Question 1Skipped

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 ElastiCache Redis

Amazon RDS MySQL

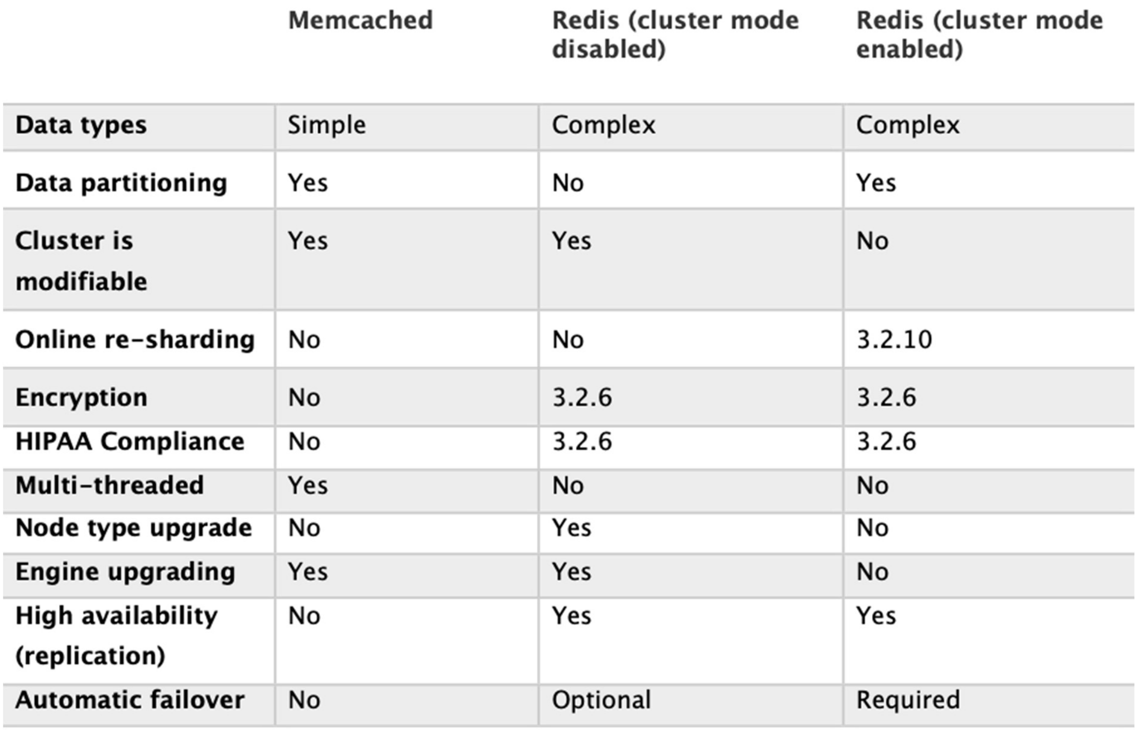
Amazon DynamoDB DAX

Correct answer

Amazon ElastiCache Memcached

Overall 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/

Domain

AWS Database

Question 2Skipped

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?

Correct answer

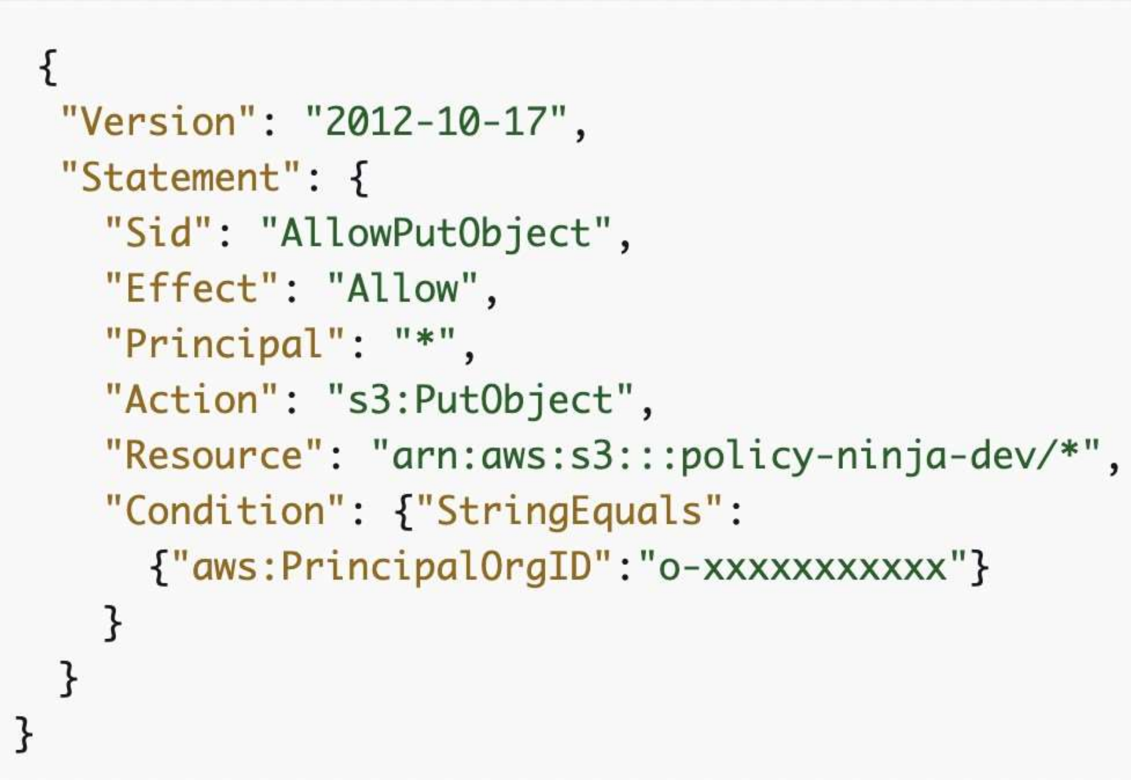
Add the aws:PrincipalOrgID global condition key with a reference to the organization ID to the S3 bucket policy.

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.

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

Overall 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-xxxxxxxxxxx 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/

Domain

AWS Management & Governance

Question 3Skipped

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)

Correct answer

Migrate the data to Amazon FSx for Windows File Server using AWS DataSync

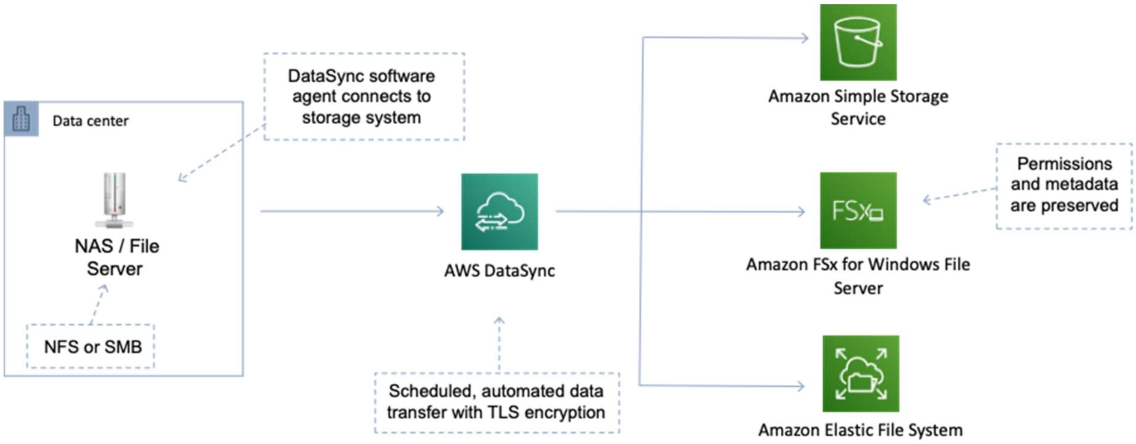
Migrate the data to Amazon FSx for Lustre using AWS DataSync

Migrate the data to Amazon S3 using and AWS Snowball Edge device

Overall 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.


Data center
NAS / File Server
NFS or SMB
DataSync software agent connects to storage system
AWS DataSync
Scheduled, automated data transfer with TLS encryption
Amazon Simple Storage Service
Amazon FSx for Windows File Server
Permissions and metadata are preserved
Amazon Elastic File System

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/

Domain

AWS Storage

Question 4Skipped

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 EC2 Auto Scaling group to run the application containers.

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.

Correct answer

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

Overall 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/

Domain

AWS Compute

Question 5Skipped

An international logistics company has web applications running on AWS in the us-west-2 Region and database servers in the eu-central-1 Region. The applications running in a VPC in us-west-2 need to communicate securely with the databases running in a VPC in eu-central-1.

Which network design will meet these requirements?

Create a VPC peering connection between the us-west-2 VPC and the eu-central-1 VPC. Add the appropriate routes to the subnet route tables. Create an inbound rule in the us-west-2 application security group that allows traffic from the eu-central-1 database server IP addresses.

Establish a transit gateway with a peering attachment between the us-west-2 VPC and the eu-central-1 VPC. After the transit gateways are properly peered and routing is configured, create an inbound rule in the eu-central-1 database security group that references the security group ID of the application servers in us-west-2.

Establish a VPC peering connection between the us-west-2 VPC and the eu-central-1 VPC. Modify the subnet route tables accordingly. Create an inbound rule in the eu-central-1 database security group that references the security group ID of the application servers in us-west-2.

Correct answer

Configure a VPC peering connection between the us-west-2 VPC and the eu-central-1 VPC. Update the subnet route tables accordingly. Create an inbound rule in the eu-central-1 database security group that allows traffic from the us-west-2 application server IP addresses.

Overall explanation

The correct solution establishes a VPC peering connection between the two regions, and it properly sets up the inbound rule in the eu-central-1 database security group to allow traffic from the us-west-2 application server IP addresses, which is the correct way to configure this as security groups can't be referenced across regions.

CORRECT: "Configure a VPC peering connection between the us-west-2 VPC and the eu-central-1 VPC. Update the subnet route tables accordingly. Create an inbound rule in the eu-central-1 database security group that allows traffic from the us-west-2 application server IP addresses" is the correct answer (as explained above.)

INCORRECT: "Establish a VPC peering connection between the us-west-2 VPC and the eu-central-1 VPC. Modify the subnet route tables accordingly. Create an inbound rule in the eu-central-1 database security group that references the security group ID of the application servers in us-west-2" is incorrect.

You cannot reference a security group from another region. Security groups are region-specific and can only be referenced within the same region.

INCORRECT: "Create a VPC peering connection between the us-west-2 VPC and the eu-central-1 VPC. Add the appropriate routes to the subnet route tables. Create an inbound rule in the us-west-2 application security group that allows traffic from the eu-central-1 database server IP addresses" is incorrect.

In this scenario, we want to allow traffic from the application servers in us-west-2 to the database servers in eu-central-1. The inbound rule should be configured in the eu-central-1 database security group to allow this traffic.

INCORRECT: "Establish a transit gateway with a peering attachment between the us-west-2 VPC and the eu-central-1 VPC. After the transit gateways are properly peered and routing is configured, create an inbound rule in the eu-central-1 database security group that references the security group ID of the application servers in us-west-2" is incorrect.

You cannot reference a security group from another region. Security groups are region-specific and can only be referenced within the same region.

References:

https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-security-groups.html

Save time with our AWS cheat sheets:

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

Domain

AWS Networking & Content Delivery

Question 6Skipped

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 an AWS Managed VPN between each Amazon VPC and configure route tables

Correct answer

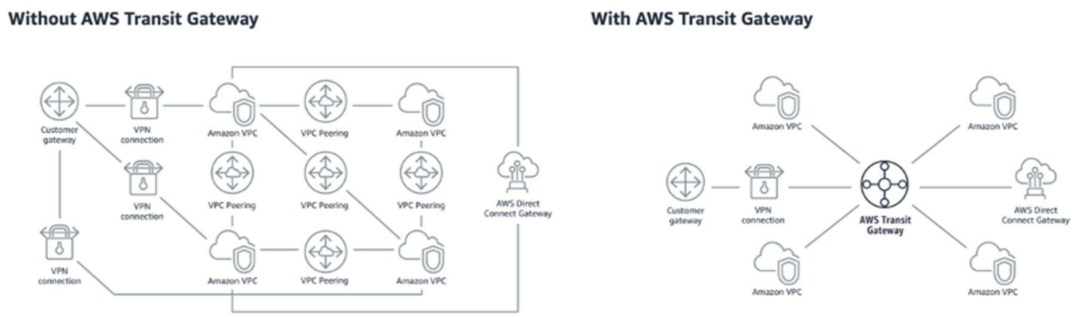
Create an AWS Transit Gateway and share it with each account using AWS Resource Access Manager

Create a hub-and-spoke topology with AWS App Mesh and use AWS Resource Access Manager to share route tables

Create a transitive VPC peering connection between each Amazon VPC and configure route tables

Overall 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/

Domain

AWS Networking & Content Delivery

Question 7Skipped

A global logistics company collects shipment tracking information, which updates every few seconds. The company wishes to perform real-time analysis on these data updates to monitor shipment progress and predict delays, after which they want the data to be ingested into their Amazon S3-based data lake. Which solution will fulfill these requirements with the MOST operational efficiency?

