Question 1Skipped

A company hosts an application on Amazon EC2 instances behind Application Load Balancers in several AWS Regions. Distribution rights for the content require that users in different geographies must be served content from specific regions.

Which configuration meets these requirements?

Correct answer

Create Amazon Route 53 records with a geolocation routing policy.

Create Amazon Route 53 records with a geoproximity routing policy.

Configure Application Load Balancers with multi-Region routing.

Configure Amazon CloudFront with multiple origins and AWS WAF.

Overall explanation

To protect the distribution rights of the content and ensure that users are directed to the appropriate AWS Region based on the location of the user, the geolocation routing policy can be used with Amazon Route 53.

Geolocation routing lets you choose the resources that serve your traffic based on the geographic location of your users, meaning the location that DNS queries originate from.

When you use geolocation routing, you can localize your content and present some or all of your website in the language of your users. You can also use geolocation routing to restrict distribution of content to only the locations in which you have distribution rights.

CORRECT: "Create Amazon Route 53 records with a geolocation routing policy" is the correct answer.

INCORRECT: "Create Amazon Route 53 records with a geoproximity routing policy" is incorrect. Use this routing policy when you want to route traffic based on the location of your resources and, optionally, shift traffic from resources in one location to resources in another.

INCORRECT: "Configure Amazon CloudFront with multiple origins and AWS WAF" is incorrect. AWS WAF protects against web exploits but will not assist with directing users to different content (from different origins).

INCORRECT: "Configure Application Load Balancers with multi-Region routing" is incorrect. There is no such thing as multi-Region routing for ALBs.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Networking & Content Delivery

Question 2Skipped

A company is deploying a fleet of Amazon EC2 instances running Linux across multiple Availability Zones within an AWS Region. The application requires a data storage solution that can be accessed by all of the EC2 instances simultaneously. The solution must be highly scalable and easy to implement. The storage must be mounted using the NFS protocol.

Which solution meets these requirements?

Create an Amazon EBS volume and use EBS Multi-Attach to mount the volume to all EC2 instances across each Availability Zone.

Create an Amazon RDS database and store the data in a BLOB format. Point the application instances to the RDS endpoint.

Create an Amazon S3 bucket and create an S3 gateway endpoint to allow access to the file system using the NFS protocol.

Correct answer

Create an Amazon EFS file system with mount targets in each Availability Zone. Configure the application instances to mount the file system.

Overall explanation

Amazon EFS provides scalable file storage for use with Amazon EC2. You can use an EFS file system as a common data source for workloads and applications running on multiple instances. The EC2 instances can run in multiple AZs within a Region and the NFS protocol is used to mount the file system.

With EFS you can create mount targets in each AZ for lower latency. The application instances in each AZ will mount the file system using the local mount target.

CORRECT: "Create an Amazon EFS file system with mount targets in each Availability Zone. Configure the application instances to mount the file system" is the correct answer.

INCORRECT: "Create an Amazon S3 bucket and create an S3 gateway endpoint to allow access to the file system using the NFS protocol" is incorrect. You cannot use NFS with S3 or with gateway endpoints.

INCORRECT: "Create an Amazon EBS volume and use EBS Multi-Attach to mount the volume to all EC2 instances across each Availability Zone" is incorrect. You cannot use Amazon EBS Multi-Attach across multiple AZs.

INCORRECT: "Create an Amazon RDS database and store the data in a BLOB format. Point the application instances to the RDS endpoint" is incorrect. This is not a suitable storage solution for a file system that is mounted over NFS.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 3Skipped

A website runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB) which serves as an origin for an Amazon CloudFront distribution. An AWS WAF is being used to protect against SQL injection attacks. A review of security logs revealed an external malicious IP that needs to be blocked from accessing the website.

What should a solutions architect do to protect the application?

Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address

Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address

Correct answer

Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address

Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.

Overall explanation

A new version of the AWS Web Application Firewall was released in November 2019. With AWS WAF classic you create “IP match conditions”, whereas with AWS WAF (new version) you create “IP set match statements”. Look out for wording on the exam.

The IP match condition / IP set match statement inspects the IP address of a web request's origin against a set of IP addresses and address ranges. Use this to allow or block web requests based on the IP addresses that the requests originate from.

AWS WAF supports all IPv4 and IPv6 address ranges. An IP set can hold up to 10,000 IP addresses or IP address ranges to check.

CORRECT: "Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address" is the correct answer.

INCORRECT: "Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address" is incorrect as CloudFront does not sit within a subnet so network ACLs do not apply to it.

INCORRECT: "Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address" is incorrect as the source IP addresses of the data in the EC2 instances’ subnets will be the ELB IP addresses.

INCORRECT: "Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address." is incorrect as you cannot create deny rules with security groups.

References:

https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-ipset-match.html

Save time with our AWS cheat sheets:

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

Domain

AWS Security, Identity, & Compliance

Question 4Skipped

A company runs containerized applications for many application workloads in an on-premise data center. The company is planning to deploy containers to AWS and the chief architect has mandated that the same configuration and administrative tools must be used across all containerized environments. The company also wishes to remain cloud agnostic to safeguard against the impact of future changes in cloud strategy.

How can a Solutions Architect design a managed solution that will align with open-source software?

Launch the containers on Amazon Elastic Container Service (ECS) with Amazon EC2 instance worker nodes.

Correct answer

Launch the containers on Amazon Elastic Kubernetes Service (EKS) and EKS worker nodes.

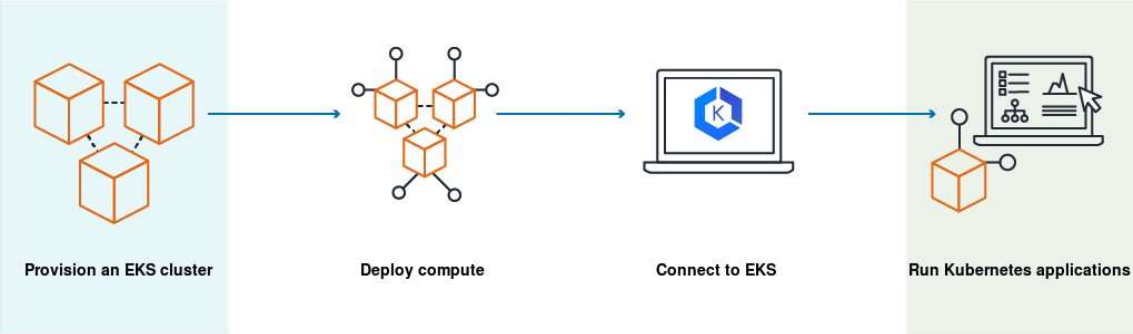
Launch the containers on Amazon Elastic Container Service (ECS) with AWS Fargate instances.

Launch the containers on a fleet of Amazon EC2 instances in a cluster placement group.

Overall explanation

Amazon EKS is a managed service that can be used to run Kubernetes on AWS. Kubernetes is an open-source system for automating the deployment, scaling, and management of containerized applications. Applications running on Amazon EKS are fully compatible with applications running on any standard Kubernetes environment, whether running in on-premises data centers or public clouds. This means that you can easily migrate any standard Kubernetes application to Amazon EKS without any code modification.

This solution ensures that the same open-source software is used for automating the deployment, scaling, and management of containerized applications both on-premises and in the AWS Cloud.



CORRECT: "Launch the containers on Amazon Elastic Kubernetes Service (EKS) and EKS worker nodes" is the correct answer.

INCORRECT: "Launch the containers on a fleet of Amazon EC2 instances in a cluster placement group" is incorrect

INCORRECT: "Launch the containers on Amazon Elastic Container Service (ECS) with AWS Fargate instances" is incorrect

INCORRECT: "Launch the containers on Amazon Elastic Container Service (ECS) with Amazon EC2 instance worker nodes" is incorrect

References:

https://docs.aws.amazon.com/eks/latest/userguide/what-is-eks.html

Save time with our AWS cheat sheets:

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

Domain

AWS Compute

Question 5Skipped

A company is working with a strategic partner that has an application that must be able to send messages to one of the company's Amazon SQS queues. The partner company has its own AWS account.

How can a Solutions Architect provide least privilege access to the partner?

Correct answer

Update the permission policy on the SQS queue to grant the sqs:SendMessage permission to the partner's AWS account.

Create a user account and grant the sqs:SendMessage permission for Amazon SQS. Share the credentials with the partner company.

Update the permission policy on the SQS queue to grant all permissions to the partner's AWS account.

Create a cross-account role with access to all SQS queues and use the partner's AWS account in the trust document for the role.

Overall explanation

Amazon SQS supports resource-based policies. The best way to grant the permissions using the principle of least privilege is to use a resource-based policy attached to the SQS queue that grants the partner company's AWS account the sqs:SendMessage privilege.

The following policy is an example of how this could be configured:

```
{
  "Version": "2012-10-17",
  "Id": "Queue1_Policy_UUID",
  "Statement": [{
    "Sid":"Queue1_SendMessage",
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "111122223333"
      ]
    },
    "Action": "sqs:SendMessage",
    "Resource": "arn:aws:sqs:us-east-2:444455556666:queue1"
  }]
}
```

CORRECT: "Update the permission policy on the SQS queue to grant the sqs:SendMessage permission to the partner's AWS account" is the correct answer.

INCORRECT: "Create a user account that and grant the sqs:SendMessage permission for Amazon SQS. Share the credentials with the partner company" is incorrect. This would provide the permissions for all SQS queues, not just the queue the partner company should be able to access.

INCORRECT: "Create a cross-account role with access to all SQS queues and use the partner's AWS account in the trust document for the role" is incorrect. This would provide access to all SQS queues and the partner company should only be able to access one SQS queue.

INCORRECT: "Update the permission policy on the SQS queue to grant all permissions to the partner's AWS account" is incorrect. This provides too many permissions; the partner company only needs to send messages to the queue.

References:

https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-basic-examples-of-sqs-policies.html

Save time with our AWS cheat sheets:

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

Domain

AWS Application Integration

Question 6Skipped

A Solutions Architect has been tasked with re-deploying an application running on AWS to enable high availability. The application processes messages that are received in an ActiveMQ queue running on a single Amazon EC2 instance. Messages are then processed by a consumer application running on Amazon EC2. After processing the messages the consumer application writes results to a MySQL database running on Amazon EC2.

Which architecture offers the highest availability and low operational complexity?

Deploy Amazon MQ with active/standby brokers configured across two Availability Zones. Launch an additional consumer EC2 instance in another Availability Zone. Use MySQL database replication to another Availability Zone.

Deploy Amazon MQ with active/standby brokers configured across two Availability Zones. Launch an additional consumer EC2 instance in another Availability Zone. Use Amazon RDS for MySQL with Multi-AZ enabled.

Correct answer

Deploy Amazon MQ with active/standby brokers configured across two Availability Zones. Create an Auto Scaling group for the consumer EC2 instances across two Availability Zones. Use an Amazon RDS MySQL database with Multi-AZ enabled.

Deploy a second Active MQ server to another Availability Zone. Launch an additional consumer EC2 instance in another Availability Zone. Use MySQL database replication to another Availability Zone.

Overall explanation

The correct answer offers the highest availability as it includes Amazon MQ active/standby brokers across two AZs, an Auto Scaling group across two AZ,s and a Multi-AZ Amazon RDS MySQL database deployment.

This architecture not only offers the highest availability it is also operationally simple as it maximizes the usage of managed services.

CORRECT: "Deploy Amazon MQ with active/standby brokers configured across two Availability Zones. Create an Auto Scaling group for the consumer EC2 instances across two Availability Zones. Use an Amazon RDS MySQL database with Multi-AZ enabled" is the correct answer.

INCORRECT: "Deploy a second Active MQ server to another Availability Zone. Launch an additional consumer EC2 instance in another Availability Zone. Use MySQL database replication to another Availability Zone" is incorrect. This architecture does not offer the highest availability as it does not use Auto Scaling. It is also not the most operationally efficient architecture as it does not use AWS managed services.

INCORRECT: "Deploy Amazon MQ with active/standby brokers configured across two Availability Zones. Launch an additional consumer EC2 instance in another Availability Zone. Use MySQL database replication to another Availability Zone" is incorrect. This architecture does not use Auto Scaling for best HA or the RDS managed service.

INCORRECT: "Deploy Amazon MQ with active/standby brokers configured across two Availability Zones. Launch an additional consumer EC2 instance in another Availability Zone. Use Amazon RDS for MySQL with Multi-AZ enabled" is incorrect. This solution does not use Auto Scaling.

References:

https://aws.amazon.com/architecture/well-architected/

Save time with our AWS cheat sheets:

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

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

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

Domain

AWS Application Integration

Question 7Skipped

A company is migrating from an on-premises infrastructure to the AWS Cloud. One of the company's applications stores files on a Windows file server farm that uses Distributed File System Replication (DFSR) to keep data in sync. A solutions architect needs to replace the file server farm.

Which service should the solutions architect use?

Amazon S3

Correct answer

Amazon FSx

Amazon EFS

AWS Storage Gateway

Overall explanation

Amazon FSx for Windows File Server provides fully managed, highly reliable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol.

Amazon FSx is built on Windows Server and provides a rich set of administrative features that include end-user file restore, user quotas, and Access Control Lists (ACLs).

Additionally, Amazon FSX for Windows File Server supports Distributed File System Replication (DFSR) in Single-AZ deployments as can be seen in the feature comparison table below.

Deployment type	SSD storage	HDD storage	DFS namespaces	DFS replication	Custom DNS name	CA shares
Single-AZ 1	✓		✓	✓	✓	
Single-AZ 2	✓	✓	✓		Coming soon	✓*
Multi-AZ	✓	✓	✓		Coming soon	✓*

CORRECT: "Amazon FSx" is the correct answer.

INCORRECT: "Amazon EFS" is incorrect as EFS only supports Linux systems.

INCORRECT: "Amazon S3" is incorrect as this is not a suitable replacement for a Microsoft filesystem.

INCORRECT: "AWS Storage Gateway" is incorrect as this service is primarily used for connecting on-premises storage to cloud storage. It consists of a software device installed on-premises and can be used with SMB shares but it actually stores the data on S3. It is also used for migration. However, in this case the company need to replace the file server farm and Amazon FSx is the best choice for this job.

References:

https://docs.aws.amazon.com/fsx/latest/WindowsGuide/high-availability-multiAZ.html

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 8Skipped

A company offers an online product brochure that is delivered from a static website running on Amazon S3. The company's customers are mainly in the United States, Canada, and Mexico. The company is looking to cost-effectively reduce the latency for users in these regions.

What is the most cost-effective solution to these requirements?

Create an Amazon CloudFront distribution and set the price class to use all Edge Locations for best performance.

Create an Amazon CloudFront distribution and use Lambda@Edge to run the website's data processing closer to the users.

Correct answer

Create an Amazon CloudFront distribution and set the price class to use only U.S, Canada and Mexico.

Create an Amazon CloudFront distribution that uses origins in U.S, Canada and Mexico.

Overall explanation

With Amazon CloudFront you can set the price class to determine where in the world the content will be cached. One of the price classes is "U.S, Canada and Mexico" and this is where the company's users are located. Choosing this price class will result in lower costs and better performance for the company's users.

CORRECT: "Create an Amazon CloudFront distribution and set the price class to use only U.S, Canada and Mexico." is the correct answer.

INCORRECT: "Create an Amazon CloudFront distribution and set the price class to use all Edge Locations for best performance" is incorrect. This will be more expensive as it will cache content in Edge Locations all over the world.

INCORRECT: "Create an Amazon CloudFront distribution that uses origins in U.S, Canada and Mexico" is incorrect. The origin can be in one place, there's no need to add origins in different Regions. The price class should be used to limit the caching of the content to reduce cost.

INCORRECT: "Create an Amazon CloudFront distribution and use Lambda@Edge to run the website's data processing closer to the users" is incorrect. Lambda@Edge will not assist in this situation as there is no data processing required, the content from the static website must simply be cached at an edge location.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Networking & Content Delivery

Question 9Skipped

There are two applications in a company: a sender application that sends messages containing payloads, and a processing application that receives messages containing payloads. The company wants to implement an AWS service to handle messages between these two different applications. The sender application sends on average 1,000 messages each hour and the messages depending on the type sometimes take up to 2 days to be processed. If the messages fail to process, they must be retained so that they do not impact the processing of any remaining messages.

Which solution meets these requirements and is the MOST operationally efficient?

Correct answer

Provide an Amazon Simple Queue Service (Amazon SQS) queue for the sender and processor applications. Set up a dead-letter queue to collect failed messages.

Receive the messages from the sender application using an Amazon Kinesis data stream. Utilize the Kinesis Client Library (KCL) to integrate the processing application.

Subscribe the processing application to an Amazon Simple Notification Service (Amazon SNS) topic to receive notifications. Write to the SNS topic using the sender application.

Set up a Redis database on Amazon EC2. Configure the instance to be used by both applications. The messages should be stored, processed, and deleted, respectively.

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.

SQS eliminates the complexity and overhead associated with managing and operating message-oriented middleware and empowers developers to focus on differentiating work.

CORRECT: "Provide an Amazon Simple Queue Service (Amazon SQS) queue for the sender and processor applications. Set up a dead-letter queue to collect failed messages" is the correct answer (as explained above.)

INCORRECT: "Set up a Redis database on Amazon EC2. Configure the instance to be used by both applications. The messages should be stored, processed, and deleted, respectively" is incorrect, as the most operationally efficient way is to use the managed service Amazon SQS.

