AWS Certified Solutions Architect Associate Practice Test 5 - 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 new department will begin using AWS services an AWS account and a Solutions Architect needs to create an authentication and authorization strategy. Select the correct statements regarding IAM groups? (choose 2)

- **IAM groups can be nested up to 4 levels**
- **An IAM group is not an identity and cannot be identified as a principal in an IAM policy**

  (Correct)
- **IAM groups can be used to group EC2 instances**
- **IAM groups can be used to assign permissions to users**

  (Correct)
- **IAM groups can temporarily assume a role to take on permissions for a specific task**

Explanation
An IAM group is a collection of IAM users. Groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users.

The following facts apply to IAM Groups:

- Groups are collections of users and have policies attached to them.

- A group is not an identity and cannot be identified as a principal in an IAM policy.

- Use groups to assign permissions to users.

- IAM groups cannot be used to group EC2 instances.

- Only users and services can assume a role to take on permissions (not groups).

CORRECT: "IAM groups can be used to assign permissions to users" is a correct answer.

CORRECT: "An IAM group is not an identity and cannot be identified as a principal in an IAM policy" is also a correct answer.

INCORRECT: "IAM groups can be nested up to 4 levels" is incorrect as this not possible.

INCORRECT: "IAM groups can be used to group EC2 instances" is incorrect as they can only be used to group user accounts.

INCORRECT: "IAM groups can temporarily assume a role to take on permissions for a specific task" is incorrect as this is not possible.

References:

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

Save time with our AWS cheat sheets:

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

Question 2:

Skipped

A finance organization has bootstrapped a golden image for their in-house application and the resultant AMI is to be shared across various AWS accounts as a base image. This image is to be used across many applications. The company needs to design an application that captures AWS API calls and sends alerts whenever the Amazon EC2 CreateImage API operation is called within the company's account.

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

- 

- **Configure an Amazon SQS FIFO queue as a target for AWS CloudTrail logs. Create an AWS Lambda function to send an alert to an Amazon SNS topic when a CreateImage API call is detected.**

- **Configure AWS CloudTrail with an Amazon SNS notification that occurs when updated logs are sent to Amazon S3. Use Amazon Athena to create a new table and to query on CreateImage when an API call is detected**

- **Create an Amazon EventBridge rule for the CreateImage API call. Configure the target as an Amazon SNS topic to send an alert when a CreateImage API call is detected.**

  (Correct)

- **Create an AWS Lambda function to query AWS CloudTrail logs and to send an alert when a CreateImage API call is detected.**

Explanation

You can create an Amazon EventBridge rule that triggers on an action by an AWS service that does not emit events. In this case you can base the rule on API calls made by AWS CloudTrail. The rule can trigger when the Amazon EC2 CreateImage API is called. The rule can then trigger another service or action.

CORRECT: "Create an Amazon EventBridge rule for the CreateImage API call. Configure the target as an Amazon SNS topic to send an alert when a CreateImage API call is detected" is the correct answer (as explained above.)

INCORRECT: "Configure AWS CloudTrail with an Amazon SNS notification that occurs when updated logs are sent to Amazon S3. Use Amazon Athena to create a new table and to query on CreateImage when an API call is detected" is incorrect.

Athena is a query analysis tool hence this option is incorrect.

INCORRECT: "Create an AWS Lambda function to query AWS CloudTrail logs and to send an alert when a CreateImage API call is detected" is incorrect.

Since the question asks about least operational overhead, this option becomes incorrect. This is an achievable solution but involves building custom code in Lambda and requires more effort.

INCORRECT: "Configure an Amazon SQS FIFO queue as a target for AWS CloudTrail logs. Create an AWS Lambda function to send an alert to an Amazon SNS topic when a CreateImage API call is detected" is incorrect.

You cannot configure CloudTrail logs to be sent directly to an SQS queue.

References:

https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-log-api-call.html

Question 3:

Skipped

An e-commerce company has developed a new application which has been successfully deployed on AWS. For an upcoming sale, the company is expecting a huge rise in traffic and while testing for the event they have encountered performance issues in the application when many requests are sent to the application.

The current application stack is Amazon Aurora PostgreSQL database with an AWS Lambda compute layer fronted by API Gateway. A solutions architect must recommend improvements scalability whilst minimizing the configuration effort.

Which solution will meet these requirements?

- **Refactor the Lambda function code to Apache Tomcat code that runs on Amazon EC2 instances. Connect the database by using native Java Database Connectivity (JDBC) drivers.**
- **Set up two Lambda functions. Configure one function to receive the information. Configure the other function to load the information into the database. Integrate the Lambda functions by using Amazon Simple Notification Service (Amazon SNS).**
- **Change the platform from Aurora to Amazon DynamoDB. Provision a DynamoDB Accelerator (DAX) cluster. Use the DAX client SDK to point the existing DynamoDB API calls at the DAX cluster.**

Set up two Lambda functions. Configure one function to receive the information. Configure the other function to load the information into the database. Integrate the Lambda functions by using an Amazon Simple Queue Service (Amazon SQS) queue.

(Correct)

Explanation
With Amazon SQS, you can offload tasks from one component of your application by sending them to a queue and processing them asynchronously. Lambda polls the queue and invokes your Lambda function synchronously with an event that contains the message from the SQS queue. This solution improves scalability as the message bus decouples the processing components of the application meaning it is less likely that the application will suffer outages or lost data.

CORRECT: "Set up two Lambda functions. Configure one function to receive the information. Configure the other function to load the information into the database. Integrate the Lambda functions by using an Amazon Simple Queue Service (Amazon SQS) queue" is the correct answer (as explained above.)

INCORRECT: "Refactor the Lambda function code to Apache Tomcat code that runs on Amazon EC2 instances. Connect the database by using native Java Database Connectivity (JDBC) drivers" is incorrect. You cannot run Lambda code on Amazon EC2 instances.

INCORRECT: "Change the platform from Aurora to Amazon DynamoDB. Provision a DynamoDB Accelerator (DAX) cluster. Use the DAX client SDK to point the existing DynamoDB API calls at the DAX cluster" is incorrect. Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for Amazon DynamoDB. The question doesn't talk about hot or frequently accessed data only about an increase in volume so introducing DAX might not completely solve the issues.

INCORRECT: "Set up two Lambda functions. Configure one function to receive the information. Configure the other function to load the information into the database. Integrate the Lambda functions by using Amazon Simple Notification Service (Amazon SNS)" is incorrect. SNS is used for fan-out scenarios when a single event is to be broadcasted among consumers and hence is not a good fit here.

References:

https://docs.aws.amazon.com/lambda/latest/dg/with-sqs.html

Save time with our AWS cheat sheets:

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

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

Question 4:

Skipped

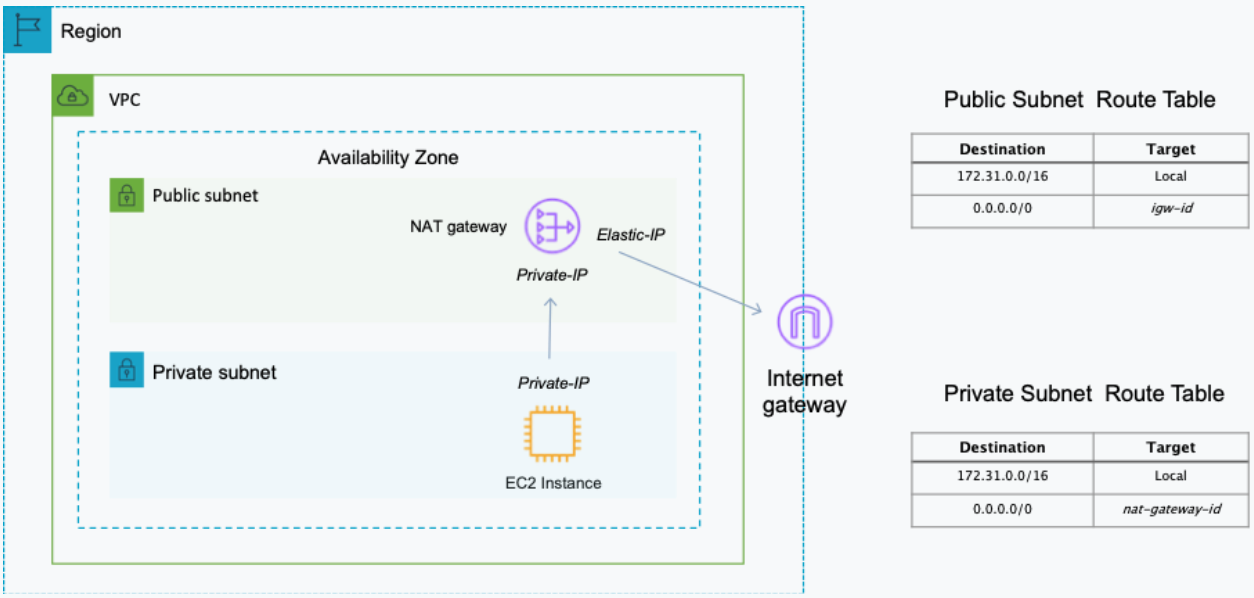
An application is running in a private subnet of an Amazon VPC and must have outbound internet access for downloading updates. The Solutions Architect does not want the application exposed to inbound connection attempts. Which steps should be taken?

- **Attach an internet gateway to the VPC but do not create a NAT gateway**
- **Create a NAT gateway but do not attach an internet gateway to the VPC**
- **Create a NAT gateway and attach an internet gateway to the VPC**

  (Correct)
- **Attach an internet gateway to the private subnet and create a NAT gateway**

Explanation

To enable outbound connectivity for instances in private subnets a NAT gateway can be created. The NAT gateway is created in a public subnet and a route must be created in the private subnet pointing to the NAT gateway for internet-bound traffic. An internet gateway must be attached to the VPC to facilitate outbound connections.



You cannot directly connect to an instance in a private subnet from the internet. You would need to use a bastion/jump host. Therefore, the application will not be exposed to inbound connection attempts.

CORRECT: "Create a NAT gateway and attach an internet gateway to the VPC" is the correct answer.

INCORRECT: "Create a NAT gateway but do not create attach an internet gateway to the VPC" is incorrect. An internet gateway must be attached to the VPC for any outbound connections to work.

INCORRECT: "Attach an internet gateway to the private subnet and create a NAT gateway" is incorrect. You do not attach internet gateways to subnets, you attach them to VPCs.

INCORRECT: "Attach an internet gateway to the VPC but do not create a NAT gateway" is incorrect. Without a NAT gateway the instances in the private subnet will not be able to download updates from 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 in a large finance organization must restrict access for a specific S3 bucket to only users in accounts within the organization in AWS Organizations. This is due to the confidentiality of project reports data.

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

- **Add the aws:PrincipalOrgID global condition key with a reference to the organization ID to the S3 bucket policy.**

  (Correct)

- **Create an organizational unit (OU) for each department. Add the aws:PrincipalOrgPaths global condition key to the S3 bucket policy.**

- **Use AWS CloudTrail to monitor the CreateAccount, InviteAccountToOrganization, LeaveOrganization, and RemoveAccountFromOrganization events. Update the S3 bucket policy accordingly.**

- **Tag each user that needs access to the S3 bucket. Add the aws:PrincipalTag global condition key to the S3 bucket policy.**

Explanation

```
{
 "Version": "2012-10-17",
 "Statement": {
   "Sid": "AllowPutObject",
   "Effect": "Allow",
   "Principal": "*",
   "Action": "s3:PutObject",
   "Resource": "arn:aws:s3:::policy-ninja-dev/*",
   "Condition": {"StringEquals":
     {"aws:PrincipalOrgID":"o-xxxxxxxxxxx"}
   }
  }
}
```

PrincipalOrgId is used by specifying the Principal element in a resource-based policy. You can specify the organization ID in the condition element. When you add and remove accounts, policies that include the aws:PrincipalOrgID key automatically include the correct accounts and don't require manual updating.

For example, the following Amazon S3 bucket policy allows members of any account in the o-xxxxxxxxxx organization to add an object into the policy-ninja-dev bucket.

CORRECT: "Add the aws:PrincipalOrgID global condition key with a reference to the organization ID to the S3 bucket policy" is the correct answer (as explained above.)

INCORRECT: "Create an organizational unit (OU) for each department. Add the aws:PrincipalOrgPaths global condition key to the S3 bucket policy" is incorrect.

This condition key ensures that the requester is an account member within the specified organization root or organizational units (OUs) in AWS Organizations. It is not required for this solution.

INCORRECT: "Use AWS CloudTrail to monitor the CreateAccount, InviteAccountToOrganization, LeaveOrganization, and RemoveAccountFromOrganization events. Update the S3 bucket policy accordingly" is incorrect. This option would be required for monitoring but not sharing access.

INCORRECT: "Tag each user that needs access to the S3 bucket. Add the aws:PrincipalTag global condition key to the S3 bucket policy" is incorrect. Since question is around cross account access, this option wouldn't work as is.

References:

https://aws.amazon.com/blogs/security/control-access-to-aws-resources-by-using-the-aws-organization-of-iam-principals/

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_condition-keys.html

https://aws.amazon.com/blogs/security/iam-share-aws-resources-groups-aws-accounts-aws-organizations/

Save time with our AWS cheat sheets:

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

Question 6:

Skipped

A data analytics company is hosting a data lake which consists of data in Amazon S3 and Amazon RDS for PostgreSQL. The company needs a reporting solution that provides data visualization for the latest dataset and includes all the data sources within the data lake. Only the company's management team should have full access to all the visualizations. The rest of the company should have only limited access.

Which solution will meet these requirements?

- **Create an analysis in Amazon QuickSight. Connect all the data sources and create new datasets. Publish dashboards to visualize the data. Share the dashboards with the appropriate users and groups.**

- **Create an AWS Glue table and crawler for the data in Amazon S3. Use Amazon Athena Federated Query to access data within Amazon RDS for PostgreSQL. Generate reports by using Amazon Athena. Publish the reports to Amazon S3. Use S3 bucket policies to limit access to the reports.**

  (Correct)

-

Create an AWS Glue table and crawler for the data in Amazon S3. Create an AWS Glue extract, transform, and load (ETL) job to produce reports. Publish the reports to Amazon S3. Use S3 bucket policies to limit access to the reports.

- 

Create an analysis in Amazon QuickSight. Connect all the data sources and create new datasets. Publish dashboards to visualize the data. Share the dashboards with the appropriate IAM roles.

Explanation

If you have data in sources other than Amazon S3, you can use Athena Federated Query to query the data in place or build pipelines that extract data from multiple data sources and store them in Amazon S3. With Athena Federated Query, you can run SQL queries across data stored in relational, non-relational, object, and custom data sources.

Athena uses *data source connectors* that run on AWS Lambda to run federated queries. A data source connector is a piece of code that can translate between your target data source and Athena. You can think of a connector as an extension of Athena's query engine. Prebuilt Athena data source connectors exist for data sources like Amazon CloudWatch Logs, Amazon DynamoDB, Amazon DocumentDB, and Amazon RDS, and JDBC-compliant relational data sources such MySQL, and PostgreSQL under the Apache 2.0 license.

CORRECT: "Create an AWS Glue table and crawler for the data in Amazon S3. Use Amazon Athena Federated Query to access data within Amazon RDS for PostgreSQL. Generate reports by using Amazon Athena. Publish the reports to Amazon S3. Use S3 bucket policies to limit access to the reports" is the correct answer (as explained above.)

INCORRECT: "Create an analysis in Amazon QuickSight. Connect all the data sources and create new datasets. Publish dashboards to visualize the data. Share the dashboards with the appropriate IAM roles" is incorrect.

This would have worked for one time data set which only needed visualization. For any new data, analysis would need to be performed again. Also, you connect user and groups in your QuickSight account but not IAM Roles.

INCORRECT: "Create an analysis in Amazon QuickSight. Connect all the data sources and create new datasets. Publish dashboards to visualize the data. Share the dashboards with the appropriate users and groups " is incorrect.

As with the previous answer, this option solves the problem of access sharing with resources but does not take care of delta in data. Also, you connect user and groups in your QuickSight account but not IAM Roles.

INCORRECT: "Create an AWS Glue table and crawler for the data in Amazon S3. Create an AWS Glue extract, transform, and load (ETL) job to produce reports. Publish the reports to Amazon S3. Use S3 bucket policies to limit access to the reports" is incorrect.

Amazon Athena should be used with AWS Glue to provide the required functionality as described in the explanation above and the article linked below.

References:

https://docs.aws.amazon.com/athena/latest/ug/connect-to-a-data-source.html

Save time with our AWS cheat sheets:

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

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

Question 7:

Skipped

A Solutions Architect is building a small web application running on Amazon EC2 that will be serving static content. The user base is spread out globally and speed is important. Which AWS service can deliver the best user experience cost-effectively and reduce the load on the web server?

- **Amazon RedShift**
- **Amazon S3**
- **Amazon EBS volume**
- **Amazon CloudFront**

(Correct)

Explanation

This is a good use case for Amazon CloudFront as the user base is spread out globally and CloudFront can cache the content closer to users and also reduce the load on the web server running on EC2.

CORRECT: "Amazon CloudFront" is the correct answer.

INCORRECT: "Amazon RedShift" is incorrect. Amazon RedShift is a data warehouse and is not suitable in this solution.

INCORRECT: "Amazon S3" is incorrect. Amazon S3 is very cost-effective however a bucket is located in a single region and therefore performance is not so great for users a long distance from the bucket.

INCORRECT: "Amazon EBS volume" is incorrect. EBS is not the most cost-effective storage solution and the data would be located in a single region to latency could be an issue.

References:

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html

Save time with our AWS cheat sheets:

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

Question 8:

Skipped

An organization is planning their disaster recovery solution. They plan to run a scaled down version of a fully functional environment. In a DR situation the recovery time must be minimized.

Which DR strategy should a Solutions Architect recommend?

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

- 

Warm standby

(Correct)

Explanation
The term warm standby is used to describe a DR scenario in which a scaled-down version of a fully functional environment is always running in the cloud. A warm standby solution extends the pilot light elements and preparation.

It further decreases the recovery time because some services are always running. By identifying your business-critical systems, you can fully duplicate these systems on AWS and have them always on.

CORRECT: "Warm standby" is the correct answer.

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

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

INCORRECT: "Multi-site" is incorrect. A multi-site solution runs on AWS as well as on your existing on-site infrastructure in an active- active configuration.

References:

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

Question 9:
Skipped
A Solutions Architect is deploying a high performance computing (HPC) application on Amazon EC2 instances. The application requires extremely low inter-instance latency. How should the instances be deployed for BEST performance?

- 

Add multiple Elastic Network Adapters (ENAs) to each instance and create a NIC team

- 

Use an instance with enhanced networking and deploy the instances in a partition placement group

- **Use an Elastic Fabric Adapter (EFA) and deploy instances in a cluster placement group**

  (Correct)

- **Use an EBS-optimized instance with 10 Gigabit networking and deploy to a single subnet**

Explanation

It is recommended to use either enhanced networking or an Elastic Fabric Adapter (EFA) for the nodes of an HPC application. This will assist with decreasing latency. Additionally, a cluster placement group packs instances close together inside an Availability Zone.

Using a cluster placement group enables workloads to achieve the low-latency network performance necessary for tightly-coupled node-to-node communication that is typical of HPC applications.

The table below helps you to understand the key differences between the different placement group options:

	Clustered	Spread	Partition
What	Instances are placed into a low-latency group within a single AZ	Instances are spread across underlying hardware	Instances are grouped into logical segments called partitions which use distinct hardware
When	Need low network latency and/or high network throughput	Reduce the risk of simultaneous instance failure if underlying hardware fails	Need control and visibility into instance placement
Pros	Get the most out of enhanced networking Instances	Can span multiple AZs	Reduces likelihood of correlated failures for large workloads.
Cons	Finite capacity: recommend launching all you might need up front	Maximum of 7 instances running per group, per AZ	Partition placement groups are not supported for Dedicated Hosts

CORRECT: "Use an Elastic Fabric Adapter (EFA) and deploy instances in a cluster placement group" is the correct answer.

INCORRECT: "Use an instance with enhanced networking and deploy the instances in a partition placement group" is incorrect. A partition placement group protects instances from correlated hardware failures, it does not offer the best inter-instance network performance.

INCORRECT: "Add multiple Elastic Network Adapters (ENAs) to each instance and create a NIC team" is incorrect. You cannot use NIC teaming methods on AWS to increase the bandwidth to your application. This will also not reduce latency.

INCORRECT: "Use an EBS-optimized instance with 10 Gigabit networking and deploy to a single subnet" is incorrect. EBS optimization is related to storage, not to network performance. A 10 Gigabit adapter offers great bandwidth but for lowest latency enhanced networking with a cluster placement group should be used.

References:

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

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

Save time with our AWS cheat sheets:

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

Question 10:

Skipped

A Solutions Architect has deployed an API using Amazon API Gateway and created usage plans and API keys for several customers. Requests from one particular customer have been excessive and the solutions architect needs to limit the rate of requests. Other customers should not be affected. How should the solutions architect proceed?

