traffic both inbound and outbound by default.

Network ACL's function at the subnet level and you can have permit and deny rules. Network ACLs have separate inbound and outbound rules and each rule can allow or deny traffic.

Network ACLs are stateless so responses are subject to the rules for the direction of traffic. NACLs only apply to traffic that is ingress or egress to the subnet not to traffic within the subnet.

CORRECT: "There is a default inbound rule denying all traffic" is a correct answer.

CORRECT: "There is a default outbound rule denying all traffic" is also a correct answer.

INCORRECT: "There is a default inbound rule allowing traffic from the VPC CIDR block" is incorrect as inbound traffic is not allowed from anywhere by default.

INCORRECT: "There is a default outbound rule allowing traffic to the Internet Gateway" is incorrect as outbound traffic is not allowed to anywhere by default.

INCORRECT: "There is a default outbound rule allowing all traffic" is incorrect as all traffic is denied.

References:

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-vpc/

Domain

AWS Networking & Content Delivery

Question 61Skipped

A Solutions Architect has created an AWS Organization with several AWS accounts. Security policy requires that use of specific API actions are limited across all accounts. The Solutions Architect requires a method of centrally controlling these actions.

What is the SIMPLEST method of achieving the requirements?

Create a Network ACL that limits access to the services or actions and attach it to all relevant subnets

Create cross-account roles in each account to limit access to the services and actions that are allowed

Correct answer

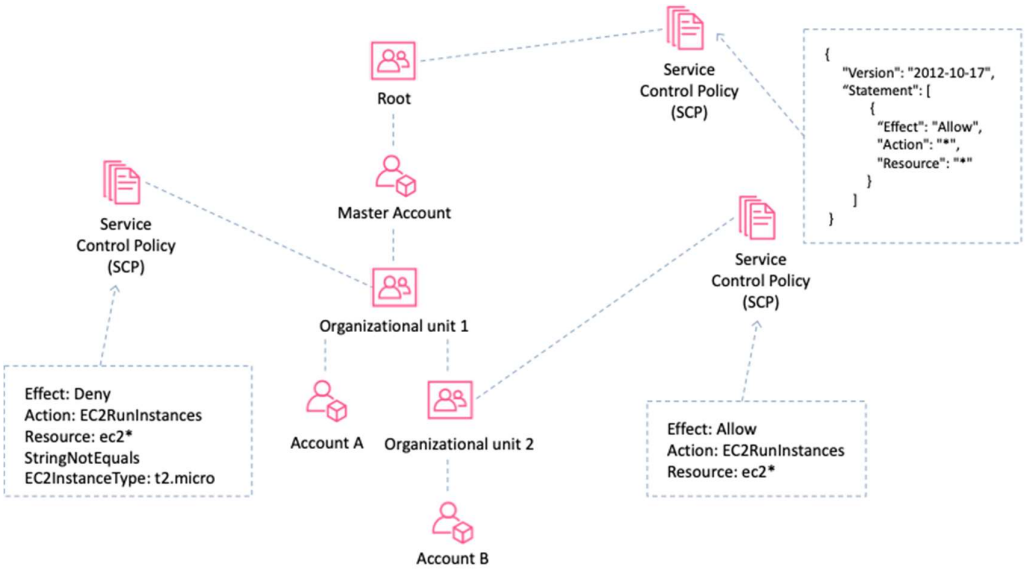
Create a service control policy in the root organizational unit to deny access to the services or actions

Create an IAM policy in the root account and attach it to users and groups in each account

Overall explanation

Service control policies (SCPs) offer central control over the maximum available permissions for all accounts in your organization allowing you to ensure your accounts stay within your organization's access control guidelines.

In the example below, a policy in OU1 restricts all users from launching EC2 instance types other than a t2.micro:



CORRECT: "Create a service control policy in the root organizational unit to deny access to the services or actions" is the correct answer.