Use Amazon SQS for data ingestion and Amazon EMR for real-time analysis.

Use Amazon Kinesis Data Streams for data ingestion and AWS Lambda for real-time data analysis.

Use AWS Direct Connect for data ingestion and Amazon Athena for real-time analysis.

Correct answer

Use Amazon Kinesis Data Firehose for data ingestion and Amazon Kinesis Data Analytics for real-time analysis.

Overall explanation

Amazon Kinesis Data Firehose is ideal for ingesting high-velocity data into AWS, like the shipment tracking data in this scenario. It can capture, transform, and load streaming data into data lakes on S3. Kinesis Data Analytics can then analyze this data in real-time, making this the most operationally efficient solution.

CORRECT: "Use Amazon Kinesis Data Firehose for data ingestion and Amazon Kinesis Data Analytics for real-time analysis" is the correct answer (as explained above.)

INCORRECT: "Use Amazon Kinesis Data Streams for data ingestion and AWS Lambda for real-time data analysis" is incorrect.

Kinesis Data Streams can handle real-time data ingestion and Lambda can perform real-time processing, but this approach requires managing the stream consumers (like AWS Lambda) and ensuring they are scaled properly. This may not be the most operationally efficient solution.

INCORRECT: "Use AWS Direct Connect for data ingestion and Amazon Athena for real-time analysis" is incorrect.

AWS Direct Connect is a networking service primarily for establishing dedicated network connections from on-premises to AWS, not typically used for high-velocity data ingestion. Amazon Athena is more suitable for ad-hoc querying on S3 data, not real-time analysis.

INCORRECT: "Use Amazon SQS for data ingestion and Amazon EMR for real-time analysis" is incorrect.

Amazon SQS is capable of handling high-throughput workloads, but it's more suited to decoupling and scaling microservices, distributed systems, and serverless applications. Amazon EMR is a managed cluster platform that simplifies running big data frameworks, but it is not suitable for real-time data analysis.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Analytics

Question 8Skipped

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 web application to be hosted on a containerized solution using AWS Fargate.

Migrate the entire application stack to AWS Elastic Beanstalk with both web server and worker environments.

Correct selection

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

Correct selection

Create a CloudFront distribution and place it in front of the Application Load Balancer.

Migrate the DynamoDB database to Amazon Aurora with a multi-AZ deployment model.

Overall 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/

Domain

AWS Database

Question 9Skipped

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.

Correct answer

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.

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.

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

Overall 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/

Domain

AWS Database

Question 10Skipped

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?

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.

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

Correct answer

Configure a CloudWatch Logs subscription to stream 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).

Overall 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/

Domain

AWS Management & Governance

Question 11Skipped

A music streaming company needs to incorporate a third-party song feed. The song feed sends a webhook to notify an external service when new songs are ready for consumption. A developer has written an AWS Lambda function to retrieve songs when the company receives a webhook callback. The developer must expose the Lambda function for the third party to invoke.

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

Correct answer

Generate an API Gateway endpoint for the Lambda function. Provide the API Gateway endpoint to the third party for the webhook.

Deploy a Network Load Balancer (NLB) to distribute requests to the Lambda function. Provide the NLB URL to the third party for the webhook.

Create an Amazon Simple Queue Service (Amazon SQS) queue. Connect the queue to the Lambda function. Provide the ARN of the SQS queue to the third party for the webhook.

Create an Amazon Simple Notification Service (Amazon SNS) topic. Link the topic to the Lambda function. Provide the SNS topic ARN to the third party for the webhook.

Overall explanation

API Gateway enables you to create, deploy, and manage a RESTful API to expose backend HTTP endpoints, AWS Lambda functions, or other AWS services. You can provide the third party with the API Gateway endpoint, and they can invoke the Lambda function through it. This solution is the most operationally efficient because it requires the fewest resources and management overhead.

CORRECT: "Generate an API Gateway endpoint for the Lambda function. Provide the API Gateway endpoint to the third party for the webhook" is the correct answer (as explained above.)

INCORRECT: "Deploy a Network Load Balancer (NLB) to distribute requests to the Lambda function. Provide the NLB URL to the third party for the webhook" is incorrect.

While it is possible to trigger AWS Lambda from an Application Load Balancer (ALB), not NLB, using ALB would add unnecessary complexity to the solution.

INCORRECT: "Create an Amazon Simple Notification Service (Amazon SNS) topic. Link the topic to the Lambda function. Provide the SNS topic ARN to the third party for the webhook" is incorrect.

Amazon SNS is a pub/sub messaging service, but it is not meant to expose a public-facing endpoint for third-party webhooks. Also, providing ARN to a third party would not be possible as SNS topics cannot be invoked directly from the internet.

INCORRECT: "Create an Amazon Simple Queue Service (Amazon SQS) queue. Connect the queue to the Lambda function. Provide the ARN of the SQS queue to the third party for the webhook" is incorrect.

SQS is a message queuing service used to decouple and scale microservices, distributed systems, and serverless applications. It is not suitable for exposing a public-facing endpoint for third-party webhooks. Moreover, like SNS, SQS cannot be invoked directly from the internet.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Networking & Content Delivery

Question 12Skipped

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.)

Correct selection

Migrate the PostgreSQL database to Amazon Aurora.

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

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

Correct selection

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

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

Overall 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/

Domain

AWS Database

Question 13Skipped

A health tech company runs a multi-tier medical records application in the AWS Cloud, which operates across three Availability Zones. The application architecture includes an Application Load Balancer, a cluster of Amazon EC2 instances that handle user session states, and a PostgreSQL database running on an EC2 instance.

The company anticipates a sharp surge in application traffic due to a new partnership. The company needs to scale to accommodate future application capacity demands and ensure high availability across all three Availability Zones.

Which solution will meet these requirements?

Migrate the PostgreSQL database to Amazon DynamoDB. Use DynamoDB Accelerator (DAX) to cache reads. Store the session data in DynamoDB. Migrate the application server to an Auto Scaling group across three Availability Zones.

Migrate the PostgreSQL database to Amazon Aurora with PostgreSQL compatibility with a single AZ deployment. Use Amazon ElastiCache for Memcached to manage session data and cache reads. Migrate the application server to an Auto Scaling group across three Availability Zones.

Keep the PostgreSQL database on EC2 instance. Use Amazon ElastiCache for Redis to manage session data and cache reads. Migrate the application server to an Auto Scaling group across three Availability Zones.

Correct answer

Migrate the PostgreSQL database to Amazon RDS for PostgreSQL with a Multi-AZ DB instance deployment. Use Amazon ElastiCache for Redis with a replication group to manage session data and cache reads. Migrate the application server to an Auto Scaling group across three Availability Zones.

Overall explanation

This solution fulfills all the requirements. Amazon RDS with Multi-AZ instances provides high availability and failover support for DB instances. ElastiCache for Redis supports storing session state data and can provide sub-millisecond response times, enabling applications to achieve instant, high-speed reads and writes. Auto Scaling ensures that the application has the correct number of Amazon EC2 instances to handle the load for your application.

CORRECT: "Migrate the PostgreSQL database to Amazon RDS for PostgreSQL with a Multi-AZ DB instance deployment. Use Amazon ElastiCache for Redis with a replication group to manage session data and cache reads. Migrate the application server to an Auto Scaling group across three Availability Zones" is the correct answer (as explained above.)

INCORRECT: "Migrate the PostgreSQL database to Amazon Aurora with PostgreSQL compatibility with a single AZ deployment. Use Amazon ElastiCache for Memcached to manage session data and cache reads. Migrate the application server to an Auto Scaling group across three Availability Zones" is incorrect.

Aurora is a high-performance database service, but using a single AZ deployment doesn't provide the high availability across multiple AZs the company wants. Also, while ElastiCache for Memcached can be used for caching, it doesn't offer the durability and atomicity that Redis offers, which is particularly useful for session data.

INCORRECT: "Migrate the PostgreSQL database to Amazon DynamoDB. Use DynamoDB Accelerator (DAX) to cache reads. Store the session data in DynamoDB. Migrate the application server to an Auto Scaling group across three Availability Zones" is incorrect.

Although DynamoDB is a high-performance, scalable NoSQL database, it is not a drop-in replacement for a relational database like PostgreSQL. It has a different data model and supports a different set of query options. This change could require significant modifications to the application code and may not support the same transactional capabilities as PostgreSQL.

INCORRECT: "Keep the PostgreSQL database on EC2 instance. Use Amazon ElastiCache for Redis to manage session data and cache reads. Migrate the application server to an Auto Scaling group across three Availability Zones" is incorrect.

Although the EC2 instance can run the PostgreSQL database, it does not provide the same level of managed service benefits (like automatic patching, backups, and high availability with Multi-AZ deployments) as Amazon RDS. This option would likely result in higher operational overhead and doesn't fully utilize the benefits of managed AWS services.

References:

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

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

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

Save time with our AWS cheat sheets:

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

Domain

AWS Database

Question 14Skipped

A travel agency operates a web service in an AWS Region. The service is accessed by customers via a REST API on Amazon API Gateway. The agency uses Amazon Route 53 for DNS and wants to provide individual and secure URLs for each travel agent using the service.

Which combination of steps will meet these requirements with the LEAST operational complexity? (Select THREE.)

Request a wildcard certificate that corresponds to the custom domain name in AWS Certificate Manager (ACM), within a different Region.

Correct selection

Request a wildcard certificate that matches the custom domain name in AWS Certificate Manager (ACM) in the same Region.

Correct selection

Register the desired domain with a domain registrar. Set up a wildcard custom domain in a Route 53 hosted zone and create a record in the zone that points to the API Gateway endpoint.

Establish separate API endpoints in API Gateway for each travel agent.

Correct selection

Establish a custom domain name in API Gateway for the REST API. Import the corresponding certificate from AWS Certificate Manager (ACM).

Create separate hosted zones in Route 53 for each travel agent as needed. Set up zone records that point to the API Gateway endpoint.

Overall explanation

Registering a wildcard custom domain name in Route 53 and creating a record pointing to API Gateway endpoint allows you to create unique URLs for each customer under the same domain name.

Requesting a wildcard certificate in the same AWS region as the REST API would provide secure URLs (https) for all customers under the same domain name. This would minimize the operational complexity of managing multiple certificates in different regions.

By creating a custom domain name in API Gateway and importing the wildcard certificate from ACM, the company can provide secure and unique URLs for each customer. API Gateway's custom domain names provide paths for API methods, helping maintain a consistent experience for customers.

CORRECT: "Register the desired domain with a domain registrar. Set up a wildcard custom domain in a Route 53 hosted zone and create a record in the zone that points to the API Gateway endpoint" is a correct answer (as explained above.)

CORRECT: "Request a wildcard certificate that matches the custom domain name in AWS Certificate Manager (ACM) in the same Region" is also a correct answer (as explained above.)

CORRECT: "Establish a custom domain name in API Gateway for the REST API. Import the corresponding certificate from AWS Certificate Manager (ACM)" is also a correct answer (as explained above.)

INCORRECT: "Request a wildcard certificate that corresponds to the custom domain name in AWS Certificate Manager (ACM), within a different Region" is incorrect.

Requesting a wildcard certificate in a different AWS region than your API Gateway increases operational complexity and doesn't provide any significant benefit.

INCORRECT: "Create separate hosted zones in Route 53 for each travel agent as needed. Set up zone records that point to the API Gateway endpoint" is incorrect.

Creating separate hosted zones for each travel agent can significantly increase operational complexity and cost. It would be more efficient to use a single hosted zone with a wildcard domain and use paths for differentiation.

INCORRECT: "Establish separate API endpoints in API Gateway for each travel agent" is incorrect.