- **Configure per-client throttling limits**

  (Correct)

- **Configure a server-side throttling limit**

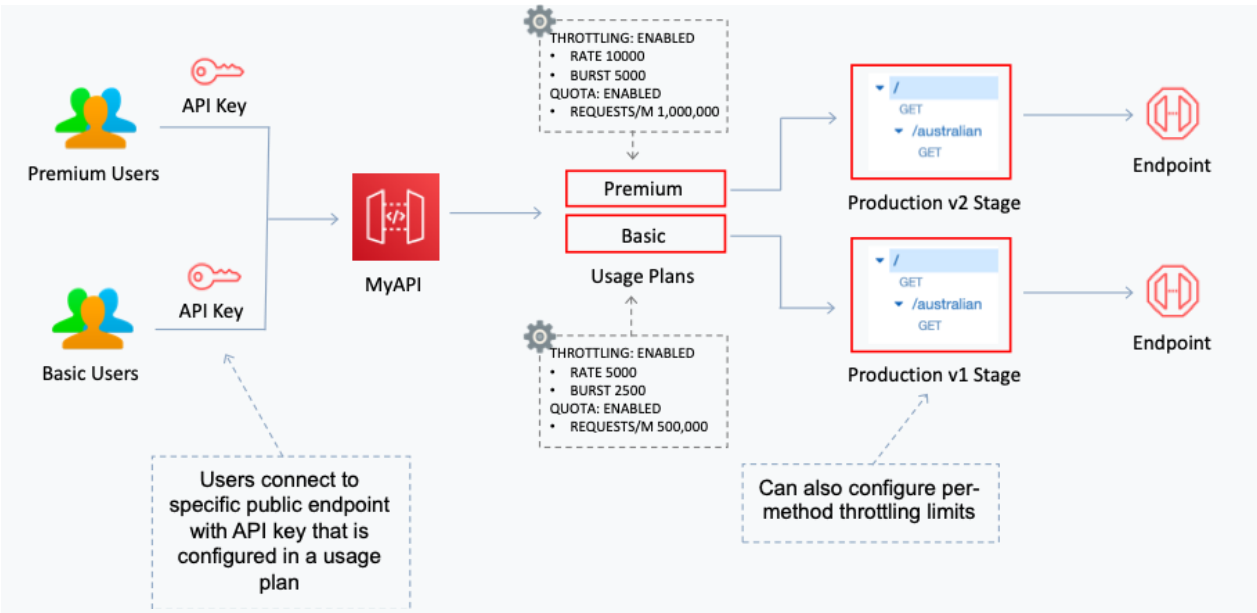
- **Configure the account-level throttling limits**

- **Configure the per-method throttling limits**

Explanation

Per-client throttling limits are applied to clients that use API keys associated with your usage policy as client identifier. This can be applied to the single customer that is issuing excessive API requests. This is the best option to ensure that only one customer is affected.

In the diagram below, per-client throttling limits are set in a usage plan:



CORRECT: "Configure per-client throttling limits" is the correct answer.

INCORRECT: "Configure a server-side throttling limit" is incorrect. Server-side throttling limits are applied across all clients. These limit settings exist to prevent your API—and your account—from being overwhelmed by too many requests. In this case, the solutions architect need to apply the throttling to a single client.

INCORRECT: "Configure the per-method throttling limits" is incorrect. Per-method throttling limits apply to all customers using the same method. This will affect all customers who are using the API.

INCORRECT: "Configure the account-level throttling limits" is incorrect. Account-level throttling limits define the maximum steady-state request rate and burst limits for the account. This does not apply to individual customers.

References:

https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-request-throttling.html

Save time with our AWS cheat sheets:

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

Question 11:

Skipped

An e-commerce website uses Amazon EC2 instance stores for storing session data. The company want to make sure that this data is highly available, and that the information is stored durably.

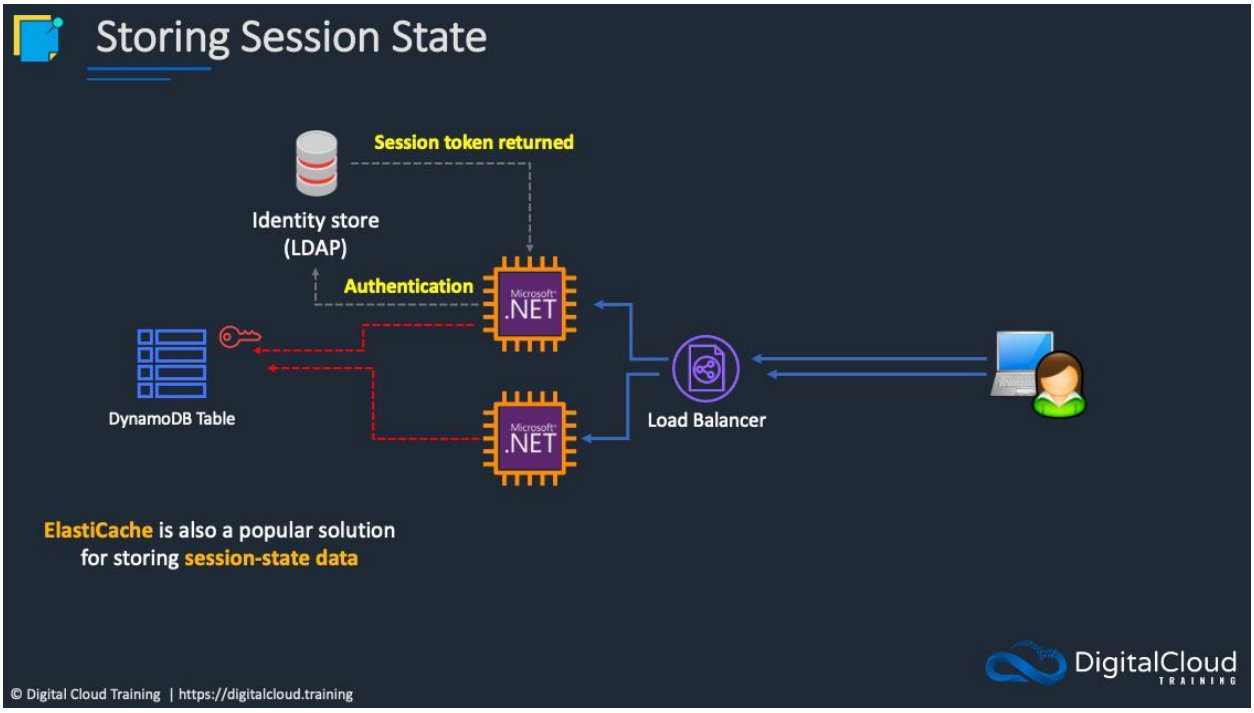
What should a solutions architect do to meet these requirements?

- **Move the session data to Amazon S3 Glacier Deep Archive.**
- **Store the session data in an Amazon DynamoDB table.**

  (Correct)
- **Move the session data to Amazon ElastiCache for Memcached.**
- **Deploy a larger EC2 instance with a larger instance store.**

Explanation

Amazon DynamoDB is a NoSQL database and is ideal for storing session data. The data will be both highly available and durable and can be stored persistently. DynamoDB also offers time to live (TTL) attributes that can be used to automatically expire items from the table after specified time periods.



CORRECT: "Store the session data in an Amazon DynamoDB table" is the correct answer (as explained above.)

INCORRECT: "Move the session data to Amazon ElastiCache for Memcached" is incorrect. ElastiCache Memcached does not store data durably or persistently. ElastiCache can be used for storing session data, but the Redis engine should be used instead.

INCORRECT: "Deploy a larger EC2 instance with a larger instance store" is incorrect. Instance stores use ephemeral storage which means it is non-persistent. The size of the instance store does not change anything here.

INCORRECT: " Move the session data to Amazon S3 Glacier Deep Archive" is incorrect. Glacier is an archiving solution and cannot be used for data that requires immediate access. It is unsuitable for storing session data.

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

Save time with our AWS cheat sheets:

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

Question 12:

Skipped

The database layer of an on-premises web application is being migrated to AWS. The database uses a multi-threaded, in-memory caching layer to improve performance for

repeated queries. Which service would be the most suitable replacement for the database cache?

- **Amazon RDS MySQL**
- **Amazon ElastiCache Redis**
- **Amazon DynamoDB DAX**
- **Amazon ElastiCache Memcached**

  (Correct)

Explanation
Amazon ElastiCache with the Memcached engine is an in-memory database that can be used as a database caching layer. The memached engine supports multiple cores and threads and large nodes.

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

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

INCORRECT: "Amazon ElastiCache Redis" is incorrect. The Redis engine does not support multiple CPU cores or threads.

INCORRECT: "Amazon DynamoDB DAX" is incorrect. Amazon DynamoDB Accelerator (DAX) is a database cache that should be used with DynamoDB only.

INCORRECT: "Amazon RDS MySQL" is incorrect as this is not an example of an in-memory database that can be used as a database caching layer.

References:

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

Save time with our AWS cheat sheets:

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

Question 13:
Skipped

As a security measure, a finance-based organization want to introduce additional security measures for an existing application deployed in AWS. The application is serverless and has an Amazon API Gateway in front which is deployed in the us-east-1 Region and the eu-west-1 Region. The company requires the accounts to be secured against SQL injection and cross-site scripting attacks.

Which solution will meet these requirements with the LEAST amount of administrative effort?

- **Set up AWS Shield in both Regions. Associate Regional web ACLs with an API stage.**
- **Set up AWS Shield in one of the Regions. Associate Regional web ACLs with an API stage.**
- **Set up AWS WAF in both Regions. Associate Regional web ACLs with an API stage**
- **Set up AWS Firewall Manager in both Regions. Centrally configure AWS WAF rules.**

  (Correct)

Explanation
AWS Firewall Manager simplifies your administration and maintenance tasks across multiple accounts and resources for a variety of protections, including AWS WAF, AWS Shield Advanced, Amazon VPC security groups, AWS Network Firewall, and Amazon Route 53 Resolver DNS Firewall. With Firewall Manager, you set up your protections just once and the service automatically applies them across your accounts and resources, even as you add new accounts and resources.

AWS WAF is used for protecting against malicious web attacks and is the best service to use to protect against SQL injection and cross-site scripting attacks. Used in combination with AWS Firewall Manager this solution protects both Regions and requires the least administrative effort.

CORRECT: "Set up AWS Firewall Manager in both Regions. Centrally configure AWS WAF rules" is the correct answer (as explained above.)

INCORRECT: "Set up AWS WAF in both Regions. Associate Regional web ACLs with an API stage" is incorrect. This solution requires more administrative effort in rule management.

INCORRECT: "Set up AWS Shield in both Regions. Associate Regional web ACLs with an API stage" is incorrect. The primary difference between AWS Shield and WAF is that while AWS WAF can mitigate DDoS attacks at layer 7 of the OSI reference model, AWS Shield protects web services from DDoS attacks at layer 3 and 4 of the OSI reference model. In this case AWS WAF should be used.

INCORRECT: "Set up AWS Shield in one of the Regions. Associate Regional web ACLs with an API stage" is incorrect. As mentioned above, AWS Shield is not an appropriate choice for securing the accounts from SQL injection and cross-site scripting attacks.

References:

https://docs.aws.amazon.com/waf/latest/developerguide/fms-chapter.html

https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/aws-waf-shield/

Question 14:

Skipped

A telemarketing company has developed customer call center functionality on AWS. The company plans to enhance the current application by enabling support for multiple speaker recognition and transcript generation. They also want to query the transcript files to analyze business patterns.

Which solution will meet these requirements?

- **Use Amazon Rekognition for multiple speaker recognition. Store the transcript files in Amazon S3. Use machine learning models for transcript file analysis.**

Use Amazon Transcribe for multiple speaker recognition. Use Amazon Athena for transcript file analysis.

(Correct)

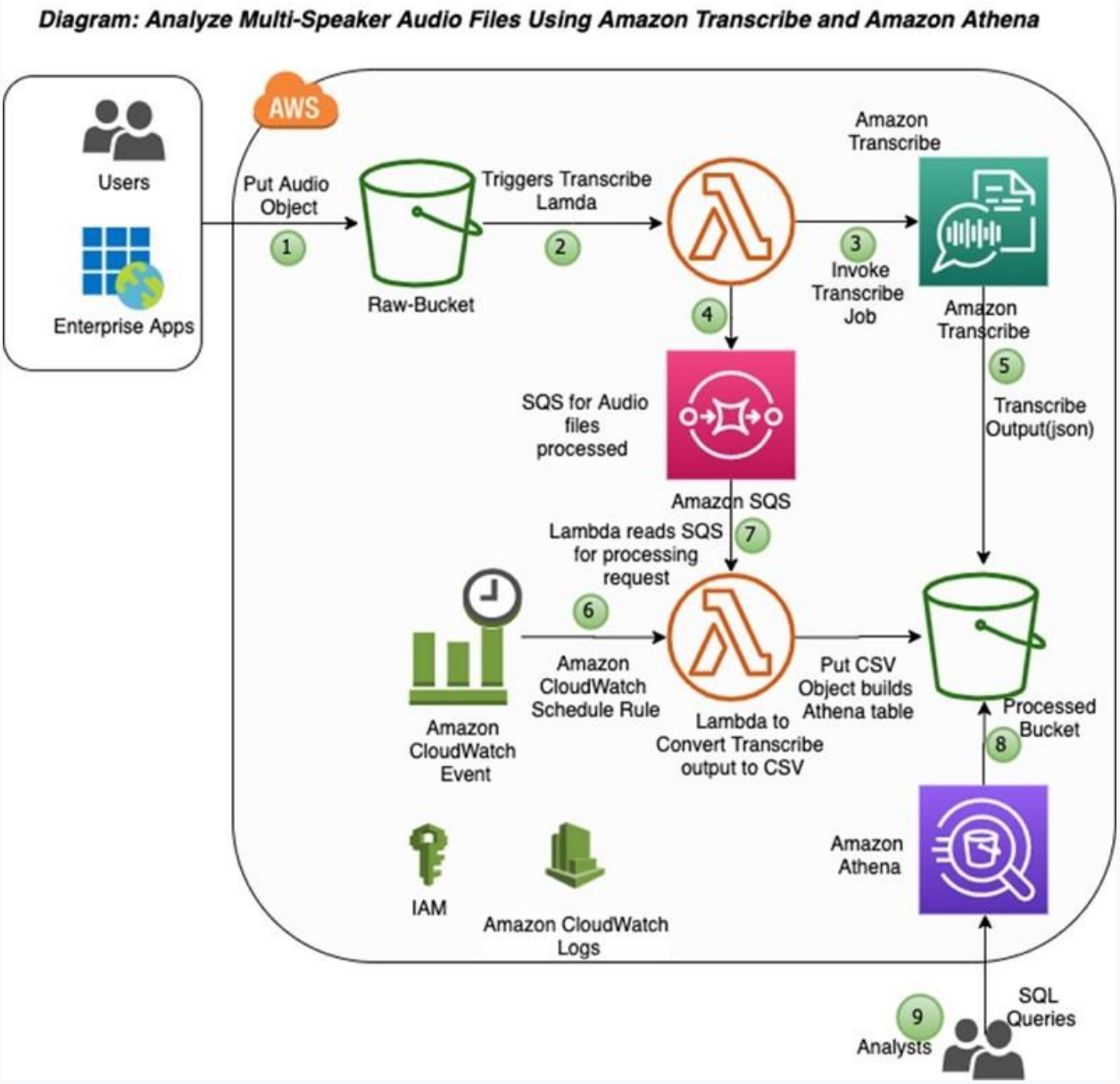
- **Use Amazon Rekognition for multiple speaker recognition. Store the transcript files in Amazon S3. Use Amazon Textract for transcript file analysis.**

- **Use Amazon Translate for multiple speaker recognition. Store the transcript files in Amazon Redshift. Use SQL queries for transcript file analysis.**

Explanation

Amazon Transcribe converts audio input into text, which opens the door for various text analytics applications on voice input. For instance, by using Amazon Comprehend on the converted text data from Amazon Transcribe, customers can perform sentiment analysis or extract entities and key phrases.

Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run.



CORRECT: "Use Amazon Transcribe for multiple speaker recognition. Use Amazon Athena for transcript file analysis" is the correct answer (as explained above.)

INCORRECT: " Use Amazon Rekognition for multiple speaker recognition. Store the transcript files in Amazon S3. Use machine learning models for transcript file analysis" is incorrect.

Amazon Rekognition Video can detect objects, scenes, faces, celebrities, text, and inappropriate content in videos. You can also search for faces appearing in a video using your own repository or collection of face images.

INCORRECT: "Use Amazon Translate for multiple speaker recognition. Store the transcript files in Amazon Redshift. Use SQL queries for transcript file analysis" is incorrect.

Amazon Translate can provide automatic translation to enable cross-lingual communications between users for your applications.

INCORRECT: "Use Amazon Rekognition for multiple speaker recognition. Store the transcript files in Amazon S3. Use Amazon Textract for transcript file analysis" is incorrect.

As mentioned above, Rekognition is better suited for identifying content in videos. Also,

Amazon Textract is a machine learning (ML) service that automatically extracts text, handwriting, and data from scanned documents.

References:

https://aws.amazon.com/blogs/machine-learning/automating-the-analysis-of-multi-speaker-audio-files-using-amazon-transcribe-and-amazon-athena/

Save time with our AWS cheat sheets:

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

Question 15:

Skipped

A company provides a Voice over Internet Protocol (VoIP) service that uses UDP as the protocol. The service utilizes Amazon EC2 instances that are scaled automatically using an Auto Scaling group. The company currently uses multiple AWS Regions for its AWS deployments.

The company needs to route users to the appropriate Region based on the lowest latency. The company also needs automated failover between Regions.

Which solution will meet these requirements?

- **Create a Network Load Balancer (NLB) and an associated target group. Assign the target group to the Auto Scaling group and create an Amazon Route 53 latency record that points to aliases for each NLB.**
-

Set up an Application Load Balancer (ALB) and a target group. Associate the target group with the Auto Scaling group and use the ALB as an AWS Global Accelerator endpoint in each Region.

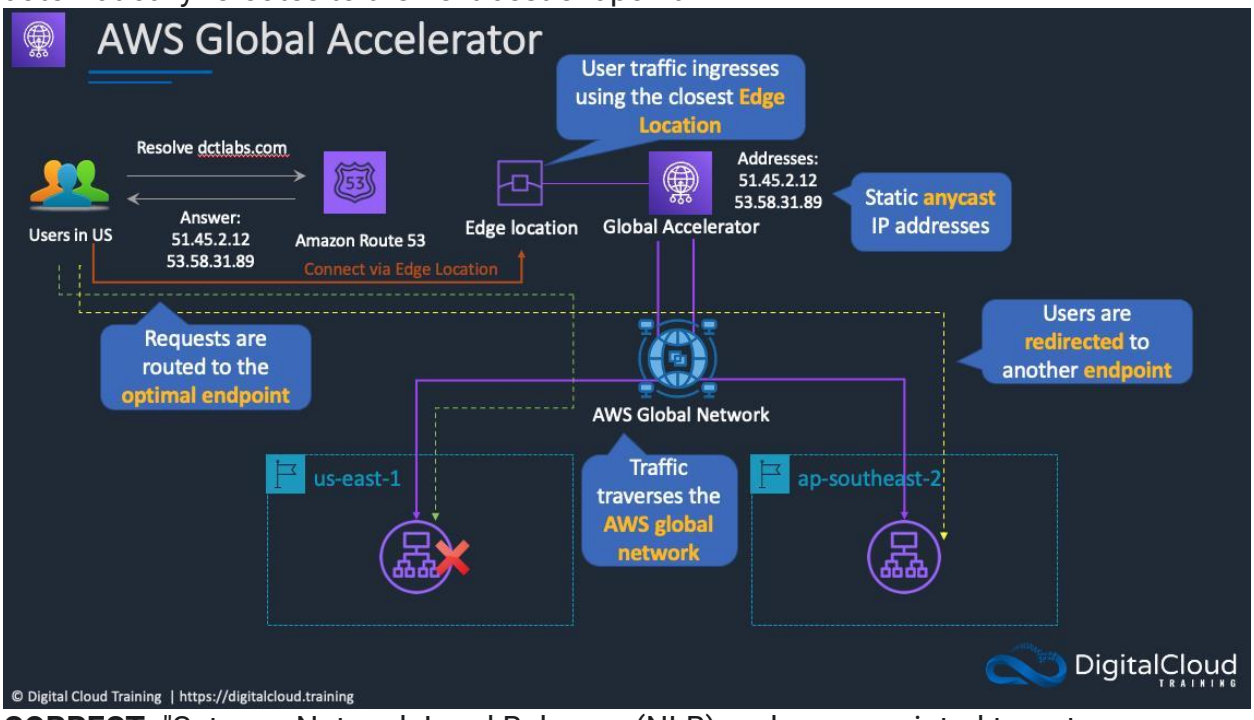
- **Deploy an Application Load Balancer (ALB) and its associated target group. Assign the target group to the Auto Scaling group and create an Amazon Route 53 weighted record that points to aliases for each ALB.**

- **Set up a Network Load Balancer (NLB) and an associated target group. Assign the target group with the Auto Scaling group. In each region, use the NLB as an AWS Global Accelerator endpoint.**

  (Correct)

Explanation

For UDP traffic the solution must use a Network Load Balancer as ALBs do not support UDP. The solution also requires both latency-based routing and automated failover. AWS Global Accelerator can be used to achieve both these requirements. It will direct users to the lowest latency endpoint and if an endpoint becomes unhealthy it automatically reroutes to the next best endpoint.



CORRECT: "Set up a Network Load Balancer (NLB) and an associated target group. Assign the target group with the Auto Scaling group. In each region, use the NLB as an AWS Global Accelerator endpoint" is the correct answer (as explained above.)

INCORRECT: "Create a Network Load Balancer (NLB) and an associated target group. Assign the target group to the Auto Scaling group and create an Amazon Route 53 latency record that points to aliases for each NLB" is incorrect. An NLB must be used but Route 53 latency-based routing will not automatically failover the application to another endpoint unless health checks are enabled, and this is not described.

INCORRECT: "Set up an Application Load Balancer (ALB) and a target group. Associate the target group with the Auto Scaling group and use the ALB as an AWS Global Accelerator endpoint in each Region" is incorrect as Application Load Balancers balance HTTP and HTTPS traffic at Layer 7, not UDP traffic.