INCORRECT: "Receive the messages from the sender application using an Amazon Kinesis data stream. Utilize the Kinesis Client Library (KCL) to integrate the processing application" is incorrect, as the most operationally efficient way is to use the managed service Amazon SQS

INCORRECT: "Subscribe the processing application to an Amazon Simple Notification Service (Amazon SNS) topic to receive notifications. Write to the SNS topic using the sender application" is incorrect as Amazon SNS is not a queuing service, but a pub-sub one to many notification service and cannot be used as a queue.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Application Integration

Question 10Skipped

An application running on Amazon EC2 needs to asynchronously invoke an AWS Lambda function to perform data processing. The services should be decoupled.

Which service can be used to decouple the compute services?

Amazon MQ

Correct answer

Amazon SNS

AWS Config

AWS Step Functions

Overall explanation

You can use a Lambda function to process Amazon Simple Notification Service notifications. Amazon SNS supports Lambda functions as a target for messages sent to a topic. This solution decouples the Amazon EC2 application from Lambda and ensures the Lambda function is invoked.

CORRECT: "Amazon SNS" is the correct answer.

INCORRECT: "AWS Config" is incorrect. AWS Config is a service that is used for continuous compliance, not application decoupling.

INCORRECT: "Amazon MQ" is incorrect. Amazon MQ is similar to SQS but is used for existing applications that are being migrated into AWS. SQS should be used for new applications being created in the cloud.

INCORRECT: "AWS Step Functions" is incorrect. AWS Step Functions is a workflow service. It is not the best solution for this scenario.

References:

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

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

Save time with our AWS cheat sheets:

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

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

Domain

AWS Application Integration

Question 11Skipped

A video production company is planning to move some of its workloads to the AWS Cloud. The company will require around 5 TB of storage for video processing with the maximum possible I/O performance. They also require over 400 TB of extremely durable storage for storing video files and 800 TB of storage for long-term archival.

Which combinations of services should a Solutions Architect use to meet these requirements?

Amazon EBS for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage.

Correct answer

Amazon EC2 instance store for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage.

Amazon EBS for maximum performance, Amazon EFS for durable data storage, and Amazon S3 Glacier for archival storage.

Amazon EC2 instance store for maximum performance, Amazon EFS for durable data storage, and Amazon S3 for archival storage.

Overall explanation

The best I/O performance can be achieved by using instance store volumes for the video processing. This is safe to use for use cases where the data can be recreated from the source files so this is a good use case.

For storing data durably Amazon S3 is a good fit as it provides 99.999999999% of durability. For archival the video files can then be moved to Amazon S3 Glacier which is a low cost storage option that is ideal for long-term archival.

CORRECT: "Amazon EC2 instance store for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage" is the correct answer.

INCORRECT: "Amazon EBS for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage" is incorrect. EBS is not going to provide as much I/O performance as an instance store volume so is not the best choice for this use case.

INCORRECT: "Amazon EC2 instance store for maximum performance, Amazon EFS for durable data storage, and Amazon S3 for archival storage" is incorrect. EFS does not provide as much durability as Amazon S3 and will not be as cost-effective.

INCORRECT: "Amazon EBS for maximum performance, Amazon EFS for durable data storage, and Amazon S3 Glacier for archival storage" is incorrect. EBS and EFS are not the best choices here as described above.

References:

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

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

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 12Skipped

A solutions architect needs to backup some application log files from an online ecommerce store to Amazon S3. It is unknown how often the logs will be accessed or which logs will be accessed the most. The solutions architect must keep costs as low as possible by using the appropriate S3 storage class.

Which S3 storage class should be implemented to meet these requirements?

S3 One Zone-Infrequent Access (S3 One Zone-IA)

S3 Glacier

S3 Standard-Infrequent Access (S3 Standard-IA)

Correct answer

S3 Intelligent-Tiering

Overall explanation

The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead.

It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. This is an ideal use case for intelligent-tiering as the access patterns for the log files are not known.

CORRECT: "S3 Intelligent-Tiering" is the correct answer.

INCORRECT: "S3 Standard-Infrequent Access (S3 Standard-IA)" is incorrect as if the data is accessed often retrieval fees could become expensive.

INCORRECT: "S3 One Zone-Infrequent Access (S3 One Zone-IA)" is incorrect as if the data is accessed often retrieval fees could become expensive.

INCORRECT: "S3 Glacier" is incorrect as if the data is accessed often retrieval fees could become expensive. Glacier also requires more work in retrieving the data from the archive and quick access requirements can add further costs.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 13Skipped

A company's web application is using multiple Amazon EC2 Linux instances and storing data on Amazon EBS volumes. The company is looking for a solution to increase the resiliency of the application in case of a failure.

What should a solutions architect do to meet these requirements?

Correct answer

Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data on Amazon EFS and mount a target on each instance

Launch the application on EC2 instances in each Availability Zone. Attach EBS volumes to each EC2 instance

Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data using Amazon S3 One Zone-Infrequent Access (S3 One Zone-A)

Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Mount an instance store on each EC2 instance

Overall explanation

To increase the resiliency of the application the solutions architect can use Auto Scaling groups to launch and terminate instances across multiple availability zones based on demand. An application load balancer (ALB) can be used to direct traffic to the web application running on the EC2 instances.

Lastly, the Amazon Elastic File System (EFS) can assist with increasing the resilience of the application by providing a shared file system that can be mounted by multiple EC2 instances from multiple availability zones.

CORRECT: "Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data on Amazon EFS and mount a target on each instance" is the correct answer.

INCORRECT: "Launch the application on EC2 instances in each Availability Zone. Attach EBS volumes to each EC2 instance" is incorrect as the EBS volumes are single points of failure which are not shared with other instances.

INCORRECT: "Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Mount an instance store on each EC2 instance" is incorrect as instance stores are ephemeral data stores which means data is lost when powered down. Also, instance stores cannot be shared between instances.

INCORRECT: "Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data using Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)" is incorrect as there are data retrieval charges associated with this S3 tier. It is not a suitable storage tier for application files.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 14Skipped

An Amazon VPC contains several Amazon EC2 instances. The instances need to make API calls to Amazon DynamoDB. A solutions architect needs to ensure that the API calls do not traverse the internet.

How can this be accomplished? (Select TWO.)

Create a new DynamoDB table that uses the endpoint

Correct selection

Create a gateway endpoint for DynamoDB

Create a VPC peering connection between the VPC and DynamoDB

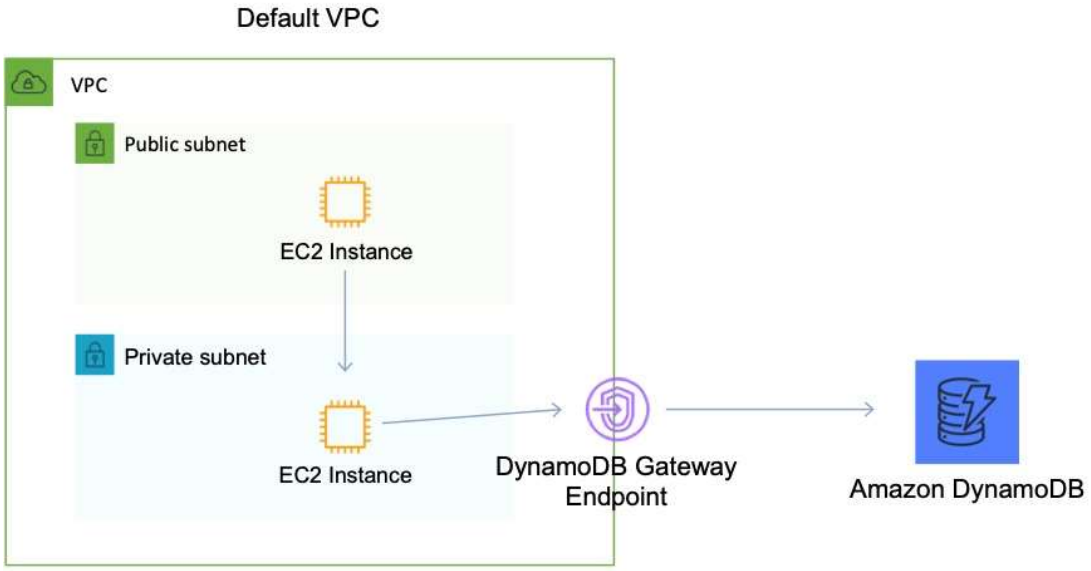
Correct selection

Create a route table entry for the endpoint

Create an ENI for the endpoint in each of the subnets of the VPC

Overall explanation

Amazon DynamoDB and Amazon S3 support gateway endpoints, not interface endpoints. With a gateway endpoint you create the endpoint in the VPC, attach a policy allowing access to the service, and then specify the route table to create a route table entry in.



Route Table

Destination	Target
pl-6ca54005 (com.amazonaws.ap-southeast-2.s3, 54.231.248.0/22, 54.231.252.0/24, 52.95.128.0/21)	*vpce-ID*

CORRECT: "Create a route table entry for the endpoint" is a correct answer.

CORRECT: "Create a gateway endpoint for DynamoDB" is also a correct answer.

INCORRECT: "Create a new DynamoDB table that uses the endpoint" is incorrect as it is not necessary to create a new DynamoDB table.

INCORRECT: "Create an ENI for the endpoint in each of the subnets of the VPC" is incorrect as an ENI is used by an interface endpoint, not a gateway endpoint.

INCORRECT: "Create a VPC peering connection between the VPC and DynamoDB" is incorrect as you cannot create a VPC peering connection between a VPC and a public AWS service as public services are outside of VPCs.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Networking & Content Delivery

Question 15Skipped

A company is investigating methods to reduce the expenses associated with on-premises backup infrastructure. The Solutions Architect wants to reduce costs by eliminating the use of physical backup tapes. It is a requirement that existing backup applications and workflows should continue to function.

What should the Solutions Architect recommend?

Connect the backup applications to an AWS Storage Gateway using the iSCSI protocol.

Correct answer

Connect the backup applications to an AWS Storage Gateway using an iSCSI-virtual tape library (VTL).

Create an Amazon EFS file system and connect the backup applications using the NFS protocol.

Create an Amazon EFS file system and connect the backup applications using the iSCSI protocol.

Overall explanation

The AWS Storage Gateway Tape Gateway enables you to replace using physical tapes on premises with virtual tapes in AWS without changing existing backup workflows. Tape Gateway emulates physical tape libraries, removes the cost and complexity of managing physical tape infrastructure, and provides more durability than physical tapes.

CORRECT: "Connect the backup applications to an AWS Storage Gateway using an iSCSI-virtual tape library (VTL)" is the correct answer.

INCORRECT: "Create an Amazon EFS file system and connect the backup applications using the NFS protocol" is incorrect. The NFS protocol is used by AWS Storage Gateway File Gateways but these do not provide virtual tape functionality that is suitable for replacing the existing backup infrastructure.

INCORRECT: "Create an Amazon EFS file system and connect the backup applications using the iSCSI protocol" is incorrect. The NFS protocol is used by AWS Storage Gateway File Gateways but these do not provide virtual tape functionality that is suitable for replacing the existing backup infrastructure.

INCORRECT: "Connect the backup applications to an AWS Storage Gateway using the NFS protocol" is incorrect. The iSCSI protocol is used by AWS Storage Gateway Volume Gateways but these do not provide virtual tape functionality that is suitable for replacing the existing backup infrastructure.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 16Skipped

An Amazon S3 bucket in the us-east-1 Region hosts the static website content of a company. The content is made available through an Amazon CloudFront origin pointing to that bucket. A second copy of the bucket is created in the ap-southeast-1 Region using cross-region replication. The chief solutions architect wants a solution that provides greater availability for the website.

Which combination of actions should a solutions architect take to increase availability? (Select TWO.)

Correct selection

Add an origin for ap-southeast-1 to CloudFront.

Set up failover routing in Amazon Route 53.

Create an origin for CloudFront for both buckets.

Point Amazon Route 53 to the replica bucket by creating a record.

Correct selection

Using us-east-1 bucket as the primary bucket and ap-southeast-1 bucket as the secondary bucket, create a CloudFront origin group.

Overall explanation

You can set up CloudFront with origin failover for scenarios that require high availability. To get started, you create an *origin group* with two origins: a primary and a secondary. If the primary origin is unavailable or returns specific HTTP response status codes that indicate a failure, CloudFront automatically switches to the secondary origin.

CORRECT: "Add an origin for ap-southeast-1 to CloudFront" is the correct answer (as explained above.)

CORRECT: "Using us-east-1 bucket as the primary bucket and ap-southeast-1 bucket as the secondary bucket, create a CloudFront origin group" is also a correct answer (as explained above.)

INCORRECT: "Create an origin for CloudFront for both buckets" is incorrect. This would not increase the availability of the solution on its own.

INCORRECT: "Set up failover routing in Amazon Route 53" is incorrect as we are trying to enable failover in CloudFront and using Route 53 is for routing domain names.

INCORRECT: "Create a record in Amazon Route 53 pointing to the replica bucket" is incorrect as we are trying to enable failover in CloudFront and using Route 53 is for routing domain names.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Networking & Content Delivery

Question 17Skipped

A company runs an application in an on-premises data center that collects environmental data from production machinery. The data consists of JSON files stored on network attached storage (NAS) and around 5 TB of data is collected each day. The company must upload this data to Amazon S3 where it can be processed by an analytics application. The data must be transferred securely.

Which solution offers the MOST reliable and time-efficient data transfer?

Correct answer

AWS DataSync over AWS Direct Connect.

AWS Database Migration Service over the Internet.

Multiple AWS Snowcone devices.

Amazon S3 Transfer Acceleration over the Internet.

Overall explanation

The most reliable and time-efficient solution that keeps the data secure is to use AWS DataSync and synchronize the data from the NAS device directly to Amazon S3. This should take place over an AWS Direct Connect connection to ensure reliability, speed, and security.

AWS DataSync can copy data between Network File System (NFS) shares, Server Message Block (SMB) shares, self-managed object storage, AWS Snowcone, Amazon Simple Storage Service (Amazon S3) buckets, Amazon Elastic File System (Amazon EFS) file systems, and Amazon FSx for Windows File Server file systems.

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

INCORRECT: "AWS Database Migration Service over the Internet" is incorrect. DMS is for migrating databases, not files.

INCORRECT: "Amazon S3 Transfer Acceleration over the Internet" is incorrect. The Internet does not offer the reliability, speed or performance that this company requires.

INCORRECT: "Multiple AWS Snowcone devices" is incorrect. This is not a time-efficient approach as it can take time to ship these devices in both directions.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Migration & Transfer

Question 18Skipped

A company runs an application that uses an Amazon RDS PostgreSQL database. The database is currently not encrypted. A Solutions Architect has been instructed that due to new compliance requirements all existing and new data in the database must be encrypted. The database experiences high volumes of changes and no data can be lost.

How can the Solutions Architect enable encryption for the database without incurring any data loss?

Create an RDS read replica and specify an encryption key. Promote the encrypted read replica to primary. Update the application to point to the new RDS DB endpoint.

Correct answer

Create a snapshot of the existing RDS DB instance. Create an encrypted copy of the snapshot. Create a new RDS DB instance from the encrypted snapshot and update the application. Use AWS DMS to synchronize data between the source and destination RDS DBs.

Create a snapshot of the existing RDS DB instance. Create an encrypted copy of the snapshot. Create a new RDS DB instance from the encrypted snapshot. Configure the application to use the new DB endpoint.

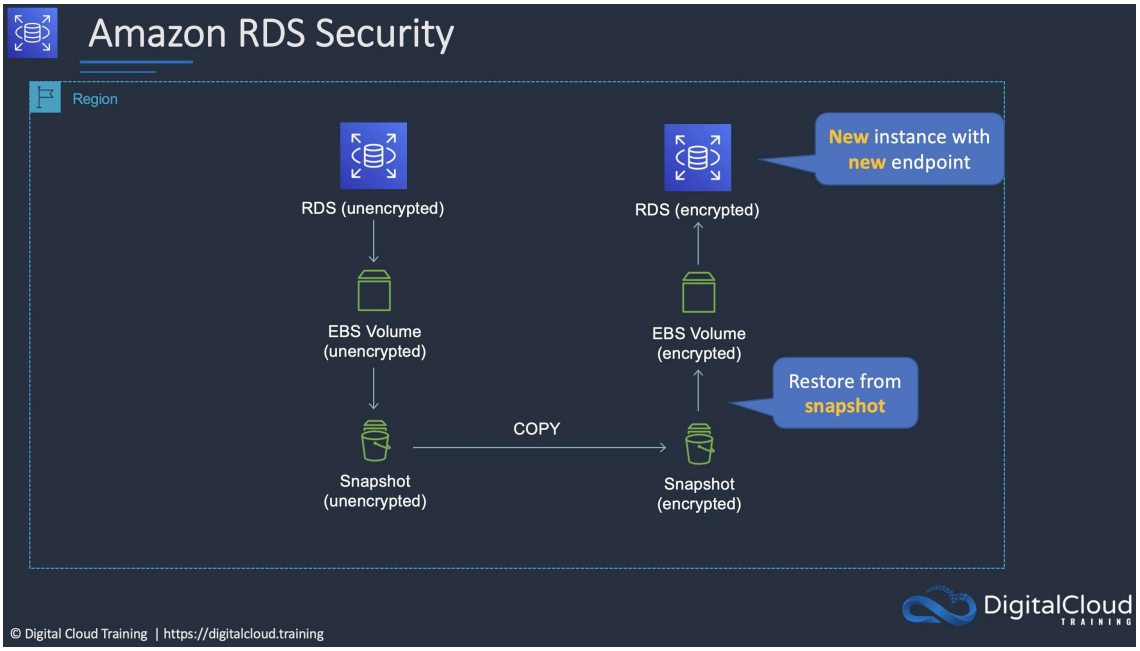
Update the RDS DB to Multi-AZ mode and enable encryption for the standby replica. Perform a failover to the standby instance and then delete the unencrypted RDS DB instance.

