AWS Certified Solutions Architect Associate Practice Test 3 - 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 solutions architect is designing a microservices architecture. AWS Lambda will store data in an Amazon DynamoDB table named Orders. The solutions architect needs to apply an IAM policy to the Lambda function's execution role to allow it to put, update, and delete items in the Orders table. No other actions should be allowed.

Which of the following code snippets should be included in the IAM policy to fulfill this requirement whilst providing the LEAST privileged access?

- ```
  "Sid": "PutUpdateDeleteOnOrders",
  "Effect": "Allow",
  "Action": "dynamodb:* ",
  "Resource": "arn:aws:dynamodb:us-east-1:227392126428:table/Orders"
  ```
- ```
  "Sid": "PutUpdateDeleteOnOrders",
  "Effect": "Allow",
  "Action": [
  "dynamodb:PutItem",
  "dynamodb:UpdateItem",
  "dynamodb:DeleteItem"
  ],
  "Resource": "arn:aws:dynamodb:us-east-1:227392126428:table/Orders"
  ```

  (Correct)

- ```
  "Sid": "PutUpdateDeleteOnOrders",
  "Effect": "Allow",
  "Action": [
  "dynamodb:PutItem",
  "dynamodb:UpdateItem",
  "dynamodb:DeleteItem"
  ],
  "Resource": "arn:aws:dynamodb:us-east-1:227392126428:table/*"
  ```
-
  ```

```
"Sid": "PutUpdateDeleteOnOrders",
"Effect": "Deny",
"Action": "dynamodb:* ",
"Resource": "arn:aws:dynamodb:us-east-1:227392126428:table/Orders"
```

Explanation
The key requirements are to allow the Lambda function the put, update, and delete actions on a single table. Using the principle of least privilege the answer should not allow any other access.

CORRECT: The following answer is correct:

```
"Sid": "PutUpdateDeleteOnOrders",
"Effect": "Allow",
"Action": [
"dynamodb:PutItem",
"dynamodb:UpdateItem",
"dynamodb:DeleteItem"
],
"Resource": "arn:aws:dynamodb:us-east-1:227392126428:table/Orders"
```

This code snippet specifies the exact actions to allow and also specified the resource to apply those permissions to.

INCORRECT: the following answer is incorrect:

```
"Sid": "PutUpdateDeleteOnOrders",
"Effect": "Allow",
"Action": [
"dynamodb:PutItem",
"dynamodb:UpdateItem",
"dynamodb:DeleteItem"
],
"Resource": "arn:aws:dynamodb:us-east-1:227392126428:table/*"
```

This code snippet specifies the correct list of actions but it provides a wildcard “*” instead of specifying the exact resource. Therefore, the function will be able to put, update, and delete items on any table in the account.

INCORRECT: the following answer is incorrect:

```
"Sid": "PutUpdateDeleteOnOrders",
"Effect": "Allow",
"Action": "dynamodb:* ",
"Resource": "arn:aws:dynamodb:us-east-1:227392126428:table/Orders"
```

This code snippet allows any action on DynamoDB by using a wildcard “dynamodb:*”. This does not follow the principle of least privilege.

INCORRECT: the following answer is incorrect:

```
"Sid": "PutUpdateDeleteOnOrders",
"Effect": "Deny",
"Action": "dynamodb:* ",
"Resource": "arn:aws:dynamodb:us-east-1:227392126428:table/Orders"
```

This code snippet denies any action on the table. This does not have the desired effect.

References:

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

Save time with our AWS cheat sheets:

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

Question 2:

Skipped

A company has some statistical data stored in an Amazon RDS database. The company wants to allow users to access this information using an API. A solutions architect must create a solution that allows sporadic access to the data, ranging from no requests to large bursts of traffic.

Which solution should the solutions architect suggest?

- **Set up an Amazon API Gateway and use Amazon ECS**
- **Set up an Amazon API Gateway and use Amazon EC2 with Auto Scaling**
- **Set up an Amazon API Gateway and use AWS Lambda functions**

  (Correct)
- **Set up an Amazon API Gateway and use AWS Elastic Beanstalk**

Explanation

This question is simply asking you to work out the best compute service for the stated requirements. The key requirements are that the compute service should be suitable for a workload that can range quite broadly in demand from no requests to large bursts of traffic.

AWS Lambda is an ideal solution as you pay only when requests are made and it can easily scale to accommodate the large bursts in traffic. Lambda works well with both API Gateway and Amazon RDS.

CORRECT: "Set up an Amazon API Gateway and use AWS Lambda functions" is the correct answer.

INCORRECT: "Set up an Amazon API Gateway and use Amazon ECS" is incorrect as Lambda is a better fit for this use case as the traffic patterns are highly dynamic.

INCORRECT: "Set up an Amazon API Gateway and use AWS Elastic Beanstalk" is incorrect as Lambda is a better fit for this use case as the traffic patterns are highly dynamic.

INCORRECT: "Set up an Amazon API Gateway and use Amazon EC2 with Auto Scaling" is incorrect as Lambda is a better fit for this use case as the traffic patterns are highly dynamic.

References:

https://docs.aws.amazon.com/lambda/latest/dg/invocation-scaling.html

Save time with our AWS cheat sheets:

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

Question 3:

Skipped

An application runs on Amazon EC2 instances in a private subnet. The EC2 instances process data that is stored in an Amazon S3 bucket. The data is highly confidential and a private and secure connection is required between the EC2 instances and the S3 bucket.

Which solution meets these requirements?

- **Configure a custom SSL/TLS certificate on the S3 bucket.**
-

Set up an IAM policy to grant read-write access to the S3 bucket.

- **Configure encryption for the S3 bucket using an AWS KMS key.**

- **Set up S3 bucket policies to allow access from a VPC endpoint.**

  (Correct)

Explanation
A gateway VPC endpoint can be used to access an Amazon S3 bucket using private IP addresses. To further secure the solution an S3 bucket policy can be created that restricts access to the VPC endpoint so connections cannot be made to the bucket from other sources.

CORRECT: "Set up S3 bucket policies to allow access from a VPC endpoint" is the correct answer.

INCORRECT: "Set up an IAM policy to grant read-write access to the S3 bucket" is incorrect. This does not enable private access from EC2. A gateway VPC endpoint is required.

INCORRECT: "Configure encryption for the S3 bucket using an AWS KMS key" is incorrect. This will encrypt data at rest but does not secure the connection to the bucket or ensure private connections must be made.

INCORRECT: "Configure a custom SSL/TLS certificate on the S3 bucket" is incorrect. You cannot add a custom SSL/TLS certificate to Amazon S3.

References:

https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-bucket-policies-vpc-endpoint.html

Save time with our AWS cheat sheets:

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

Question 4:
Skipped
An application consists of a web tier in a public subnet and a MySQL cluster hosted on Amazon EC2 instances in a private subnet. The MySQL instances must retrieve product

data from a third-party provider over the internet. A Solutions Architect must determine a strategy to enable this access with maximum security and minimum operational overhead.

What should the Solutions Architect do to meet these requirements?

- **Deploy a NAT gateway in the public subnet. Modify the route table in the private subnet to direct all internet traffic to the NAT gateway.**

  (Correct)

- **Create an internet gateway and attach it to the VPC. Modify the private subnet route table to direct internet traffic to the internet gateway.**

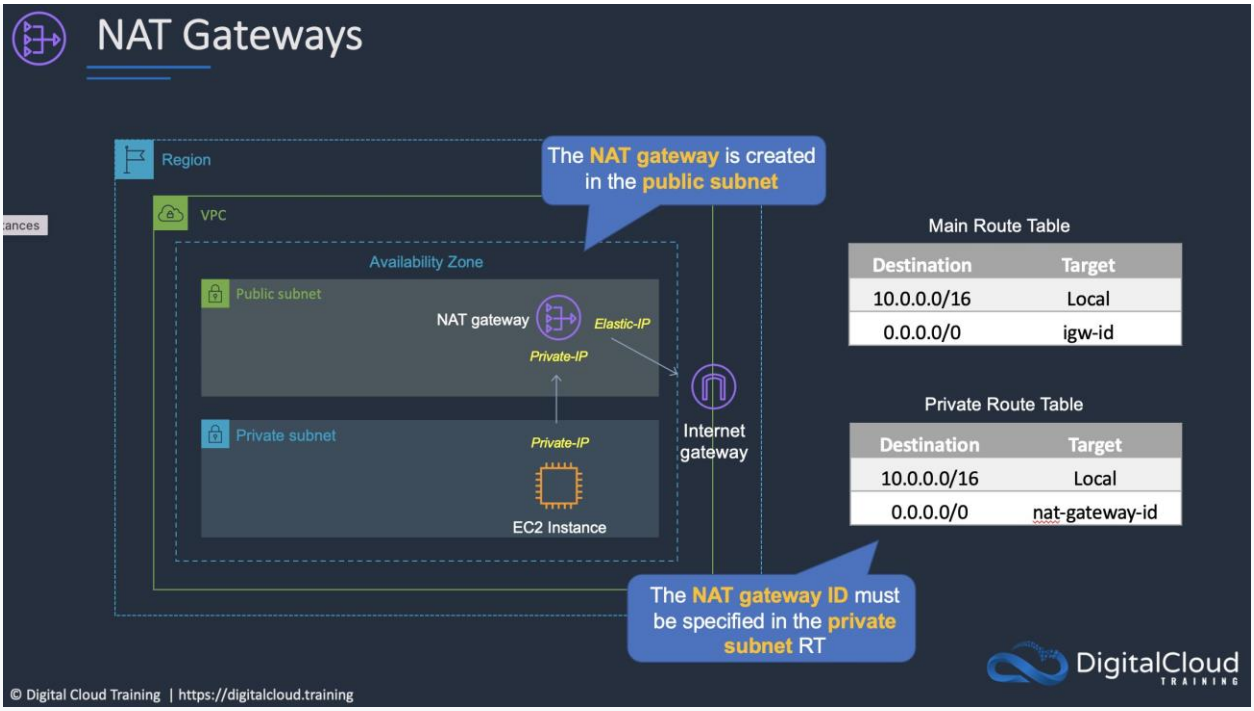
- **Deploy a NAT instance in the private subnet. Direct all internet traffic to the NAT instance.**

- **Create a virtual private gateway and attach it to the VPC. Modify the private subnet route table to direct internet traffic to the virtual private gateway.**

Explanation

The MySQL clusters instances need to access a service on the internet. The most secure method of enabling this access with low operational overhead is to create a NAT gateway. When deploying a NAT gateway, the gateway itself should be deployed in a public subnet whilst the route table in the private subnet must be updated to point traffic to the NAT gateway ID.

The configuration can be seen in the diagram below:



CORRECT: "Deploy a NAT gateway in the public subnet. Modify the route table in the private subnet to direct all internet traffic to the NAT gateway" is the correct answer.

INCORRECT: "Deploy a NAT instance in the private subnet. Direct all internet traffic to the NAT instance" is incorrect. NAT instances require more operational overhead and need to be deployed in a public subnet.

INCORRECT: "Create an internet gateway and attach it to the VPC. Modify the private subnet route table to direct internet traffic to the internet gateway" is incorrect. You cannot point the instances in the private subnet to an internet gateway as they do not have public IP addresses which is required to use an internet gateway.

INCORRECT: "Create a virtual private gateway and attach it to the VPC. Modify the private subnet route table to direct internet traffic to the virtual private gateway" is incorrect. A virtual private gateway (VGW) is used with a VPN connection, not for connecting instances in private subnets to the internet.

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 5:

Skipped

A Solutions Architect needs a solution for hosting a website that will be used by a development team. The website contents will consist of HTML, CSS, client-side JavaScript, and images.

Which solution is MOST cost-effective?

- **Use a Docker container to host the website on AWS Fargate.**
- **Create an Application Load Balancer with an AWS Lambda target.**
- **Create an Amazon S3 bucket and host the website there.**

  (Correct)
- **Launch an Amazon EC2 instance and host the website there.**

Explanation

Amazon S3 can be used for hosting static websites and cannot be used for dynamic content. In this case the content is purely static with client-side code running. Therefore, an S3 static website will be the most cost-effective solution for hosting this website.

CORRECT: "Create an Amazon S3 bucket and host the website there" is the correct answer.

INCORRECT: "Launch an Amazon EC2 instance and host the website there" is incorrect. This will be more expensive as it uses an EC2 instances.

INCORRECT: "Use a Docker container to host the website on AWS Fargate" is incorrect. A static website on S3 is sufficient for this use case and will be more cost-effective than Fargate.

INCORRECT: "Create an Application Load Balancer with an AWS Lambda target" is incorrect. This is also a more expensive solution and unnecessary for this use case.

References:

https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteHosting.html

Save time with our AWS cheat sheets:

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

Question 6:

Skipped

A company is planning to use Amazon S3 to store documents uploaded by its customers. The images must be encrypted at rest in Amazon S3. The company does not want to spend time managing and rotating the keys, but it does want to control who can access those keys.

What should a solutions architect use to accomplish this?

- **Server-Side Encryption with Customer-Provided Keys (SSE-C)**
- **Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)**
- **Server-Side Encryption with keys stored in an S3 bucket**
- **Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)**

  (Correct)

Explanation

SSE-KMS requires that AWS manage the data key but you manage the customer master key (CMK) in AWS KMS. You can choose a customer managed CMK or the AWS managed CMK for Amazon S3 in your account.

Customer managed CMKs are CMKs in your AWS account that you create, own, and manage. You have full control over these CMKs, including establishing and maintaining their key policies, IAM policies, and grants, enabling and disabling them, rotating their cryptographic material, adding tags, creating aliases that refer to the CMK, and scheduling the CMKs for deletion.

For this scenario, the solutions architect should use SSE-KMS with a customer managed CMK. That way KMS will manage the data key but the company can configure key policies defining who can access the keys.

CORRECT: "Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)" is the correct answer.

INCORRECT: "Server-Side Encryption with keys stored in an S3 bucket" is incorrect as you cannot store your keys in a bucket with server-side encryption

INCORRECT: "Server-Side Encryption with Customer-Provided Keys (SSE-C)" is incorrect as the company does not want to manage the keys.

INCORRECT: "Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)" is incorrect as the company needs to manage access control for the keys which is not possible when they're managed by Amazon.

References:

https://docs.aws.amazon.com/kms/latest/developerguide/services-s3.html#sse

https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master_keys

Save time with our AWS cheat sheets:

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

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

Question 7:

Skipped

A company copies 250 TB of data from a recent land survey onto multiple AWS Snowball Edge Storage Optimized devices. The company has a high-performance computing (HPC) cluster that is hosted within AWS to look for items of archaeological interest. A solutions architect must provide the cluster with consistent low latency and high-throughput access to the data which is hosted on the Snowball Edge Storage Optimized devices. The company is sending the devices back to AWS.

Which solution will meet these requirements?

- **Set up an Amazon Elastic File System (Amazon EFS) file system and an Amazon S3 bucket. Upload the data to the S3 bucket. Using the EFS file system, copy the**

data from the S3 bucket and access the EFS file system from the HPC cluster instances.

- **Create an Amazon FSx for Lustre file system and import the data directly into the FSx for Lustre file system and access the FSx for Lustre file system from the HPC cluster instances.**

- **Set up an Amazon S3 bucket. Configure an Amazon FSx for Lustre file system and integrate it with the S3 bucket after importing the data then access the FSx for Lustre file system from the HPC cluster instances.**

  (Correct)

- **Create a bucket in Amazon S3 and import the data into the S3 bucket. Set up an AWS Storage Gateway file gateway to use the S3 bucket and access the file gateway from the HPC cluster instances.**

Explanation

Using an Amazon FSX for Lustre file system is ideal as it is designed for High Performance Compute workloads. The native connection between Snowball and Amazon S3 ensures this solution meets the stated requirements.

CORRECT: "Set up an Amazon S3 bucket. Configure an Amazon FSx for Lustre file system and integrate it with the S3 bucket after importing the data then access the FSx for Lustre file system from the HPC cluster instances" is the correct answer (as explained above.)

INCORRECT: "Create a bucket in Amazon S3 and import the data into the S3 bucket. Set up an AWS Storage Gateway file gateway to use the S3 bucket and access the file gateway from the HPC cluster instances" is incorrect. AWS Storage Gateway File Gateway is not designed to allow extremely low latency file systems. It is a hybrid cloud storage service not designed for this application.

INCORRECT: "Set up an Amazon Elastic File System (Amazon EFS) file system and an Amazon S3 bucket. Upload the data to the S3 bucket. Using the EFS file system, copy the data from the S3 bucket and access the EFS file system from the HPC cluster instances" is incorrect. Although this would work, a standard EFS File System would not provide enough performance to fit the applications requirements.

INCORRECT: "Create an Amazon FSx for Lustre file system and import the data directly into the FSx for Lustre file system and access the FSx for Lustre file system from the HPC cluster instances" is incorrect. You cannot access the FSx for Lustre file system from the HPC cluster instances and this is only possible via S3.

References:

https://aws.amazon.com/fsx/lustre/

Save time with our AWS cheat sheets:

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

Question 8:

Skipped

A company is planning to migrate a large quantity of important data to Amazon S3. The data will be uploaded to a versioning enabled bucket in the us-west-1 Region. The solution needs to include replication of the data to another Region for disaster recovery purposes.

How should a solutions architect configure the replication?

- **Create an additional S3 bucket in another Region and configure cross-Region replication**
- **Create an additional S3 bucket with versioning in another Region and configure cross-Region replication**

  (Correct)
- **Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS)**
- **Create an additional S3 bucket with versioning in another Region and configure cross-origin resource sharing (CORS)**

Explanation

Replication enables automatic, asynchronous copying of objects across Amazon S3 buckets. Buckets that are configured for object replication can be owned by the same AWS account or by different accounts. You can copy objects between different AWS Regions or within the same Region. Both source and destination buckets must have versioning enabled.

CORRECT: "Create an additional S3 bucket with versioning in another Region and configure cross-Region replication" is the correct answer.

INCORRECT: "Create an additional S3 bucket in another Region and configure cross-Region replication" is incorrect as the destination bucket must also have versioning enabled.

INCORRECT: "Create an additional S3 bucket in another Region and configure cross-origin resource sharing (CORS)" is incorrect as CORS is not related to replication.

INCORRECT: "Create an additional S3 bucket with versioning in another Region and configure cross-origin resource sharing (CORS)" is incorrect as CORS is not related to replication.

References:

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

Save time with our AWS cheat sheets:

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

Question 9:

Skipped

An application runs on Amazon EC2 Linux instances. The application generates log files which are written using standard API calls. A storage solution is required that can be used to store the files indefinitely and must allow concurrent access to all files.

Which storage service meets these requirements and is the MOST cost-effective?

- **Amazon S3**

  (Correct)

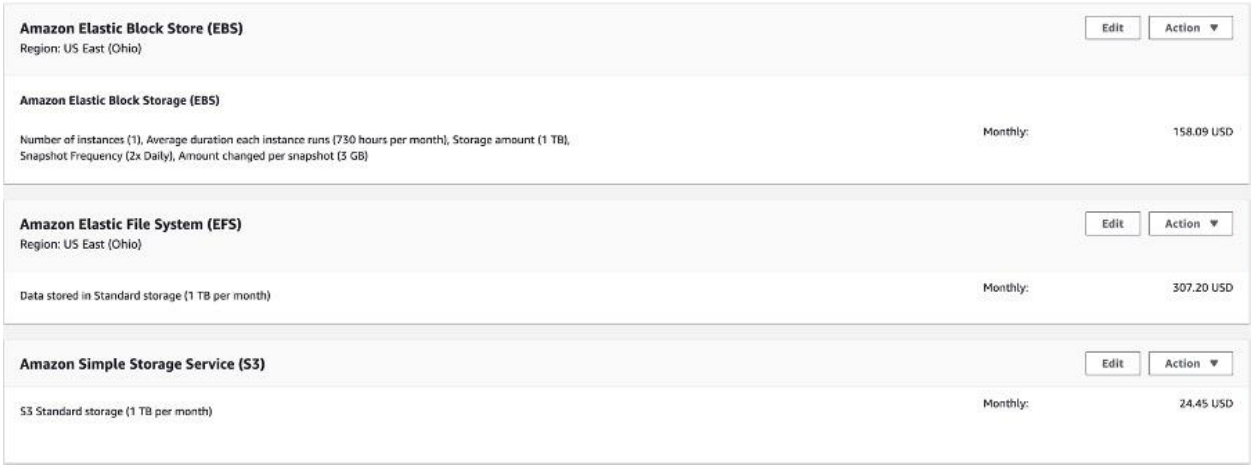
- **Amazon EBS**

- **Amazon EC2 instance store**
- **Amazon EFS**

Explanation

The application is writing the files using API calls which means it will be compatible with Amazon S3 which uses a REST API. S3 is a massively scalable key-based object store that is well-suited to allowing concurrent access to the files from many instances.

Amazon S3 will also be the most cost-effective choice. A rough calculation using the AWS pricing calculator shows the cost differences between 1TB of storage on EBS, EFS, and S3 Standard.



CORRECT: "Amazon S3" is the correct answer.

INCORRECT: "Amazon EFS" is incorrect as though this does offer concurrent access from many EC2 Linux instances, it is not the most cost-effective solution.

INCORRECT: "Amazon EBS" is incorrect. The Elastic Block Store (EBS) is not a good solution for concurrent access from many EC2 instances and is not the most cost-effective option either. EBS volumes are mounted to a single instance except when using multi-attach which is a new feature and has several constraints.