Creating separate API endpoints for each travel agent can significantly increase the complexity and management overhead. Instead, it would be more efficient to use different paths under the same API endpoint.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Networking & Content Delivery

Question 15Skipped

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?

Deploy a transit gateway in the inspection VPC. Configure route tables to route the incoming packets through the transit gateway.

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

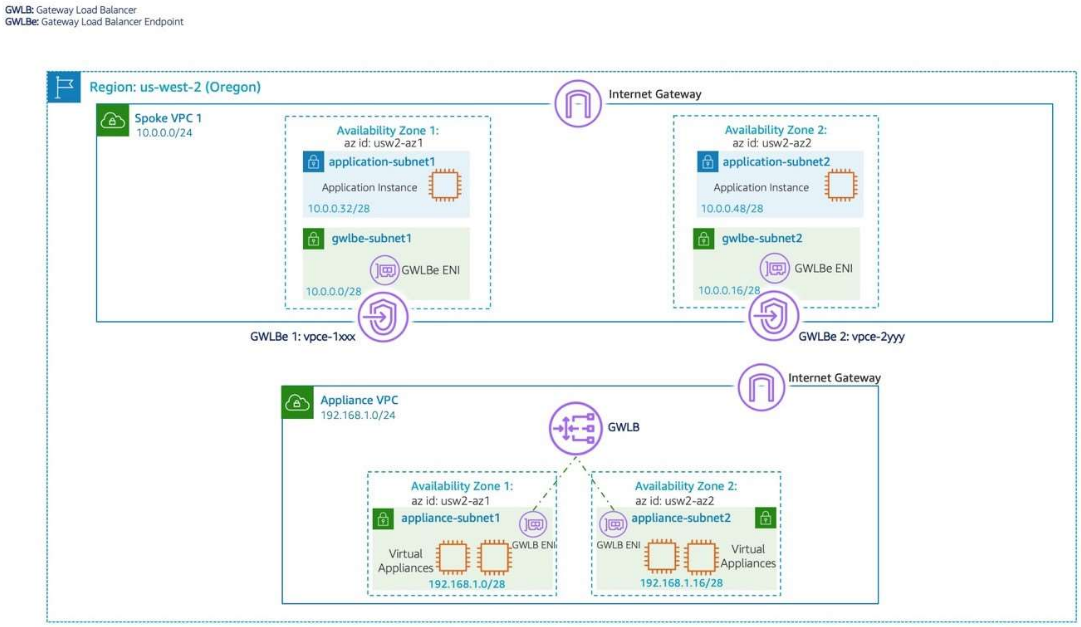
Correct answer

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.

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

Overall 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.



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/

Domain

AWS Compute

Question 16Skipped

An online game platform company is launching a new game feature that involves a significant update to their existing API hosted on Amazon API Gateway. The company wants to minimize the impact on their existing users, and they need a deployment strategy that allows them to gradually roll out the changes while monitoring for any potential issues.

What should the company do to achieve this?

Update the existing API directly in API Gateway with the new feature and immediately direct all traffic to the updated API.

Create a new version of the API and use Route 53 to gradually shift DNS queries from the existing API endpoint to the new API endpoint.

Create a completely new API for the new game feature and redirect half of the user traffic to the new API while maintaining the other half on the existing API.

Correct answer

Use an API Gateway canary release deployment. Initially direct a small percentage of user traffic to the new API version. After API verification, promote the canary stage to the production stage.

Overall explanation

The correct answer is to use Amazon API Gateway's canary release deployments. This allows the company to gradually roll out the new API version, initially exposing only a small percentage of their users to the new API. As they monitor the system and confirm that the new API is working as expected, they can increase the percentage of traffic directed to the new version.

CORRECT: "Use an API Gateway canary release deployment. Initially direct a small percentage of user traffic to the new API version. After API verification, promote the canary stage to the production stage" is the correct answer (as explained above.)

INCORRECT: "Update the existing API directly in API Gateway with the new feature and immediately direct all traffic to the updated API" is incorrect.

Updating the existing API directly in API Gateway and immediately redirecting all traffic to the updated API is risky. If there are any issues with the new API, it could negatively impact all users, rather than just a small subset of users.

INCORRECT: "Create a completely new API for the new game feature and redirect half of the user traffic to the new API while maintaining the other half on the existing API" is incorrect.

Creating a completely new API and redirecting half the user traffic to the new API is not a gradual rollout strategy. This approach would immediately expose many users to potential issues with the new API.

INCORRECT: "Create a new version of the API and use Route 53 to gradually shift DNS queries from the existing API endpoint to the new API endpoint" is incorrect.

Using Route 53 to gradually shift DNS queries from the existing API endpoint to the new API endpoint could work, but it is not as simple or efficient as using API Gateway's canary release deployments. DNS changes can also take time to propagate, potentially leading to inconsistent behavior for users.

References:

https://docs.aws.amazon.com/apigateway/latest/developerguide/canary-release.html

Save time with our AWS cheat sheets:

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

Domain

AWS Networking & Content Delivery

Question 17Skipped

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?

Correct answer

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

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

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

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

Overall 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/

Domain

AWS Security, Identity, & Compliance

Question 18Skipped

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?

Correct answer

Use the Elastic File System (EFS) and mount the file system using NFS

Add EBS volumes to each EC2 instance and configure data replication

Add EBS volumes to each EC2 instance and use an ELB to distribute data evenly between the volumes

Use the Elastic Block Store (EBS) and mount the file system at the block level

Overall 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/

Domain

AWS Storage

Question 19Skipped

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

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.

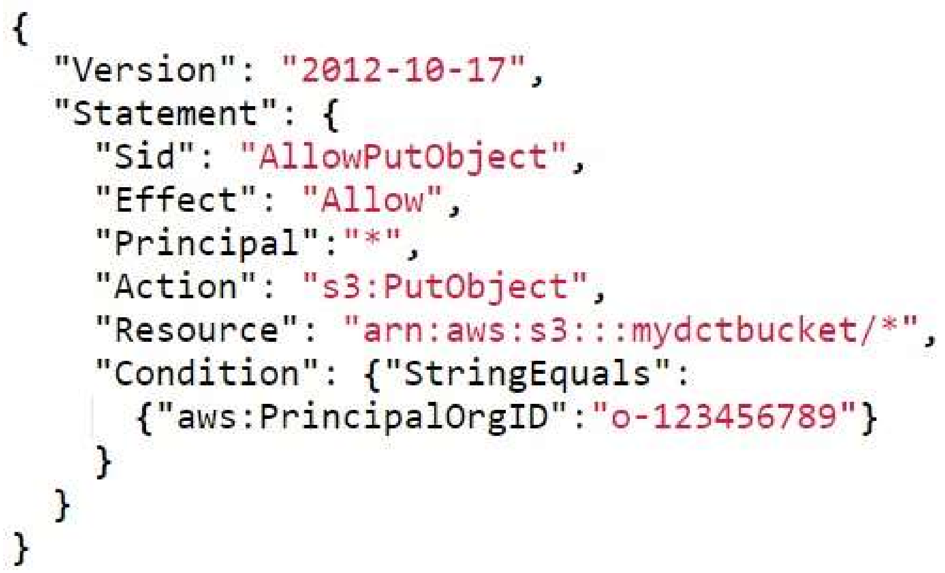
Use AWS Config and AWS Lambda functions to make remediations to the bucket policy as and when new accounts are created and tagged as not being part of AWS Organizations. Update the S3 bucket policy accordingly.

Correct answer

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.

Overall 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.



```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "AllowPutObject",
    "Effect": "Allow",
    "Principal":"*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::mydctbucket/*",
    "Condition": {"StringEquals":
      {"aws:PrincipalOrgID":"o-123456789"}
    }
  }
}
```

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/

Domain

AWS Management & Governance

Question 20Skipped

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?

You must retain all snapshots as the process is incremental and therefore data is required from each snapshot

Correct answer

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

Two snapshots, the oldest and most recent snapshots

The oldest snapshot, as this references data in all other snapshots

Overall 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/

Domain

AWS Storage

Question 21Skipped

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 AWS Transit Gateway

Create an Amazon CloudFront distribution

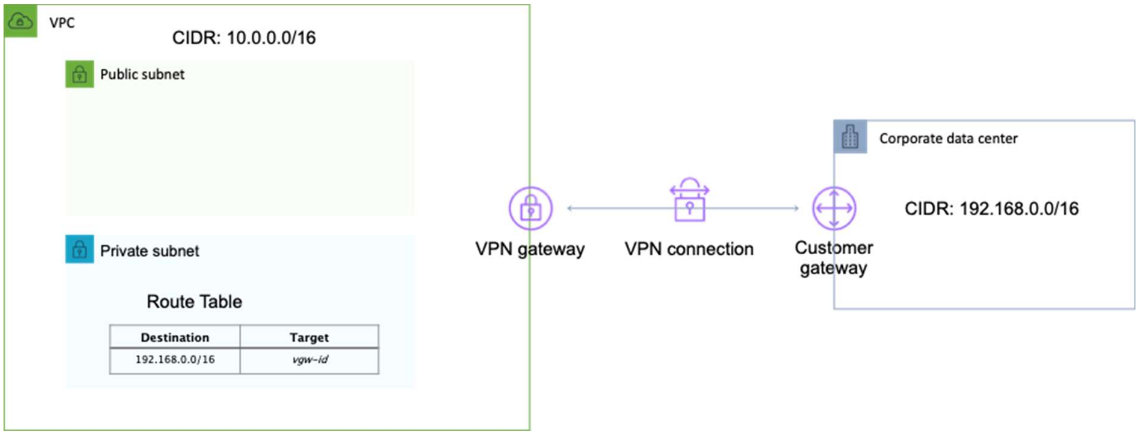
Setup an AWS Direct Connect connection

Correct answer

Configure a Virtual Private Gateway

Overall 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.



Destination	Target
192.168.0.0/16	vgw-id

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/

Domain

AWS Networking & Content Delivery

Question 22Skipped

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?

Correct answer

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

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

Overall 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 Createlmage 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

Domain

AWS Security, Identity, & Compliance

Question 23Skipped

A software firm is developing a microservices-based application to be deployed on Amazon ECS. This application needs to interact with a resilient, shared filesystem capable of restoring data to a different AWS Region with a Recovery Point Objective (RPO) of 2 hours.

The filesystem is also expected to provide a mount target in each Availability Zone (AZ) within a Region. The solutions architect intends to employ AWS Backup to oversee the cross-Region data replication.

Which option will meet these requirements?

Amazon FSx for NetApp ONTAP with a Multi-AZ deployment.

Amazon FSx for OpenZFS.

Correct answer

Amazon Elastic File System (Amazon EFS) with the Standard storage class.

Amazon FSx for Windows File Server with a Multi-AZ deployment.

Overall explanation

Amazon Elastic File System (Amazon EFS) provides simple, scalable file storage for use with Amazon EC2 instances and other AWS services. It supports the Network File System (NFS) protocol and can be configured with mount points in multiple AZs.

EFS can be used with AWS Backup for automated and centralized backup across AWS services, and supports replication to another region, satisfying the given requirement.

All replication traffic stays on the AWS global backbone, and most changes are replicated within a minute, with an overall Recovery Point Objective (RPO) of 15 minutes for most file systems.

CORRECT: "Amazon Elastic File System (Amazon EFS) with the Standard storage class" is the correct answer (as explained above.)

INCORRECT: "Amazon FSx for Windows File Server with a Multi-AZ deployment" is incorrect.

Amazon FSx for Windows File Server provides fully managed, reliable, and scalable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol. It is built on Windows Server and offers a native Windows file system experience for Windows-based applications. However, it doesn't support cross-Region data replication, making it unsuitable for the given requirement.

INCORRECT: "Amazon FSx for NetApp ONTAP with a Multi-AZ deployment" is incorrect.

Amazon FSx for NetApp ONTAP is more suitable to scenarios where you want to migrate applications using ONTAP software and if you’re already using NetApp systems. It is better in this case to use Amazon EFS.

INCORRECT: "Amazon FSx for OpenZFS" is incorrect.

