Question 1Skipped

An application has been deployed on Amazon EC2 instances behind an Application Load Balancer (ALB). A Solutions Architect must improve the security posture of the application and minimize the impact of a DDoS attack on resources.

Which of the following solutions is MOST effective?

Create a custom AWS Lambda function that monitors for suspicious traffic and modifies a network ACL when a potential DDoS attack is identified.

Enable access logs on the Application Load Balancer and configure Amazon CloudWatch to monitor the access logs and trigger a Lambda function when potential attacks are identified. Configure the Lambda function to modify the ALBs security group and block the attack.

Enable VPC Flow Logs and store them in Amazon S3. Use Amazon Athena to parse the logs and identify and block potential DDoS attacks.

Correct answer

Configure an AWS WAF ACL with rate-based rules. Enable the WAF ACL on the Application Load Balancer.

Overall explanation

A rate-based rule tracks the rate of requests for each originating IP address, and triggers the rule action on IPs with rates that go over a limit. You set the limit as the number of requests per 5-minute time span.

You can use this type of rule to put a temporary block on requests from an IP address that's sending excessive requests. By default, AWS WAF aggregates requests based on the IP address from the web request origin, but you can configure the rule to use an IP address from an HTTP header, like X-Forwarded-For, instead.

CORRECT: "Configure an AWS WAF ACL with rate-based rules. Enable the WAF ACL on the Application Load Balancer" is the correct answer.

INCORRECT: "Create a custom AWS Lambda function that monitors for suspicious traffic and modifies a network ACL when a potential DDoS attack is identified" is incorrect. There’s not description here of how Lambda is going to monitor for traffic.

INCORRECT: "Enable VPC Flow Logs and store them in Amazon S3. Use Amazon Athena to parse the logs and identify and block potential DDoS attacks" is incorrect. Amazon Athena is not able to block DDoS attacks, another service would be needed.

INCORRECT: "Enable access logs on the Application Load Balancer and configure Amazon CloudWatch to monitor the access logs and trigger a Lambda function when potential attacks are identified. Configure the Lambda function to modify the ALBs security group and block the attack" is incorrect. Access logs are exported to S3 but not to CloudWatch. Also, it would not be possible to block an attack from a specific IP using a security group (while still allowing any other source access) as they do not support deny rules.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Security, Identity, & Compliance

Question 2Skipped

A website is running on Amazon EC2 instances and access is restricted to a limited set of IP ranges. A solutions architect is planning to migrate static content from the website to an Amazon S3 bucket configured as an origin for an Amazon CloudFront distribution. Access to the static content must be restricted to the same set of IP addresses.

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

Create an AWS WAF web ACL that includes the same IP restrictions that exist in the EC2 security group. Associate this new web ACL with the Amazon S3 bucket.

Create an origin access identity (OAI) and associate it with the distribution. Generate presigned URLs that limit access to the OAI.

Correct selection

Create an AWS WAF web ACL that includes the same IP restrictions that exist in the EC2 security group. Associate this new web ACL with the CloudFront distribution.

Correct selection

Create an origin access identity (OAI) and associate it with the distribution. Change the permissions in the bucket policy so that only the OAI can read the objects.

Attach the existing security group that contains the IP restrictions to the Amazon CloudFront distribution.

Overall explanation

To prevent users from circumventing the controls implemented on CloudFront (using WAF or presigned URLs / signed cookies) you can use an origin access identity (OAI). An OAI is a special CloudFront user that you associate with a distribution.

The next step is to change the permissions either on your Amazon S3 bucket or on the files in your bucket so that only the origin access identity has read permission (or read and download permission). This can be implemented through a bucket policy.

To control access at the CloudFront layer the AWS Web Application Firewall (WAF) can be used. With WAF you must create an ACL that includes the IP restrictions required and then associate the web ACL with the CloudFront distribution.

CORRECT: "Create an origin access identity (OAI) and associate it with the distribution. Change the permissions in the bucket policy so that only the OAI can read the objects" is a correct answer.

CORRECT: "Create an AWS WAF web ACL that includes the same IP restrictions that exist in the EC2 security group. Associate this new web ACL with the CloudFront distribution" is also a correct answer.

INCORRECT: "Create an origin access identity (OAI) and associate it with the distribution. Generate presigned URLs that limit access to the OAI" is incorrect. Presigned URLs can be used to protect access to CloudFront but they cannot be used to limit access to an OAI.

INCORRECT: "Create an AWS WAF web ACL that includes the same IP restrictions that exist in the EC2 security group. Associate this new web ACL with the Amazon S3 bucket" is incorrect. The Web ACL should be associated with CloudFront, not S3.

INCORRECT: "Attach the existing security group that contains the IP restrictions to the Amazon CloudFront distribution" is incorrect. You cannot attach a security group to a CloudFront distribution.

References:

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

https://docs.aws.amazon.com/waf/latest/developerguide/cloudfront-features.html

Save time with our AWS cheat sheets:

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

Domain

AWS Security, Identity, & Compliance

Question 3Skipped

A stock trading startup company has a custom web application to sell trading data to its users online. The company uses Amazon DynamoDB to store its data and wants to build a new service that sends an alert to the managers of four internal teams every time a new trading event is recorded. The company does not want this new service to affect the performance of the current application.

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

Correct answer

On the table, enable Amazon DynamoDB Streams. Subscriptions can be made to a single Amazon Simple Notification Service (Amazon SNS) topic using triggers.

Create a custom attribute for each record to flag new items. A cron job can be written to scan the table every minute for new items and notify an Amazon Simple Queue Service (Amazon SQS) queue.

Write new event data to the table using DynamoDB transactions. The transactions should be configured to notify internal teams.

Use the current application to publish a message to four Amazon Simple Notification Service (Amazon SNS) topics. Each team should subscribe to one topic.

Overall explanation

DynamoDB Streams captures a time-ordered sequence of item-level modifications in any DynamoDB table and stores this information in a log for up to 24 hours. Applications can access this log and view the data items as they appeared before and after they were modified, in near-real time. This is the native way to handle this within DynamoDB, therefore will incur the least amount of operational overhead.

CORRECT: "On the table, enable Amazon DynamoDB Streams. Subscriptions can be made to a single Amazon Simple Notification Service (Amazon SNS) topic using triggers" is the correct answer (as explained above.)

INCORRECT: "Write new event data to the table using DynamoDB transactions. The transactions should be configured to notify internal teams" is incorrect. With Amazon DynamoDB transactions, you can group multiple actions together and submit them as a single all-or-nothing TransactWriteItems or TransactGetItems operation. The following sections describe API operations, capacity management, best practices, and other details about using transactional operations in DynamoDB. This is not suitable for this use case.

INCORRECT: "Use the current application to publish a message to four Amazon Simple Notification Service (Amazon SNS) topics. Each team should subscribe to one topic" is incorrect. Using four separate SNS topics will take a significant amount of overhead, and this functionality can be managed natively within DynamoDB using DynamoDB streams.

INCORRECT: "Create a custom attribute for each record to flag new items. A cron job can be written to scan the table every minute for new items and notify an Amazon Simple Queue Service (Amazon SQS) queue" is incorrect. Writing a CRON job also takes significant overhead compared to using DynamoDB streams.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Database

Question 4Skipped

A High Performance Computing (HPC) application will be migrated to AWS. The application requires low network latency and high throughput between nodes and will be deployed in a single AZ.

How should the application be deployed for best inter-node performance?

In a partition placement group

Behind a Network Load Balancer (NLB)

Correct answer

In a cluster placement group

In a spread placement group

Overall explanation

A cluster placement group provides low latency and high throughput for instances deployed in a single AZ. It is the best way to provide the performance required for this application.

CORRECT: "In a cluster placement group" is the correct answer.

INCORRECT: "In a partition placement group" is incorrect. A partition placement group is used for grouping instances into logical segments. It provides control and visibility into instance placement but is not the best option for performance.

INCORRECT: "In a spread placement group" is incorrect. A spread placement group is used to spread instances across underlying hardware. It is not the best option for performance.

INCORRECT: "Behind a Network Load Balancer (NLB)" is incorrect. A network load balancer is used for distributing incoming connections, this does assist with inter-node performance.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Compute

Question 5Skipped

A company is architecting a shared storage solution for an AWS-hosted gaming application. The company needs the ability to use Lustre clients to access data. The solution must be fully managed.

Which solution meets these requirements?

Create an Amazon Elastic File System (Amazon EFS) file system and configure it to support Lustre. Attach the file system to the origin server. Connect the application server to the file system.

Correct answer

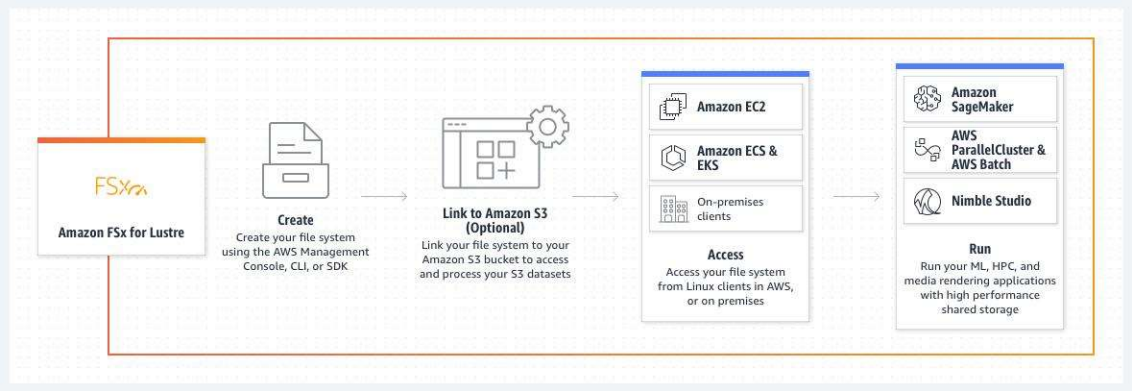
Create an Amazon FSx for Lustre file system. Connect the file system to the origin server. Ensure that the file system is connected to the application server.

Assign the AWS DataSync task to share the data as a mountable file system. Sync the file system with the application server.

Create a file gateway with AWS Storage Gateway. Create a client-side file share using the required protocol. Share the file with the application server.

Overall explanation

Amazon FSx for Lustre provides fully managed shared storage with the scalability and performance of the popular Lustre file system. It is fully managed and will allow the company to attach the file system to the origin server and connect the application server to the file system.



CORRECT: "Create an Amazon FSx for Lustre file system. Connect the file system to the origin server. Ensure that the file system is connected to the application server" is the correct answer (as explained above.)

INCORRECT: "Assign the AWS DataSync task to share the data as a mountable file system. Sync the file system with the application server" is incorrect. The solution requires a managed Lustre file system, so this would not work.

INCORRECT: "Create a file gateway with AWS Storage Gateway. Create a client-side file share using the required protocol. Share the file with the application server" is incorrect. The solution requires a managed Lustre file system, so this would not work.

INCORRECT: "Create an Amazon Elastic File System (Amazon EFS) file system and configure it to support Lustre. Attach the file system to the origin server. Connect the application server to the file system" is incorrect. The solution requires a managed Lustre file system, so this would not work.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 6Skipped

A company is storing a large quantity of small files in an Amazon S3 bucket. An application running on an Amazon EC2 instance needs permissions to access and process the files in the S3 bucket.

Which action will MOST securely grant the EC2 instance access to the S3 bucket?

Generate access keys and store the credentials on the EC2 instance for use in making API calls.

Create an IAM user for the application with specific permissions to the S3 bucket.

Correct answer

Create an IAM role with least privilege permissions and attach it to the EC2 instance profile.

Create a bucket ACL on the S3 bucket and configure the EC2 instance ID as a grantee.

Overall explanation

IAM roles should be used in place of storing credentials on Amazon EC2 instances. This is the most secure way to provide permissions to EC2 as no credentials are stored and short-lived credentials are obtained using AWS STS. Additionally, the policy attached to the role should provide least privilege permissions.

CORRECT: "Create an IAM role with least privilege permissions and attach it to the EC2 instance profile" is the correct answer.

INCORRECT: "Generate access keys and store the credentials on the EC2 instance for use in making API calls" is incorrect. This is not best practice, IAM roles are preferred.

INCORRECT: "Create an IAM user for the application with specific permissions to the S3 bucket" is incorrect. Instances should use IAM Roles for delegation not user accounts.

INCORRECT: "Create a bucket ACL on the S3 bucket and configure the EC2 instance ID as a grantee" is incorrect. You cannot configure an EC2 instance ID on a bucket ACL and bucket ACLs cannot be used to restrict access in this scenario.

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/amazon-ec2/

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

Domain

AWS Security, Identity, & Compliance

Question 7Skipped

An IoT sensor is being rolled out to thousands of a company's existing customers. The sensors will stream high volumes of data each second to a central location. A solution must be designed to ingest and store the data for analytics. The solution must provide near-real time performance and millisecond responsiveness.

Which solution should a Solutions Architect recommend?

Ingest the data into an Amazon SQS queue. Process the data using an AWS Lambda function and then store the data in Amazon DynamoDB.

Correct answer

Ingest the data into an Amazon Kinesis Data Stream. Process the data with an AWS Lambda function and then store the data in Amazon DynamoDB.

Ingest the data into an Amazon SQS queue. Process the data using an AWS Lambda function and then store the data in Amazon RedShift.

Ingest the data into an Amazon Kinesis Data Stream. Process the data with an AWS Lambda function and then store the data in Amazon RedShift.

Overall explanation

A Kinesis data stream is a set of shards. Each shard contains a sequence of data records. A **consumer** is an application that processes the data from a Kinesis data stream. You can map a Lambda function to a shared-throughput consumer (standard iterator), or to a dedicated-throughput consumer with enhanced fan-out.

Amazon DynamoDB is the best database for this use case as it supports near-real time performance and millisecond responsiveness.

CORRECT: "Ingest the data into an Amazon Kinesis Data Stream. Process the data with an AWS Lambda function and then store the data in Amazon DynamoDB" is the correct answer.

INCORRECT: "Ingest the data into an Amazon Kinesis Data Stream. Process the data with an AWS Lambda function and then store the data in Amazon RedShift" is incorrect. Amazon RedShift cannot provide millisecond responsiveness.

INCORRECT: "Ingest the data into an Amazon SQS queue. Process the data using an AWS Lambda function and then store the data in Amazon RedShift" is incorrect. Amazon SQS does not provide near real-time performance and RedShift does not provide millisecond responsiveness.

INCORRECT: "Ingest the data into an Amazon SQS queue. Process the data using an AWS Lambda function and then store the data in Amazon DynamoDB" is incorrect. Amazon SQS does not provide near real-time performance.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Application Integration

Question 8Skipped

An automotive company plans to implement IoT sensors in manufacturing equipment that will send data to AWS in real time. The solution must receive events in an ordered manner from each asset and ensure that the data is saved for future processing.

Which solution would be MOST efficient?

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

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

Correct answer

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

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

Overall explanation

Amazon Kinesis Data Streams is the ideal service for receiving streaming data. The Amazon Kinesis Client Library (KCL) delivers all records for a given partition key to the same record processor, making it easier to build multiple applications reading from the same Amazon Kinesis data stream. Therefore, a separate partition (rather than shard) should be used for each equipment asset.