INCORRECT: "Amazon EC2 instance store" is incorrect as this is an ephemeral storage solution which means the data is lost when powered down. Therefore, this is not an option for long-term data storage.

References:

https://docs.aws.amazon.com/AmazonS3/latest/dev/optimizing-performance.html

Save time with our AWS cheat sheets:

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

Question 10:

Skipped

A Financial Services company currently stores data in Amazon S3. Each bucket contains items which have different access patterns. The Chief Financial officer of the organization wants to reduce costs, as they have noticed a sharp increase in their S3 bill. The Chief Financial Officer wants to reduce the S3 spend as quickly as possible.

What is the quickest way to reduce the S3 spend with the LEAST operational overhead?

- **Create a Lambda function to scan your S3 buckets, check which objects are stored in the appropriate buckets, and move them there.**
- **Place all objects in S3 Glacier Instant Retrieval.**
- **Transition the objects to the appropriate storage class by using an S3 Lifecycle configuration.**

  (Correct)
- **Automate the move of your S3 objects to the best storage class with AWS Trusted Advisor.**

Explanation

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 – These 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 creating them, or archive objects to the S3 Glacier Flexible Retrieval storage class one year after creating them. For more information, see Using Amazon S3 storage classes.

● Expiration actions – These actions define when objects expire. Amazon S3 deletes expired objects on your behalf.

CORRECT: "Transition the objects to the appropriate storage class by using an S3 Lifecycle configuration" is the correct answer (as explained above.)

INCORRECT: "Automate the move of your S3 objects to the best storage class with AWS Trusted Advisor" is incorrect. Trusted Advisor does not automatically transfer objects into the most appropriate buckets. You can use Trusted Advisor to review cost optimization options, and check for public access to your buckets but you cannot automatically transition objects.

INCORRECT: "Create a Lambda function to scan your S3 buckets, check which objects are stored in the appropriate buckets, and move them there" is incorrect. You could perhaps build a Lambda function to do this, however the easiest way to do this would be to use an S3 Lifecycle configuration.

INCORRECT: "Place all objects in S3 Glacier Instant Retrieval" is incorrect. It states in the question that each bucket contains items which have different access patterns, therefore S3 Glacier is not a suitable use case.

References:

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

Save time with our AWS cheat sheets:

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

Question 11:

Skipped

A high-performance file system is required for a financial modelling application. The data set will be stored on Amazon S3 and the storage solution must have seamless integration so objects can be accessed as files.

Which storage solution should be used?

- **Amazon Elastic Block Store (EBS)**
- **Amazon FSx for Lustre**

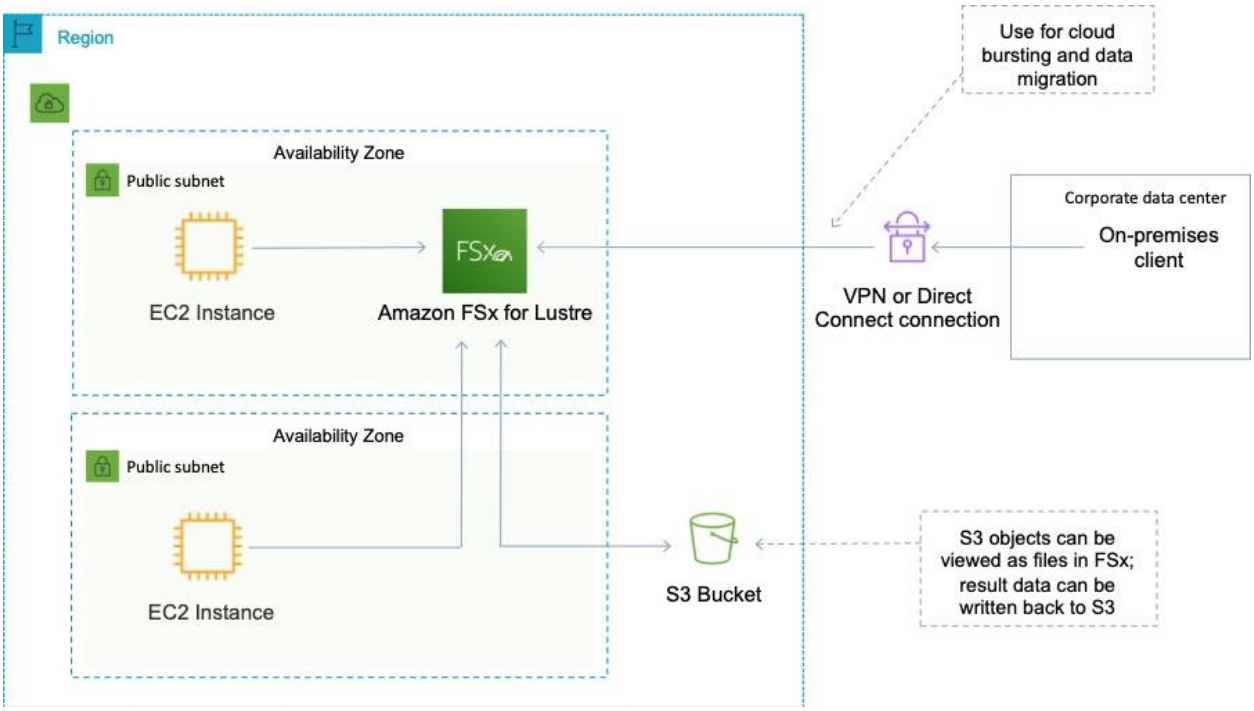
(Correct)

- **Amazon FSx for Windows File Server**

- **Amazon Elastic File System (EFS)**

Explanation

Amazon FSx for Lustre provides a high-performance file system optimized for fast processing of workloads such as machine learning, high performance computing (HPC), video processing, financial modeling, and electronic design automation (EDA). Amazon FSx works natively with Amazon S3, letting you transparently access your S3 objects as files on Amazon FSx to run analyses for hours to months.



CORRECT: "Amazon FSx for Lustre" is the correct answer.

INCORRECT: "Amazon FSx for Windows File Server" is incorrect. Amazon FSx for Windows File Server provides a fully managed native Microsoft Windows file system so you can easily move your Windows-based applications that require shared file storage to AWS. This solution integrates with Windows file shares, not with Amazon S3.

INCORRECT: "Amazon Elastic File System (EFS)" is incorrect. EFS and EBS are not good use cases for this solution. Neither storage solution is capable of presenting Amazon S3 objects as files to the application.

INCORRECT: "Amazon Elastic Block Store (EBS)" is incorrect. EFS and EBS are not good use cases for this solution. Neither storage solution is capable of presenting Amazon S3 objects as files to the application.

References:

https://aws.amazon.com/fsx/

Save time with our AWS cheat sheets:

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

Question 12:

Skipped

A company has a Production VPC and a Pre-Production VPC. The Production VPC uses VPNs through a customer gateway to connect to a single device in an on-premises data center. The Pre-Production VPC uses a virtual private gateway attached to two AWS Direct Connect (DX) connections. Both VPCs are connected using a single VPC peering connection.

How can a Solutions Architect improve this architecture to remove any single point of failure?

- **Add additional VPNs to the Production VPC from a second customer gateway device.**

  (Correct)

- **Add a set of VPNs between the Production and Pre-Production VPCs.**

- **Add an additional VPC peering connection between the two VPCs.**

- **Add a second virtual private gateway and attach it to the Production VPC.**

Explanation
The only single point of failure in this architecture is the customer gateway device in the on-premises data center. A customer gateway device is the on-premises (client) side of the connection into the VPC. The customer gateway configuration is created within AWS, but the actual device is a physical or virtual device running in the on-premises data center. If this device is a single device, then if it fails the VPN connections will fail. The AWS side of the VPN link is the virtual private gateway, and this is a redundant device.

CORRECT: "Add additional VPNs to the Production VPC from a second customer gateway device" is the correct answer.

INCORRECT: "Add an additional VPC peering connection between the two VPCs" is incorrect. VPC peering connections are already redundant, you do not need multiple connections.

INCORRECT: "Add a set of VPNs between the Production and Pre-Production VPCs" is incorrect. You cannot create VPN connections between VPCs (using AWS VPNs).

INCORRECT: "Add a second virtual private gateway and attach it to the Production VPC" is incorrect. Virtual private gateways (VGWs) are redundant devices so a second one is not necessary.

References:

https://docs.aws.amazon.com/vpn/latest/s2svpn/your-cgw.html

Save time with our AWS cheat sheets:

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

Question 13:
Skipped
A Solutions Architect is designing an application that will run on Amazon EC2 instances. The application will use Amazon S3 for storing image files and an Amazon DynamoDB table for storing customer information. The security team require that traffic between the EC2 instances and AWS services must not traverse the public internet.

How can the Solutions Architect meet the security team's requirements?

- **Create a NAT gateway in a public subnet and configure route tables.**

Create gateway VPC endpoints for Amazon S3 and DynamoDB.

(Correct)

- **Create a virtual private gateway and configure VPC route tables.**

- **Create interface VPC endpoints for Amazon S3 and DynamoDB.**

Explanation

A VPC endpoint enables private connections between your VPC and supported AWS services and VPC endpoint services powered by AWS PrivateLink. A gateway endpoint is used for Amazon S3 and Amazon DynamoDB. You specify a gateway endpoint as a route table target for traffic that is destined for the supported AWS services.

CORRECT: "Create gateway VPC endpoints for Amazon S3 and DynamoDB" is the correct answer.

INCORRECT: "Create a NAT gateway in a public subnet and configure route tables" is incorrect. A NAT gateway is used for enabling internet connectivity for instances in private subnets. Connections will traverse the internet.

INCORRECT: "Create interface VPC endpoints for Amazon S3 and DynamoDB" is incorrect. You should use a gateway VPC endpoint for S3 and DynamoDB.

INCORRECT: "Create a virtual private gateway and configure VPC route tables" is incorrect VGWs are used for VPN connections, they do not allow access to AWS services from a VPC.

References:

https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints.html

Save time with our AWS cheat sheets:

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

Question 14:

Skipped

An application generates unique files that are returned to customers after they submit requests to the application. The application uses an Amazon CloudFront distribution for sending the files to customers. The company wishes to reduce data transfer costs without modifying the application.

How can this be accomplished?

- **Use AWS Global Accelerator to reduce application latency for customers.**
- **Use Lambda@Edge to compress the files as they are sent to users.**

  (Correct)
- **Enable caching on the CloudFront distribution to store generated files at the edge.**
- **Enable Amazon S3 Transfer Acceleration to reduce the transfer times.**

Explanation

Lambda@Edge is a feature of Amazon CloudFront that lets you run code closer to users of your application, which improves performance and reduces latency. Lambda@Edge runs code in response to events generated by the Amazon CloudFront.

You simply upload your code to AWS Lambda, and it takes care of everything required to run and scale your code with high availability at an AWS location closest to your end user.

In this case Lambda@Edge can compress the files before they are sent to users which will reduce data egress costs.

CORRECT: "Use Lambda@Edge to compress the files as they are sent to users" is the correct answer.

INCORRECT: "Enable caching on the CloudFront distribution to store generated files at the edge" is incorrect. The files are unique to each customer request, so caching does not help.

INCORRECT: "Use AWS Global Accelerator to reduce application latency for customers" is incorrect. The aim is to reduce cost not latency and AWS GA uses the same network as CloudFront so does not assist with latency anyway.

INCORRECT: "Enable Amazon S3 Transfer Acceleration to reduce the transfer times" is incorrect. This does not lower costs.

References:

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

Save time with our AWS cheat sheets:

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

Question 15:

Skipped

A company is deploying a solution for sharing media files around the world using Amazon CloudFront with an Amazon S3 origin configured as a static website. The company requires that all traffic for the website must be inspected by AWS WAF.

Which solution meets these requirements?

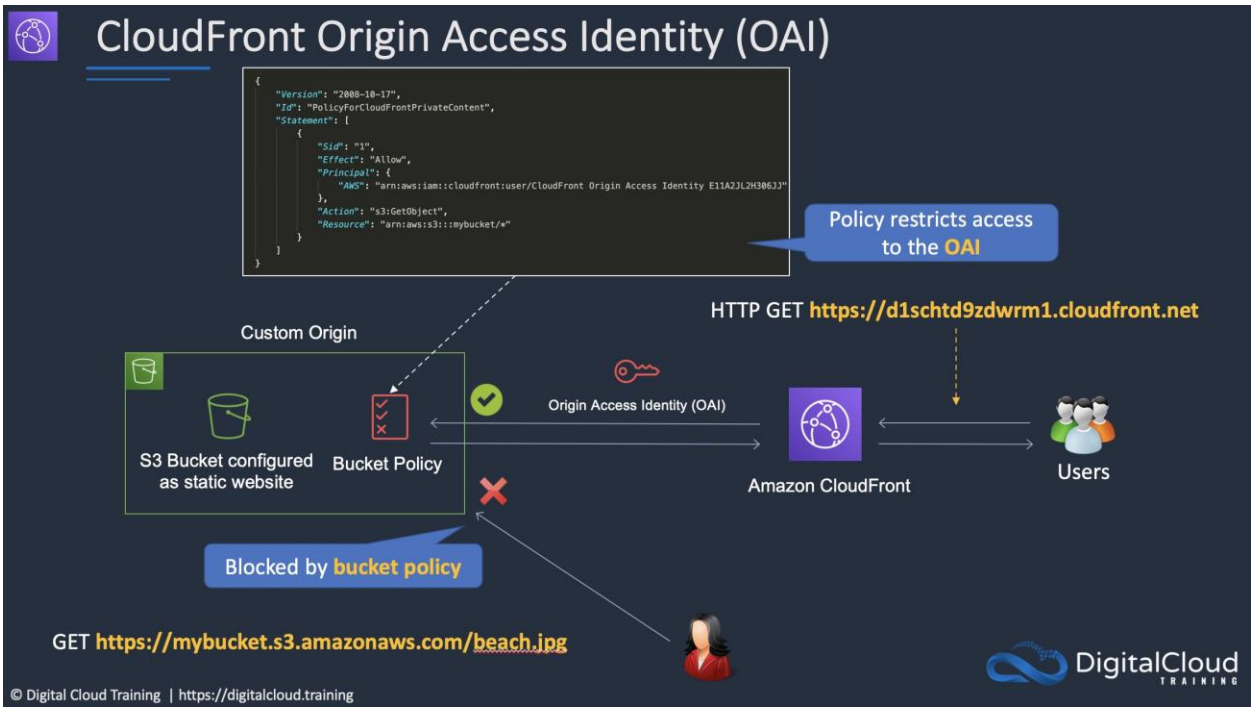
- **Create an S3 bucket policy with a condition that only allows requests that originate from AWS WAF.**
- **Use an Amazon Route 53 Alias record to forward traffic for the website to AWS WAF. Configure AWS WAF to inspect traffic and attach the CloudFront distribution.**
- **Deploy CloudFront with an S3 origin and configure an origin access identity (OAI) to restrict access to the S3 bucket. Enable AWS WAF on the CloudFront distribution.**

  (Correct)
- **Create a Network ACL that limits access to the S3 bucket to the CloudFront IP addresses. Attach a WebACL to the CloudFront distribution.**

Explanation

The AWS Web Application Firewall (WAF) can be attached to an Amazon CloudFront distribution to enable protection from web exploits. In this case the distribution uses an S3 origin, and the question is stating that all traffic must be inspected by AWS WAF. This means we need to ensure that requests cannot circumvent AWS WAF and hit the S3 bucket directly.

This can be achieved by configuring an origin access identity (OAI) which is a special type of CloudFront user that is created within the distribution and configured in an S3 bucket policy. The policy will only allow requests that come from the OAI which means all requests must come via the distribution and cannot hit S3 directly.



CORRECT: "Deploy CloudFront with an S3 origin and configure an origin access identity (OAI) to restrict access to the S3 bucket. Enable AWS WAF on the CloudFront distribution" is the correct answer.

INCORRECT: "Create a Network ACL that limits access to the S3 bucket to the CloudFront IP addresses. Attach a WebACL to the CloudFront distribution" is incorrect. Network ACLs restrict traffic in/out of subnets but S3 is a public service.

INCORRECT: "Use an Amazon Route 53 Alias record to forward traffic for the website to AWS WAF. Configure AWS WAF to inspect traffic and attach the CloudFront distribution" is incorrect. You cannot direct traffic to AWS WAF using an Alias record.

INCORRECT: "Create an S3 bucket policy with a condition that only allows requests that originate from AWS WAF" is incorrect. This cannot be done. Instead use an OAI in the bucket policy.

References:

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

Save time with our AWS cheat sheets:

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

Question 16:

Skipped

A company has several AWS accounts that are used by developers for development, testing and pre-production environments. The company has received large bills for Amazon EC2 instances that are underutilized. A Solutions Architect has been tasked with restricting the ability to launch large EC2 instances in all accounts.

How can the Solutions Architect meet this requirement with the LEAST operational overhead?

- **Create a resource-based policy that denies the launch of large EC2 instances and attach it to Amazon EC2 in each account.**

- **Create an organization in AWS Organizations that includes all accounts and create a service control policy (SCP) that denies the launch of large EC2 instances.**

  (Correct)

- **Create an IAM role in each account that denies the launch of large EC2 instances. Grant the developers IAM group access to the role.**

- **Create a service-linked role for Amazon EC2 and attach a policy the denies the launch of large EC2 instances.**

Explanation

Service control policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization. An SCP defines a guardrail, or sets limits, on the actions that the account's administrator can delegate to the IAM users and roles in the affected accounts.

In this case the Solutions Architect can use an SCP to define a restriction that denies the launch of large EC2 instances. The SCP can be applied to all accounts, and this will

ensure that even those users with permissions to launch EC2 instances will be restricted to smaller EC2 instance types.

CORRECT: "Create an organization in AWS Organizations that includes all accounts and create a service control policy (SCP) that denies the launch of large EC2 instances" is the correct answer.

INCORRECT: "Create a service-linked role for Amazon EC2 and attach a policy the denies the launch of large EC2 instances" is incorrect. You cannot create service-linked roles yourself; they are created by AWS with predefined policies.

INCORRECT: "Create a resource-based policy that denies the launch of large EC2 instances and attach it to Amazon EC2 in each account" is incorrect. You cannot attach a resource-based policy to Amazon EC2.

INCORRECT: "Create an IAM role in each account that denies the launch of large EC2 instances. Grant the developers IAM group access to the role" is incorrect. This is much less operationally efficient compared to using SCPs with AWS Organizations.

References:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html

Save time with our AWS cheat sheets:

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

Question 17:

Skipped

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

What is the best way to achieve this?

- **Use the AWS Organizations API**
- **Use the AWS Management Console**
-

Use CloudFormation with scripts

(Correct)

- **Use the AWS CLI**

Explanation

The best solution is to use a combination of scripts and AWS CloudFormation. You will also leverage the AWS Organizations API. This solution can provide all of the requirements.

CORRECT: "Use CloudFormation with scripts" is the correct answer.

INCORRECT: "Use the AWS Organizations API" is incorrect. You can create member accounts with the AWS Organizations API. However, you cannot use that API to configure the account and create VPCs and subnets.

INCORRECT: "Use the AWS Management Console" is incorrect. Using the AWS Management Console is not a method of automatically creating the resources.

INCORRECT: "Use the AWS CLI" is incorrect. You can do all tasks using the AWS CLI but it is better to automate the process using AWS CloudFormation.

References:

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

Save time with our AWS cheat sheets:

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

Question 18:

Skipped

A security officer requires that access to company financial reports is logged. The reports are stored in an Amazon S3 bucket. Additionally, any modifications to the log files must be detected.

Which actions should a solutions architect take?

- **Use S3 server access logging on the bucket that houses the reports with the read and write management events and log file validation options enabled**

- **Use S3 server access logging on the bucket that houses the reports with the read and write data events and the log file validation options enabled**

- **Use AWS CloudTrail to create a new trail. Configure the trail to log read and write data events on the S3 bucket that houses the reports. Log these events to a new bucket, and enable log file validation**

  (Correct)

- **Use AWS CloudTrail to create a new trail. Configure the trail to log read and write management events on the S3 bucket that houses the reports. Log these events to a new bucket, and enable log file validation**

Explanation

Amazon CloudTrail can be used to log activity on the reports. The key difference between the two answers that include CloudTrail is that one references data events whereas the other references management events.

Data events provide visibility into the resource operations performed on or within a resource. These are also known as data plane operations. Data events are often high-volume activities.

Example data events include:

• Amazon S3 object-level API activity (for example, GetObject, DeleteObject, and PutObject API operations).

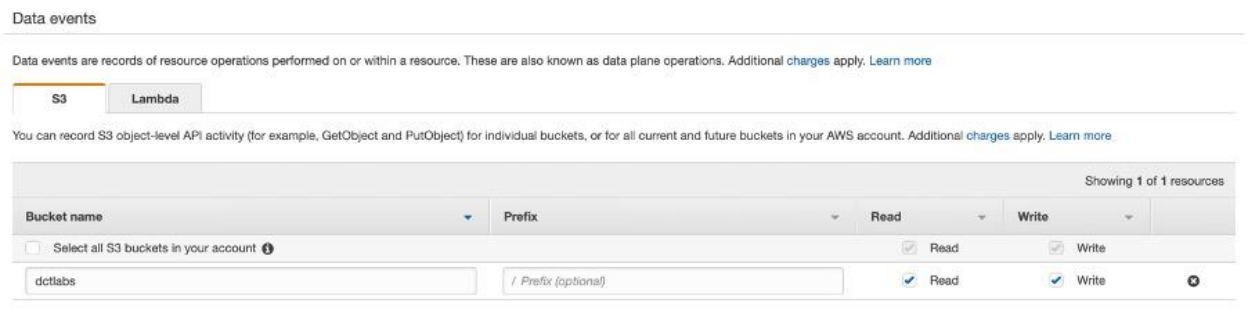
• AWS Lambda function execution activity (the Invoke API).