INCORRECT: "Deploy an Application Load Balancer (ALB) and its associated target group. Assign the target group to the Auto Scaling group and create an Amazon Route 53 weighted record that points to aliases for each ALB" is incorrect as ALBs do not support UDP listeners and weighted routing is not used for latency or failover.

References:

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

Save time with our AWS cheat sheets:

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

Question 16:

Skipped

A traffic law enforcement company is building a solution that has thousands of edge devices that collectively generate 1 TB of status alerts each day. These devices provide vehicle information and number plate data whenever alerts detecting red light jumps are detected. Each entry is around 2Kb in size. A solutions architect needs to implement a solution to ingest and store the alerts for future analysis.

The company wants a highly available solution. However, the company needs to minimize costs and does not want to manage additional infrastructure. Additionally, the company wants to keep 14 days of data available for immediate analysis and archive any data older than 14 days.

What is the MOST operationally efficient solution that meets these requirements?

- **Launch Amazon EC2 instances across two Availability Zones and place them behind an Elastic Load Balancer to ingest the alerts. Create a script on the EC2 instances that will store the alerts in an Amazon S3 bucket. Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days.**

- **Create an Amazon Simple Queue Service (Amazon SQS) standard queue to ingest the alerts and set the message retention period to 14 days. Configure consumers to poll the SQS queue, check the age of the message, and analyze the message data as needed. If the message is 14 days old, the consumer should copy the message to an Amazon S3 bucket and delete the message from the SQS queue.**

- **Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts. Configure the kinesis Data Firehose stream to deliver the alerts to an Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster. Set up the Amazon Open Search Service (Amazon Elasticsearch Service) cluster to take manual snapshots every day and delete data from the cluster that is older than 14 days.**

- **Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts. Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon S3 bucket. Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days.**

  (Correct)

Explanation
Data ingestion is a good use case for since it is scalable and can achieve the volumes required. Also, an S3 lifecycle configuration is appropriate for the requirement for data retention.

CORRECT: "Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts. Configure the kinesis Data Firehose stream to deliver the alerts to an Amazon S3 bucket. Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days" is the correct answer (as explained above.)

INCORRECT: "Launch Amazon EC2 instances across two Availability Zones and place them behind an Elastic Load Balancer to ingest the alerts. Create a script on the EC2 instances that will store the alerts in an Amazon S3 bucket. Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days" is incorrect. Provisioning additional EC2 instances means provisioning infrastructure, and the question states that the company wants to avoid this.

INCORRECT: "Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts. Configure the kinesis Data Firehose stream to deliver the alerts to an Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster. Set up the Amazon Open Search Service (Amazon Elasticsearch Service) cluster to take manual snapshots every day and delete data from the cluster that is older than 14 days" is incorrect. This option would mean provisioning ECS clusters and since the question is asking for archival of data, S3 is a better fit (data deletion is not desired).

INCORRECT: "Create an Amazon Simple Queue Service (Amazon SQS) standard queue to ingest the alerts and set the message retention period to 14 days. Configure consumers to poll the SQS queue, check the age of the message, and analyze the message data as needed. If the message is 14 days old, the consumer should copy the message to an Amazon S3 bucket and delete the message from the SQS queue" is incorrect.

With an SQS queue you must have processing components adding and retrieving messages from the queue and this means additional infrastructure to manage. With Kinesis Data Firehose the data is loaded straight to the destination without any need for additional infrastructure.

References:

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

https://aws.amazon.com/kinesis/data-firehose/features/

Save time with our AWS cheat sheets:

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

Question 17:

Skipped

An application that is being installed on an Amazon EC2 instance requires a persistent block storage volume. The data must be encrypted at rest and regular volume-level backups must be automated.

Which solution options should be used?

- **Use an encrypted Amazon EFS filesystem and use an Amazon CloudWatch Events rule to start a backup copy of data using AWS Lambda**
-

Use an encrypted Amazon EC2 instance store and copy the data to another EC2 instance using a cron job and a batch script

- **Use server-side encryption on an Amazon S3 bucket and use Cross-Region-Replication to backup on a schedule**

- **Use an encrypted Amazon EBS volume and use Data Lifecycle Manager to automate snapshots**

  (Correct)

Explanation
For block storage the Solutions Architect should use either Amazon EBS or EC2 instance store. However, the instance store is non-persistent so EBS must be used. With EBS you can encrypt your volume and automate volume-level backups using snapshots that are run by Data Lifecycle Manager.

CORRECT: "Use an encrypted Amazon EBS volume and use Data Lifecycle Manager to automate snapshots" is the correct answer.

INCORRECT: "Use an encrypted Amazon EFS filesystem and use an Amazon CloudWatch Events rule to start a backup copy of data using AWS Lambda" is incorrect. EFS is not block storage, it is a file-level storage service.

INCORRECT: "Use server-side encryption on an Amazon S3 bucket and use Cross-Region-Replication to backup on a schedule" is incorrect. Amazon S3 is an object-based storage system not a block-based storage system.

INCORRECT: "Use an encrypted Amazon EC2 instance store and copy the data to another EC2 instance using a cron job and a batch script " is incorrect as the EC2 instance store is a non-persistent volume.

References:

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

Save time with our AWS cheat sheets:

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

Question 18:

Skipped

A reporting team receives files each day in an Amazon S3 bucket. The reporting team manually reviews and copies the files from this initial S3 bucket to an analysis S3 bucket each day at the same time to use with Amazon QuickSight. Additional teams are starting to send more files in larger sizes to the initial S3 bucket.

The reporting team wants to move the files automatically to the analysis S3 bucket as the files enter the initial S3 bucket. The reporting team also wants to use AWS Lambda functions to run pattern-matching code on the copied data. In addition, the reporting team wants to send the data files to a pipeline in Amazon SageMaker Pipelines.

What should a solutions architect do to meet these requirements with the LEAST operational overhead?

- **Configure S3 replication between the S3 buckets. Create an S3 event notification for the analysis S3 bucket. Configure Lambda and SageMaker Pipelines as destinations of the event notification. Configure s3:ObjectCreated:Put as the event type.**

- **Configure S3 replication between the S3 buckets. Configure the analysis S3 bucket to send event notifications to Amazon EventBridge. Configure an ObjectCreated rule in EventBridge. Configure Lambda and SageMaker Pipelines as targets for the rule.**

  (Correct)

- **Create a Lambda function to copy the files to the analysis S3 bucket. Configure the analysis S3 bucket to send event notifications to Amazon EventBridge. Configure an ObjectCreated rule in EventBridge. Configure Lambda and SageMaker Pipelines as targets for the rule.**

- **Create a Lambda function to copy the files to the analysis S3 bucket. Create an S3 event notification for the analysis S3 bucket. Configure Lambda and SageMaker Pipelines as destinations of the event notification. Configure s3:ObjectCreated:Put as the event type.**

Explanation

With Amazon S3 you can configure same region replication (SRR) to automatically copy files from one bucket to another one as they are added to the source bucket. S3 event notifications can also be configured to trigger event driven responses when changes happen in an Amazon S3 bucket.

Amazon SageMaker Pipelines, the first purpose-built, continuous integration and continuous deployment (CI/CD) service for machine learning (ML), is now supported as a target for routing events in Amazon EventBridge. This enables customers to trigger the execution of the Amazon SageMaker model building pipeline based on any event in their event bus or on a schedule by selecting the pipeline as the target in Amazon EventBridge.

For example, customers can set up EventBridge to trigger the execution of the SageMaker model building pipeline when a new file with the training data set is uploaded to an Amazon S3 bucket or when the SageMaker Model Monitor indicates a deviation in model quality through alarms in Amazon CloudWatch metrics. Customers can also create rules in Amazon EventBridge that trigger the pipeline execution on an automated schedule.

CORRECT: "Configure S3 replication between the S3 buckets. Configure the analysis S3 bucket to send event notifications to Amazon EventBridge. Configure an ObjectCreated rule in EventBridge. Configure Lambda and SageMaker Pipelines as targets for the rule " is the correct answer (as explained above.)

INCORRECT: "Create a Lambda function to copy the files to the analysis S3 bucket. Configure the analysis S3 bucket to send event notifications to Amazon EventBridge. Configure an ObjectCreated rule in EventBridge. Configure Lambda and SageMaker Pipelines as targets for the rule " is incorrect.

This is the closest option with one flaw in that it involves setting up a Lambda function which would require more effort. S3 replication is an out of the box feature from AWS which will be more efficient.

INCORRECT: "Create a Lambda function to copy the files to the analysis S3 bucket. Create an S3 event notification for the analysis S3 bucket. Configure Lambda and SageMaker Pipelines as destinations of the event notification. Configure s3:ObjectCreated:Put as the event type" is incorrect.

This options involves manual steps to set up Lambda and any manual intervention could be avoided with S3 replication. Hence this is an incorrect option.

INCORRECT: "Configure S3 replication between the S3 buckets. Create an S3 event notification for the analysis S3 bucket. Configure Lambda and SageMaker Pipelines as destinations of the event notification. Configure s3:ObjectCreated:Put as the event type" is incorrect.

This option could work but again avoiding writing a Lambda function and using EventBridge reduces the manual intervention and the effort needed.

References:

https://aws.amazon.com/blogs/compute/using-dynamic-amazon-s3-event-handling-with-amazon-eventbridge/

Save time with our AWS cheat sheets:

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

Question 19:

Skipped

A company has multiple Windows workloads which are .NET application servers and Microsoft SQL Server databases running on Amazon EC2 instances with Windows Server 2016. The company requires a shared file system which is highly available, durable and provides high levels of throughput and IOPS.

What is the best way to meet this requirement?

- **Extend the file share environment to Amazon FSx for Windows File Server with a Multi-AZ configuration. Migrate all the data to FSx for Windows File Server.**

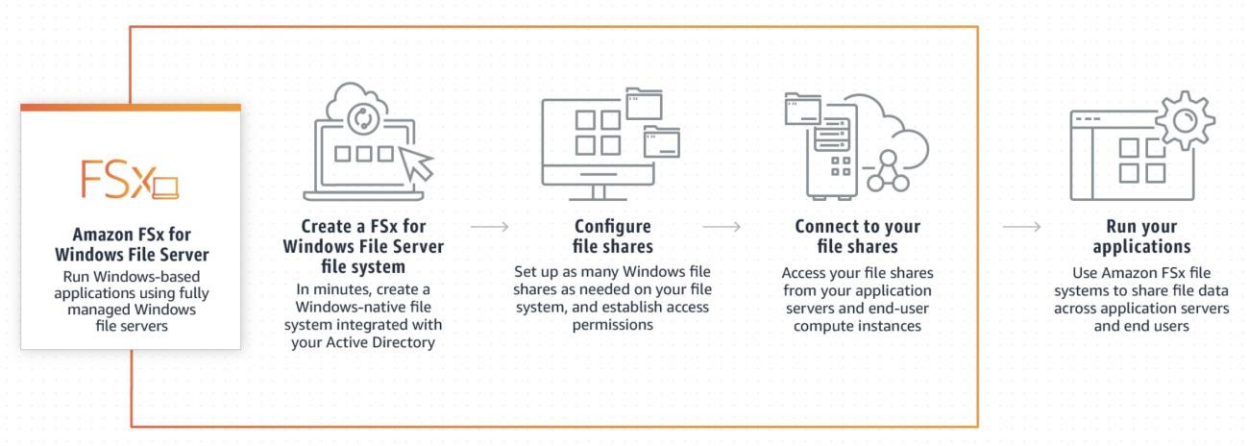
  (Correct)

- **Set up an Amazon S3 File Gateway, mount the S3 File Gateway on the existing EC2 instances.**

- **Migrate all the data to Amazon S3. Set up IAM authentication for users to access files.**

- **Extend the file share environment to Amazon Elastic File System (Amazon EFS) with a Multi-AZ configuration. Migrate all the data to Amazon EFS.**

Explanation



As a fully managed service, FSx for Windows File Server eliminates the administrative overhead of setting up and provisioning file servers and storage volumes. Additionally, Amazon FSx keeps Windows software up to date, detects and addresses hardware failures, and performs backups.

Amazon FSx also provides rich integration with other AWS services like AWS IAM, AWS Directory Service for Microsoft Active Directory, Amazon WorkSpaces, AWS Key Management Service, and AWS CloudTrail.

CORRECT: "Extend the file share environment to Amazon FSx for Windows File Server with a Multi-AZ configuration. Migrate all the data to FSx for Windows File Server" is the correct answer (as explained above.)

INCORRECT: "Migrate all the data to Amazon S3. Set up IAM authentication for users to access files" is incorrect. Since the workload is Windows specific, S3 wouldn't really help as an optimal solution though S3 can be still used to backup objects.

INCORRECT: "Set up an Amazon S3 File Gateway, mount the S3 File Gateway on the existing EC2 instances" is incorrect. Amazon S3 File Gateway provides a seamless way to connect to the cloud to store application data files and backup images as durable objects in Amazon S3 cloud storage with SMB or NFS-based access and local caching. However, this is a solution designed for on-premises servers, not EC2 instances and is not the best option for this scenario.

INCORRECT: "Extend the file share environment to Amazon Elastic File System (Amazon EFS) with a Multi-AZ configuration. Migrate all the data to Amazon EFS" is incorrect. EFS cannot be used with Microsoft workloads using the SMB protocol as it only supports Linux and NFS.

References:

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

https://docs.aws.amazon.com/fsx/latest/WindowsGuide/managing-file-shares.html

Save time with our AWS cheat sheets:

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

Question 20:

Skipped

A Solutions Architect is designing an application for processing and extracting data from log files. The log files are generated by an application and the number and frequency of updates varies. The files are up to 1 GB in size and processing will take around 40 seconds for each file.

Which solution is the most cost-effective?

- **Write the log files to an Amazon EC2 instance with an attached EBS volume. After processing, save the files to an Amazon S3 bucket**
- **Write the log files to an Amazon S3 bucket. Create an event notification to invoke an AWS Lambda function that will process the files**

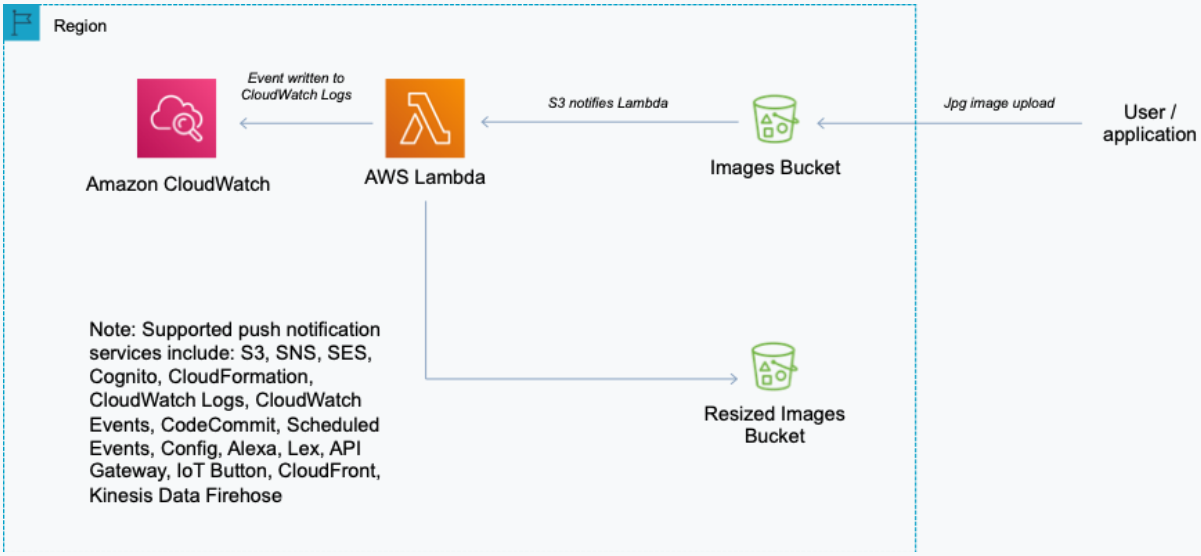
  (Correct)
- **Write the log files to an Amazon S3 bucket. Create an event notification to invoke an Amazon ECS task to process the files and save to an Amazon S3 bucket**
- **Write the log files to an Amazon SQS queue. Use AWS Lambda to process the files from the queue and save to an Amazon S3 bucket**

Explanation

The question asks for the most cost-effective solution and therefor a serverless and automated solution will be the best choice.

AWS Lambda can run custom code in response to Amazon S3 bucket events. You upload your custom code to AWS Lambda and create a function. When Amazon S3 detects an event of a specific type (for example, an object created event), it can publish

the event to AWS Lambda and invoke your function in Lambda. In response, AWS Lambda executes your function.



CORRECT: "Write the log files to an Amazon S3 bucket. Create an event notification to invoke an AWS Lambda function that will process the files" is the correct answer.

INCORRECT: "Write the log files to an Amazon EC2 instance with an attached EBS volume. After processing, save the files to an Amazon S3 bucket" is incorrect. This is not cost effective as it is not serverless.

INCORRECT: "Write the log files to an Amazon SQS queue. Use AWS Lambda to process the files from the queue and save to an Amazon S3 bucket" is incorrect. SQS has a maximum message size of 256 KB so the message body would need to be saved in S3 anyway. Using an event source mapping from S3 would be less complex and preferable.

INCORRECT: "Write the log files to an Amazon S3 bucket. Create an event notification to invoke an Amazon ECS task to process the files and save to an Amazon S3 bucket" is incorrect. You cannot use event notifications to process Amazon ECS tasks.

References:

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

Save time with our AWS cheat sheets:

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

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

Question 21:

Skipped

A three-tier web application is composed of a front end hosted on an Amazon EC2 instance in public subnet, application middleware hosted on EC2 in a private subnet and a database hosted on an Amazon RDS MySQL database in a private subnet. The database layer should be restricted to only allow incoming connections from the application.

Which of the following options makes sure that database can only be accessed by the application layer?

- **Create a security group that allows inbound traffic from the security group that is assigned to instances in the private subnets. Attach the security group to the DB instances.**

  (Correct)

- **Create a new route table that excludes the route to the public subnets' CIDR blocks. Associate the route table with the database subnets.**

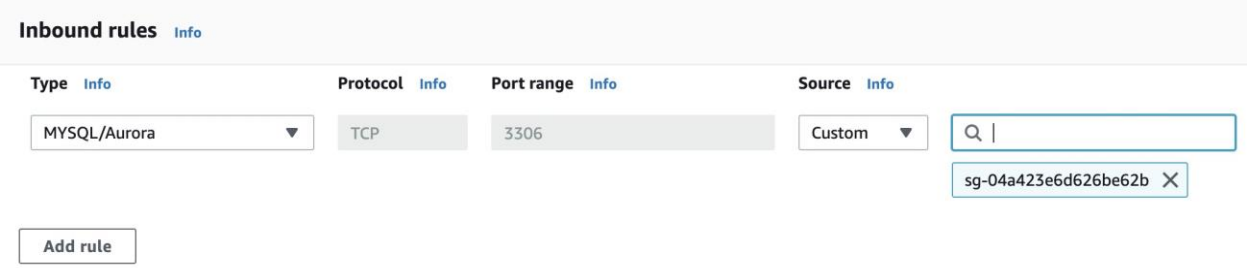
- **Create a security group that denies inbound traffic from the security group that is assigned to instances in the public subnets. Attach the security group to the DB instances.**

- **Create a new peering connection between the public subnets and the private subnets. Create a different peering connection between the private subnets and the database subnets.**

Explanation

Security groups are stateful. All inbound traffic is blocked by default in custom security groups. If you create an inbound rule allowing traffic in, that traffic is automatically allowed back out again. You cannot block specific IP address using Security groups (instead use Network Access Control Lists).

In this case the solution is to allow inbound traffic from the security group ID of the security group attached to the application layer. The rule should specify the appropriate protocol and port. This will ensure only the application layer can communicate with the database.



CORRECT: "Create a security group that allows inbound traffic from the security group that is assigned to instances in the private subnets. Attach the security group to the DB instances" is the correct answer (as explained above.)

INCORRECT: "Create a new route table that excludes the route to the public subnets' CIDR blocks. Associate the route table with the database subnets" is incorrect. This would simply stop routing from working within the VPC.

INCORRECT: "Create a security group that denies inbound traffic from the security group that is assigned to instances in the public subnets. Attach the security group to the DB instances" is incorrect.

You cannot create deny rules with security groups.

INCORRECT: "Create a new peering connection between the public subnets and the private subnets. Create a different peering connection between the private subnets and the database subnets" is incorrect.

Peering is used when multiple VPC's are to be connected with each other hence this is also an incorrect option.

References

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

Save time with our AWS cheat sheets:

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

Question 22:

Skipped

An application has been migrated from on-premises to an Amazon EC2 instance. The migration has failed due to an unknown dependency that the application must communicate with an on-premises server using private IP addresses.