Overall explanation

You cannot change the encryption status of an existing RDS DB instance. Encryption must be specified when creating the RDS DB instance. The best way to encrypt an existing database is to take a snapshot, encrypt a copy of the snapshot and restore the snapshot to a new RDS DB instance. This results in an encrypted database that is a new instance. Applications must be updated to use the new RDS DB endpoint.

In this scenario as there is a high rate of change, the databases will be out of sync by the time the new copy is created and is functional. The best way to capture the changes between the source (unencrypted) and destination (encrypted) DB is to use AWS Database Migration Service (DMS) to synchronize the data.

The slide below depicts the process for encrypting an unencrypted RDS DB instance:



CORRECT: "Create a snapshot of the existing RDS DB instance. Create an encrypted copy of the snapshot. Create a new RDS DB instance from the encrypted snapshot and update the application. Use AWS DMS to synchronize data between the source and destination RDS DBs" is the correct answer.

INCORRECT: "Create a snapshot of the existing RDS DB instance. Create an encrypted copy of the snapshot. Create a new RDS DB instance from the encrypted snapshot. Configure the application to use the new DB endpoint" is incorrect. This answer creates an encrypted DB instance but does not synchronize the data.

INCORRECT: "Create an RDS read replica and specify an encryption key. Promote the encrypted read replica to primary. Update the application to point to the new RDS DB endpoint" is incorrect. You cannot create an encrypted read replica of an unencrypted RDS DB. The read replica will always have the same encryption status as the RDS DB it is created from.

INCORRECT: "Update the RDS DB to Multi-AZ mode and enable encryption for the standby replica. Perform a failover to the standby instance and then delete the unencrypted RDS DB instance" is incorrect. You also cannot have an encrypted Multi-AZ standby instance of an unencrypted RDS DB.

References:

https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/encrypt-an-existing-amazon-rds-for-postgresql-db-instance.html

Save time with our AWS cheat sheets:

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

Domain

AWS Database

Question 19Skipped

A new application will run across multiple Amazon ECS tasks. Front-end application logic will process data and then pass that data to a back-end ECS task to perform further processing and write the data to a datastore. The Architect would like to reduce-interdependencies so failures do no impact other components.

Which solution should the Architect use?

Create an Amazon Kinesis Firehose delivery stream that delivers data to an Amazon S3 bucket, configure the front-end to write data to the stream and the back-end to read data from Amazon S3

Create an Amazon SQS queue that pushes messages to the back-end. Configure the front-end to add messages to the queue

Correct answer

Create an Amazon SQS queue and configure the front-end to add messages to the queue and the back-end to poll the queue for messages

Create an Amazon Kinesis Firehose delivery stream and configure the front-end to add data to the stream and the back-end to read data from the stream

Overall explanation

This is a good use case for Amazon SQS. SQS is a service that is used for decoupling applications, thus reducing interdependencies, through a message bus. The front-end application can place messages on the queue and the back-end can then poll the queue for new messages. Please remember that Amazon SQS is pull-based (polling) not push-based (use SNS for push-based).

CORRECT: "Create an Amazon SQS queue and configure the front-end to add messages to the queue and the back-end to poll the queue for messages" is the correct answer.

INCORRECT: "Create an Amazon Kinesis Firehose delivery stream and configure the front-end to add data to the stream and the back-end to read data from the stream" is incorrect. Amazon Kinesis Firehose is used for streaming data. With Firehose the data is immediately loaded into a destination that can be Amazon S3, RedShift, Elasticsearch, or Splunk. This is not an ideal use case for Firehose as this is not streaming data and there is no need to load data into an additional AWS service.

INCORRECT: "Create an Amazon Kinesis Firehose delivery stream that delivers data to an Amazon S3 bucket, configure the front-end to write data to the stream and the back-end to read data from Amazon S3" is incorrect as per the previous explanation.

INCORRECT: "Create an Amazon SQS queue that pushes messages to the back-end. Configure the front-end to add messages to the queue " is incorrect as SQS is pull-based, not push-based. EC2 instances must poll the queue to find jobs to process.

References:

https://docs.aws.amazon.com/AmazonECS/latest/developerguide/common_use_cases.html

Save time with our AWS cheat sheets:

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

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

Domain

AWS Application Integration

Question 20Skipped

A solutions architect is creating a system that will run analytics on financial data for several hours a night, 5 days a week. The analysis is expected to run for the same duration and cannot be interrupted once it is started. The system will be required for a minimum of 1 year.

What should the solutions architect configure to ensure the EC2 instances are available when they are needed?

Savings Plans

On-Demand Instances

Correct answer

On-Demand Capacity Reservations

Regional Reserved Instances

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. This gives you the ability to create and manage Capacity Reservations independently from the billing discounts offered by Savings Plans or Regional Reserved Instances.

By creating Capacity Reservations, you ensure that you always have access to EC2 capacity when you need it, for as long as you need it. You can create Capacity Reservations at any time, without entering a one-year or three-year term commitment, and the capacity is available immediately.

The table below shows the difference between capacity reservations and other options:

	Capacity Reservations	Zonal Reserved Instances	Regional Reserved Instances	Savings Plans
Term	No commitment required. Can be created and canceled as needed.	Requires a fixed one-year or three-year commitment		
Capacity benefit	Capacity reserved in a specific Availability Zone.		No capacity reserved.	
Billing discount	No billing discount. †	Provides a billing discount.		
Instance Limits	Your On-Demand Instance limits per Region apply.	Default is 20 per Availability Zone. You can request a limit increase.	Default is 20 per Region. You can request a limit increase.	No limit.

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

INCORRECT: "Regional Reserved Instances" is incorrect. This type of reservation does not reserve capacity.

INCORRECT: "On-Demand Instances" is incorrect. This does not provide any kind of capacity reservation.

INCORRECT: "Savings Plans" is incorrect. This pricing option does not provide a capacity reservation.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html

Save time with our AWS cheat sheets:

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

Domain

AWS Compute

Question 21Skipped

A company needs to connect its on-premises data center network to a new virtual private cloud (VPC). There is a symmetrical internet connection of 100 Mbps in the data center network. The data transfer rate for an on-premises application is multiple gigabytes per day. Processing will be done using an Amazon Kinesis Data Firehose stream.

What should a solutions architect recommend for maximum performance?

Establish a peering connection between the on-premises network and the VPC. Configure routing for the on-premises network to use the VPC peering connection.

Establish an AWS Site-to-Site VPN connection between the on-premises network and the VPC. Set up BGP routing between the customer gateway and the virtual private gateway. Send data to Kinesis Data Firehose using a VPN connection.

Correct answer

Kinesis Data Firehose can be connected to the VPC using AWS PrivateLink. Install a 1 Gbps AWS Direct Connect connection between the on-premises network and AWS. To send data from on-premises to Kinesis Data Firehose, use the PrivateLink endpoint.

Get an AWS Snowball Edge Storage Optimized device. Data must be copied to the device after several days and shipped to AWS for expedited transfer to Kinesis Data Firehose. Repeat as necessary.

Overall explanation

Explanation:

Using AWS PrivateLink to create an interface endpoint will allow your traffic to traverse the AWS Global Backbone to allow maximum performance and security. Also by using an AWS Direct Connect cable you can ensure you have a dedicated cable to provide maximum performance and low latency to and from AWS.

CORRECT: "Kinesis Data Firehose can be connected to the VPC using AWS PrivateLink. Install a 1 Gbps AWS Direct Connect connection between the on-premises network and AWS. To send data from on-premises to Kinesis Data Firehose, use the PrivateLink endpoint" is the correct answer (as explained above.)

INCORRECT: "Establish a peering connection between the on-premises network and the VPC. Configure routing for the on-premises network to use the VPC peering connection" is incorrect also because VPC peering connections can only exist between two VPCs within the AWS Cloud.

INCORRECT: "Get an AWS Snowball Edge Storage Optimized device. Data must be copied to the device after several days and shipped to AWS for expedited transfer to Kinesis Data Firehose. Repeat as necessary" is incorrect. AWS Snowball Edge is designed to be more of a one-time migration service which you physically receive from AWS, and then ship it into an AWS Region of your choice.

INCORRECT: "Establish an AWS Site-to-Site VPN connection between the on-premises network and the VPC. Set up BGP routing between the customer gateway and the virtual private gateway. Send data to Kinesis Data Firehose using a VPN connection" is incorrect. This is a functional solution; however a physical connection would provide a much more reliable and performant solution.

References:

https://aws.amazon.com/privatelink/

Save time with our AWS cheat sheets:

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

Domain

AWS Networking & Content Delivery

Question 22Skipped

An Amazon RDS Read Replica is being deployed in a separate region. The master database is not encrypted but all data in the new region must be encrypted. How can this be achieved?

Enable encryption using Key Management Service (KMS) when creating the cross-region Read Replica

Encrypt a snapshot from the master DB instance, create an encrypted cross-region Read Replica from the snapshot

Correct answer

Encrypt a snapshot from the master DB instance, create a new encrypted master DB instance, and then create an encrypted cross-region Read Replica

Enable encryption on the master DB instance, then create an encrypted cross-region Read Replica

Overall explanation

You cannot create an encrypted Read Replica from an unencrypted master DB instance. You also cannot enable encryption after launch time for the master DB instance. Therefore, you must create a new master DB by taking a snapshot of the existing DB, encrypting it, and then creating the new DB from the snapshot. You can then create the encrypted cross-region Read Replica of the master DB.

CORRECT: "Encrypt a snapshot from the master DB instance, create a new encrypted master DB instance, and then create an encrypted cross-region Read Replica" is the correct answer.

INCORRECT: "Enable encryption using Key Management Service (KMS) when creating the cross-region Read Replica" is incorrect. All other options will not work due to the limitations explained above.

INCORRECT: "Encrypt a snapshot from the master DB instance, create an encrypted cross-region Read Replica from the snapshot" is incorrect. All other options will not work due to the limitations explained above.

INCORRECT: "Enabled encryption on the master DB instance, then create an encrypted cross-region Read Replica" is incorrect. All other options will not work due to the limitations explained above.

References:

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

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

Save time with our AWS cheat sheets:

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

Domain

AWS Database

Question 23Skipped

A web application allows users to upload photos and add graphical elements to them. The application offers two tiers of service: free and paid. Photos uploaded by paid users should be processed before those submitted using the free tier. The photos are uploaded to an Amazon S3 bucket which uses an event notification to send the job information to Amazon SQS.

How should a Solutions Architect configure the Amazon SQS deployment to meet these requirements?

Use one SQS standard queue. Use batching for the paid photos and short polling for the free photos.

Correct answer

Use a separate SQS Standard queue for each tier. Configure Amazon EC2 instances to prioritize polling for the paid queue over the free queue.

Use one SQS FIFO queue. Assign a higher priority to the paid photos so they are processed first.

Use a separate SQS FIFO queue for each tier. Set the free queue to use short polling and the paid queue to use long polling.

Overall explanation

AWS recommend using separate queues when you need to provide prioritization of work. The logic can then be implemented at the application layer to prioritize the queue for the paid photos over the queue for the free photos.

CORRECT: "Use a separate SQS Standard queue for each tier. Configure Amazon EC2 instances to prioritize polling for the paid queue over the free queue" is the correct answer.

INCORRECT: "Use one SQS FIFO queue. Assign a higher priority to the paid photos so they are processed first" is incorrect. FIFO queues preserve the order of messages but they do not prioritize messages within the queue. The orders would need to be placed into the queue in a priority order and there's no way of doing this as the messages are sent automatically through event notifications as they are received by Amazon S3.

INCORRECT: "Use one SQS standard queue. Use batching for the paid photos and short polling for the free photos" is incorrect. Batching adds efficiency but it has nothing to do with ordering or priority.

INCORRECT: "Use a separate SQS FIFO queue for each tier. Set the free queue to use short polling and the paid queue to use long polling" is incorrect. Short polling and long polling are used to control the amount of time the consumer process waits before closing the API call and trying again. Polling should be configured for efficiency of API calls and processing of messages but does not help with message prioritization.

References:

https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-how-it-works.html

Save time with our AWS cheat sheets:

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

Domain

AWS Application Integration

Question 24Skipped

A company uses an Amazon RDS MySQL database instance to store customer order data. The security team have requested that SSL/TLS encryption in transit must be used for encrypting connections to the database from application servers. The data in the database is currently encrypted at rest using an AWS KMS key.

How can a Solutions Architect enable encryption in transit?

Correct answer

Download the AWS-provided root certificates. Use the certificates when connecting to the RDS DB instance.

Enable encryption in transit using the RDS Management console and obtain a key using AWS KMS.

Add a self-signed certificate to the RDS DB instance. Use the certificates in all connections to the RDS DB instance.

Take a snapshot of the RDS instance. Restore the snapshot to a new instance with encryption in transit enabled.

Overall explanation

Amazon RDS creates an SSL certificate and installs the certificate on the DB instance when Amazon RDS provisions the instance. These certificates are signed by a certificate authority. The SSL certificate includes the DB instance endpoint as the Common Name (CN) for the SSL certificate to guard against spoofing attacks.

You can download a root certificate from AWS that works for all Regions or you can download Region-specific intermediate certificates.

CORRECT: "Download the AWS-provided root certificates. Use the certificates when connecting to the RDS DB instance" is the correct answer.

INCORRECT: "Take a snapshot of the RDS instance. Restore the snapshot to a new instance with encryption in transit enabled" is incorrect. There is no need to do this as a certificate is created when the DB instances is launched.

INCORRECT: "Enable encryption in transit using the RDS Management console and obtain a key using AWS KMS" is incorrect. You cannot enable/disable encryption in transit using the RDS management console or use a KMS key.

INCORRECT: "Add a self-signed certificate to the RDS DB instance. Use the certificates in all connections to the RDS DB instance" is incorrect. You cannot use self-signed certificates with RDS.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Database

Question 25Skipped

A company runs an application on six web application servers in an Amazon EC2 Auto Scaling group in a single Availability Zone. The application is fronted by an Application Load Balancer (ALB). A Solutions Architect needs to modify the infrastructure to be highly available without making any modifications to the application.

Which architecture should the Solutions Architect choose to enable high availability?

Correct answer

Modify the Auto Scaling group to use two instances across each of three Availability Zones.

Create a launch template that can be used to quickly create more instances in another Region.

Create an Auto Scaling group to launch three instances across each of two Regions.

Create an Amazon CloudFront distribution with a custom origin across multiple Regions.

Overall explanation

The only thing that needs to be changed in this scenario to enable HA is to split the instances across multiple Availability Zones. The architecture already uses Auto Scaling and Elastic Load Balancing so there is plenty of resilience to failure. Once the instances are running across multiple AZs there will be AZ-level fault tolerance as well.

CORRECT: "Modify the Auto Scaling group to use two instances across each of three Availability Zones" is the correct answer.

INCORRECT: "Create an Amazon CloudFront distribution with a custom origin across multiple Regions" is incorrect. CloudFront is not used to create HA for your application, it is used to accelerate access to media content.

INCORRECT: "Create a launch template that can be used to quickly create more instances in another Region" is incorrect. Multi-AZ should be enabled rather than multi-Region.

INCORRECT: "Create an Auto Scaling group to launch three instances across each of two Regions" is incorrect. HA can be achieved within a Region by simply enabling more AZs in the ASG. An ASG cannot launch instances in multiple Regions.

References:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-add-availability-zone.html

Save time with our AWS cheat sheets:

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

Domain

AWS Compute

Question 26Skipped

A solutions architect is designing the infrastructure to run an application on Amazon EC2 instances. The application requires high availability and must dynamically scale based on demand to be cost efficient.

What should the solutions architect do to meet these requirements?

Configure an Amazon API Gateway API in front of an Auto Scaling group to deploy instances to multiple Availability Zones

Configure an Application Load Balancer in front of an Auto Scaling group to deploy instances to multiple Regions

Correct answer

Configure an Application Load Balancer in front of an Auto Scaling group to deploy instances to multiple Availability Zones

Configure an Amazon CloudFront distribution in front of an Auto Scaling group to deploy instances to multiple Regions

Overall explanation

The Amazon EC2-based application must be highly available and elastically scalable. Auto Scaling can provide the elasticity by dynamically launching and terminating instances based on demand. This can take place across availability zones for high availability.

Incoming connections can be distributed to the instances by using an Application Load Balancer (ALB).

CORRECT: "Configure an Application Load Balancer in front of an Auto Scaling group to deploy instances to multiple Availability Zones" is the correct answer.

INCORRECT: "Configure an Amazon API Gateway API in front of an Auto Scaling group to deploy instances to multiple Availability Zones" is incorrect as API gateway is not used for load balancing connections to Amazon EC2 instances.

INCORRECT: "Configure an Application Load Balancer in front of an Auto Scaling group to deploy instances to multiple Regions" is incorrect as you cannot launch instances in multiple Regions from a single Auto Scaling group.

INCORRECT: "Configure an Amazon CloudFront distribution in front of an Auto Scaling group to deploy instances to multiple Regions" is incorrect as you cannot launch instances in multiple Regions from a single Auto Scaling group.