Management events provide visibility into management operations that are performed on resources in your AWS account. These are also known as control plane operations. Example management events include:

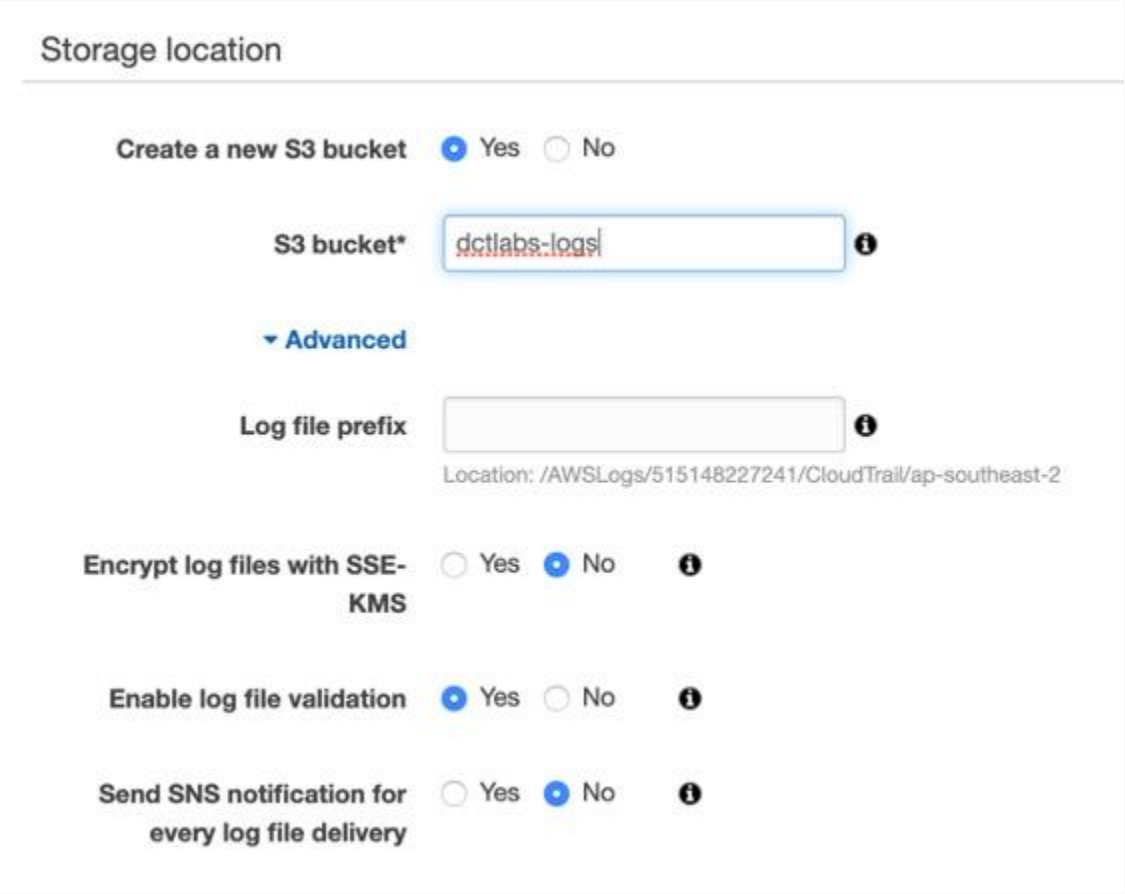
• Configuring security (for example, IAM AttachRolePolicy API operations)

• Registering devices (for example, Amazon EC2 CreateDefaultVpc API operations).

Therefore, to log data about access to the S3 objects the solutions architect should log read and write data events.



Log file validation can also be enabled on the destination bucket:



CORRECT: "Use AWS CloudTrail to create a new trail. Configure the trail to log read and write data events on the S3 bucket that houses the reports. Log these events to a new bucket, and enable log file validation" is the correct answer.

INCORRECT: "Use AWS CloudTrail to create a new trail. Configure the trail to log read and write management events on the S3 bucket that houses the reports. Log these events to a new bucket, and enable log file validation" is incorrect as data events should be logged rather than management events.

INCORRECT: "Use S3 server access logging on the bucket that houses the reports with the read and write data events and the log file validation options enabled" is incorrect as server access logging does not have an option for choosing data events or log file validation.

INCORRECT: "Use S3 server access logging on the bucket that houses the reports with the read and write management events and log file validation options enabled" is incorrect as server access logging does not have an option for choosing management events or log file validation.

References:

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-data-events-with-cloudtrail.html

Save time with our AWS cheat sheets:

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

Question 19:

Skipped

A High Performance Computing (HPC) application needs storage that can provide 135,000 IOPS. The storage layer is replicated across all instances in a cluster.

What is the optimal storage solution that provides the required performance and is cost-effective?

- **Use Amazon Instance Store**

  (Correct)

- **Use Amazon S3 with byte-range fetch**

- **Use Amazon EC2 Enhanced Networking with an EBS HDD Throughput Optimized volume**

- **Use Amazon EBS Provisioned IOPS volume with 135,000 IOPS**

Explanation
Instance stores offer very high performance and low latency. As long as you can afford to lose an instance, i.e. you are replicating your data, these can be a good solution for high performance/low latency requirements. Also, the cost of instance stores is included in the instance charges so it can also be more cost-effective than EBS Provisioned IOPS.

CORRECT: "Use Amazon Instance Store" is the correct answer.

INCORRECT: "Use Amazon EBS Provisioned IOPS volume with 135,000 IOPS" is incorrect. In the case of a HPC cluster that replicates data between nodes you don't necessarily need a shared storage solution such as Amazon EBS Provisioned IOPS – this would also be a more expensive solution as the Instance Store is included in the cost of the HPC instance.

INCORRECT: "Use Amazon S3 with byte-range fetch" is incorrect. Amazon S3 is not a solution for this HPC application as in this case it will require block-based storage to provide the required IOPS.

INCORRECT: "Use Amazon EC2 Enhanced Networking with an EBS HDD Throughput Optimized volume" o\is incorrect. Enhanced networking provides higher bandwidth and lower latency and is implemented using an Elastic Network Adapter (ENA). However, using an ENA with an HDD Throughput Optimized volume is not recommended and the volume will not provide the performance required for this use case.

References:

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

Save time with our AWS cheat sheets:

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

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

Question 20:
Skipped
Health related data in Amazon S3 needs to be frequently accessed for up to 90 days. After that time the data must be retained for compliance reasons for seven years and is rarely accessed.

Which storage classes should be used?

-

Store data in INTELLIGENT_TIERING for 90 days then transition to STANDARD_IA

- **Store data in STANDARD for 90 days then transition the data to DEEP_ARCHIVE**

  (Correct)

- **Store data in STANDARD for 90 days then expire the data**

- **Store data in STANDARD for 90 days then transition to REDUCED_REDUNDANCY**

Explanation

In this case the data is frequently accessed so must be stored in standard for the first 90 days. After that the data is still to be kept for compliance reasons but is rarely accessed so is a good use case for DEEP_ARCHIVE.

CORRECT: "Store data in STANDARD for 90 days then transition the data to DEEP_ARCHIVE" is the correct answer.

INCORRECT: "Store data in INTELLIGENT_TIERING for 90 days then transition to STANDARD_IA" is incorrect. You cannot transition from INTELLIGENT_TIERING to STANDARD_IA.

INCORRECT: "Store data in STANDARD for 90 days then expire the data" is incorrect. Expiring the data is not possible as it must be retained for compliance.

INCORRECT: "Store data in STANDARD for 90 days then transition to REDUCED_REDUNDANCY" is incorrect. You cannot transition from any storage class to REDUCED_REDUNDANCY.

References:

https://docs.aws.amazon.com/AmazonS3/latest/dev/lifecycle-transition-general-considerations.html

Save time with our AWS cheat sheets:

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

Question 21:

Skipped

A company is deploying an analytics application on AWS Fargate. The application requires connected storage that offers concurrent access to files and high performance.

Which storage option should the solutions architect recommend?

- **Create an Amazon S3 bucket for the application and establish an IAM role for Fargate to communicate with Amazon S3.**
- **Create an Amazon FSx for Lustre file share and establish an IAM role that allows Fargate to communicate with FSx for Lustre.**
- **Create an Amazon EFS file share and establish an IAM role that allows Fargate to communicate with Amazon EFS.**

  (Correct)
- **Create an Amazon EBS volume for the application and establish an IAM role that allows Fargate to communicate with Amazon EBS.**

Explanation

The Amazon Elastic File System offers concurrent access to a shared file system and provides high performance. You can create file system policies for controlling access and then use an IAM role that is specified in the policy for access.

CORRECT: "Create an Amazon EFS file share and establish an IAM role that allows Fargate to communicate with Amazon EFS" is the correct answer.

INCORRECT: "Create an Amazon S3 bucket for the application and establish an IAM role for Fargate to communicate with Amazon S3" is incorrect. S3 uses a REST API not a file system API so access can be shared but is not concurrent.

INCORRECT: "Create an Amazon EBS volume for the application and establish an IAM role that allows Fargate to communicate with Amazon EBS" is incorrect. EBS volumes cannot be shared amongst Fargate tasks, they are used with EC2 instances.

INCORRECT: "Create an Amazon FSx for Lustre file share and establish an IAM role that allows Fargate to communicate with FSx for Lustre" is incorrect. It is not supported to connect Fargate to FSx for Lustre.

References:

https://docs.aws.amazon.com/efs/latest/ug/iam-access-control-nfs-efs.html

Save time with our AWS cheat sheets:

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

Question 22:
Skipped
An application allows users to upload and download files. Files older than 2 years will be accessed less frequently. A solutions architect needs to ensure that the application can scale to any number of files while maintaining high availability and durability.

Which scalable solutions should the solutions architect recommend?

- **Store the files on Amazon Elastic File System (EFS) with a lifecycle policy that moves objects older than 2 years to EFS Infrequent Access (EFS IA)**
- **Store the files in Amazon Elastic Block Store (EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data older than 2 years**
- **Store the files in Amazon Elastic Block Store (EBS) volumes. Create a lifecycle policy to move files older than 2 years to Amazon S3 Glacier**
- **Store the files on Amazon S3 with a lifecycle policy that moves objects older than 2 years to S3 Standard Infrequent Access (S3 Standard-IA)**

  (Correct)

Explanation
S3 Standard-IA is for data that is accessed less frequently, but requires rapid access when needed. S3 Standard-IA offers the high durability, high throughput, and low latency

of S3 Standard, with a low per GB storage price and per GB retrieval fee. This combination of low cost and high performance make S3 Standard-IA ideal for long-term storage, backups, and as a data store for disaster recovery files.

CORRECT: "Store the files on Amazon S3 with a lifecycle policy that moves objects older than 2 years to S3 Standard Infrequent Access (S3 Standard-IA)" is the correct answer.

INCORRECT: "Store the files on Amazon Elastic File System (EFS) with a lifecycle policy that moves objects older than 2 years to EFS Infrequent Access (EFS IA)" is incorrect. With EFS you can transition files to EFS IA after a file has not been accessed for a specified period of time with options up to 90 days. You cannot transition based on an age of 2 years.

INCORRECT: "Store the files in Amazon Elastic Block Store (EBS) volumes. Schedule snapshots of the volumes. Use the snapshots to archive data older than 2 years" is incorrect. You cannot identify the age of data and archive snapshots in this way with EBS.

INCORRECT: "Store the files in Amazon Elastic Block Store (EBS) volumes. Create a lifecycle policy to move files older than 2 years to Amazon S3 Glacier" is incorrect. You cannot archive files from an EBS volume to Glacier using lifecycle policies.

References:

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

Save time with our AWS cheat sheets:

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

Question 23:

Skipped

A systems administrator of a company wants to detect and remediate the compromise of services such as Amazon EC2 instances and Amazon S3 buckets.

Which AWS service can the administrator use to protect the company against attacks?

- **Amazon Inspector**
- **Amazon Macie**

- **Amazon Cognito**
- **Amazon GuardDuty**

  (Correct)

Explanation
Amazon GuardDuty gives you access to built-in detection techniques that are developed and optimized for the cloud. The detection algorithms are maintained and continuously improved upon by AWS Security. The primary detection categories include reconnaissance, instance compromise, account compromise, and bucket compromise.

Amazon GuardDuty offers HTTPS APIs, CLI tools, and Amazon CloudWatch Events to support automated security responses to security findings. For example, you can automate the response workflow by using CloudWatch Events as an event source to trigger an AWS Lambda function.

CORRECT: "Amazon GuardDuty" is the correct answer.

INCORRECT: "Amazon Cognito" is incorrect. Cognito provides sign up and sign services for mobiles apps.

INCORRECT: "Amazon Inspector" is incorrect. Inspector is more about identifying vulnerabilities and evaluating against security best practices. It does not detect compromise.

INCORRECT: "Amazon Macie" is incorrect. Macie is used for detecting and protecting sensitive data that is in Amazon S3.

References:

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

Save time with our AWS cheat sheets:

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

Question 24:
Skipped
A Solutions Architect must design a solution to allow many Amazon EC2 instances across multiple subnets to access a shared data store. The data must be accessed by

all instances simultaneously and access should use the NFS protocol. The solution must also be highly scalable and easy to implement.

Which solution best meets these requirements?

- **Create an Amazon S3 bucket and configure a Network ACL. Grant the EC2 instances permission to access the bucket using the NFS protocol.**

- **Configure an additional EC2 instance as a file server. Create a role in AWS IAM that grants permissions to the file share and attach the role to the EC2 instances.**

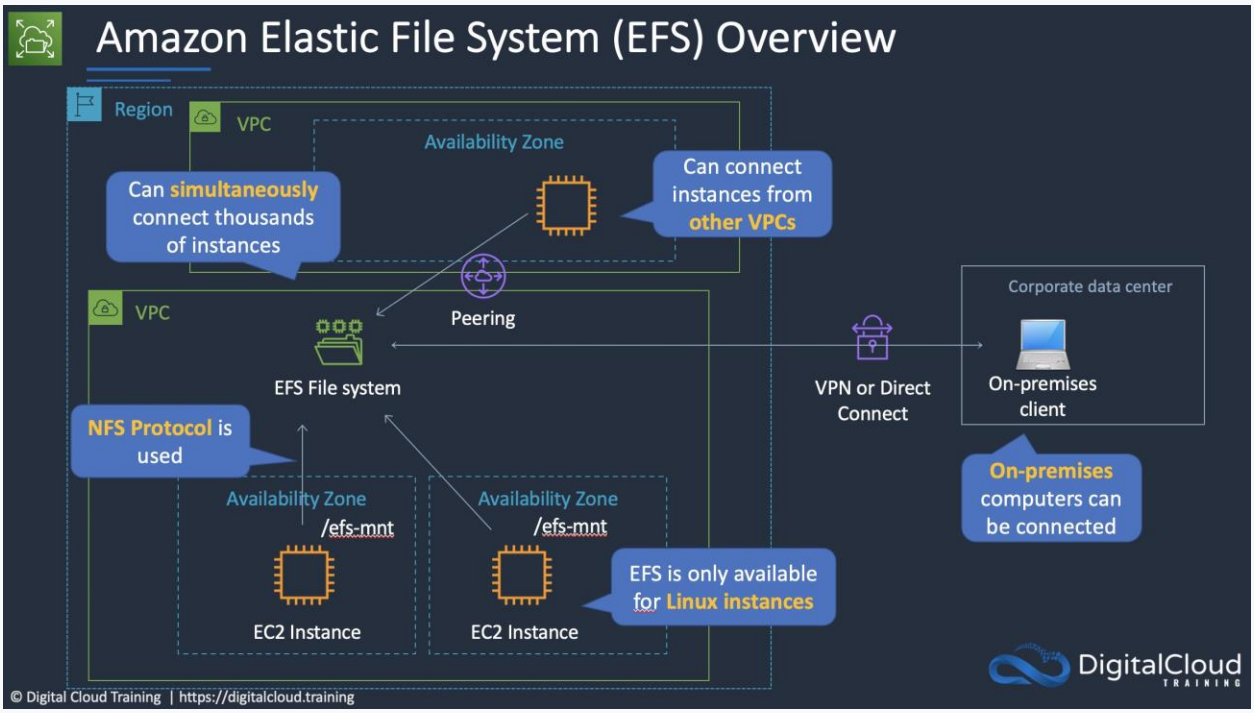
- **Create an Amazon EFS file system. Configure a mount target in each Availability Zone. Attach each instance to the appropriate mount target.**

  (Correct)

- **Create an Amazon EBS volume and create a resource-based policy that grants an AWS IAM role access to the data. Attach the role to the EC2 instances.**

Explanation

The Amazon Elastic File System (EFS) is a perfect solution for this requirement. Amazon EFS filesystems are accessed using the NFS protocol and can be mounted by many instances across multiple subnets simultaneously. EFS filesystems are highly scalable and very easy to implement.



CORRECT: "Create an Amazon EFS file system. Configure a mount target in each Availability Zone. Attach each instance to the appropriate mount target" is the correct answer.

INCORRECT: "Configure an additional EC2 instance as a file server. Create a role in AWS IAM that grants permissions to the file share and attach the role to the EC2 instances" is incorrect. You cannot use IAM roles to grant permissions to a file share created within the operating system of an EC2 instance. Also, this solution is not as highly scalable or easy to implement as Amazon EFS.

INCORRECT: "Create an Amazon S3 bucket and configure a Network ACL. Grant the EC2 instances permission to access the bucket using the NFS protocol" is incorrect. A Network ACL is created to restrict traffic in and out of subnets, it is not used to control access to S3 buckets (use a bucket policy or bucket ACL instead). You cannot grant permission to access an S3 bucket using a protocol, and NFS is not supported for S3 as it is an object-based storage system.

INCORRECT: "Create an Amazon EBS volume and create a resource-based policy that grants an AWS IAM role access to the data. Attach the role to the EC2 instances" is incorrect. You cannot configure a resource-based policy on an Amazon EBS volume.

References:

https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html

Save time with our AWS cheat sheets:

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

Question 25:

Skipped

A Solutions Architect created the following policy and associated to an AWS IAM group containing several administrative users:

```
{
  "Version": "2012-10-17",
   "Statement": [
   {
        "Effect": "Allow",
        "Action": "ec2:TerminateInstances",
        "Resource": "*",
        "Condition": {
             "IpAddress": {
                 "aws:SourceIp": "10.1.2.0/24"
            }
        }
   },
  {
            "Effect": "Deny",
            "Action": "ec2:*",
             "Resource": "*",
             "Condition": {
```

```
                "StringNotEquals": {
                        "ec2:Region": "us-east-1"
                }
            }
        }
    ]
}
```

What is the effect of this policy?

- **Administrators can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.1.2.28.**

  (Correct)

- **Administrators can terminate an EC2 instance in any AWS Region except us-east-1.**

- **Administrators can terminate an EC2 instance with the IP address 10.1.2.5 in the us-east-1 Region.**

- **Administrators cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.1.2.28.**

Explanation

The Condition element (or Condition *block*) lets you specify conditions for when a policy is in effect. The Condition element is optional. In the Condition element, you build expressions in which you use condition operators (equal, less than, etc.) to match the condition keys and values in the policy against keys and values in the request context.

In this policy statement the first block allows the "ec2:TerminateInstances" API action only if the IP address of the requester is within the "10.1.2.0/24" range. This is specified using the "aws:SourceIp" condition.

The second block denies all EC2 API actions with a conditional operator (StringNotEquals) that checks the Region the request is being made in ("ec2:Region"). If the Region is any value other than us-east-1 the request will be denied. If the Region the request is being made in is us-east-1 the request will not be denied.

CORRECT: "Administrators can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.1.2.28" is the correct answer.

INCORRECT: "Administrators cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.1.2.28" is incorrect. This is not true; the conditions allow this action.

INCORRECT: "Administrators can terminate an EC2 instance in any AWS Region except us-east-1" is incorrect. The API action to terminate instances only has a condition of the source IP. If the source IP is in the range it will allow. The second block only denies API actions if the Region is NOT us-east-1. Therefore, the user can terminate instances in us-east-1

INCORRECT: "Administrators can terminate an EC2 instance with the IP address 10.1.2.5 in the us-east-1 Region" is incorrect. The aws:SourceIp condition is checking the IP address of the requester (where you're making the call from), not the resource you want to terminate.

References:

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

Save time with our AWS cheat sheets:

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

Question 26:

Skipped

A company requires a high-performance file system that can be mounted on Amazon EC2 Windows instances and Amazon EC2 Linux instances. Applications running on the EC2 instances perform separate processing of the same files and the solution must provide a file system that can be mounted by all instances simultaneously.

Which solution meets these requirements?

