AWS Certified Solutions Architect Associate Practice Test 6 - Results

Return to review
Chart
Pie chart with 4 slices.
End of interactive chart.
Attempt 1
All knowledge areas
All questions
Question 1:
Skipped
A customer is deploying services in a hybrid cloud model. The customer has mandated that data is transferred directly between cloud data centers, bypassing ISPs.

Which AWS service can be used to enable hybrid cloud connectivity?

- **AWS Direct Connect**

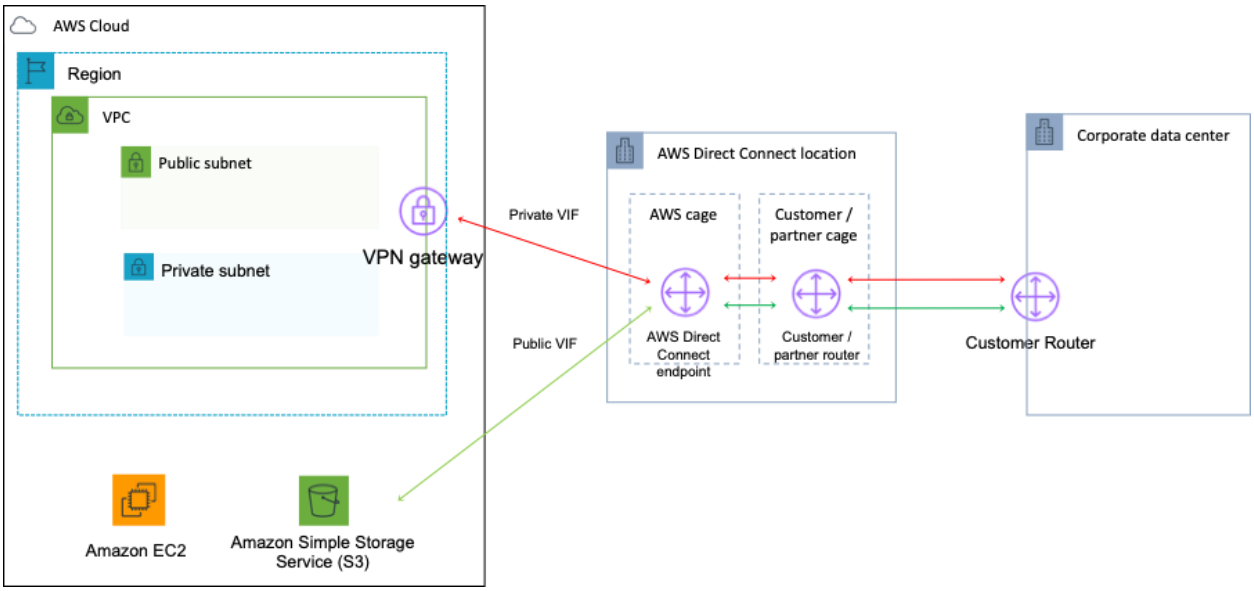
  (Correct)

- **IPSec VPN**

- **Amazon Route 53**

- **Amazon VPC**

Explanation
With AWS Direct Connect, you can connect to all your AWS resources in an AWS Region, transfer your business-critical data directly from your datacenter, office, or colocation environment into and from AWS, bypassing your Internet service provider and removing network congestion.



CORRECT: "AWS Direct Connect" is the correct answer.

INCORRECT: "Amazon VPC" is incorrect. Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined.

INCORRECT: "IPSec VPN" is incorrect. An IPSec VPN can be used to connect to AWS however it does not bypass the ISPs or Internet.

INCORRECT: "Amazon Route 53" is incorrect. Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service.

References:

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

Save time with our AWS cheat sheets:

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

Question 2:

Skipped

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 CodeDeploy**

- **AWS Config**
- **AWS OpsWorks**
- **Run Command**

  (Correct)

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/

Question 3:
Skipped

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)**
- **Cold HDD (sc1)**
- **Provisioned IOPS SSD (io1)**

  (Correct)
- **Throughput Optimized HDD (st1)**

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/

Question 4:

Skipped

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)

- ☐ **SSL**
- ☐ **HTTP**

  (Correct)
- ☐ **HTTPS**

  (Correct)
- ☐ **ICMP**
- ☐ **TCP**

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/

Question 5:

Skipped

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 Redis**

  (Correct)

- **Amazon ElastiCache Memcached**

- **Amazon DynamoDB**

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/

Question 6:

Skipped

A customer has requested some advice on how to implement security measures in their Amazon VPC. The client has recently been the victim of some hacking attempts. The client wants to implement measures to mitigate further threats. The client has explained that the attacks always come from the same small block of IP addresses.

What would be a quick and easy measure to help prevent further attacks?

- **Use CloudFront's DDoS prevention features**
- **Use a Security Group rule that denies connections from the block of IP addresses**
- **Use a Network ACL rule that denies connections from the block of IP addresses**

  (Correct)

Create a Bastion Host restrict all connections to the Bastion Host only

Explanation

With NACLs you can have permit and deny rules. Network ACLs contain a numbered list of rules that are evaluated in order from the lowest number until the explicit deny. Network ACLs have separate inbound and outbound rules and each rule can allow or deny traffic.

Security Group	Network ACL
Operates at the instance (interface) level	Operates at the subnet level
Supports allow rules only	Supports allow and deny rules
Stateful	Stateless
Evaluates all rules	Processes rules in order
Applies to an instance only if associated with a group	Automatically applies to all instances in the subnets its associated with

CORRECT: "Use a Network ACL rule that denies connections from the block of IP addresses" is the correct answer.

INCORRECT: "Use a Security Group rule that denies connections from the block of IP addresses" is incorrect. With Security Groups you can only assign permit rules, you cannot assign deny rules.

INCORRECT: "Use CloudFront's DDoS prevention features" is incorrect. CloudFront does have DDoS prevention features but we don't know that this is a DDoS style of attack and CloudFront can only help where the traffic is using the CloudFront service to access cached content.

INCORRECT: "Create a Bastion Host restrict all connections to the Bastion Host only" is incorrect. A bastion host is typically used for admin purposes, allowing access to a single endpoint in the AWS cloud for administration using SSH/RDP. From the bastion instance you then connect to other EC2 instances in your subnets. This is not used as a method of adding security to production systems and cannot stop traffic from hitting application ports.

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/

Question 7:

Skipped

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?

- **Write a Ruby script that checks the age of objects and deletes any that are more than 60 days old**
- **Use an S3 bucket policy that deletes objects that are more than 60 days old**
- **Use an S3 lifecycle policy with object expiration configured to automatically remove objects that are more than 60 days old**

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

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/

Question 8:

Skipped

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 DynamoDB 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 S3 and use Kinesis for processing the log files**

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

  (Correct)

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/

Question 9:
Skipped
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?