Amazon Kinesis Firehose can be used to receive streaming data from Data Streams and then load the data into Amazon S3 for future processing.

CORRECT: "Use Amazon Kinesis Data Streams for real-time events with a partition for each equipment asset. 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 equipment asset. Use Amazon Kinesis Data Firehose to save data to Amazon EBS" is incorrect. A partition should be used rather than a shard as explained above.

INCORRECT: "Use an Amazon SQS FIFO queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function for the SQS queue to save data to Amazon EFS" is incorrect. Amazon SQS cannot be used for real-time use cases.

INCORRECT: "Use an Amazon SQS standard queue for real-time events with one queue for each equipment asset. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3" is incorrect. Amazon SQS cannot be used for real-time use cases.

References:

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

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

Save time with our AWS cheat sheets:

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

Domain

AWS Application Integration

Question 9Skipped

An application upgrade caused some issues with stability. The application owner enabled logging and has generated a 5 GB log file in an Amazon S3 bucket. The log file must be securely shared with the application vendor to troubleshoot the issues.

What is the MOST secure way to share the log file?

Create an IAM user for the vendor to provide access to the S3 bucket and the application. Enforce multi-factor authentication.

Create access keys using an administrative account and share the access key ID and secret access key with the vendor.

Correct answer

Generate a presigned URL and ask the vendor to download the log file before the URL expires.

Enable default encryption for the bucket and public access. Provide the S3 URL of the file to the vendor.

Overall explanation

A presigned URL gives you access to the object identified in the URL. When you create a presigned URL, you must provide your security credentials and then specify a bucket name, an object key, an HTTP method (PUT for uploading objects), and an expiration date and time. The presigned URLs are valid only for the specified duration. That is, you must start the action before the expiration date and time.

This is the most secure way to provide the vendor with time-limited access to the log file in the S3 bucket.

CORRECT: "Generate a presigned URL and ask the vendor to download the log file before the URL expires" is the correct answer.

INCORRECT: "Create an IAM user for the vendor to provide access to the S3 bucket and the application. Enforce multi-factor authentication" is incorrect. This is less secure as you have to create an account to access AWS and then ensure you lock down the account appropriately.

INCORRECT: "Create access keys using an administrative account and share the access key ID and secret access key with the vendor" is incorrect. This is extremely insecure as the access keys will provide administrative permissions to AWS and should never be shared.

INCORRECT: "Enable default encryption for the bucket and public access. Provide the S3 URL of the file to the vendor" is incorrect. Encryption does not assist here as the bucket would be public and anyone could access it.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 10Skipped

A solutions architect is designing a two-tier web application. The application consists of a public-facing web tier hosted on Amazon EC2 in public subnets. The database tier consists of Microsoft SQL Server running on Amazon EC2 in a private subnet. Security is a high priority for the company.

How should security groups be configured in this situation? (Select TWO.)

Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier

Correct selection

Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0 and to allow outbound traffic on port 1433 to the RDS

Correct selection

Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier

Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0

Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier

Overall explanation

In this scenario an inbound rule is required to allow traffic from any internet client to the web front end on SSL/TLS port 443. The source should therefore be set to 0.0.0.0/0 to allow any inbound traffic.

To secure the connection from the web frontend to the database tier, an outbound rule should be created from the public EC2 security group with a destination of the private EC2 security group. The port should be set to 1433 for MySQL. The private EC2 security group will also need to allow inbound traffic on 1433 from the public EC2 security group.

This configuration can be seen in the diagram:

CORRECT: "Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0 and to allow outbound traffic on port 1433 to the RDS" is a correct answer.

CORRECT: "Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier" is also a correct answer.

INCORRECT: "Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0" is incorrect as this is configured backwards.

INCORRECT: "Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier" is incorrect as the MySQL database instance does not need to send outbound traffic on either of these ports.

INCORRECT: "Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier" is incorrect as the database tier does not need to allow inbound traffic on port 443.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Security, Identity, & Compliance

Question 11Skipped

A highly sensitive application runs on Amazon EC2 instances using EBS volumes. The application stores data temporarily on Amazon EBS volumes during processing before saving results to an Amazon RDS database. The company's security team mandate that the sensitive data must be encrypted at rest.

Which solution should a Solutions Srchitect recommend to meet this requirement?

Use AWS Certificate Manager to generate certificates that can be used to encrypt the connections between the EC2 instances and RDS.

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

Use Amazon Data Lifecycle Manager to encrypt all data as it is stored to the EBS volumes and RDS database.

Correct answer

Configure encryption for the Amazon EBS volumes and Amazon RDS database with AWS KMS keys.

Overall explanation

As the data is stored both in the EBS volumes (temporarily) and the RDS database, both the EBS and RDS volumes must be encrypted at rest. This can be achieved by enabling encryption at creation time of the volume and AWS KMS keys can be used to encrypt the data. This solution meets all requirements.

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

INCORRECT: "Use AWS Certificate Manager to generate certificates that can be used to encrypt the connections between the EC2 instances and RDS" is incorrect. This would encrypt the data in-transit but not at-rest.

INCORRECT: "Use Amazon Data Lifecycle Manager to encrypt all data as it is stored to the EBS volumes and RDS database" is incorrect. DLM is used for automating the process of taking and managing snapshots for EBS volumes.

INCORRECT: "Configure SSL/TLS encryption using AWS KMS customer master keys (CMKs) to encrypt database volumes" is incorrect. You cannot configure SSL/TLS encryption using KMS CMKs or use SSL/TLS to encrypt data at rest.

References:

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

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

Save time with our AWS cheat sheets:

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

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

Domain

AWS Security, Identity, & Compliance

Question 12Skipped

An application has been migrated to Amazon EC2 Linux instances. The EC2 instances run several 1-hour tasks on a schedule. There is no common programming language among these tasks, as they were written by different teams. Currently, these tasks run on a single instance, which raises concerns about performance and scalability. To resolve these concerns, a solutions architect must implement a solution.

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

Convert the EC2 instance to a container. Use AWS App Runner to create the container on demand to run the tasks as jobs.

Use AWS Batch to run the tasks as jobs. Schedule the jobs by using Amazon EventBridge (Amazon CloudWatch Events).

Correct answer

Create an Amazon Machine Image (AMI) of the EC2 instance that runs the tasks. Create an Auto Scaling group with the AMI to run multiple copies of the instance.

Copy the tasks into AWS Lambda functions. Schedule the Lambda functions by using Amazon EventBridge (Amazon CloudWatch Events).

Overall explanation

The best solution is to create an AMI of the EC2 instance, and then use it as a template for which to launch additional instances using an Auto Scaling Group. This removes the issues of performance, scalability, and redundancy by allowing the EC2 instances to automatically scale and be launched across multiple Availability Zones.

CORRECT: "Create an Amazon Machine Image (AMI) of the EC2 instance that runs the tasks. Create an Auto Scaling group with the AMI to run multiple copies of the instance" is the correct answer (as explained above.)

INCORRECT: "Use AWS Batch to run the tasks as jobs. Schedule the jobs by using Amazon EventBridge (Amazon CloudWatch Events)" is incorrect. AWS Batch is designed to run jobs across multiple instances, there would be less operational overhead by creating an AMI instead.

INCORRECT: "Convert the EC2 instance to a container. Use AWS App Runner to create the container on demand to run the tasks as jobs" is incorrect. Converting your EC2 instances to containers is not the easiest way to achieve this task.

INCORRECT: "Copy the tasks into AWS Lambda functions. Schedule the Lambda functions by using Amazon EventBridge (Amazon CloudWatch Events)" is incorrect. The maximum execution time for a Lambda function is 15 minutes, making it unsuitable for tasks running on a one-hour schedule.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Compute

Question 13Skipped

A solutions architect has been tasked with designing a highly resilient hybrid cloud architecture connecting an on-premises data center and AWS. The network should include AWS Direct Connect (DX).

Which DX configuration offers the HIGHEST resiliency?

Configure a DX connection with an encrypted VPN on top of it.

Correct answer

Configure DX connections at multiple DX locations.

Configure multiple private VIFs on top of a DX connection.

Configure multiple public VIFs on top of a DX connection.

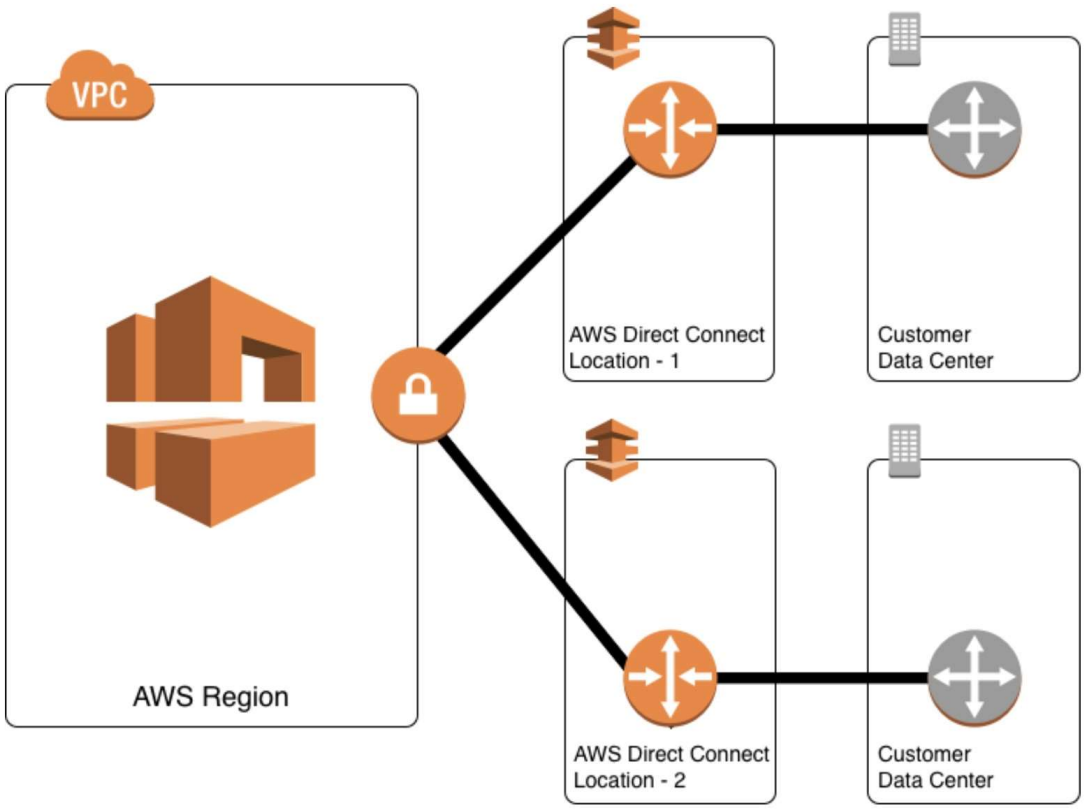
Overall explanation

The most resilient solution is to configure DX connections at multiple DX locations. This ensures that any issues impacting a single DX location do not affect availability of the network connectivity to AWS.

Take note of the following AWS recommendations for resiliency:

AWS recommends connecting from multiple data centers for physical location redundancy. When designing remote connections, consider using redundant hardware and telecommunications providers. Additionally, it is a best practice to use dynamically routed, active/active connections for automatic load balancing and failover across redundant network connections. Provision sufficient network capacity to ensure that the failure of one network connection does not overwhelm and degrade redundant connections.

The diagram below is an example of an architecture that offers high resiliency:



CORRECT: "Configure DX connections at multiple DX locations" is the correct answer.

INCORRECT: "Configure a DX connection with an encrypted VPN on top of it" is incorrect. A VPN that is separate to the DX connection can be a good backup. But a VPN on top of the DX connection does not help. Also, encryption provides security but not resilience.

INCORRECT: "Configure multiple public VIFs on top of a DX connection" is incorrect. Virtual interfaces do not add resiliency as resiliency must be designed into the underlying connection.

INCORRECT: "Configure multiple private VIFs on top of a DX connection" is incorrect. Virtual interfaces do not add resiliency as resiliency must be designed into the underlying connection.

References:

https://aws.amazon.com/directconnect/resiliency-recommendation/

Save time with our AWS cheat sheets:

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

Domain

AWS Networking & Content Delivery

Question 14Skipped

A solutions architect is finalizing the architecture for a distributed database that will run across multiple Amazon EC2 instances. Data will be replicated across all instances so the loss of an

instance will not cause loss of data. The database requires block storage with low latency and throughput that supports up to several million transactions per second per server.

Which storage solution should the solutions architect use?

Correct answer

Amazon EC2 instance store

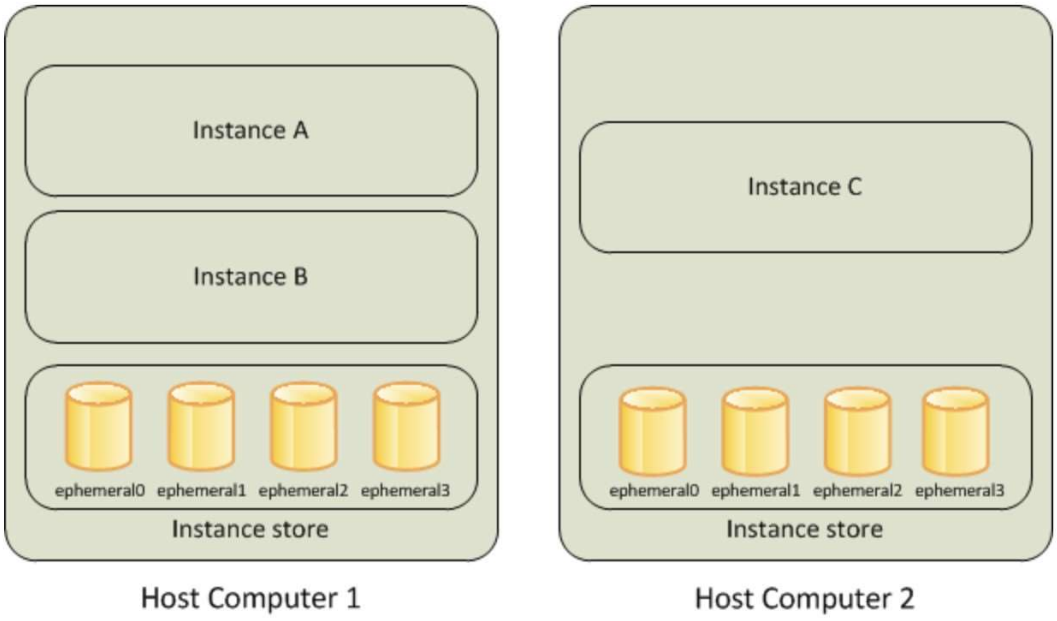
Amazon S3

Amazon EFS

Amazon EBS

Overall explanation

An *instance store* provides temporary block-level storage for your instance. This storage is located on disks that are physically attached to the host computer. Instance store is ideal for temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as a load-balanced pool of web servers.



Some instance types use NVMe or SATA-based solid state drives (SSD) to deliver high random I/O performance. This is a good option when you need storage with very low latency, but you don't need the data to persist when the instance terminates or you can take advantage of fault-tolerant architectures.