- **Use Amazon FSx for Windows File Server for the Windows instances and the Linux instances.**

  (Correct)

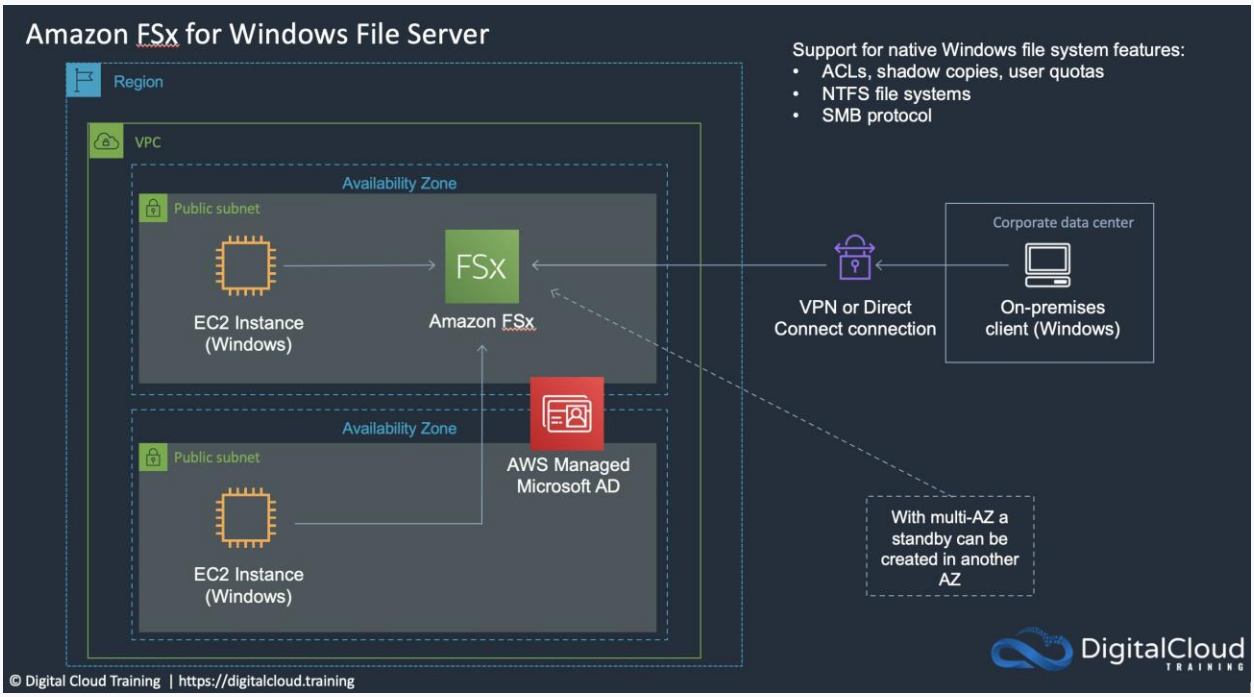
- **Use Amazon FSx for Windows File Server for the Windows instances. Use Amazon FSx for Lustre for the Linux instances. Link both Amazon FSx file systems to the same Amazon S3 bucket.**

- **Use Amazon FSx for Windows File Server for the Windows instances. Use Amazon Elastic File System (Amazon EFS) with Max I/O performance mode for the Linux instances.**

- **Use Amazon Elastic File System (Amazon EFS) with General Purpose performance mode for the Windows instances and the Linux instances.**

Explanation

Amazon FSx for Windows File Server provides a fully managed native Microsoft Windows file system so you can easily move your Windows-based applications that require shared file storage to AWS. You can easily connect Linux instances to the file system by installing the cifs-utils package. The Linux instances can then mount an SMB/CIFS file system.



CORRECT: "Use Amazon FSx for Windows File Server for the Windows instances and the Linux instances" is the correct answer.

INCORRECT: "Use Amazon FSx for Windows File Server for the Windows instances. Use Amazon Elastic File System (Amazon EFS) with Max I/O performance mode for the Linux instances" is incorrect. This solution results in two separate file systems and a shared file system is required.

INCORRECT: "Use Amazon Elastic File System (Amazon EFS) with General Purpose performance mode for the Windows instances and the Linux instances" is incorrect. You cannot use Amazon EFS for Windows instances as this is not supported.

INCORRECT: "Use Amazon FSx for Windows File Server for the Windows instances. Use Amazon FSx for Lustre for the Linux instances. Link both Amazon FSx file systems to the same Amazon S3 bucket" is incorrect. Amazon FSx for Windows File Server does not use Amazon S3 buckets, so this is another solution that results in separate file systems.

References:

https://docs.aws.amazon.com/fsx/latest/WindowsGuide/using-file-shares.html#map-shares-linux

Save time with our AWS cheat sheets:

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

Question 27:

Skipped

An application runs on Amazon EC2 instances across multiple Availability Zones. The instances run in an Amazon EC2 Auto Scaling group behind an Application Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 40%.

What should a solutions architect do to maintain the desired performance across all instances in the group?

- **Use an AWS Lambda function to update the desired Auto Scaling group capacity**
- **Use scheduled scaling actions to scale up and scale down the Auto Scaling group**
- **Use a target tracking policy to dynamically scale the Auto Scaling group**

  (Correct)
- **Use a simple scaling policy to dynamically scale the Auto Scaling group**

Explanation

With target tracking scaling policies, you select a scaling metric and set a target value. Amazon EC2 Auto Scaling creates and manages the CloudWatch alarms that trigger the scaling policy and calculates the scaling adjustment based on the metric and the target value.

The scaling policy adds or removes capacity as required to keep the metric at, or close to, the specified target value. In addition to keeping the metric close to the target value, a target tracking scaling policy also adjusts to the changes in the metric due to a changing load pattern.

CORRECT: "Use a target tracking policy to dynamically scale the Auto Scaling group" is the correct answer.

INCORRECT: "Use a simple scaling policy to dynamically scale the Auto Scaling group" is incorrect as target tracking is a better way to keep the aggregate CPU usage at around 40%

INCORRECT: "Use an AWS Lambda function to update the desired Auto Scaling group capacity" is incorrect as this can be done automatically.

INCORRECT: "Use scheduled scaling actions to scale up and scale down the Auto Scaling group" is incorrect as dynamic scaling is required to respond to changes in utilization.

References:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html

Save time with our AWS cheat sheets:

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

Question 28:

Skipped

A company needs to migrate a large quantity of data from an on-premises environment to Amazon S3. The company is connected via an AWS Direct Connect (DX) connection. The company requires a fully managed solution that will keep the data private and automate and accelerate the replication of the data to AWS storage services.

Which solution should a Solutions Architect recommend?

- **Deploy an AWS Storage Gateway file gateway with a local cache and store the primary data set in Amazon S3.**
- **Deploy an AWS Storage Gateway volume gateway in stored volume mode and take point-in-time copies of the volumes using AWS Backup.**
- **Deploy an AWS DataSync agent for the on-premises environment. Configure a task to replicate the data and connect it to a public endpoint.**

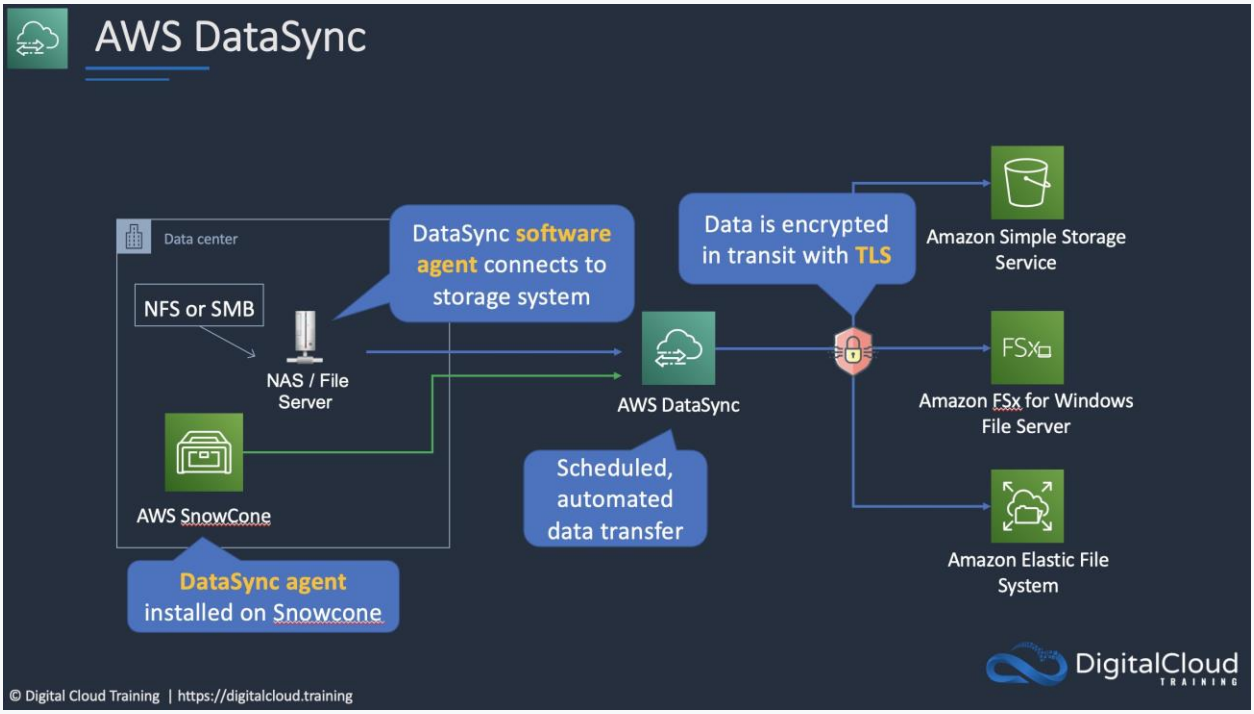
Deploy an AWS DataSync agent for the on-premises environment. Configure a task to replicate the data and connect it to a VPC endpoint.

(Correct)

Explanation

AWS DataSync can be used to automate and accelerate the replication of data to AWS storage services. Note that Storage Gateway is used for hybrid scenarios where servers need local access to data with various options for storing and synchronizing the data to AWS storage services. Storage Gateway does not accelerate replication of data.

To deploy DataSync an agent must be installed. Then a task must be configured to replicated data to AWS. The task requires a connection to a service endpoint. To keep the data private and send it across the DX connection, a VPC endpoint should be used.



CORRECT: "Deploy an AWS DataSync agent for the on-premises environment. Configure a task to replicate the data and connect it to a VPC endpoint" is the correct answer.

INCORRECT: "Deploy an AWS DataSync agent for the on-premises environment. Configure a task to replicate the data and connect it to a public endpoint" is incorrect. A public endpoint will send data over the public internet which should be avoided in this scenario.

INCORRECT: "Deploy an AWS Storage Gateway volume gateway in stored volume mode and take point-in-time copies of the volumes using AWS Backup" is incorrect. Storage

Gateway will not accelerate replication and a volume gateway will create EBS snapshots (not S3 objects).

INCORRECT: "Deploy an AWS Storage Gateway file gateway with a local cache and store the primary data set in Amazon S3" is incorrect. Storage Gateway will not accelerate replication and a file gateway should be used for providing NFS or CIFS/SMB access to data locally which is not required.

References:

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

Save time with our AWS cheat sheets:

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

Question 29:

Skipped

A company hosts statistical data in an Amazon S3 bucket that users around the world download from their website using a URL that resolves to a domain name. The company needs to provide low latency access to users and plans to use Amazon Route 53 for hosting DNS records.

Which solution meets these requirements?

- **Create an A record in Route 53, use a Route 53 traffic policy for the web application, and configure a geoproximity rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.**
- **Create a web distribution on Amazon CloudFront pointing to an Amazon S3 origin. Create a CNAME record in a Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name.**
- **Create a web distribution on Amazon CloudFront pointing to an Amazon S3 origin. Create an ALIAS record in the Amazon Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name.**

(Correct)

- **Create an A record in Route 53, use a Route 53 traffic policy for the web application, and configure a geolocation rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy.**

Explanation

This is a simple requirement for low latency access to the contents of an Amazon S3 bucket for global users. The best solution here is to use Amazon CloudFront to cache the content in Edge Locations around the world. This involves creating a web distribution that points to an S3 origin (the bucket) and then create an Alias record in Route 53 that resolves the applications URL to the CloudFront distribution endpoint.

CORRECT: "Create a web distribution on Amazon CloudFront pointing to an Amazon S3 origin. Create an ALIAS record in the Amazon Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name" is the correct answer.

INCORRECT: "Create a web distribution on Amazon CloudFront pointing to an Amazon S3 origin. Create a CNAME record in a Route 53 hosted zone that points to the CloudFront distribution, resolving to the application's URL domain name" is incorrect. An Alias record should be used to point to an Amazon CloudFront distribution.

INCORRECT: "Create an A record in Route 53, use a Route 53 traffic policy for the web application, and configure a geolocation rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy" is incorrect. There is only a single endpoint (the Amazon S3 bucket) so this strategy would not work. Much better to use CloudFront to cache in multiple locations.

INCORRECT: "Create an A record in Route 53, use a Route 53 traffic policy for the web application, and configure a geoproximity rule. Configure health checks to check the health of the endpoint and route DNS queries to other endpoints if an endpoint is unhealthy" is incorrect. Again, there is only one endpoint so this strategy will simply not work.

References:

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/RoutingToS3Bucket.html

Save time with our AWS cheat sheets:

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

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

Question 30:

Skipped

A company has created an application that stores sales performance data in an Amazon DynamoDB table. A web application is being created to display the data. A Solutions Architect must design the web application using managed services that require minimal operational maintenance.

Which architectures meet these requirements? (Select TWO.)

- ☐ **An Elastic Load Balancer forwards requests to a target group with the DynamoDB table configured as the target.**
- ☐ **An Amazon API Gateway REST API directly accesses the sales performance data in the DynamoDB table.**

  (Correct)
- ☐ **An Elastic Load Balancer forwards requests to a target group of Amazon EC2 instances. The EC2 instances run an application that reads data from the DynamoDB table.**
- ☐ **An Amazon Route 53 hosted zone routes requests to an AWS Lambda endpoint to invoke a Lambda function that reads data from the DynamoDB table.**
- ☐ **An Amazon API Gateway REST API invokes an AWS Lambda function. The Lambda function reads data from the DynamoDB table.**

  (Correct)

Explanation

There are two architectures here that fulfill the requirement to create a web application that displays the data from the DynamoDB table.

The first one is to use an API Gateway REST API that invokes an AWS Lambda function. A Lambda proxy integration can be used, and this will proxy the API requests to the Lambda function which processes the request and accesses the DynamoDB table.

The second option is to use an API Gateway REST API to directly access the sales performance data. In this case a proxy for the DynamoDB query API can be created using a method in the REST API.

CORRECT: "An Amazon API Gateway REST API invokes an AWS Lambda function. The Lambda function reads data from the DynamoDB table" is a correct answer.

CORRECT: "An Amazon API Gateway REST API directly accesses the sales performance data in the DynamoDB table" is also a correct answer.

INCORRECT: "An Amazon Route 53 hosted zone routes requests to an AWS Lambda endpoint to invoke a Lambda function that reads data from the DynamoDB table" is incorrect. An Alias record could be created in a hosted zone but a hosted zone itself does not route to a Lambda endpoint. Using an Alias, it is possible to route to a VPC endpoint that uses a Lambda function however there would not be a web front end so a REST API would be preferable.

INCORRECT: "An Elastic Load Balancer forwards requests to a target group with the DynamoDB table configured as the target" is incorrect. You cannot configure DynamoDB as a target in a target group.

INCORRECT: "An Elastic Load Balancer forwards requests to a target group of Amazon EC2 instances. The EC2 instances run an application that reads data from the DynamoDB table" is incorrect. This would not offer low operational maintenance as you must manage the EC2 instances.

References:

https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-create-api-as-simple-proxy-for-lambda.html

https://aws.amazon.com/blogs/compute/using-amazon-api-gateway-as-a-proxy-for-dynamodb/

Save time with our AWS cheat sheets:

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

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

Question 31:

Skipped

A solutions architect is designing a high performance computing (HPC) application using Amazon EC2 Linux instances. All EC2 instances need to communicate to each other with low latency and high throughput network performance.

Which EC2 solution BEST meets these requirements?

- **Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones**
- **Launch the EC2 instances in an Auto Scaling group in two Regions. Place a Network Load Balancer in front of the instances**
- **Launch the EC2 instances in a spread placement group in one Availability Zone**
- **Launch the EC2 instances in a cluster placement group in one Availability Zone**

  (Correct)

Explanation

When you launch a new EC2 instance, the EC2 service attempts to place the instance in such a way that all of your instances are spread out across underlying hardware to minimize correlated failures. You can use *placement groups* to influence the placement of a group of *interdependent* instances to meet the needs of your workload. Depending on the type of workload, you can create a placement group using one of the following placement strategies:

• *Cluster* – packs instances close together inside an Availability Zone. This strategy enables workloads to achieve the low-latency network performance necessary for tightly-coupled node-to-node communication that is typical of HPC applications.

• *Partition* – spreads your instances across logical partitions such that groups of instances in one partition do not share the underlying hardware with groups of instances in different partitions. This strategy is typically used by large distributed and replicated workloads, such as Hadoop, Cassandra, and Kafka.

• *Spread* – strictly places a small group of instances across distinct underlying hardware to reduce correlated failures.

For this scenario, a cluster placement group should be used as this is the best option for providing low-latency network performance for a HPC application.

CORRECT: "Launch the EC2 instances in a cluster placement group in one Availability Zone" is the correct answer.

INCORRECT: "Launch the EC2 instances in a spread placement group in one Availability Zone" is incorrect as the spread placement group is used to spread instances across distinct underlying hardware.

INCORRECT: "Launch the EC2 instances in an Auto Scaling group in two Regions. Place a Network Load Balancer in front of the instances" is incorrect as this does not achieve the stated requirement to provide low-latency, high throughput network performance between instances. Also, you cannot use an ELB across Regions.

INCORRECT: "Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones" is incorrect as this does not reduce network latency or improve performance.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

Save time with our AWS cheat sheets:

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

Question 32:

Skipped

An application runs on Amazon EC2 instances backed by Amazon EBS volumes and an Amazon RDS database. The application is highly sensitive and security compliance requirements mandate that all personally identifiable information (PII) be encrypted at rest.

Which solution should a Solutions Architect choose to this requirement?

- **Configure Amazon EBS encryption and Amazon RDS encryption with AWS KMS keys to encrypt instance and database volumes.**

  (Correct)

- **Deploy AWS CloudHSM, generate encryption keys, and use the customer master key (CMK) to encrypt database volumes.**

- **Enable encryption on Amazon RDS during creation. Use Amazon Macie to identify sensitive data.**

- **Configure SSL/TLS encryption using AWS KMS customer master keys (CMKs) to encrypt database volumes.**

Explanation

The data must be encrypted at rest on both the EC2 instance's attached EBS volumes and the RDS database. Both storage locations can be encrypted using AWS KMS keys. With RDS, KMS uses a customer master key (CMK) to encrypt the DB instance, all logs, backups, and snapshots.

CORRECT: "Configure Amazon EBS encryption and Amazon RDS encryption with AWS KMS keys to encrypt instance and database volumes" is the correct answer.

INCORRECT: "Enable encryption on Amazon RDS during creation. Use Amazon Macie to identify sensitive data" is incorrect. This does not encrypt the EBS volumes attached to the EC2 instance and Macie cannot be used with RDS.

INCORRECT: "Configure SSL/TLS encryption using AWS KMS customer master keys (CMKs) to encrypt database volumes" is incorrect. SSL encryption encrypts data in transit but not at rest.

INCORRECT: "Deploy AWS CloudHSM, generate encryption keys, and use the customer master key (CMK) to encrypt database volumes" is incorrect. CloudHSM is not required for this solution, and we need to encrypt the database volumes and the EBS volumes.

References:

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

Save time with our AWS cheat sheets:

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

Question 33:

Skipped

A company has deployed an API in a VPC behind an internal Network Load Balancer (NLB). An application that consumes the API as a client is deployed in a second account in private subnets.

Which architectural configurations will allow the API to be consumed without using the public Internet? (Select TWO.)