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

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

  (Correct)

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

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

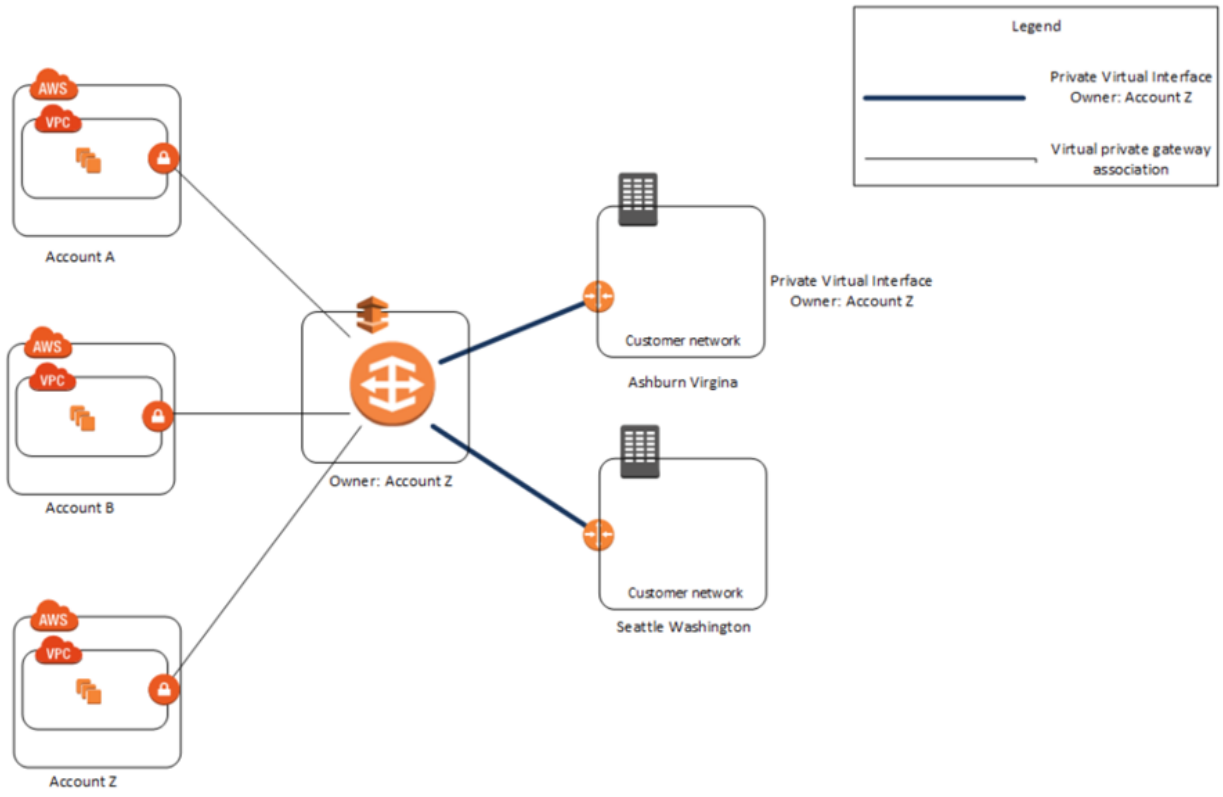
Explanation

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/

Question 10:

Skipped

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 become available for processing again after the visibility timeout expires**

  (Correct)

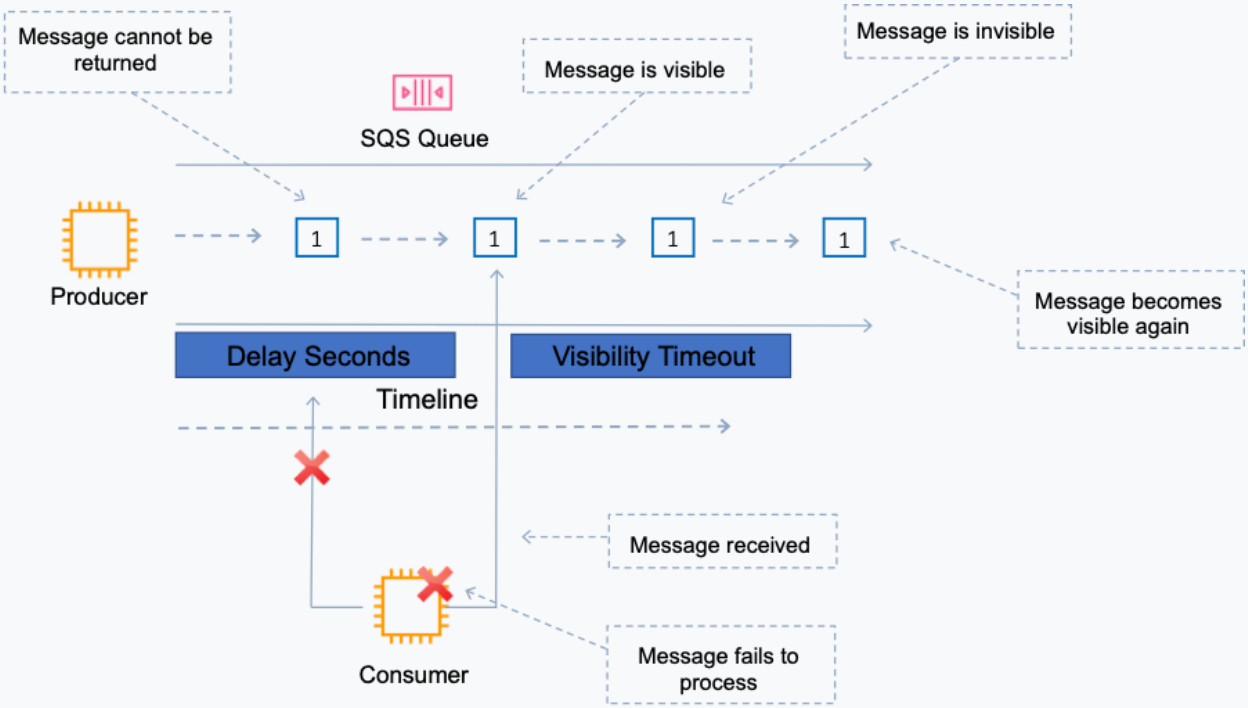
- **The message will remain in the queue and be immediately picked up by another instance**

- **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**

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/

Question 11:

Skipped

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 notifies you of increased/decreased load, and manually adjust the provisioned throughput**
- **Use DynamoDB DAX to increase the performance of the database**
- **Create a CloudWatch alarm that triggers an AWS Lambda function that adjusts the provisioned throughput**
- **Create a DynamoDB Auto Scaling scaling policy**

  (Correct)

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/

Question 12:

Skipped

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?

- **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**
- **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**

  (Correct)

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

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.

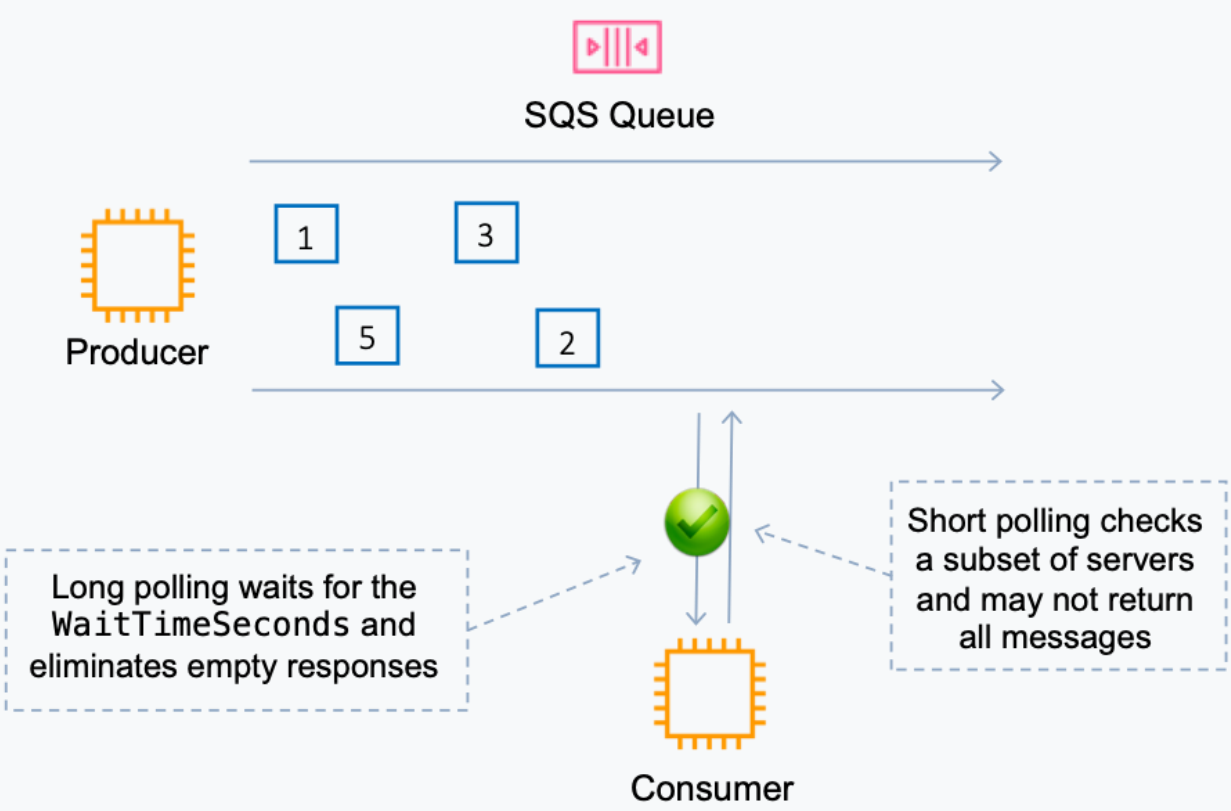
Short Polling:

– 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/

Question 13:

Skipped

An Amazon Elastic File System (EFS) has been created to store data that will be accessed by a large number of Amazon EC2 instances. The data is sensitive and a Solutions Architect is creating a design for security measures to protect the data. It is required that network traffic is restricted correctly based on firewall rules and access from hosts is restricted by user or group.

How can this be achieved with Amazon EFS? (choose 2)

- **Use Network ACLs to control the traffic**
- **Use POSIX permissions to control access from hosts by user or group**

  (Correct)
- **Use EFS Security Groups to control network traffic**

  (Correct)
- **Use AWS Web Application Firewall (WAF) to protect EFS**
- **Use IAM groups to control access by user or group**

Explanation

You can control who can administer your file system using IAM. You can control access to files and directories with POSIX-compliant user and group-level permissions. POSIX permissions allows you to restrict access from hosts by user and group. EFS Security Groups act as a firewall, and the rules you add define the traffic flow.

CORRECT: "Use POSIX permissions to control access from hosts by user or group" is the correct answer.

CORRECT: "Use EFS Security Groups to control network traffic" is the correct answer.

INCORRECT: "Use AWS Web Application Firewall (WAF) to protect EFS" is incorrect. You cannot use AWS WAF to protect EFS data using users and groups.

INCORRECT: "Use Network ACLs to control the traffic" is incorrect. You use EFS Security Groups to control network traffic to EFS, not Network ACLs.

INCORRECT: "Use IAM groups to control access by user or group" is incorrect. You do not use IAM to control access to files and directories by user and group, but you can use IAM to control who can administer the file system configuration.

References:

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

Save time with our AWS cheat sheets:

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

Question 14:

Skipped

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?

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

  (Correct)

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

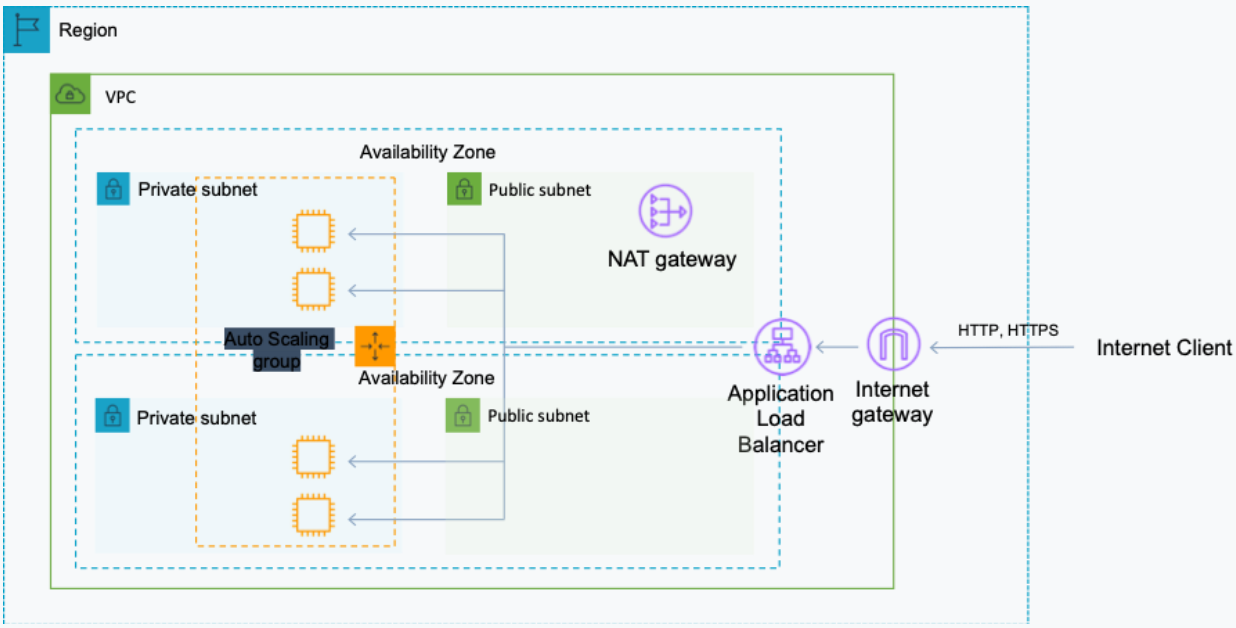
- **Launch the EC2 instances in a private subnet with a NAT gateway and update the route table**

-

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

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/

Question 15:

Skipped

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?

- **Backup and restore**
- **Pilot light**
- **Warm standby**
- **Multi-site**

  (Correct)

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/

Question 16:

Skipped

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)

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

  (Correct)

- ☐ **Provides 99.9% availability of archives**

- ☐ **Data is resilient in the event of one entire region destruction**

- ☐ **Data is replicated globally**

- ☐ **Provides 99.999999999% durability of archives**

  (Correct)

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/

Question 17:

Skipped

Some data has become corrupted in an Amazon RDS database. A Solutions Architect plans to use point-in-time restore to recover the data to the last known good configuration. Which of the following statements is correct about restoring an RDS database to a specific point-in-time? (choose 2)

- **You can restore up to the last 1 minute**
- **You can restore up to the last 5 minutes**

  (Correct)
-

The default DB security group is applied to the new DB instance

(Correct)

- ☐

Custom DB security groups are applied to the new DB instance

- ☐

The database restore overwrites the existing database

Explanation

You can restore a DB instance to a specific point in time, creating a new DB instance. When you restore a DB instance to a point in time, the default DB security group is applied to the new DB instance. If you need custom DB security groups applied to your DB instance, you must apply them explicitly using the AWS Management Console, the AWS CLI modify-db-instance command, or the Amazon RDS API ModifyDBInstance operation after the DB instance is available.

Restored DBs will always be a new RDS instance with a new DNS endpoint and you can restore up to the last 5 minutes.

CORRECT: "You can restore up to the last 5 minutes" is a correct answer.

CORRECT: "The default DB security group is applied to the new DB instance" is also a correct answer.