In this scenario the data is replicated and fault tolerant so the best option to provide the level of performance required is to use instance store volumes.

CORRECT: "Amazon EC2 instance store" is the correct answer.

INCORRECT: "Amazon EBS " is incorrect. The Elastic Block Store (EBS) is a block storage device but as the data is distributed and fault tolerant a better option for performance would be to use instance stores.

INCORRECT: "Amazon EFS " is incorrect as EFS is not a block device, it is a filesystem that is accessed using the NFS protocol.

INCORRECT: "Amazon S3" is incorrect as S3 is an object-based storage system, not a block-based storage system.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Compute

Question 15Skipped

A company runs an application on Amazon EC2 instances which requires access to sensitive data in an Amazon S3 bucket. All traffic between the EC2 instances and the S3 bucket must not traverse the internet and must use private IP addresses. Additionally, the bucket must only allow access from services in the VPC.

Which combination of actions should a Solutions Architect take to meet these requirements? (Select TWO.)

Create a peering connection to the S3 bucket VPC.

Enable default encryption on the bucket.

Correct selection

Apply a bucket policy to restrict access to the S3 endpoint.

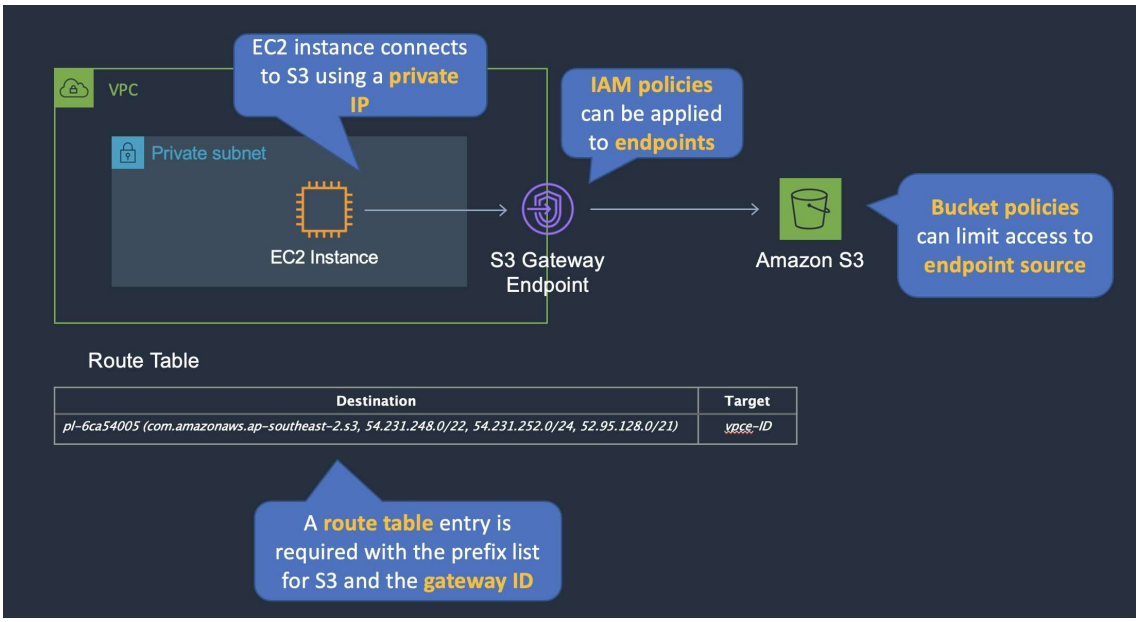
Apply an IAM policy to a VPC peering connection.

Correct selection

Create a VPC endpoint for Amazon S3.

Overall explanation

Private access to public services such as Amazon S3 can be achieved by creating a VPC endpoint in the VPC. For S3 this would be a gateway endpoint. The bucket policy can then be configured to restrict access to the S3 endpoint only which will ensure that only services originating from the VPC will be granted access.



CORRECT: "Create a VPC endpoint for Amazon S3" is a correct answer.

CORRECT: "Apply a bucket policy to restrict access to the S3 endpoint" is also a correct answer.

INCORRECT: "Enable default encryption on the bucket" is incorrect. This will encrypt data at rest but does not restrict access.

INCORRECT: "Create a peering connection to the S3 bucket VPC" is incorrect. You cannot create a peering connection to S3 as it is a public service and does not run in a VPC.

INCORRECT: "Apply an IAM policy to a VPC peering connection" is incorrect. You cannot apply an IAM policy to a peering connection.

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 16Skipped

A company is planning to upload a large quantity of sensitive data to Amazon S3. The company's security department require that the data is encrypted before it is uploaded.

Which option meets these requirements?

Use server-side encryption with customer-provided encryption keys.

Use server-side encryption with keys stored in KMS.

Correct answer

Use client-side encryption with a master key stored in AWS KMS.

Use client-side encryption with Amazon S3 managed encryption keys.

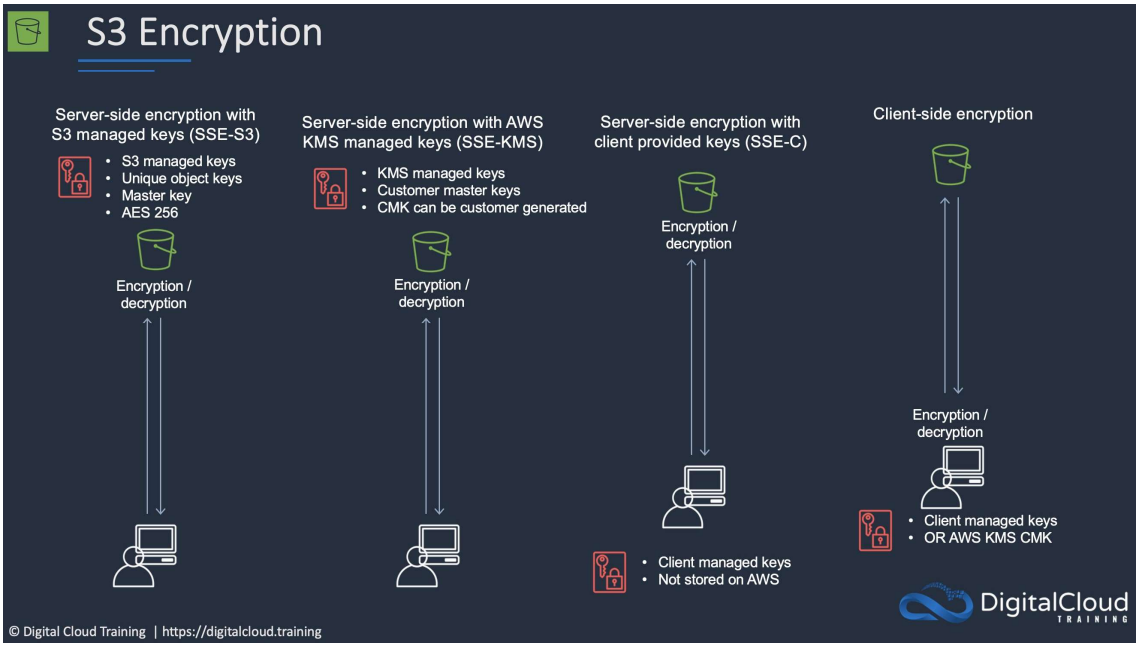
Overall explanation

The requirement is that the objects must be encrypted before they are uploaded. The only option presented that meets this requirement is to use client-side encryption. You then have two options for the keys you use to perform the encryption:

• Use a customer master key (CMK) stored in AWS Key Management Service (AWS KMS).

• Use a master key that you store within your application.

In this case the correct answer is to use an AWS KMS key. Note that you cannot use client-side encryption with keys managed by Amazon S3.



CORRECT: "Use client-side encryption with a master key stored in AWS KMS" is the correct answer.

INCORRECT: "Use client-side encryption with Amazon S3 managed encryption keys" is incorrect. You cannot use S3 managed keys with client-side encryption.

INCORRECT: "Use server-side encryption with customer-provided encryption keys" is incorrect. With this option the encryption takes place after uploading to S3.

INCORRECT: "Use server-side encryption with keys stored in KMS" is incorrect. With this option the encryption takes place after uploading to S3.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 17Skipped

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?

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)

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. Mount an instance store on each EC2 instance

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

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 Compute

Question 18Skipped

An organization manages its own MySQL databases, which are hosted on Amazon EC2 instances. In response to changes in demand, replication and scaling are manually managed by the company. It is essential for the company to have a way to add and remove compute capacity as needed from the database tier. The solution also must offer improved performance, scaling, and durability with minimal effort from operations.

Which solution meets these requirements?

Consolidate the databases into a single MySQL database. Use larger EC2 instances for the larger database.

Migrate the databases to Amazon Aurora Serverless (Aurora PostgreSQL).

For the database tier, create an EC2 Auto Scaling group. Create a new database environment and migrate the existing databases.

Correct answer

Migrate the databases to Amazon Aurora Serverless (Aurora MySQL).

Overall explanation

Amazon Aurora provides automatic scaling for MySQL databases. Amazon Aurora provides built-in security, continuous backups, serverless compute, up to 15 read replicas, automated multi-Region replication, and integrations with other AWS services. Aurora Serverless reduces any effort from operations also to provision any servers to manage the database cluster.

CORRECT: "Migrate the databases to Amazon Aurora Serverless (Aurora MySQL)" is the correct answer (as explained above.)

INCORRECT: "Migrate the databases to Amazon Aurora Serverless (Aurora PostgreSQL)" is incorrect. Although PostgreSQL is an option for Aurora, the database schema would have to be changed to allow PostgreSQL compatibility.

INCORRECT: "Consolidate the databases into a single MySQL database. Use larger EC2 instances for the larger database" is incorrect. Databases run on a larger EC2 instance would not provide improved performance, scaling, and durability.

INCORRECT: "For the database tier, create an EC2 Auto Scaling group. Create a new database environment and migrate the existing databases" is incorrect. This would improve the scalability of the solution but would still have to be heavily managed by the organization, something that would not be needed with Aurora Serverless.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Database

Question 19Skipped

A company runs a number of core enterprise applications in an on-premises data center. The data center is connected to an Amazon VPC using AWS Direct Connect. The company will be creating additional AWS accounts and these accounts will also need to be quickly, and cost-effectively connected to the on-premises data center in order to access the core applications.

What deployment changes should a Solutions Architect implement to meet these requirements with the LEAST operational overhead?

Configure VPC endpoints in the Direct Connect VPC for all required services. Route the network traffic to the on-premises servers.

Create a VPN connection between each new account and the Direct Connect VPC. Route the network traffic to the on-premises servers.

Create a Direct Connect connection in each new account. Route the network traffic to the on-premises servers.

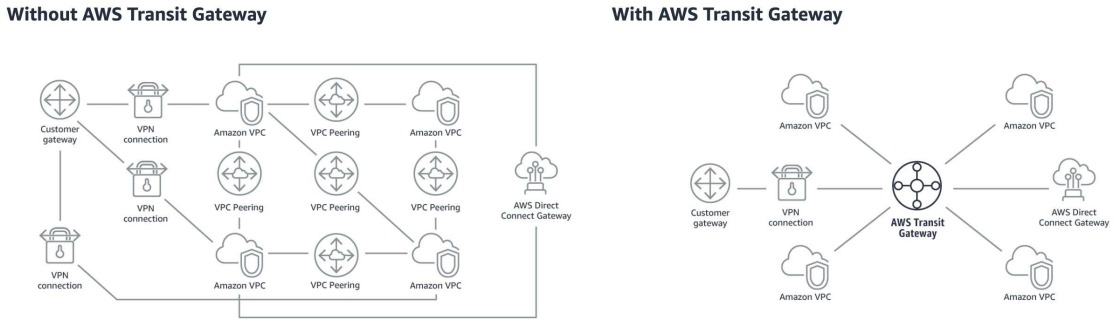
Correct answer

Configure AWS Transit Gateway between the accounts. Assign Direct Connect to the transit gateway and route network traffic to the on-premises servers.

Overall explanation

AWS Transit Gateway connects VPCs and on-premises networks through a central hub. With AWS Transit Gateway, you can quickly add Amazon VPCs, AWS accounts, VPN capacity, or AWS Direct Connect gateways to meet unexpected demand, without having to wrestle with complex connections or massive routing tables. This is the operationally least complex solution and is also cost-effective.

The image below depicts how transit gateway can assist with simplifying network deployments:



CORRECT: "Configure AWS Transit Gateway between the accounts. Assign Direct Connect to the transit gateway and route network traffic to the on-premises servers" is the correct answer.

INCORRECT: "Create a VPN connection between each new account and the Direct Connect VPC. Route the network traffic to the on-premises servers" is incorrect. You cannot connect VPCs using AWS managed VPNs and would need to configure a software VPN and then complex routing configurations. This is not the best solution.

INCORRECT: "Create a Direct Connect connection in each new account. Route the network traffic to the on-premises servers" is incorrect. This is an expensive solution as you would need to have multiple Direct Connect links.

INCORRECT: "Configure VPC endpoints in the Direct Connect VPC for all required services. Route the network traffic to the on-premises servers" is incorrect. You cannot create VPC endpoints for all services and this would be a complex solution for those you can.

References:

https://aws.amazon.com/transit-gateway/

Save time with our AWS cheat sheets:

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

Domain

AWS Networking & Content Delivery

Question 20Skipped

A company migrated a two-tier application from its on-premises data center to AWS Cloud. A Multi-AZ Amazon RDS for Oracle deployment is used for the data tier, along with 12 TB of General Purpose SSD Amazon EBS storage. With an average document size of 6 MB, the application processes, and stores documents as binary large objects (blobs) in the database.

Over time, the database size has grown, which has reduced performance and increased storage costs. A highly available and resilient solution is needed to improve database performance.

Which solution will meet these requirements MOST cost-effectively?

Correct answer

Set up an Amazon S3 bucket. The application should be updated to use S3 buckets to store documents. Store the object metadata in the existing database.

Create a table in Amazon DynamoDB and update the application to use DynamoDB. Migrate Oracle data to DynamoDB using AWS Database Migration Service (AWS DMS).

Reduce the size of the RDS DB instance. Increase the storage capacity to 24 TiB. Magnetic storage should be selected.

Increase the RDS DB instance size. Increase the storage capacity to 24 TiB. Change the storage type to Provisioned IOPS.

Overall explanation

Amazon Simple Storage Service (Amazon S3) is an object storage service offering industry-leading scalability, data availability, security, and performance. The key in this question is the reference to binary large objects (blobs) which are stored in the database. Amazon S3 is an easy to use and very cost-effective solution for Write Once Read Many (WORM) applications and use cases.

CORRECT: "Set up an Amazon S3 bucket. The application should be updated to use S3 buckets to store documents. Store the object metadata in the existing database" is the correct answer (as explained above.)

INCORRECT: "Increase the RDS DB instance size. Increase the storage capacity to 24 TiB. Change the storage type to Provisioned IOPS" is incorrect. Doing this will increase the performance of your application, however the cost will go up and not go down.

INCORRECT: "Reduce the size of the RDS DB instance. Increase the storage capacity to 24 TiB. Magnetic storage should be selected" is incorrect. Reducing the instance size will only decrease the performance of your application, alongside changing your EBS volume to a Magnetic volume.