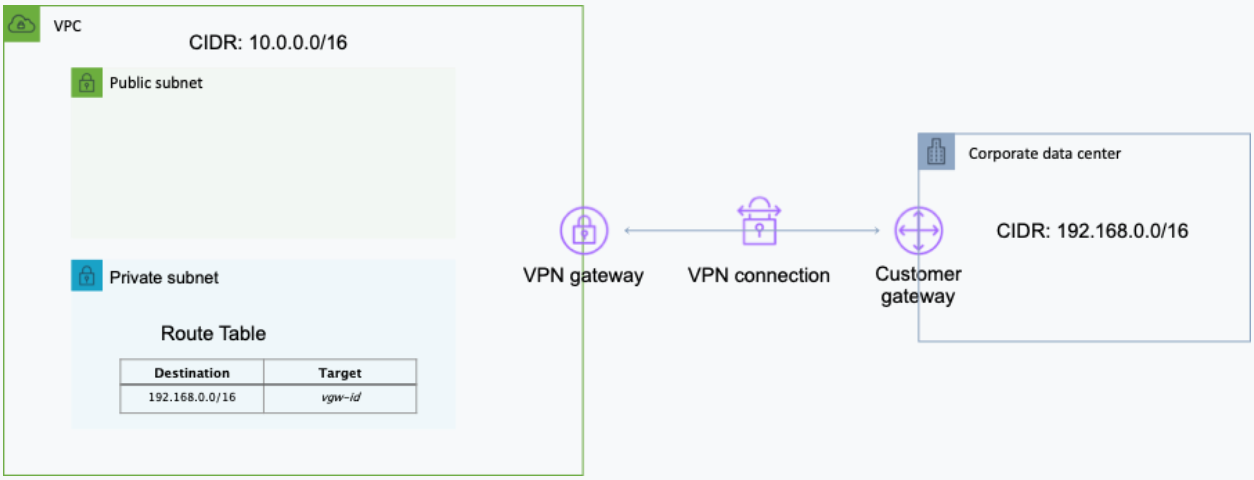
Which action should a solutions architect take to quickly provision the necessary connectivity?

- **Create an Amazon CloudFront distribution**
- **Configure a Virtual Private Gateway**

  (Correct)
- **Setup an AWS Direct Connect connection**
- **Create an AWS Transit Gateway**

Explanation

A virtual private gateway is a logical, fully redundant distributed edge routing function that sits at the edge of your VPC. You must create a VPG in your VPC before you can establish an AWS Managed site-to-site VPN connection. The other end of the connection is the customer gateway which must be established on the customer side of the connection.



CORRECT: "Configure a Virtual Private Gateway" is the correct answer.

INCORRECT: "Setup an AWS Direct Connect connection" is incorrect as this would take too long to provision.

INCORRECT: "Create an Amazon CloudFront distribution" is incorrect. This is not a solution for enabling connectivity using private addresses to an on-premises site. CloudFront is a content delivery network (CDN).

INCORRECT: "Create an AWS Transit Gateway" is incorrect. AWS Transit Gateway connects VPCs and on-premises networks through a central hub which is not a requirement of this solution.

References:

https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html

Save time with our AWS cheat sheets:

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

Question 23:

Skipped

A media company is running a production workload on thousands of EC2 instances which run a custom solution powered by third-party software. This software is subjected to regular updates and patches by the third-party organization.

How can a solutions architect patch all the instances quickly to remediate a security exposure?

- **Configure AWS Systems Manager Patch Manager to apply the patch to all EC2 instances.**

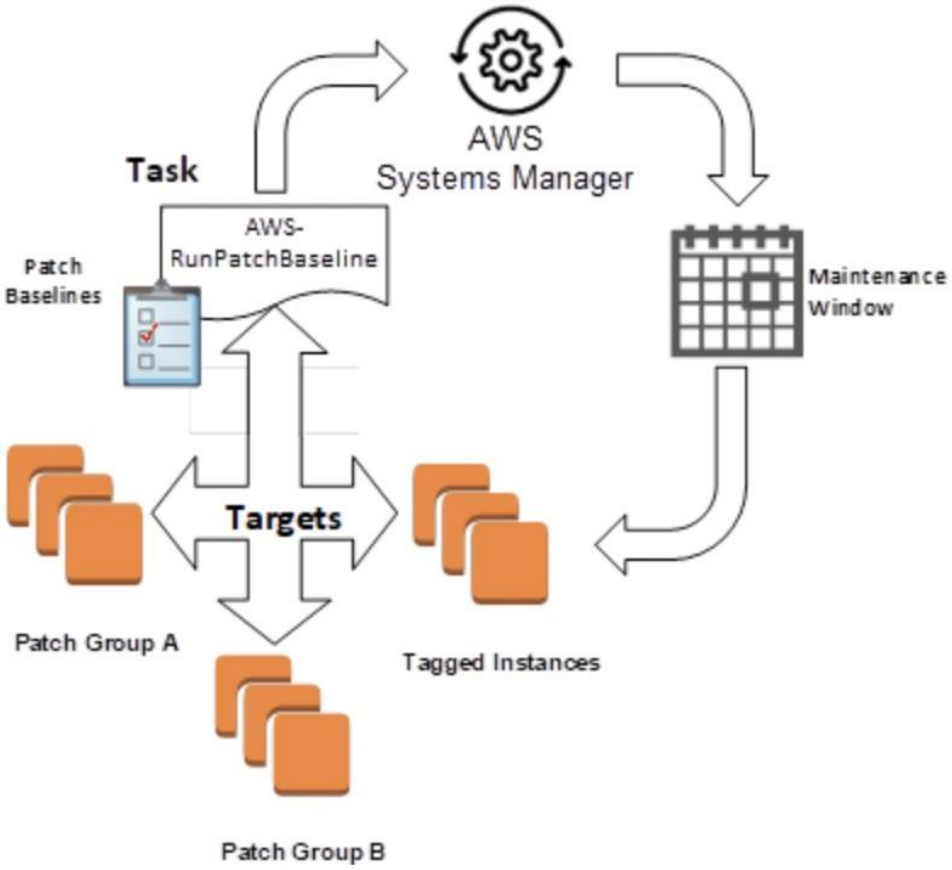
  (Correct)

- **Create an AWS Lambda function to apply the patch to all EC2 instances.**

- **Use AWS Systems Manager Run Command to run a custom command that applies the patch to all EC2 instances.**

- **Schedule an AWS Systems Manager maintenance window to apply the patch to all EC2 instances.**

Explanation



Patch Manager automates the process of patching Windows and Linux managed instances. Use this feature of AWS Systems Manager to scan your instances for missing patches or scan and install missing patches. You can install patches individually or to large groups of instances by using Amazon EC2 tags.

CORRECT: "Configure AWS Systems Manager Patch Manager to apply the patch to all EC2 instances" is the correct answer (as explained above.)

INCORRECT: "Create an AWS Lambda function to apply the patch to all EC2 instances" is incorrect. Since AWS already provides an out of the box solution of creating customizable patch groups enabling easy patching of EC2 instances, writing custom AWS Lambda is not the quickest/easiest solution.

INCORRECT: "Schedule an AWS Systems Manager maintenance window to apply the patch to all EC2 instances" is incorrect. This is a valid option and would hold in case there's a specific downtime or maintenance window when the patches are to be applied.

INCORRECT: "Use AWS Systems Manager Run Command to run a custom command that applies the patch to all EC2 instances" is incorrect. This option wouldn't work since the requirement is to have the patching done as quickly as possible and this would slow down the process.

References:

https://aws.amazon.com/blogs/mt/patching-your-windows-ec2-instances-using-aws-systems-manager-patch-manager/

Save time with our AWS cheat sheets:

https://digitalcloud.training/aws-systems-manager/

Question 24:

Skipped

A company has multiple AWS accounts for several environments (Prod, Dev, Test etc.). A Solutions Architect would like to copy an Amazon EBS snapshot from DEV to PROD. The snapshot is from an EBS volume that was encrypted with a custom key.

What steps must be performed to share the encrypted EBS snapshot with the Prod account? (choose 2)

- ☐ **Make a copy of the EBS volume and unencrypt the data in the process**
- ☐ **Create a snapshot of the unencrypted volume and share it with the Prod account**
- ☐ **Use CloudHSM to distribute the encryption keys use to encrypt the volume**
- ☐ **Modify the permissions on the encrypted snapshot to share it with the Prod account**

  (Correct)
- ☐

Share the custom key used to encrypt the volume

(Correct)

Explanation
When an EBS volume is encrypted with a custom key you must share the custom key with the PROD account. You also need to modify the permissions on the snapshot to share it with the PROD account. The PROD account must copy the snapshot before they can then create volumes from the snapshot

Note that you cannot share encrypted volumes created using a default CMK key and you cannot change the CMK key that is used to encrypt a volume.

CORRECT: "Share the custom key used to encrypt the volume" is a correct answer.

CORRECT: "Modify the permissions on the encrypted snapshot to share it with the Prod account" is also a correct answer.

INCORRECT: "Make a copy of the EBS volume and unencrypt the data in the process" is incorrect. You do not need to decrypt the data as there is a workable solution that keeps the data secure at all times.

INCORRECT: "Create a snapshot of the unencrypted volume and share it with the Prod account" is incorrect as the volume is already encrypted as security should be maintained.

INCORRECT: "Use CloudHSM to distribute the encryption keys use to encrypt the volume" is incorrect. CloudHSM is used for key management and storage but not distribution..

References:

https://aws.amazon.com/blogs/aws/new-cross-account-copying-of-encrypted-ebs-snapshots/

Save time with our AWS cheat sheets:

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

Question 25:
Skipped
A company runs an application on-premises that must consume a REST API running on Amazon API Gateway. The company has an AWS Direct Connect connection to their Amazon VPC. The solutions architect wants all API calls to use private addressing only and avoid the internet. How can this be achieved?

- **Use a hosted virtual interface and create a VPC Endpoint for Amazon API Gateway**

- **Use a public virtual interface and an AWS VPN to create a secure tunnel to Amazon API Gateway**

- **Use a private virtual interface and create a VPC Endpoint for Amazon API Gateway**

  (Correct)

- **Use a transit virtual interface and an AWS VPN to create a secure tunnel to Amazon API Gateway**

Explanation

The requirements are to avoid the internet and use private IP addresses only. The best solution is to use a private virtual interface across the Direct Connect connection to connect to the VPC using private IP addresses. A VPC endpoint for Amazon API Gateway can be created and this will provide access to API Gateway using private IP addresses and avoids the internet completely.

CORRECT: "Use a private virtual interface and create a VPC Endpoint for Amazon API Gateway" is the correct answer.

INCORRECT: "Use a hosted virtual interface and create a VPC Endpoint for Amazon API Gateway" is incorrect. A hosted virtual interface is used to allow another account to access your Direct Connect link.

INCORRECT: "Use a transit virtual interface and an AWS VPN to create a secure tunnel to Amazon API Gateway" is incorrect. A transit virtual interface is used to access Amazon VPC Transit Gateways which are not included in the solution.

INCORRECT: "Use a public virtual interface and an AWS VPN to create a secure tunnel to Amazon API Gateway" is incorrect. This will use the public internet so it is not allowed in this scenario.

References:

https://docs.aws.amazon.com/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.html

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

Save time with our AWS cheat sheets:

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

Question 26:

Skipped

A large company is currently using multiple AWS accounts as part of its cloud deployment model, and these accounts are currently structured using AWS Organizations. A Solutions Architect has been tasked with limiting access to an Amazon S3 bucket to only users of accounts that are enrolled with AWS Organizations. The Solutions Architect wants to avoid listing the many dozens of account IDs in the Bucket policy, as there are many accounts the frequent changes.

Which strategy meets these requirements with the LEAST amount of effort?

- **Use the global key of AWS Organizations within a bucket policy using the aws:PrincipalOrgID key to allow access only to accounts which are part of the Organization.**

  (Correct)

- **Add all the non-organizational accounts to an Organizational Unit (OU) and attached a Service Control Policy (SCP) which denies access to the specific Amazon S3 bucket.**

- **Use Attribute Based Access Control by referencing Tags of accounts which are either enrolled as part of AWS Organizations, or not.**

- **Use AWS Config and AWS Lambda functions to make remediations to the bucket policy as and when new accounts are created and tagged as not being part of AWS Organizations. Update the S3 bucket policy accordingly.**

Explanation

The aws:PrincipalOrgID global key provides a simpler alternative to manually listing and updating all the account IDs for all AWS accounts that exist within an Organization. The following Amazon S3 bucket policy allows members of any account in the '123456789' organization to add an object into the 'mydctbucket' bucket.

CORRECT: "Use the global key of AWS Organizations within a bucket policy using the aws:PrincipalOrgID key to allow access only to accounts which are part of the Organization" is the correct answer (as explained above.)

INCORRECT: "Use Attribute Based Access Control by referencing Tags of accounts which are either enrolled as part of AWS Organizations, or not" is incorrect. This could be a viable option, however maintaining an accurate tagging policy as opposed to referencing the PrincipalOrgID would much more difficult.

INCORRECT: "Use AWS Config and AWS Lambda functions to make remediations to the bucket policy as and when new accounts are created and tagged as not being part of AWS Organizations. Update the S3 bucket policy accordingly" is incorrect.

Every time an account is added or removed from the organization this workflow would have to fire. This solution would need to be built and maintained, whereas it is much easier to refer to the PrincipalOrgID once and avoid needing to change the Bucket Policy.

INCORRECT: "Add all the non-organizational accounts to an Organizational Unit (OU) and attached a Service Control Policy (SCP) which denies access to the specific Amazon S3 bucket" is incorrect. You can only use Organization Units (OUs) and Service Control Policies (SCPs) with accounts that are a part of AWS Organizations – meaning this solution could not work.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_condition-keys.html

Save time with our AWS cheat sheets:

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

Question 27:

Skipped

A company has deployed an API using Amazon API Gateway. There are many repeat requests and a solutions architect has been asked to implement measures to reduce request latency and the number of calls to the Amazon EC2 endpoint.

How can this be most easily achieved?

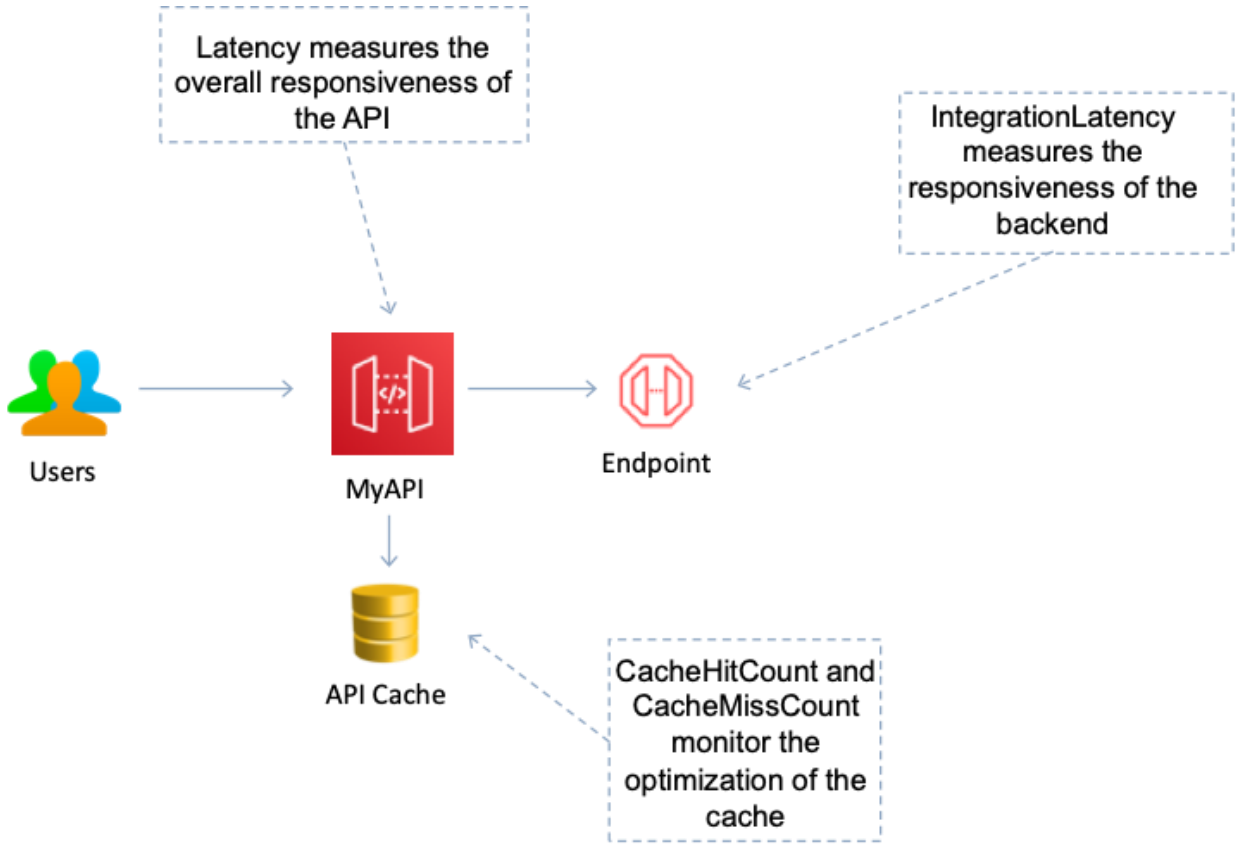
- **Configure a private endpoint place ElastiCache in front**
- **Create a cache for a stage and configure a TTL**

  (Correct)
- **Configure an edge-optimized endpoint with CloudFront**
- **Create a cache for a method and configure a TTL**

Explanation

You can enable API caching in Amazon API Gateway to cache your endpoint's responses. With caching, you can reduce the number of calls made to your endpoint and also improve the latency of requests to your API.

When you enable caching for a stage, API Gateway caches responses from your endpoint for a specified time-to-live (TTL) period, in seconds. API Gateway then responds to the request by looking up the endpoint response from the cache instead of making a request to your endpoint. The default TTL value for API caching is 300 seconds. The maximum TTL value is 3600 seconds. TTL=0 means caching is disabled.



CORRECT: "Create a cache for a stage and configure a TTL" is the correct answer.

INCORRECT: "Create a cache for a method and configure a TTL" is incorrect. An API cache is not enabled for a method, it is enabled for a stage.

INCORRECT: "Configure an edge-optimized endpoint with CloudFront" is incorrect. This is the default endpoint type with API Gateway so there's no reason to believe the solution architect needs to configure this. Users are routed to the nearest CloudFront point of presence (POP). However, caching still takes place within API gateway using a stage cache.

INCORRECT: "Configure a private endpoint place ElastiCache in front" is incorrect. You cannot use Amazon ElastiCache to cache API requests.

References:

https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-caching.html

Save time with our AWS cheat sheets:

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

Question 28:

Skipped

A Solutions Architect is attempting to clean up unused EBS volumes and snapshots to save some space and cost. How many of the most recent snapshots of an EBS volume need to be maintained to guarantee that you can recreate the full EBS volume from the snapshot?

- **The oldest snapshot, as this references data in all other snapshots**
- **Two snapshots, the oldest and most recent snapshots**
- **You must retain all snapshots as the process is incremental and therefore data is required from each snapshot**
- **Only the most recent snapshot. Snapshots are incremental, but the deletion process will ensure that no data is lost**

  (Correct)

Explanation

Snapshots capture a point-in-time state of an instance. If you make periodic snapshots of a volume, the snapshots are incremental, which means that only the blocks on the device that have changed after your last snapshot are saved in the new snapshot.

Even though snapshots are saved incrementally, the snapshot deletion process is designed so that you need to retain only the most recent snapshot in order to restore the volume.

CORRECT: "Only the most recent snapshot. Snapshots are incremental, but the deletion process will ensure that no data is lost" is the correct answer.

INCORRECT: "You must retain all snapshots as the process is incremental and therefore data is required from each snapshot" is incorrect as explained above.

INCORRECT: "Two snapshots, the oldest and most recent snapshots" is incorrect as explained above.

INCORRECT: "The oldest snapshot, as this references data in all other snapshots" is incorrect as explained above.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-deleting-snapshot.html

Save time with our AWS cheat sheets:

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

Question 29:

Skipped

A Solutions Architect manages multiple Amazon RDS MySQL databases. To improve security, the Solutions Architect wants to enable secure user access with short-lived credentials. How can these requirements be met?

- **Create the MySQL user accounts to use the AWSAuthenticationPlugin with IAM**

  (Correct)

- **Configure the MySQL databases to use the AWS Security Token Service (STS)**

- **Configure the MySQL databases to use AWS KMS data encryption keys**

- **Configure the application to use the AUTH command to send a unique password**

Explanation

With MySQL, authentication is handled by AWSAuthenticationPlugin—an AWS-provided plugin that works seamlessly with IAM to authenticate your IAM users. Connect to the DB instance and issue the CREATE USER statement, as shown in the following example.

```
1. CREATE USER jane_doe IDENTIFIED WITH AWSAuthenticationPlugin AS 'RDS';
```

The IDENTIFIED WITH clause allows MySQL to use the AWSAuthenticationPlugin to authenticate the database account (jane_doe). The AS 'RDS' clause refers to the authentication method, and the specified database account should have the same

name as the IAM user or role. In this example, both the database account and the IAM user or role are named jane_doe.

CORRECT: "Create the MySQL user accounts to use the AWSAuthenticationPlugin with IAM" is the correct answer.

INCORRECT: "Configure the MySQL databases to use the AWS Security Token Service (STS)" is incorrect. You cannot configure MySQL to directly use the AWS STS.

INCORRECT: "Configure the application to use the AUTH command to send a unique password" is incorrect. This is used with Redis databases, not with RDS databases.

INCORRECT: "Configure the MySQL databases to use AWS KMS data encryption keys" is incorrect. Data encryption keys are used for data encryption not management of connections strings.

References:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.IAMDBAuth.DBAccounts.html

Save time with our AWS cheat sheets:

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

Question 30:

Skipped

The AWS Acceptable Use Policy describes permitted and prohibited behavior on AWS and includes descriptions of prohibited security violations and network abuse. According to the policy, what is AWS's position on penetration testing?

- **AWS allow penetration testing for all resources**
- **AWS allow penetration testing by customers on their own VPC resources**
- **AWS allow penetration for some resources without prior authorization**

  (Correct)

- **AWS do not allow any form of penetration testing**

Explanation
AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for 8 services. Please check the AWS link below for the latest information.

CORRECT: "AWS allow penetration for some resources without prior authorization" is the correct answer.

INCORRECT: "AWS do not allow any form of penetration testing" is incorrect as explained above.