INCORRECT: "Create a Network ACL that limits access to the services or actions and attach it to all relevant subnets" is incorrect. Network ACLs control network traffic - not API actions.

INCORRECT: "Create an IAM policy in the root account and attach it to users and groups in each account" is incorrect. This is not an efficient or centrally managed method of applying the security restrictions.

INCORRECT: "Create cross-account roles in each account to limit access to the services and actions that are allowed" is incorrect. This is another example of a complex and inefficient method of providing access across accounts and does not restrict API actions within the account.

References:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_about-scps.html

Save time with our AWS cheat sheets:

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

Domain

AWS Management & Governance

Question 62Skipped

A large quantity of data that is rarely accessed is being archived onto Amazon Glacier. Your CIO wants to understand the resilience of the service. Which of the statements below is correct about Amazon Glacier storage? (choose 2)

Provides 99.9% availability of archives

Correct selection

Provides 99.999999999% durability of archives

Data is resilient in the event of one entire region destruction

Correct selection

Data is resilient in the event of one entire Availability Zone destruction

Data is replicated globally

Overall explanation

Glacier is designed for durability of 99.999999999% of objects across multiple Availability Zones. Data is resilient in the event of one entire Availability Zone destruction. Glacier supports SSL for data in transit and encryption of data at rest. Glacier is extremely low cost and is ideal for long-term archival.

CORRECT: "Provides 99.999999999% durability of archives" is the correct answer.

CORRECT: "Data is resilient in the event of one entire Availability Zone destruction" is the correct answer.

INCORRECT: "Data is replicated globally" is incorrect. Data is not replicated globally.

INCORRECT: "Data is resilient in the event of one entire region destruction" is incorrect. Data is not resilient to the failure of an entire region.

INCORRECT: "Provides 99.9% availability of archives" is incorrect. Glacier is “designed for” availability of **99.99%**

References:

https://aws.amazon.com/s3/storage-classes/

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-s3-and-glacier/

Domain

AWS Storage

Question 63Skipped

A Solutions Architect is designing the disk configuration for an Amazon EC2 instance. The instance needs to support a MapReduce process that requires high throughput for a large dataset with large I/O sizes.

Which Amazon EBS volume is the MOST cost-effective solution for these requirements?

EBS General Purpose SSD in a RAID 1 configuration

EBS General Purpose SSD

EBS Provisioned IOPS SSD

Correct answer

EBS Throughput Optimized HDD

Overall explanation

EBS Throughput Optimized HDD is good for the following use cases (and is the most cost-effective option:

- Frequently accessed, throughput intensive workloads with large datasets and large I/O sizes, such as MapReduce, Kafka, log processing, data warehouse, and ETL workloads.

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

CORRECT: "EBS Throughput Optimized HDD" is the correct answer.

INCORRECT: "EBS General Purpose SSD in a RAID 1 configuration" is incorrect. This is not the best solution for the requirements or the most cost-effective.

INCORRECT: "EBS Provisioned IOPS SSD" is incorrect. SSD disks are more expensive.

INCORRECT: "EBS General Purpose SSD" is incorrect. SSD disks are more expensive.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-ebs/

Domain

AWS Storage

Question 64Skipped

An on-premise data center will be connected to an Amazon VPC by a hardware VPN that has public and VPN-only subnets. The security team has requested that traffic hitting public subnets on AWS that's destined to on-premise applications must be directed over the VPN to the corporate firewall.

How can this be achieved?

Configure a NAT Gateway and configure all traffic to be directed via the virtual private gateway

In the VPN-only subnet route table, add a route that directs all Internet traffic to the virtual private gateway

Correct answer

In the public subnet route table, add a route for your remote network and specify the virtual private gateway as the target

In the public subnet route table, add a route for your remote network and specify the customer gateway as the target

Overall explanation

Route tables determine where network traffic is directed. In your route table, you must add a route for your remote network and specify the virtual private gateway as the target. This enables traffic from your VPC that's destined for your remote network to route via the virtual private gateway and over one of the VPN tunnels. You can enable route propagation for your route table to automatically propagate your network routes to the table for you.