INCORRECT: "Create a table in Amazon DynamoDB and update the application to use DynamoDB. Migrate Oracle data to DynamoDB using AWS Database Migration Service (AWS DMS)" is incorrect. DynamoDB is more expensive than Amazon S3.

References:

https://aws.amazon.com/s3/

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 21Skipped

A company is planning a migration for a high performance computing (HPC) application and associated data from an on-premises data center to the AWS Cloud. The company uses tiered storage on premises with hot high-performance parallel storage to support the application during periodic runs of the application, and more economical cold storage to hold the data when the application is not actively running.

Which combination of solutions should a solutions architect recommend to support the storage needs of the application? (Select TWO.)

Correct selection

Amazon S3 for cold data storage

Amazon S3 for high-performance parallel storage

Amazon EFS for cold data storage

Correct selection

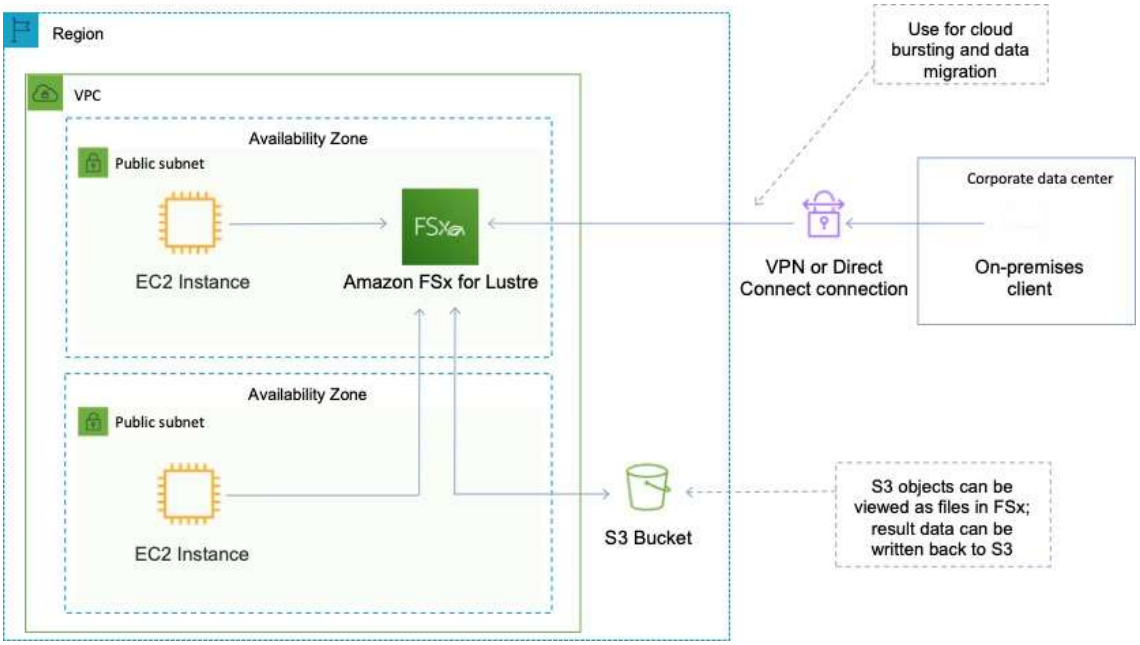
Amazon FSx for Lustre for high-performance parallel storage

Amazon FSx for Windows for high-performance parallel storage

Overall explanation

Amazon FSx for Lustre provides a high-performance file system optimized for fast processing of workloads such as machine learning, high-performance computing (HPC), video processing, financial modeling, and electronic design automation (EDA).

These workloads commonly require data to be presented via a fast and scalable file system interface, and typically have data sets stored on long-term data stores like Amazon S3.



Amazon FSx works natively with Amazon S3, making it easy to access your S3 data to run data processing workloads. Your S3 objects are presented as files in your file system, and you can write your results back to S3. This lets you run data processing workloads on FSx for Lustre and store your long-term data on S3 or on-premises data stores.

Therefore, the best combination for this scenario is to use S3 for cold data and FSx for Lustre for the parallel HPC job.

CORRECT: "Amazon S3 for cold data storage" is the correct answer.

CORRECT: "Amazon FSx for Lustre for high-performance parallel storage" is the correct answer.

INCORRECT: "Amazon EFS for cold data storage" is incorrect as FSx works natively with S3 which is also more economical.

INCORRECT: "Amazon S3 for high-performance parallel storage" is incorrect as S3 is not suitable for running high-performance computing jobs.

INCORRECT: "Amazon FSx for Windows for high-performance parallel storage" is incorrect as FSx for Lustre should be used for HPC use cases and use cases that require storing data on S3.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 22Skipped

A group of business analysts perform read-only SQL queries on an Amazon RDS database. The queries have become quite numerous and the database has experienced some performance degradation. The queries must be run against the latest data. A Solutions Architect must solve the performance problems with minimal changes to the existing web application.

What should the Solutions Architect recommend?

Export the data to Amazon S3 and instruct the business analysts to run their queries using Amazon Athena.

Load the data into Amazon ElastiCache and instruct the business analysts to run their queries against the ElastiCache endpoint.

Load the data into an Amazon Redshift cluster and instruct the business analysts to run their queries against the cluster.

Correct answer

Create a read replica of the primary database and instruct the business analysts to direct queries to the replica.

Overall explanation

The performance issues can be easily resolved by offloading the SQL queries the business analysts are performing to a read replica. This ensures that data that is being queries is up to date and the existing web application does not require any modifications to take place.

CORRECT: "Create a read replica of the primary database and instruct the business analysts to direct queries to the replica" is the correct answer.

INCORRECT: "Export the data to Amazon S3 and instruct the business analysts to run their queries using Amazon Athena" is incorrect. The data must be the latest data and this method would therefore require constant exporting of the data.

INCORRECT: "Load the data into an Amazon Redshift cluster and instruct the business analysts to run their queries against the cluster" is incorrect. This is another solution that requires exporting the loading the data which means over time it will become out of date.

INCORRECT: "Load the data into Amazon ElastiCache and instruct the business analysts to run their queries against the ElastiCache endpoint" is incorrect. It will be much easier to create a read replica. ElastiCache requires updates to the application code so should be avoided in this example.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Database

Question 23Skipped

A company has acquired another business and needs to migrate their 50TB of data into AWS within 1 month. They also require a secure, reliable and private connection to the AWS cloud.

How are these requirements best accomplished?

Provision an AWS Direct Connect connection and migrate the data over the link

Provision an AWS VPN CloudHub connection and migrate the data over redundant links

Launch a Virtual Private Gateway (VPG) and migrate the data over the AWS VPN

Correct answer

Migrate data using AWS Snowball. Provision an AWS VPN initially and order a Direct Connect link

Overall explanation

AWS Direct Connect provides a secure, reliable and private connection. However, lead times are often longer than 1 month so it cannot be used to migrate data within the timeframes. Therefore, it is better to use AWS Snowball to move the data and order a Direct Connect connection to satisfy the other requirement later on. In the meantime the organization can use an AWS VPN for secure, private access to their VPC.

CORRECT: "Migrate data using AWS Snowball. Provision an AWS VPN initially and order a Direct Connect link" is the correct answer.

INCORRECT: "Provision an AWS Direct Connect connection and migrate the data over the link" is incorrect due to the lead time for installation.

INCORRECT: "Launch a Virtual Private Gateway (VPG) and migrate the data over the AWS VPN" is incorrect. A VPG is the AWS-side of an AWS VPN. A VPN does not provide a private connection and is not reliable as you can never guarantee the latency over the Internet

INCORRECT: "Provision an AWS VPN CloudHub connection and migrate the data over redundant links" is incorrect. AWS VPN CloudHub is a service for connecting multiple sites into your VPC over VPN connections. It is not used for aggregating links and the limitations of Internet bandwidth from the company where the data is stored will still be an issue. It also uses the public Internet so is not a private or reliable connection.

References:

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

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

Save time with our AWS cheat sheets:

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

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

Domain

AWS Migration & Transfer

Question 24Skipped

A company runs several NFS file servers in an on-premises data center. The NFS servers must run periodic backups to Amazon S3 using automatic synchronization for small volumes of data.

Which solution meets these requirements and is MOST cost-effective?

Set up an SFTP sync using AWS Transfer for SFTP to sync data from on premises to Amazon S3.

Set up an AWS Direct Connect connection between the on-premises data center and AWS and copy the data to Amazon S3.

Set up AWS Glue to extract the data from the NFS shares and load it into Amazon S3.

Correct answer

Set up an AWS DataSync agent on the on-premises servers and sync the data to Amazon S3.

Overall explanation

AWS DataSync is an online data transfer service that simplifies, automates, and accelerates copying large amounts of data between on-premises systems and AWS Storage services, as well as between AWS Storage services. DataSync can copy data between Network File System (NFS) shares, or 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.

This is the most cost-effective solution from the answer options available.

CORRECT: "Set up an AWS DataSync agent on the on-premises servers and sync the data to Amazon S3" is the correct answer.

INCORRECT: "Set up an SFTP sync using AWS Transfer for SFTP to sync data from on premises to Amazon S3" is incorrect. This solution does not provide the scheduled synchronization features of AWS DataSync and is more expensive.

INCORRECT: "Set up AWS Glue to extract the data from the NFS shares and load it into Amazon S3" is incorrect. AWS Glue is an ETL service and cannot be used for copying data to Amazon S3 from NFS shares.

INCORRECT: "Set up an AWS Direct Connect connection between the on-premises data center and AWS and copy the data to Amazon S3" is incorrect. An AWS Direct Connect connection is an expensive option and no solution is provided for automatic synchronization.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 25Skipped

A solutions architect is required to move 750 TB of data from a branch office's network-attached file system to Amazon S3 Glacier. The branch office's internet connection is poor, and the solution must not saturate the connection. Normal business traffic loads must not be affected by the migration.

What is the MOST cost-effective solution?

Correct answer

Order 10 AWS Snowball appliances and select an Amazon S3 bucket as the destination. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.

Copy the files directly from the network-attached file system to Amazon S3. Build a lifecycle policy to move the S3 objects across storage classes into Amazon S3 Glacier.

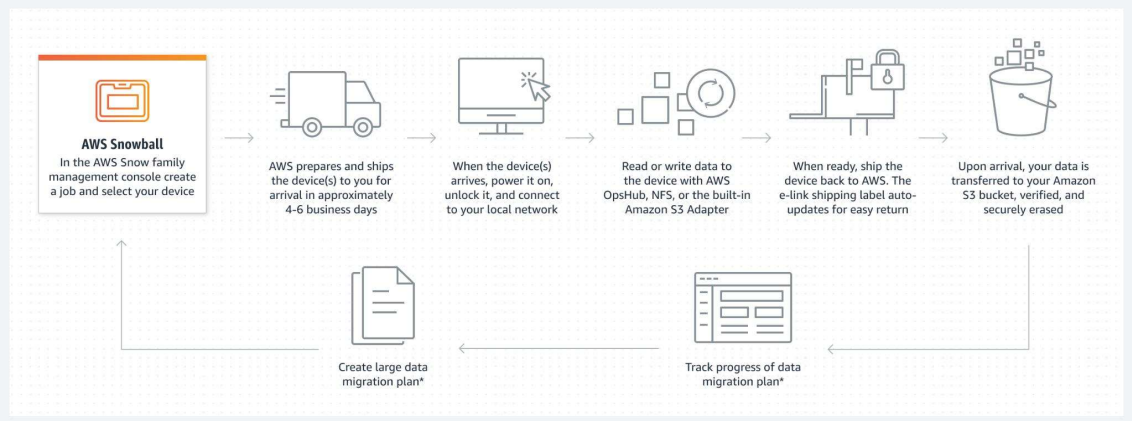
Create a site-to-site VPN connection directly to an Amazon S3 bucket, Enforce the connection with an VPC Endpoint.

Order 10 AWS Snowball appliances and point these appliances to an S3 Glacier vault and put in place a bucket policy which will only allow access via a VPC endpoint.

Overall explanation

The AWS Snow Family consists of several physical devices which can be used for edge computing, and to migrate large amounts of data into Amazon S3.

The process for using AWS Snowball is as follows:



The solutions architect will need 10 Snowball devices to fulfill the capacity required in this instance as each Snowball contains up to 80TB of usable storage.

CORRECT: "Order 10 AWS Snowball appliances and select an Amazon S3 bucket as the destination. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier" is the correct answer (as explained above.)

INCORRECT: "Create a site-to-site VPN connection directly to an Amazon S3 bucket, Enforce the connection with an VPC Endpoint" is incorrect, as although this would achieve the solution, it would be using the branch's internet connection and would saturate it - preventing normal business activities from taking place.

INCORRECT: "Order 10 AWS Snowball appliances and point these appliances to an S3 Glacier vault and put in place a bucket policy which will only allow access via a VPC endpoint" is incorrect as S3 Glacier is not a viable destination for Snowball, and you need to place it into S3 Standard first then transition the data in Glacier after the fact.

INCORRECT: "Copy the files directly from the network-attached file system to Amazon S3. Build a lifecycle policy to move the S3 objects across storage classes into Amazon S3 Glacier" is incorrect. It is not possible to mount third-party NAS appliance to an S3 bucket. You could use a service like AWS DataSync to move data from the network attached file system into S3, however this would still be traveling over the branch's internet line.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Migration & Transfer

Question 26Skipped

A company runs an application in an Amazon VPC that requires access to an Amazon Elastic Container Service (Amazon ECS) cluster that hosts an application in another VPC. The company's security team requires that all traffic must not traverse the internet.

Which solution meets this requirement?

Configure an Amazon Route 53 private hosted zone for each VPC. Use private records to resolve internal IP addresses in each VPC.

Correct answer

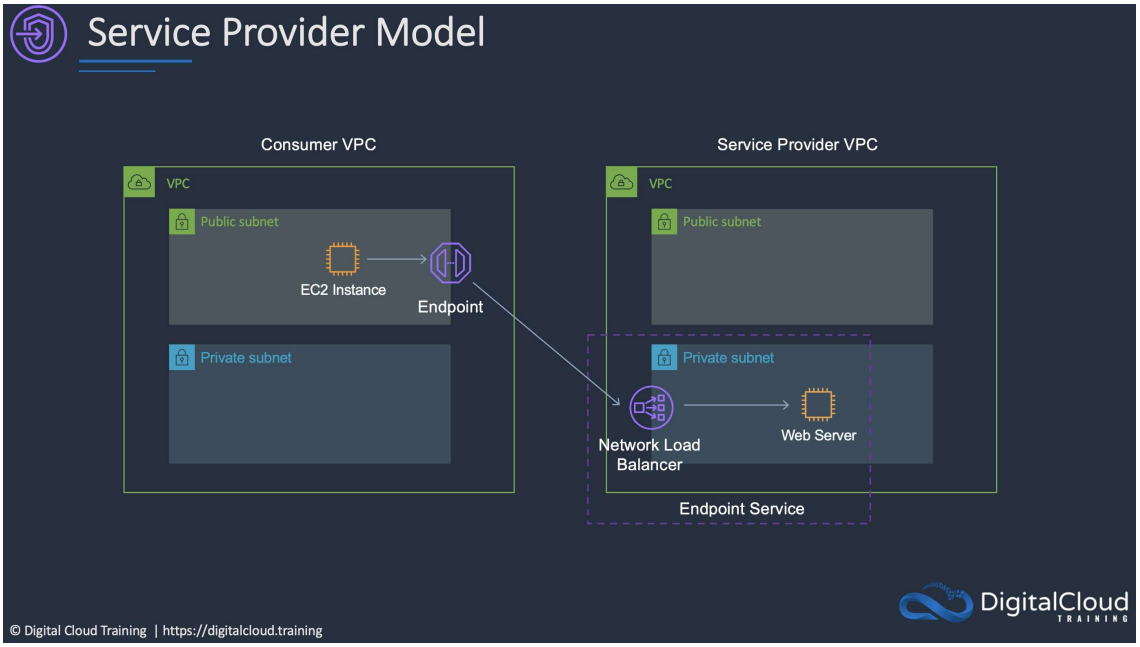
Create a Network Load Balancer in one VPC and an AWS PrivateLink endpoint for Amazon ECS in another VPC.