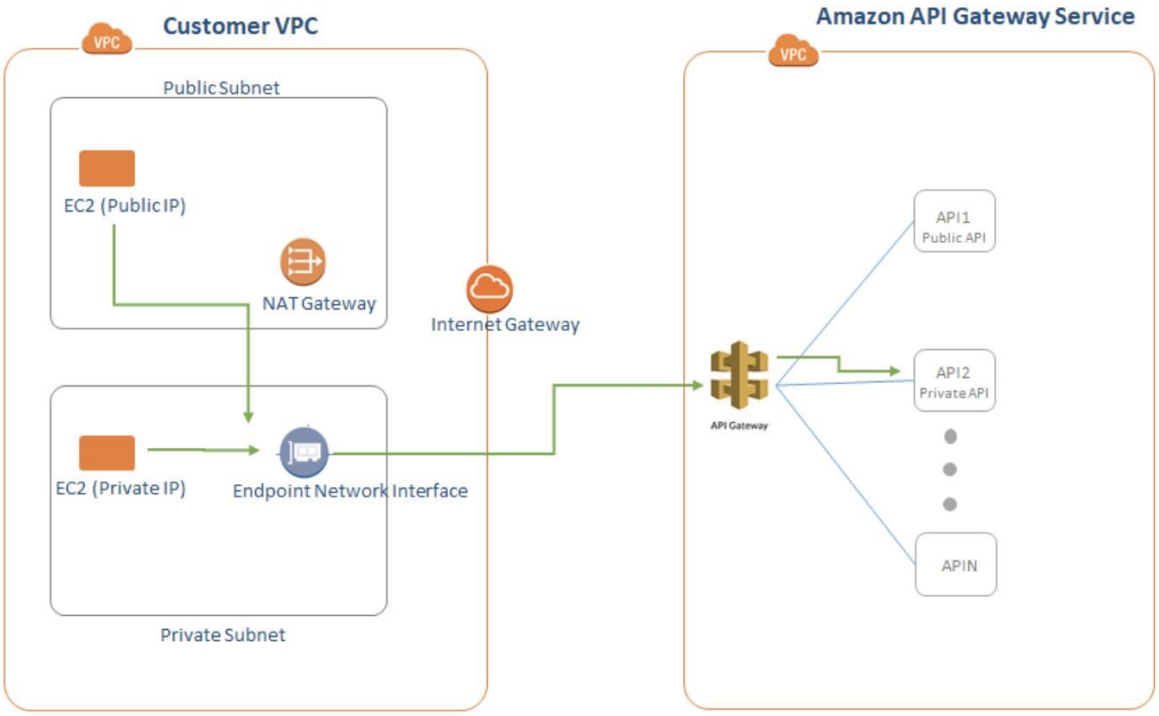
- **Configure an AWS Resource Access Manager connection between the two accounts. Access the API using the private address**
- **Configure a ClassicLink connection for the API into the client VPC. Access the API using the ClassicLink address**
- **Configure a PrivateLink connection for the API into the client VPC. Access the API using the PrivateLink address**

  (Correct)
- **Configure an AWS Direct Connect connection between the two VPCs. Access the API using the private address**
- **Configure a VPC peering connection between the two VPCs. Access the API using the private address**

  (Correct)

Explanation

You can create your own application in your VPC and configure it as an AWS PrivateLink-powered service (referred to as an *endpoint service*). Other AWS principals can create a connection from their VPC to your endpoint service using an interface VPC endpoint. You are the *service provider*, and the AWS principals that create connections to your service are *service consumers*.



This configuration is powered by AWS PrivateLink and clients do not need to use an internet gateway, NAT device, VPN connection or AWS Direct Connect connection, nor do they require public IP addresses.

Another option is to use a VPC Peering connection. A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account.

CORRECT: "Configure a VPC peering connection between the two VPCs. Access the API using the private address" is a correct answer.

CORRECT: "Configure a PrivateLink connection for the API into the client VPC. Access the API using the PrivateLink address" is also a correct answer.

INCORRECT: "Configure an AWS Direct Connect connection between the two VPCs. Access the API using the private address" is incorrect. Direct Connect is used for connecting from on-premises data centers into AWS. It is not used from one VPC to another.

INCORRECT: "Configure a ClassicLink connection for the API into the client VPC. Access the API using the ClassicLink address" is incorrect. ClassicLink allows you to

link EC2-Classic instances to a VPC in your account, within the same Region. This is not relevant to sending data between two VPCs.

INCORRECT: "Configure an AWS Resource Access Manager connection between the two accounts. Access the API using the private address" is incorrect. AWS RAM lets you share resources that are provisioned and managed in other AWS services. However, APIs are not shareable resources with AWS RAM.

References:

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

https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html

Save time with our AWS cheat sheets:

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

Question 34:

Skipped

An application runs on-premises and produces data that must be stored in a locally accessible file system that servers can mount using the NFS protocol. The data must be subsequently analyzed by Amazon EC2 instances in the AWS Cloud.

How can these requirements be met?

- **Use an AWS Storage Gateway tape gateway to take a backup of the local data and store it on AWS, then perform analytics on this data in the AWS Cloud.**

- **Use an AWS Storage Gateway volume gateway in cached mode to back up all the local storage in the AWS Cloud, then perform analytics on this data in the cloud.**

- **Use an AWS Storage Gateway file gateway to provide a locally accessible file system that replicates data to the cloud, then analyze the data in the AWS Cloud.**

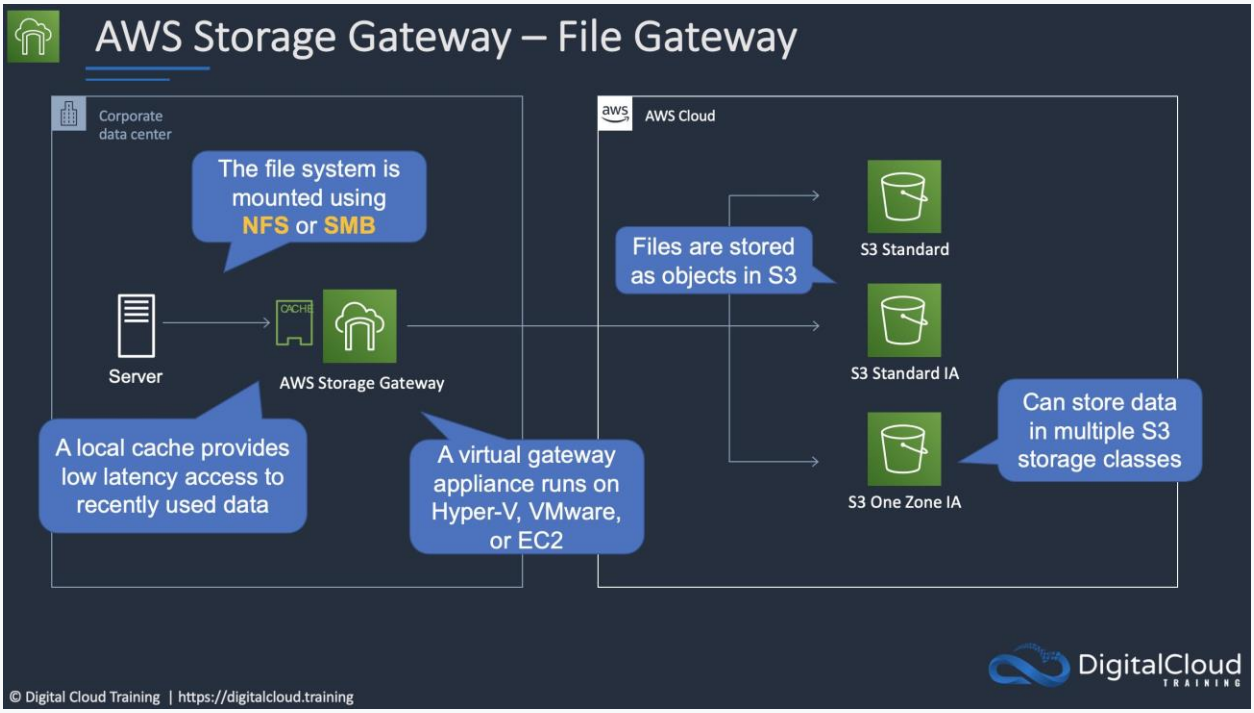
  (Correct)

-

Use an AWS Storage Gateway volume gateway in stored mode to regularly take snapshots of the local data, then copy the data to AWS.

Explanation

The best solution for this requirement is to use an AWS Storage Gateway file gateway. This will provide a local NFS mount point for the data and a local cache. The data is then replicated to Amazon S3 where it can be analyzed by the Amazon EC2 instances in the AWS Cloud.



CORRECT: "Use an AWS Storage Gateway file gateway to provide a locally accessible file system that replicates data to the cloud, then analyze the data in the AWS Cloud" is the correct answer.

INCORRECT: "Use an AWS Storage Gateway tape gateway to take a backup of the local data and store it on AWS, then perform analytics on this data in the AWS Cloud" is incorrect. A tape gateway does not provide a local NFS mount point, it is simply a backup solution not a file system.

INCORRECT: "Use an AWS Storage Gateway volume gateway in stored mode to regularly take snapshots of the local data, then copy the data to AWS" is incorrect. Volume gateways use block-based protocols not NFS.

INCORRECT: "Use an AWS Storage Gateway volume gateway in cached mode to back up all the local storage in the AWS Cloud, then perform analytics on this data in the cloud" is incorrect. Volume gateways use block-based protocols not NFS.

References:

https://aws.amazon.com/storagegateway/file/

Save time with our AWS cheat sheets:

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

Question 35:

Skipped

A Solutions Architect has been tasked with migrating 30 TB of data from an on-premises data center within 20 days. The company has an internet connection that is limited to 25 Mbps and the data transfer cannot use more than 50% of the connection speed.

What should a Solutions Architect do to meet these requirements?

- **Use AWS Snowball.**

  (Correct)

- **Use AWS Storage Gateway.**

- **Use AWS DataSync.**

- **Use a site-to-site VPN.**

Explanation

This is a simple case of working out roughly how long it will take to migrate the data using the 12.5 Mbps of bandwidth that is available for transfer and seeing which options are feasible. Transferring 30 TB of data across a 25 Mbps connection could take upwards of 200 days.

Therefore, we know that using the Internet connection will not meet the requirements and we can rule out any solution that will use the internet (all options except for Snowball). AWS Snowball is a physical device that is shipped to your office or data center. You can then load data onto it and ship it back to AWS where the data is uploaded to Amazon S3.

Snowball is the only solution that will achieve the data migration requirements within the 20-day period.

CORRECT: "Use AWS Snowball" is the correct answer.

INCORRECT: "Use AWS DataSync" is incorrect. This uses the internet which will not meet the 20-day deadline.

INCORRECT: "Use AWS Storage Gateway" is incorrect. This uses the internet which will not meet the 20-day deadline.

INCORRECT: "Use a site-to-site VPN" is incorrect. This uses the internet which will not meet the 20-day deadline.

References:

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

Save time with our AWS cheat sheets:

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

Question 36:

Skipped

An application on Amazon Elastic Container Service (ECS) performs data processing in two parts. The second part takes much longer to complete. How can an Architect decouple the data processing from the backend application component?

- **Process both parts using the same ECS task. Create an Amazon Kinesis Firehose stream**
- **Process each part using a separate ECS task. Create an Amazon SNS topic and send a notification when the processing completes**

Process each part using a separate ECS task. Create an Amazon SQS queue

(Correct)

- 

Create an Amazon DynamoDB table and save the output of the first part to the table

Explanation

Processing each part using a separate ECS task may not be essential but means you can separate the processing of the data. An Amazon Simple Queue Service (SQS) is used for decoupling applications. It is a message queue on which you place messages for processing by application components. In this case you can process each data processing part in separate ECS tasks and have them write an Amazon SQS queue. That way the backend can pick up the messages from the queue when they're ready and there is no delay due to the second part not being complete.

CORRECT: "Process each part using a separate ECS task. Create an Amazon SQS queue" is the correct answer.

INCORRECT: "Process both parts using the same ECS task. Create an Amazon Kinesis Firehose stream" is incorrect. Amazon Kinesis Firehose is used for streaming data. This is not an example of streaming data. In this case SQS is better as a message can be placed on a queue to indicate that the job is complete and ready to be picked up by the backend application component.

INCORRECT: "Process each part using a separate ECS task. Create an Amazon SNS topic and send a notification when the processing completes" is incorrect. Amazon Simple Notification Service (SNS) can be used for sending notifications. It is useful when you need to notify multiple AWS services. In this case an Amazon SQS queue is a better solution as there is no mention of multiple AWS services and this is an ideal use case for SQS.

INCORRECT: "Create an Amazon DynamoDB table and save the output of the first part to the table" is incorrect. Amazon DynamoDB is unlikely to be a good solution for this requirement. There is a limit on the maximum amount of data that you can store in an entry in a DynamoDB table.

References:

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

Save time with our AWS cheat sheets:

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

Question 37:

Skipped

A company has created a disaster recovery solution for an application that runs behind an Application Load Balancer (ALB). The DR solution consists of a second copy of the application running behind a second ALB in another Region. The Solutions Architect requires a method of automatically updating the DNS record to point to the ALB in the second Region.

What action should the Solutions Architect take?

- **Configure an alarm on a CloudTrail trail.**
- **Use Amazon EventBridge to cluster the ALBs.**
- **Enable an ALB health check.**
- **Enable an Amazon Route 53 health check.**

  (Correct)

Explanation

Amazon Route 53 health checks monitor the health and performance of your web applications, web servers, and other resources. Each health check that you create can monitor one of the following:

- The health of a specified resource, such as a web server
- The status of other health checks
- The status of an Amazon CloudWatch alarm

Health checks can be used with other configurations such as a failover routing policy. In this case a failover routing policy will direct traffic to the ALB of the primary Region unless health checks fail at which time it will direct traffic to the secondary record for the DR ALB.

CORRECT: "Enable an Amazon Route 53 health check" is the correct answer.

INCORRECT: "Enable an ALB health check" is incorrect. This will simply perform health checks of the instances behind the ALB, rather than the ALB itself. This could be used in combination with Route 53 health checks.

INCORRECT: "Use Amazon EventBridge to cluster the ALBs" is incorrect. You cannot cluster ALBs in any way.

INCORRECT: "Configure an alarm on a CloudTrail trail" is incorrect. CloudTrail records API activity so this does not help.

References:

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html

Save time with our AWS cheat sheets:

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

Question 38:

Skipped

An online store uses an Amazon Aurora database. The database is deployed as a Multi-AZ deployment. Recently, metrics have shown that database read requests are high and causing performance issues which result in latency for write requests.

What should the solutions architect do to separate the read requests from the write requests?

- **Enable read through caching on the Amazon Aurora database**
- **Update the application to read from the Aurora Replica**

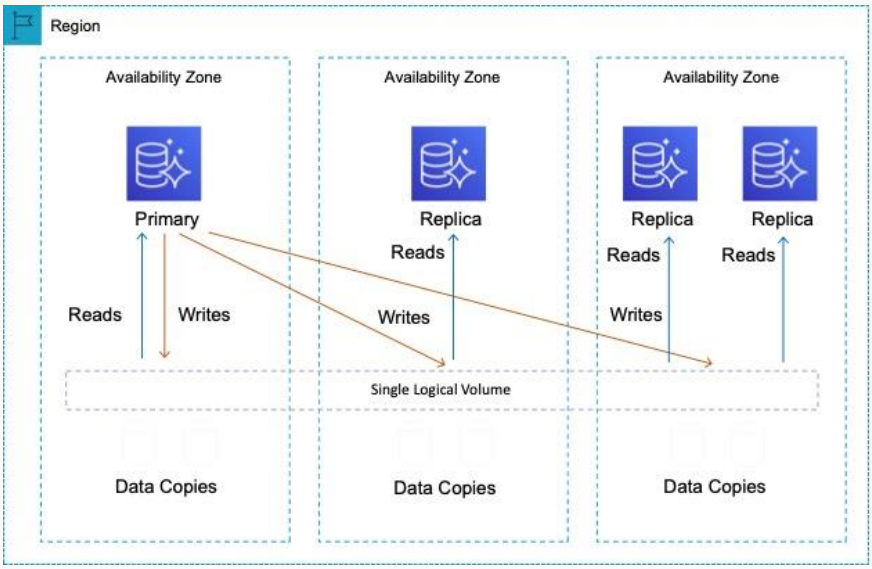
  (Correct)
- **Create a read replica and modify the application to use the appropriate endpoint**

Create a second Amazon Aurora database and link it to the primary database as a read replica

Explanation

Aurora Replicas are independent endpoints in an Aurora DB cluster, best used for scaling read operations and increasing availability. Up to 15 Aurora Replicas can be distributed across the Availability Zones that a DB cluster spans within an AWS Region.

The DB cluster volume is made up of multiple copies of the data for the DB cluster. However, the data in the cluster volume is represented as a single, logical volume to the primary instance and to Aurora Replicas in the DB cluster.



Aurora Fault Tolerance

- Fault tolerance across 3 AZs
- Single logical volume
- Aurora Replicas scale-out read requests
- Up to 15 Aurora Replicas with sub-10ms replica lag
- Aurora Replicas are independent endpoints
- Can promote Aurora Replica to be a new primary or create new primary
- Set priority (tiers) on Aurora Replicas to control order of promotion
- Can use Auto Scaling to add replicas

As well as providing scaling for reads, Aurora Replicas are also targets for multi-AZ. In this case the solutions architect can update the application to read from the Aurora Replica

CORRECT: "Update the application to read from the Aurora Replica" is the correct answer.

INCORRECT: "Create a read replica and modify the application to use the appropriate endpoint" is incorrect. An Aurora Replica is both a standby in a Multi-AZ configuration and a target for read traffic. The architect simply needs to direct traffic to the Aurora Replica.

INCORRECT: "Enable read through caching on the Amazon Aurora database." is incorrect as this is not a feature of Amazon Aurora.

INCORRECT: "Create a second Amazon Aurora database and link it to the primary database as a read replica" is incorrect as an Aurora Replica already exists as this is a

Multi-AZ configuration and the standby is an Aurora Replica that can be used for read traffic.

References:

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html

Save time with our AWS cheat sheets:

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

Question 39:

Skipped

A company is deploying an application that produces data that must be processed in the order it is received. The company requires a solution for decoupling the event data from the processing layer. The solution must minimize operational overhead.

How can a Solutions Architect meet these requirements?

- **Create an Amazon SQS standard queue to decouple the application. Set up an AWS Lambda function to process messages from the queue independently.**
- **Create an Amazon SQS FIFO queue to decouple the application. Configure an AWS Lambda function to process messages from the queue.**

  (Correct)
- **Create an Amazon SNS topic to decouple the application. Configure an Amazon SQS queue as a subscriber.**
- **Create an Amazon SNS topic to decouple the application. Configure an AWS Lambda function as a subscriber.**

Explanation

Amazon SQS can be used to decouple this application using a FIFO queue. With a FIFO queue the order in which messages are sent and received is strictly preserved. You can

configure an AWS Lambda function to poll the queue, or you can configure a Lambda function as a destination to asynchronously process messages from the queue.

CORRECT: "Create an Amazon SQS FIFO queue to decouple the application. Configure an AWS Lambda function to process messages from the queue" is the correct answer.

INCORRECT: "Create an Amazon SQS standard queue to decouple the application. Set up an AWS Lambda function to process messages from the queue independently" is incorrect. A standard queue only offers best-effort ordering so it may not preserve the order of the data.

INCORRECT: "Create an Amazon SNS topic to decouple the application. Configure an AWS Lambda function as a subscriber" is incorrect. Amazon SQS is better for this use case as there are a sequence of events for which the order must be maintained, and these events can be queued for processing whereas SNS delivers them for immediate processing.

INCORRECT: "Create an Amazon SNS topic to decouple the application. Configure an Amazon SQS queue as a subscriber" is incorrect. As above an SQS queue would be preferred for queuing the messages.

References:

https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-configure-lambda-function-trigger.html

Save time with our AWS cheat sheets:

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

Question 40:
Skipped

A security team wants to limit access to specific services or actions in all of the team's AWS accounts. All accounts belong to a large organization in AWS Organizations. The solution must be scalable and there must be a single point where permissions can be maintained.

What should a solutions architect do to accomplish this?

- **Create cross-account roles in each account to deny access to the services or actions**
- **Create a security group to allow accounts and attach it to user groups**
- **Create an ACL to provide access to the services or actions**
- **Create a service control policy in the root organizational unit to deny access to the services or actions**

(Correct)

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.

SCPs alone are not sufficient for allowing access in the accounts in your organization. Attaching an SCP to an AWS Organizations entity (root, OU, or account) defines a

guardrail for what actions the principals can perform. You still need to attach identity-based or resource-based policies to principals or resources in your organization's accounts to actually grant permissions to them.

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 an ACL to provide access to the services or actions" is incorrect as access control lists are not used for permissions associated with IAM. Permissions policies are used with IAM.

INCORRECT: "Create a security group to allow accounts and attach it to user groups" is incorrect as security groups are instance level firewalls. They do not limit service actions.

INCORRECT: "Create cross-account roles in each account to deny access to the services or actions" is incorrect as this is a complex solution and does not provide centralized control

References:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html

Save time with our AWS cheat sheets:

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

Question 41:

Skipped

An application runs on a fleet of Amazon EC2 instances in an Amazon EC2 Auto Scaling group behind an Elastic Load Balancer. The operations team has determined that the application performs best when the CPU utilization of the EC2 instances is at or near 60%.

Which scaling configuration should a Solutions Architect use to optimize the applications performance?

- **Use a target tracking policy to dynamically scale the Auto Scaling group.**

  (Correct)

-

Use a scheduled scaling policy to dynamically the Auto Scaling group.

-

Use a simple scaling policy to dynamically scale the Auto Scaling group.