INCORRECT: "AWS allow penetration testing by customers on their own VPC resources" is incorrect as explained above.

INCORRECT: "AWS allow penetration testing for all resources" is incorrect as explained above.

References:

https://aws.amazon.com/security/penetration-testing/

Save time with our AWS cheat sheets:

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

Question 31:
Skipped
A company uses several Windows Servers as the operating system of choice for all their application servers hosted in their data center. The company wants to move some file servers into the cloud, and keep some in their data center, mounted to the same File System. The company also wants to maintain extremely low latency access to their on-premises data center, across a private network. The company has an AWS Direct Connect connection set up into the us-east-1 Region.

What should a solutions architect do to meet these requirements?

- **Install an SMB client on to the on-premises servers and mount an Amazon FSx file system to the servers. Mount the same file system to the EC2 instances within the Amazon VPC. Use the existing Direct Connect connection to connect the on-premises data center to the Amazon VPC.**

(Correct)

- **Migrate all the data to Amazon DynamoDB Local. Ensure all users have the appropriate IAM permissions to access the relevant files.**

- **Use Amazon S3 on Outposts and mount the S3 File Gateway on to the on-premises servers.**

- **Install an NFS client on to the on-premises servers and mount an Amazon EFS file system to the servers. Mount the same file system to the EC2 instances within the Amazon VPC. Use the existing Direct Connect connection to connect the on-premises data center to the Amazon VPC.**

Explanation

The current AWS Direct connect connection will provide the ability to share a file system between on-premises servers and Amazon EC2 instances in the AWS Cloud. Direct Connect provides low latency access to their on-premises data center, and the company's use of Windows File Servers necessitates the use of an SMB-based Amazon FSx File System.

CORRECT: "Install an SMB client on to the on-premises servers and mount an Amazon FSx file system to the servers. Mount the same file system to the EC2 instances within the Amazon VPC. Use the existing Direct Connect connection to connect the on-premises data center to the Amazon VPC" is the correct answer (as explained above.)

INCORRECT: "Migrate all the data to Amazon DynamoDB Local. Ensure all users have the appropriate IAM permissions to access the relevant files" is incorrect. This will not give the company the use of a Windows File Server, and instead give them a NoSQL database. DynamoDB Local is not suitable for this use case.

INCORRECT: "Use Amazon S3 on Outposts and mount the S3 File Gateway on to the on-premises servers" is incorrect. Amazon S3 on Outposts would not provide a hybrid cloud experience as required by the customer, and S3 File Gateway uses a Linux based file system, which is incompatible with the Windows setup the company currently uses.

INCORRECT: "Install an NFS client on to the on-premises servers and mount an Amazon EFS file system to the servers. Mount the same file system to the EC2 instances within the Amazon VPC. Use the existing Direct Connect connection to connect the on-premises data center to the Amazon VPC" is incorrect.

Amazon EFS is a file system that is accessed using the NFS protocol and is suitable for Linux clients only. This is not natively supported for Window Servers, making this an unsuitable option.

References:

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

Save time with our AWS cheat sheets:

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

Question 32:

Skipped

A company runs an API on a Linux server in their on-premises data center. The company are planning to migrate the API to the AWS cloud. The company require a highly available, scalable and cost-effective solution. What should a Solutions Architect recommend?

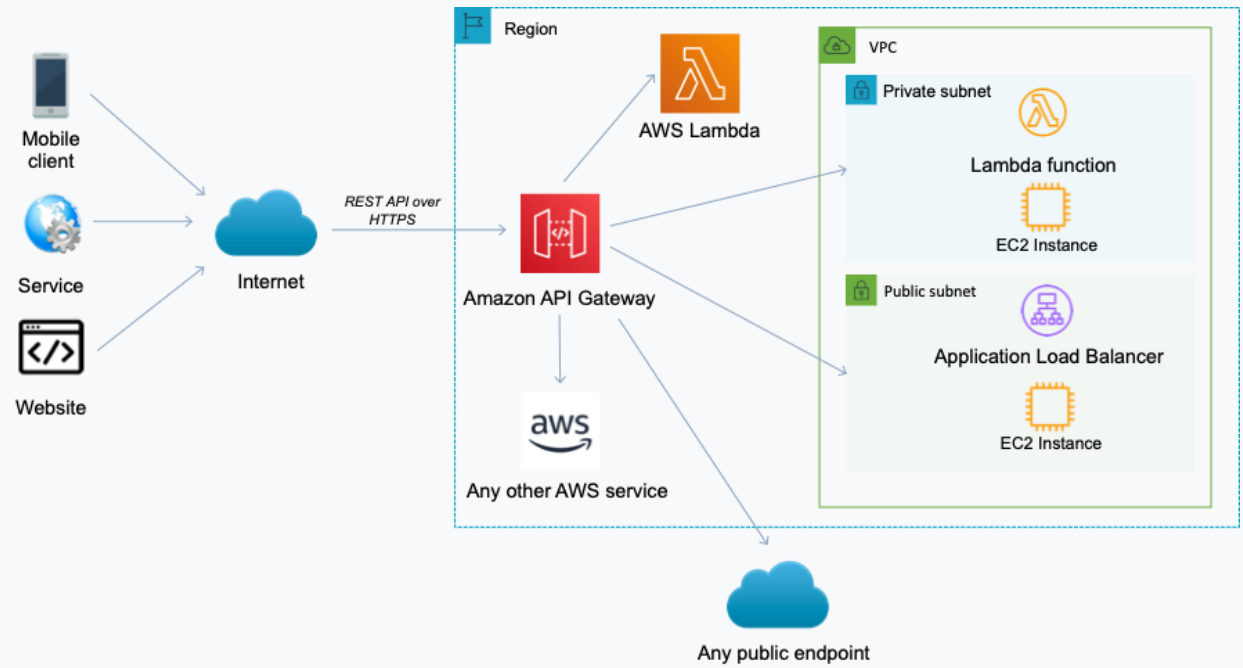
- **Migrate the API to Amazon API Gateway and migrate the backend to Amazon EC2**
- **Migrate the API server to Amazon EC2 instances in an Auto Scaling group and attach an Application Load Balancer**
- **Migrate the API to Amazon CloudFront and use AWS Lambda as the origin**
- **Migrate the API to Amazon API Gateway and use AWS Lambda as the backend**

(Correct)

Explanation

The best option is to use a fully serverless solution. This will provide high availability, scalability and be cost-effective. The components for this would be Amazon API Gateway for hosting the API and AWS Lambda for running the backend.

As you can see in the image below, API Gateway can be the frontend for multiple backend services:



CORRECT: "Migrate the API to Amazon API Gateway and use AWS Lambda as the backend" is the correct answer.

INCORRECT: "Migrate the API to Amazon API Gateway and migrate the backend to Amazon EC2" is incorrect. This is a less available and cost-effective solution for the backend compared to AWS Lambda.

INCORRECT: "Migrate the API server to Amazon EC2 instances in an Auto Scaling group and attach an Application Load Balancer" is incorrect. Firstly, it may be difficult to load balance to an API. Additionally, this is a less cost-effective solution.

INCORRECT: "Migrate the API to Amazon CloudFront and use AWS Lambda as the origin" is incorrect. You cannot migrate an API to CloudFront. You can use CloudFront in front of API Gateway but that is not what this answer specifies.

References:

https://docs.aws.amazon.com/apigateway/latest/developerguide/getting-started-with-lambda-integration.html

Save time with our AWS cheat sheets:

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

Question 33:

Skipped

A retail company is running an important event. The company require guaranteed capacity in two specific Availability Zones in a specific AWS Region for running Amazon EC2 instances for 5 consecutive days.

What is the best way to ensure guaranteed EC2 capacity?

- **Create an On-Demand Capacity Reservation that specifies the Region.**
- **Create an On-Demand Capacity Reservation that specifies the Region and two Availability Zones needed.**

  (Correct)
- **Purchase Reserved Instances that specify the Region and two Availability Zones needed.**
- **Purchase Reserved Instances that specify the Region.**

Explanation

On-Demand Capacity Reservations enable you to reserve compute capacity for your Amazon EC2 instances in a specific Availability Zone for any duration.

When creating Capacity Reservations, you ensure that you always have access to EC2 capacity when you need it, for as long as you need it, in this case for 5 days. You can create Capacity Reservations at any time, without entering a one-year or three-year term commitment.

Also, when you create a Capacity Reservation, you specify:

- The Availability Zone in which to reserve the capacity.

- The number of instances for which to reserve capacity.

- The instance attributes, including the instance type, tenancy, and platform/OS.

CORRECT: "Create an On-Demand Capacity Reservation that specifies the Region and two Availability Zones needed" is the correct answer (as explained above.)

INCORRECT: "Purchase Reserved Instances that specify the Region" is incorrect. Reserved Instances do not provide guaranteed capacity and are solely a billing discount.

INCORRECT: "Create an On-Demand Capacity Reservation that specifies the Region" is incorrect as you must specify the Availability zones required when reserving capacity.

INCORRECT: "Purchase Reserved Instances that specify the Region and two Availability Zones needed" is incorrect. Reserved Instances do not provide guaranteed capacity and are solely a billing discount.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-capacity-reservations.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/aws-billing-and-pricing/

Question 34:

Skipped

An application is used by a large bank to ingest incoming messages. The messages are then quickly consumed by dozens of other applications and microservices. The number of messages can increase suddenly from a few messages per second up to 120,000 messages per second. In response to several recent outages and failures, the company wants to decouple this applications architecture and solution to ensure scalability.

Which solution meets these requirements?

- **Persist the messages in Amazon Kinesis Data Analytics. Make sure the consumer applications are configured to read and process the messages.**
- **Write the messages to Amazon Kinesis Data Streams using one shard. Use an AWS Lambda function to process messages and place them in a DynamoDB table. The Applications can then be read from the DynamoDB table.**

Post the messages to an Amazon Simple Notification Service topic with multiple Amazon Simple Queue Service subscriptions. Process messages from queues using the Consumer Applications.

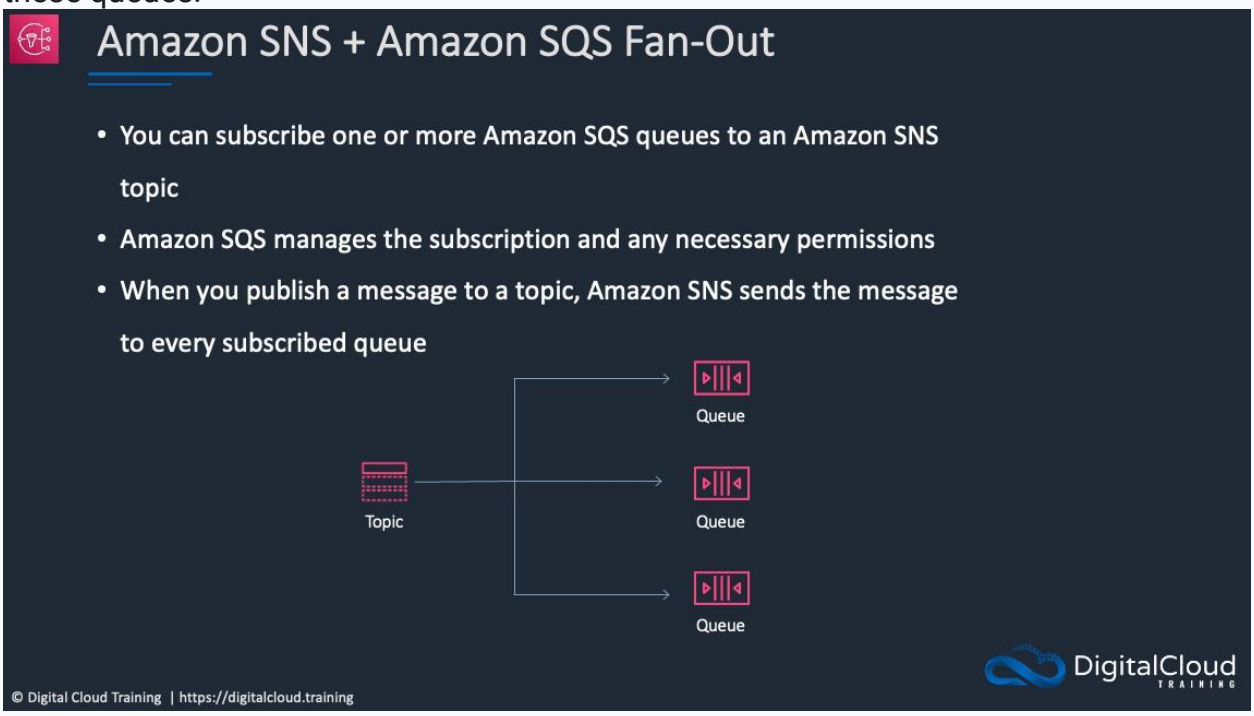
(Correct)

-

Deploy the ingestion application on Amazon EC2 instances in an Auto Scaling group and scale up and down based on CPU Utilization.

Explanation

Amazon SNS can be used in this situation in a fanout architecture where messages sent to the SNS topic and then forwarded to multiple SQS queues that are subscribed to the topic. The messages can then be processed by different consumer applications from these queues.



CORRECT: "Post the messages to an Amazon Simple Notification Service topic with multiple Amazon Simple Queue Service subscriptions. Process messages from queues using the Consumer Applications" is the correct answer (as explained above.)

INCORRECT: "Persist the messages in Amazon Kinesis Data Analytics. Make sure the consumer applications are configured to read and process the messages" is incorrect. Amazon Kinesis Data Analytics is used for analyzing data using SQL, it is not used for ingesting messages.

INCORRECT: "Deploy the ingestion application on Amazon EC2 instances in an Auto Scaling group and scale up and down based on CPU Utilization" is incorrect. This is not

a scalable enough architecture for the application's needs as scaling based on auto scaling groups can take many minutes, not seconds as is required for the application.

INCORRECT: "Write the messages to Amazon Kinesis Data Streams using one shard. Use an AWS Lambda function to process messages and place them in a DynamoDB table. The Applications can then be read from the DynamoDB table" is incorrect. A single shard is limited to 1 MB or 1000 messages/sec, therefore multiple shards would be required.

References:

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

Save time with our AWS cheat sheets:

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

Question 35:

Skipped

A company wants to improve its ability to clone large amounts of production data into a test environment in the same AWS Region. The data is stored in Amazon EC2 instances on Amazon Elastic Block Store (Amazon EBS) volumes. Modifications to the cloned data must not affect the production environment. The software that accesses this data requires consistently high I/O performance.

A solutions architect needs to minimize the time that is required to clone the production data into the test environment.

Which solution will meet these requirements?

- **Take EBS snapshots of the production EBS volumes. Restore the snapshots onto EC2 instance store volumes in the test environment.**
- **Configure the production EBS volumes to use the EBS Multi-Attach feature. Take EBS snapshots of the production EBS volumes. Attach the production EBS volumes to the EC2 instances in the test environment.**
- **Take EBS snapshots of the production EBS volumes. Turn on the EBS fast snapshot restore feature on the EBS snapshots. Restore the snapshots into**

new EBS volumes. Attach the new EBS volumes to EC2 instances in the test environment.

(Correct)

- 

Take EBS snapshots of the production EBS volumes. Create and initialize new EBS volumes. Attach the new EBS volumes to EC2 instances in the test environment before restoring the volumes from the production EBS snapshots.

Explanation

Amazon EBS fast snapshot restore (FSR) enables you to create a volume from a snapshot that is fully initialized at creation. This eliminates the latency of I/O operations on a block when it is accessed for the first time. Volumes that are created using fast snapshot restore instantly deliver all their provisioned performance.

CORRECT: "Take EBS snapshots of the production EBS volumes. Turn on the EBS fast snapshot restore feature on the EBS snapshots. Restore the snapshots into new EBS volumes. Attach the new EBS volumes to EC2 instances in the test environment" is the correct answer (as explained above.)

INCORRECT: "Take EBS snapshots of the production EBS volumes. Restore the snapshots onto EC2 instance store volumes in the test environment" is incorrect. You cannot restore EBS snapshots to instance store volumes. Instance store volumes are ephemeral storage volumes and are not used for data that requires persistence.

INCORRECT: "Take EBS snapshots of the production EBS volumes. Create and initialize new EBS volumes. Attach the new EBS volumes to EC2 instances in the test environment before restoring the volumes from the production EBS snapshots" is incorrect.

This solution may take longer and may not have the consistent performance that is offered with the correct answer.

INCORRECT: "Configure the production EBS volumes to use the EBS Multi-Attach feature. Take EBS snapshots of the production EBS volumes. Attach the production EBS volumes to the EC2 instances in the test environment" is incorrect.

Amazon EBS Multi-Attach enables you to attach a single Provisioned IOPS SSD (io1 or io2) volume to multiple instances that are in the same Availability Zone. You can attach multiple Multi-Attach enabled volumes to an instance or set of instances. This does not help with the requirements of this solution.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-fast-snapshot-restore.html

Save time with our AWS cheat sheets:

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

Question 36:

Skipped

A social media application is creating new functionality that will convert uploaded images to smaller, thumbnail images. When a user uploads an image through the web interface, the application should store the image in an Amazon S3 bucket, process and compress the image with an AWS Lambda function and store the image in its compressed form in a different S3 bucket.

The solution architect must develop a stateless, durable solution to process images automatically upon upload.

Which combination of actions will meet these requirements? (Select TWO.)

- ☐ **Configure the Lambda function to use the Amazon SQS queue as the event source. The Lambda function will resize the image and store it in a separate S3 Bucket.**

  (Correct)

- ☐ **Create an Amazon SQS queue. Configure an event notification to add a message to the SQS queue when an image is uploaded to the S3 bucket.**

  (Correct)

- ☐ **Launch an Amazon EC2 instance to connect to an Amazon SQS queue. When items are added to the queue, log the file name in a text file on the EC2 instance and invoke the Lambda function.**

- ☐

Configure an Amazon EventBridge event to monitor the S3 bucket. When an image is uploaded, send an alert to an Amazon SNS topic with the application owner's email address for further processing.

-

Configure the S3 Bucket to be an event source for a Lambda Function. When an uploaded image is detected, write the file name to a text file in memory and use the text file to keep track of the images that were processed.

Explanation

You can use event notifications to publish an event to a destination when something happens in a bucket. Destinations include Lambda, SNS, and SQS. In this case the event notification can be configured to publish a message to an SQS queue when an object creation event occurs.

Lambda can be configured to poll the queue looking for new messages. When a message is added to the queue Lambda can process the message which will let the function know which image to resize. The resized image can then be saved to an output bucket.

CORRECT: "Create an Amazon SQS queue. Configure an event notification to add a message to the SQS queue when an image is uploaded to the S3 bucket" is the correct answer (as explained above.)

CORRECT: "Configure the Lambda function to use the Amazon SQS queue as the event source. The Lambda function will resize the image and store it in a separate S3 Bucket" is also the correct answer (as explained above.)

INCORRECT: "Configure the S3 Bucket to be an event source for a Lambda Function. When an uploaded image is detected, write the file name to a text file in memory and use the text file to keep track of the images that were processed" is incorrect. This solution saves state in memory which is not durable.

INCORRECT: "Launch an Amazon EC2 instance to connect to an Amazon SQS queue. When items are added to the queue, log the file name in a text file on the EC2 instance and invoke the Lambda function" is incorrect. A single EC2 instance is not a durable solution, as if the single instance failed the solution would no longer work.

INCORRECT: "Configure an Amazon EventBridge event to monitor the S3 bucket. When an image is uploaded, send an alert to an Amazon SNS topic with the application owner's email address for further processing" is incorrect. An event notification should be created on the S3 bucket to publish information about object creation events. Destinations can be Lambda, SNS, or SQS.

References:

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

Save time with our AWS cheat sheets:

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

Question 37:

Skipped

To trace a recent production incident a product manager needs to view logs in the Amazon CloudWatch logs. These logs are linked to events over the course of a week and may be needed in the future if incidents occur again. The product manager doesn't have administrative access to the AWS account as it is managed by a third-party management company.

According to principal of least privilege, which option out of the below will fulfill the requirement to provide the necessary access for the product manager?

- **Share the dashboard from the CloudWatch console. Enter the client's email address and complete the sharing steps. Provide a shareable link for the dashboard to the product manager.**

  (Correct)

- **Create an IAM user specifically for the product manager. Attach the CloudWatchReadOnlyAccess AWS managed policy to the user. Share the new login credentials with the product manager. Share the browser URL of the correct dashboard with the product manager.**

- **Create an IAM user for the company's employees. Attach the ViewOnly Access AWS managed policy to the IAM user. Share the new login credentials with the product manager. Ask the product manager to navigate to the CloudWatch console and locate the dashboard by name in the Dashboards section.**

- **Deploy a bastion server in a public subnet. When the product manager requires access to the dashboard, start the server and share the RDP credentials. On the bastion server, ensure that the browser is configured to**

open the dashboard URL with cached AWS credentials that have appropriate permissions to view the dashboard.

Explanation

Below is the sequence for sharing the dashboard from Cloud watch console.

CloudWatch > Dashboard > Select your board > Share Dashboard>Share your dashboard and require a username and password>Enter mail address

You can share your CloudWatch dashboards with people who do not have direct access to your AWS account. This enables you to share dashboards across teams, with stakeholders, and with people external to your organization. You can even display dashboards on big screens in team areas or embed them in Wikis and other webpages.

CORRECT: "Share the dashboard from the CloudWatch console. Enter the product manager's email address and complete the sharing steps. Provide a shareable link for the dashboard to the product manager" is the correct answer (as explained above.)

INCORRECT: "Create an IAM user specifically for the product manager. Attach the CloudWatchReadOnlyAccess AWS managed policy to the user. Share the new login credentials with the product manager. Share the browser URL of the correct dashboard with the product manager" is incorrect.