INCORRECT: "Custom DB security groups are applied to the new DB instance" is incorrect. Only default DB parameters and security groups are restored – you must manually associate all other DB parameters and SGs..

INCORRECT: "You can restore up to the last 1 minute" is incorrect. You can restore up to the last 5 minutes.

INCORRECT: "The database restore overwrites the existing database" is incorrect. You cannot restore from a DB snapshot to an existing DB – a new instance is created when you restore.

References:

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

Save time with our AWS cheat sheets:

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

Question 18:

Skipped

An Amazon EC2 instance has been launched into an Amazon VPC. A Solutions Architect needs to ensure that instances have both a private and public DNS hostnames. Assuming settings were not changed during creation of the VPC, how will DNS hostnames be assigned by default? (choose 2)

- ☐ **In all VPCs instances no DNS hostnames will be assigned**
- ☐ **In a default VPC instances will be assigned a public and private DNS hostname**

  (Correct)
- ☐ **In a default VPC instances will be assigned a private but not a public DNS hostname**
- ☐ **In a non-default VPC instances will be assigned a public and private DNS hostname**
- ☐ **In a non-default VPC instances will be assigned a private but not a public DNS hostname**

  (Correct)

Explanation

When you launch an instance into a default VPC, we provide the instance with public and private DNS hostnames that correspond to the public IPv4 and private IPv4 addresses for the instance.

When you launch an instance into a nondefault VPC, we provide the instance with a private DNS hostname and we might provide a public DNS hostname, depending on the DNS attributes you specify for the VPC and if your instance has a public IPv4 address.

All other statements are incorrect with default settings.

CORRECT: "In a default VPC instances will be assigned a public and private DNS hostname" is the correct answer.

CORRECT: "In a non-default VPC instances will be assigned a private but not a public DNS hostname" is the correct answer.

INCORRECT: "In all VPCs instances no DNS hostnames will be assigned" is incorrect as explained above.

INCORRECT: "In a non-default VPC instances will be assigned a public and private DNS hostname" is incorrect as explained above.

INCORRECT: "In a default VPC instances will be assigned a private but not a public DNS hostname" is incorrect as explained above.

References:

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

Save time with our AWS cheat sheets:

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

Question 19:

Skipped

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**
- **AWS Lambda functions**

  (Correct)
- **Amazon Elastic Beanstalk**
-

AWS Fargate tasks

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/

Question 20:

Skipped

A company has multiple Amazon VPCs that are peered with each other. The company would like to use a single Elastic Load Balancer (ELB) to route traffic to multiple EC2 instances in peered VPCs within the same region. How can this be achieved?

- **This is not possible with ELB, you would need to use Route 53**
- **This is possible using the Classic Load Balancer (CLB) if using Instance IDs**
-

This is possible using the Network Load Balancer (NLB) and Application Load Balancer (ALB) if using IP addresses as targets

(Correct)

- 

This is not possible, the instances that an ELB routes traffic to must be in the same VPC

Explanation

With ALB and NLB IP addresses can be used to register:

- Instances in a peered VPC.

- AWS resources that are addressable by IP address and port.

- On-premises resources linked to AWS through Direct Connect or a VPN connection.

CORRECT: "This is possible using the Network Load Balancer (NLB) and Application Load Balancer (ALB) if using IP addresses as targets" is the correct answer.

INCORRECT: "This is not possible, the instances that an ELB routes traffic to must be in the same VPC" is incorrect. Instances can be in peered VPCs.

INCORRECT: "This is possible using the Classic Load Balancer (CLB) if using Instance IDs" is incorrect. This is not possible with the CLB.

INCORRECT: "This is not possible with ELB, you would need to use Route 53" is incorrect. This is not true, as detailed above.

References:

https://aws.amazon.com/blogs/aws/new-application-load-balancing-via-ip-address-to-aws-on-premises-resources/

Save time with our AWS cheat sheets:

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

Question 21:

Skipped

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 Scheduled scaling policy**

  (Correct)

- **Use a Dynamic scaling policy**

- **Use a Simple scaling policy**

- **Use a Step scaling policy**

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/

Question 22:

Skipped

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 DynamoDB**

  (Correct)

- **Amazon RDS MySQL**

- **Amazon EBS**

- **Amazon EFS**

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/

Question 23:

Skipped

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**
- **EBS Provisioned IOPS SSD**
- **EBS Throughput Optimized HDD**

  (Correct)
- **EBS General Purpose SSD in a RAID 1 configuration**

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/

Question 24:

Skipped

An application is generating a large amount of clickstream events data that is being stored on S3. The business needs to understand customer behaviour and want to run complex analytics queries against the data.

Which AWS service can be used for this requirement?

- **Amazon Kinesis Firehose**
- **Amazon Neptune**
- **Amazon RedShift**

  (Correct)

Amazon RDS

Explanation

Amazon Redshift is a fast, fully managed data warehouse that makes it simple and cost-effective to analyze all your data using standard SQL and existing Business Intelligence (BI) tools.

RedShift is used for running complex analytic queries against petabytes of structured data, using sophisticated query optimization, columnar storage on high-performance local disks, and massively parallel query execution.

With RedShift you can load data from Amazon S3 and perform analytics queries. RedShift Spectrum can analyze data directly in Amazon S3, but was not presented as an option.

CORRECT: "Amazon RedShift" is the correct answer.

INCORRECT: "Amazon Neptune" is incorrect. Amazon Neptune is a new product that offers a fully-managed Graph database.

INCORRECT: "Amazon RDS" is incorrect. RDS is a relational database that is used for transactional workloads not analytics workloads.

INCORRECT: "Amazon Kinesis Firehose" is incorrect. Amazon Kinesis Firehose processes streaming data, not data stored on S3.

References:

https://aws.amazon.com/redshift/

Save time with our AWS cheat sheets:

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

Question 25:

Skipped

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)

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

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

(Correct)

- **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 inbound rule that allows all traffic from the security group itself**

(Correct)

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/

Question 26:

Skipped

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?

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

- **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**

  (Correct)

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

- **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**

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/

Question 27:

Skipped

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)

- ☐ **Use a larger instance size within the instance family**
- ☐ **Use EBS optimized instances**

  (Correct)
- ☐ **Use Provisioned IOPS (I01) EBS volumes**

  (Correct)
- ☐

Use HDD, Cold (SC1) EBS volumes

- ☐

Create a RAID 1 array from multiple EBS volumes

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/

Question 28:

Skipped

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?

- **General Purpose SSD (gp2)**
- **Cold HDD (sc1)**

  (Correct)
- **Provisioned IOPS SSD (io1)**
- **Throughput Optimized HDD (st1)**

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/

Question 29:

Skipped

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 traffic to the Internet Gateway**
- ☐ **There is a default outbound rule allowing all traffic**
- ☐ **There is a default outbound rule denying all traffic**

  (Correct)
- ☐ **There is a default inbound rule denying all traffic**

  (Correct)
- ☐ **There is a default inbound rule allowing traffic from the VPC CIDR block**

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/

Question 30:

Skipped

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 Elastic Beanstalk**

  (Correct)

- **AWS CloudFormation**

- **AWS CodeDeploy**

- **AWS OpsWorks**

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/

Question 31:

Skipped

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**
- **Add multiple Elastic IP addresses to the instance**
-

Use enhanced networking

(Correct)

-

Configure a RAID 1 array from multiple EBS volumes

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/

Question 32:

Skipped

A Solutions Architect created a new IAM user account for a temporary employee who recently joined the company. The user does not have permissions to perform any actions, which statement is true about newly created users in IAM?