-

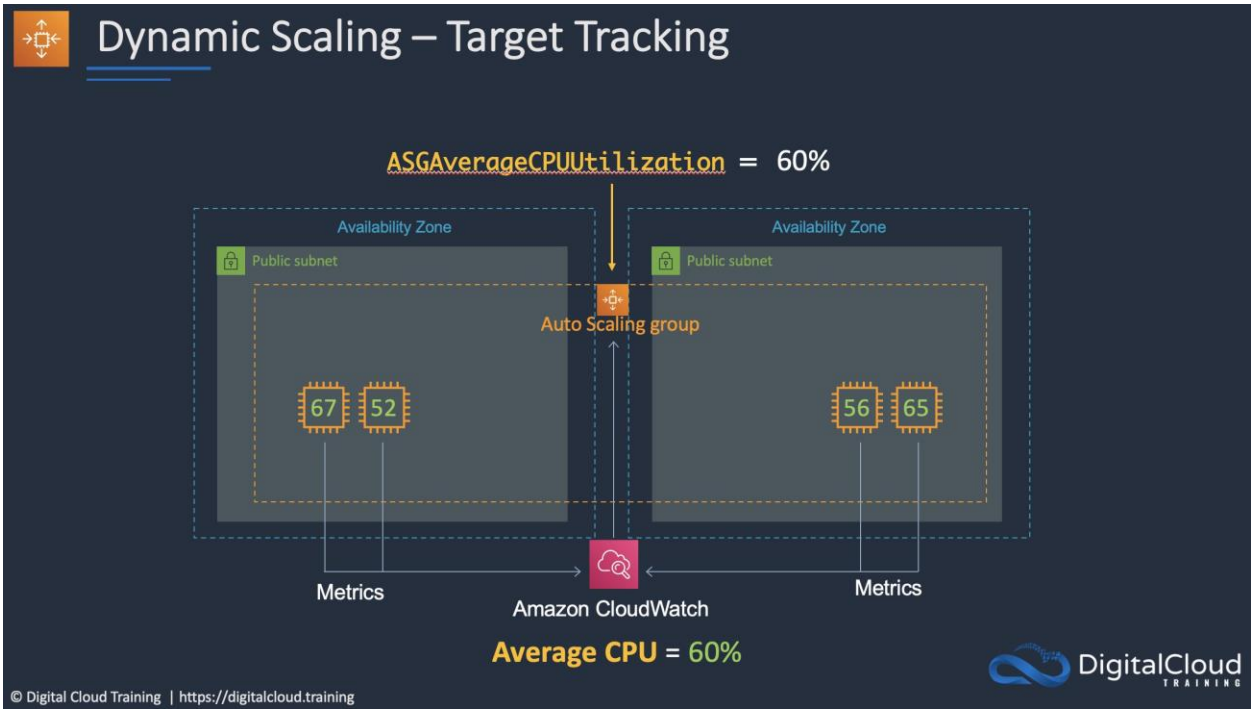
Use a step scaling policy to dynamically scale the Auto Scaling group.

Explanation

With target tracking scaling policies, you select a scaling metric and set a target value. Amazon EC2 Auto Scaling creates and manages the CloudWatch alarms that trigger the scaling policy and calculates the scaling adjustment based on the metric and the target value.

The scaling policy adds or removes capacity as required to keep the metric at, or close to, the specified target value. In addition to keeping the metric close to the target value, a target tracking scaling policy also adjusts to changes in the metric due to a changing load pattern.

The following diagram shows a target tracking policy set to keep the CPU utilization of the EC2 instances at or close to 60%.



CORRECT: "Use a target tracking policy to dynamically scale the Auto Scaling group" is the correct answer.

INCORRECT: "Use a simple scaling policy to dynamically scale the Auto Scaling group" is incorrect. Simple scaling is not used for maintaining a target utilization. It is used for making simple adjustments up or down based on a threshold value.

INCORRECT: "Use a step scaling policy to dynamically scale the Auto Scaling group" is incorrect. Step scaling is not used for maintaining a target utilization. It is used for making step adjustments that vary based on the size of the alarm breach.

INCORRECT: "Use a scheduled scaling policy to dynamically the Auto Scaling group" is incorrect. Scheduled scaling is not used for maintaining a target utilization. It is used for scheduling changes at specific dates and times.

References:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html

Save time with our AWS cheat sheets:

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

Question 42:

Skipped

A company requires a fully managed replacement for an on-premises storage service. The company's employees often work remotely from various locations. The solution should also be easily accessible to systems connected to the on-premises environment.

Which solution meets these requirements?

- **Use Amazon FSx to create an SMB file share. Connect remote clients to the file share over a client VPN.**

  (Correct)

- **Use AWS Storage Gateway to create a volume gateway to store and transfer files to Amazon S3.**

- **Use AWS Transfer Acceleration to replicate files to Amazon S3 and enable public access.**

- 

Use AWS DataSync to synchronize data between the on-premises service and Amazon S3.

Explanation

Amazon FSx for Windows File Server (Amazon FSx) is a fully managed, highly available, and scalable file storage solution built on Windows Server that uses the Server Message Block (SMB) protocol. It allows for Microsoft Active Directory integration, data deduplication, and fully managed backups, among other critical enterprise features.

An Amazon FSx file system can be created to host the file shares. Clients can then be connected to an AWS Client VPN endpoint and gateway to enable remote access. The protocol used in this solution will be SMB.

CORRECT: "Use Amazon FSx to create an SMB file share. Connect remote clients to the file share over a client VPN" is the correct answer.

INCORRECT: "Use AWS Transfer Acceleration to replicate files to Amazon S3 and enable public access" is incorrect. This is simply a way of improving upload speeds to S3, it is not suitable for enabling internal and external access to a file system.

INCORRECT: "Use AWS DataSync to synchronize data between the on-premises service and Amazon S3" is incorrect. The on-premises solution is to be replaced so this is not a satisfactory solution. Also, DataSync syncs one way, it is not bidirectional.

INCORRECT: "Use AWS Storage Gateway to create a volume gateway to store and transfer files to Amazon S3" is incorrect. Storage Gateway volume gateways are mounted using block-based protocols (iSCSI), so this would not be workable.

References:

https://aws.amazon.com/blogs/storage/accessing-smb-file-shares-remotely-with-amazon-fsx-for-windows-file-server/

Save time with our AWS cheat sheets:

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

Question 43:

Skipped

An application has multiple components for receiving requests that must be processed and subsequently processing the requests. The company requires a solution for decoupling the application components. The application receives around 10,000 requests per day and requests can take up to 2 days to process. Requests that fail to process must be retained.

Which solution meets these requirements most efficiently?

- **Decouple the application components with an Amazon SQS Topic. Configure the receiving component to subscribe to the SNS Topic.**

- **Create an Amazon DynamoDB table and enable DynamoDB streams. Configure the processing component to process requests from the stream.**

- **Decouple the application components with an Amazon SQS queue. Configure a dead-letter queue to collect the requests that failed to process.**

  (Correct)

- **Use an Amazon Kinesis data stream to decouple application components and integrate the processing component with the Kinesis Client Library (KCL).**

Explanation

The Amazon Simple Queue Service (SQS) is ideal for decoupling the application components. Standard queues can support up to 120,000 in flight messages and messages can be retained for up to 14 days in the queue.

To ensure the retention of requests (messages) that fail to process, a dead-letter queue can be configured. Messages that fail to process are sent to the dead-letter queue (based on the redrive policy) and can be subsequently dealt with.

CORRECT: "Decouple the application components with an Amazon SQS queue. Configure a dead-letter queue to collect the requests that failed to process" is the correct answer.

INCORRECT: "Decouple the application components with an Amazon SQS Topic. Configure the receiving component to subscribe to the SNS Topic" is incorrect. SNS does not store requests, it immediately forwards all notifications to subscribers.

INCORRECT: "Use an Amazon Kinesis data stream to decouple application components and integrate the processing component with the Kinesis Client Library (KCL)" is incorrect. This is a less efficient solution and will likely be less cost-effective compared to using Amazon SQS. There is also no option for retention of requests that fail to process.

INCORRECT: "Create an Amazon DynamoDB table and enable DynamoDB streams. Configure the processing component to process requests from the stream" is incorrect. This solution does not offer any way of retaining requests that fail to process of removal of items from the table and is therefore less efficient.

References:

https://aws.amazon.com/sqs/faqs/

https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letter-queues.html

Save time with our AWS cheat sheets:

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

Question 44:

Skipped

An organization is extending a secure development environment into AWS. They have already secured the VPC including removing the Internet Gateway and setting up a Direct Connect connection. What else needs to be done to add encryption?

- **Configure an AWS Direct Connect Gateway**
- **Enable IPSec encryption on the Direct Connect connection**
- **Setup the Border Gateway Protocol (BGP) with encryption**
- **Setup a Virtual Private Gateway (VPG)**

  (Correct)

Explanation

A VPG is used to setup an AWS VPN which you can use in combination with Direct Connect to encrypt all data that traverses the Direct Connect link. This combination provides an IPsec-encrypted private connection that also reduces network costs,

increases bandwidth throughput, and provides a more consistent network experience than internet-based VPN connections.

CORRECT: "Setup a Virtual Private Gateway (VPG)" is the correct answer.

INCORRECT: "Enable IPSec encryption on the Direct Connect connection" is incorrect. There is no option to enable IPSec encryption on the Direct Connect connection.

INCORRECT: "Setup the Border Gateway Protocol (BGP) with encryption" is incorrect. The BGP protocol is not used to enable encryption for Direct Connect, it is used for routing.

INCORRECT: "Configure an AWS Direct Connect Gateway" is incorrect. An AWS Direct Connect Gateway is used to connect to VPCs across multiple AWS regions. It is not involved with encryption.

References:

https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-plus-vpn-network-to-amazon.html

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

Save time with our AWS cheat sheets:

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

Question 45:

Skipped

An application requires a MySQL database which will only be used several times a week for short periods. The database needs to provide automatic instantiation and scaling. Which database service is most suitable?

- **Amazon EC2 instance with MySQL database installed**
- **Amazon RDS MySQL**
- **Amazon Aurora**

- **Amazon Aurora Serverless**

  (Correct)

Explanation
Amazon Aurora Serverless is an on-demand, auto-scaling configuration for Amazon Aurora. The database automatically starts up, shuts down, and scales capacity up or down based on application needs. This is an ideal database solution for infrequently-used applications.

CORRECT: "Amazon Aurora Serverless" is the correct answer.

INCORRECT: "Amazon RDS MySQL" is incorrect as this service requires an instance to be running all the time which is more costly.

INCORRECT: "Amazon EC2 instance with MySQL database installed" is incorrect as this service requires an instance to be running all the time which is more costly.

INCORRECT: "Amazon Aurora" is incorrect as this service requires an instance to be running all the time which is more costly.

References:

https://aws.amazon.com/rds/aurora/serverless/

Save time with our AWS cheat sheets:

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

Question 46:
Skipped
A new application will be launched on an Amazon EC2 instance with an Elastic Block Store (EBS) volume. A solutions architect needs to determine the most cost-effective storage option. The application will have infrequent usage, with peaks of traffic for a couple of hours in the morning and evening. Disk I/O is variable with peaks of up to 3,000 IOPS.

Which solution should the solutions architect recommend?

- **Amazon EBS General Purpose SSD (gp2)**

(Correct)

- **Amazon EBS Throughput Optimized HDD (st1)**
- **Amazon EBS Cold HDD (sc1)**
- **Amazon EBS Provisioned IOPS SSD (io1)**

Explanation

General Purpose SSD (gp2) volumes offer cost-effective storage that is ideal for a broad range of workloads. These volumes deliver single-digit millisecond latencies and the ability to burst to 3,000 IOPS for extended periods of time.

Between a minimum of 100 IOPS (at 33.33 GiB and below) and a maximum of 16,000 IOPS (at 5,334 GiB and above), baseline performance scales linearly at 3 IOPS per GiB of volume size. AWS designs gp2 volumes to deliver their provisioned performance 99% of the time. A gp2 volume can range in size from 1 GiB to 16 TiB.

In this case the volume would have a baseline performance of 3 x 200 = 600 IOPS. The volume could also burst to 3,000 IOPS for extended periods. As the I/O varies, this should be suitable.

CORRECT: "Amazon EBS General Purpose SSD (gp2)" is the correct answer.

INCORRECT: "Amazon EBS Provisioned IOPS SSD (io1) " is incorrect as this would be a more expensive option and is not required for the performance characteristics of this workload.

INCORRECT: "Amazon EBS Cold HDD (sc1)" is incorrect as there is no IOPS SLA for HDD volumes and they would likely not perform well enough for this workload.

INCORRECT: "Amazon EBS Throughput Optimized HDD (st1)" is incorrect as there is no IOPS SLA for HDD volumes and they would likely not perform well enough for this workload.

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 47:

Skipped

A web application in a three-tier architecture runs on a fleet of Amazon EC2 instances. Performance issues have been reported and investigations point to insufficient swap space. The operations team requires monitoring to determine if this is correct.

What should a solutions architect recommend?

- **Configure an Amazon CloudWatch SwapUsage metric dimension. Monitor the SwapUsage dimension in the EC2 metrics in CloudWatch**
- **Enable detailed monitoring in the EC2 console. Create an Amazon CloudWatch SwapUtilization custom metric. Monitor SwapUtilization metrics in CloudWatch**
- **Install an Amazon CloudWatch agent on the instances. Run an appropriate script on a set schedule. Monitor SwapUtilization metrics in CloudWatch**

  (Correct)
- **Use EC2 metadata to collect information, then publish it to Amazon CloudWatch custom metrics. Monitor SwapUsage metrics in CloudWatch**

Explanation

You can use the CloudWatch agent to collect both system metrics and log files from Amazon EC2 instances and on-premises servers. The agent supports both Windows Server and Linux, and enables you to select the metrics to be collected, including sub-resource metrics such as per-CPU core.

There is now a unified agent and previously there were monitoring scripts. Both of these tools can capture SwapUtilization metrics and send them to CloudWatch. This is the best way to get memory utilization metrics from Amazon EC2 instnaces.

CORRECT: "Install an Amazon CloudWatch agent on the instances. Run an appropriate script on a set schedule. Monitor SwapUtilization metrics in CloudWatch" is the correct answer.

INCORRECT: "Enable detailed monitoring in the EC2 console. Create an Amazon CloudWatch SwapUtilization custom metric. Monitor SwapUtilization metrics in CloudWatch" is incorrect as you do not create custom metrics in the console, you must configure the instances to send the metric information to CloudWatch.

INCORRECT: "Configure an Amazon CloudWatch SwapUsage metric dimension. Monitor the SwapUsage dimension in the EC2 metrics in CloudWatch" is incorrect as there is no SwapUsage metric in CloudWatch. All memory metrics must be custom metrics.

INCORRECT: "Use EC2 metadata to collect information, then publish it to Amazon CloudWatch custom metrics. Monitor SwapUsage metrics in CloudWatch" is incorrect as performance related information is not stored in metadata.

References:

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Install-CloudWatch-Agent.html

Save time with our AWS cheat sheets:

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

Question 48:

Skipped

A company has created a duplicate of its environment in another AWS Region. The application is running in warm standby mode. There is an Application Load Balancer (ALB) in front of the application. Currently, failover is manual and requires updating a DNS alias record to point to the secondary ALB.

How can a solutions architect automate the failover process?

- **Create a CNAME record on Amazon Route 53 pointing to the ALB endpoint**
- **Create a latency based routing policy on Amazon Route 53**
- **Enable an Amazon Route 53 health check**

  (Correct)

- **Enable an ALB health check**

Explanation

You can use Route 53 to check the health of your resources and only return healthy resources in response to DNS queries. There are three types of DNS failover configurations:

1. Active-passive: Route 53 actively returns a primary resource. In case of failure, Route 53 returns the backup resource. Configured using a failover policy.

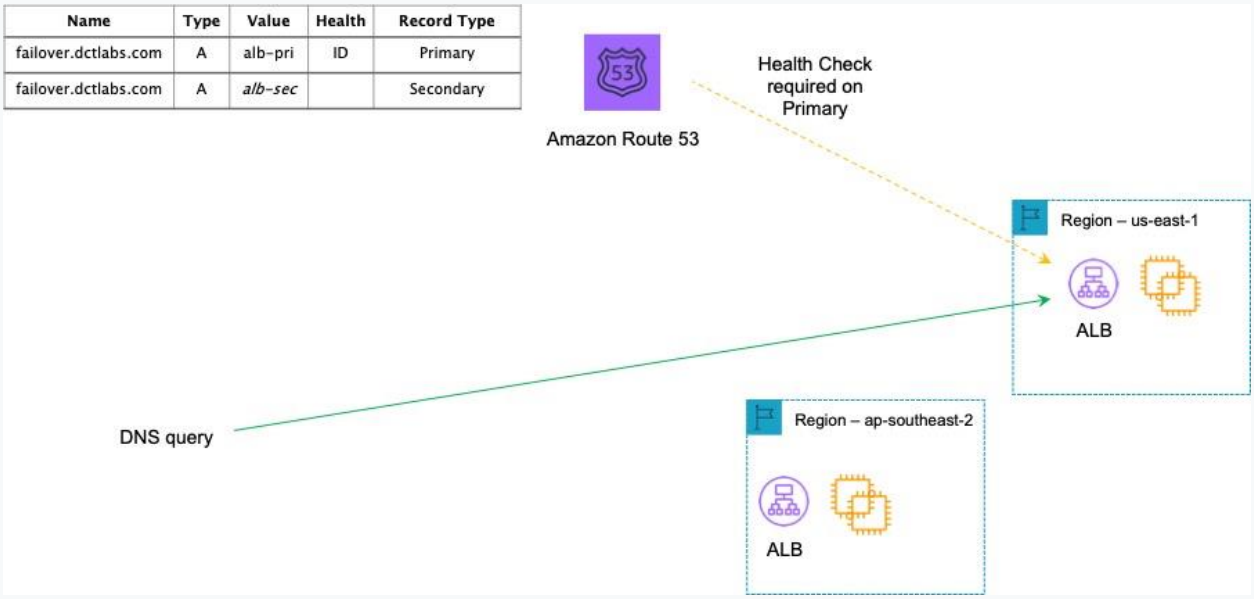
2. Active-active: Route 53 actively returns more than one resource. In case of failure, Route 53 fails back to the healthy resource. Configured using any routing policy besides failover.

3. Combination: Multiple routing policies (such as latency-based, weighted, etc.) are combined into a tree to configure more complex DNS failover.

In this case an alias already exists for the secondary ALB. Therefore, the solutions architect just needs to enable a failover configuration with an Amazon Route 53 health check.

The configuration would look something like this:

Name	Type	Value	Health	Record Type
failover.dctlabs.com	A	alb-pri	ID	Primary
failover.dctlabs.com	A	*alb-sec*		Secondary



CORRECT: "Enable an Amazon Route 53 health check" is the correct answer.

INCORRECT: "Enable an ALB health check" is incorrect. The point of an ALB health check is to identify the health of targets (EC2 instances). It cannot redirect clients to another Region.

INCORRECT: "Create a CNAME record on Amazon Route 53 pointing to the ALB endpoint" is incorrect as an Alias record already exists and is better for mapping to an ALB.

INCORRECT: "Create a latency based routing policy on Amazon Route 53" is incorrect as this will only take into account latency, it is not used for failover.

References:

https://aws.amazon.com/premiumsupport/knowledge-center/route-53-dns-health-checks/

Save time with our AWS cheat sheets:

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

Question 49:

Skipped

A company runs a containerized application on an Amazon Elastic Kubernetes Service (EKS) using a microservices architecture. The company requires a solution to collect, aggregate, and summarize metrics and logs. The solution should provide a centralized dashboard for viewing information including CPU and memory utilization for EKS namespaces, services, and pods.

Which solution meets these requirements?

- **Run the Amazon CloudWatch agent in the existing EKS cluster. View the metrics and logs in the CloudWatch console.**
- **Configure AWS X-Ray to enable tracing for the EKS microservices. Query the trace data using Amazon Elasticsearch.**
- **Migrate the containers to Amazon ECS and enable Amazon CloudWatch Container Insights. View the metrics and logs in the CloudWatch console.**

- **Configure Amazon CloudWatch Container Insights in the existing EKS cluster. View the metrics and logs in the CloudWatch console.**

  (Correct)

Explanation
Use CloudWatch Container Insights to collect, aggregate, and summarize metrics and logs from your containerized applications and microservices. Container Insights is available for Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS), and Kubernetes platforms on Amazon EC2.

With Container Insights for EKS you can see the top contributors by memory or CPU, or the most recently active resources. This is available when you select any of the following dashboards in the drop-down box near the top of the page:

- ECS Services
- ECS Tasks
- EKS Namespaces
- EKS Services
- EKS Pods

CORRECT: "Configure Amazon CloudWatch Container Insights in the existing EKS cluster. View the metrics and logs in the CloudWatch console" is the correct answer.

INCORRECT: "Run the Amazon CloudWatch agent in the existing EKS cluster. View the metrics and logs in the CloudWatch console" is incorrect. Container Insights is the best way to view the required data.

INCORRECT: "Migrate the containers to Amazon ECS and enable Amazon CloudWatch Container Insights. View the metrics and logs in the CloudWatch console" is incorrect. There is no need to migrate containers to ECS as EKS is supported for Container Insights.

INCORRECT: "Configure AWS X-Ray to enable tracing for the EKS microservices. Query the trace data using Amazon Elasticsearch" is incorrect. X-Ray will not deliver the required statistics to a centralized dashboard.

References:

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/ContainerInsights.html

Save time with our AWS cheat sheets:

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

Question 50:

Skipped

A web app allows users to upload images for viewing online. The compute layer that processes the images is behind an Auto Scaling group. The processing layer should be decoupled from the front end and the ASG needs to dynamically adjust based on the number of images being uploaded.

How can this be achieved?

- **Create a target tracking policy that keeps the ASG at 70% CPU utilization**
- **Create a scheduled policy that scales the ASG at times of expected peak load**
- **Create an Amazon SQS queue and custom CloudWatch metric to measure the number of messages in the queue. Configure the ASG to scale based on the number of messages in the queue**

  (Correct)
- **Create an Amazon SNS Topic to generate a notification each time a message is uploaded. Have the ASG scale based on the number of SNS messages**

Explanation

The best solution is to use Amazon SQS to decouple the front end from the processing compute layer. To do this you can create a custom CloudWatch metric that measures the number of messages in the queue and then configure the ASG to scale using a target tracking policy that tracks a certain value.