If the dashboard needs to be shared with additional users, this option increases manual effort every time and hence is not an optimal option.

INCORRECT: "Create an IAM user for the company's employees. Attach the ViewOnly Access AWS managed policy to the IAM user. Share the new login credentials with the product manager. Ask the product manager to navigate to the CloudWatch console and locate the dashboard by name in the Dashboards section" is incorrect.

This option also involves lot of manual steps and as the recipients for the dashboard increase in number, manual effort increase and hence this is not an optimal option.

INCORRECT: "Deploy a bastion server in a public subnet. When the product manager requires access to the dashboard, start the server and share the RDP credentials. On the bastion server, ensure that the browser is configured to open the dashboard URL with cached AWS credentials that have appropriate permissions to view the dashboard" is incorrect.

Exposing bastion server isn’t required here for sharing the dashboard. Bastion servers are meant to be jump boxes to allow accesses to EC2 instances which isn’t the ask in the question hence this is also an incorrect option.

References:

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-dashboard-sharing.html

Save time with our AWS cheat sheets:

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

Question 38:

Skipped

A Solutions Architect needs to create a file system that can be concurrently accessed by multiple Amazon EC2 instances across multiple availability zones. The file system needs to support high throughput and the ability to burst. As the data that will be stored on the file system will be sensitive, it must be encrypted at rest and in transit.

Which storage solution should the Solutions Architect use for the shared file system?

- **Use the Elastic Block Store (EBS) and mount the file system at the block level**
- **Add EBS volumes to each EC2 instance and use an ELB to distribute data evenly between the volumes**
- **Add EBS volumes to each EC2 instance and configure data replication**
- **Use the Elastic File System (EFS) and mount the file system using NFS**

  (Correct)

Explanation

EFS is a fully-managed service that makes it easy to set up and scale file storage in the Amazon Cloud. EFS file systems are mounted using the NFSv4.1 protocol. EFS is designed to burst to allow high throughput levels for periods of time. EFS also offers the ability to encrypt data at rest and in transit.

CORRECT: "Use the Elastic File System (EFS) and mount the file system using NFS" is the correct answer.

INCORRECT: "Add EBS volumes to each EC2 instance and configure data replication" is incorrect. Adding EBS volumes to each instance and configuring data replication is not the best solution for this scenario and there is no native capability within AWS for performing the replication. Some 3rd party data management software does use this model, however.

INCORRECT: "Use the Elastic Block Store (EBS) and mount the file system at the block level" is incorrect. EBS is a block-level storage system not a file-level storage system. You cannot mount EBS volumes from multiple instances across AZs.

INCORRECT: "Add EBS volumes to each EC2 instance and use an ELB to distribute data evenly between the volumes" is incorrect. You cannot use an ELB to distribute data between EBS volumes.

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 39:

Skipped

A Solutions Architect is designing a migration strategy for a company moving to the AWS Cloud. The company use a shared Microsoft filesystem that uses Distributed File System Namespaces (DFSN). What will be the MOST suitable migration strategy for the filesystem?

- **Use AWS DataSync to migrate to Amazon FSx for Windows File Server**

  (Correct)

- **Use the AWS Server Migration Service to migrate to Amazon FSx for Lustre**

- **Use AWS DataSync to migrate to an Amazon EFS filesystem**

-

Use the AWS Server Migration Service to migrate to an Amazon S3 bucket

Explanation

The destination filesystem should be Amazon FSx for Windows File Server. This supports DFSN and is the most suitable storage solution for Microsoft filesystems. AWS DataSync supports migrating to the Amazon FSx and automates the process.

CORRECT: "Use AWS DataSync to migrate to Amazon FSx for Windows File Server" is the correct answer.

INCORRECT: "Use the AWS Server Migration Service to migrate to Amazon FSx for Lustre" is incorrect. The server migration service is used to migrate virtual machines and FSx for Lustre does not support Windows filesystems.

INCORRECT: "Use AWS DataSync to migrate to an Amazon EFS filesystem" is incorrect. You can migrate data to EFS using DataSync but it is the wrong destination for a Microsoft filesystem (Linux only).

INCORRECT: "Use the AWS Server Migration Service to migrate to an Amazon S3 bucket" is incorrect. The server migration service is used to migrate virtual machines and Amazon S3 is an object-based storage system and unsuitable for hosting a Microsoft filesystem.

References:

https://aws.amazon.com/blogs/storage/migrate-to-amazon-fsx-for-windows-file-server-using-aws-datasync/

https://docs.aws.amazon.com/fsx/latest/WindowsGuide/migrate-files-fsx.html

Save time with our AWS cheat sheets:

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

Question 40:

Skipped

An application analyzes images of people that are uploaded to an Amazon S3 bucket. The application determines demographic data which is then saved to a .CSV file in another S3 bucket. The data must be encrypted at rest and then queried using SQL. The solution should be fully serverless.

Which actions should a Solutions Architect take to encrypt and query the data?

Use AWS KMS encryption keys for the S3 bucket and use Amazon Kinesis Data Analytics to query the data

-

Use AWS KMS encryption keys for the S3 bucket and use Amazon Athena to query the data

(Correct)

-

Use Amazon S3 server-side encryption and use Amazon RedShift Spectrum to query the data

-

Use Amazon S3 server-side encryption and Amazon QuickSight to query the data

Explanation

Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run. Amazon Athena supports encrypted data for both the source data and query results, for example, using Amazon S3 with AWS KMS.

CORRECT: "Use AWS KMS encryption keys for the S3 bucket and use Amazon Athena to query the data" is the correct answer.

INCORRECT: "Use Amazon S3 server-side encryption and use Amazon RedShift Spectrum to query the data" is incorrect. RedShift Spectrum is not serverless as it requires a RedShift cluster which is based on EC2 instances.

INCORRECT: "Use AWS KMS encryption keys for the S3 bucket and use Amazon Kinesis Data Analytics to query the data" is incorrect. Kinesis Data Analytics is used for analyzing real-time streaming data in Kinesis streams.

INCORRECT: "Use Amazon S3 server-side encryption and Amazon QuickSight to query the data" is incorrect. Amazon QuickSight is an interactive dashboard, it is not a service for running queries on data.

References:

https://d1.awsstatic.com/whitepapers/architecture/wellarchitected-Machine-Learning-Lens.pdf

https://aws.amazon.com/athena/

Save time with our AWS cheat sheets:

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

Question 41:

Skipped

A law firm has recently productionized a three-tier web application that is deployed on AWS. The web servers are deployed in a public subnet in a VPC. The application servers and database servers are deployed in private subnets in the same VPC. The company has deployed a third-party virtual firewall appliance from the AWS Marketplace in an inspection VPC. The appliance is configured with an IP interface that can accept IP packets.

A solutions architect needs to integrate the web application with the appliance to inspect all traffic to the application before the traffic reaches the web server.

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

- **Create an Application Load Balancer in the public subnet of the application's VPC to route the traffic to the appliance for packet inspection.**
- **Deploy a Gateway Load Balancer in the inspection VPC. Create a Gateway Load Balancer endpoint to receive the incoming packets and forward the packets to the appliance.**

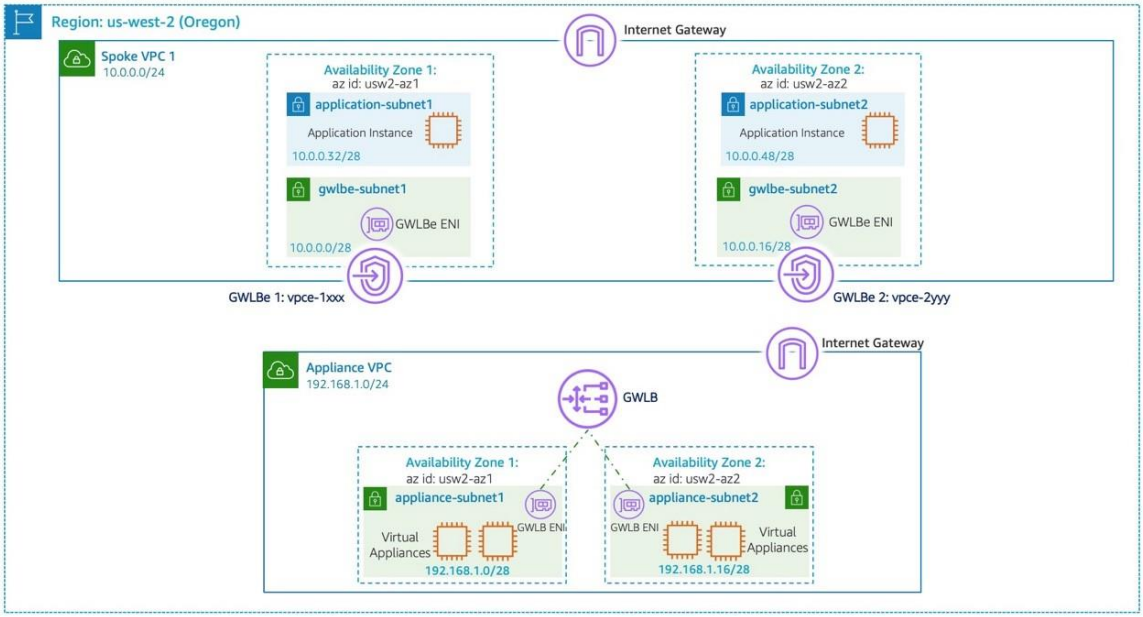
  (Correct)
- **Create a Network Load Balancer in the public subnet of the application's VPC to route the traffic to the appliance for packet inspection.**
- **Deploy a transit gateway in the inspection VPC. Configure route tables to route the incoming packets through the transit gateway.**

Explanation

Gateway Load Balancers enable you to deploy, scale, and manage virtual appliances, such as firewalls, intrusion detection and prevention systems, and deep packet

inspection systems. It combines a transparent network gateway (that is, a single entry and exit point for all traffic) and distributes traffic while scaling your virtual appliances with the demand.

GWLB: Gateway Load Balancer
GWLBe: Gateway Load Balancer Endpoint



CORRECT: "Deploy a Gateway Load Balancer in the inspection VPC. Create a Gateway Load Balancer endpoint to receive the incoming packets and forward the packets to the appliance" is the correct answer (as explained above.)

INCORRECT: "Create a Network Load Balancer in the public subnet of the application's VPC to route the traffic to the appliance for packet inspection" is incorrect.

Network load balancers work on Layer 4 of the OSI model and work on TCP, UDP and TLS protocols. They are not used for packet inspection.

INCORRECT: "Create an Application Load Balancer in the public subnet of the application's VPC to route the traffic to the appliance for packet inspection" is incorrect.

Application load balancers work on Layer 7 and used with HTTP/HTTPS traffic. They are also not used for packet inspection.

INCORRECT: "Deploy a transit gateway in the inspection VPC. Configure route tables to route the incoming packets through the transit gateway" is incorrect.

Transit Gateways are used for routing traffic and connecting networks and VPCs, they are not used for packet inspection purposes. In this case a load balancer is required to distributed connections to the virtual firewall appliances.

References:

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

https://aws.amazon.com/blogs/networking-and-content-delivery/scaling-network-traffic-inspection-using-aws-gateway-load-balancer/

Save time with our AWS cheat sheets:

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

Question 42:

Skipped

A law firm has recently moved an on-premises multi-tier web application to AWS. Currently, the web application is based on a containerized solution and is running inside Linux based EC2 instances which connect to a PostgreSQL database hosted on separate but dedicated EC2 instances. The company wishes to optimize operational efficiency and performance.

Which combination of actions should the solutions architect take? (Select TWO.)

- ☐ **Migrate the web application to be hosted on AWS Fargate with Amazon Elastic Container Service (Amazon ECS).**

  (Correct)

- ☐ **Set up Amazon ElastiCache between the web application and the PostgreSQL database.**

- ☐ **Migrate the web application to the same Amazon EC2 instances as the database.**

- ☐ **Set up an Amazon CloudFront distribution for the web application content.**

- ☐ **Migrate the PostgreSQL database to Amazon Aurora.**

(Correct)

Explanation
Amazon Aurora (Aurora) is a fully managed relational database engine that's compatible with MySQL and PostgreSQL. You already know how MySQL and PostgreSQL combine the speed and reliability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases. The code, tools, and applications you use today with your existing MySQL and PostgreSQL databases can be used with Aurora. With some workloads, Aurora can deliver up to five times the throughput of MySQL and up to three times the throughput of PostgreSQL without requiring changes to most of your existing applications.

Amazon ECS is a fully managed container orchestration service that makes it easy for you to deploy, manage, and scale containerized applications. This is a better hosting solution for a containerized solution rather than managing the underlying container platform yourself. In the case of Fargate, the solution is serverless, so it massively reduces operational overhead.

CORRECT: "Migrate the PostgreSQL database to Amazon Aurora and Migrate the web application to be hosted on AWS Fargate with Amazon Elastic Container Service (Amazon ECS)" are the correct answers (as explained above)

INCORRECT: "Migrate the web application to the same Amazon EC2 instances as the database" is incorrect. This might reduce cost but doesn't offer any other advantages.

INCORRECT: "Set up an Amazon CloudFront distribution for the web application content" is incorrect. CloudFront helps with caching content globally for better performance but does not help reduce the operational overhead or performance of this solution.

INCORRECT: "Set up Amazon ElastiCache between the web application and the PostgreSQL database" is incorrect. Caching will only help when you have hot data segments and does not reduce the operational overhead of this solution.

References:

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

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Updates.Versions.html#AuroraMySQL.Updates.UpgradePaths

Save time with our AWS cheat sheets:

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

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

Question 43:

Skipped

A large quantity of data is stored on a NAS device on-premises and accessed using the SMB protocol. The company require a managed service for hosting the filesystem and a tool to automate the migration.

Which actions should a Solutions Architect take?

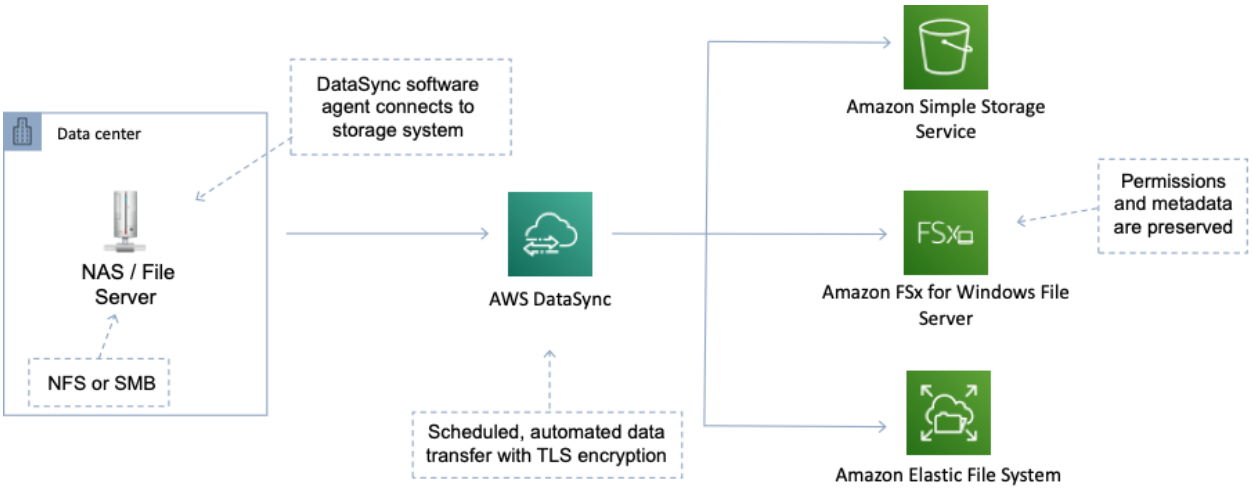
- **Migrate the data to Amazon EFS using the AWS Server Migration Service (SMS)**
- **Migrate the data to Amazon FSx for Windows File Server using AWS DataSync**

  (Correct)
- **Migrate the data to Amazon S3 using and AWS Snowball Edge device**
- **Migrate the data to Amazon FSx for Lustre using AWS DataSync**

Explanation

Amazon FSx for Windows File Server provides fully managed, highly reliable, and scalable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol. This is the most suitable destination for this use case.

AWS DataSync can be used to move large amounts of data online between on-premises storage and Amazon S3, Amazon EFS, or Amazon FSx for Windows File Server. The source datastore can be Server Message Block (SMB) file servers.



CORRECT: "Migrate the data to Amazon FSx for Windows File Server using AWS DataSync" is the correct answer.

INCORRECT: "Migrate the data to Amazon EFS using the AWS Server Migration Service (SMS)" is incorrect. EFS is used for hosting filesystems accessed over NFS from Linux (not Windows). The SMS service is used for migrating virtual machines, not data.

INCORRECT: "Migrate the data to Amazon FSx for Lustre using AWS DataSync" is incorrect. Amazon FSx for Windows File Server should be used for hosting SMB shares.

INCORRECT: "Migrate the data to Amazon S3 using and AWS Snowball Edge device" is incorrect. Amazon S3 is an object store and unsuitable for hosting an SMB filesystem. Snowball is not required in this case as the data is not going to S3 and there are no time or bandwidth limitations mentioned in the scenario.

References:

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

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

Save time with our AWS cheat sheets:

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

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

Question 44:

Skipped

A company has over 2000 users and is planning to migrate data into the AWS Cloud. Some of the data is user's home folders on an existing file share and the plan is to move

this data to Amazon S3. Each user will have a folder in a shared bucket under the folder structure: *bucket*/home/%username%.

What steps should a Solutions Architect take to ensure that each user can access their own home folder and no one else's? (choose 2)

- ☐ **Create a bucket policy that applies access permissions based on username**
- ☐ **Attach an S3 ACL sub-resource that grants access based on the %username% variable**
- ☐ **Create an IAM policy that applies folder-level permissions**

  (Correct)
- ☐ **Create an IAM policy that applies object-level S3 ACLs**
- ☐ **Create an IAM group and attach the IAM policy**

  (Correct)

Explanation
The AWS blog URL below explains how to construct an IAM policy for a similar scenario. Please refer to the article for detailed instructions.

CORRECT: "Create an IAM policy that applies folder-level permissions" is a correct answer.

CORRECT: "Create an IAM group and attach the IAM policy, add IAM users to the group" is also a correct answer.

INCORRECT: "Create a bucket policy that applies access permissions based on username" is incorrect. An IAM policy rather than a bucket policy should be used.

INCORRECT: "Create an IAM policy that applies object-level S3 ACLs" is incorrect as this cannot be done through an IAM policy.

INCORRECT: "Attach an S3 ACL sub-resource that grants access based on the %username% variable" is incorrect as an IAM policy should be used to control access.

References:

https://aws.amazon.com/blogs/security/writing-iam-policies-grant-access-to-user-specific-folders-in-an-amazon-s3-bucket/

Save time with our AWS cheat sheets:

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

Question 45:

Skipped

An application regularly uploads files from an Amazon EC2 instance to an Amazon S3 bucket. The files can be a couple of gigabytes in size and sometimes the uploads are slower than desired. What method can be used to increase throughput and reduce upload times?

- **Use Amazon S3 multipart upload**

  (Correct)

- **Upload the files using the S3 Copy SDK or REST API**

- **Randomize the object names when uploading**

- **Turn off versioning on the destination bucket**

Explanation

Multipart upload can be used to speed up uploads to S3. Multipart upload uploads objects in parts independently, in parallel and in any order. It is performed using the S3 Multipart upload API and is recommended for objects of 100MB or larger. It can be used for objects from 5MB up to 5TB and must be used for objects larger than 5GB.

CORRECT: "Use Amazon S3 multipart upload" is the correct answer.

INCORRECT: "Turn off versioning on the destination bucket" is incorrect. Turning off versioning will not speed up the upload.

INCORRECT: "Randomize the object names when uploading" is incorrect. Randomizing object names provides no value in this context, random prefixes are used for intensive read requests.

INCORRECT: "Upload the files using the S3 Copy SDK or REST API" is incorrect. Copy is used for copying, moving and renaming objects within S3 not for uploading to S3.

References:

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

Save time with our AWS cheat sheets:

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

Question 46:

Skipped

An Amazon ElastiCache for Redis cluster runs across multiple Availability Zones. A solutions architect is concerned about the security of sensitive data as it is replicated between nodes. How can the solutions architect protect the sensitive data?

- **Enable in-transit encryption**

  (Correct)

- **Enable at-rest encryption**

- **Set up MFA and API logging**

- **Issue a Redis AUTH command**

Explanation

Amazon ElastiCache in-transit encryption is an optional feature that allows you to increase the security of your data at its most vulnerable points—when it is in transit from one location to another. Because there is some processing needed to encrypt and decrypt the data at the endpoints, enabling in-transit encryption can have some performance impact. You should benchmark your data with and without in-transit encryption to determine the performance impact for your use cases.

ElastiCache in-transit encryption implements the following features:

- **Encrypted connections**—both the server and client connections are Secure Socket Layer (SSL) encrypted.

- **Encrypted replication—**data moving between a primary node and replica nodes is encrypted.

- **Server authentication**—clients can authenticate that they are connecting to the right server.

- **Client authentication**—using the Redis AUTH feature, the server can authenticate the clients.

CORRECT: "Enable in-transit encryption" is the correct answer.

INCORRECT: "Issue a Redis AUTH command" is incorrect. This is used when using a password to access the database.

INCORRECT: "Enable at-rest encryption" is incorrect. ElastiCache for Redis at-rest encryption is an optional feature to increase data security by encrypting on-disk data. This does not encrypt the data in-transit when it is being replicated between nodes.

INCORRECT: "Set up MFA and API logging" is incorrect. Neither multi-factor authentication or API logging is going to assist with encrypting data.