Configure a gateway endpoint for Amazon ECS. Update the route table to include an entry pointing to the ECS cluster.

Create a Network Load Balancer and AWS PrivateLink endpoint for Amazon ECS in the VPC that hosts the ECS cluster.

Overall explanation

The correct solution is to use AWS PrivateLink in a service provider model. In this configuration a network load balancer will be implemented in the service provider VPC (the one with the ECS cluster in this example), and a PrivateLink endpoint will be created in the consumer VPC (the one with the company's application).



CORRECT: "Create a Network Load Balancer in one VPC and an AWS PrivateLink endpoint for Amazon ECS in another VPC" is the correct answer.

INCORRECT: "Create a Network Load Balancer and AWS PrivateLink endpoint for Amazon ECS in the VPC that hosts the ECS cluster" is incorrect. The endpoint should be in the consumer VPC, not the service provider VPC (see the diagram above).

INCORRECT: "Configure a gateway endpoint for Amazon ECS. Update the route table to include an entry pointing to the ECS cluster" is incorrect. You cannot use a gateway endpoint to connect to a private service. Gateway endpoints are only for S3 and DynamoDB.

INCORRECT: "Configure an Amazon Route 53 private hosted zone for each VPC. Use private records to resolve internal IP addresses in each VPC" is incorrect. This does not provide a mechanism for resolving each other's addresses and there's no method of internal communication using private IPs such as VPC peering.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Networking & Content Delivery

Question 27Skipped

To accelerate experimentation and agility, a company allows developers to apply existing IAM policies to existing IAM roles. Nevertheless, the security operations team is concerned that the developers could attach the existing administrator policy, circumventing any other security policies.

How should a solutions architect address this issue?

Correct answer

Set a permissions boundary on the developer IAM role that denies attaching administrator access.

Assign all IAM duties to the security operations team and prevent developers from attaching policies.

Disable IAM activity across all organizational accounts using service control policies.

Send an alert every time a developer creates a new policy using an Amazon SNS topic.

Overall explanation

Setting a permissions boundary is the easiest and safest way to ensure that any IAM users cannot assume any elevated permissions. A permissions boundary is an advanced feature for using a managed policy to set the maximum permissions that an identity-based policy can grant to an IAM entity. An entity's permissions boundary allows it to perform only the actions that are allowed by both its identity-based policies and its permissions boundaries.

CORRECT: "Set a permissions boundary on the developer IAM role that denies attaching administrator access" is the correct answer (as explained above.)

INCORRECT: "Send an alert every time a developer creates a new policy using an Amazon SNS topic" is incorrect. This does not explicitly prevent any developers from attaching the policy, only sending a notification.

INCORRECT: "Disable IAM activity across all organizational accounts using service control policies" is incorrect. If all IAM activity was disabled across all accounts within the Organizational unit, each IAM user would not be able to do anything within the account.

INCORRECT: "Assign all IAM duties to the security operations team and prevent developers from attaching policies" is incorrect. The easiest way to do this is to use a permissions boundary, to make sure the permissions are being administered appropriately.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Security, Identity, & Compliance

Question 28Skipped

A company have 500 TB of data in an on-premises file share that needs to be moved to Amazon S3 Glacier. The migration must not saturate the company's low-bandwidth internet connection and the migration must be completed within a few weeks.

What is the MOST cost-effective solution?

Order 7 AWS Snowball appliances and select an S3 Glacier vault as the destination. Create a bucket policy to enforce a VPC endpoint

Correct answer

Order 7 AWS Snowball appliances and select an Amazon S3 bucket as the destination. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier

Use AWS Global Accelerator to accelerate upload and optimize usage of the available bandwidth

Create an AWS Direct Connect connection and migrate the data straight into Amazon Glacier

Overall explanation

As the company's internet link is low-bandwidth uploading directly to Amazon S3 (ready for transition to Glacier) would saturate the link. The best alternative is to use AWS Snowball appliances. The Snowball edge appliance can hold up to 80 TB of data so 7 devices would be required to migrate 500 TB of data.

Snowball moves data into AWS using a hardware device and the data is then copied into an Amazon S3 bucket of your choice. From there, lifecycle policies can transition the S3 objects to Amazon S3 Glacier.

CORRECT: "Order 7 AWS Snowball appliances and select an Amazon S3 bucket as the destination. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier" is the correct answer.

INCORRECT: "Order 7 AWS Snowball appliances and select an S3 Glacier vault as the destination. Create a bucket policy to enforce a VPC endpoint" is incorrect as you cannot set a Glacier vault as the destination, it must be an S3 bucket. You also can't enforce a VPC endpoint using a bucket policy.

INCORRECT: "Create an AWS Direct Connect connection and migrate the data straight into Amazon Glacier" is incorrect as this is not the most cost-effective option and takes time to setup.

INCORRECT: "Use AWS Global Accelerator to accelerate upload and optimize usage of the available bandwidth" is incorrect as this service is not used for accelerating or optimizing the upload of data from on-premises networks.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Migration & Transfer

Question 29Skipped

A company is deploying a new web application that will run on Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. The application requires a shared storage solution that offers strong consistency as the content will be regularly updated.

Which solution requires the LEAST amount of effort?

Correct answer

Create an Amazon Elastic File System (Amazon EFS) file system and mount it on the individual Amazon EC2 instances

Create an Amazon S3 bucket to store the web content and use Amazon CloudFront to deliver the content

Create a shared Amazon Block Store (Amazon EBS) volume and mount it on the individual Amazon EC2 instances

Create a volume gateway using AWS Storage Gateway to host the data and mount it to the Auto Scaling group

Overall explanation

Amazon EFS is a fully-managed service that makes it easy to set up, scale, and cost-optimize file storage in the Amazon Cloud. EFS file systems are accessible to Amazon EC2 instances via a file system interface (using standard operating system file I/O APIs) and support full file system access semantics (such as strong consistency and file locking).

EFS is a good solution for when you need to attach a shared filesystem to multiple EC2 instances across multiple Availability Zones.

CORRECT: "Create an Amazon Elastic File System (Amazon EFS) file system and mount it on the individual Amazon EC2 instances" is the correct answer.

INCORRECT: "Create an Amazon S3 bucket to store the web content and use Amazon CloudFront to deliver the content" is incorrect as this may require more effort in terms of reprogramming the application to use the S3 API.

INCORRECT: "Create a shared Amazon Block Store (Amazon EBS) volume and mount it on the individual Amazon EC2 instances" is incorrect. Please note that you can multi-attach an EBS volume to multiple EC2 instances but the instances must be in the same AZ.

INCORRECT: "Create a volume gateway using AWS Storage Gateway to host the data and mount it to the Auto Scaling group" is incorrect as a storage gateway is used on-premises.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 30Skipped

A solutions architect is optimizing a website for real-time streaming and on-demand videos. The website's users are located around the world and the solutions architect needs to optimize the performance for both the real-time and on-demand streaming.

Which service should the solutions architect choose?

Amazon S3 Transfer Acceleration

Amazon Route 53

AWS Global Accelerator

Correct answer

Amazon CloudFront

Overall explanation

Amazon CloudFront can be used to stream video to users across the globe using a wide variety of protocols that are layered on top of HTTP. This can include both on-demand video as well as real time streaming video.

CORRECT: "Amazon CloudFront" is the correct answer.

INCORRECT: "AWS Global Accelerator" is incorrect as this would be an expensive way of getting the content closer to users compared to using CloudFront. As this is a use case for CloudFront and there are so many edge locations it is the better option.

INCORRECT: "Amazon Route 53" is incorrect as you still need a solution for getting the content closer to users.

INCORRECT: "Amazon S3 Transfer Acceleration" is incorrect as this is used to accelerate uploads of data to Amazon S3 buckets.

References:

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

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/on-demand-streaming-video.html

Save time with our AWS cheat sheets:

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

Domain

AWS Networking & Content Delivery

Question 31Skipped

An application uses Amazon EC2 instances and an Amazon RDS MySQL database. The database is not currently encrypted. A solutions architect needs to apply encryption to the database for all new and existing data.

How should this be accomplished?

Correct answer

Take a snapshot of the RDS instance. Create an encrypted copy of the snapshot. Restore the RDS instance from the encrypted snapshot

Enable encryption for the database using the API. Take a full snapshot of the database. Delete old snapshots

Create an RDS read replica with encryption at rest enabled. Promote the read replica to master and switch the application over to the new master. Delete the old RDS instance

Create an Amazon ElastiCache cluster and encrypt data using the cache nodes

Overall explanation

There are some limitations for encrypted Amazon RDS DB Instances: you can't modify an existing unencrypted Amazon RDS DB instance to make the instance encrypted, and you can't create an encrypted read replica from an unencrypted instance.

However, you can use the Amazon RDS snapshot feature to encrypt an unencrypted snapshot that's taken from the RDS database that you want to encrypt. Restore a new RDS DB instance from the encrypted snapshot to deploy a new encrypted DB instance. Finally, switch your connections to the new DB instance.

CORRECT: "Take a snapshot of the RDS instance. Create an encrypted copy of the snapshot. Restore the RDS instance from the encrypted snapshot" is the correct answer.

INCORRECT: "Create an Amazon ElastiCache cluster and encrypt data using the cache nodes" is incorrect as you cannot encrypt an RDS database using an ElastiCache cache node.

INCORRECT: "Enable encryption for the database using the API. Take a full snapshot of the database. Delete old snapshots" is incorrect as you cannot enable encryption for an existing database.

INCORRECT: "Create an RDS read replica with encryption at rest enabled. Promote the read replica to master and switch the application over to the new master. Delete the old RDS instance" is incorrect as you cannot create an encrypted read replica from an unencrypted database instance.

References:

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

https://aws.amazon.com/premiumsupport/knowledge-center/rds-encrypt-instance-mysql-mariadb/

Save time with our AWS cheat sheets:

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

Domain

AWS Database

Question 32Skipped

A company allows its developers to attach existing IAM policies to existing IAM roles to enable faster experimentation and agility. However, the security operations team is concerned that the developers could attach the existing administrator policy, which would allow the developers to circumvent any other security policies.

How should a solutions architect address this issue?

Prevent the developers from attaching any policies and assign all IAM duties to the security operations team

Correct answer

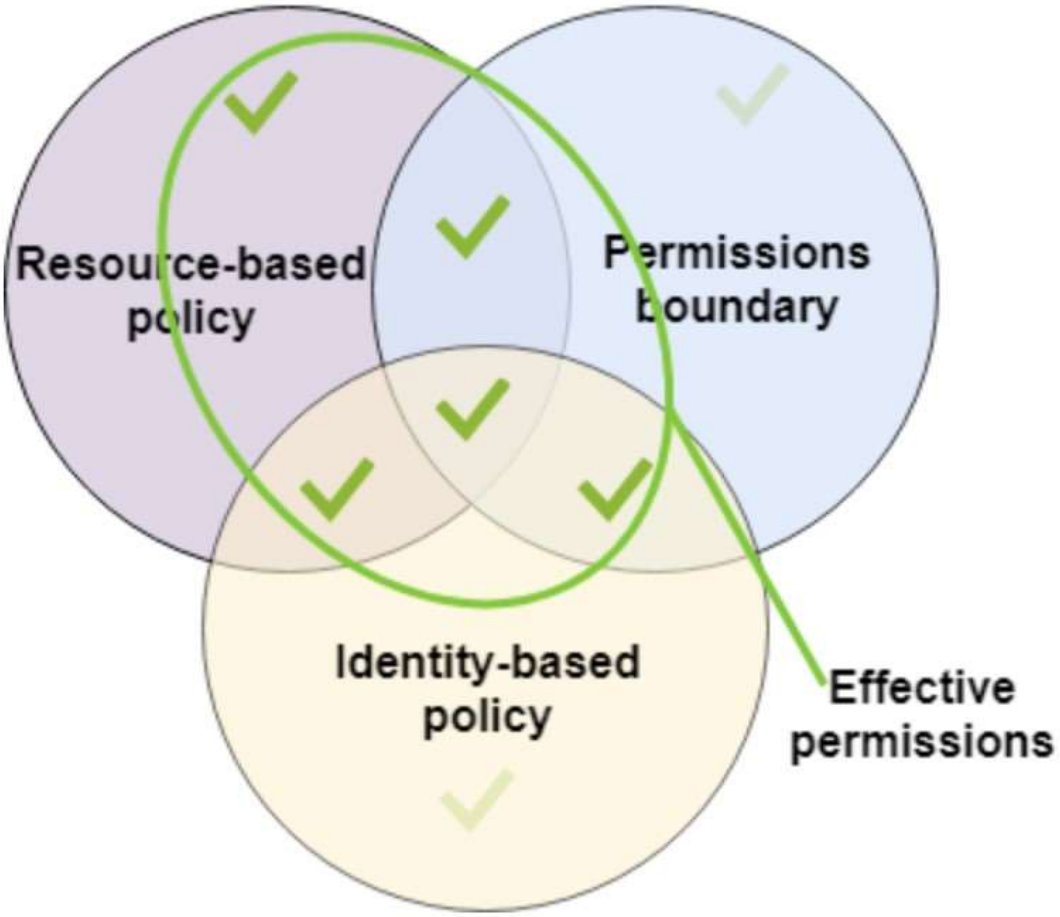
Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy

Create an Amazon SNS topic to send an alert every time a developer creates a new policy

Use service control policies to disable IAM activity across all accounts in the organizational unit

Overall explanation

The permissions boundary for an IAM entity (user or role) sets the maximum permissions that the entity can have. This can change the effective permissions for that user or role. The effective permissions for an entity are the permissions that are granted by all the policies that affect the user or role. Within an account, the permissions for an entity can be affected by identity-based policies, resource-based policies, permissions boundaries, Organizations SCPs, or session policies.



Therefore, the solutions architect can set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy.

CORRECT: "Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy" is the correct answer.

INCORRECT: "Create an Amazon SNS topic to send an alert every time a developer creates a new policy" is incorrect as this would mean investigating every incident which is not an efficient solution.