References:

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

https://aws.amazon.com/elasticloadbalancing/

Save time with our AWS cheat sheets:

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

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

Domain

AWS Compute

Question 27Skipped

A Solutions Architect has deployed an application on several Amazon EC2 instances across three private subnets. The application must be made accessible to internet-based clients with the least amount of administrative effort.

How can the Solutions Architect make the application available on the internet?

Correct answer

Create an Application Load Balancer and associate three public subnets from the same Availability Zones as the private instances. Add the private instances to the ALB.

Create an Application Load Balancer and associate three private subnets from the same Availability Zones as the private instances. Add the private instances to the ALB.

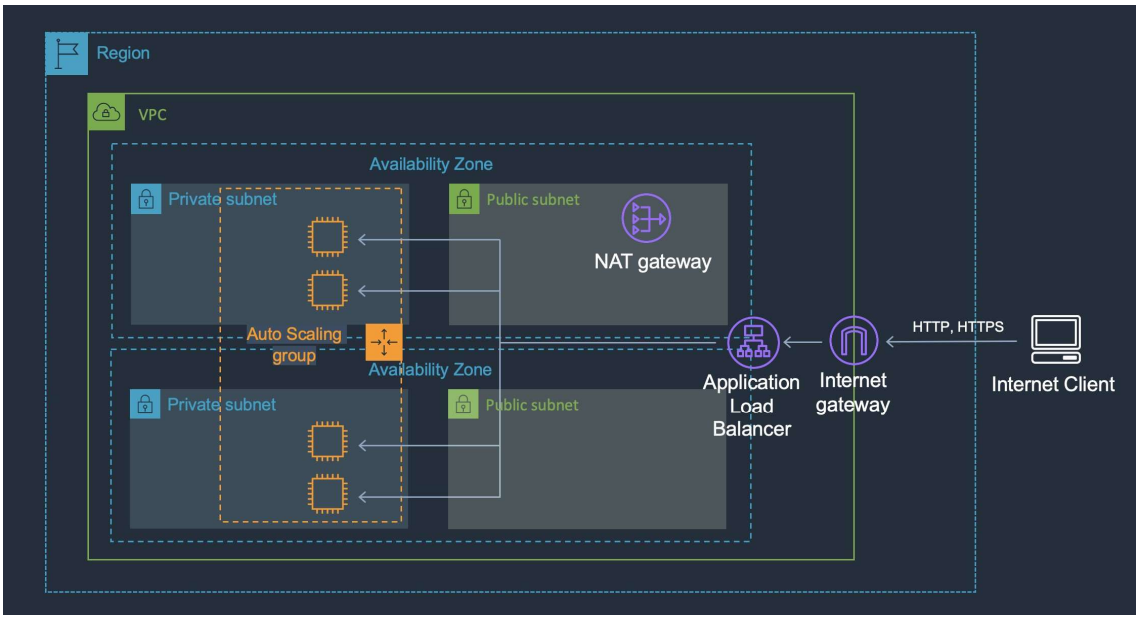
Create a NAT gateway in a public subnet. Add a route to the NAT gateway to the route tables of the three private subnets.

Create an Amazon Machine Image (AMI) of the instances in the private subnet and launch new instances from the AMI in public subnets. Create an Application Load Balancer and add the public instances to the ALB.

Overall explanation

To make the application instances accessible on the internet the Solutions Architect needs to place them behind an internet-facing Elastic Load Balancer. The way you add instances in private subnets to a public facing ELB is to add public subnets in the same AZs as the private subnets to the ELB. You can then add the instances and to the ELB and they will become targets for load balancing.

An example of this architecture is shown below:



CORRECT: "Create an Application Load Balancer and associate three public subnets from the same Availability Zones as the private instances. Add the private instances to the ALB" is the correct answer.

INCORRECT: "Create an Application Load Balancer and associate three private subnets from the same Availability Zones as the private instances. Add the private instances to the ALB" is incorrect. Public subnets in the same AZs as the private subnets must be added to make this configuration work.

INCORRECT: "Create an Amazon Machine Image (AMI) of the instances in the private subnet and launch new instances from the AMI in public subnets. Create an Application Load Balancer and add the public instances to the ALB" is incorrect. There is no need to use an AMI to create new instances in a public subnet. You can add instances in private subnets to a public-facing ELB.

INCORRECT: "Create a NAT gateway in a public subnet. Add a route to the NAT gateway to the route tables of the three private subnets" is incorrect. A NAT gateway is used for outbound traffic not inbound traffic and cannot make the application available to internet-based clients.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Compute

Question 28Skipped

A solutions architect is creating a document submission application for a school. The application will use an Amazon S3 bucket for storage. The solution must prevent accidental deletion of the documents and ensure that all versions of the documents are available. Users must be able to upload and modify the documents.

Which combination of actions should be taken to meet these requirements? (Select TWO.)

Set read-only permissions on the bucket

Attach an IAM policy to the bucket

Correct selection

Enable MFA Delete on the bucket

Correct selection

Enable versioning on the bucket

Encrypt the bucket using AWS SSE-S3

Overall explanation

None of the options present a good solution for specifying permissions required to write and modify objects so that requirement needs to be taken care of separately. The other requirements are to prevent accidental deletion and the ensure that all versions of the document are available.

The two solutions for these requirements are versioning and MFA delete. Versioning will retain a copy of each version of the document and multi-factor authentication delete (MFA delete) will prevent any accidental deletion as you need to supply a second factor when attempting a delete.

CORRECT: "Enable versioning on the bucket" is a correct answer.

CORRECT: "Enable MFA Delete on the bucket" is also a correct answer.

INCORRECT: "Set read-only permissions on the bucket" is incorrect as this will also prevent any writing to the bucket which is not desired.

INCORRECT: "Attach an IAM policy to the bucket" is incorrect as users need to modify documents which will also allow delete. Therefore, a method must be implemented to just control deletes.

INCORRECT: "Encrypt the bucket using AWS SSE-S3" is incorrect as encryption doesn't stop you from deleting an object.**References:**

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

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

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 29Skipped

An AWS Organization has an OU with multiple member accounts in it. The company needs to restrict the ability to launch only specific Amazon EC2 instance types. How can this policy be applied across the accounts with the least effort?

Correct answer

Create an SCP with a deny rule that denies all but the specific instance types

Create an SCP with an allow rule that allows launching the specific instance types

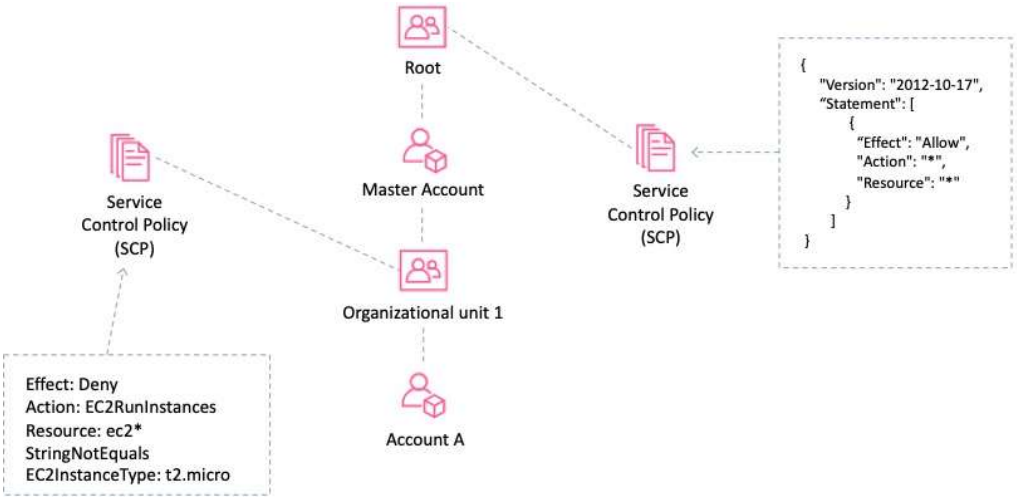
Use AWS Resource Access Manager to control which launch types can be used

Create an IAM policy to deny launching all but the specific instance types

Overall explanation

To apply the restrictions across multiple member accounts you must use a Service Control Policy (SCP) in the AWS Organization. The way you would do this is to create a deny rule that applies to anything that does not equal the specific instance type you want to allow.

The following architecture could be used to achieve this goal:



CORRECT: "Create an SCP with a deny rule that denies all but the specific instance types" is the correct answer.

INCORRECT: "Create an SCP with an allow rule that allows launching the specific instance types" is incorrect as a deny rule is required.

INCORRECT: "Create an IAM policy to deny launching all but the specific instance types" is incorrect. With IAM you need to apply the policy within each account rather than centrally so this would require much more effort.

INCORRECT: "Use AWS Resource Access Manager to control which launch types can be used" is incorrect. AWS Resource Access Manager (RAM) is a service that enables you to easily and securely share AWS resources with any AWS account or within your AWS Organization. It is not used for restricting access or permissions.

References:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_example-scps.html#example-ec2-instances

Save time with our AWS cheat sheets:

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

Domain

AWS Management & Governance

Question 30Skipped

A legacy tightly-coupled High Performance Computing (HPC) application will be migrated to AWS. Which network adapter type should be used?

Elastic IP Address

Elastic Network Adapter (ENA)

Elastic Network Interface (ENI)

Correct answer

Elastic Fabric Adapter (EFA)

Overall explanation

An Elastic Fabric Adapter is an AWS Elastic Network Adapter (ENA) with added capabilities. The EFA lets you apply the scale, flexibility, and elasticity of the AWS Cloud to tightly-coupled HPC apps. It is ideal for tightly coupled app as it uses the Message Passing Interface (MPI).

CORRECT: "Elastic Fabric Adapter (EFA)" is the correct answer.

INCORRECT: "Elastic Network Interface (ENI)" is incorrect. The ENI is a basic type of adapter and is not the best choice for this use case.

INCORRECT: "Elastic Network Adapter (ENA)" is incorrect. The ENA, which provides Enhanced Networking, does provide high bandwidth and low inter-instance latency but it does not support the features for a tightly-coupled app that the EFA does.

INCORRECT: "Elastic IP Address" is incorrect. An Elastic IP address is just a static public IP address, it is not a type of network adapter.

References:

https://aws.amazon.com/blogs/aws/now-available-elastic-fabric-adapter-efa-for-tightly-coupled-hpc-workloads/

Save time with our AWS cheat sheets:

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

Domain

AWS Compute

Question 31Skipped

A company runs a large batch processing job at the end of every quarter. The processing job runs for 5 days and uses 15 Amazon EC2 instances. The processing must run uninterrupted for 5 hours per day. The company is investigating ways to reduce the cost of the batch processing job.

Which pricing model should the company choose?

Reserved Instances

Spot Instances

Correct answer

On-Demand Instances

Dedicated Instances

Overall explanation

Each EC2 instance runs for 5 hours a day for 5 days per quarter or 20 days per year. This is time duration is insufficient to warrant reserved instances as these require a commitment of a minimum of 1 year and the discounts would not outweigh the costs of having the reservations unused for a large percentage of time. In this case, there are no options presented that can reduce the cost and therefore on-demand instances should be used.

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

INCORRECT: "Reserved Instances" is incorrect. Reserved instances are good for continuously running workloads that run for a period of 1 or 3 years.

INCORRECT: "Spot Instances" is incorrect. Spot instances may be interrupted and this is not acceptable. Note that Spot Block is deprecated and unavailable to new customers.

INCORRECT: "Dedicated Instances" is incorrect. These do not provide any cost advantages and will be more expensive.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Compute

Question 32Skipped

A developer created an application that uses Amazon EC2 and an Amazon RDS MySQL database instance. The developer stored the database user name and password in a configuration file on the root EBS volume of the EC2 application instance. A Solutions Architect has been asked to design a more secure solution.

What should the Solutions Architect do to achieve this requirement?

Correct answer

Create an IAM role with permission to access the database. Attach this IAM role to the EC2 instance.

Attach an additional volume to the EC2 instance with encryption enabled. Move the configuration file to the encrypted volume.

Install an Amazon-trusted root certificate on the application instance and use SSL/TLS encrypted connections to the database.

Move the configuration file to an Amazon S3 bucket. Create an IAM role with permission to the bucket and attach it to the EC2 instance.

Overall explanation

The key problem here is having plain text credentials stored in a file. Even if you encrypt the volume there is still as security risk as the credentials are loaded by the application and passed to RDS.

The best way to secure this solution is to get rid of the credentials completely by using an IAM role instead. The IAM role can be assigned permissions to the database instance and can be attached to the EC2 instance. The instance will then obtain temporary security credentials from AWS STS which is much more secure.

CORRECT: "Create an IAM role with permission to access the database. Attach this IAM role to the EC2 instance" is the correct answer.

INCORRECT: "Move the configuration file to an Amazon S3 bucket. Create an IAM role with permission to the bucket and attach it to the EC2 instance" is incorrect. This just relocates the file; the contents are still unsecured and must be loaded by the application and passed to RDS. This is an insecure process.

INCORRECT: "Attach an additional volume to the EC2 instance with encryption enabled. Move the configuration file to the encrypted volume" is incorrect. This will only encrypt the file at rest, it still must be read, and the contents passed to RDS which is insecure.

INCORRECT: "Install an Amazon-trusted root certificate on the application instance and use SSL/TLS encrypted connections to the database" is incorrect. The file is still unsecured on the EBS volume so encrypting the credentials in an encrypted channel between the EC2 instance and RDS does not solve all security issues.

References:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html

Save time with our AWS cheat sheets:

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

Domain

AWS Security, Identity, & Compliance

Question 33Skipped

A persistent database must be migrated from an on-premises server to an Amazon EC2 instances. The database requires 64,000 IOPS and, if possible, should be stored on a single Amazon EBS volume.

Which solution should a Solutions Architect recommend?

Use an instance from the I3 I/O optimized family and leverage instance store storage to achieve the IOPS requirement.

Create an Amazon EC2 instance with four Amazon EBS General Purpose SSD (gp2) volumes attached. Max out the IOPS on each volume and use a RAID 0 stripe set.

Correct answer

Create a Nitro-based Amazon EC2 instance with an Amazon EBS Provisioned IOPS SSD (i01) volume attached. Provision 64,000 IOPS for the volume.

Create an Amazon EC2 instance with two Amazon EBS Provisioned IOPS SSD (i01) volumes attached. Provision 32,000 IOPS per volume and create a logical volume using the OS that aggregates the capacity.

Overall explanation

Amazon EC2 Nitro-based systems are not required for this solution but do offer advantages in performance that will help to maximize the usage of the EBS volume. For the data storage volume an i01 volume can support up to 64,000 IOPS so a single volume with sufficient capacity (50 IOPS per GiB) can be deliver the requirements.

The current list of EBS volume types is in the table below:

	General Purpose SSD		Provisioned IOPS SSD		
Volume type	gp3	gp2	io2 Block Express ‡	io2	io1
Durability	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)	99.999% durability (0.001% annual failure rate)		99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)
Use cases	• Low-latency interactive apps • Development and test environments		Workloads that require sub-millisecond latency, and sustained IOPS performance or more than 64,000 IOPS or 1,000 MiB/s of throughput	• Workloads that require sustained IOPS performance or more than 16,000 IOPS • I/O-intensive database workloads	
Volume size	1 GiB - 16 TiB		4 GiB - 64 TiB	4 GiB - 16 TiB	
Max IOPS per volume (16 KiB I/O)	16,000		256,000	64,000 †	
Max throughput per volume	1,000 MiB/s	250 MiB/s *	4,000 MiB/s	1,000 MiB/s †	
Amazon EBS Multi-attach	Not supported		Not supported	Supported	
Boot volume	Supported				

CORRECT: "Create a Nitro-based Amazon EC2 instance with an Amazon EBS Provisioned IOPS SSD (i01) volume attached. Provision 64,000 IOPS for the volume" is the correct answer.

INCORRECT: "Use an instance from the I3 I/O optimized family and leverage instance store storage to achieve the IOPS requirement" is incorrect.

INCORRECT: "Create an Amazon EC2 instance with four Amazon EBS General Purpose SSD (gp2) volumes attached. Max out the IOPS on each volume and use a RAID 0 stripe set" is incorrect. This is not a good use case for gp2 volumes. It is much better to use io1 which also meets the requirement of having a single volume with 64,000 IOPS.

INCORRECT: "Create an Amazon EC2 instance with two Amazon EBS Provisioned IOPS SSD (i01) volumes attached. Provision 32,000 IOPS per volume and create a logical volume using the OS that aggregates the capacity" is incorrect. There is no need to create two volumes and aggregate capacity through the OS, the Solutions Architect can simply create a single volume with 64,000 IOPS.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Compute

Question 34Skipped

A company has deployed a new website on Amazon EC2 instances behind an Application Load Balancer (ALB). Amazon Route 53 is used for the DNS service. The company has asked a Solutions Architect to create a backup website with support contact details that users will be directed to automatically if the primary website is down.

How should the Solutions Architect deploy this solution cost-effectively?

Correct answer

Configure a static website using Amazon S3 and create a Route 53 failover routing policy.

Create the backup website on EC2 and ALB in another Region and create an AWS Global Accelerator endpoint.

Deploy the backup website on EC2 and ALB in another Region and use Route 53 health checks for failover routing.

Configure a static website using Amazon S3 and create a Route 53 weighted routing policy.