- **They are created with no permissions**

  (Correct)

- **They are created with full permissions**

- **They are created with user privileges**

- **They are created with limited permissions**

Explanation

Every IAM user starts with no permissions.. In other words, by default, users can do nothing, not even view their own access keys. To give a user permission to do something, you can add the permission to the user (that is, attach a policy to the user). Or you can add the user to a group that has the intended permission.

CORRECT: "They are created with no permissions" is the correct answer.

INCORRECT: "They are created with limited permissions" is incorrect as they are created with no permissions.

INCORRECT: "They are created with full permissions" is incorrect as they are created with no permissions.

INCORRECT: "They are created with user privileges" is incorrect as they are created with no permissions.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_controlling.html

Save time with our AWS cheat sheets:

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

Question 33:

Skipped

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 a single PUT request to upload the large file**
- **Use Multipart Upload**

  (Correct)
- **Use AWS Import/Export**
- **Use Amazon Snowball**

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/

Question 34:

Skipped

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?

- **Enable Access Logs and store the data on S3**

  (Correct)

- **Use CloudTrail to capture all API calls made to the ALB**

- **Configure metrics in CloudWatch for the ALB**

- **Enable EC2 detailed monitoring**

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/

Question 35:

Skipped

A Solutions Architect is designing the system monitoring and deployment layers of a serverless application. The system monitoring layer will manage system visibility through recording logs and metrics and the deployment layer will deploy the application stack and manage workload changes through a release management process.

The Architect needs to select the most appropriate AWS services for these functions. Which services and frameworks should be used for the system monitoring and deployment layers? (choose 2)

- **Use AWS Lambda to package, test, and deploy the serverless application stack**
- **Use AWS CloudTrail for consolidating system and application logs and monitoring custom metrics**
- **Use AWS X-Ray to package, test, and deploy the serverless application stack**
- **Use Amazon CloudWatch for consolidating system and application logs and monitoring custom metrics**

  (Correct)
- **Use AWS SAM to package, test, and deploy the serverless application stack**

  (Correct)

Explanation
AWS Serverless Application Model (AWS SAM) is an extension of AWS CloudFormation that is used to package, test, and deploy serverless applications.

With Amazon CloudWatch, you can access system metrics on all the AWS services you use, consolidate system and application level logs, and create business key performance indicators (KPIs) as custom metrics for your specific needs.

CORRECT: "Use AWS SAM to package, test, and deploy the serverless application stack" is a correct answer.

CORRECT: "Use Amazon CloudWatch for consolidating system and application logs and monitoring custom metrics" is also a correct answer.

INCORRECT: "Use AWS CloudTrail for consolidating system and application logs and monitoring custom metrics" is incorrect as CloudTrail is used for auditing not performance monitoring.

INCORRECT: "Use AWS X-Ray to package, test, and deploy the serverless application stack" is incorrect. AWS X-Ray lets you analyze and debug serverless applications by providing distributed tracing and service maps to easily identify performance bottlenecks by visualizing a request end-to-end.

INCORRECT: "Use AWS Lambda to package, test, and deploy the serverless application stack" is incorrect. AWS Lambda is used for executing your code as functions, it is not used for packaging, testing and deployment. AWS Lambda is used with AWS SAM.

References:

https://docs.aws.amazon.com/lambda/latest/dg/serverless_app.html

Save time with our AWS cheat sheets:

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

Question 36:
Skipped
A Solutions Architect is deploying a production application that will use several Amazon EC2 instances and run constantly on an ongoing basis. The application cannot be interrupted or restarted. Which EC2 pricing model would be best for this workload?

- **Reserved instances**

(Correct)

- **Flexible instances**

- **On-demand instances**

- **Spot instances**

Explanation

In this scenario for a stable process that will run constantly on an ongoing basis RIs will be the most affordable solution.

RIs provide you with a significant discount (up to 75%) compared to On-Demand instance pricing. You have the flexibility to change families, OS types, and tenancies while benefitting from RI pricing when you use Convertible RIs.

CORRECT: "Reserved instances" is the correct answer.

INCORRECT: "On-demand instances" is incorrect. On-demand is useful for short term ad-hoc requirements for which the job cannot afford to be interrupted and are typically more expensive than Spot instances.

INCORRECT: "Spot instances" is incorrect. Spot is more suited to short term jobs that can afford to be interrupted and offer the lowest price of all options.

INCORRECT: "Flexible instances" is incorrect. There's no such thing as flexible instances.

References:

https://aws.amazon.com/ec2/pricing/reserved-instances/

Save time with our AWS cheat sheets:

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

Question 37:

Skipped

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?

- **On-Demand**

  (Correct)

- **Reserved**

- **Dedicated instances**

- **Spot**

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/

Question 38:

Skipped

A large multi-national client has requested a design for a multi-region database. The master database will be in the EU (Frankfurt) region and databases will be located in 4 other regions to service local read traffic. The database should be a managed service including the replication.

The solution should be cost-effective and secure. Which AWS service can deliver these requirements?

- **RDS with Multi-AZ**
- **EC2 instances with EBS replication**
- **ElastiCache with Redis and clustering mode enabled**
- **RDS with cross-region Read Replicas**

  (Correct)

Explanation

Amazon RDS Read replicas are used for read heavy databases and the replication is asynchronous. Read replicas are used for workload sharing and offloading. Read replicas can be in another region. This solution will enable better performance for users in the other AWS regions for database queries and is a managed service.

CORRECT: "RDS with cross-region Read Replicas" is the correct answer.

INCORRECT: "RDS with Multi-AZ" is incorrect. RDS with Multi-AZ is within a region only

INCORRECT: "EC2 instances with EBS replication" is incorrect. EC2 instances with EBS replication is not a suitable solution.

INCORRECT: "ElastiCache with Redis and clustering mode enabled" is incorrect. ElastiCache is an in-memory key/value store database (more OLAP than OLTP) and is not suitable for this scenario. Clustering mod is only available within the same region.

References:

https://aws.amazon.com/blogs/aws/cross-region-read-replicas-for-amazon-rds-for-mysql/

Save time with our AWS cheat sheets:

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

Question 39:

Skipped

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 Inbound rule that allows HTTP/HTTPS, and specify the source as 0.0.0.0/32**
- **Add an Outbound rule that allows HTTP/HTTPS, and specify the destination as the web server security group**

  (Correct)
- **Add an Outbound rule that allows HTTP/HTTPS, and specify the destination as VPC CIDR**
- **Add an Inbound rule that allows HTTP/HTTPS, and specify the source as 0.0.0.0/0**

  (Correct)

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

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/

Question 40:

Skipped

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**
- **Connection Draining**

  (Correct)
- **Sticky Sessions**
- **Deletion Protection**

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/

Question 41:

Skipped

An Auto Scaling group of Amazon EC2 instances behind an Elastic Load Balancer (ELB) is running in an Amazon VPC. Health checks are configured on the ASG to use EC2 status checks. The ELB has determined that an EC2 instance is unhealthy and has removed it from service. A Solutions Architect noticed that the instance is still running and has not been terminated by EC2 Auto Scaling.

What would be an explanation for this behavior?

- **The ASG is waiting for the cooldown timer to expire before terminating the instance**
- **The ELB health check type has not been selected for the ASG and so it is unaware that the instance has been determined to be unhealthy by the ELB and has been removed from service**

  (Correct)
- **The health check grace period has not yet expired**
- **Connection draining is enabled and the ASG is waiting for in-flight requests to complete**

Explanation

If using an ELB it is best to enable ELB health checks as otherwise EC2 status checks may show an instance as being healthy that the ELB has determined is unhealthy. In this case the instance will be removed from service by the ELB but will not be terminated by Auto Scaling

More information on ASG health checks:

- By default uses EC2 status checks.