INCORRECT: "Use service control policies to disable IAM activity across all accounts in the organizational unit" is incorrect as this would prevent the developers from being able to work with IAM completely.

INCORRECT: "Prevent the developers from attaching any policies and assign all IAM duties to the security operations team" is incorrect as this is not necessary. The requirement is to allow developers to work with policies, the solution needs to find a secure way of achieving this.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Security, Identity, & Compliance

Question 33Skipped

IAM permissions-related Access Denied errors and Unauthorized errors need to be analyzed and troubleshooted by a company. AWS CloudTrail has been enabled at the company.

Which solution will meet these requirements with the LEAST effort?

Search CloudTrail logs with Amazon RedShift. Create a dashboard to identify the errors

Correct answer

Search CloudTrail logs with Amazon QuickSight. Create a dashboard to identify the errors.

Create a custom script and execute it against CloudTrail logs to find errors using AWS Batch

Write custom scripts to query CloudTrail logs using AWS Glue

Overall explanation

CloudTrail logs are stored natively within an S3 bucket , which can then be easily integrated with Amazon QuickSight. Amazon QuickSight is a data visualization tool which will show any IAM permissions-related Access Denied errors and Unauthorized errors.

CORRECT: "Search CloudTrail logs with Amazon QuickSight. Create a dashboard to identify the errors" is the correct answer (as explained above.)

INCORRECT: "Create a custom script and execute it against CloudTrail logs to find errors using AWS Batch" is incorrect. Writing custom scripts is inevitably more effort than using the native connection between AWS CloudTrail and Amazon QuickSight.

INCORRECT: "Search CloudTrail logs with Amazon RedShift. Create a dashboard to identify the errors" is incorrect. Amazon RedShift would not be a simple way of achieving this outcome.

INCORRECT: "Write custom scripts to query CloudTrail logs using AWS Glue" is incorrect. AWS Batch requires configuring several EC2 instances to run jobs for you. This, and writing custom scripts will significantly increase the effort involved.

References:

https://docs.aws.amazon.com/quicksight/latest/user/logging-using-cloudtrail.html

Save time with our AWS cheat sheets:

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

Domain

AWS Analytics

Question 34Skipped

A Solutions Architect must select the most appropriate database service for two use cases. A team of data scientists perform complex queries on a data warehouse that take several hours to complete. Another team of scientists need to run fast, repeat queries and update dashboards for customer support staff.

Which solution delivers these requirements MOST cost-effectively?

RedShift for the analytics use case and RDS for the customer support dashboard

RDS for both use cases

Correct answer

RedShift for both use cases

RedShift for the analytics use case and ElastiCache in front of RedShift for the customer support dashboard

Overall explanation

RedShift is a columnar data warehouse DB that is ideal for running long complex queries. RedShift can also improve performance for repeat queries by caching the result and returning the cached result when queries are re-run. Dashboard, visualization, and business intelligence (BI) tools that execute repeat queries see a significant boost in performance due to result caching.

CORRECT: "RedShift for both use cases" is the correct answer.

INCORRECT: "RDS for both use cases" is incorrect. RDS may be a good fit for the fast queries (not for the complex queries) but you now have multiple DBs to manage and multiple sets of data which is not going to be cost-effective.

INCORRECT: "RedShift for the analytics use case and ElastiCache in front of RedShift for the customer support dashboard" is incorrect. You could put ElastiCache in front of the RedShift DB and this would provide good performance for the fast, repeat queries. However, it is not essential and would add cost to the solution so is not the most cost-effective option available.

INCORRECT: "RedShift for the analytics use case and RDS for the customer support dashboard" is incorrect as RedShift is a better fit for both use cases.

References:

https://aws.amazon.com/about-aws/whats-new/2017/11/amazon-redshift-introduces-result-caching-for-sub-second-response-for-repeat-queries/

Save time with our AWS cheat sheets:

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

Domain

AWS Database

Question 35Skipped

A web application that allows users to upload and share documents is running on a single Amazon EC2 instance with an Amazon EBS volume. To increase availability the architecture has been updated to use an Auto Scaling group of several instances across Availability Zones behind an Application Load Balancer. After the change users can only see a subset of the documents.

What is the BEST method for a solutions architect to modify the solution so users can see all documents?

Use Sticky Sessions with the ALB to ensure users are directed to the same EC2 instance in a session

Run a script to synchronize the data between Amazon EBS volumes

Configure the Application Load Balancer to send the request to all servers. Return each document from the correct server

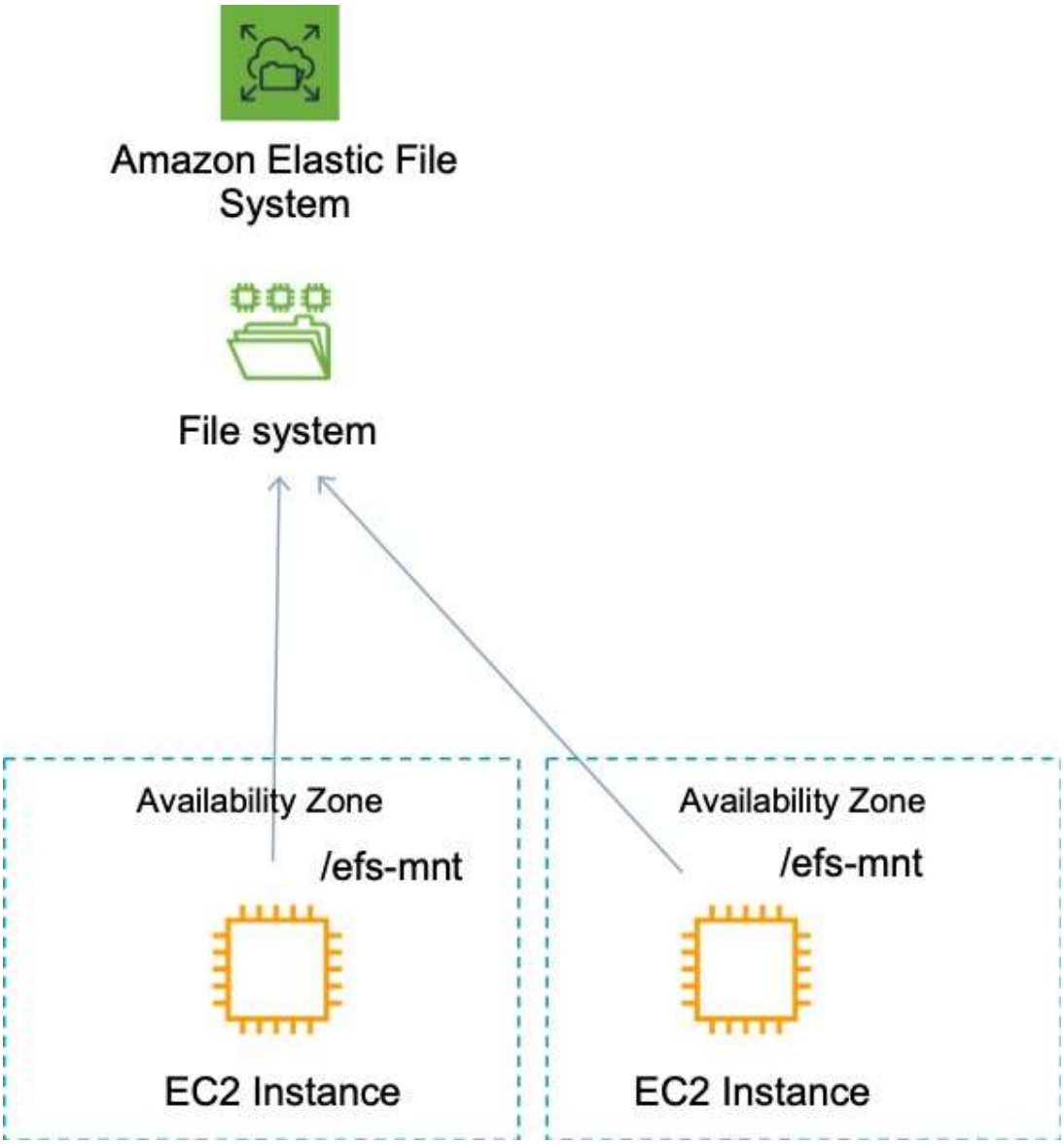
Correct answer

Copy the data from all EBS volumes to Amazon EFS. Modify the application to save new documents to Amazon EFS

Overall explanation

The problem that is being described is that the users are uploading the documents to an individual EC2 instance with a local EBS volume. Therefore, as EBS volumes cannot be shared across AZs, the data is stored separately and the ALB will be distributing incoming connections to different instances / data sets.

The simple resolution is to implement a shared storage layer for the documents so that they can be stored in one place and seen by any user who connects no matter which instance they connect to.



CORRECT: "Copy the data from all EBS volumes to Amazon EFS. Modify the application to save new documents to Amazon EFS" is the correct answer.

INCORRECT: "Run a script to synchronize the data between Amazon EBS volumes" is incorrect. This is a complex and messy approach. A better solution is to use a shared storage layer.

INCORRECT: "Use Sticky Sessions with the ALB to ensure users are directed to the same EC2 instance in a session" is incorrect as this will just “stick” a user to the same instance. They won’t see documents uploaded to other instances / EBS volumes.

INCORRECT: "Configure the Application Load Balancer to send the request to all servers. Return each document from the correct server" is incorrect as there is no mechanism here for selecting a specific document. The requirement also requests that all documents are visible.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 36Skipped

A company has refactored a legacy application to run as two microservices using Amazon ECS. The application processes data in two parts and the second part of the process takes longer than the first.

How can a solutions architect integrate the microservices and allow them to scale independently?

Implement code in microservice 1 to send data to an Amazon S3 bucket. Use S3 event notifications to invoke microservice 2

Implement code in microservice 1 to publish data to an Amazon SNS topic. Implement code in microservice 2 to subscribe to this topic

Implement code in microservice 1 to send data to Amazon Kinesis Data Firehose. Implement code in microservice 2 to read from Kinesis Data Firehose

Correct answer

Implement code in microservice 1 to send data to an Amazon SQS queue. Implement code in microservice 2 to process messages from the queue

Overall explanation

This is a good use case for Amazon SQS. The microservices must be decoupled so they can scale independently. An Amazon SQS queue will enable microservice 1 to add messages to the queue. Microservice 2 can then pick up the messages and process them. This ensures that if there's a spike in traffic on the frontend, messages do not get lost due to the backend process not being ready to process them.

CORRECT: "Implement code in microservice 1 to send data to an Amazon SQS queue. Implement code in microservice 2 to process messages from the queue" is the correct answer.

INCORRECT: "Implement code in microservice 1 to send data to an Amazon S3 bucket. Use S3 event notifications to invoke microservice 2" is incorrect as a message queue would be preferable to an S3 bucket.

INCORRECT: "Implement code in microservice 1 to publish data to an Amazon SNS topic. Implement code in microservice 2 to subscribe to this topic" is incorrect as notifications to topics are pushed to subscribers. In this case we want the second microservice to pickup the messages when ready (pull them).

INCORRECT: "Implement code in microservice 1 to send data to Amazon Kinesis Data Firehose. Implement code in microservice 2 to read from Kinesis Data Firehose" is incorrect as this is not how Firehose works. Firehose sends data directly to destinations, it is not a message queue.

References:

https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html

Save time with our AWS cheat sheets:

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

Domain

AWS Application Integration

Question 37Skipped

A company uses a Microsoft Windows file share for storing documents and media files. Users access the share using Microsoft Windows clients and are authenticated using the company's Active Directory. The chief information officer wants to move the data to AWS as they are approaching capacity limits. The existing user authentication and access management system should be used.

How can a Solutions Architect meet these requirements?

Move the documents and media files to an Amazon FSx for Lustre file system.

Correct answer

Move the documents and media files to an Amazon FSx for Windows File Server file system.

Move the documents and media files to an Amazon Elastic File System and use POSIX permissions.

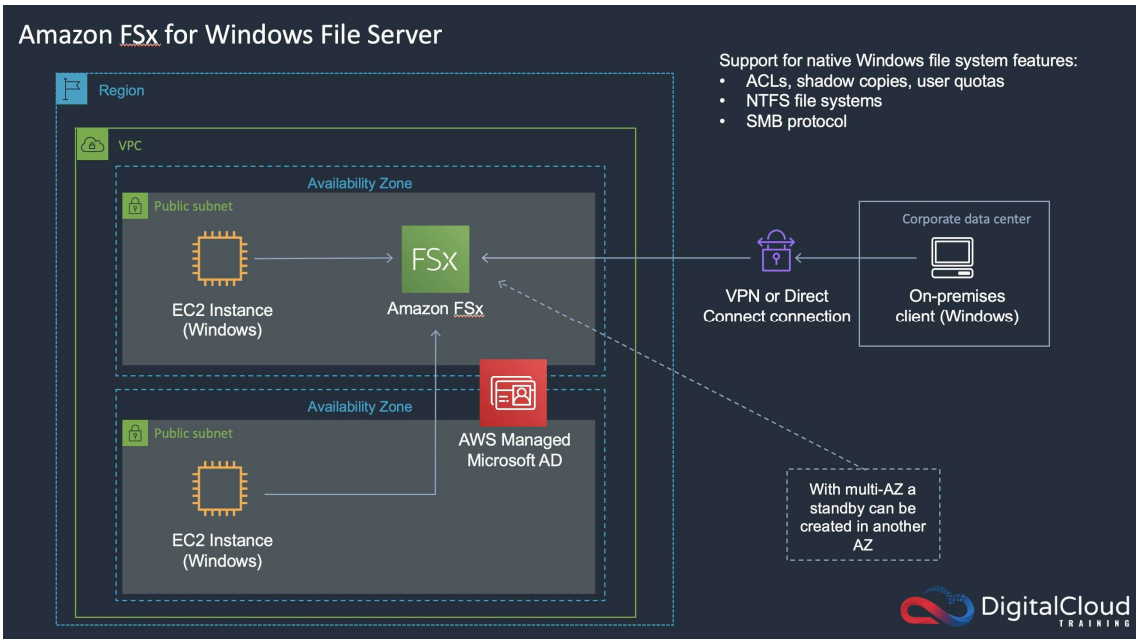
Move the documents and media files to an Amazon Simple Storage Service bucket and apply bucket ACLs.

Overall explanation

Amazon FSx for Windows File Server makes it easy for you to launch and scale reliable, performant, and secure shared file storage for your applications and end users. With Amazon FSx, you can launch highly durable and available file systems that can span multiple availability zones (AZs) and can be accessed from up to thousands of compute instances using the industry-standard Server Message Block (SMB) protocol.

It provides a rich set of administrative and security features, and integrates with Microsoft Active Directory (AD). To serve a wide spectrum of workloads, Amazon FSx provides high levels of file system throughput and IOPS and consistent sub-millisecond latencies.

You can also mount FSx file systems from on-premises using a VPN or Direct Connect connection. This topology is depicted in the image below:



CORRECT: "Move the documents and media files to an Amazon FSx for Windows File Server file system" is the correct answer.

INCORRECT: "Move the documents and media files to an Amazon FSx for Lustre file system" is incorrect. FSx for Lustre is not suitable for migrating a Microsoft Windows File Server implementation.