Overall explanation

The most cost-effective solution is to create a static website using an Amazon S3 bucket and then use a failover routing policy in Amazon Route 53. With a failover routing policy users will be directed to the main website as long as it is responding to health checks successfully.

If the main website fails to respond to health checks (its down), Route 53 will begin to direct users to the backup website running on the Amazon S3 bucket. It's important to set the TTL on the Route 53 records appropriately to ensure that users resolve the failover address within a short time.

CORRECT: "Configure a static website using Amazon S3 and create a Route 53 failover routing policy" is the correct answer.

INCORRECT: "Configure a static website using Amazon S3 and create a Route 53 weighted routing policy" is incorrect. Weighted routing is used when you want to send a percentage of traffic between multiple endpoints. In this case all traffic should go to the primary until if fails, then all should go to the backup.

INCORRECT: "Deploy the backup website on EC2 and ALB in another Region and use Route 53 health checks for failover routing" is incorrect. This is not a cost-effective solution for the backup website. It can be implemented using Route 53 failover routing which uses health checks but would be an expensive option.

INCORRECT: "Create the backup website on EC2 and ALB in another Region and create an AWS Global Accelerator endpoint" is incorrect. Global Accelerator is used for performance as it directs traffic to the nearest healthy endpoint. It is not useful for failover in this scenario and is also a very expensive solution.

References:

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

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

Save time with our AWS cheat sheets:

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

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

Domain

AWS Networking & Content Delivery

Question 35Skipped

A company has uploaded some highly critical data to an Amazon S3 bucket. Management are concerned about data availability and require that steps are taken to protect the data from accidental deletion. The data should still be accessible, and a user should be able to delete the data intentionally.

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

Enable default encryption on the S3 bucket.

Correct selection

Enable versioning on the S3 bucket.

Create a bucket policy on the S3 bucket.

Correct selection

Enable MFA Delete on the S3 bucket.

Create a lifecycle policy for the objects in the S3 bucket.

Overall explanation

Multi-factor authentication (MFA) delete adds an additional step before an object can be deleted from a versioning-enabled bucket.

With MFA delete the bucket owner must include the x-amz-mfa request header in requests to permanently delete an object version or change the versioning state of the bucket.

CORRECT: "Enable versioning on the S3 bucket" is a correct answer.

CORRECT: "Enable MFA Delete on the S3 bucket" is also a correct answer.

INCORRECT: "Create a bucket policy on the S3 bucket" is incorrect. A bucket policy is not required to enable MFA delete.

INCORRECT: "Enable default encryption on the S3 bucket" is incorrect. Encryption does not protect against deletion.

INCORRECT: "Create a lifecycle policy for the objects in the S3 bucket" is incorrect. A lifecycle policy will move data to another storage class but does not protect against deletion.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 36Skipped

A solutions architect is designing a new service that will use an Amazon API Gateway API on the frontend. The service will need to persist data in a backend database using key-value requests. Initially, the data requirements will be around 1 GB and future growth is unknown. Requests can range from 0 to over 800 requests per second.

Which combination of AWS services would meet these requirements? (Select TWO.)

Amazon EC2 Auto Scaling

Correct selection

AWS Lambda

Correct selection

Amazon DynamoDB

AWS Fargate

Amazon RDS

Overall explanation

In this case AWS Lambda can perform the computation and store the data in an Amazon DynamoDB table. Lambda can scale concurrent executions to meet demand easily and DynamoDB is built for key-value data storage requirements and is also serverless and easily scalable. This is therefore a cost effective solution for unpredictable workloads.

CORRECT: "AWS Lambda" is a correct answer.

CORRECT: "Amazon DynamoDB" is also a correct answer.

INCORRECT: "AWS Fargate" is incorrect as containers run constantly and therefore incur costs even when no requests are being made.

INCORRECT: "Amazon EC2 Auto Scaling" is incorrect as this uses EC2 instances which will incur costs even when no requests are being made.

INCORRECT: "Amazon RDS" is incorrect as this is a relational database not a No-SQL database. It is therefore not suitable for key-value data storage requirements.

References:

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

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

Save time with our AWS cheat sheets:

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

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

Domain

AWS Database

Question 37Skipped

A company plans to make an Amazon EC2 Linux instance unavailable outside of business hours to save costs. The instance is backed by an Amazon EBS volume. There is a requirement that the contents of the instance's memory must be preserved when it is made unavailable.

How can a solutions architect meet these requirements?

Stop the instance outside business hours. Start the instance again when required.

Use Auto Scaling to scale down the instance outside of business hours. Scale up the instance when required.

Correct answer

Hibernate the instance outside business hours. Start the instance again when required.

Terminate the instance outside business hours. Recover the instance again when required.

Overall explanation

When you hibernate an instance, Amazon EC2 signals the operating system to perform hibernation (suspend-to-disk). Hibernation saves the contents from the instance memory (RAM) to your Amazon Elastic Block Store (Amazon EBS) root volume. Amazon EC2 persists the instance's EBS root volume and any attached EBS data volumes. When you start your instance:

- The EBS root volume is restored to its previous state

- The RAM contents are reloaded

- The processes that were previously running on the instance are resumed

- Previously attached data volumes are reattached and the instance retains its instance ID

CORRECT: "Hibernate the instance outside business hours. Start the instance again when required" is the correct answer.

INCORRECT: "Stop the instance outside business hours. Start the instance again when required" is incorrect. When an instance is stopped the operating system is shut down and the contents of memory will be lost.

INCORRECT: "Use Auto Scaling to scale down the instance outside of business hours. Scale out the instance when required" is incorrect. Auto Scaling scales does not scale up and down, it scales in by terminating instances and out by launching instances. When scaling out new instances are launched and no state will be available from terminated instances.

INCORRECT: "Terminate the instance outside business hours. Recover the instance again when required" is incorrect. You cannot recover terminated instances, you can recover instances that have become impaired in some circumstances.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Compute

Question 38Skipped

A Microsoft Windows file server farm uses Distributed File System Replication (DFSR) to synchronize data in an on-premises environment. The infrastructure is being migrated to the AWS Cloud.

Which service should the solutions architect use to replace the file server farm?

Amazon EFS

Amazon EBS

AWS Storage Gateway

Correct answer

Amazon FSx

Overall explanation

Amazon FSx for Windows file server supports DFS namespaces and DFS replication. This is the best solution for replacing the on-premises infrastructure. Note the limitations for deployment:

Deployment type	SSD storage	HDD storage	DFS namespaces	DFS replication	Custom DNS names	CA shares
Single-AZ 1	✓		✓	✓	✓	
Single-AZ 2	✓	✓	✓		✓	✓*
Multi-AZ	✓	✓	✓		✓	✓*

CORRECT: "Amazon FSx" is the correct answer.

INCORRECT: "Amazon EFS" is incorrect. You cannot replace a Windows file server farm with EFS as it uses a completely different protocol.

INCORRECT: "Amazon EBS" is incorrect. Amazon EBS provides block-based volumes that are attached to EC2 instances. It cannot be used for replacing a shared Windows file server farm using DFSR.

INCORRECT: "AWS Storage Gateway" is incorrect. This service is used for providing cloud storage solutions for on-premises servers. In this case the infrastructure is being migrated into the AWS Cloud.

References:

https://docs.aws.amazon.com/fsx/latest/WindowsGuide/high-availability-multiAZ.html

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 39Skipped

Storage capacity has become an issue for a company that runs application servers on-premises. The servers are connected to a combination of block storage and NFS storage solutions. The company requires a solution that supports local caching without re-architecting its existing applications.

Which combination of changes can the company make to meet these requirements? (Select TWO.)

Correct selection

Use an AWS Storage Gateway volume gateway to replace the block storage.

Use AWS Direct Connect and mount an Amazon FSx for Windows File Server using iSCSI.

Use the mount command on servers to mount Amazon S3 buckets using NFS.

Use Amazon Elastic File System (EFS) volumes to replace the block storage.

Correct selection

Use an AWS Storage Gateway file gateway to replace the NFS storage.

Overall explanation

In this scenario the company should use cloud storage to replace the existing storage solutions that are running out of capacity. The on-premises servers mount the existing storage using block protocols (iSCSI) and file protocols (NFS). As there is a requirement to avoid re-architecting existing applications these protocols must be used in the revised solution.

The AWS Storage Gateway volume gateway should be used to replace the block-based storage systems as it is mounted over iSCSI and the file gateway should be used to replace the NFS file systems as it uses NFS.

CORRECT: "Use an AWS Storage Gateway file gateway to replace the NFS storage" is a correct answer.

CORRECT: "Use an AWS Storage Gateway volume gateway to replace the block storage" is a correct answer.

INCORRECT: "Use the mount command on servers to mount Amazon S3 buckets using NFS" is incorrect. You cannot mount S3 buckets using NFS as it is an object-based storage system (not file-based) and uses an HTTP REST API.

INCORRECT: "Use AWS Direct Connect and mount an Amazon FSx for Windows File Server using iSCSI" is incorrect. You cannot mount FSx for Windows File Server file systems using iSCSI, you must use SMB.

INCORRECT: "Use Amazon Elastic File System (EFS) volumes to replace the block storage" is incorrect. You cannot use EFS to replace block storage as it uses NFS rather than iSCSI.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 40Skipped

A surveying team is using a fleet of drones to collect images of construction sites. The surveying team's laptops lack the inbuilt storage and compute capacity to transfer the images and process the data. While the team has Amazon EC2 instances for processing and Amazon S3 buckets for storage, network connectivity is intermittent and unreliable. The images need to be processed to evaluate the progress of each construction site.

What should a solutions architect recommend?

During intermittent connectivity to EC2 instances, upload images to Amazon SQS.

Configure Amazon Kinesis Data Firehose to create multiple delivery streams aimed separately at the S3 buckets for storage and the EC2 instances for processing the images.

Correct answer

Process and store the images using AWS Snowball Edge devices.

Cache the images locally on a hardware appliance pre-installed with AWS Storage Gateway to process the images when connectivity is restored.

Overall explanation

AWS physical Snowball Edge device will provide much more inbuilt compute and storage compared to the current team's laptops. This negates the need to rely on a stable connection to process any images and solves the team's problems easily and efficiently.

CORRECT: "Process and store the images using AWS Snowball Edge devices" is the correct answer (as explained above.)

INCORRECT: "During intermittent connectivity to EC2 instances, upload images to Amazon SQS" is incorrect as you would still need a reliable internet connection to upload any images to Amazon SQS.

INCORRECT: "Configure Amazon Kinesis Data Firehose to create multiple delivery streams aimed separately at the S3 buckets for storage and the EC2 instances for processing the images" is incorrect as you would still need a reliable internet connection to upload any images to the Amazon Kinesis Service.

INCORRECT: "Cache the images locally on a hardware appliance pre-installed with AWS Storage Gateway to process the images when connectivity is restored" is incorrect as you would

still need reliable internet connection to upload any images to the Amazon Storage Gateway service.

References:

https://docs.aws.amazon.com/snowball/latest/developer-guide/whatisedge.html

Save time with our AWS cheat sheets:

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

Domain

AWS Migration & Transfer

Question 41Skipped

A company's application is running on Amazon EC2 instances in a single Region. In the event of a disaster, a solutions architect needs to ensure that the resources can also be deployed to a second Region.

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

Launch a new EC2 instance in the second Region and copy a volume from Amazon S3 to the new instance

Correct selection

Copy an Amazon Machine Image (AMI) of an EC2 instance and specify the second Region for the destination

Correct selection

Launch a new EC2 instance from an Amazon Machine Image (AMI) in the second Region

Detach a volume on an EC2 instance and copy it to an Amazon S3 bucket in the second Region

Copy an Amazon Elastic Block Store (Amazon EBS) volume from Amazon S3 and launch an EC2 instance in the second Region using that EBS volume

Overall explanation

You can copy an Amazon Machine Image (AMI) within or across AWS Regions using the AWS Management Console, the AWS Command Line Interface or SDKs, or the Amazon EC2 API, all of which support the CopyImage action.

Using the copied AMI the solutions architect would then be able to launch an instance from the same EBS volume in the second Region.

Note: the AMIs are stored on Amazon S3, however you cannot view them in the S3 management console or work with them programmatically using the S3 API.

CORRECT: "Copy an Amazon Machine Image (AMI) of an EC2 instance and specify the second Region for the destination" is a correct answer.

CORRECT: "Launch a new EC2 instance from an Amazon Machine Image (AMI) in the second Region" is also a correct answer.

INCORRECT: "Detach a volume on an EC2 instance and copy it to an Amazon S3 bucket in the second Region" is incorrect. You cannot copy EBS volumes directly from EBS to Amazon S3.

INCORRECT: "Launch a new EC2 instance in the second Region and copy a volume from Amazon S3 to the new instance" is incorrect. You cannot create an EBS volume directly from Amazon S3.

INCORRECT: "Copy an Amazon Elastic Block Store (Amazon EBS) volume from Amazon S3 and launch an EC2 instance in the second Region using that EBS volume" is incorrect. You cannot create an EBS volume directly from Amazon S3.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Compute

Question 42Skipped

A retail company with many stores and warehouses is implementing IoT sensors to gather monitoring data from devices in each location. The data will be sent to AWS in real time. A solutions architect must provide a solution for ensuring events are received in order for each device and ensure that data is saved for future processing.

Which solution would be MOST efficient?

Use Amazon Kinesis Data Streams for real-time events with a shard for each device. Use Amazon Kinesis Data Firehose to save data to Amazon EBS

Correct answer

Use Amazon Kinesis Data Streams for real-time events with a partition key for each device. Use Amazon Kinesis Data Firehose to save data to Amazon S3

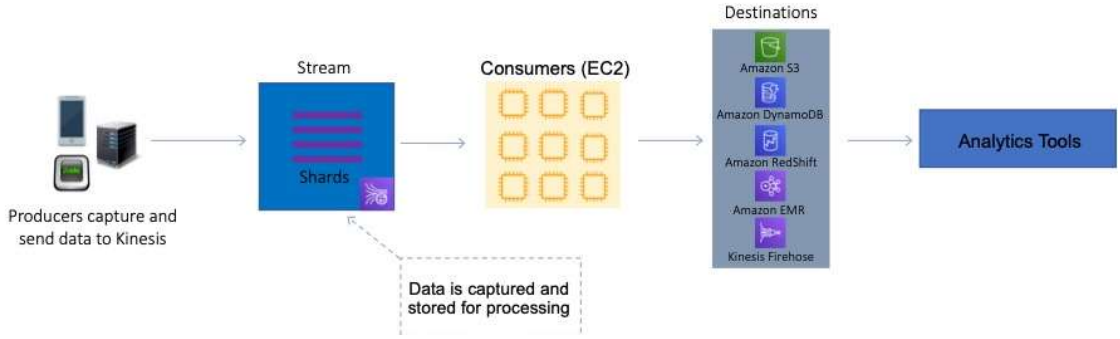
Use an Amazon SQS standard queue for real-time events with one queue for each device. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3

Use an Amazon SQS FIFO queue for real-time events with one queue for each device. Trigger an AWS Lambda function for the SQS queue to save data to Amazon EFS

Overall explanation

Amazon Kinesis Data Streams collect and process data in real time. A *Kinesis data stream* is a set of shards. Each shard has a sequence of data records. Each data record has a sequence number that is assigned by Kinesis Data Streams. A *shard* is a uniquely identified sequence of data records in a stream.

A *partition key* is used to group data by shard within a stream. Kinesis Data Streams segregates the data records belonging to a stream into multiple shards. It uses the partition key that is associated with each data record to determine which shard a given data record belongs to.



For this scenario, the solutions architect can use a partition key for each device. This will ensure the records for that device are grouped by shard and the shard will ensure ordering. Amazon S3 is a valid destination for saving the data records.

CORRECT: "Use Amazon Kinesis Data Streams for real-time events with a partition key for each device. Use Amazon Kinesis Data Firehose to save data to Amazon S3" is the correct answer.

INCORRECT: "Use Amazon Kinesis Data Streams for real-time events with a shard for each device. Use Amazon Kinesis Data Firehose to save data to Amazon EBS" is incorrect as you cannot save data to EBS from Kinesis.

INCORRECT: "Use an Amazon SQS FIFO queue for real-time events with one queue for each device. Trigger an AWS Lambda function for the SQS queue to save data to Amazon EFS" is incorrect as SQS is not the most efficient service for streaming, real time data.

INCORRECT: "Use an Amazon SQS standard queue for real-time events with one queue for each device. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3" is incorrect as SQS is not the most efficient service for streaming, real time data.

References:

https://docs.aws.amazon.com/streams/latest/dev/key-concepts.html

Save time with our AWS cheat sheets:

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

Domain

AWS Analytics

Question 43Skipped

An eCommerce application consists of three tiers. The web tier includes EC2 instances behind an Application Load balancer, the middle tier uses EC2 instances and an Amazon SQS queue to process orders, and the database tier consists of an Auto Scaling DynamoDB table. During busy periods customers have complained about delays in the processing of orders. A Solutions Architect has been tasked with reducing processing times.

Which action will be MOST effective in accomplishing this requirement?

Use Amazon DynamoDB Accelerator (DAX) in front of the DynamoDB backend tier.

Correct answer

Use Amazon EC2 Auto Scaling to scale out the middle tier instances based on the SQS queue depth.

Replace the Amazon SQS queue with Amazon Kinesis Data Firehose.

Add an Amazon CloudFront distribution with a custom origin to cache the responses for the web tier.