Amazon FSx for OpenZFS is suitable if you have a specific requirement to use OpenZFS. For this use case Amazon EFS is a better choice and will likely be more cost-effective.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 24Skipped

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

Correct answer

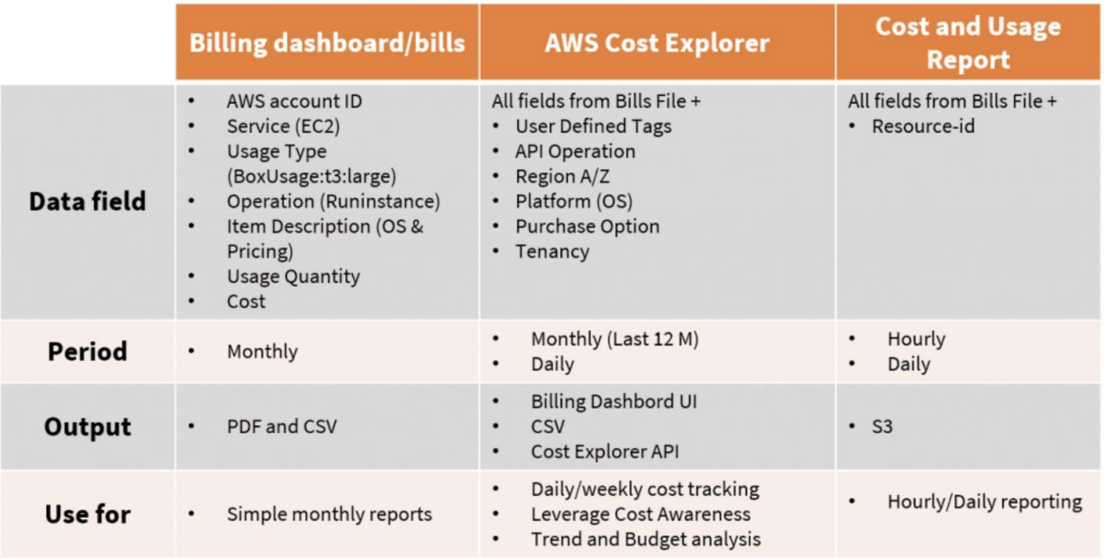
Use Cost Explorer's granular filtering feature to perform an in-depth analysis of EC2 costs based on instance types.

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.

Overall 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/

Domain

AWS Compute

Question 25Skipped

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 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.

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

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

Correct answer

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.

Overall 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/

Domain

AWS Storage

Question 26Skipped

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

Correct answer

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

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

Overall 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/

Domain

AWS Compute

Question 27Skipped

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?

Configure the MySQL databases to use AWS KMS data encryption keys

Correct answer

Create the MySQL user accounts to use the AWSAuthenticationPlugin with IAM

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

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

Overall 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/

Domain

AWS Database

Question 28Skipped

A digital marketing agency manages numerous client websites and apps on AWS. Each AWS resource is supposed to be tagged by the account for tracking and backup purposes. The agency wants to ensure that all AWS resources, including untagged ones, are backed up properly to minimize data loss risks.

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

Rely on each account owner to identify their untagged resources and then use AWS Backup for backing up.

Correct answer

Use AWS Config to identify all untagged resources and tag them programmatically. Then, use AWS Backup to automate the backup of all AWS resources based on tags.

Manually search for all untagged resources in each AWS service. Once identified, tag them appropriately and set up AWS Backup for each service separately.

Use AWS Lambda to periodically scan for untagged resources, add necessary tags, and then set up AWS Backup.

Overall explanation

This solution is the most operationally efficient due to the powerful combination of AWS Config and AWS Backup.

AWS Config: This service enables you to assess, audit, and evaluate the configurations of your AWS resources. AWS Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. You can use AWS Config to review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. In this scenario, AWS Config can be utilized to identify all resources that lack proper tags.

Tagging: Tags can be added to AWS resources programmatically. By tagging resources, you organize them into groups and subgroups, which can be based on purpose, owner, environment, or other criteria. In this context, tagging resources allows AWS Backup to identify and group resources that need to be backed up.

AWS Backup: AWS Backup is a fully managed backup service that makes it easy to centralize and automate the back up of data across AWS services. You can use AWS Backup to protect several AWS resource types, including Amazon EBS volumes, Amazon RDS databases, Amazon DynamoDB tables, Amazon EFS file systems, and AWS Storage Gateway volumes. It offers a centralized dashboard where you can manage all backups and allows you to automate and monitor backups across AWS services using policies.

With AWS Config identifying and tagging untagged resources, and AWS Backup automating the backup of tagged resources, this solution requires minimal operational overhead while ensuring all resources are adequately backed up.

CORRECT: "Use AWS Config to identify all untagged resources and tag them programmatically. Then, use AWS Backup to automate the backup of all AWS resources based on tags" is the correct answer (as explained above.)

INCORRECT: "Manually search for all untagged resources in each AWS service. Once identified, tag them appropriately and set up AWS Backup for each service separately" is incorrect.

Searching for untagged resources manually in each service and setting up AWS Backup separately for each one would require a significant amount of operational overhead.

INCORRECT: "Rely on each account owner to identify their untagged resources and then use AWS Backup for backing up" is incorrect.

Relying on individual account owners could result in inconsistency and increase the risk of missed resources or backups. Centralized backup management using AWS Backup is more efficient.

INCORRECT: "Use AWS Lambda to periodically scan for untagged resources, add necessary tags, and then set up AWS Backup" is incorrect.

Although AWS Lambda could be used to scan for untagged resources and add necessary tags, this would require developing and maintaining a custom script. AWS Config can handle this process with less operational overhead.

References:

https://docs.aws.amazon.com/aws-backup/latest/devguide/assigning-resources.html

Save time with our AWS cheat sheets:

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

Domain

AWS Management & Governance

Question 29Skipped

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

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.

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.

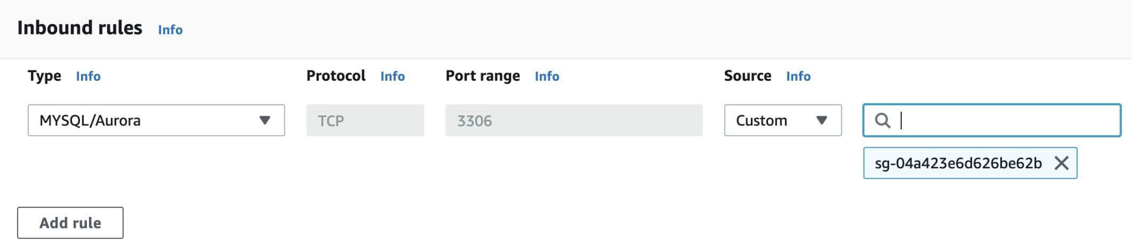
Correct answer

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.

Overall 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.



Inbound rules Info

Type Info	Protocol Info	Port range Info	Source Info	
MYSQL/Aurora ▼	TCP	3306	Custom ▼	🔍 | sg-04a423e6d626be62b ✕

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/

Domain

AWS Security, Identity, & Compliance

Question 30Skipped

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 Maintenance Windows to install the tool on all the EC2 instances within a set period of time.

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.

Correct answer

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

Use AWS Systems Manager Patch Manager to install the tool on all the EC2 instances within a single patch.

Overall 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/

Domain

AWS Management & Governance

Question 31Skipped

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. 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.

Correct answer

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.

Overall 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/

Domain

AWS Storage

Question 32Skipped

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 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.

Correct selection

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 selection

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.

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.

Overall 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/

Domain

AWS Application Integration

Question 33Skipped

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?

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).

Correct answer

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.

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.

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.

Overall 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/

Domain

AWS Application Integration

Question 34Skipped

A software development company is creating a microservices-based application using Amazon Elastic Kubernetes Service (Amazon EKS). The company needs to ensure that sensitive configuration data like database credentials and API keys stored in Kubernetes ConfigMaps and Secrets are encrypted at rest.

Which solution will meet these requirements?

Use Amazon S3 to store all sensitive data. Enable server-side encryption with a new AWS Key Management Service (AWS KMS) key.

Create the Amazon EKS cluster with default options. Use the Amazon Elastic File System (Amazon EFS) Container Storage Interface (CSI) driver as an add-on.

Implement AWS Secrets Manager to manage, rotate, and store all sensitive data. Integrate it with the Amazon EKS cluster.

Correct answer

Create a new AWS Key Management Service (AWS KMS) key. Enable Amazon EKS KMS secrets encryption on the Amazon EKS cluster.

Overall explanation

Amazon EKS supports using AWS KMS keys for envelope encryption of Kubernetes secrets. To meet the requirement of encrypting Kubernetes Secrets at rest, we can use a customer managed AWS KMS key and enable secrets encryption while creating or updating an EKS cluster.

CORRECT: "Create a new AWS Key Management Service (AWS KMS) key. Enable Amazon EKS KMS secrets encryption on the Amazon EKS cluster" is the correct answer (as explained above.)

INCORRECT: "Implement AWS Secrets Manager to manage, rotate, and store all sensitive data. Integrate it with the Amazon EKS cluster" is incorrect.

While AWS Secrets Manager can store and manage sensitive information, it doesn't directly encrypt Kubernetes Secrets and ConfigMaps stored in the etcd key-value store.

INCORRECT: "Create the Amazon EKS cluster with default options. Use the Amazon Elastic File System (Amazon EFS) Container Storage Interface (CSI) driver as an add-on" is incorrect.

The EFS CSI driver enables Kubernetes pods to mount EFS file systems, but it does not offer a mechanism for encrypting secrets stored in Kubernetes.

INCORRECT: "Use Amazon S3 to store all sensitive data. Enable server-side encryption with a new AWS Key Management Service (AWS KMS) key" is incorrect.

While S3 can store sensitive data and encrypt it using KMS, it does not provide a way to directly encrypt Kubernetes ConfigMaps and Secrets stored in etcd.

References:

https://docs.aws.amazon.com/eks/latest/userguide/enable-kms.html

Save time with our AWS cheat sheets:

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

Domain

AWS Security, Identity, & Compliance

Question 35Skipped

A game development company is planning to build a cloud-based game platform on AWS. The player activity patterns are unpredictable and could remain idle for extended periods. Only players who have purchased the game should have the ability to log in and play.

Which combination of steps will meet these requirements MOST cost-effectively? (Select THREE.)

Use Amazon S3 static web hosting with HTML, CSS, and JS. Use Amazon CloudFront to distribute the frontend game interface.

Use AWS Cognito Identity Pools to handle user authentication.

Correct selection

Implement an AWS Lambda function to fetch player information from Amazon DynamoDB. Establish an Amazon API Gateway endpoint to handle RESTful API calls, directing them to the Lambda function.

Correct selection

Use AWS Cognito User Pools to handle user authentication.

Set up an Amazon Elastic Container Service (Amazon ECS) service behind an Application Load Balancer to fetch player information from Amazon RDS. Establish an Amazon API Gateway endpoint to handle RESTful API calls, directing them to the ECS service.

Correct selection

Leverage AWS Amplify to serve the frontend game interface with HTML, CSS, and JS. Use the integrated Amazon CloudFront configuration for distribution.

Overall explanation

AWS Lambda is a cost-effective solution for unpredictable traffic patterns due to its pay-per-use pricing model. DynamoDB is also a cost-effective and highly scalable solution for storing user data. The API Gateway provides a HTTP-based endpoint that can be used to expose the Lambda function.

AWS Cognito User Pools provide user directory features including sign-up and sign-in services, which are suitable for managing game user authentication.

AWS Amplify simplifies the process of hosting web applications with automated deployment processes. It also integrates with CloudFront, providing a global content delivery network to efficiently serve the game interface.

CORRECT: "Implement an AWS Lambda function to fetch player information from Amazon DynamoDB. Establish an Amazon API Gateway endpoint to handle RESTful API calls, directing them to the Lambda function" is a correct answer (as explained above.)

CORRECT: "Use AWS Cognito User Pools to handle user authentication" is also a correct answer (as explained above.)

CORRECT: "Leverage AWS Amplify to serve the frontend game interface with HTML, CSS, and JS. Use the integrated Amazon CloudFront configuration for distribution" is also a correct answer (as explained above.)

INCORRECT: "Set up an Amazon Elastic Container Service (Amazon ECS) service behind an Application Load Balancer to fetch player information from Amazon RDS. Establish an Amazon API Gateway endpoint to handle RESTful API calls, directing them to the ECS service" is incorrect.

Using Amazon ECS might be an overkill for this scenario and might not be as cost-effective compared to Lambda and DynamoDB, especially for unpredictable and possibly idle traffic.

INCORRECT: "Use AWS Cognito Identity Pools to handle user authentication" is incorrect.

Cognito Identity Pools are used for granting access to AWS resources rather than handling user authentication.