- Can also use ELB health checks and custom health checks.

- ELB health checks are in addition to the EC2 status checks.

- If any health check returns an unhealthy status the instance will be terminated.

- With ELB an instance is marked as unhealthy if ELB reports it as OutOfService

- A healthy instance enters the InService state.

- If an instance is marked as unhealthy it will be scheduled for replacement.

- If connection draining is enabled, Auto Scaling waits for in-flight requests to complete or timeout before terminating instances.

- The health check grace period allows a period of time for a new instance to warm up before performing a health check (300 seconds by default).

CORRECT: "The ELB health check type has not been selected for the ASG and so it is unaware that the instance has been determined to be unhealthy by the ELB and has been removed from service" is the correct answer.

INCORRECT: "The ASG is waiting for the cooldown timer to expire before terminating the instance" is incorrect as the ASG does not wait for the cooldown time to expire.

INCORRECT: "Connection draining is enabled and the ASG is waiting for in-flight requests to complete" is incorrect. Connection draining is not the correct answer as the ELB has taken the instance out of service so there are no active connections.

INCORRECT: "The health check grace period has not yet expired" is incorrect. The health check grace period allows a period of time for a new instance to warm up before performing a health check.

References:

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

Save time with our AWS cheat sheets:

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

Question 42:

Skipped

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?

- 

Tags

-

Metadata

(Correct)

-

Parameters

-

User data

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/

Question 43:

Skipped

A financial services company regularly runs an analysis of the day's transaction costs, execution reporting, and market performance. The company currently uses third-party commercial software for provisioning, managing, monitoring, and scaling the computing jobs which utilize a large fleet of EC2 instances.

The company is seeking to reduce costs and utilize AWS services. Which AWS service could be used in place of the third-party software?

- **Amazon Lex**
- **AWS Batch**

  (Correct)
- **AWS Systems Manager**
- **Amazon Athena**

Explanation

AWS Batch eliminates the need to operate third-party commercial or open source batch processing solutions. There is no batch software or servers to install or manage. AWS Batch manages all the infrastructure for you, avoiding the complexities of provisioning, managing, monitoring, and scaling your batch computing jobs.

CORRECT: "AWS Batch" is the correct answer.

INCORRECT: "Amazon Athena" is incorrect. Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL.

INCORRECT: "AWS Systems Manager" is incorrect. AWS Systems Manager gives you visibility and control of your infrastructure on AWS.

INCORRECT: "Amazon Lex" is incorrect. Amazon Lex is a service for building conversational interfaces into any application using voice and text.

References:

https://aws.amazon.com/batch/

Question 44:

Skipped

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 weighted routing policy and configure the respective weights**

  (Correct)
- **Use a Network Load Balancer to distribute traffic based on Instance ID**
- **Use Route 53 with a simple routing policy**

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/

Question 45:

Skipped

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?

- **6 subnets**
- **1 subnet**
- **4 subnets**

  (Correct)
- **2 subnets**

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/

Question 46:

Skipped

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**
- **Change the EC2 instance to one with enhanced networking to reduce latency**
- **Create an Amazon SQS queue and decouple the long-running API calls**

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

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/

Question 47:

Skipped

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)

- **Snapshot**
- **Instance store volume**

  (Correct)
- **S3 bucket**
- **EBS volume**

(Correct)

- ☐

EFS volume

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/

Question 48:

Skipped

A distribution method is required for some static files. The requests will mainly be GET requests and a high volume of GETs is expected, often exceeding 2000 per second. The files are currently stored in an S3 bucket. According to AWS best practices, how can performance be optimized?

- ◌

Use ElastiCache to cache the content

- Use cross-region replication to spread the load across regions
- Use S3 Transfer Acceleration
- Integrate CloudFront with S3 to cache the content

  (Correct)

Explanation
Amazon S3 automatically scales to high request rates. For example, your application can achieve at least 3,500 PUT/POST/DELETE and 5,500 GET requests per second per prefix in a bucket. There are no limits to the number of prefixes in a bucket

If your workload is mainly sending GET requests, in addition to the preceding guidelines, you should consider using Amazon CloudFront for performance optimization. By integrating CloudFront with Amazon S3, you can distribute content to your users with low latency and a high data transfer rate.

CORRECT: "Integrate CloudFront with S3 to cache the content" is the correct answer.

INCORRECT: "Use cross-region replication to spread the load across regions" is incorrect. Cross-region replication creates a replica copy in another region but should not be used for spreading read requests across regions. There will be 2 S3 endpoints and CRR is not designed for 2 way sync so this would not work well.

INCORRECT: "Use ElastiCache to cache the content" is incorrect. CloudFront is a better fit for this use case than using ElastiCache.

INCORRECT: "Use S3 Transfer Acceleration" is incorrect. Transfer Acceleration is used to accelerate object **uploads** to S3 over long distances (latency).

References:

https://docs.aws.amazon.com/AmazonS3/latest/dev/request-rate-perf-considerations.html

Save time with our AWS cheat sheets:

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

Question 49:

Skipped

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?

- **AWS IoT Core**

  (Correct)

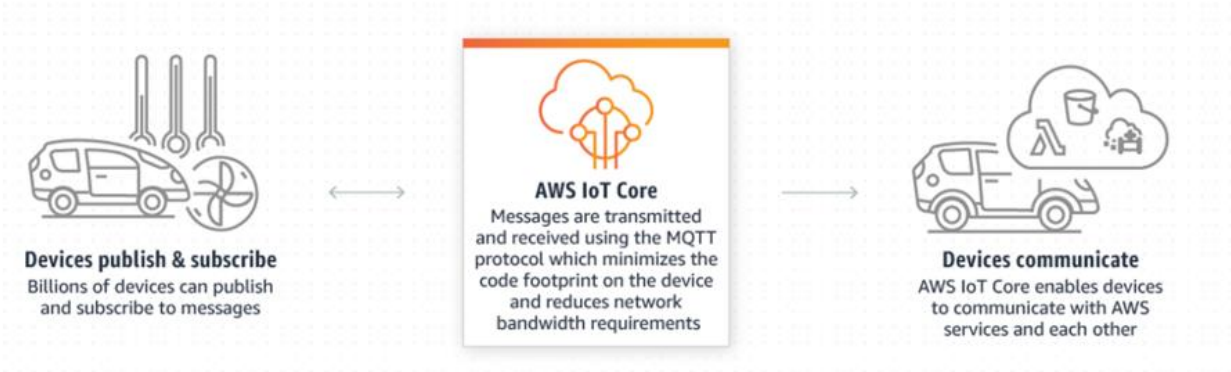
- **AWS Lambda**

- **AWS DMS**

- **AWS Glue**

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/

Question 50:

Skipped

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.)

- ☐ **Copy the snapshots using Amazon S3 cross-region replication**
- ☐ **Launch instances in the second Region from the AMIs**

  (Correct)
- ☐ **Create AMIs of the instances and copy them to another Region**

  (Correct)
- ☐ **Launch instances in the second Region using the S3 API**
- ☐ **Enable cross-region snapshots for the Amazon EC2 instances**

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/

Question 51:

Skipped

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? (choose 2)

- ☐

  All attached EBS volumes must share the same encryption state

- ☐

Not all EBS types support encryption

- **All instance types support encryption**

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

  (Correct)

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

  (Correct)

Explanation
All EBS types and all instance *families* support encryption but not all instance *types* support encryption. There is no direct way to change the encryption state of a volume. Data in transit between an instance and an encrypted volume is also encrypted.