Overall explanation

The most likely cause of the processing delays is insufficient instances in the middle tier where the order processing takes place. The most effective solution to reduce processing times in this case is to scale based on the backlog per instance (number of messages in the SQS queue) as this reflects the amount of work that needs to be done.

CORRECT: "Use Amazon EC2 Auto Scaling to scale out the middle tier instances based on the SQS queue depth" is the correct answer.

INCORRECT: "Replace the Amazon SQS queue with Amazon Kinesis Data Firehose" is incorrect. The issue is not the efficiency of queuing messages but the processing of the messages. In this case scaling the EC2 instances to reflect the workload is a better solution.

INCORRECT: "Use Amazon DynamoDB Accelerator (DAX) in front of the DynamoDB backend tier" is incorrect. The DynamoDB table is configured with Auto Scaling so this is not likely to be the bottleneck in order processing.

INCORRECT: "Add an Amazon CloudFront distribution with a custom origin to cache the responses for the web tier" is incorrect. This will cache media files to speed up web response times but not order processing times as they take place in the middle tier.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Application Integration

Question 44Skipped

A company wishes to restrict access to their Amazon DynamoDB table to specific, private source IP addresses from their VPC. What should be done to secure access to the table?

Create an AWS VPN connection to the Amazon DynamoDB endpoint

Create the Amazon DynamoDB table in the VPC

Create an interface VPC endpoint in the VPC with an Elastic Network Interface (ENI)

Correct answer

Create a gateway VPC endpoint and add an entry to the route table

Overall explanation

There are two different types of VPC endpoint: interface endpoint, and gateway endpoint. With an interface endpoint you use an ENI in the VPC. With a gateway endpoint you configure your route table to point to the endpoint. Amazon S3 and DynamoDB use gateway endpoints. This solution means that all traffic will go through the VPC endpoint straight to DynamoDB using private IP addresses.

	Interface Endpoint	Gateway Endpoint
What	Elastic Network Interface with a Private IP	A gateway that is a target for a specific route
How	Uses DNS entries to redirect traffic	Uses prefix lists in the route table to redirect traffic
Which services	API Gateway, CloudFormation, CloudWatch etc.	Amazon S3, DynamoDB
Security	Security Groups	VPC Endpoint Policies

CORRECT: "Create a gateway VPC endpoint and add an entry to the route table" is the correct answer.

INCORRECT: "Create an interface VPC endpoint in the VPC with an Elastic Network Interface (ENI)" is incorrect. As mentioned above, an interface endpoint is not used for DynamoDB, you must use a gateway endpoint.

INCORRECT: "Create the Amazon DynamoDB table in the VPC" is incorrect. You cannot create a DynamoDB table in a VPC, to connect securely using private addresses you should use a gateway endpoint instead.

INCORRECT: "Create an AWS VPN connection to the Amazon DynamoDB endpoint" is incorrect. You cannot create an AWS VPN connection to the Amazon DynamoDB endpoint.

References:

https://docs.amazonaws.cn/en_us/vpc/latest/userguide/vpc-endpoints-ddb.html

https://aws.amazon.com/premiumsupport/knowledge-center/iam-restrict-calls-ip-addresses/

https://aws.amazon.com/blogs/aws/new-vpc-endpoints-for-dynamodb/

Save time with our AWS cheat sheets:

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

Domain

AWS Networking & Content Delivery

Question 45Skipped

A company has two accounts for perform testing and each account has a single VPC: VPC-TEST1 and VPC-TEST2. The operations team require a method of securely copying files between Amazon EC2 instances in these VPCs. The connectivity should not have any single points of failure or bandwidth constraints.

Which solution should a Solutions Architect recommend?

Correct answer

Create a VPC peering connection between VPC-TEST1 and VPC-TEST2.

Attach a Direct Connect gateway to VPC-TEST1 and VPC-TEST2 and enable routing.

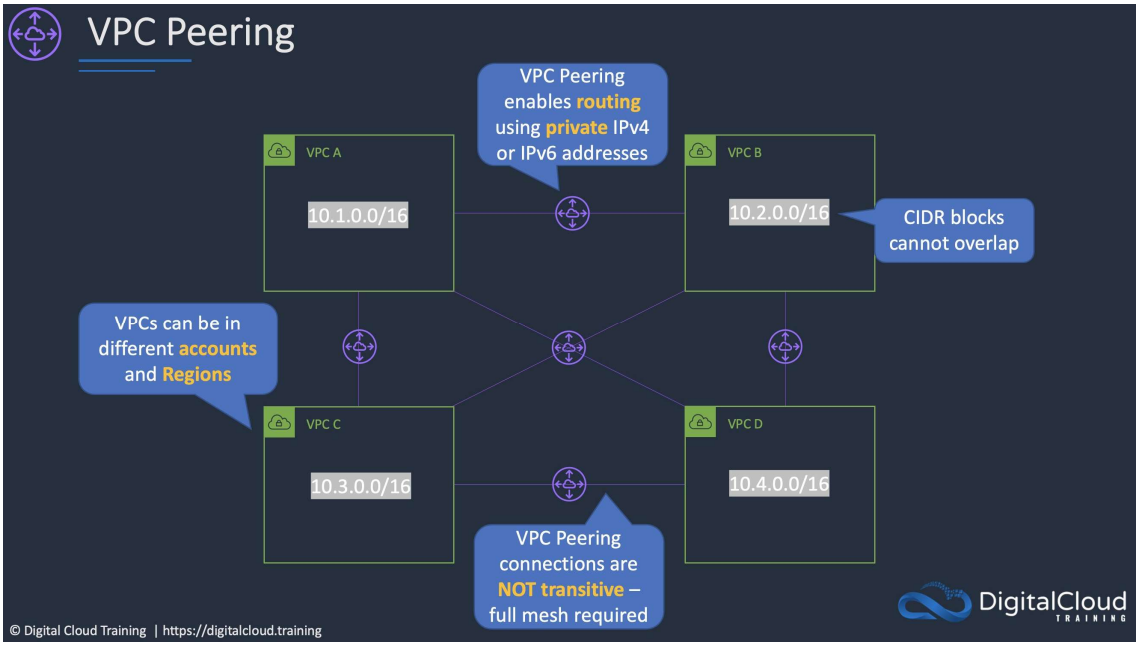
Attach a virtual private gateway to VPC-TEST1 and VPC-TEST2 and enable routing.

Create a VPC gateway endpoint for each EC2 instance and update route tables.

Overall explanation

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network.

You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection).



CORRECT: "Create a VPC peering connection between VPC-TEST1 and VPC-TEST2" is the correct answer.

INCORRECT: "Create a VPC gateway endpoint for each EC2 instance and update route tables" is incorrect. You cannot create VPC gateway endpoints for Amazon EC2 instances. These are used with DynamoDB and S3 only.

INCORRECT: "Attach a virtual private gateway to VPC-TEST1 and VPC-TEST2 and enable routing" is incorrect. You cannot create an AWS Managed VPN connection between two VPCs.

INCORRECT: "Attach a Direct Connect gateway to VPC-TEST1 and VPC-TEST2 and enable routing" is incorrect. Direct Connect gateway is used to connect a Direct Connect connection to multiple VPCs, it is not useful in this scenario as there is no Direct Connect connection.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Networking & Content Delivery

Question 46Skipped

An insurance company has a web application that serves users in the United Kingdom and Australia. The application includes a database tier using a MySQL database hosted in eu-west-2. The web tier runs from eu-west-2 and ap-southeast-2. Amazon Route 53 geoproximity routing is used to direct users to the closest web tier. It has been noted that Australian users receive slow response times to queries.

Which changes should be made to the database tier to improve performance?

Deploy MySQL instances in each Region. Deploy an Application Load Balancer in front of MySQL to reduce the load on the primary instance

Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in the Australian Region

Migrate the database to Amazon DynamoDB. Use DynamoDB global tables to enable replication to additional Regions

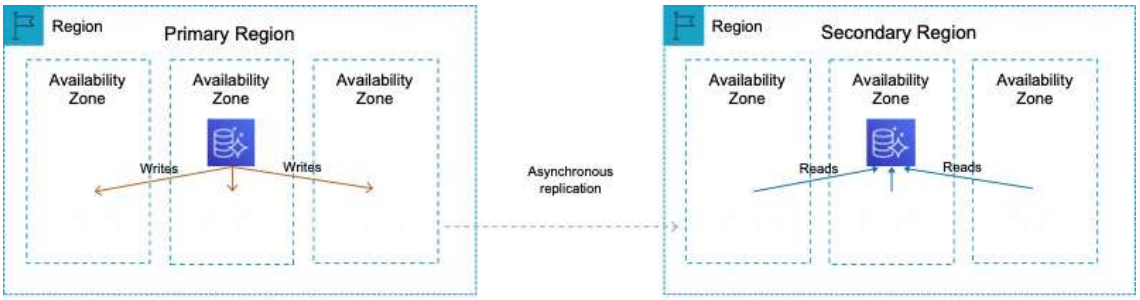
Correct answer

Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure read replicas in ap-southeast-2

Overall explanation

The issue here is latency with read queries being directed from Australia to UK which is great physical distance. A solution is required for improving read performance in Australia.

An Aurora global database consists of one primary AWS Region where your data is mastered, and up to five read-only, secondary AWS Regions. Aurora replicates data to the secondary AWS Regions with typical latency of under a second. You issue write operations directly to the primary DB instance in the primary AWS Region.



Aurora Global Database:

- Uses physical replication
- One secondary AWS region
- Uses dedicated infrastructure
- No impact on DB performance
- Good for disaster recovery

This solution will provide better performance for users in the Australia Region for queries. Writes must still take place in the UK Region but read performance will be greatly improved.

CORRECT: "Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure read replicas in ap-southeast-2" is the correct answer.

INCORRECT: "Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in the Australian Region" is incorrect. The database is located in UK. If the database is migrated to Australia then the reverse problem will occur. Multi-AZ does not assist with improving query performance across Regions.

INCORRECT: "Migrate the database to Amazon DynamoDB. Use DynamoDB global tables to enable replication to additional Regions" is incorrect as a relational database running on MySQL is unlikely to be compatible with DynamoDB.

INCORRECT: "Deploy MySQL instances in each Region. Deploy an Application Load Balancer in front of MySQL to reduce the load on the primary instance" is incorrect as you can only put ALBs in front of the web tier, not the DB tier.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Database

Question 47Skipped

Amazon EC2 instances in a development environment run between 9am and 5pm Monday-Friday. Production instances run 24/7. Which pricing models should be used to optimize cost and ensure capacity is available? (Select TWO.)

Correct selection

On-demand capacity reservations for the development environment

Use On-Demand instances for the production environment

Correct selection

Use Reserved instances for the production environment

Use Reserved instances for the development environment

Use Spot instances for the development environment

Overall explanation

Capacity reservations have no commitment and can be created and canceled as needed. This is ideal for the development environment as it will ensure the capacity is available. There is no price advantage but none of the other options provide a price advantage whilst also ensuring capacity is available

Reserved instances are a good choice for workloads that run continuously. This is a good option for the production environment**.**

CORRECT: "On-demand capacity reservations for the development environment" is a correct answer.

CORRECT: "Use Reserved instances for the production environment" is also a correct answer.

INCORRECT: "Use Spot instances for the development environment" is incorrect. Spot Instances are a cost-effective choice if you can be flexible about when your applications run and if your applications can be interrupted. Spot instances are not suitable for the development environment as important work may be interrupted.

INCORRECT: "Use Reserved instances for the development environment" is incorrect as they require a long-term commitment which is not ideal for a development environment.

INCORRECT: "Use On-Demand instances for the production environment" is incorrect. There is no long-term commitment required when you purchase On-Demand Instances. However, you do not get any discount and therefore this is the most expensive option.

References:

https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/instance-purchasing-options.html

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

Save time with our AWS cheat sheets:

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

Domain

AWS Compute

Question 48Skipped

An organization want to share regular updates about their charitable work using static webpages. The pages are expected to generate a large amount of views from around the world.

The files are stored in an Amazon S3 bucket. A solutions architect has been asked to design an efficient and effective solution.

Which action should the solutions architect take to accomplish this?

Use cross-Region replication to all Regions

Correct answer

Use Amazon CloudFront with the S3 bucket as its origin

Generate presigned URLs for the files

Use the geoproximity feature of Amazon Route 53

Overall explanation

Amazon CloudFront can be used to cache the files in edge locations around the world and this will improve the performance of the webpages.

To serve a static website hosted on Amazon S3, you can deploy a CloudFront distribution using one of these configurations:

Using a REST API endpoint as the origin with access restricted by an origin access identity (OAI)

Using a website endpoint as the origin with anonymous (public) access allowed

Using a website endpoint as the origin with access restricted by a Referer header

CORRECT: "Use Amazon CloudFront with the S3 bucket as its origin" is the correct answer.

INCORRECT: "Generate presigned URLs for the files" is incorrect as this is used to restrict access which is not a requirement.

INCORRECT: "Use cross-Region replication to all Regions" is incorrect as this does not provide a mechanism for directing users to the closest copy of the static webpages.

INCORRECT: "Use the geoproximity feature of Amazon Route 53" is incorrect as this does not include a solution for having multiple copies of the data in different geographic lcoations.

References:

https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-serve-static-website/

Save time with our AWS cheat sheets:

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

Domain

AWS Networking & Content Delivery

Question 49Skipped

A new application is to be published in multiple regions around the world. The Architect needs to ensure only 2 IP addresses need to be whitelisted. The solution should intelligently route traffic for lowest latency and provide fast regional failover.

How can this be achieved?

Launch EC2 instances into multiple regions behind an NLB with a static IP address

Correct answer

Launch EC2 instances into multiple regions behind an NLB and use AWS Global Accelerator

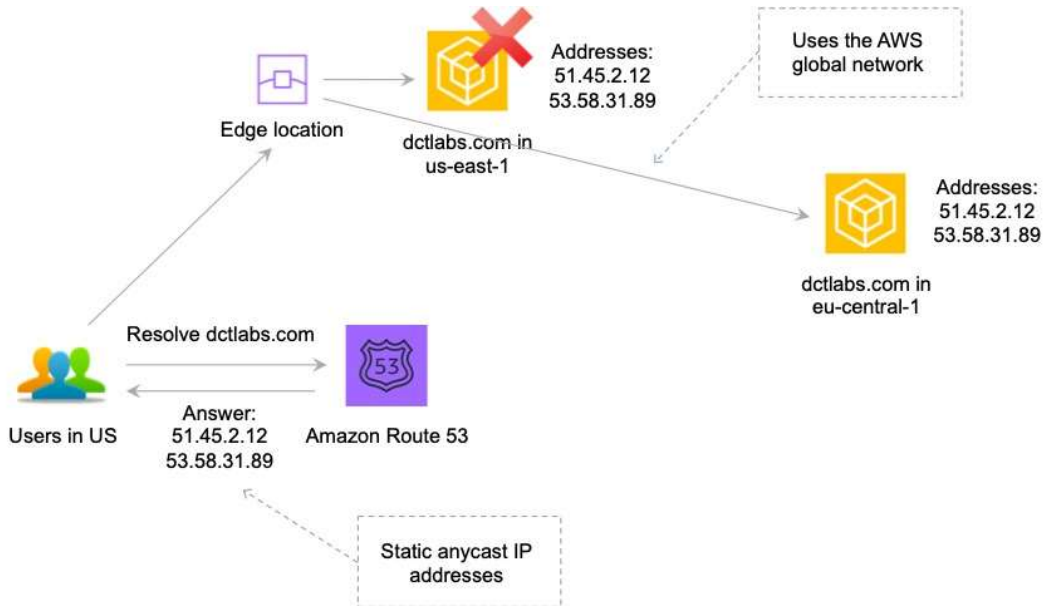
Launch EC2 instances into multiple regions behind an ALB and use Amazon CloudFront with a pair of static IP addresses

Launch EC2 instances into multiple regions behind an ALB and use a Route 53 failover routing policy

Overall explanation

AWS Global Accelerator uses the vast, congestion-free AWS global network to route TCP and UDP traffic to a healthy application endpoint in the closest AWS Region to the user.

This means it will intelligently route traffic to the closest point of presence (reducing latency). Seamless failover is ensured as AWS Global Accelerator uses anycast IP address which means the IP does not change when failing over between regions so there are no issues with client caches having incorrect entries that need to expire.



This is the only solution that provides deterministic failover.

CORRECT: "Launch EC2 instances into multiple regions behind an NLB and use AWS Global Accelerator" is the correct answer.

INCORRECT: "Launch EC2 instances into multiple regions behind an NLB with a static IP address" is incorrect. An NLB with a static IP is a workable solution as you could configure a primary and secondary address in applications. However, this solution does not intelligently route traffic for lowest latency.

INCORRECT: "Launch EC2 instances into multiple regions behind an ALB and use a Route 53 failover routing policy" is incorrect. A Route 53 failover routing policy uses a primary and standby configuration. Therefore, it sends all traffic to the primary until it fails a health check at

which time it sends traffic to the secondary. This solution does not intelligently route traffic for lowest latency.

INCORRECT: "Launch EC2 instances into multiple regions behind an ALB and use Amazon CloudFront with a pair of static IP addresses" is incorrect. Amazon CloudFront cannot be configured with “a pair of static IP addresses”.

References:

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

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

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

Save time with our AWS cheat sheets:

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

Domain

AWS Networking & Content Delivery

Question 50Skipped

A financial services company has a web application with an application tier running in the U.S and Europe. The database tier consists of a MySQL database running on Amazon EC2 in us-west-1. Users are directed to the closest application tier using Route 53 latency-based routing. The users in Europe have reported poor performance when running queries.