CORRECT: "In the public subnet route table, add a route for your remote network and specify the virtual private gateway as the target" is the correct answer.

INCORRECT: "In the VPN-only subnet route table, add a route that directs all Internet traffic to the virtual private gateway" is incorrect. You must create the route table rule in the route table attached to the public subnet, not the VPN-only subnet.

INCORRECT: "In the public subnet route table, add a route for your remote network and specify the customer gateway as the target" is incorrect. You must select the virtual private gateway (AWS side of the VPN) not the customer gateway (customer side of the VPN) in the target in the route table.

INCORRECT: "Configure a NAT Gateway and configure all traffic to be directed via the virtual private gateway" is incorrect. NAT Gateways are used to enable Internet access for EC2 instances in private subnets, they cannot be used to direct traffic to VPG.

References:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_VPN.html

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario3.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-vpc/

Domain

AWS Networking & Content Delivery

Question 65Skipped

A company operates a critical Python-based application that analyzes incoming real-time data. The application runs every 15 minutes and takes approximately 2 minutes to complete a run. It requires 1.5 GB of memory and uses the CPU intensively during its operation. The company wants to minimize the costs associated with running this application.

Which solution will meet these requirements?

Use AWS App2Container (A2C) to containerize the application. Deploy the container on an Amazon EC2 instance, configure an Amazon CloudWatch alarm to stop the instance when the application is not running.

Use AWS App2Container (A2C) to containerize the application. Run the application as an Amazon Elastic Container Service (Amazon ECS) task on AWS Fargate with 1 virtual CPU (vCPU) and 1.5 GB of memory.

Correct answer

Implement the application as an AWS Lambda function configured with 1.5 GB of memory. Use Amazon EventBridge to schedule the function to run every 15 minutes.

Deploy the application on an Amazon EC2 instance and manually start and stop the instance in alignment with the schedule of the application run.

Overall explanation

This is the most cost-effective solution. AWS Lambda is designed for running code in response to events or on a schedule, and you only pay for the compute time that you consume.

Configuring the function with 1.5GB memory would ensure the function has enough resources, and using Amazon EventBridge for scheduling would enable running the function every 15 minutes.

CORRECT: "Implement the application as an AWS Lambda function configured with 1.5 GB of memory. Use Amazon EventBridge to schedule the function to run every 15 minutes" is the correct answer (as explained above.)

INCORRECT: "Use AWS App2Container (A2C) to containerize the application. Run the application as an Amazon Elastic Container Service (Amazon ECS) task on AWS Fargate with 1 virtual CPU (vCPU) and 1.5 GB of memory" is incorrect.

This is not the most cost-effective solution. Even though AWS App2Container (A2C) would help in containerizing the application and AWS Fargate would abstract the need to manage underlying EC2 instances, it is still an overkill for an application that runs for short durations intermittently. It would still result in paying for unused compute resources.

INCORRECT: "Use AWS App2Container (A2C) to containerize the application. Deploy the container on an Amazon EC2 instance, configure an Amazon CloudWatch alarm to stop the instance when the application is not running" is incorrect.

AWS App2Container (A2C) is used to help containerize applications, but this does not optimize for cost because it requires running an EC2 instance continuously and stopping the instance when not in use can be complex and might not be timely, resulting in potential unnecessary costs.

INCORRECT: "Deploy the application on an Amazon EC2 instance and manually start and stop the instance in alignment with the schedule of the application run" is incorrect.

This solution involves significant manual intervention and managing EC2 instances. While it can work, it's not an optimized way, especially in terms of cost and operation overhead. It does not take advantage of the pay-per-use model and automatic scaling provided by AWS Lambda.

References:

https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-run-lambda-schedule.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/amazon-cloudwatch/

Domain

AWS Compute