References:

https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/at-rest-encryption.html

Save time with our AWS cheat sheets:

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

Question 47:

Skipped

There has been an increase in traffic to an application that writes data to an Amazon DynamoDB database. Thousands of random tables reads occur per second and low-latency is required. What can a Solutions Architect do to improve performance for the reads without negatively impacting the rest of the application?

- **Use an Amazon Kinesis Data Stream to decouple requests**
- **Use Amazon DynamoDB Accelerator to cache the reads**

  (Correct)
- **Add an Amazon SQS queue to decouple the requests**
- **Increase the number of Amazon DynamoDB write capacity units**

Explanation
DAX is a DynamoDB-compatible caching service that enables you to benefit from fast in-memory performance for demanding applications. DAX addresses three core scenarios:

1. As an in-memory cache, DAX reduces the response times of eventually consistent read workloads by an order of magnitude from single-digit milliseconds to microseconds.

2. DAX reduces operational and application complexity by providing a managed service that is API-compatible with DynamoDB. Therefore, it requires only minimal functional changes to use with an existing application.

3. For read-heavy or bursty workloads, DAX provides increased throughput and potential operational cost savings by reducing the need to overprovision read capacity units. This is especially beneficial for applications that require repeated reads for individual keys.

DynamoDB accelerator is the best solution for caching the reads and delivering them at extremely low latency.

CORRECT: "Use Amazon DynamoDB Accelerator to cache the reads" is the correct answer.

INCORRECT: "Increase the number of Amazon DynamoDB write capacity units" is incorrect. This will not improve read performance as write capacity units affect write performance.

INCORRECT: "Add an Amazon SQS queue to decouple the requests" is incorrect. You cannot decouple a database from the frontend with a queue in order to decrease read latency.

INCORRECT: "Use an Amazon Kinesis Data Stream to decouple requests" is incorrect. You cannot increase read performance for a database by implementing a real-time streaming service.

References:

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

Save time with our AWS cheat sheets:

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

Question 48:

Skipped

A finance organization wants to deploy end of day processing applications to a fleet of Amazon EC2 instances with a focus on reducing cost. These applications are stateless and can be re-triggered in case of failure. The company needs a solution that minimizes cost and operational overhead.

What should a solutions architect do to meet these requirements?

- **Use Spot Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group.**

  (Correct)

- **Use On-Demand Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group.**

- **Use On-Demand Instances in an Amazon EC2 Auto Scaling group to run the application containers.**

- 

Use Spot Instances in an Amazon EC2 Auto Scaling group to run the application containers.

Explanation

Since by using EC2 Spot Instances, customers can access additional compute capacity between 70%-90% off On-Demand Instance pricing, we can directly eliminate two options utilizing on demand instances.

Among the two options with spot instances, since the application is stateless, the better idea is to have a containerized approach and utilize EKS to reduce operational overhead.

CORRECT: "Use Spot Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group" is the correct answer (as explained above.)

INCORRECT: "Use Spot Instances in an Amazon EC2 Auto Scaling group to run the application containers" is incorrect. As mentioned above, EKS gives you more options towards application fleet orchestration which makes it a better choice.

INCORRECT: "Use On-Demand Instances in an Amazon EC2 Auto Scaling group to run the application containers" is incorrect.

As compared to spot instances, on demand instances are costlier and for end of day processing where failures can be re-triggered and are acceptable, spot instances are a better choice.

INCORRECT: "Use On-Demand Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group" is incorrect.

As compared to spot instances, on demand instances are more expensive and for end of day processing where failures can be re-triggered and are acceptable, spot instances are a better choice.

References:

https://aws.amazon.com/blogs/compute/best-practices-for-handling-ec2-spot-instance-interruptions/

Save time with our AWS cheat sheets:

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

Question 49:

Skipped

A Solutions Architect must enable an application to download software updates from the internet. The application runs on a series of EC2 instances in an Auto Scaling group running in a private subnet. The solution must involve minimal ongoing systems management effort. How should the Solutions Architect proceed?

- **Implement a NAT gateway**

  (Correct)

- **Launch a NAT instance**

- **Attach Elastic IP addresses**

- **Create a Virtual Private Gateway**

Explanation

Both a NAT gateway or a NAT instance can be used for this use case. Both services enable internet access for instances in private subnets. However, the NAT instance runs on an EC2 instance you must launch, configure and manage and therefore involves more ongoing systems management effort.

CORRECT: "Implement a NAT gateway" is the correct answer.

INCORRECT: "Launch a NAT instance" is incorrect as this service involves more ongoing systems management effort.

INCORRECT: "Create a Virtual Private Gateway" is incorrect. A VPG is used as part of a VPN connection (AWS side of the connection). It is not used to enable internet access.

INCORRECT: "Attach Elastic IP addresses" is incorrect. You cannot use Elastic IP addresses with instances in private subnets.

References:

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

Save time with our AWS cheat sheets:

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

Question 50:

Skipped

A Solutions Architect needs a storage solution for a fleet of Linux web application servers. The solution should provide a file system interface and be able to support millions of files. Which AWS service should the Architect choose?

- **Amazon EBS**
- **Amazon EFS**

  (Correct)
- **Amazon ElastiCache**
- **Amazon S3**

Explanation

The Amazon Elastic File System (EFS) is the only storage solution in the list that provides a file system interface. It also supports millions of files as requested.

CORRECT: "Amazon EFS" is the correct answer.

INCORRECT: "Amazon ElastiCache" is incorrect. Amazon ElastiCache is an in-memory caching solution for databases.

INCORRECT: "Amazon EBS" is incorrect. Amazon EBS provides a block storage interface.

INCORRECT: "Amazon S3" is incorrect. Amazon S3 is an object storage solution and does not provide a file system interface.

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 51:

Skipped

A global financial services company is currently operating a three-tier web application to handle their main customer facing website. This application uses several Amazon EC2 instances behind an Application Load Balancer and connects directly to a DynamoDB table.

Due to recent customer complaints of slow loading times, their Solutions Architect has been asked to implement changes to solve this problem, without rearchitecting the core application components.

Which combination of actions should the solutions architect take to accomplish this? (Select TWO.)

- **Migrate the DynamoDB database to Amazon Aurora with a multi-AZ deployment model.**
- **Migrate the entire application stack to AWS Elastic Beanstalk with both web server and worker environments.**
- **Migrate the web application to be hosted on a containerized solution using AWS Fargate.**
- **Create a CloudFront distribution and place it in front of the Application Load Balancer.**

  (Correct)
- **Set up an Amazon DynamoDB Accelerator (DAX) cluster in front of the DynamoDB table.**

(Correct)

Explanation
A CloudFront distribution would cache content in one of the many global edge locations, ensuring that any customer access to the content will be accessing it at a much lower latency compared to using the Application Load Balancer on its own.

Secondly, DynamoDB has a built-in caching solution known as DynamoDB Accelerator (DAX). If your application is serving traffic from a DynamoDB database and is struggling to scale, you can use the DynamoDB cache to improve application.

CORRECT: "Create a CloudFront distribution and place it in front of the Application Load Balancer" is a correct answer (as explained above.)

CORRECT: "Set up an Amazon DynamoDB Accelerator (DAX) cluster in front of the DynamoDB table" is also a correct answer (as explained above.)

INCORRECT: "Migrate the entire application stack to AWS Elastic Beanstalk with both web server and worker environments" is incorrect.

Migrating the entire application to AWS Elastic Beanstalk would require rearchitecting and would not necessarily improve the latency of the application for end users.

INCORRECT: "Migrate the DynamoDB database to Amazon Aurora with a multi-AZ deployment model" is incorrect.

Refactoring the application to move from a No-SQL database (DynamoDB) to a SQL database (Amazon Aurora) would take a significant amount of application and code changes, due to the fundamental differences between SQL and NoSQL databases.

INCORRECT: "Migrate the web application to be hosted on a containerized solution using AWS Fargate" is incorrect.

The application does not currently use containers, and instead uses Amazon EC2 instances. Changing the application to using a containerized compute layer would also require architectural changes and would not be suitable for this use case.

References:

https://aws.amazon.com/cloudfront/

Save time with our AWS cheat sheets:

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

Question 52:

Skipped

A company runs an application using many Amazon EC2 instances for its application servers. The application using Amazon DynamoDB for its data store. The size of this table continuously grows, but the application only requires data from the most recent 30 days. The company needs a solution that minimizes cost and effort.

Which solution meets these requirements?

- **Run a monitoring application from the AWS Marketplace using an EC2 instance configured with a Golden AMI. When a new item is created in the table, configure the monitoring application to use Amazon DynamoDB Streams to store the timestamp. For items with a timestamp older than 30 days, run a script on the EC2 instance.**

- **When a new item is created in the table, Amazon DynamoDB Streams will invoke an AWS Lambda function. Set the Lambda function to delete items in the table that are older than 30 days.**

- **Add an attribute to each new item created in the table that has a value of the current timestamp plus 30 days. Configure this attribute as the TTL attribute.**

  (Correct)

- **Deploy the entire solution using an AWS CloudFormation template. Re-deploy the CloudFormation stack every 30 days, and then delete the original stack.**

Explanation

Amazon DynamoDB Time to Live (TTL) allows you to define a per-item timestamp to determine when an item is no longer needed. Shortly after the date and time of the specified timestamp, DynamoDB deletes the item from your table without consuming any write throughput. TTL is provided at no extra cost to reduce stored data volumes by retaining only the items that remain current for your workload's needs.

CORRECT: "Add an attribute to each new item created in the table that has a value of the current timestamp plus 30 days. Configure this attribute as the TTL attribute" is the correct answer (as explained above.)

INCORRECT: "Deploy the entire solution using an AWS CloudFormation template. Re-deploy the CloudFormation stack every 30 days, and then delete the original stack" is incorrect. This solution requires significant disruption and is highly inefficient.

INCORRECT: "Run a monitoring application from the AWS Marketplace using an EC2 instance configured with a Golden AMI. When a new item is created in the table, configure the monitoring application to use Amazon DynamoDB Streams to store the timestamp. For items with a timestamp older than 30 days, run a script on the EC2 instance" is incorrect as this would require more cost and operational overhead.

INCORRECT: "When a new item is created in the table, Amazon DynamoDB Streams will invoke an AWS Lambda function. Set the Lambda function to delete items in the table that are older than 30 days" is incorrect. Whilst this is possible, it provides this entails higher operational overhead and cost.

References:

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

Save time with our AWS cheat sheets:

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

Question 53:

Skipped

A financial services company is currently using 500 Amazon EC2 instances to run batch-processing workloads to analyze financial information on a periodic basis. The organization needs to install a third-party tool on all these instances as quickly and as efficiently as possible and will have to carry out similar tasks on an ongoing basis going forward. The solution also needs to scale for the addition of future EC2 instances.

What should a solutions architect do to meet these requirements in the easiest way possible?

- **Use AWS Systems Manager Patch Manager to install the tool on all the EC2 instances within a single patch.**
- **Create an AWS Lambda Function which will make configuration changes to all the EC2 instances. Validate the tool has been installed using another Lambda function.**

- **Use AWS Systems Manager Maintenance Windows to install the tool on all the EC2 instances within a set period of time.**

- **Use AWS Systems Manager Run Command to run a custom command that installs the tool on all the EC2 instances.**

  (Correct)

Explanation
AWS Systems Manager Run command is designed to run commands across a large group of instances without having to SSH into all your instances and run the same command multiple times. You can easily run the same command to all the managed nodes as part of the workload, without having to maintain access keys or individual access for each instance.

CORRECT: "Use AWS Systems Manager Run Command to run a custom command that installs the tool on all the EC2 instances" is the correct answer (as explained above.)

INCORRECT: "Create an AWS Lambda Function which will make configuration changes to all of the EC2 instances. Validate the tool has been installed using another Lambda function" is incorrect. Whilst this may be possible, the code that would be required to create and test this solution would be difficult to design and would not scale effectively as AWS Systems Manager Run Command.

INCORRECT: "Use AWS Systems Manager Patch Manager to install the tool on all of the EC2 instances within a single patch" is incorrect. AWS Systems Manager Patch Manager is designed to apply patches to EC2 instances and is not designed to run commands across a large group of instances.

INCORRECT: "Use AWS Systems Manager Maintenance Windows to install the tool on all of the EC2 instances within a set period of time" is incorrect. AWS Systems Manager Maintenance Windows is designed to select a defined window of time in which you EC2 instances will be patched and is not capable of running commands across multiple instances.

References:

https://docs.aws.amazon.com/systems-manager/latest/userguide/execute-remote-commands.html

Save time with our AWS cheat sheets:

https://digitalcloud.training/aws-systems-manager/

Question 54:

Skipped

A retail organization is building an ecommerce application on AWS. The application sends information about new orders to a REST API hosted on Amazon API Gateway to process. The company needs the orders to be processed in the order that they are received.

Which solution will meet these requirements?

- **When an order is received, use an API Gateway integration to send a message to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. For processing, configure the SQS FIFO queue to invoke an AWS Lambda function.**

  (Correct)

- **When an order is received, use an API Gateway integration to send a message to an Amazon Simple Queue Service (Amazon SQS) standard queue. For processing, configure the SQS standard queue to invoke an AWS Lambda function.**

- **Integrate the Amazon Simple Notification Service (Amazon SNS) with API Gateway. The Amazon SNS topic will send a message to AWS Lambda where the message will be processed.**

- **While the application processes an order, API Gateway authorizers will block any requests.**

Explanation

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. Based on the application requirements of having the orders to be processed in the order that they are received, you could use a FIFO queue, which offers high throughput, exactly-once-processing, and first-in-first-out-delivery.

CORRECT: "When an order is received, use an API Gateway integration to send a message to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. For

processing, configure the SQS FIFO queue to invoke an AWS Lambda function" is the correct answer (as explained above.)

INCORRECT: "Integrate the Amazon Simple Notification Service (Amazon SNS) with API Gateway. The Amazon SNS topic will send a message to AWS Lambda where the message will be processed. " is incorrect. Amazon SNS is not suitable for this application as Amazon SNS is a one-to-many messaging service designed to deliver messages to subscribers using SMS, Emails etc.

INCORRECT: "While the application processes an order, API Gateway authorizers will block any requests" is incorrect. A Lambda authorizer (formerly known as a custom authorizer) is an API Gateway feature that uses a Lambda function to control access to your API, which does not change how the traffic is delivered in which order.

INCORRECT: "When an order is received, use an API Gateway integration to send a message to an Amazon Simple Queue Service (Amazon SQS) standard queue. For processing, configure the SQS standard queue to invoke an AWS Lambda function" is incorrect as an SQS standard queue offers best-effort-ordering, which is not suitable for this use case.

References:

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

Save time with our AWS cheat sheets:

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

Question 55:

Skipped

A media company has grown significantly in the past few months and the management team are concerned about compliance, governance, auditing, and security. The management team requires that configuration changes are tracked a history of API calls is recorded.

What should a solutions architect do to meet these requirements?

- **Use AWS CloudTrail to track configuration changes and Amazon CloudWatch to record API calls.**

Use AWS Config to track configuration changes and AWS CloudTrail to record API calls.

(Correct)

- **Use AWS Config to track configuration changes and Amazon CloudWatch to record API calls.**

- **Use AWS CloudTrail to track configuration changes and AWS Config to record API calls.**

Explanation
As per definition of AWS CloudTrail and AWS Config:

CloudTrail is a web service that records AWS API calls for your AWS account and delivers log files to an Amazon S3 bucket. The recorded information includes the identity of the user, the start time of the AWS API call, the source IP address, the request parameters, and the response elements returned by the service.

AWS Config tracks changes in the configuration of your AWS resources, and it regularly sends updated configuration details to an Amazon S3 bucket that you specify. For each resource type that AWS Config records, it sends a configuration history file every six hours.

CORRECT: "Use AWS Config to track configuration changes and AWS CloudTrail to record API calls" is the correct answer (as explained above.)

INCORRECT: "Use AWS CloudTrail to track configuration changes and AWS Config to record API calls " is incorrect.

This option is the reverse of what's needed, AWS config, as the name suggests, is used to track the configuration changes in AWS accounts.

INCORRECT: "Use AWS Config to track configuration changes and Amazon CloudWatch to record API calls" is incorrect. CloudWatch is used for performance monitoring, not tracking API calls.

INCORRECT: "Use AWS CloudTrail to track configuration changes and Amazon CloudWatch to record API calls" is incorrect. CloudTrail is not the right service for tracking configuration changes hence this option is incorrect.

References:

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

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/TrackingChanges.html

Save time with our AWS cheat sheets:

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

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

Question 56:

Skipped

A company observed an increase in Amazon EC2 costs in its most recent bill. The billing team noticed unwanted vertical scaling of instance types for a couple of EC2 instances. A solutions architect needs to create a graph comparing the last 2 months of EC2 costs and perform an in-depth analysis to identify the root cause of the vertical scaling.

How should the solutions architect generate the information with the LEAST operational overhead?

- **Use Cost Explorer's granular filtering feature to perform an in-depth analysis of EC2 costs based on instance types.**

  (Correct)

- **Use AWS Budgets to create a budget report and compare EC2 costs based on instance types.**

- **Use graphs from the AWS Billing and Cost Management dashboard to compare EC2 costs based on instance types for the last 2 months.**

- **Use AWS Cost and Usage Reports to create a report and send it to an Amazon S3 bucket. Use Amazon QuickSight with Amazon S3 as a source to generate an interactive graph based on instance types.**

Explanation

AWS Cost Explorer would be the easiest way to graph this data. Cost Explorer can be accessed easily and has features for filtering billing data and graphing across relevant time periods.

	Billing dashboard/bills	AWS Cost Explorer	Cost and Usage Report
Data field	• AWS account ID • Service (EC2) • Usage Type (BoxUsage:t3:large) • Operation (Runinstance) • Item Description (OS & Pricing) • Usage Quantity • Cost	All fields from Bills File + • User Defined Tags • API Operation • Region A/Z • Platform (OS) • Purchase Option • Tenancy	All fields from Bills File + • Resource-id
Period	• Monthly	• Monthly (Last 12 M) • Daily	• Hourly • Daily
Output	• PDF and CSV	• Billing Dashbord UI • CSV • Cost Explorer API	• S3
Use for	• Simple monthly reports	• Daily/weekly cost tracking • Leverage Cost Awareness • Trend and Budget analysis	• Hourly/Daily reporting

CORRECT: "Use Cost Explorer's granular filtering feature to perform an in-depth analysis of EC2 costs based on instance types" is the correct answer (as explained above.)

INCORRECT: "Use AWS Budgets to create a budget report and compare EC2 costs based on instance types" is incorrect.

AWS Budgets lets you set custom cost and usage budgets that alert you when your budget thresholds are exceeded (or forecasted to be exceeded).

INCORRECT: "Use graphs from the AWS Billing and Cost Management dashboard to compare EC2 costs based on instance types for the last 2 months" is incorrect.

The granularity required is not available in the billing and cost management dashboard unless using the cost and usage report.

INCORRECT: "Use AWS Cost and Usage Reports to create a report and send it to an Amazon S3 bucket. Use Amazon QuickSight with Amazon S3 as a source to generate an interactive graph based on instance types" is incorrect. This could provide the required graphs, but it involves much more operational overhead.

References:

https://aws.amazon.com/aws-cost-management/aws-cost-explorer/

Save time with our AWS cheat sheets:

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

Question 57:

Skipped

A company has an eCommerce application that runs from multiple AWS Regions. Each region has a separate database running on Amazon EC2 instances. The company plans to consolidate the data to a columnar database and run analytics queries. Which approach should the company take?

- **Create an AWS Lambda function that copies the data onto Amazon S3. Use Amazon S3 Select to query the data**
- **Run an AWS Batch job to copy and process the data into a columnar Amazon RDS database. Use Amazon Athena to analyze the data**
- **Use the COPY command to load data into an Amazon RedShift data warehouse and run the analytics queries there**

  (Correct)
- **Launch Amazon Kinesis Data Streams producers to load data into a Kinesis Data stream. Use Kinesis Data Analytics to analyze the data**

Explanation

Amazon Redshift is an enterprise-level, petabyte scale, fully managed data warehousing service. It uses columnar storage to improve the performance of complex queries.

You can use the COPY command to load data in parallel from one or more remote hosts, such Amazon EC2 instances or other computers. COPY connects to the remote hosts using SSH and executes commands on the remote hosts to generate text output.

CORRECT: "Use the COPY command to load data into an Amazon RedShift data warehouse and run the analytics queries there" is the correct answer.

INCORRECT: "Run an AWS Batch job to copy and process the data into a columnar Amazon RDS database. Use Amazon Athena to analyze the data" is incorrect. AWS Batch is used for running batch computing jobs across a fleet of EC2 instances. You

cannot create a “columnar Amazon RDS database” as RDS is optimized for transactional workloads. Athena is used to analyze data on S3.

INCORRECT: "Launch Amazon Kinesis Data Streams producers to load data into a Kinesis Data stream. Use Kinesis Data Analytics to analyze the data" is incorrect. Kinesis is a real-time streaming data service. It is not a columnar database so is unsuitable for this use case.

INCORRECT: "Create an AWS Lambda function that copies the data onto Amazon S3. Use Amazon S3 Select to query the data" is incorrect. S3 is not a columnar database and S3 select does not run analytics queries, it simply selects data from an object to retrieve.

References:

https://docs.aws.amazon.com/redshift/latest/dg/loading-data-from-remote-hosts.html

Save time with our AWS cheat sheets:

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

Question 58:

Skipped

A customer runs an application on-premise that stores large media files. The data is mounted to different servers using either the SMB or NFS protocols. The customer is having issues with scaling the storage infrastructure on-premise and is looking for a way to offload the data set into the cloud whilst retaining a local cache for frequently accessed content.