Which changes should a Solutions Architect make to the database tier to improve performance?

Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in one of the European Regions.

Migrate the database to Amazon RedShift. Use AWS DMS to synchronize data. Configure applications to use the RedShift data warehouse for queries.

Correct answer

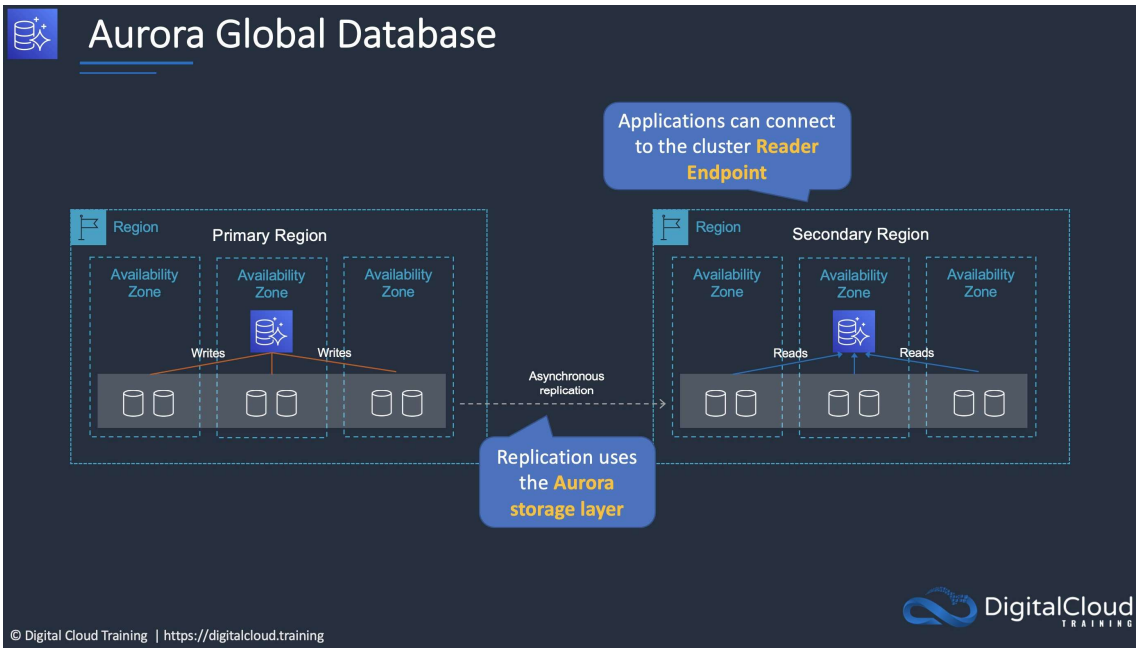
Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure the application tier in Europe to use the local reader endpoint.

Create an Amazon RDS Read Replica in one of the European regions. Configure the application tier in Europe to use the read replica for queries.

Overall explanation

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

A global database can be configured in the European region and then the application tier in Europe will need to be configured to use the local database for reads/queries. The diagram below depicts an Aurora Global Database deployment.



CORRECT: "Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure the application tier in Europe to use the local reader endpoint" is the correct answer.

INCORRECT: "Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in one of the European Regions" is incorrect. You cannot configure a multi-AZ DB instance to run in another Region, it must be in the same Region but in a different Availability Zone.

INCORRECT: "Migrate the database to Amazon RedShift. Use AWS DMS to synchronize data. Configure applications to use the RedShift data warehouse for queries" is incorrect. RedShift is a data warehouse and used for running analytics queries on data that is exported from transactional database systems. It should not be used to reduce latency for users of a database, and is not a live copy of the data.

INCORRECT: "Create an Amazon RDS Read Replica in one of the European regions. Configure the application tier in Europe to use the read replica for queries" is incorrect. You cannot create an RDS Read Replica of a database that is running on Amazon EC2. You can only create read replicas of databases running on Amazon RDS.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Database

Question 51Skipped

An eCommerce company runs an application on Amazon EC2 instances in public and private subnets. The web application runs in a public subnet and the database runs in a private subnet. Both the public and private subnets are in a single Availability Zone.

Which combination of steps should a solutions architect take to provide high availability for this architecture? (Select TWO.)

Create an EC2 Auto Scaling group in the public subnet and use an Application Load Balancer.

Create new public and private subnets in a different AZ. Create a database using Amazon EC2 in one AZ.

Create new public and private subnets in the same AZ but in a different Amazon VPC.

Correct selection

Create an EC2 Auto Scaling group and Application Load Balancer that spans across multiple AZs.

Correct selection

Create new public and private subnets in a different AZ. Migrate the database to an Amazon RDS multi-AZ deployment.

Overall explanation

High availability can be achieved by using multiple Availability Zones within the same VPC. An EC2 Auto Scaling group can then be used to launch web application instances in multiple public subnets across multiple AZs and an ALB can be used to distribute incoming load.

The database solution can be made highly available by migrating from EC2 to Amazon RDS and using a Multi-AZ deployment model. This will provide the ability to failover to another AZ in the event of a failure of the primary database or the AZ in which it runs.

CORRECT: "Create an EC2 Auto Scaling group and Application Load Balancer that spans across multiple AZs" is a correct answer.

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

INCORRECT: "Create new public and private subnets in the same AZ but in a different Amazon VPC" is incorrect. You cannot use multiple VPCs for this solution as it would be difficult to manage and direct traffic (you can't load balance across VPCs).

INCORRECT: "Create an EC2 Auto Scaling group in the public subnet and use an Application Load Balancer" is incorrect. This does not achieve HA as you need multiple public subnets across multiple AZs.

INCORRECT: "Create new public and private subnets in a different AZ. Create a database using Amazon EC2 in one AZ" is incorrect. The database solution is not HA in this answer option.

References:

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

Save time with our AWS cheat sheets:

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

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

Domain

AWS Database

Question 52Skipped

A company hosts a multiplayer game on AWS. The application uses Amazon EC2 instances in a single Availability Zone and users connect over Layer 4. Solutions Architect has been tasked with making the architecture highly available and also more cost-effective.

How can the solutions architect best meet these requirements? (Select TWO.)

Configure an Application Load Balancer in front of the EC2 instances

Correct selection

Configure a Network Load Balancer in front of the EC2 instances

Correct selection

Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically

Configure an Auto Scaling group to add or remove instances in the Availability Zone automatically

Increase the number of instances and use smaller EC2 instance types

Overall explanation

The solutions architect must enable high availability for the architecture and ensure it is cost-effective. To enable high availability an Amazon EC2 Auto Scaling group should be created to add and remove instances across multiple availability zones.

In order to distribute the traffic to the instances the architecture should use a Network Load Balancer which operates at Layer 4. This architecture will also be cost-effective as the Auto Scaling group will ensure the right number of instances are running based on demand.

CORRECT: "Configure a Network Load Balancer in front of the EC2 instances" is a correct answer.

CORRECT: "Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically" is also a correct answer.

INCORRECT: "Increase the number of instances and use smaller EC2 instance types" is incorrect as this is not the most cost-effective option. Auto Scaling should be used to maintain the right number of active instances.

INCORRECT: "Configure an Auto Scaling group to add or remove instances in the Availability Zone automatically" is incorrect as this is not highly available as it’s a single AZ.

INCORRECT: "Configure an Application Load Balancer in front of the EC2 instances" is incorrect as an ALB operates at Layer 7 rather than Layer 4.

References:

https://docsaws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html

Save time with our AWS cheat sheets:

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

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

Domain

AWS Compute

Question 53Skipped

An application is being created that will use Amazon EC2 instances to generate and store data. Another set of EC2 instances will then analyze and modify the data. Storage requirements will be significant and will continue to grow over time. The application architects require a storage solution.

Which actions would meet these needs?

Store the data in Amazon S3 Glacier. Update the vault policy to allow access to the application instances

Store the data in an Amazon EBS volume. Mount the EBS volume on the application instances

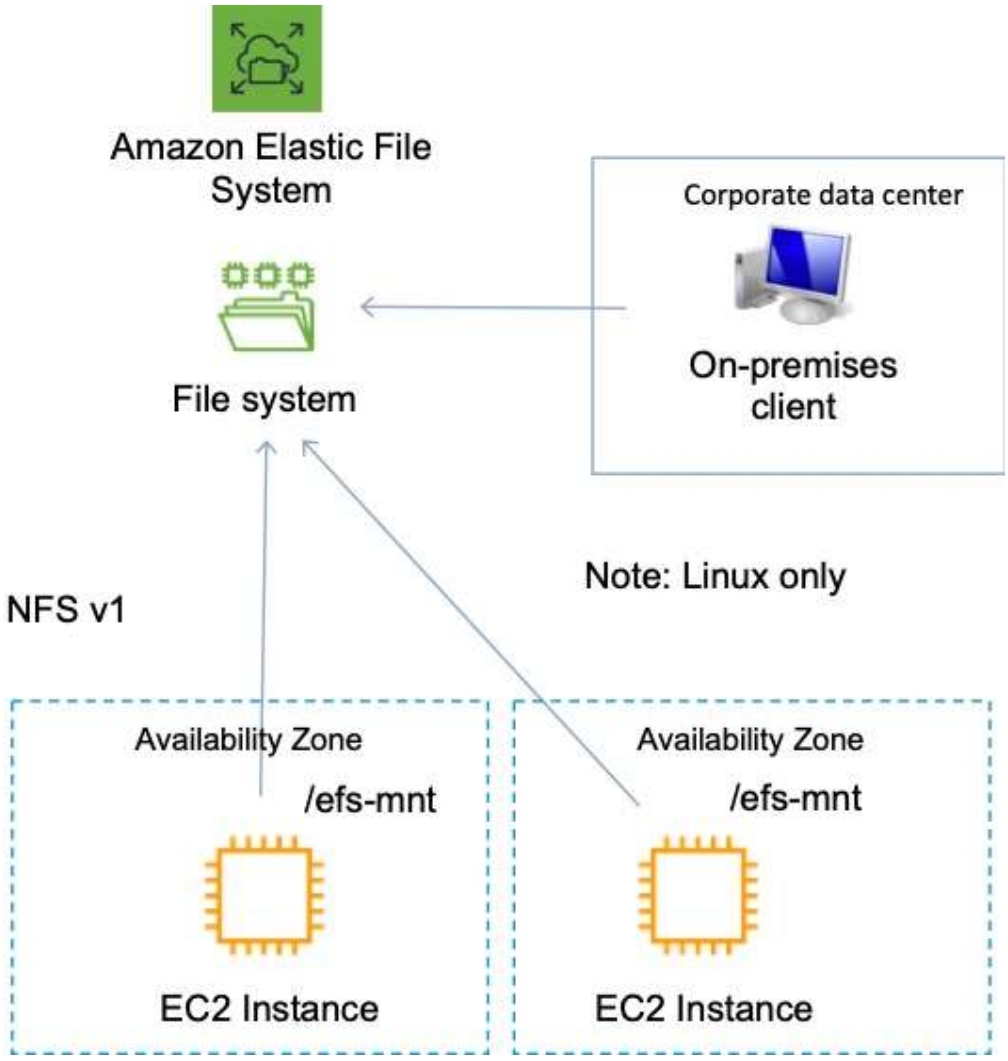
Store the data in AWS Storage Gateway. Setup AWS Direct Connect between the Gateway appliance and the EC2 instances

Correct answer

Store the data in an Amazon EFS filesystem. Mount the file system on the application instances

Overall explanation

Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources. It is built to scale on-demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth.



Amazon EFS supports the Network File System version 4 (NFSv4.1 and NFSv4.0) protocol. Multiple Amazon EC2 instances can access an Amazon EFS file system at the same time, providing a common data source for workloads and applications running on more than one instance or server.

For this scenario, EFS is a great choice as it will provide a scalable file system that can be mounted by multiple EC2 instances and accessed simultaneously.

CORRECT: "Store the data in an Amazon EFS filesystem. Mount the file system on the application instances" is the correct answer.

INCORRECT: "Store the data in an Amazon EBS volume. Mount the EBS volume on the application instances" is incorrect. Though there is a new feature that allows (EBS multi-attach) that allows attaching multiple Nitro instances to a volume, this is not on the exam yet, and has some specific constraints.

INCORRECT: "Store the data in Amazon S3 Glacier. Update the vault policy to allow access to the application instances" is incorrect as S3 Glacier is not a suitable storage location for live access to data, it is used for archival.

INCORRECT: "Store the data in AWS Storage Gateway. Setup AWS Direct Connect between the Gateway appliance and the EC2 instances" is incorrect. There is no reason to store the data on-premises in a Storage Gateway, using EFS is a much better solution.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Database

Question 54Skipped

An organization has a large amount of data on Windows (SMB) file shares in their on-premises data center. The organization would like to move data into Amazon S3. They would like to automate the migration of data over their AWS Direct Connect link.

Which AWS service can assist them?

AWS Snowball

AWS Database Migration Service (DMS)

Correct answer

AWS DataSync

AWS CloudFormation

Overall explanation

AWS DataSync can be used to move large amounts of data online between on-premises storage and Amazon S3 or Amazon Elastic File System (Amazon EFS). DataSync eliminates or automatically handles many of these tasks, including scripting copy jobs, scheduling and monitoring transfers, validating data, and optimizing network utilization. The source datastore can be Server Message Block (SMB) file servers.

CORRECT: "AWS DataSync" is the correct answer.

INCORRECT: "AWS Database Migration Service (DMS)" is incorrect. AWS Database Migration Service (DMS) is used for migrating databases, not data on file shares.

INCORRECT: "AWS CloudFormation" is incorrect. AWS CloudFormation can be used for automating infrastructure provisioning. This is not the best use case for CloudFormation as DataSync is designed specifically for this scenario.

INCORRECT: "AWS Snowball" is incorrect. AWS Snowball is a hardware device that is used for migrating data into AWS. The organization plan to use their Direct Connect link for migrating data rather than sending it in via a physical device. Also, Snowball will not automate the migration.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Migration & Transfer

Question 55Skipped

A company runs a web application that serves weather updates. The application runs on a fleet of Amazon EC2 instances in a Multi-AZ Auto scaling group behind an Application Load Balancer (ALB). The instances store data in an Amazon Aurora database. A solutions architect needs to make the application more resilient to sporadic increases in request rates.

Which architecture should the solutions architect implement? (Select TWO.)

Add an AWS Transit Gateway to the Availability Zones

Correct selection

Add Amazon Aurora Replicas

Add and AWS WAF in front of the ALB

Correct selection

Add an Amazon CloudFront distribution in front of the ALB

Add an AWS Global Accelerator endpoint

Overall explanation

The architecture is already highly resilient but the may be subject to performance degradation if there are sudden increases in request rates. To resolve this situation Amazon Aurora Read Replicas can be used to serve read traffic which offloads requests from the main database. On the frontend an Amazon CloudFront distribution can be placed in front of the ALB and this will cache content for better performance and also offloads requests from the backend.

CORRECT: "Add Amazon Aurora Replicas" is the correct answer.

CORRECT: "Add an Amazon CloudFront distribution in front of the ALB" is the correct answer.

INCORRECT: "Add and AWS WAF in front of the ALB" is incorrect. A web application firewall protects applications from malicious attacks. It does not improve performance.

INCORRECT: "Add an AWS Transit Gateway to the Availability Zones" is incorrect as this is used to connect on-premises networks to VPCs.

INCORRECT: "Add an AWS Global Accelerator endpoint" is incorrect as this service is used for directing users to different instances of the application in different regions based on latency.

References:

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

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

Save time with our AWS cheat sheets:

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

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

Domain

AWS Database

Question 56Skipped

A company runs an application in a factory that has a small rack of physical compute resources. The application stores data on a network attached storage (NAS) device using the NFS protocol. The company requires a daily offsite backup of the application data.

Which solution can a Solutions Architect recommend to meet this requirement?

Correct answer

Use an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3.

Use an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3.

Create an IPSec VPN to AWS and configure the application to mount the Amazon EFS file system. Run a copy job to backup the data to EFS.

Use an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3.

Overall explanation

The AWS Storage Gateway Hardware Appliance is a physical, standalone, validated server configuration for on-premises deployments. It comes pre-loaded with Storage Gateway software, and provides all the required CPU, memory, network, and SSD cache resources for creating and configuring File Gateway, Volume Gateway, or Tape Gateway.

A file gateway is the correct type of appliance to use for this use case as it is suitable for mounting via the NFS and SMB protocols.

CORRECT: "Use an AWS Storage Gateway file gateway hardware appliance on premises to replicate the data to Amazon S3" is the correct answer.

INCORRECT: "Use an AWS Storage Gateway volume gateway with stored volumes on premises to replicate the data to Amazon S3" is incorrect. Volume gateways are used for block-based storage and this solution requires NFS (file-based storage).

INCORRECT: "Use an AWS Storage Gateway volume gateway with cached volumes on premises to replicate the data to Amazon S3" is incorrect. Volume gateways are used for block-based storage and this solution requires NFS (file-based storage).

INCORRECT: "Create an IPSec VPN to AWS and configure the application to mount the Amazon EFS file system. Run a copy job to backup the data to EFS" is incorrect. It would be better to use

a Storage Gateway which will automatically take care of synchronizing a copy of the data to AWS.

References:

https://aws.amazon.com/storagegateway/hardware-appliance/

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 57Skipped

An application running on an Amazon ECS container instance using the EC2 launch type needs permissions to write data to Amazon DynamoDB.