INCORRECT: "Use Amazon S3 static web hosting with HTML, CSS, and JS. Use Amazon CloudFront to distribute the frontend game interface" is incorrect.

While you could host a static website on S3 and use CloudFront for distribution, AWS Amplify can provide additional capabilities tailored to modern web applications. Furthermore, Amplify's automated deployment processes can provide a more streamlined and efficient approach to managing the game's frontend compared to managing separate S3 and CloudFront configurations.

References:

https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-identity-pools.html https://aws.amazon.com/amplify/

Save time with our AWS cheat sheets:

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

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

Domain

AWS Networking & Content Delivery

Question 36Skipped

An e-commerce company operates a containerized microservices application on a fleet of Amazon EC2 instances. As part of their infrastructure improvement efforts, the company plans to migrate the application to Amazon Elastic Kubernetes Service (Amazon EKS) for enhanced scalability and management.

As part of the security protocol, the company has configured the Amazon EKS control plane with endpoint private access enabled and public access disabled. The data plane resides within private subnets. However, the company faces an issue where nodes fail to join the cluster.

What can be done to allow the nodes to join the EKS cluster?

Modify the associated IAM role to include permissions to the AmazonEKSClusterPolicy.

Move nodes to public subnet and configure security group rules for the EC2 nodes.

Establish VPC peering connection for nodes to access the control plane.

Correct answer

Set up VPC endpoints for Amazon EKS and ECR to enable nodes to communicate with the control plane.

Overall explanation

When the EKS control plane is configured with private access, and the nodes are in a private subnet, you need to create VPC endpoints for Amazon EKS and ECR. This allows the nodes to communicate with the EKS control plane and pull container images from ECR.

CORRECT: "Set up VPC endpoints for Amazon EKS and ECR to enable nodes to communicate with the control plane" is the correct answer (as explained above.)

INCORRECT: "Modify the associated IAM role to include permissions to the AmazonEKSClusterPolicy" is incorrect.

IAM roles are crucial for setting up permissions, but simply modifying the associated IAM role would not solve the issue of nodes not being able to connect to the control plane.

INCORRECT: "Establish VPC peering connection for nodes to access the control plane" is incorrect.

VPC peering is not the recommended way to allow nodes in a private subnet to access the EKS control plane. This approach might also incur additional operational overhead.

INCORRECT: "Move nodes to public subnet and configure security group rules for the EC2 nodes" is incorrect.

Moving the nodes to public subnets contradicts the original requirement of having the data plane in private subnets. Additionally, this approach might introduce unnecessary security risks.

References:

https://docs.aws.amazon.com/eks/latest/userguide/private-clusters.html

Save time with our AWS cheat sheets:

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

Domain

AWS Compute

Question 37Skipped

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

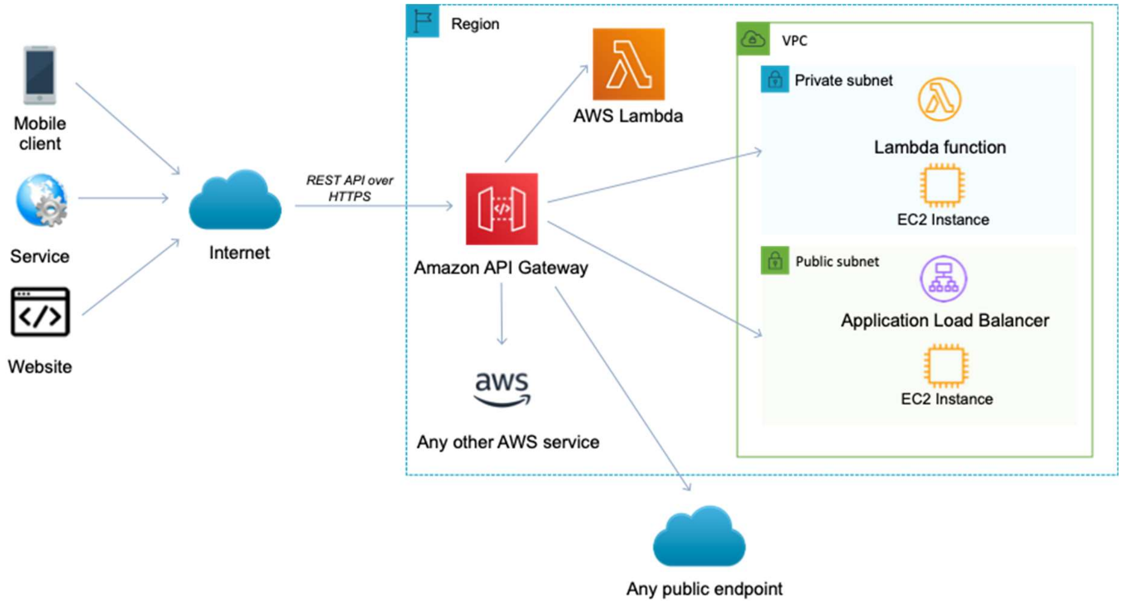
Correct answer

Migrate the API to Amazon API Gateway and use AWS Lambda as the backend

Overall 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/

Domain

AWS Networking & Content Delivery

Question 38Skipped

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 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 users and groups.

Correct answer

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.

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.

Overall 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/

Domain

AWS Database

Question 39Skipped

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?

Launch EC2 instances in a secondary AWS Region. Keep the EC2 instances in the secondary Region active at all times.

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.

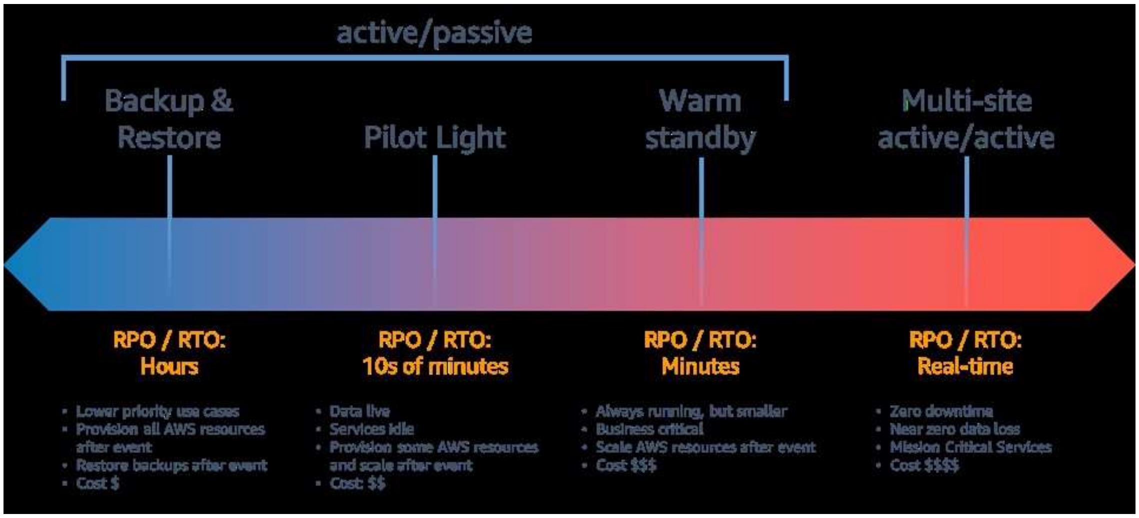
Correct answer

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.

Launch EC2 instances in a secondary Availability Zone. Keep the EC2 instances in the secondary Availability Zone active at all times.

Overall 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.


active/passive
Backup & Restore
Pilot Light
Warm standby
Multi-site active/active
RPO / RTO: Hours
RPO / RTO: 10s of minutes
RPO / RTO: Minutes
RPO / RTO: Real-time
• Lower priority use cases
• Provision all AWS resources after event
• Restore backups after event
• Cost $
• Data live
• Services idle
• Provision some AWS resources and scale after event
• Cost: $$
• Always running, but smaller
• Business critical
• Scale AWS resources after event
• Cost $$$
• Zero downtime
• Near zero data loss
• Mission Critical Services
• Cost $$$$

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/

Domain

AWS Cloud Architecture & Design

Question 40Skipped

A software development firm uses AWS to run their compute instances across multiple accounts. These instances are individually billed. The company recently purchased an EC2 Reserved Instance (RI) for an ongoing project. However, due to the completion of that project, a significant number of EC2 instances were decommissioned. The company now wishes to utilize the benefits of their unused Reserved Instance across their other AWS accounts.

Which combination of steps should the company follow to achieve this? (Select TWO.)

Correct selection

Establish an AWS Organization in the AWS account that purchased the RI and hosts the remaining active EC2 instances. Invite the other AWS accounts to join this organization from the management account.

From the AWS Organizations management account, utilize AWS Resource Access Manager (AWS RAM) to share the Reserved Instance with other accounts.

Correct selection

Enable Reserved Instance sharing in the billing preferences section of the AWS Management Console for the account that purchased the existing RI.

Use AWS Organizations to establish a new payer account and invite the other accounts to join this organization.

Enable Reserved Instance sharing in the billing preferences section of the AWS Management Console for the management account.

Overall explanation

Just like the Savings Plans, the benefits of Reserved Instances can be applied across accounts if those accounts are part of the same AWS Organization and if sharing is enabled. This can be achieved by enabling Reserved Instance sharing in the AWS Management Console for the account that purchased the RI.

Setting up an AWS Organization from the account that purchased the Reserved Instance allows you to group your accounts. After the organization is set up, you can invite other accounts to join the organization, enabling you to share the benefits of the Reserved Instance across all accounts in the organization.

CORRECT: "Enable Reserved Instance sharing in the billing preferences section of the AWS Management Console for the account that purchased the existing RI" is a correct answer (as explained above.)

CORRECT: "Establish an AWS Organization in the AWS account that purchased the RI and hosts the remaining active EC2 instances. Invite the other AWS accounts to join this organization from the management account" is also a correct answer (as explained above.)

INCORRECT: "From the AWS Organizations management account, utilize AWS Resource Access Manager (AWS RAM) to share the Reserved Instance with other accounts" is incorrect.

AWS RAM does not apply to Reserved Instances. It is used to share other resources like Subnets, Transit Gateways, etc.

INCORRECT: "Enable Reserved Instance sharing in the billing preferences section of the AWS Management Console for the management account" is incorrect.

Reserved Instance sharing needs to be enabled in the account that purchased the RI, not the management account.

INCORRECT: "Use AWS Organizations to establish a new payer account and invite the other accounts to join this organization" is incorrect.

Creating a new payer account is not necessary. It would be more efficient to use the existing account that purchased the Reserved Instance.

References:

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-what-is.html

Save time with our AWS cheat sheets:

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

Domain

AWS Management & Governance

Question 41Skipped

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?

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.

Persist the messages in Amazon Kinesis Data Analytics. Make sure the consumer applications are configured to read and process the messages.

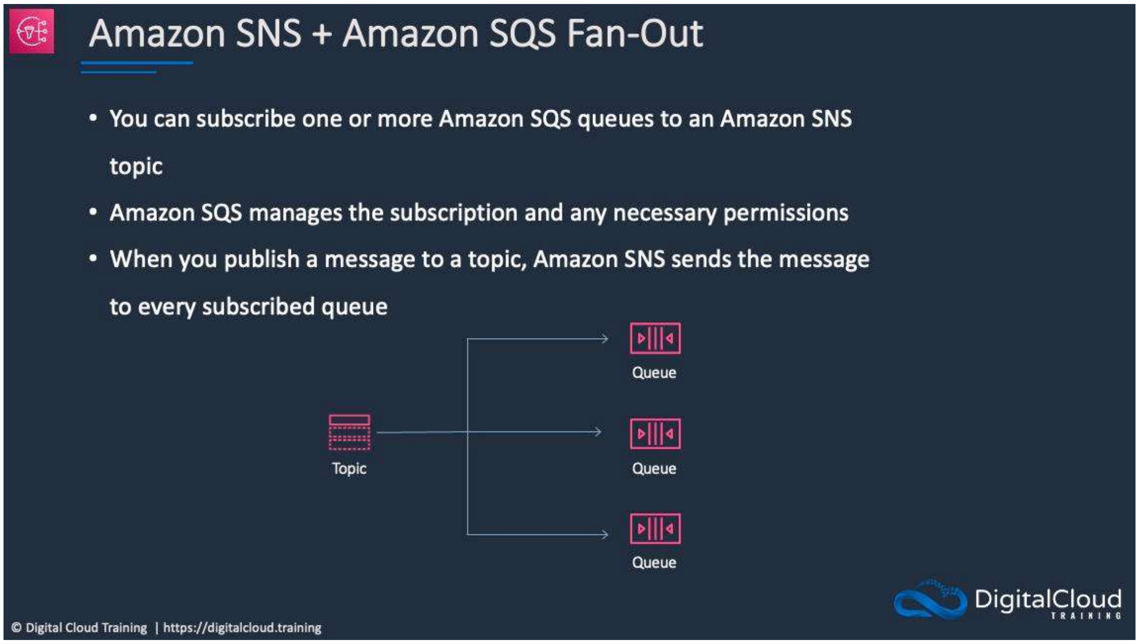
Correct answer

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.