INCORRECT: "Move the documents and media files to an Amazon Elastic File System and use POSIX permissions" is incorrect. EFS can be used from on-premises over a VPN or DX connection but POSIX permissions are very different to Microsoft permissions and mean a different authentication and access management solution is required.

INCORRECT: "Move the documents and media files to an Amazon Simple Storage Service bucket and apply bucket ACLs" is incorrect. S3 with bucket ACLs would be changing to an object-based storage system and a completely different authentication and access management solution.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 38Skipped

A company runs an eCommerce application that uses an Amazon Aurora database. The database performs well except for short periods when monthly sales reports are run. A Solutions Architect has reviewed metrics in Amazon CloudWatch and found that the Read Ops and CPUUtilization metrics are spiking during the periods when the sales reports are run.

What is the MOST cost-effective solution to solve this performance issue?

Modify the Aurora database to use an instance class with more CPU.

Create an Amazon Redshift data warehouse and run the reporting there.

Correct answer

Create an Aurora Replica and use the replica endpoint for reporting.

Enable storage Auto Scaling for the Amazon Aurora database.

Overall explanation

The simplest and most cost-effective option is to use an Aurora Replica. The replica can serve read operations which will mean the reporting application can run reports on the replica endpoint without causing any performance impact on the production database.

CORRECT: "Create an Aurora Replica and use the replica endpoint for reporting" is the correct answer.

INCORRECT: "Enable storage Auto Scaling for the Amazon Aurora database" is incorrect. Aurora storage automatically scales based on volumes, there is no storage auto scaling feature for Aurora.

INCORRECT: "Create an Amazon Redshift data warehouse and run the reporting there" is incorrect. This would be less cost-effective and require more work in copying the data to the data warehouse.

INCORRECT: "Modify the Aurora database to use an instance class with more CPU" is incorrect. This may not resolve the storage performance issues and could be more expensive depending on instances sizes.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Database

Question 39Skipped

An application running on Amazon ECS processes data and then writes objects to an Amazon S3 bucket. The application requires permissions to make the S3 API calls.

How can a Solutions Architect ensure the application has the required permissions?

Correct answer

Create an IAM role that has read/write permissions to the bucket and update the task definition to specify the role as the taskRoleArn.

Update the S3 policy in IAM to allow read/write access from Amazon ECS, and then relaunch the container.

Attach an IAM policy with read/write permissions to the bucket to an IAM group and add the container instances to the group.

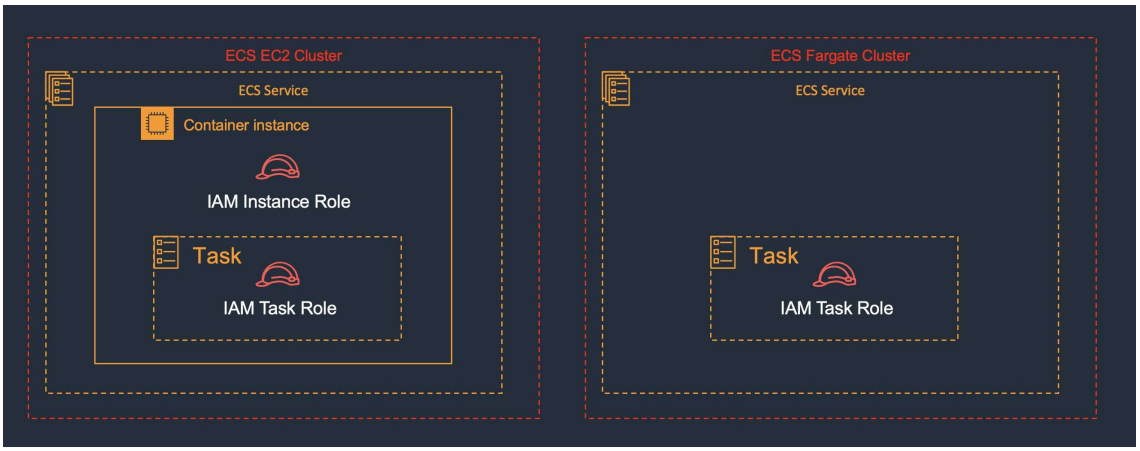
Create a set of Access Keys with read/write permissions to the bucket and update the task credential ID.

Overall explanation

With IAM roles for Amazon ECS tasks, you can specify an IAM role that can be used by the containers in a task. Applications must sign their AWS API requests with AWS credentials, and this feature provides a strategy for managing credentials for your applications to use, similar to the way that Amazon EC2 instance profiles provide credentials to EC2 instances.

You define the IAM role to use in your task definitions, or you can use a taskRoleArn override when running a task manually with the RunTask API operation.

Note that there are instances roles and task roles that you can assign in ECS when using the EC2 launch type. The task role is better when you need to assign permissions for just that specific task:



CORRECT: "Create an IAM role that has read/write permissions to the bucket and update the task definition to specify the role as the taskRoleArn" is the correct answer.

INCORRECT: "Update the S3 policy in IAM to allow read/write access from Amazon ECS, and then relaunch the container" is incorrect. Policies must be assigned to tasks using IAM Roles and this is not mentioned here.

INCORRECT: "Create a set of Access Keys with read/write permissions to the bucket and update the task credential ID" is incorrect. You cannot update the task credential ID with access keys and roles should be used instead.

INCORRECT: "Attach an IAM policy with read/write permissions to the bucket to an IAM group and add the container instances to the group" is incorrect. You cannot add container instances to an IAM group.

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 Security, Identity, & Compliance

Question 40Skipped

A company wants to migrate a legacy web application from an on-premises data center to AWS. The web application consists of a web tier, an application tier, and a MySQL database. The company does not want to manage instances or clusters.

Which combination of services should a solutions architect include in the overall architecture? (Select TWO.)

Amazon Kinesis Data Streams

Correct selection

AWS Fargate

Amazon EC2 Spot Instances

Correct selection

Amazon RDS for MySQL

Amazon DynamoDB

Overall explanation

Amazon RDS is a managed service and you do not need to manage the instances. This is an ideal backend for the application and you can run a MySQL database on RDS without any refactoring. For the application components these can run on Docker containers with AWS Fargate. Fargate is a serverless service for running containers on AWS.

CORRECT: "AWS Fargate" is a correct answer.

CORRECT: "Amazon RDS for MySQL" is also a correct answer.

INCORRECT: "Amazon DynamoDB" is incorrect. This is a NoSQL database and would be incompatible with the relational MySQL DB.

INCORRECT: "Amazon EC2 Spot Instances" is incorrect. This would require managing instances.

INCORRECT: "Amazon Kinesis Data Streams" is incorrect. This is a service for streaming data.

References:

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

https://aws.amazon.com/fargate/

Save time with our AWS cheat sheets:

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

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

Domain

AWS Database

Question 41Skipped

Some objects that are uploaded to Amazon S3 standard storage class are initially accessed frequently for a period of 30 days. Then, objects are infrequently accessed for up to 90 days. After that, the objects are no longer needed.

How should lifecycle management be configured?

Transition to REDUCED_REDUNDANCY after 30 days. After 90 days expire the objects

Correct answer

Transition to ONEZONE_IA after 30 days. After 90 days expire the objects

Transition to STANDARD_IA after 30 days. After 90 days transition to ONEZONE_IA

Transition to STANDARD_IA after 30 days. After 90 days transition to GLACIER

Overall explanation

In this scenario we need to keep the objects in the STANDARD storage class for 30 days as the objects are being frequently accessed. We can configure a lifecycle action that then transitions the objects to INTELLIGENT_TIERING, STANDARD_IA, or ONEZONE_IA. After that we don't need the objects so they can be expired.

All other options do not meet the stated requirements or are not supported lifecycle transitions. For example:

· You cannot transition to REDUCED_REDUNDANCY from any storage class.

· Transitioning from STANDARD_IA to ONEZONE_IA is possible but we do not want to keep the objects so it incurs unnecessary costs.

· Transitioning to GLACIER is possible but again incurs unnecessary costs.

CORRECT: "Transition to ONEZONE_IA after 30 days. After 90 days expire the objects " is the correct answer.

INCORRECT: "Transition to STANDARD_IA after 30 days. After 90 days transition to GLACIER" is incorrect.

INCORRECT: "Transition to STANDARD_IA after 30 days. After 90 days transition to ONEZONE_IA" is incorrect.

INCORRECT: "Transition to REDUCED_REDUNDANCY after 30 days. After 90 days expire the objects " is incorrect.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 42Skipped

A company needs to store data from an application. Data in the application changes frequently. All levels of stored data must be audited under a new regulation which the company adheres to.

Application storage capacity is running out on the company's on-premises infrastructure. To comply with the new regulation, a solutions architect must offload some data securely to AWS to relieve the on-premises capacity issues.

Which solution will meet these requirements?

Move the existing data to Amazon S3 with AWS Snowcone. Using AWS CloudTrail, you can log management events.

The existing data can be transferred to Amazon S3 with the help of Amazon S3 Transfer Acceleration. Log data events using AWS CloudTrail.

Correct answer

Use AWS Storage Gateway to move the existing data to Amazon S3. Use AWS CloudTrail to log management events.

Move existing data to Amazon S3 using AWS DataSync. Log data events using AWS CloudTrail.

Overall explanation

AWS Storage Gateway is a set of hybrid cloud storage services that provide on-premises access to virtually unlimited cloud storage. Secondly AWS CloudTrail monitors and records account activity across your AWS infrastructure, giving you control over storage, analysis, and remediation actions.

CORRECT: "Use AWS Storage Gateway to move the existing data to Amazon S3. Use AWS CloudTrail to log management events" is the correct answer (as explained above.)

INCORRECT: "Move existing data to Amazon S3 using AWS DataSync. Log data events using AWS CloudTrail" is incorrect. AWS DataSync is a secure, online service that automates and accelerates moving data between on-premises and AWS storage service and is not designed as a hybrid storage service.

INCORRECT: "The existing data can be transferred to Amazon S3 with the help of Amazon S3 Transfer Acceleration. Log data events using AWS CloudTrail" is incorrect. Amazon S3 Transfer Acceleration is a bucket-level feature that enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. Transfer Acceleration is designed to optimize transfer speeds from across the world into S3 buckets and is not a migration service.

INCORRECT: "Move the existing data to Amazon S3 with AWS Snowcone. Using AWS CloudTrail, you can log management events" is incorrect. AWS Snowcone is not suitable as a hybrid cloud service.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Migration & Transfer

Question 43Skipped

An Amazon RDS PostgreSQL database is configured as Multi-AZ. A solutions architect needs to scale read performance and the solution must be configured for high availability. What is the most cost-effective solution?

Deploy a read replica in a different AZ to the master DB instance

Deploy a read replica using Amazon ElastiCache

Deploy a read replica in the same AZ as the master DB instance

Correct answer

Create a read replica as a Multi-AZ DB instance

Overall explanation

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

CORRECT: "Create a read replica as a Multi-AZ DB instance" is the correct answer.

INCORRECT: "Deploy a read replica in a different AZ to the master DB instance" is incorrect as this does not provide high availability for the read replica

INCORRECT: "Deploy a read replica using Amazon ElastiCache" is incorrect as ElastiCache is not used to create read replicas of RDS database.

INCORRECT: "Deploy a read replica in the same AZ as the master DB instance" is incorrect as this solution does not include HA for the read replica.

References:

https://aws.amazon.com/about-aws/whats-new/2018/01/amazon-rds-read-replicas-now-support-multi-az-deployments/

Save time with our AWS cheat sheets:

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

Domain

AWS Database

Question 44Skipped

An Amazon EC2 instance runs in a VPC network, and the network must be secured by a solutions architect. The EC2 instances contain highly sensitive data and have been launched in private subnets. Company policy restricts EC2 instances that run in the VPC from accessing the internet. The instances need to access the software repositories using a third-party URL to download and install software product updates. All other internet traffic must be blocked, with no exceptions.

Which solution meets these requirements?

Create an AWS WAF web ACL. Filter traffic requests based on source and destination IP address ranges with custom rules.

Establish strict inbound rules for your security groups. Specify the URLs of the authorized software repositories on the internet in your outbound rule.

Correct answer

Configure the route table for the private subnet so that it routes the outbound traffic to an AWS Network Firewall firewall then configure domain list rule groups.

Place an Application Load Balancer in front of your EC2 instances. Direct all outbound traffic to the ALB. For outbound access to the internet, use a URL-based rule listener in the ALB's target group.

Overall explanation

The AWS Network Firewall is a managed service that makes it easy to deploy essential network protections for all your Amazon Virtual Private Clouds, and you can then use domain list rules to block HTTP or HTTPS traffic to domains identified as low-reputation, or that are known or suspected to be associated with malware or botnets.

CORRECT: "Configure the route table for the private subnet so that it routes the outbound traffic to an AWS Network Firewall firewall then configure domain list rule groups" is the correct answer (as explained above.)

INCORRECT: "Create an AWS WAF web ACL. Filter traffic requests based on source and destination IP address ranges with custom rules" is incorrect. AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits and bots that may affect availability, compromise security, or consume excessive resources. It is designed to protect your applications from malicious traffic, not your VPC.

INCORRECT: "Establish strict inbound rules for your security groups. Specify the URLs of the authorized software repositories on the internet in your outbound rule" is incorrect. You cannot specify URLs in security group rules so this would not work.

INCORRECT: "Place an Application Load Balancer in front of your EC2 instances. Direct all outbound traffic to the ALB. For outbound access to the internet, use a URL-based rule listener

in the ALB's target group" is incorrect. The ALB would not work as this sits within the VPC and is unable to control traffic entering and leaving the VPC itself.

References:

https://aws.amazon.com/network-firewall/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc

Save time with our AWS cheat sheets:

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

Domain

AWS Networking & Content Delivery

Question 45Skipped

A small Python application is used by a company to process JSON documents and output the results to a SQL database which currently lives on-premises. The application is run thousands of times every day, and the company wants to move the application to the AWS Cloud. To maximize scalability and minimize operational overhead, the company needs a highly available solution.

Which solution will meet these requirements?

Create an Amazon Elastic Block Store (Amazon EBS) volume for the JSON documents. Attach the volume to multiple Amazon EC2 instances using the EBS Multi-Attach feature. Process the documents with Python code on the EC2 instances and then extract the results to an Amazon RDS DB instance.

Build an S3 bucket to place the JSON documents in. Run the Python code on multiple Amazon EC2 instances to process the documents. Store the results in a database using the Amazon Aurora Database engine.

Correct answer

Put the JSON documents in an Amazon S3 bucket. As documents arrive in the S3 bucket, create an AWS Lambda function that runs Python code to process them. Use Amazon Aurora DB clusters to store the results.

The JSON documents should be queued as messages in the Amazon Simple Queue Service (Amazon SQS). Using the Amazon Elastic Container Service (Amazon ECS) with the Amazon EC2 launch type, deploy the Python code as a container. The container can be used to process SQS messages. Using Amazon RDS, store the results.

Overall explanation

Firstly, S3 is a highly available and durable place to store these JSON documents that will be written once and read many times (WORM). As this application runs thousands of times per day, AWS Lambda would be ideal to use as it will scale whenever the application needs to be ran, and Python is a runtime environment that is natively supported by AWS Lambda, whenever the events arrive in the S3 bucket, and this could be easily achieved using S3 event notifications. Finally Amazon Aurora is a highly available and durable AWS managed database. Amazon

Aurora automatically maintains six copies of your data across three Availability Zones (AZs) to adhere to your redundancy requirements.