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: "All instance types support encryption" is incorrect. All instance families support encryption, but not all 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/

Question 52:

Skipped

A company is investigating ways to analyze and process large amounts of data in the cloud faster, without needing to load or transform the data in a data warehouse. The data resides in Amazon S3.

Which AWS services would allow the company to query the data in place? (choose 2)

- **Amazon SWF**
- **Amazon RedShift Spectrum**

  (Correct)
- **Amazon Kinesis Data Streams**
- **Amazon Elasticsearch**
- **Amazon S3 Select**

  (Correct)

Explanation

Amazon S3 Select is designed to help analyze and process data within an object in Amazon S3 buckets, faster and cheaper. It works by providing the ability to retrieve a subset of data from an object in Amazon S3 using simple SQL expressions

Amazon Redshift Spectrum allows you to directly run SQL queries against exabytes of unstructured data in Amazon S3. No loading or transformation is required.

CORRECT: "Amazon S3 Select" is a correct answer.

CORRECT: "Amazon RedShift Spectrum" is also a correct answer.

INCORRECT: "Amazon Kinesis Data Streams" is incorrect. Amazon Kinesis Data Streams (KDS) is a massively scalable and durable real-time data streaming service. It does not allow you to perform query-in-place operations on S3.

INCORRECT: "Amazon Elasticsearch" is incorrect. Amazon Elasticsearch Service, is a fully managed service that makes it easy for you to deploy, secure, operate, and scale Elasticsearch to search, analyze, and visualize data in real-time.

INCORRECT: "Amazon SWF" is incorrect. Amazon SWF helps developers build, run, and scale background jobs that have parallel or sequential steps.

References:

https://aws.amazon.com/blogs/aws/s3-glacier-select/

https://aws.amazon.com/about-aws/whats-new/2017/11/amazon-redshift-spectrum-is-now-available-in-four-additional-aws-regions-and-enhances-query-performance-in-all-available-aws-regions/

Save time with our AWS cheat sheets:

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

Question 53:

Skipped

A fleet of Amazon EC2 instances running Linux will be launched in an Amazon VPC. An application development framework and some custom software must be installed on the instances. The installation will be initiated using some scripts. What feature enables a Solutions Architect to specify the scripts the software can be installed during the EC2 instance launch?

- **User data**

  (Correct)

- **Metadata**

- **Run command**

- **AWS Config**

Explanation

When you launch an instance in Amazon EC2, you have the option of passing user data to the instance that can be used to perform common automated configuration tasks and even run scripts after the instance starts. You can pass two types of user data to Amazon EC2: shell scripts and cloud-init directives

User data is data that is supplied by the user at instance launch in the form of a script and is limited to 16KB.

CORRECT: "User Data" is the correct answer.

INCORRECT: "Metadata" is incorrect. *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.

INCORRECT: "Run Command" is incorrect. The AWS Systems Manager run command is used to manage the configuration of existing instances by using remotely executed commands. User data is better for specifying scripts to run at startup.

INCORRECT: "AWS Config" is incorrect. This service is used to manage the configuration of AWS resources, it does not run scripts on instances.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/user-data.html

Save time with our AWS cheat sheets:

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

Question 54:

Skipped

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)

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

  (Correct)

- There is an outbound rule allowing traffic to the Internet Gateway
- There is an inbound rule allowing traffic from the Internet to port 22 for management
- There are is an inbound rule that allows traffic from the Internet Gateway
- There are no inbound rules and traffic will be implicitly denied

(Correct)

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/

Question 55:

Skipped

A company has a fleet of Amazon EC2 instances behind an Elastic Load Balancer (ELB) that are a mixture of c4.2xlarge instance types and c5.large instances. The load on the CPUs on the c5.large instances has been very high, often hitting 100% utilization, whereas the c4.2xlarge instances have been performing well.

What should a Solutions Architect recommend to resolve the performance issues?

- **Enable the weighted routing policy on the ELB and configure a higher weighting for the c4.2xlarge instances**
- **Change the configuration to use only c4.2xlarge instance types**

  (Correct)
- **Add all of the instances into a Placement Group**
- **Add more c5.large instances to spread the load more evenly**

Explanation

The 2xlarge instance type provides more CPUs. The best answer is to use this instance type for all instances as the CPU utilization has been lower.

CORRECT: "Change the configuration to use only c4.2xlarge instance types" is the correct answer.

INCORRECT: "Enable the weighted routing policy on the ELB and configure a higher weighting for the c4.2xlarge instances" is incorrect. The weighted routing policy is a Route 53 feature that would not assist in this situation.

INCORRECT: "Add all of the instances into a Placement Group" is incorrect. A placement group helps provide low-latency connectivity between instances and would not help here.

INCORRECT: "Add more c5.large instances to spread the load more evenly" is incorrect. This would not help as this instance type is underperforming with high CPU utilization rates.

References:

https://aws.amazon.com/ec2/instance-types/

Save time with our AWS cheat sheets:

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

Question 56:

Skipped

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.)

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

  (Correct)

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

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

(Correct)

- ☐

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

- ☐

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

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/

Question 57:

Skipped

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?

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

  (Correct)

- **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**

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/

Question 58:

Skipped

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?

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

  (Correct)

-

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

-

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

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/

Question 59:

Skipped

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?

- **In the VPN-only subnet route table, add a route that directs all Internet traffic to the virtual private gateway**
- **Configure a NAT Gateway and configure all traffic to be directed via the virtual private gateway**
- **In the public subnet route table, add a route for your remote network and specify the customer gateway as the target**
- **In the public subnet route table, add a route for your remote network and specify the virtual private gateway as the target**

  (Correct)

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/

Question 60:

Skipped

A government agency is using CloudFront for a web application that receives personally identifiable information (PII) from citizens.

What feature of CloudFront applies an extra level of encryption at CloudFront edge locations to ensure the PII data is secured end-to-end?

- **Field-level encryption**

  (Correct)

- **RTMP distribution**

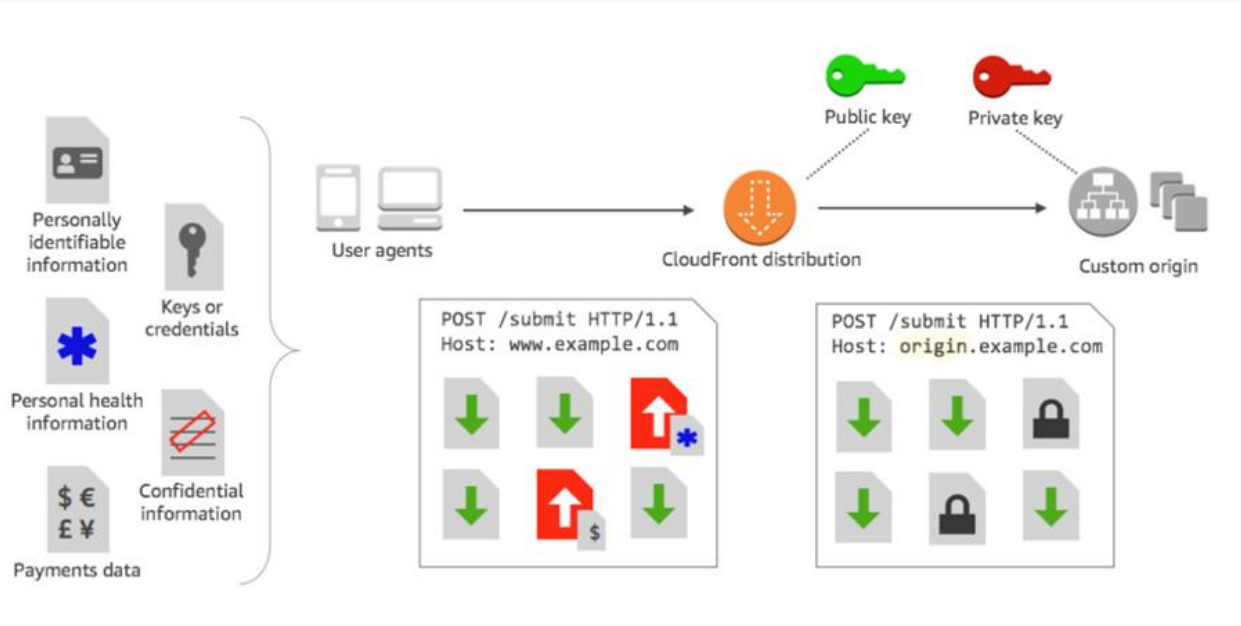
- **Origin access identity**

- **Object invalidation**

Explanation

With Amazon CloudFront, you can enforce secure end-to-end connections to origin servers by using HTTPS. Field-level encryption adds an additional layer of security that lets you protect specific data throughout system processing so that only certain applications can see it.