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

Overall 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.



Amazon SNS + Amazon SQS Fan-Out

- You can subscribe one or more Amazon SQS queues to an Amazon SNS topic
- Amazon SQS manages the subscription and any necessary permissions
- When you publish a message to a topic, Amazon SNS sends the message to every subscribed queue

Topic

Queue

Queue

Queue

© Digital Cloud Training | https://digitalcloud.training

DigitalCloud TRAINING

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/

Domain

AWS Application Integration

Question 42Skipped

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.

Correct answer

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

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

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

Overall 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/

Domain

AWS Security, Identity, & Compliance

Question 43Skipped

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

Correct answer

Warm standby

Multi-site

Backup and restore

Overall 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/

Domain

AWS Cloud Architecture & Design

Question 44Skipped

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 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

Correct answer

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

Overall 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/

Domain

AWS Migration & Transfer

Question 45Skipped

A healthcare company maintains patient records in Amazon S3. To comply with HIPAA regulations, the stored data must not contain any protected health information (PHI). The company recently found out that some objects in the S3 buckets contain PHI. The company needs to automate the detection of PHI in the S3 buckets and notify its compliance team when such data is detected.

Which solution will meet these requirements?

Use Amazon Macie. Create an Amazon EventBridge rule to filter the 'SensitiveData:S3Object/Health' event type from Macie findings and trigger an Amazon Simple Email Service (Amazon SES) notification to the compliance team.

Correct answer

Use Amazon Macie. Create an AWS Lambda function to filter the ‘SensitiveData:S3Object/Personal’ event type from Macie findings and trigger an Amazon Simple Notification Service (Amazon SNS) notification to the compliance team.

Use AWS Security Hub. Create an Amazon EventBridge rule to filter the ‘Security Hub findings - High severity’ event type and send an Amazon Simple Notification Service (Amazon SNS) notification to the compliance team.

Use AWS Security Hub. Create an AWS Lambda function to filter the ‘Security Hub findings - High severity’ event type and trigger an Amazon Simple Email Service (Amazon SES) notification to the compliance team.

Overall explanation

Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data like PHI. An Amazon EventBridge rule can be created to filter specific event types from Macie findings. When Macie identifies PHI in the S3 bucket, the EventBridge rule triggers an Amazon SNS notification to the compliance team.

CORRECT: "Use Amazon Macie. Create an AWS Lambda function to filter the ‘SensitiveData:S3Object/Personal’ event type from Macie findings and trigger an Amazon Simple Notification Service (Amazon SNS) notification to the compliance team" is the correct answer (as explained above.)

INCORRECT: "Use Amazon Macie. Create an Amazon EventBridge rule to filter the ‘SensitiveData:S3Object/Health’ event type from Macie findings and trigger an Amazon Simple Email Service (Amazon SES) notification to the compliance team" is incorrect.

The correct filder is ‘SensitiveData:S3Object/Personal’ which includes personally identifiable information (PII) such as passport numbers or driver's license identification numbers, personal health information (PHI) such as health insurance or medical identification numbers, or a combination of PII and PHI.

INCORRECT: "Use AWS Security Hub. Create an Amazon EventBridge rule to filter the ‘Security Hub findings - High severity’ event type and send an Amazon Simple Notification Service (Amazon SNS) notification to the compliance team" is incorrect.

AWS Security Hub gives a comprehensive view of high-priority security alerts and compliance status, but it does not offer data-specific detection like PHI in S3 objects.

INCORRECT: "Use AWS Security Hub. Create an AWS Lambda function to filter the ‘Security Hub findings - High severity’ event type and trigger an Amazon Simple Email Service (Amazon SES) notification to the compliance team" is incorrect.

AWS Security Hub does not offer detection of specific data types like PHI in S3 objects. Therefore, using it for this purpose would not meet the requirements.

References:

https://docs.aws.amazon.com/macie/latest/user/findings-types.html

Domain

AWS Security, Identity, & Compliance

Question 46Skipped

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 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

Correct answer

Set up AWS Firewall Manager in both Regions. Centrally configure AWS WAF rules.

Set up AWS Shield in both Regions. Associate Regional web ACLs with an API stage.

Overall 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/

Domain

AWS Security, Identity, & Compliance

Question 47Skipped

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 SQS queue. Use AWS Lambda to process the files from the queue and save to an Amazon S3 bucket

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

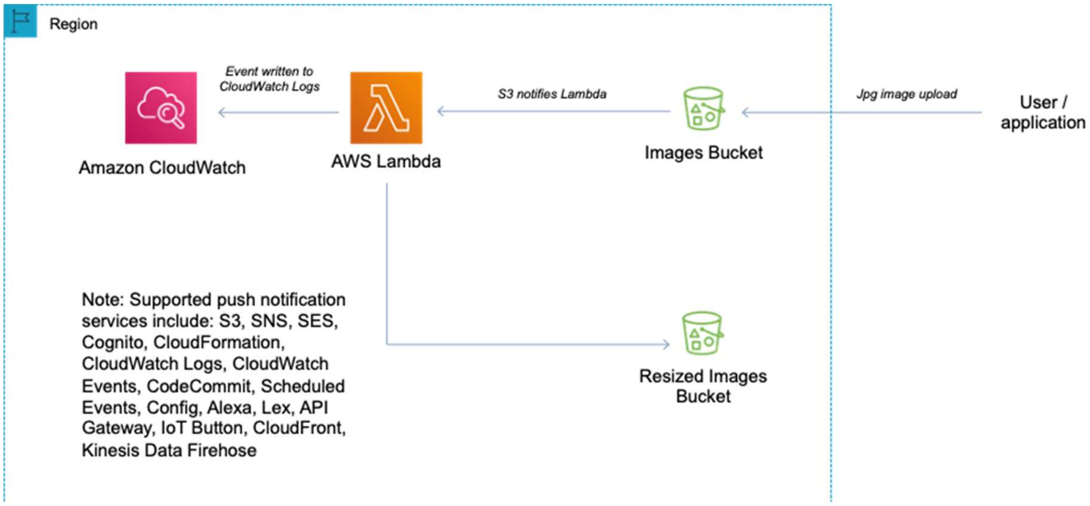
Correct answer

Write the log files to an Amazon S3 bucket. Create an event notification to invoke an AWS Lambda function that will process the files

Overall 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.


Region
Event written to CloudWatch Logs
Amazon CloudWatch
AWS Lambda
S3 notifies Lambda
Images Bucket
Jpg image upload
User / application
Note: Supported push notification services include: S3, SNS, SES, Cognito, CloudFormation, CloudWatch Logs, CloudWatch Events, CodeCommit, Scheduled Events, Config, Alexa, Lex, API Gateway, IoT Button, CloudFront, Kinesis Data Firehose
Resized Images Bucket

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/

Domain

AWS Compute

Question 48Skipped

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

Correct answer

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

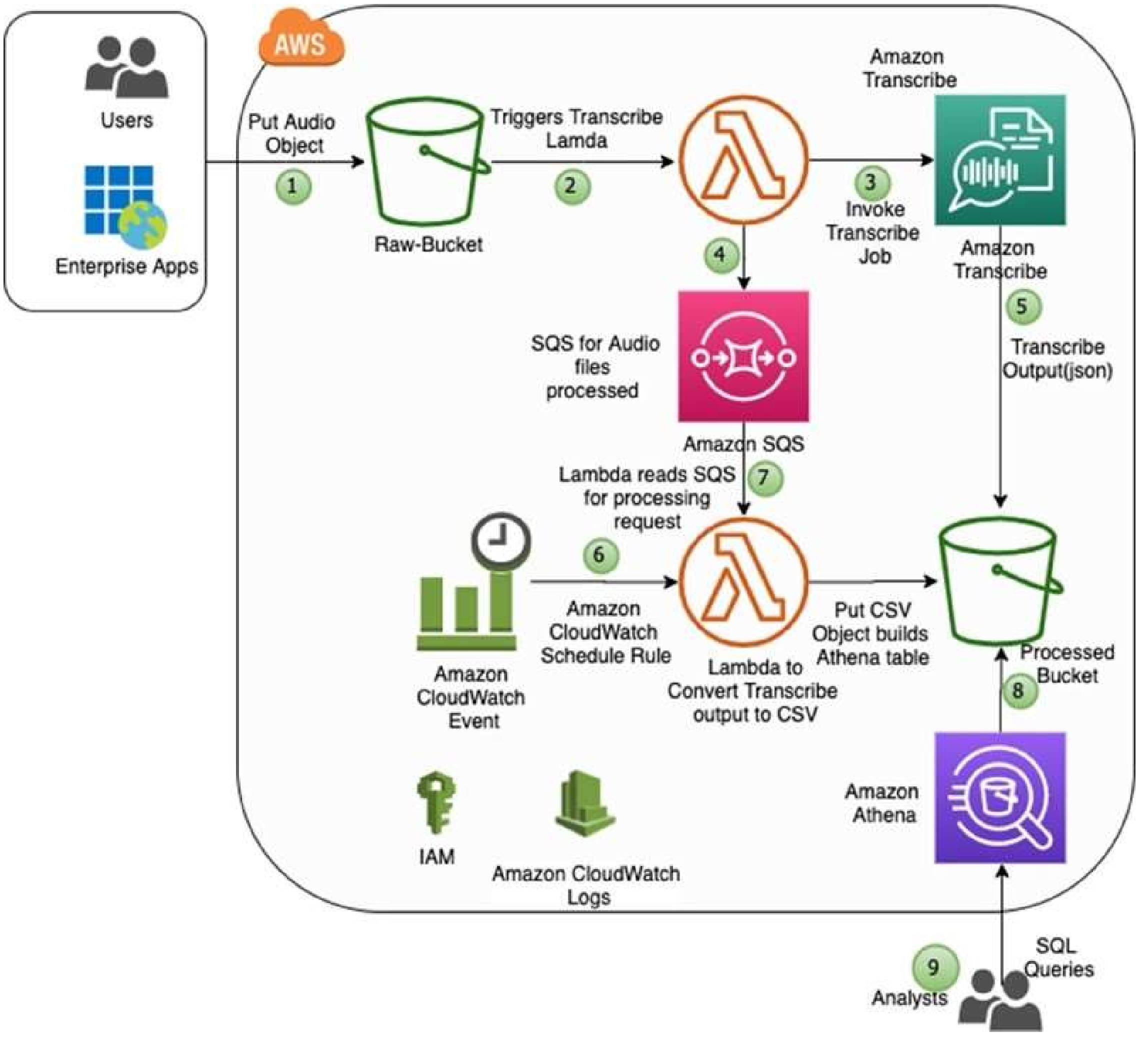
Use Amazon Translate for multiple speaker recognition. Store the transcript files in Amazon Redshift. Use SQL queries for transcript file analysis.

Overall 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.

Diagram: Analyze Multi-Speaker Audio Files Using Amazon Transcribe and Amazon Athena



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/

Domain

AWS Machine Learning

Question 49Skipped

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?

Correct answer

Store the session data in an Amazon DynamoDB table.