CORRECT: "Create an Amazon SQS queue and custom CloudWatch metric to measure the number of messages in the queue. Configure the ASG to scale based on the number of messages in the queue" is the correct answer.

INCORRECT: "Create an Amazon SNS Topic to generate a notification each time a message is uploaded. Have the ASG scale based on the number of SNS messages" is incorrect. The Amazon Simple Notification Service (SNS) is used for sending notifications using topics. Amazon SQS is a better solution for this scenario as it provides a decoupling mechanism where the actual images can be stored for processing. SNS does not provide somewhere for the images to be stored.

INCORRECT: "Create a target tracking policy that keeps the ASG at 70% CPU utilization" is incorrect. Using a target tracking policy with the ASG that tracks CPU utilization does not allow scaling based on the number of images being uploaded.

INCORRECT: "Create a scheduled policy that scales the ASG at times of expected peak load" is incorrect. Using a scheduled policy is less dynamic as though you may be able to predict usage patterns, it would be better to adjust dynamically based on actual usage.

References:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html

Save time with our AWS cheat sheets:

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

Question 51:

Skipped

A Solutions Architect working for a large financial institution is building an application to manage their customers financial information and their sensitive personal information. The Solutions Architect requires that the storage layer can store immutable data out of the box, with the ability to encrypt the data at rest and requires that the storage layer provides ACID properties. They also want to use a containerized solution to manage the compute layer.

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

- **Create a cluster of ECS instances on AWS Fargate within an Auto Scaling Group behind an Application Load Balancer. To manage the storage layer, use Amazon S3.**
-

Set up an ECS cluster behind an Application Load Balancer on AWS Fargate. Use Amazon Quantum Ledger Database (QLDB) to manage the storage layer.

(Correct)

- **Create an Auto Scaling Group with EC2 instances behind an Application Load Balancer. To manage the storage layer, use Amazon S3.**

- **Configure an ECS cluster on EC2 behind an Application Load Balancer within an Auto Scaling Group. Store data using Amazon DynamoDB.**

Explanation

The solution requires that the storage layer be immutable. This immutability can only be delivered by Amazon Quantum Ledger Database (QLDB), as Amazon QLDB has a built-in immutable journal that stores an accurate and sequenced entry of every data change. The journal is append-only, meaning that data can only be added to a journal, and it cannot be overwritten or deleted.

Secondly the compute layer needs to not only be containerized, and implemented with the least possible operational overhead. The option that best fits these requirements is Amazon ECS on AWS Fargate, as AWS Fargate is a Serverless, containerized deployment option.

CORRECT: "Set up an ECS cluster behind an Application Load Balancer on AWS Fargate. Use Amazon Quantum Ledger Database (QLDB) to manage the storage layer" is the correct answer (as explained above.)

INCORRECT: "Create an Auto Scaling Group with EC2 instances behind an Application Load Balancer. To manage the storage layer, use Amazon S3" is incorrect. EC2 instances are virtual machines, not a container product and Amazon S3 is an object storage service which does not act as an immutable storage layer.

INCORRECT: "Configure an ECS cluster on EC2 behind an Application Load Balancer within an Auto Scaling Group. Store data using Amazon DynamoDB" is incorrect. ECS on EC2 provides a higher level of operational overhead than using AWS Fargate, as Fargate is a Serverless service.

INCORRECT: "Create a cluster of ECS instances on AWS Fargate within an Auto Scaling Group behind an Application Load Balancer. To manage the storage layer, use Amazon S3" is incorrect. Although Fargate would be a suitable deployment option, Amazon S3 is not suitable for the storage layer as it is not immutable by default.

References:

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

Save time with our AWS cheat sheets:

https://digitalcloud.training/category/aws-cheat-sheets/aws-solutions-architect-associate/aws-database-saa/

Question 52:

Skipped

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

- **Amazon RDS**
- **Amazon ElastiCache**
- **Amazon DynamoDB**

  (Correct)
- **Amazon RedShift**

Explanation

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

CORRECT: "Amazon DynamoDB" is the correct answer.

INCORRECT: "Amazon RDS" is incorrect. Amazon RDS is a relational (SQL) type of database, not a key-value / nonrelational database.

INCORRECT: "Amazon RedShift" is incorrect. Amazon RedShift is a data warehouse service used for online analytics processing (OLAP) workloads.

INCORRECT: "Amazon ElastiCache" is incorrect. Amazon ElastiCache is an in-memory caching database. This is not a nonrelational key-value database.

References:

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

Save time with our AWS cheat sheets:

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

Question 53:

Skipped

A company runs a financial application using an Amazon EC2 Auto Scaling group behind an Application Load Balancer (ALB). When running month-end reports on a specific day and time each month the application becomes unacceptably slow. Amazon CloudWatch metrics show the CPU utilization hitting 100%.

What should a solutions architect recommend to ensure the application is able to handle the workload and avoid downtime?

- **Configure an Amazon CloudFront distribution in front of the ALB**
- **Configure Amazon ElastiCache to remove some of the workload from the EC2 instances**
- **Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization**
- **Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule**

  (Correct)

Explanation

Scheduled scaling allows you to set your own scaling schedule. In this case the scaling action can be scheduled to occur just prior to the time that the reports will be run each month. Scaling actions are performed automatically as a function of time and date. This

will ensure that there are enough EC2 instances to serve the demand and prevent the application from slowing down.

CORRECT: "Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule" is the correct answer.

INCORRECT: "Configure an Amazon CloudFront distribution in front of the ALB" is incorrect as this would be more suitable for providing access to global users by caching content.

INCORRECT: "Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization" is incorrect as this would not prevent the slow-down from occurring as there would be a delay between when the CPU hits 100% and the metric being reported and additional instances being launched.

INCORRECT: "Configure Amazon ElastiCache to remove some of the workload from the EC2 instances" is incorrect as ElastiCache is a database cache, it cannot replace the compute functions of an EC2 instance.

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 54:

Skipped

A company has deployed an application that consists of several microservices running on Amazon EC2 instances behind an Amazon API Gateway API. A Solutions Architect is concerned that the microservices are not designed to elastically scale when large increases in demand occur.

Which solution addresses this concern?

- **Use an Elastic Load Balancer to distribute the traffic between the microservices. Configure Amazon CloudWatch metrics to monitor traffic to the microservices.**

Spread the microservices across multiple Availability Zones and configure Amazon Data Lifecycle Manager to take regular snapshots.

- 

Create an Amazon SQS queue to store incoming requests. Configure the microservices to retrieve the requests from the queue for processing.

(Correct)

- 

Use Amazon CloudWatch alarms to notify operations staff when the microservices are suffering high CPU utilization.

Explanation

The individual microservices are not designed to scale. Therefore, the best way to ensure they are not overwhelmed by requests is to decouple the requests from the microservices. An Amazon SQS queue can be created, and the API Gateway can be configured to add incoming requests to the queue. The microservices can then pick up the requests from the queue when they are ready to process them.

CORRECT: "Create an Amazon SQS queue to store incoming requests. Configure the microservices to retrieve the requests from the queue for processing" is the correct answer.

INCORRECT: "Use Amazon CloudWatch alarms to notify operations staff when the microservices are suffering high CPU utilization" is incorrect. This solution requires manual intervention and does not help the application to elastically scale.

INCORRECT: "Spread the microservices across multiple Availability Zones and configure Amazon Data Lifecycle Manager to take regular snapshots" is incorrect. This does not automate the elasticity of the application.

INCORRECT: "Use an Elastic Load Balancer to distribute the traffic between the microservices. Configure Amazon CloudWatch metrics to monitor traffic to the microservices" is incorrect. You cannot use an ELB spread traffic across many different individual microservices as the requests must be directed to individual microservices. Therefore, you would need a target group per microservice, and you would need Auto Scaling to scale the microservices.

References:

https://aws.amazon.com/blogs/compute/understanding-asynchronous-messaging-for-microservices/

Save time with our AWS cheat sheets:

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

Question 55:

Skipped

A Solutions Architect is designing a solution for an application that requires very low latency between the client and the backend. The application uses the UDP protocol, and the backend is hosted on Amazon EC2 instances. The solution must be highly available across multiple Regions and users around the world should be directed to the most appropriate Region based on performance.

How can the Solutions Architect meet these requirements?

- **Deploy Amazon EC2 instances in multiple Regions. Create a multivalue answer routing record in Amazon Route 53 that includes all EC2 endpoints.**

- **Deploy a Network Load Balancer in front of the EC2 instances in each Region. Use AWS Global Accelerator to route traffic to the most optimal Regional endpoint.**

  (Correct)

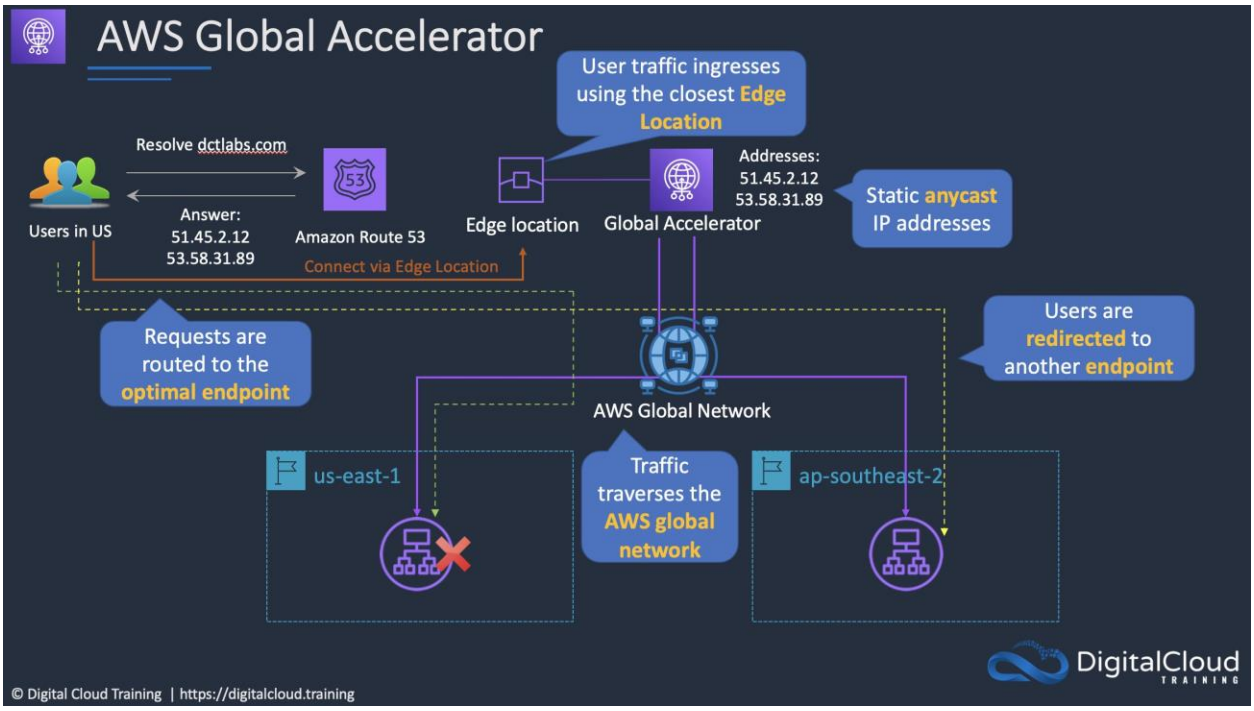
- **Deploy an Application Load Balancer in front of the EC2 instances in each Region. Use AWS WAF to direct traffic to the most optimal Regional endpoint.**

- **Deploy an Amazon CloudFront distribution with a custom origin pointing to Amazon EC2 instances in multiple Regions.**

Explanation

An NLB is ideal for latency-sensitive applications and can listen on UDP for incoming requests. As Elastic Load Balancers are region-specific it is necessary to have an NLB in each Region in front of the EC2 instances.

To direct traffic based on optimal performance, AWS Global Accelerator can be used. GA will ensure traffic is routed across the AWS global network to the most optimal endpoint based on performance.



CORRECT: "Deploy a Network Load Balancer in front of the EC2 instances in each Region. Use AWS Global Accelerator to route traffic to the most optimal Regional endpoint" is the correct answer.

INCORRECT: "Deploy an Application Load Balancer in front of the EC2 instances in each Region. Use AWS WAF to direct traffic to the most optimal Regional endpoint" is incorrect. You cannot use WAF to direct traffic to endpoints based on performance.

INCORRECT: "Deploy an Amazon CloudFront distribution with a custom origin pointing to Amazon EC2 instances in multiple Regions" is incorrect. CloudFront cannot listen on UDP, it is used for HTTP/HTTPS.

INCORRECT: "Deploy Amazon EC2 instances in multiple Regions. Create a multivalue answer routing record in Amazon Route 53 that includes all EC2 endpoints" is incorrect. This configuration would not route incoming requests to the most optimal endpoint based on performance, it would provide multiple records in answers and traffic would be distributed across multiple Regions.

References:

https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works.html

Save time with our AWS cheat sheets:

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

Question 56:

Skipped

An application is deployed on multiple AWS regions and accessed from around the world. The application exposes static public IP addresses. Some users are experiencing poor performance when accessing the application over the Internet.

What should a solutions architect recommend to reduce internet latency?

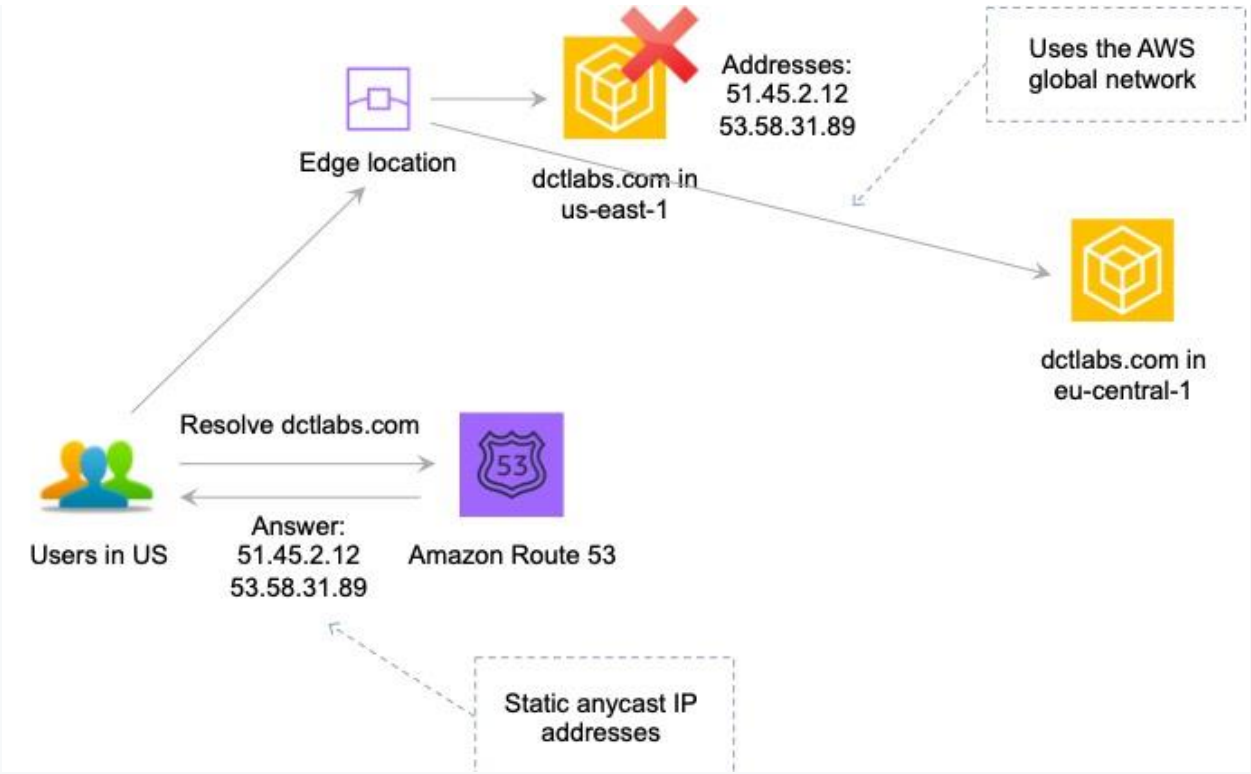
- **Set up an Amazon Route 53 geoproximity routing policy to route traffic**
- **Set up AWS Global Accelerator and add endpoints**

  (Correct)
- **Set up AWS Direct Connect locations in multiple Regions**
- **Set up an Amazon CloudFront distribution to access an application**

Explanation

AWS Global Accelerator is a service in which you create *accelerators* to improve availability and performance of your applications for local and global users. Global Accelerator directs traffic to optimal endpoints over the AWS global network. This improves the availability and performance of your internet applications that are used by a global audience. Global Accelerator is a global service that supports endpoints in multiple AWS Regions, which are listed in the AWS Region Table.

By default, Global Accelerator provides you with two static IP addresses that you associate with your accelerator. (Or, instead of using the IP addresses that Global Accelerator provides, you can configure these entry points to be IPv4 addresses from your own IP address ranges that you bring to Global Accelerator.)



The static IP addresses are anycast from the AWS edge network and distribute incoming application traffic across multiple endpoint resources in multiple AWS Regions, which increases the availability of your applications. Endpoints can be Network Load Balancers, Application Load Balancers, EC2 instances, or Elastic IP addresses that are located in one AWS Region or multiple Regions.

CORRECT: "Set up AWS Global Accelerator and add endpoints" is the correct answer.

INCORRECT: "Set up AWS Direct Connect locations in multiple Regions" is incorrect as this is used to connect from an on-premises data center to AWS. It does not improve performance for users who are not connected to the on-premises data center.

INCORRECT: "Set up an Amazon CloudFront distribution to access an application" is incorrect as CloudFront cannot expose static public IP addresses.

INCORRECT: "Set up an Amazon Route 53 geoproximity routing policy to route traffic" is incorrect as this does not reduce internet latency as well as using Global Accelerator. GA will direct users to the closest edge location and then use the AWS global network.

References:

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

Save time with our AWS cheat sheets:

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

Question 57:

Skipped

A company is creating a solution that must offer disaster recovery across multiple AWS Regions. The solution requires a relational database that can support a Recovery Point Objective (RPO) of 1 second and a Recovery Time Objective (RTO) of 1 minute.

Which AWS solution can achieve this?

- **Amazon RDS for with a cross-Region replica.**
- **Amazon Aurora Global Database.**

  (Correct)
- **Amazon RDS for with Multi-AZ enabled.**
- **Amazon DynamoDB global tables.**

Explanation

Aurora Global Database lets you easily scale database reads across the world and place your applications close to your users. Your applications enjoy quick data access regardless of the number and location of secondary regions, with typical cross-region replication latencies below 1 second.

If your primary region suffers a performance degradation or outage, you can promote one of the secondary regions to take read/write responsibilities. An Aurora cluster can recover in less than 1 minute even in the event of a complete regional outage. This provides your application with an effective Recovery Point Objective (RPO) of 1 second and a Recovery Time Objective (RTO) of less than 1 minute, providing a strong foundation for a global business continuity plan.

CORRECT: "Amazon Aurora Global Database" is the correct answer.

INCORRECT: "Amazon RDS for with Multi-AZ enabled" is incorrect. RDS Multi-AZ is across availability zones, not across Regions.

INCORRECT: "Amazon RDS for with a cross-Region replica" is incorrect. A cross-Region replica for RDS cannot provide an RPO of 1 second as there is typically more latency. You also cannot achieve a minute RPO as it takes much longer to promote a replica to a master.

INCORRECT: "Amazon DynamoDB global tables" is incorrect. This is not a relational database; it is a non-relational database (NoSQL).

References:

https://aws.amazon.com/rds/aurora/global-database/

Save time with our AWS cheat sheets:

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

Question 58:

Skipped

A company runs a business-critical application in the us-east-1 Region. The application uses an Amazon Aurora MySQL database cluster which is 2 TB in size. A Solutions Architect needs to determine a disaster recovery strategy for failover to the us-west-2 Region. The strategy must provide a recovery time objective (RTO) of 10 minutes and a recovery point objective (RPO) of 5 minutes.

Which strategy will meet these requirements?

- **Recreate the database as an Aurora global database with the primary DB cluster in us-east-1 and a secondary DB cluster in us-west-2. Use an Amazon EventBridge rule that invokes an AWS Lambda function to promote the DB cluster in us-west-2 when failure is detected.**

  (Correct)

- **Create a cross-Region Aurora MySQL read replica in us-west-2 Region. Configure an Amazon EventBridge rule that invokes an AWS Lambda function that promotes the read replica in us-west-2 when failure is detected.**

-

Create a multi-Region Aurora MySQL DB cluster in us-east-1 and us-west-2. Use an Amazon Route 53 health check to monitor us-east-1 and fail over to us-west-2 upon failure.