Which of the following is the best solution?

- **Use the AWS Storage Gateway File Gateway**

  (Correct)

- **Establish a VPN and use the Elastic File System (EFS)**

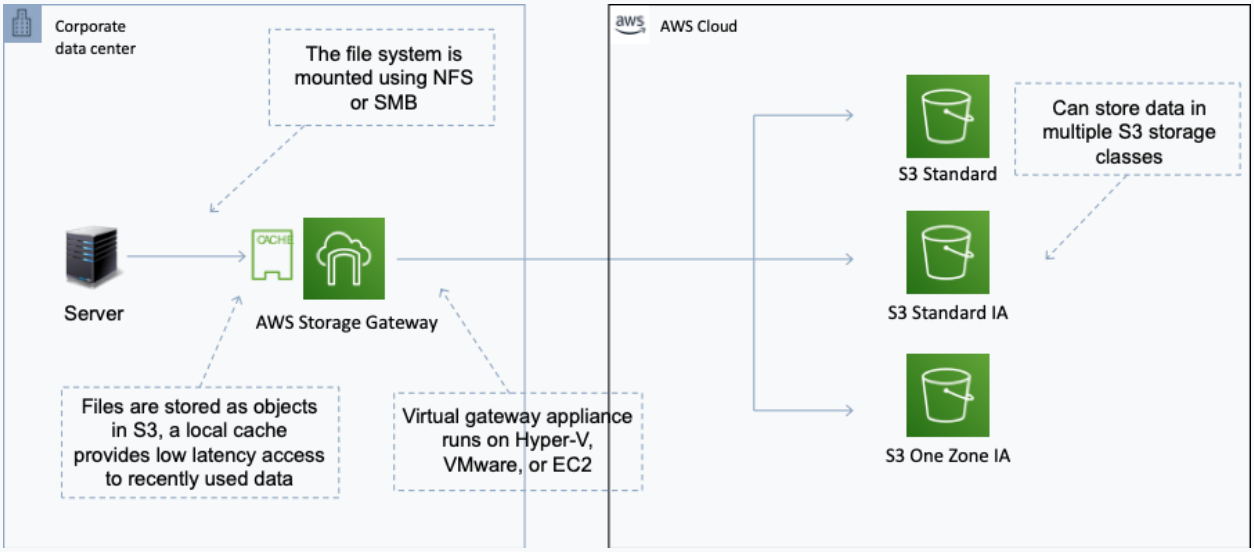
- **Use the AWS Storage Gateway Volume Gateway in cached volume mode**

-

Create a script that migrates infrequently used data to S3 using multi-part upload

Explanation

File gateway provides a virtual on-premises file server, which enables you to store and retrieve files as objects in Amazon S3. It can be used for on-premises applications, and for Amazon EC2-resident applications that need file storage in S3 for object based workloads. Used for flat files only, stored directly on S3. File gateway offers SMB or NFS-based access to data in Amazon S3 with local caching.



CORRECT: "Use the AWS Storage Gateway File Gateway" is the correct answer.

INCORRECT: "Use the AWS Storage Gateway Volume Gateway in cached volume mode" is incorrect. The AWS Storage Gateway Volume Gateway in cached volume mode is a block-based (not file-based) solution so you cannot mount the storage with the SMB or NFS protocols With Cached Volume mode – the entire dataset is stored on S3 and a cache of the most frequently accessed data is cached on-site.

INCORRECT: "Create a script that migrates infrequently used data to S3 using multi-part upload" is incorrect. Creating a script the migrates infrequently used data to S3 is possible but that data would then not be indexed on the primary filesystem so you wouldn't have a method of retrieving it without developing some code to pull it back from S3. This is not the best solution.

INCORRECT: "Establish a VPN and use the Elastic File System (EFS)" is incorrect. You could mount EFS over a VPN but it would not provide you a local cache of the data.

References:

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

Save time with our AWS cheat sheets:

https://digitalcloud.training/aws-storage-gateway/

Question 59:

Skipped

A company has several AWS accounts each with multiple Amazon VPCs. The company must establish routing between all private subnets. The architecture should be simple and allow transitive routing to occur.

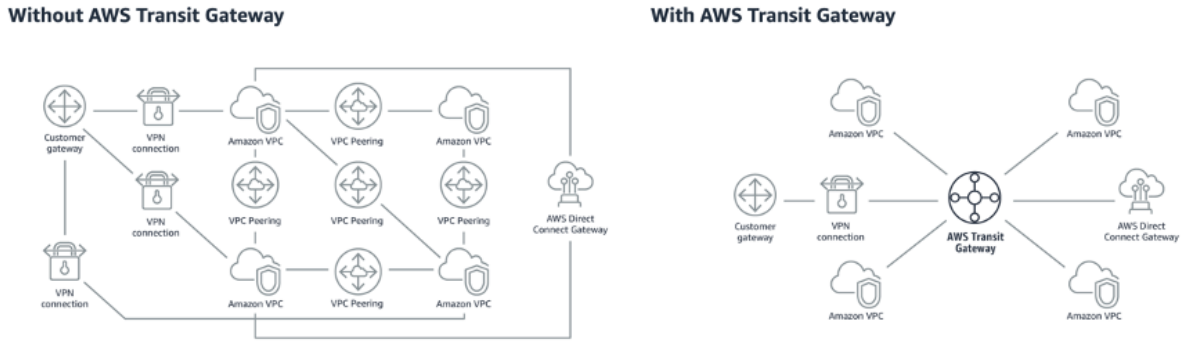
How should the network connectivity be configured?

- **Create a transitive VPC peering connection between each Amazon VPC and configure route tables**
- **Create a hub-and-spoke topology with AWS App Mesh and use AWS Resource Access Manager to share route tables**
- **Create an AWS Managed VPN between each Amazon VPC and configure route tables**
- **Create an AWS Transit Gateway and share it with each account using AWS Resource Access Manager**

  (Correct)

Explanation

You can build a hub-and-spoke topology with AWS Transit Gateway that supports transitive routing. This simplifies the network topology and adds additional features over VPC peering. AWS Resource Access Manager can be used to share the connection with the other AWS accounts.



CORRECT: "Create an AWS Transit Gateway and share it with each account using AWS Resource Access Manager" is the correct answer.

INCORRECT: "Create a transitive VPC peering connection between each Amazon VPC and configure route tables" is incorrect. You cannot create transitive connections with VPC peering.

INCORRECT: "Create an AWS Managed VPN between each Amazon VPC and configure route tables" is incorrect. This is a much more complex solution compared to AWS Transit Gateway so is not the best option.

INCORRECT: "Create a hub-and-spoke topology with AWS App Mesh and use AWS Resource Access Manager to share route tables" is incorrect. AWS App Mesh is used for application-level networking for microservices applications.

References:

https://aws.amazon.com/blogs/aws/new-use-an-aws-transit-gateway-to-simplify-your-network-architecture/

Save time with our AWS cheat sheets:

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

Question 60:

Skipped

A large manufacturing company is migrating many of its on-premises applications to AWS. The applications are staged in many different AWS accounts under a payer account, using AWS Organizations. The company's security team needs to enable a single sign-on (SSO) solution across all the company's accounts, and this must be integrated with the company's existing Active Directory setup.

Which solution will meet these requirements?

- **Deploy an identity provider (IDP) on-premises. Enable AWS IAM Identity Center (successor to AWS SSO) from the AWS Identity Center console.**

- **Enable AWS IAM Identity Center (successor to AWS SSO). Create a one-way domain trust to connect the company's self-managed Microsoft Active Directory by using AWS Directory Service for Microsoft Active Directory.**

- **Enable AWS IAM Identity Center (successor to AWS SSO). Create a two-way forest trust to connect the company's self-managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory.**

  (Correct)

- **Use AWS Directory Service. Create a two-way trust relationship with the company's self-managed Microsoft Active Directory.**

Explanation

AWS IAM Identity Center (successor to AWS Single Sign-On) requires a two-way trust so that it has permissions to read user and group information from your domain to synchronize user and group metadata. IAM Identity Center uses this metadata when assigning access to permission sets or applications.

User and group metadata is also used by applications for collaboration, like when you share a dashboard with another user or group. The trust from AWS Directory Service for Microsoft Active Directory to your domain permits IAM Identity Center to trust your domain for authentication. The trust in the opposite direction grants AWS permissions to read user and group metadata.

CORRECT: "Enable AWS IAM Identity Center (successor to AWS SSO). Create a two-way forest trust to connect the company's self-managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory" is the correct answer (as explained above.)

INCORRECT: "Enable AWS IAM Identity Center (successor to AWS SSO). Create a one-way domain trust to connect the company's self-managed Microsoft Active Directory by using AWS Directory Service for Microsoft Active Directory" is incorrect. A two-way trust is required by IAM Identity Center.

INCORRECT: "Use AWS Directory Service. Create a two-way trust relationship with the company's self-managed Microsoft Active Directory" is incorrect. This solution does not enable SSO across the accounts as it does not involve IAM Identity Center.

INCORRECT: "Deploy an identity provider (IdP) on premises. Enable AWS IAM Identity Center (successor to AWS SSO) from the AWS Identity Center console" is incorrect. The IdP is already deployed as the company has Microsoft AD. This does not provide a solution for integrating and enabling SSO.

References:

https://docs.aws.amazon.com/singlesignon/latest/userguide/connectonpremad.html

Save time with our AWS cheat sheets:

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

Question 61:

Skipped

A company stores its application logs in an Amazon CloudWatch Logs log group. A new policy requires the company to store all application logs in Amazon OpenSearch Service (Amazon Elasticsearch Service) in near-real time.

Which solution will meet this requirement with the LEAST operational overhead?

- **Configure a CloudWatch Logs subscription to stream the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).**

  (Correct)

- **Create an AWS Lambda function. Use the log group to invoke the function to write the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).**

- **Install and configure Amazon Kinesis Agent on each application server to deliver the logs to Amazon Kinesis Data Streams. Configure Kinesis Data Streams to deliver the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).**

-

Create an Amazon Kinesis Data Firehose delivery stream. Configure the log group as the delivery stream's source. Configure Amazon OpenSearch Service (Amazon Elasticsearch Service) as the delivery stream's destination.

Explanation

You can configure a CloudWatch Logs log group to stream data it receives to your Amazon OpenSearch Service cluster in near real-time through a CloudWatch Logs subscription. This is the solution that requires the least operational overhead. Subscription filters can also be created for Kinesis, Kinesis Data Firehose, and AWS Lambda.

CORRECT: " Configure a CloudWatch Logs subscription to stream the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service) " is the correct answer (as explained above.)

INCORRECT: "Create an Amazon Kinesis Data Firehose delivery stream. Configure the log group as the delivery stream's source. Configure Amazon OpenSearch Service (Amazon Elasticsearch Service) as the delivery stream's destination" is incorrect.

This is a possible solution but requires more operational overhead as it includes an additional service which must also be configured and managed.

INCORRECT: "Create an AWS Lambda function. Use the log group to invoke the function to write the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service)" is incorrect. This would require more operational overhead as you must write and manage the code for the function yourself.

INCORRECT: "Install and configure Amazon Kinesis Agent on each application server to deliver the logs to Amazon Kinesis Data Streams. Configure Kinesis Data Streams to deliver the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service)" is incorrect. Since the requirement is to dump the logs into OpenSearch and no further computation is needed, Firehose is a better candidate here.

References:

https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_OpenSearch_Stream.html

Save time with our AWS cheat sheets:

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

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

Question 62:

Skipped

A media company is designing a disaster recovery (DR) solution for a business-critical application. The recovery time objective (RTO) should be 4 hours or less. The application is running on Amazon EC2 instances using the fewest possible AWS resources during normal operations.

Which of the following is recommended to implement the DR solution across regions cost-effectively?

- **Create Amazon Machine Images (AMIs) to back up the EC2 instances. Copy the AMIs to a secondary AWS Region. Automate infrastructure deployment in the secondary Region by using AWS CloudFormation.**

  (Correct)

- **Create Amazon Machine Images (AMI) to back up the EC2 instances. Copy the AMIs to a secondary AWS Region. Automate infrastructure deployment in the secondary Region by using AWS Lambda and custom scripts.**

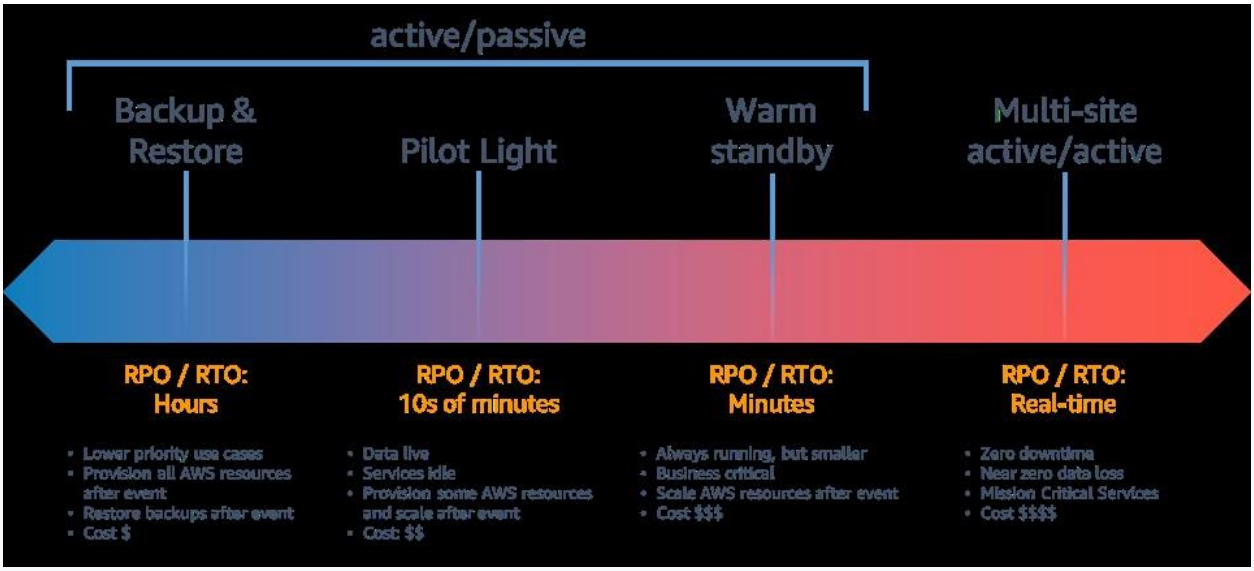
- **Launch EC2 instances in a secondary Availability Zone. Keep the EC2 instances in the secondary Availability Zone active at all times.**

- **Launch EC2 instances in a secondary AWS Region. Keep the EC2 instances in the secondary Region active at all times.**

Explanation

When you have a few hours to achieve disaster recovery, copying AMI's across regions is an achievable solution. AWS CloudFormation can then be us

ed to quickly spin up the instances in the second region when a disaster recovery event occurs. This is the most cost-effective option as only the active site has running instances.



CORRECT: "Create Amazon Machine Images (AMIs) to back up the EC2 instances. Copy the AMIs to a secondary AWS Region. Automate infrastructure deployment in the secondary Region by using AWS CloudFormation" is the correct answer (as explained above.)

INCORRECT: "Create Amazon Machine Images (AMI) to back up the EC2 instances. Copy the AMIs to a secondary AWS Region. Automate infrastructure deployment in the secondary Region by using AWS Lambda and custom scripts" is incorrect.

AWS CloudFormation is more suited to deploying infrastructure than using Lambda with custom scripts.

INCORRECT: "Launch EC2 instances in a secondary AWS Region. Keep the EC2 instances in the secondary Region active at all times" is incorrect.

This approach can work but this is not a cost-effective choice.

INCORRECT: "Launch EC2 instances in a secondary Availability Zone. Always keep the EC2 instances in the secondary Availability Zone active" is incorrect. As with the previous answer, this is not cost-effective.

References:

https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-i-strategies-for-recovery-in-the-cloud/

https://aws.amazon.com/blogs/architecture/creating-a-multi-region-application-with-aws-services-part-1-compute-and-security/

Save time with our AWS cheat sheets:

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

Question 63:

Skipped

Encrypted Amazon Elastic Block Store (EBS) volumes are attached to some Amazon EC2 instances. Which statements are correct about using encryption with Amazon EBS volumes? (choose 2)

- **You cannot mix encrypted with unencrypted volumes on an instance**
- **Data is only encrypted at rest**
- **Encryption is supported on all Amazon EBS volume types**

  (Correct)
- **Volumes created from encrypted snapshots are unencrypted**
- **Data in transit between an instance and an encrypted volume is also encrypted**

  (Correct)

Explanation

Some facts about Amazon EBS encrypted volumes and snapshots:

- All **EBS** types support encryption and all instance **families** now support encryption.

- Not all **instance** types support encryption.

- Data in transit between an instance and an encrypted volume is also encrypted (data is encrypted in trans.

- You can have encrypted an unencrypted EBS volumes attached to an instance at the same time.

- Snapshots of encrypted volumes are encrypted automatically.

- EBS volumes restored from encrypted snapshots are encrypted automatically.

- EBS volumes created from encrypted snapshots are also encrypted.

CORRECT: "Encryption is supported on all Amazon EBS volume types" is a correct answer.

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

INCORRECT: "Data is only encrypted at rest" is incorrect. Please refer to the facts above.

INCORRECT: "Volumes created from encrypted snapshots are unencrypted" is incorrect. Please refer to the facts above.

INCORRECT: "You cannot mix encrypted with unencrypted volumes on an instance" is incorrect. Please refer to the facts above.

References:

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

Save time with our AWS cheat sheets:

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

Question 64:

Skipped

An e-commerce company wants to ensure all its resources used to host its various Web Applications are tagged using the appropriate application name to allow the company to easily differentiate and group resources. The company wants to minimize effort involved and automate this task.

What should a solutions architect do to accomplish this with the LEAST operational overhead?

- **Use Cost Explorer to display any application components that are not properly tagged. Tag those resources using a Python Script.**

Configure AWS CloudTrail to send events to an Amazon CloudWatch Logs log group. Use insights queries to detect API events that do not include TagResources actions.

- 

Write API calls to check all resources for proper tag allocation. Schedule an AWS Lambda function through Amazon CloudWatch to periodically run the code.

- 

Use AWS Config to detect resources that are not properly tagged. Create a Systems Manager automation document for remediation.

(Correct)

Explanation
AWS Config enables AWS resource inventory and change management as well as Config Rules to confirm that resources are configured in compliance with policies that you define. This is the easiest way to automate the detection of non-compliant resources.

You can create custom Systems Manager automation documents to remediate the missing tags. The documents can be configured for automatic remediation in AWS Config.

CORRECT: "Use AWS Config to detect resources that are not properly tagged. Create a Systems Manager automation document for remediation" is the correct answer (as explained above.)

INCORRECT: "Use Cost Explorer to display any application components that are not properly tagged. Tag those resources using a Python Script" is incorrect. Cost Explorer is not designed for configuration compliance and would not provide the required information.

INCORRECT: "Configure AWS CloudTrail to send events to an Amazon CloudWatch Logs log group. Use insights queries to detect API events that do not include TagResources actions" is incorrect. This is an unworkable and highly inefficient attempt at configuration compliance. Much better to use AWS Config which is designed for this purpose.

INCORRECT: "Write API calls to check all resources for proper tag allocation. Schedule an AWS Lambda function through Amazon CloudWatch to periodically run the code" is incorrect as this would contain a significant amount of operational overhead.

References:

https://aws.amazon.com/config/

Save time with our AWS cheat sheets:

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

Question 65:

Skipped

A financial services company has a large, multi-Region footprint on AWS. A recent security audit highlighted some issues that must be addressed. The company must track all configuration changes affecting AWS resources and have detailed records of who has accessed the AWS environment. The data should include information such as which user has logged in and which API calls they made

What actions should a Solutions Architect take to meet these requirements?

- **Use AWS Config to track configuration changes and AWS CloudTrail to record API calls and track access patterns in the AWS Cloud.**

  (Correct)

- **Use Amazon Macie to track configuration changes and Amazon CloudTrail to record API calls and track access patterns in the AWS Cloud.**

- **Use AWS Config to track configuration changes and Amazon EventBridge to record API calls and track access patterns in the AWS Cloud.**

- **Use Amazon CloudWatch to track configuration changes and AWS Config to record API calls and track access patterns in the AWS Cloud.**

Explanation

AWS Config is a service used to track and remediation any unauthorized configuration changes made with your AWS Account. AWS Config could be used in this example with AWS AWS CloudTrail which keeps detailed logs of all API calls made within the account such as who logged in, which AWS Identity and Access Management (IAM) role is being used and also how they interact with the AWS Cloud.

CORRECT: "Use AWS Config to track configuration changes and AWS CloudTrail to record API calls and track access patterns in the AWS Cloud" is the correct answer (as explained above.)

INCORRECT: "Use Amazon CloudWatch to track configuration changes and AWS Config to record API calls and track access patterns in the AWS Cloud" is incorrect. Amazon CloudWatch does not make track configuration changes, it tracks performance metrics and AWS Config does not track API calls, it tracks configuration changes.

INCORRECT: "Use AWS Config to track configuration changes and Amazon EventBridge to record API calls and track access patterns in the AWS Cloud" is incorrect. Although AWS Config would work in this scenario, *Amazon EventBridge* is a serverless event bus used to build event-driven- architectures so it cannot be used for tracking API calls.

INCORRECT: "Use Amazon Macie to track configuration changes and Amazon CloudTrail to record API calls and track access patterns in the AWS Cloud" is incorrect. Amazon Macie is used with Amazon S3 to detect sensitive PII data, which has nothing to do with tracking configuration changes.

References:

https://aws.amazon.com/config

Save time with our AWS cheat sheets:

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