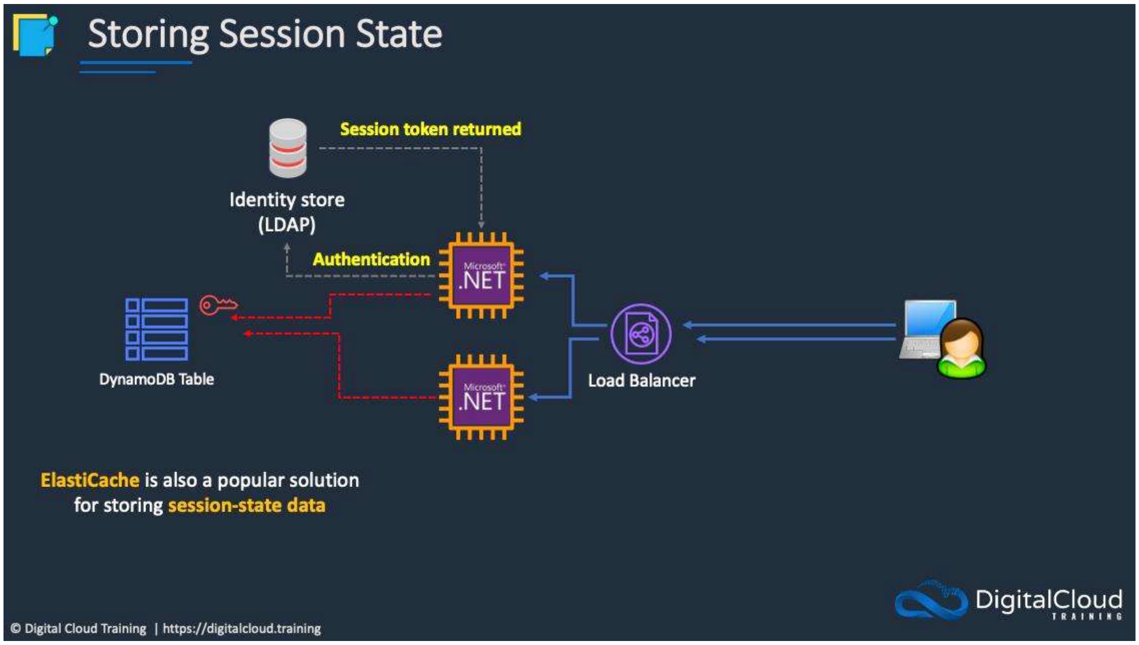
Move the session data to Amazon S3 Glacier Deep Archive.

Move the session data to Amazon ElastiCache for Memcached.

Deploy a larger EC2 instance with a larger instance store.

Overall 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/

Domain

AWS Database

Question 50Skipped

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?

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

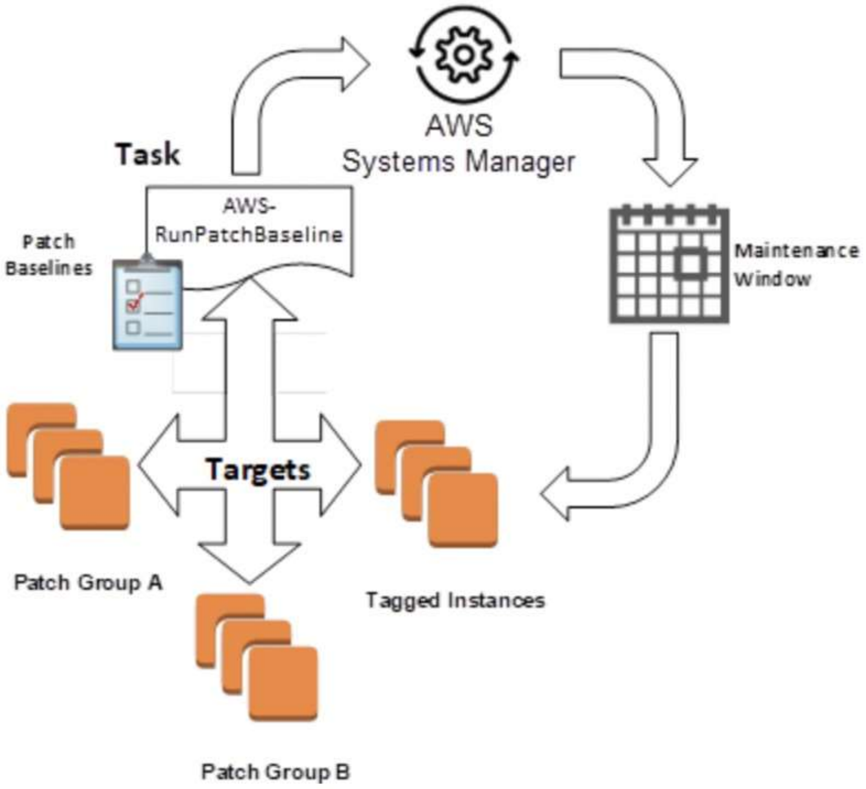
Schedule an AWS Systems Manager maintenance window to apply the patch to all EC2 instances.

Correct answer

Configure AWS Systems Manager Patch Manager 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.

Overall 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/

Domain

AWS Management & Governance

Question 51Skipped

A financial firm is aiming to leverage AWS Cloud for augmenting its on-premises disaster recovery (DR) architecture. The firm's main application, running on PostgreSQL, is housed on a virtual machine (VM) on-premises. The DR solution needs to align with the application's recovery point objective (RPO) of less than a minute and a recovery time objective (RTO) of within two hours, all while keeping costs to a minimum.

Which solution will meet these requirements?

Configure an active-active multi-site setup between the on-premises server and AWS using PostgreSQL with a third-party high availability solution.

Utilize third-party backup software to perform daily backups and store a secondary set of backups in Amazon S3.

Use AWS Elastic Disaster Recovery with continuous replication to act as a pilot light solution on AWS.

Correct answer

Set up a warm standby Amazon RDS for PostgreSQL database on AWS. Configure AWS Database Migration Service (AWS DMS) to use change data capture (CDC).

Overall explanation

Configuring a warm standby Amazon RDS for PostgreSQL database on AWS and using AWS DMS with change data capture will meet the RTO and RPO requirements. DMS can handle the ongoing replication from the on-premises PostgreSQL to the standby RDS instance, providing a near real-time replica of the data.

In a DR scenario, this standby instance can be promoted to become the new primary database, meeting the required RTO and RPO.

CORRECT: "Set up a warm standby Amazon RDS for PostgreSQL database on AWS. Configure AWS Database Migration Service (AWS DMS) to use change data capture (CDC)" is the correct answer (as explained above.)

INCORRECT: "Configure an active-active multi-site setup between the on-premises server and AWS using PostgreSQL with a third-party high availability solution" is incorrect.

Setting up an active-active multi-site setup between the on-premises server and AWS using PostgreSQL with a third-party high availability solution might meet the RPO and RTO requirements, but it would likely be more expensive and complex than the correct answer.

INCORRECT: "Use AWS Elastic Disaster Recovery with continuous replication to act as a pilot light solution on AWS" is incorrect.

AWS Elastic Disaster Recovery with continuous replication can provide a DR solution, but for a database, it is typically more efficient to use a service designed for that purpose, like RDS with DMS.

INCORRECT: "Utilize third-party backup software to perform daily backups and store a secondary set of backups in Amazon S3" is incorrect.

Using third-party backup software to perform daily backups and storing a secondary set of backups in Amazon S3 would not meet the RPO of less than a minute, as this approach could lead to a data loss up to 24 hours. Also, the process of restoring from a backup might not meet the RTO of within two hours.

References:

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

Save time with our AWS cheat sheets:

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

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

Domain

AWS Database

Question 52Skipped

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?

Correct answer

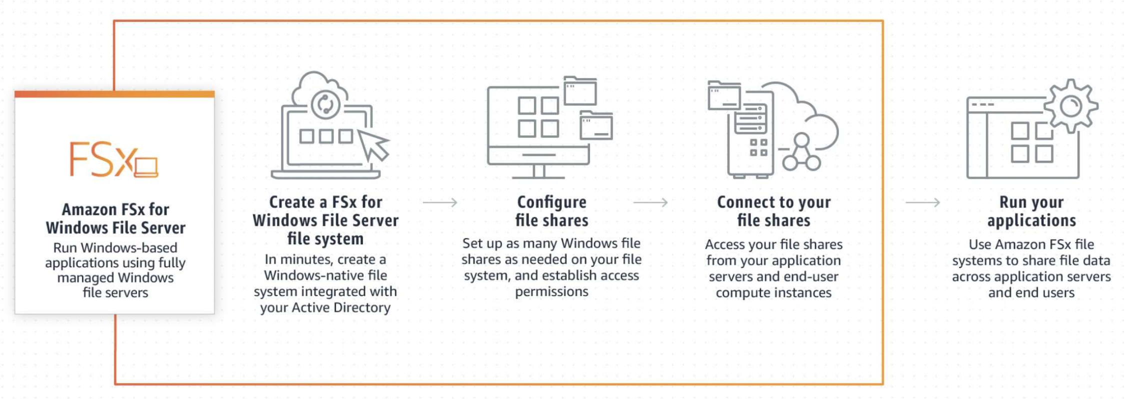
Extend the file share environment to Amazon FSx for Windows File Server with a Multi-AZ configuration. Migrate all the data to FSx for Windows File Server.

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.

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

Overall explanation



FSx
Amazon FSx for Windows File Server
Run Windows-based applications using fully managed Windows file servers
Create a FSx for Windows File Server file system
In minutes, create a Windows-native file system integrated with your Active Directory
Configure file shares
Set up as many Windows file shares as needed on your file system, and establish access permissions
Connect to your file shares
Access your file shares from your application servers and end-user compute instances
Run your applications
Use Amazon FSx file systems to share file data across application servers and end users

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/

Domain

AWS Storage

Question 53Skipped

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.

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.

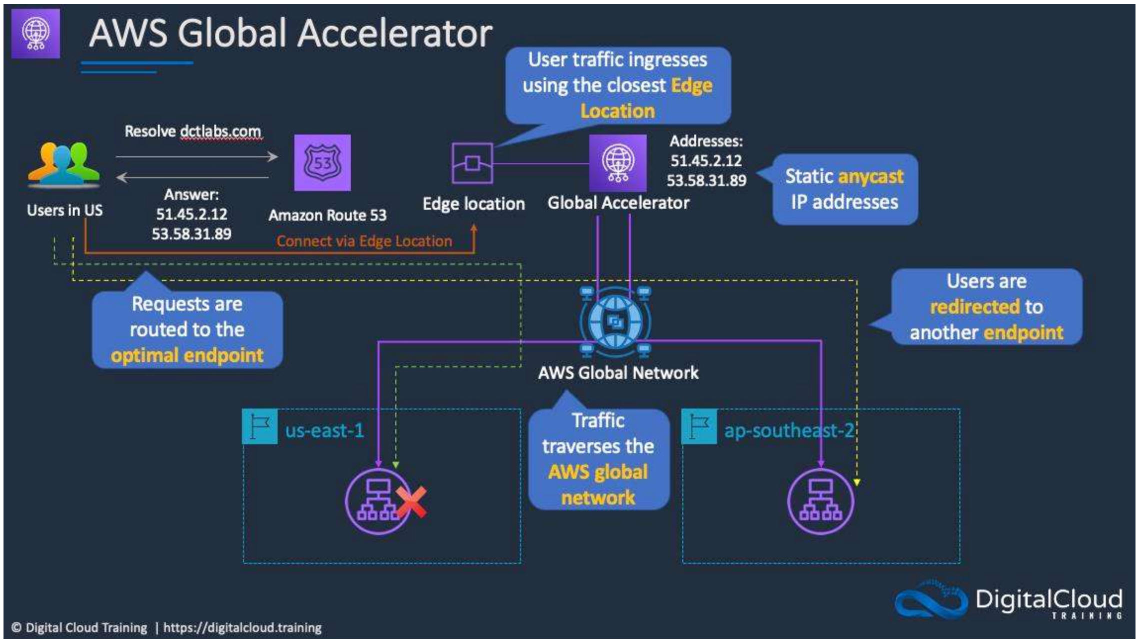
Correct answer

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.

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.

Overall 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.


AWS Global Accelerator
User traffic ingresses using the closest Edge Location
Resolve dctlabs.com
Answer: 51.45.2.12 53.58.31.89
Users in US
Amazon Route 53
Connect via Edge Location
Edge location
Global Accelerator
Addresses: 51.45.2.12 53.58.31.89
Static anycast IP addresses
Requests are routed to the optimal endpoint
AWS Global Network
Users are redirected to another endpoint
us-east-1
Traffic traverses the AWS global network
ap-southeast-2
DigitalCloud TRAINING
© Digital Cloud Training | https://digitalcloud.training

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/

Domain

AWS Networking & Content Delivery

Question 54Skipped

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?

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.

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.

Correct answer

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.

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

Overall 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/

Domain

AWS Application Integration

Question 55Skipped

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.

Correct answer

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.

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.