Field-level encryption allows you to enable your users to securely upload sensitive information to your web servers. The sensitive information provided by your users is encrypted at the edge, close to the user, and remains encrypted throughout your entire application stack. This encryption ensures that only applications that need the data—and have the credentials to decrypt it—are able to do so.



CORRECT: "Field-level encryption" is the correct answer.

INCORRECT: "Object invalidation" is incorrect. Object invalidation is a method to remove objects from the cache.

INCORRECT: "RTMP distribution" is incorrect. An RTMP distribution is a method of streaming media using Adobe Flash.

INCORRECT: "Origin access identity" is incorrect. Origin access identity applies to S3 bucket origins, not web servers.

References:

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html

Save time with our AWS cheat sheets:

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

Question 61:

Skipped

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?

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

  (Correct)

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

- **Use Amazon CloudWatch Logs to review detailed logging information**

- **Enable Amazon CloudTrail logging and configure packet capturing**

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/

Question 62:

Skipped

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?

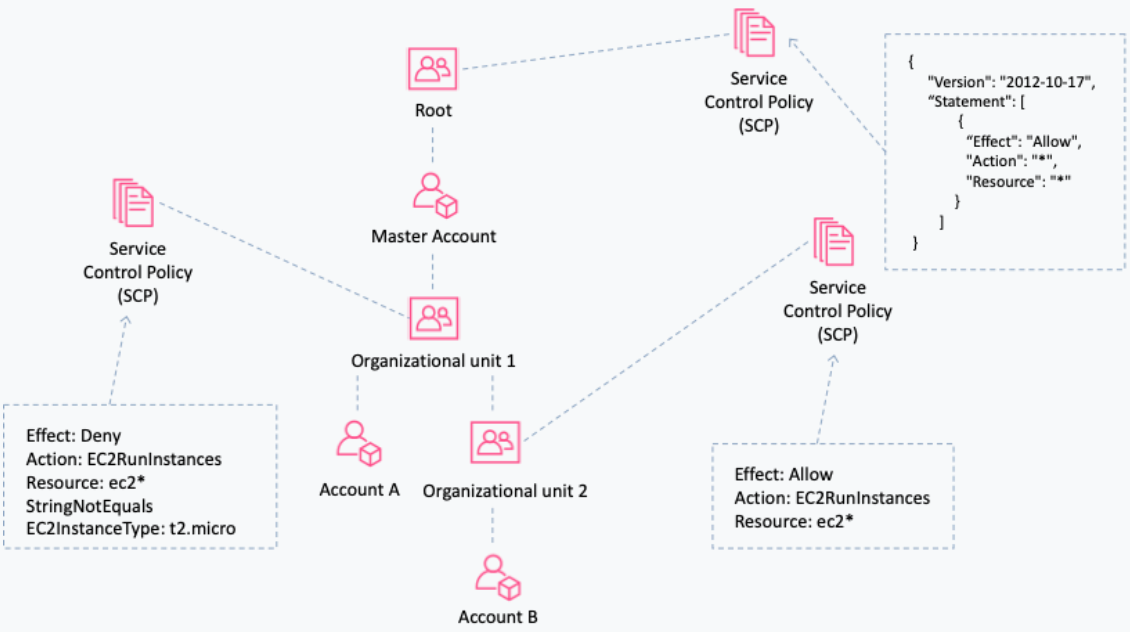
- **Create an IAM policy in the root account and attach it to users and groups in each account**
- **Create cross-account roles in each account to limit access to the services and actions that are allowed**
- **Create a service control policy in the root organizational unit to deny access to the services or actions**

  (Correct)
- **Create a Network ACL that limits access to the services or actions and attach it to all relevant subnets**

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/

Question 63:

Skipped

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?

- **Network Load Balancer**

  (Correct)

- **Route 53**

- **Classic Load Balancer**

- **Application Load Balancer**

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/

Question 64:

Skipped

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?

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

  (Correct)

- **Implement Amazon CloudFront and cache the content at Edge Locations**

- **Implement an Instance store volume on the media catalog server**

- **Update the application code to use an Amazon DynamoDB Accelerator cluster**

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/

Question 65:

Skipped

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?

- **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 an Amazon EC2 MySQL Multi-AZ deployment**

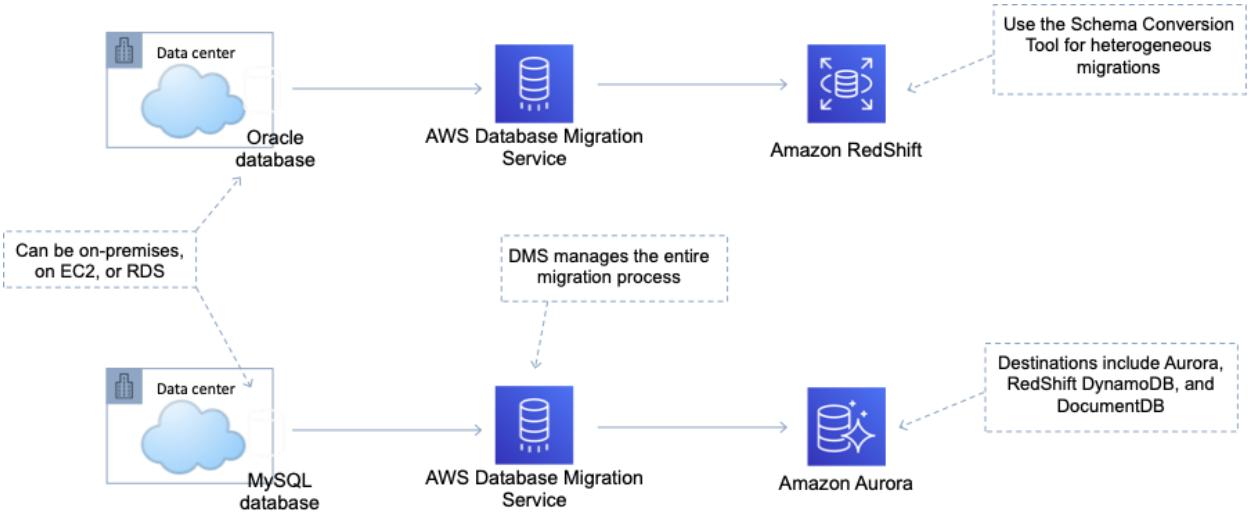
- **Use the AWS Database Migration Service (DMS) to directly migrate the database to an Amazon RDS MySQL Multi-AZ deployment**

  (Correct)

- **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**

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/