-

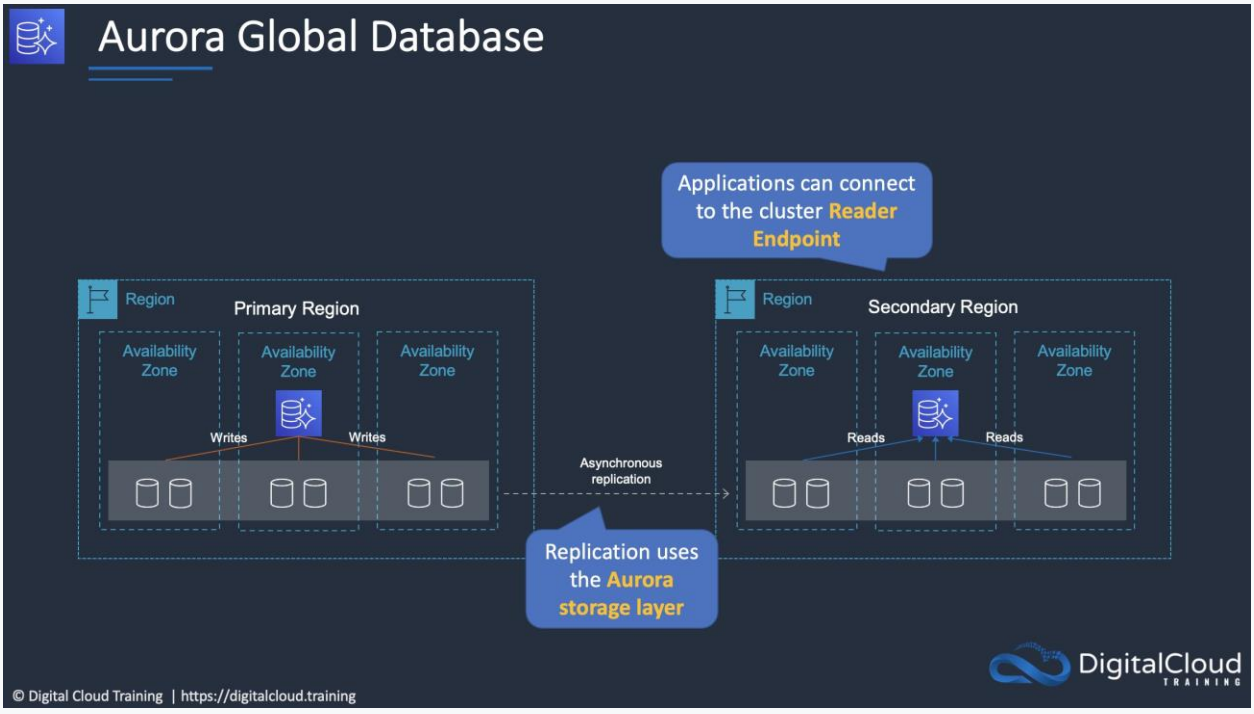
Recreate the database as an Aurora multi master cluster across the us-east-1 and us-west-2 Regions with multiple writers to allow read/write capabilities from all database instances.

Explanation

Amazon Aurora Global Database is designed for globally distributed applications, allowing a single Amazon Aurora database to span multiple AWS regions. It replicates your data with no impact on database performance, enables fast local reads with low latency in each region, and provides disaster recovery from region-wide outages

If your primary region suffers a performance degradation or outage, you can promote one of the secondary regions to take read/write responsibilities. An Aurora cluster can recover in less than 1 minute even in the event of a complete regional outage.

This provides your application with an effective Recovery Point Objective (RPO) of 1 second and a Recovery Time Objective (RTO) of less than 1 minute, providing a strong foundation for a global business continuity plan



CORRECT: "Recreate the database as an Aurora global database with the primary DB cluster in us-east-1 and a secondary DB cluster in us-west-2. Use an Amazon

EventBridge rule that invokes an AWS Lambda function to promote the DB cluster in us-west-2 when failure is detected" is the correct answer.

INCORRECT: "Create a multi-Region Aurora MySQL DB cluster in us-east-1 and us-west-2. Use an Amazon Route 53 health check to monitor us-east-1 and fail over to us-west-2 upon failure" is incorrect. You cannot create a multi-Region Aurora MySQL DB cluster. Options are to create MySQL Replicas (may meet the RTO objectives), or to use global database.

INCORRECT: "Create a cross-Region Aurora MySQL read replica in us-west-2 Region. Configure an Amazon EventBridge rule that invokes an AWS Lambda function that promotes the read replica in us-west-2 when failure is detected" is incorrect. This may not meet the RTO objectives as large databases may well take more than 10 minutes to promote.

INCORRECT: "Recreate the database as an Aurora multi master cluster across the us-east-1 and us-west-2 Regions with multiple writers to allow read/write capabilities from all database instances" is incorrect. Multi master only works within a Region it does not work across Regions.

References:

https://aws.amazon.com/rds/aurora/global-database/

Save time with our AWS cheat sheets:

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

Question 59:

Skipped

A company's staff connect from home office locations to administer applications using bastion hosts in a single AWS Region. The company requires a resilient bastion host architecture that requires minimal ongoing operational overhead.

How can a Solutions Architect best meet these requirements?

- **Create a Network Load Balancer backed by an Auto Scaling group with instances in multiple Availability Zones.**

  (Correct)

-

Create a Network Load Balancer backed by the existing servers in different Availability Zones.

- 

  Create a Network Load Balancer backed by Reserved Instances in a cluster placement group.

- 

  Create a Network Load Balancer backed by an Auto Scaling group with instances in multiple AWS Regions.

Explanation

Bastion hosts (aka “jump hosts”) are EC2 instances in public subnets that administrators and operations staff can connect to from the internet. From the bastion host they are then able to connect to other instances and applications within AWS by using internal routing within the VPC.

All answers use a Network Load Balancer which is acceptable for forwarding incoming connections to targets. The differences are in where the connections are forwarded to. The best option is to create an Auto Scaling group with EC2 instances in multiple Availability Zones. This creates a resilient architecture within a single AWS Region which is exactly what the question asks for.

CORRECT: "Create a Network Load Balancer backed by an Auto Scaling group with instances in multiple Availability Zones" is the correct answer.

INCORRECT: "Create a Network Load Balancer backed by an Auto Scaling group with instances in multiple AWS Regions" is incorrect. You cannot have instances in an ASG across multiple Regions and you can’t have an NLB distribute connections across multiple Regions.

INCORRECT: "Create a Network Load Balancer backed by Reserved Instances in a cluster placement group" is incorrect. A cluster placement group packs instances close together inside an Availability Zone. This strategy enables workloads to achieve the low-latency network performance necessary for tightly coupled node-to-node communication that is typical of HPC applications.

INCORRECT: "Create a Network Load Balancer backed by the existing servers in different Availability Zones" is incorrect. An Auto Scaling group is required to maintain instances in different AZs for resilience.

References:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-benefits.html

Save time with our AWS cheat sheets:

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

Question 60:

Skipped

A Solutions Architect works for a company looking to centralize its Machine Learning Operations. Currently they have a large amount of existing cloud storage to store their operational data which is used for machine learning analysis. There is some data which exists within an Amazon RDS MySQL database, and they need a solution which can easily retrieve data from the database.

Which service can be used to build a centralized data repository to be used for Machine Learning purposes?

- **Amazon Neptune**
- **Amazon Quantum Ledger Database (QLDB)**
- **AWS Lake Formation**

  (Correct)
- **Amazon S3**

Explanation

AWS Lake Formation is a service that makes it easy to set up a secure data lake in days. A data lake is a centralized, curated, and secured repository that stores all your data, both in its original form and prepared for analysis. With AWS Lake Formation, you can import data from MySQL, PostgreSQL, SQL Server, MariaDB, and Oracle databases running in Amazon Relational Database Service (RDS) or hosted in Amazon Elastic Compute Cloud (EC2). Both bulk and incremental data loading are supported.

CORRECT: "AWS Lake Formation" is the correct answer (as explained above.)

INCORRECT: "Amazon S3" is incorrect. Amazon Simple Storage Service (Amazon S3) is an object storage service offering industry-leading scalability, data availability, security,

and performance. It is not however suitable for directly retrieving data from MySQL on RDS and using the data for a Machine learning use case.

INCORRECT: "Amazon Quantum Ledger Database" is incorrect. Amazon Quantum Ledger Database (QLDB) is a fully managed ledger database that provides a transparent, immutable, and cryptographically verifiable transaction log. It is not suitable for directly retrieving data from MySQL on RDS and using the data for a Machine learning use case.

INCORRECT: "Amazon Neptune" is incorrect. Amazon Neptune is a fast, reliable, fully managed graph database service that makes it easy to build and run applications. It is not suitable for directly retrieving data from MySQL on RDS and using the data for a Machine learning use case.

References:

https://aws.amazon.com/lake-formation/features/

Save time with our AWS cheat sheets:

https://digitalcloud.training/category/aws-cheat-sheets/aws-solutions-architect-associate/aws-storage-saa/

Question 61:

Skipped

A gaming company collects real-time data and stores it in an on-premises database system. The company are migrating to AWS and need better performance for the database. A solutions architect has been asked to recommend an in-memory database that supports data replication.

Which database should a solutions architect recommend?

- **Amazon ElastiCache for Redis**

  (Correct)

- **Amazon RDS for PostgreSQL**

-

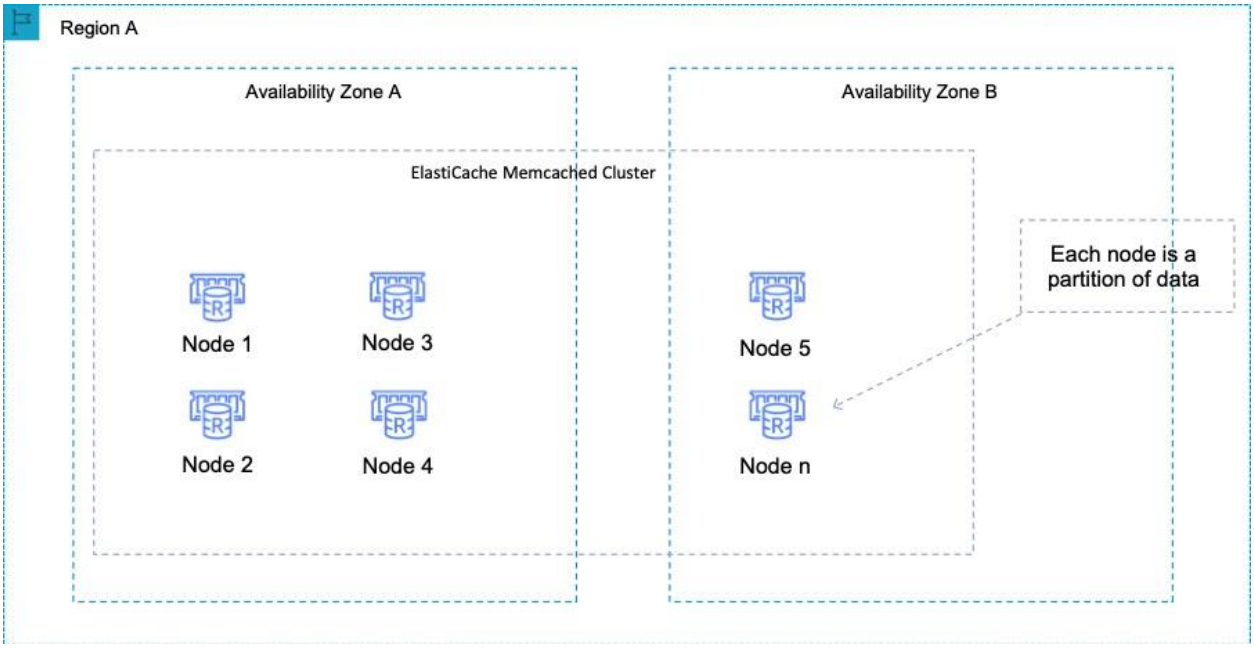
Amazon ElastiCache for Memcached

-

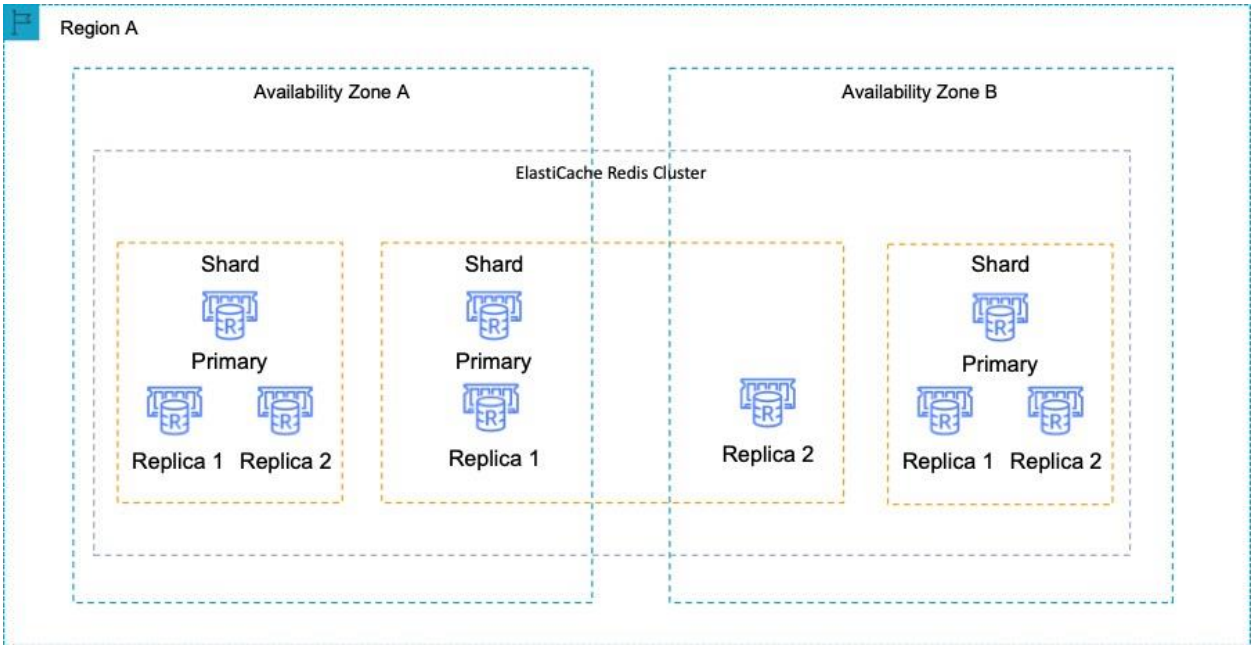
Amazon RDS for MySQL

Explanation

Amazon ElastiCache is an in-memory database. With ElastiCache Memcached there is no data replication or high availability. As you can see in the diagram, each node is a separate partition of data:



Therefore, the Redis engine must be used which does support both data replication and clustering. The following diagram shows a Redis architecture with cluster mode enabled:



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

INCORRECT: "Amazon ElastiCache for Memcached" is incorrect as Memcached does not support data replication or high availability.

INCORRECT: "Amazon RDS for MySQL" is incorrect as this is not an in-memory database.

INCORRECT: "Amazon RDS for PostgreSQL" is incorrect as this is not an in-memory database.

References:

https://aws.amazon.com/elasticache/redis/

Save time with our AWS cheat sheets:

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

Question 62:

Skipped

A production application runs on an Amazon RDS MySQL DB instance. A solutions architect is building a new reporting tool that will access the same data. The reporting tool must be highly available and not impact the performance of the production application.

How can this be achieved?

- **Use Amazon Data Lifecycle Manager to automatically create and manage snapshots**

- **Create a cross-region Multi-AZ deployment and create a read replica in the second region**

- **Create a Single-AZ RDS Read Replica of the production RDS DB instance. Create a second Single-AZ RDS Read Replica from the replica**

- **Create a Multi-AZ RDS Read Replica of the production RDS DB instance**

  (Correct)

Explanation
You can create a read replica as a Multi-AZ DB instance. Amazon RDS creates a standby of your replica in another Availability Zone for failover support for the replica. Creating your read replica as a Multi-AZ DB instance is independent of whether the source database is a Multi-AZ DB instance.

CORRECT: "Create a Multi-AZ RDS Read Replica of the production RDS DB instance" is the correct answer.

INCORRECT: "Create a Single-AZ RDS Read Replica of the production RDS DB instance. Create a second Single-AZ RDS Read Replica from the replica" is incorrect. Read replicas are primarily used for horizontal scaling. The best solution for high availability is to use a Multi-AZ read replica.

INCORRECT: "Create a cross-region Multi-AZ deployment and create a read replica in the second region" is incorrect as you cannot create a cross-region Multi-AZ deployment with RDS.

INCORRECT: "Use Amazon Data Lifecycle Manager to automatically create and manage snapshots" is incorrect as using snapshots is not the best solution for high availability.

References:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_MySQL.Replication.ReadReplicas.html#USER_MySQL.Replication.ReadReplicas.MultiAZ

Save time with our AWS cheat sheets:

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

Question 63:

Skipped

A web application is running on a fleet of Amazon EC2 instances using an Auto Scaling Group. It is desired that the CPU usage in the fleet is kept at 40%.

How should scaling be configured?

- **Use a step scaling policy that uses the PercentChangeInCapacity value to adjust the group size as required**
- **Use a simple scaling policy that launches instances when the average CPU hits 40%**
- **Use a custom CloudWatch alarm to monitor CPU usage and notify the ASG using Amazon SNS**
- **Use a target tracking policy that keeps the average aggregate CPU utilization at 40%**

(Correct)

Explanation

This is a perfect use case for a target tracking scaling policy. With target tracking scaling policies, you select a scaling metric and set a target value. In this case you can just set the target value to 40% average aggregate CPU utilization.

CORRECT: "Use a target tracking policy that keeps the average aggregate CPU utilization at 40%" is the correct answer.

INCORRECT: "Use a simple scaling policy that launches instances when the average CPU hits 40%" is incorrect. A simple scaling policy will add instances when 40% CPU utilization is reached, but it is not designed to maintain 40% CPU utilization across the group.

INCORRECT: "Use a step scaling policy that uses the PercentChangeInCapacity value to adjust the group size as required" is incorrect. The step scaling policy makes scaling adjustments based on a number of factors. The PercentChangeInCapacity value increments or decrements the group size by a specified percentage. This does not relate to CPU utilization.

INCORRECT: "Use a custom CloudWatch alarm to monitor CPU usage and notify the ASG using Amazon SNS" is incorrect. You do not need to create a custom Amazon CloudWatch alarm as the ASG can scale using a policy based on CPU utilization using standard configuration.

References:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-simple-step.html

Save time with our AWS cheat sheets:

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

Question 64:

Skipped

A company operates a production web application that uses an Amazon RDS MySQL database. The database has automated, non-encrypted daily backups. To increase the security of the data, it has been recommended that encryption should be enabled for backups. Unencrypted backups will be destroyed after the first encrypted backup has been completed.

What should be done to enable encryption for future backups?

- **Create a snapshot of the database. Copy it to an encrypted snapshot. Restore the database from the encrypted snapshot**

  (Correct)

-

Enable an encrypted read replica on RDS for MySQL. Promote the encrypted read replica to primary. Remove the original database instance

- 

Modify the backup section of the database configuration to toggle the Enable encryption check box

- 

Enable default encryption for the Amazon S3 bucket where backups are stored

Explanation

Amazon RDS uses snapshots for backup. Snapshots are encrypted when created only if the database is encrypted and you can only select encryption for the database when you first create it. In this case the database, and hence the snapshots, ad unencrypted.

However, you can create an encrypted copy of a snapshot. You can restore using that snapshot which creates a new DB instance that has encryption enabled. From that point on encryption will be enabled for all snapshots.

CORRECT: "Create a snapshot of the database. Copy it to an encrypted snapshot. Restore the database from the encrypted snapshot" is the correct answer.

INCORRECT: "Enable an encrypted read replica on RDS for MySQL. Promote the encrypted read replica to primary. Remove the original database instance" is incorrect as you cannot create an encrypted read replica from an unencrypted master.

INCORRECT: "Modify the backup section of the database configuration to toggle the Enable encryption check box" is incorrect as you cannot add encryption for an existing database.

INCORRECT: "Enable default encryption for the Amazon S3 bucket where backups are stored" is incorrect because you do not have access to the S3 bucket in which snapshots are stored.

References:

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

Save time with our AWS cheat sheets:

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

Question 65:

Skipped

A company has experienced malicious traffic from some suspicious IP addresses. The security team discovered the requests are from different IP addresses under the same CIDR range.

What should a solutions architect recommend to the team?

- **Add a deny rule in the outbound table of the network ACL with a lower rule number than other rules**
- **Add a rule in the inbound table of the security group to deny the traffic from that CIDR range**
- **Add a rule in the outbound table of the security group to deny the traffic from that CIDR range**
- **Add a deny rule in the inbound table of the network ACL with a lower rule number than other rules**

(Correct)

Explanation

You can only create deny rules with network ACLs, it is not possible with security groups. Network ACLs process rules in order from the lowest numbered rules to the highest until they reach and allow or deny. The following table describes some of the differences between security groups and network ACLs:

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

Therefore, the solutions architect should add a deny rule in the inbound table of the network ACL with a lower rule number than other rules.

CORRECT: "Add a deny rule in the inbound table of the network ACL with a lower rule number than other rules" is the correct answer.

INCORRECT: "Add a deny rule in the outbound table of the network ACL with a lower rule number than other rules" is incorrect as this will only block outbound traffic.

INCORRECT: "Add a rule in the inbound table of the security group to deny the traffic from that CIDR range" is incorrect as you cannot create a deny rule with a security group.

INCORRECT: "Add a rule in the outbound table of the security group to deny the traffic from that CIDR range" is incorrect as you cannot create a deny rule with a security group.

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/