Overall 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/

Domain

AWS Analytics

Question 56Skipped

A company has an on-premises server that uses a MySQL database to process and store customer information. The company wants to migrate to an AWS database service to achieve higher availability and to improve application performance. Additionally, the company wants to offload reporting workloads from its primary database to ensure it remains performant.

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

Use AWS Database Migration Service (AWS DMS) to create an Amazon Aurora DB cluster in multiple AWS Regions. Point the reporting functions toward a separate DB instance from the primary DB instance.

Correct answer

Use Amazon Aurora with MySQL compatibility. Direct the reporting functions to use one of the Aurora Replicas.

Use Amazon EC2 instances to deploy a self-managed MySQL database with a replication setup for reporting purposes. Place instances in multiple availability zones and manage backups and patching manually.

Use Amazon RDS with MySQL in a Single-AZ deployment. Create a read replica in the same availability zone as the primary DB instance. Direct the reporting functions to the read replica.

Overall explanation

Amazon Aurora with MySQL compatibility is a good fit for achieving high availability and improved performance. Aurora automatically distributes the data across multiple AZs in a single region. Additionally, Aurora allows the creation of up to 15 Aurora Replicas that share the same underlying volume as the primary instance. Directing reporting functions to the Aurora Replica is an effective way to offload reporting workloads from the primary database.

CORRECT: "Use Amazon Aurora with MySQL compatibility. Direct the reporting functions to use one of the Aurora Replicas" is the correct answer (as explained above.)

INCORRECT: "Use Amazon RDS with MySQL in a Single-AZ deployment. Create a read replica in the same availability zone as the primary DB instance. Direct the reporting functions to the read replica" is incorrect.

Though you can use Amazon RDS with MySQL in a Single-AZ deployment and create a read replica, it is not the most operationally efficient option as it does not provide the high availability that Aurora's architecture offers.

INCORRECT: "Use AWS Database Migration Service (AWS DMS) to create an Amazon Aurora DB cluster in multiple AWS Regions. Point the reporting functions toward a separate DB instance from the primary DB instance" is incorrect.

Using AWS DMS to create Amazon Aurora DB clusters in multiple AWS Regions would be overkill for the requirements. It could also introduce additional complexity and doesn’t specifically address using a replica for reporting purposes.

INCORRECT: "Use Amazon EC2 instances to deploy a self-managed MySQL database with a replication setup for reporting purposes. Place instances in multiple availability zones and manage backups and patching manually" is incorrect.

Managing your own database on Amazon EC2 instances requires a significant operational overhead as you need to handle backups, patch management, and high availability yourself. This option is not the most operationally efficient compared to using a managed database service like Amazon Aurora.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Database

Question 57Skipped

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 private subnet and create a NAT gateway

Attach an internet gateway to the VPC but do not create a NAT gateway

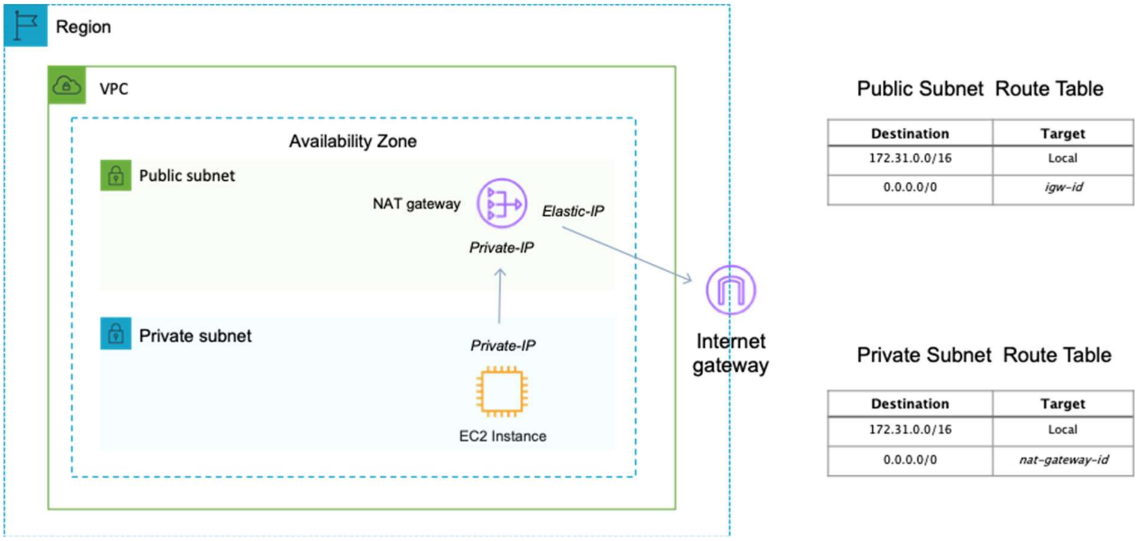
Create a NAT gateway but do not attach an internet gateway to the VPC

Correct answer

Create a NAT gateway and attach an internet gateway to the VPC

Overall 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.



Public Subnet Route Table

Destination	Target
172.31.0.0/16	Local
0.0.0.0/0	*igw-id*

Private Subnet Route Table

Destination	Target
172.31.0.0/16	Local
0.0.0.0/0	*nat-gateway-id*

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/

Domain

AWS Networking & Content Delivery

Question 58Skipped

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?

Correct answer

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.

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.

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.

Overall 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/

Domain

AWS Management & Governance

Question 59Skipped

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?

Correct answer

Use AWS Config to detect resources that are not properly tagged. Create a Systems Manager automation document for remediation.

Use Cost Explorer to display any application components that are not properly tagged. Tag those resources using a Python Script.

Write API calls to check all resources for proper tag allocation. Schedule an AWS Lambda function through Amazon CloudWatch to periodically run the code.

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.

Overall 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/

Domain

AWS Management & Governance

Question 60Skipped

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?

Correct answer

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

Purchase Reserved Instances that specify the Region.

Purchase Reserved Instances that specify the Region and two Availability Zones needed.

Create an On-Demand Capacity Reservation that specifies the Region.

Overall 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/

Domain

AWS Compute

Question 61Skipped

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?

Correct answer

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.

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.

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

Overall 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/

Domain

AWS Security, Identity, & Compliance

Question 62Skipped

An online education platform uses Amazon CloudFront to distribute learning resources globally. The company wants to ensure that only enrolled students have access to the course materials. These materials are stored in an Amazon S3 bucket. In addition, the company occasionally provides exclusive resources to certain students for research and project work.

Which solution will meet these requirements?

Utilize Amazon S3 object-level encryption for course materials.

Implement CloudFront Field-Level Encryption to block access to non-enrolled students.

Correct answer

Implement CloudFront signed cookies for authenticated students.

Create and provide S3 pre-signed URLs to authenticated students.

Overall explanation

CloudFront signed cookies are a method to control who can access your content. When a user authenticates and is verified as an enrolled student, the application can set a cookie in the student's browser. The cookie contains the same information that can be included in a signed URL but applies to multiple files in one or multiple directories.

CORRECT: "Implement CloudFront signed cookies for authenticated students" is the correct answer (as explained above.)

INCORRECT: "Create and provide S3 pre-signed URLs to authenticated students" is incorrect.

S3 pre-signed URLs are used to grant temporary access to a specific S3 object. This could be a valid option for individual file access but would be less efficient for multiple files or directories.

INCORRECT: "Utilize Amazon S3 object-level encryption for course materials" is incorrect.

Amazon S3 object-level encryption is mainly about securing data at rest, it won't control who can or cannot access the content.

INCORRECT: "Implement CloudFront Field-Level Encryption to block access to non-enrolled students" is incorrect.

CloudFront Field-Level Encryption handles sensitive information in HTTP POST requests to help prevent the information from being seen by unauthorized viewers. It's not designed to control access to content.

References:

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-cookies.html

Save time with our AWS cheat sheets:

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

Domain

AWS Networking & Content Delivery

Question 63Skipped

A multinational podcast company uses Amazon CloudFront for distributing its digital content. The company wants to gradually introduce content across various regions. It also needs to ensure that listeners who are outside the regions to which the content is currently released, cannot access the content.

Which solution will meet these requirements?

Encrypt the company's distributed content data and establish a custom error message.

Establish a new URL for the restricted content, control access with signed URLs and cookies, and set up a custom error message.

Correct answer

Implement geographical restrictions on CloudFront content using a deny list and create a custom error message.

Create a new URL for the restricted content and establish an expiration date-based access policy for signed URLs.

Overall explanation

By setting geographical restrictions on CloudFront content using a deny list, the company can block access to content for users outside of the released regions. If a user from a blocked region attempts to access the content, they would receive the custom error message, thereby meeting the company's requirements.

CORRECT: "Implement geographical restrictions on CloudFront content using a deny list and create a custom error message" is the correct answer (as explained above.)

INCORRECT: "Establish a new URL for the restricted content, control access with signed URLs and cookies, and set up a custom error message" is incorrect.

While signed URLs and cookies can be used to control access to content, they don't inherently consider the geographical location of the users, thus it would not guarantee that only users in the released regions could access the content.

INCORRECT: "Encrypt the company's distributed content data and establish a custom error message" is incorrect.

Although encrypting the content data adds a layer of security, it does not restrict access based on the geographical location of the users.

INCORRECT: "Create a new URL for the restricted content and establish an expiration date-based access policy for signed URLs" is incorrect.

Time-based access policies with signed URLs can limit access to the content after a certain time, but it does not restrict access based on the geographical location of the users.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Networking & Content Delivery

Question 64Skipped

A multinational enterprise plans to transition from numerous independent AWS accounts to a structured, multi-account AWS setup. The enterprise anticipates creating multiple AWS accounts to cater to various departments. The enterprise seeks to authenticate access to these AWS accounts using a centralized corporate directory service.

What combination of steps should a solutions architect suggest to meet these needs? (Select TWO.)

Install and configure AWS Control Tower for centralized account management. Incorporate AWS Identity Center to manage identity.

Correct selection

Create a new AWS Organizations entity with all features enabled. Create the new AWS accounts within the organization.

Establish an AWS Transit Gateway for centralized network management, linking AWS accounts.

Correct selection

Deploy AWS Directory Service and integrate it with the corporate directory service. Set up AWS Identity Center for authentication across accounts.

Set up an Amazon Cognito identity pool and configure AWS Identity Center to accept Amazon Cognito authentication.

Overall explanation

AWS Organizations provides policy-based management for multiple AWS accounts. With Organizations, you can create member accounts that are part of your organization and centrally manage your accounts.

AWS Directory Service allows you to connect your AWS resources with an existing on-premises Microsoft Active Directory or to set up a new, stand-alone directory in the AWS Cloud. AWS Identity Center makes it easy to centrally manage access to multiple AWS accounts and business applications and provide users with single sign-on access to all their assigned accounts and applications from one place.

CORRECT: "Create a new AWS Organizations entity with all features enabled. Create the new AWS accounts within the organization" is a correct answer (as explained above.)

CORRECT: "Deploy AWS Directory Service and integrate it with the corporate directory service. Set up AWS Identity Center for authentication across accounts" is also a correct answer (as explained above.)

INCORRECT: "Install and configure AWS Control Tower for centralized account management. Incorporate AWS Identity Center to manage identity" is incorrect.

AWS Control Tower does have certain benefits, but it doesn't directly cater to the company's need for centralized corporate directory service integration. However, it could be used in conjunction with AWS Identity Center for user access management.

INCORRECT: "Set up an Amazon Cognito identity pool and configure AWS Identity Center to accept Amazon Cognito authentication" is incorrect.

Amazon Cognito is primarily used to add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily. It isn't typically used in multi-account management scenarios and isn't directly relevant to the requirement for corporate directory service integration.

INCORRECT: "Establish an AWS Transit Gateway for centralized network management, linking AWS accounts" is incorrect.

AWS Transit Gateway connects VPCs and on-premises networks through a central hub. It is a network transit hub, not a user authentication and management service. It doesn't directly address the need for centralized corporate directory service integration.

References:

https://docs.aws.amazon.com/singlesignon/latest/userguide/manage-your-identity-source-ad.html

Save time with our AWS cheat sheets:

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

Domain

AWS Management & Governance

Question 65Skipped

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?

Correct answer

Use AWS Config to track configuration changes and AWS CloudTrail 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.

Use AWS Config to track configuration changes and Amazon EventBridge to record API calls and track access patterns in the AWS Cloud.

Use Amazon Macie to track configuration changes and Amazon CloudTrail to record API calls and track access patterns in the AWS Cloud.

Overall 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/

Domain

AWS Management & Governance