How can you assign these permissions only to the specific ECS task that is running the application?

Modify the *AmazonECSTaskExecutionRolePolicy* policy to add permissions for DynamoDB

Use a security group to allow outbound connections to DynamoDB and assign it to the container instance

Create an IAM policy with permissions to DynamoDB and attach it to the container instance

Correct answer

Create an IAM policy with permissions to DynamoDB and assign It to a task using the *taskRoleArn* parameter

Overall explanation

To specify permissions for a specific task on Amazon ECS you should use IAM Roles for Tasks. The permissions policy can be applied to tasks when creating the task definition, or by using an IAM task role override using the AWS CLI or SDKs. The *taskRoleArn* parameter is used to specify the policy.

CORRECT: "Create an IAM policy with permissions to DynamoDB and assign It to a task using the *taskRoleArn* parameter" is the correct answer.

INCORRECT: "Create an IAM policy with permissions to DynamoDB and attach it to the container instance" is incorrect. You should not apply the permissions to the container instance as they will then apply to all tasks running on the instance as well as the instance itself.

INCORRECT: "Use a security group to allow outbound connections to DynamoDB and assign it to the container instance" is incorrect. Though you will need a security group to allow outbound connections to DynamoDB, the question is asking how to assign permissions to write data to DynamoDB and a security group cannot provide those permissions.

INCORRECT: "Modify the *AmazonECSTaskExecutionRolePolicy* policy to add permissions for DynamoDB" is incorrect. The *AmazonECSTaskExecutionRolePolicy* policy is the Task Execution

IAM Role. This is used by the container agent to be able to pull container images, write log file etc.

References:

https://docs.aws.amazon.com/AmazonECS/latest/developerguide/task-iam-roles.html

Save time with our AWS cheat sheets:

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

Domain

AWS Compute

Question 58Skipped

A team are planning to run analytics jobs on log files each day and require a storage solution. The size and number of logs is unknown and data will persist for 24 hours only.

What is the MOST cost-effective solution?

Amazon S3 Intelligent-Tiering

Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

Correct answer

Amazon S3 Standard

Amazon S3 Glacier Deep Archive

Overall explanation

S3 standard is the best choice in this scenario for a short term storage solution. In this case the size and number of logs is unknown and it would be difficult to fully assess the access patterns at this stage. Therefore, using S3 standard is best as it is cost-effective, provides immediate access, and there are no retrieval fees or minimum capacity charge per object.

CORRECT: "Amazon S3 Standard" is the correct answer.

INCORRECT: "Amazon S3 Intelligent-Tiering" is incorrect as there is an additional fee for using this service and for a short-term requirement it may not be beneficial.

INCORRECT: "Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)" is incorrect as this storage class has a minimum capacity charge per object (128 KB) and a per GB retrieval fee.

INCORRECT: "Amazon S3 Glacier Deep Archive" is incorrect as this storage class is used for archiving data. There are retrieval fees and it take hours to retrieve data from an archive.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 59Skipped

A web application runs in public and private subnets. The application architecture consists of a web tier and database tier running on Amazon EC2 instances. Both tiers run in a single Availability Zone (AZ).

Which combination of steps should a solutions architect take to provide high availability for this architecture? (Select TWO.)

Correct selection

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

Create new public and private subnets in a new AZ. Create a database using Amazon EC2 in one AZ

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

Correct selection

Create new public and private subnets in the same VPC, each in a new AZ. Migrate the database to an Amazon RDS multi-AZ deployment

Create new public and private subnets in the same AZ for high availability

Overall explanation

To add high availability to this architecture both the web tier and database tier require changes. For the web tier an Auto Scaling group across multiple AZs with an ALB will ensure there are always instances running and traffic is being distributed to them.

The database tier should be migrated from the EC2 instances to Amazon RDS to take advantage of a managed database with Multi-AZ functionality. This will ensure that if there is an issue preventing access to the primary database a secondary database can take over.

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

CORRECT: "Create new public and private subnets in the same VPC, each in a new AZ. Migrate the database to an Amazon RDS multi-AZ deployment" is the correct answer.

INCORRECT: "Create new public and private subnets in the same AZ for high availability" is incorrect as this would not add high availability.

INCORRECT: "Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer (ALB)" is incorrect because the existing servers are in a single subnet. For HA we need to instances in multiple subnets.

INCORRECT: "Create new public and private subnets in a new AZ. Create a database using Amazon EC2 in one AZ" is incorrect because we also need HA for the database layer.

References:

https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html

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

Save time with our AWS cheat sheets:

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

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

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

Domain

AWS Compute

Question 60Skipped

A company delivers content to subscribers distributed globally from an application running on AWS. The application uses a fleet of Amazon EC2 instance in a private subnet behind an Application Load Balancer (ALB). Due to an update in copyright restrictions, it is necessary to block access for specific countries.

What is the EASIEST method to meet this requirement?

Modify the ALB security group to deny incoming traffic from blocked countries

Modify the security group for EC2 instances to deny incoming traffic from blocked countries

Correct answer

Use Amazon CloudFront to serve the application and deny access to blocked countries

Use a network ACL to block the IP address ranges associated with the specific countries

Overall explanation

When a user requests your content, CloudFront typically serves the requested content regardless of where the user is located. If you need to prevent users in specific countries from accessing your content, you can use the CloudFront geo restriction feature to do one of the following:

Allow your users to access your content only if they're in one of the countries on a whitelist of approved countries.

Prevent your users from accessing your content if they're in one of the countries on a blacklist of banned countries.

For example, if a request comes from a country where, for copyright reasons, you are not authorized to distribute your content, you can use CloudFront geo restriction to block the request.

This is the easiest and most effective way to implement a geographic restriction for the delivery of content.

CORRECT: "Use Amazon CloudFront to serve the application and deny access to blocked countries" is the correct answer.

INCORRECT: "Use a Network ACL to block the IP address ranges associated with the specific countries" is incorrect as this would be extremely difficult to manage.

INCORRECT: "Modify the ALB security group to deny incoming traffic from blocked countries" is incorrect as security groups cannot block traffic by country.

INCORRECT: "Modify the security group for EC2 instances to deny incoming traffic from blocked countries" is incorrect as security groups cannot block traffic by country.

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 61Skipped

A company requires that all AWS IAM user accounts have specific complexity requirements and minimum password length.

How should a Solutions Architect accomplish this?

Use an AWS Config rule to enforce the requirements when creating user accounts.

Create an IAM policy that enforces the requirements and apply it to all users.

Correct answer

Set a password policy for the entire AWS account.

Set a password policy for each IAM user in the AWS account.

Overall explanation

The easiest way to enforce this requirement is to update the password policy that applies to the entire AWS account. When you create or change a password policy, most of the password policy settings are enforced the next time your users change their passwords. However, some of the settings are enforced immediately such as the password expiration period.

CORRECT: "Set a password policy for the entire AWS account" is the correct answer.

INCORRECT: "Set a password policy for each IAM user in the AWS account" is incorrect. There's no need to set an individual password policy for each user, it will be easier to set the policy for everyone.

INCORRECT: "Create an IAM policy that enforces the requirements and apply it to all users" is incorrect. As there is no specific targeting required it is easier to update the account password policy.

INCORRECT: "Use an AWS Config rule to enforce the requirements when creating user accounts" is incorrect. You cannot use AWS Config to enforce the password requirements at the time of creating a user account.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

Save time with our AWS cheat sheets:

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

Domain

AWS Security, Identity, & Compliance

Question 62Skipped

A company runs a dynamic website that is hosted on an on-premises server in the United States. The company is expanding to Europe and is investigating how they can optimize the performance of the website for European users. The website's backed must remain in the United States. The company requires a solution that can be implemented within a few days.

What should a Solutions Architect recommend?

Use Amazon CloudFront with Lambda@Edge to direct traffic to an on-premises origin.

Launch an Amazon EC2 instance in an AWS Region in the United States and migrate the website to it.

Migrate the website to Amazon S3. Use cross-Region replication between Regions and a latency-based Route 53 policy.

Correct answer

Use Amazon CloudFront with a custom origin pointing to the on-premises servers.

Overall explanation

A custom origin can point to an on-premises server and CloudFront is able to cache content for dynamic websites. CloudFront can provide performance optimizations for custom origins even if they are running on on-premises servers. These include persistent TCP connections to the origin, SSL enhancements such as Session tickets and OCSP stapling.

Additionally, connections are routed from the nearest Edge Location to the user across the AWS global network. If the on-premises server is connected via a Direct Connect (DX) link this can further improve performance.

CORRECT: "Use Amazon CloudFront with a custom origin pointing to the on-premises servers" is the correct answer.

INCORRECT: "Use Amazon CloudFront with Lambda@Edge to direct traffic to an on-premises origin" is incorrect. Lambda@Edge is not used to direct traffic to on-premises origins.

INCORRECT: "Launch an Amazon EC2 instance in an AWS Region in the United States and migrate the website to it" is incorrect. This would not necessarily improve performance for European users.

INCORRECT: "Migrate the website to Amazon S3. Use cross-Region replication between Regions and a latency-based Route 53 policy" is incorrect. You cannot host dynamic websites on Amazon S3 (static only).

References:

https://aws.amazon.com/cloudfront/dynamic-content/

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 63Skipped

A company runs an application on an Amazon EC2 instance the requires 250 GB of storage space. The application is not used often and has small spikes in usage on weekday mornings and afternoons. The disk I/O can vary with peaks hitting a maximum of 3,000 IOPS. A Solutions Architect must recommend the most cost-effective storage solution that delivers the performance required.

Which configuration should the Solutions Architect recommend?

Which solution should the solutions architect recommend?

Amazon EBS Cold HDD (sc1)

Correct answer

Amazon EBS General Purpose SSD (gp2)

Amazon EBS Throughput Optimized HDD (st1)

Amazon EBS Provisioned IOPS SSD (i01)

Overall explanation

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

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

In this configuration the volume will provide a baseline performance of 750 IOPS but will always be able to burst to the required 3,000 IOPS during periods of increased traffic.

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

INCORRECT: "Amazon EBS Provisioned IOPS SSD (i01)" is incorrect. The i01 volume type will be more expensive and is not necessary for the performance levels required.

INCORRECT: "Amazon EBS Cold HDD (sc1)" is incorrect. The sc1 volume type is not going to deliver the performance requirements as it cannot burst to 3,000 IOPS.

INCORRECT: "Amazon EBS Throughput Optimized HDD (st1)" is incorrect. The st1 volume type is not going to deliver the performance requirements as it cannot burst to 3,000 IOPS.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Compute

Question 64Skipped

The database tier of a web application is running on a Windows server on-premises. The database is a Microsoft SQL Server database. The application owner would like to migrate the database to an Amazon RDS instance.

How can the migration be executed with minimal administrative effort and downtime?

Use AWS DataSync to migrate the data from the database to Amazon S3. Use AWS Database Migration Service (DMS) to migrate the database to RDS

Correct answer

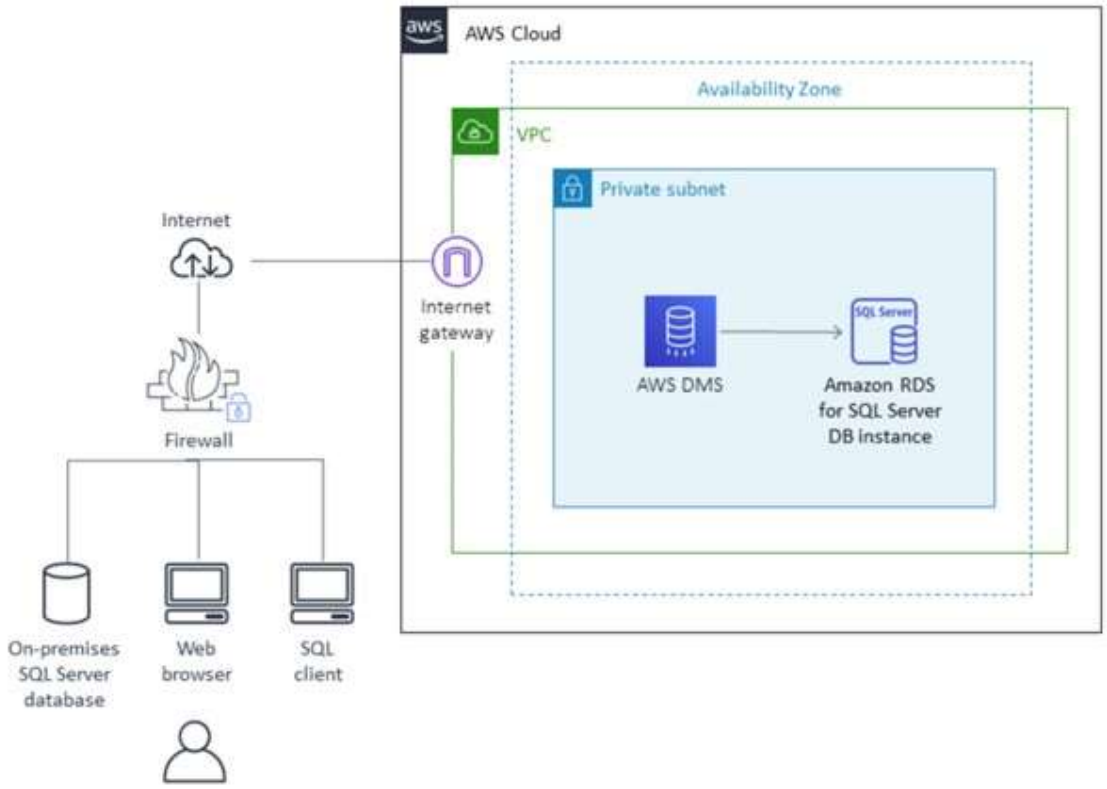
Use the AWS Database Migration Service (DMS) to directly migrate the database to RDS

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

Use the AWS Server Migration Service (SMS) to migrate the server to Amazon EC2.Use AWS Database Migration Service (DMS) to migrate the database to RDS

Overall explanation

You can directly migrate Microsoft SQL Server from an on-premises server into Amazon RDS using the Microsoft SQL Server database engine. This can be achieved using the native Microsoft SQL Server tools, or using AWS DMS as depicted below:



CORRECT: "Use the AWS Database Migration Service (DMS) to directly migrate the database to RDS" is the correct answer.

INCORRECT: "Use the AWS Server Migration Service (SMS) to migrate the server to Amazon EC2. Use AWS Database Migration Service (DMS) to migrate the database to RDS" is incorrect. You do not need to use the AWS SMS service to migrate the server into EC2 first. You can directly migrate the database online with minimal downtime.

INCORRECT: "Use AWS DataSync to migrate the data from the database to Amazon S3. Use AWS Database Migration Service (DMS) to migrate the database to RDS" is incorrect. AWS DataSync is used for migrating data, not databases.

INCORRECT: "Use the AWS Database Migration Service (DMS) to directly migrate the database to RDS. Use the Schema Conversion Tool (SCT) to enable conversion from Microsoft SQL Server to Amazon RDS" is incorrect. You do not need to use the SCT as you are migrating into the same destination database engine (RDS is just the platform).

References:

https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-microsoft-sql-server-database-to-amazon-rds-for-sql-server.html

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

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

https://aws.amazon.com/dms/schema-conversion-tool/

Save time with our AWS cheat sheets:

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

Domain

AWS Migration & Transfer

Question 65Skipped

A company provides a REST-based interface to an application that allows a partner company to send data in near-real time. The application then processes the data that is received and stores it for later analysis. The application runs on Amazon EC2 instances.

The partner company has received many 503 Service Unavailable Errors when sending data to the application and the compute capacity reaches its limits and is unable to process requests when spikes in data volume occur.

Which design should a Solutions Architect implement to improve scalability?

Use Amazon API Gateway in front of the existing application. Create a usage plan with a quota limit for the partner company.

Use Amazon SNS to ingest the data and trigger AWS Lambda functions to process the data in near-real time.

Correct answer

Use Amazon Kinesis Data Streams to ingest the data. Process the data using AWS Lambda functions.

Use Amazon SQS to ingest the data. Configure the EC2 instances to process messages from the SQS queue.

Overall explanation

Amazon Kinesis enables you to ingest, buffer, and process streaming data in real-time. Kinesis can handle any amount of streaming data and process data from hundreds of thousands of sources with very low latencies. This is an ideal solution for data ingestion.

To ensure the compute layer can scale to process increasing workloads, the EC2 instances should be replaced by AWS Lambda functions. Lambda can scale seamlessly by running multiple executions in parallel.

CORRECT: "Use Amazon Kinesis Data Streams to ingest the data. Process the data using AWS Lambda functions" is the correct answer.

INCORRECT: "Use Amazon API Gateway in front of the existing application. Create a usage plan with a quota limit for the partner company" is incorrect. A usage plan will limit the amount of data that is received and cause more errors to be received by the partner company.

INCORRECT: "Use Amazon SQS to ingest the data. Configure the EC2 instances to process messages from the SQS queue" is incorrect. Amazon Kinesis Data Streams should be used for near-real time or real-time use cases instead of Amazon SQS.

INCORRECT: "Use Amazon SNS to ingest the data and trigger AWS Lambda functions to process the data in near-real time" is incorrect. SNS is not a near-real time solution for data ingestion. SNS is used for sending notifications.

References:

https://aws.amazon.com/kinesis/

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

Save time with our AWS cheat sheets:

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

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

Domain

AWS Analytics