CORRECT: "Put the JSON documents in an Amazon S3 bucket. As documents arrive in the S3 bucket, create an AWS Lambda function that runs Python code to process them. Use Amazon Aurora DB clusters to store the results" is the correct answer (as explained above.)

INCORRECT: "Build an S3 bucket to place the JSON documents in. Run the Python code on multiple Amazon EC2 instances to process the documents. Store the results in a database using the Amazon Aurora Database engine" is incorrect.

Multiple EC2 instances could work, however if you wanted to use EC2 to process the JSON documents you would need to either leave the EC2 instances running all the time (not cost effective) or have them spin up and spin down thousands of times per day (this would be slow and not ideal).

INCORRECT: "Create an Amazon Elastic Block Store (Amazon EBS) volume for the JSON documents. Attach the volume to multiple Amazon EC2 instances using the EBS Multi-Attach feature. Process the documents with Python code on the EC2 instances and then extract the results to an Amazon RDS DB instance" is incorrect.

EBS is not optimized for write once read many use-cases, and if you wanted to use EC2 to process the JSON documents you would need to either leave the EC2 instances running all the time (not cost effective) or have them spin up and spin down thousands of times per day (this would be slow and not ideal).

INCORRECT: "The JSON documents should be queued as messages in the Amazon Simple Queue Service (Amazon SQS). Using the Amazon Elastic Container Service (Amazon ECS) with the Amazon EC2 launch type, deploy the Python code as a container. The container can be used to process SQS messages. Using Amazon RDS, store the results" is incorrect.

A queue within Amazon SQS is not designed to be used for write once read many solutions, and it is designed to be used to decouple separate layers of your architecture. Secondly, ECS for EC2 is not ideal as you would need to either leave the EC2 instances running all the time (not cost effective) or have them spin up and spin down thousands of times per day (this would be slow and not ideal) if you wanted to use ECS for EC2.

References:

https://docs.aws.amazon.com/lambda/latest/dg/services-rds.html

Save time with our AWS cheat sheets:

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

Domain

AWS Database

Question 46Skipped

A solutions architect is designing an application on AWS. The compute layer will run in parallel across EC2 instances. The compute layer should scale based on the number of jobs to be

processed. The compute layer is stateless. The solutions architect must ensure that the application is loosely coupled and the job items are durably stored.

Which design should the solutions architect use?

Correct answer

Create an Amazon SQS queue to hold the jobs that needs to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue

Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the Auto Scaling group to add and remove nodes based on network usage

Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the Auto Scaling group to add and remove nodes based on CPU usage

Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of messages published to the SNS topic

Overall explanation

In this case we need to find a durable and loosely coupled solution for storing jobs. Amazon SQS is ideal for this use case and can be configured to use dynamic scaling based on the number of jobs waiting in the queue.

To configure this scaling you can use the *backlog per instance* metric with the target value being the *acceptable backlog per instance* to maintain. You can calculate these numbers as follows:

Backlog per instance: To calculate your backlog per instance, start with the ApproximateNumberOfMessages queue attribute to determine the length of the SQS queue (number of messages available for retrieval from the queue). Divide that number by the fleet's running capacity, which for an Auto Scaling group is the number of instances in the InService state, to get the backlog per instance.

Acceptable backlog per instance: To calculate your target value, first determine what your application can accept in terms of latency. Then, take the acceptable latency value and divide it by the average time that an EC2 instance takes to process a message.

This solution will scale EC2 instances using Auto Scaling based on the number of jobs waiting in the SQS queue.

CORRECT: "Create an Amazon SQS queue to hold the jobs that needs to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue" is the correct answer.

INCORRECT: "Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the

Auto Scaling group to add and remove nodes based on network usage" is incorrect as scaling on network usage does not relate to the number of jobs waiting to be processed.

INCORRECT: "Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the Auto Scaling group to add and remove nodes based on CPU usage" is incorrect. Amazon SNS is a notification service so it delivers notifications to subscribers. It does store data durably but is less suitable than SQS for this use case. Scaling on CPU usage is not the best solution as it does not relate to the number of jobs waiting to be processed.

INCORRECT: "Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of messages published to the SNS topic" is incorrect. Amazon SNS is a notification service so it delivers notifications to subscribers. It does store data durably but is less suitable than SQS for this use case. Scaling on the number of notifications in SNS is not possible.

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/

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

Domain

AWS Application Integration

Question 47Skipped

A company has a file share on a Microsoft Windows Server in an on-premises data center. The server uses a local network attached storage (NAS) device to store several terabytes of files. The management team require a reduction in the data center footprint and to minimize storage costs by moving on-premises storage to AWS.

What should a Solutions Architect do to meet these requirements?

Correct answer

Configure an AWS Storage Gateway file gateway.

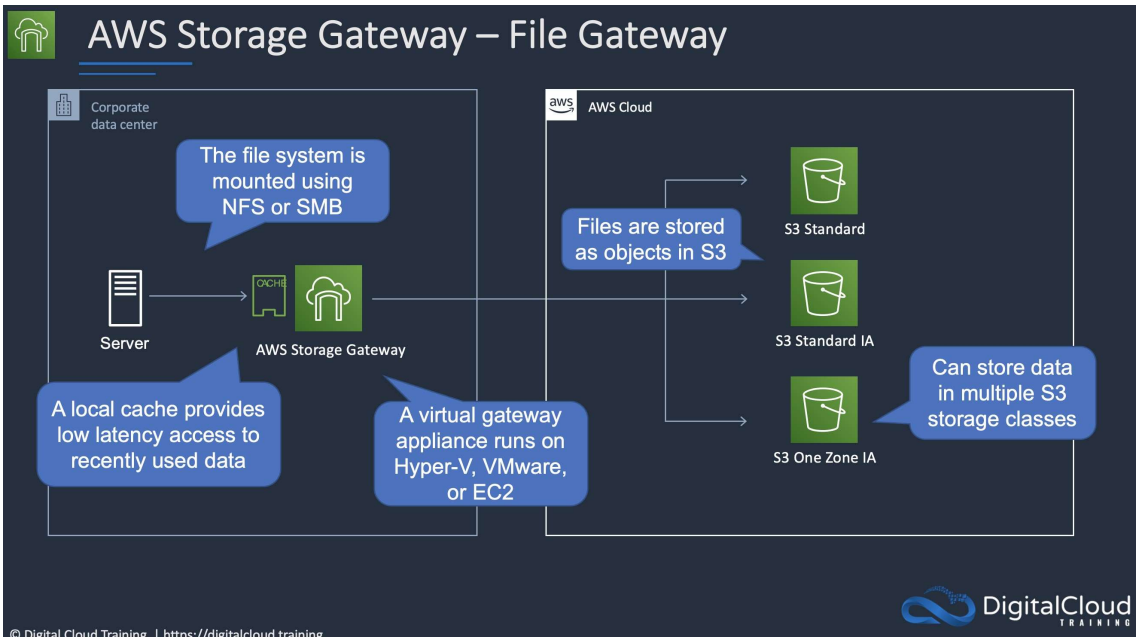
Create an Amazon EFS volume and use an IPSec VPN.

Create an Amazon S3 bucket and an S3 gateway endpoint.

Configure an AWS Storage Gateway as a volume gateway.

Overall explanation

An AWS Storage Gateway File Gateway provides your applications a file interface to seamlessly store files as objects in Amazon S3, and access them using industry standard file protocols. This removes the files from the on-premises NAS device and provides a method of directly mounting the file share for on-premises servers and clients.



CORRECT: "Configure an AWS Storage Gateway file gateway" is the correct answer.

INCORRECT: "Configure an AWS Storage Gateway as a volume gateway" is incorrect. A volume gateway uses block-based protocols. In this case we are replacing a NAS device which uses file-level protocols so the best option is a file gateway.

INCORRECT: "Create an Amazon EFS volume and use an IPSec VPN" is incorrect. EFS can be mounted over a VPN but it would have more latency than using a storage gateway.

INCORRECT: "Create an Amazon S3 bucket and an S3 gateway endpoint" is incorrect. S3 is an object-level storage system so is not suitable for this use case. A gateway endpoint is a method of accessing S3 using private addresses from your VPC, not from your data center.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 48Skipped

A company runs an internal browser-based application. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. The Auto Scaling group scales up to 20 instances during work hours, but scales down to 2 instances overnight. Staff are complaining that the application is very slow when the day begins, although it runs well by midmorning

How should the scaling be changed to address the staff complaints and keep costs to a minimum?

Correct answer

Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period

Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period

Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens

Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens

Overall explanation

Though this sounds like a good use case for scheduled actions, both answers using scheduled actions will have 20 instances running regardless of actual demand. A better option to be more cost effective is to use a target tracking action that triggers at a lower CPU threshold.

With this solution the scaling will occur before the CPU utilization gets to a point where performance is affected. This will result in resolving the performance issues whilst minimizing costs. Using a reduced cooldown period will also more quickly terminate unneeded instances, further reducing costs.

CORRECT: "Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period" is the correct answer.

INCORRECT: "Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens" is incorrect as this is not the most cost-effective option. Note you can choose min, max, or desired for a scheduled action.

INCORRECT: "Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens" is incorrect as this is not the most cost-effective option. Note you can choose min, max, or desired for a scheduled action.

INCORRECT: "Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period" is incorrect as AWS recommend you use target tracking in place of step scaling for most use cases.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Compute

Question 49Skipped

A solutions architect has created a new AWS account and must secure AWS account root user access.

Which combination of actions will accomplish this? (Select TWO.)

Correct selection

Ensure the root user uses a strong password

Delete the root user account

Store root user access keys in an encrypted Amazon S3 bucket

Add the root user to a group containing administrative permissions

Correct selection

Enable multi-factor authentication for the root user

Overall explanation

There are several security best practices for securing the root user account:

· Lock away root user access keys OR delete them if possible

· Use a strong password

· Enable multi-factor authentication (MFA)

The root user automatically has full privileges to the account and these privileges cannot be restricted so it is extremely important to follow best practice advice about securing the root user account.

CORRECT: "Ensure the root user uses a strong password" is the correct answer.

CORRECT: "Enable multi-factor authentication to the root user" is the correct answer.

INCORRECT: "Store root user access keys in an encrypted Amazon S3 bucket" is incorrect as the best practice is to lock away or delete the root user access keys. An S3 bucket is not a suitable location for storing them, even if encrypted.

INCORRECT: "Add the root user to a group containing administrative permissions" is incorrect as this does not restrict access and is unnecessary.

INCORRECT: "Delete the root user account" is incorrect as you cannot delete the root user account.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

Save time with our AWS cheat sheets:

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

Domain

AWS Security, Identity, & Compliance

Question 50Skipped

A shared services VPC is being setup for use by several AWS accounts. An application needs to be securely shared from the shared services VPC. The solution should not allow consumers to connect to other instances in the VPC.

How can this be setup with the least administrative effort? (choose 2)

Correct selection

Create a Network Load Balancer (NLB)

Setup VPC peering between each AWS VPC

Correct selection

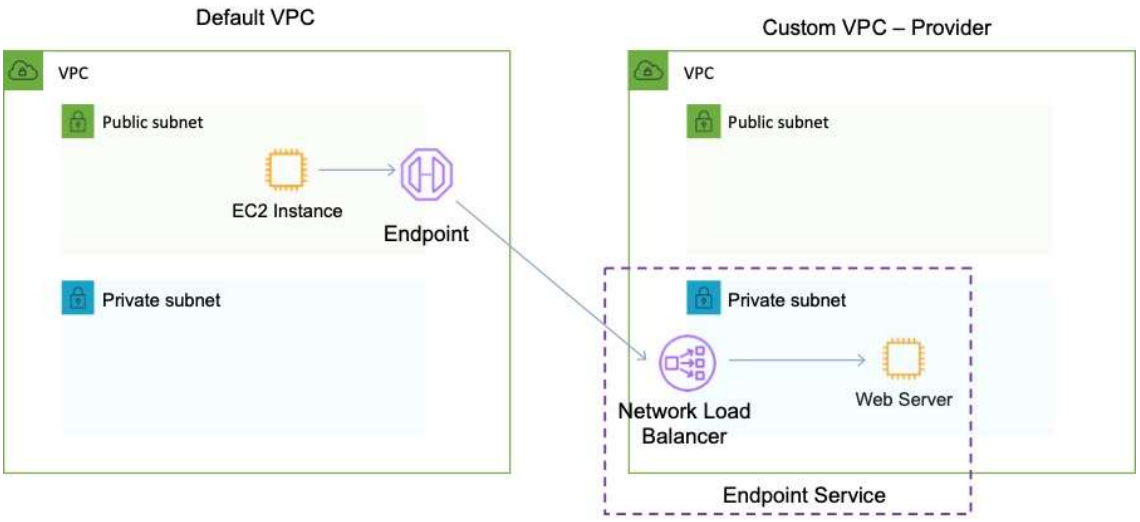
Use AWS PrivateLink to expose the application as an endpoint service

Use AWS ClassicLink to expose the application as an endpoint service

Configure security groups to restrict access

Overall explanation

VPCs can be shared among multiple AWS accounts. Resources can then be shared amongst those accounts. However, to restrict access so that consumers cannot connect to other instances in the VPC the best solution is to use PrivateLink to create an endpoint for the application. The endpoint type will be an interface endpoint and it uses an NLB in the shared services VPC.



CORRECT: "Create a Network Load Balancer (NLB)" is a correct answer.

CORRECT: "Use AWS PrivateLink to expose the application as an endpoint service" is also a correct answer.

INCORRECT: "Use AWS ClassicLink to expose the application as an endpoint service" is incorrect. ClassicLink allows you to link EC2-Classic instances to a VPC in your account, within the same region. This solution does not include EC2-Classic which is now deprecated (replaced by VPC).

INCORRECT: "Setup VPC peering between each AWS VPC" is incorrect. VPC peering could be used along with security groups to restrict access to the application and other instances in the VPC. However, this would be administratively difficult as you would need to ensure that you maintain the security groups as resources and addresses change.

INCORRECT: "Configure security groups to restrict access" is incorrect. This could be used in conjunction with VPC peering but better method is to use PrivateLink for this use case.

References:

https://aws.amazon.com/about-aws/whats-new/2018/12/amazon-virtual-private-clouds-can-now-be-shared-with-other-aws-accounts/

https://aws.amazon.com/blogs/networking-and-content-delivery/vpc-sharing-a-new-approach-to-multiple-accounts-and-vpc-management/

https://d1.awsstatic.com/whitepapers/aws-privatelink.pdf

Save time with our AWS cheat sheets:

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

Domain

AWS Networking & Content Delivery

Question 51Skipped

A company hosts a serverless application on AWS. The application consists of Amazon API Gateway, AWS Lambda, and Amazon RDS for PostgreSQL. During times of peak traffic and when traffic spikes are experienced, the company notices an increase in application errors caused by database connection timeouts. The company is looking for a solution that will reduce the number of application failures with the least amount of code changes.

What should a solutions architect do to meet these requirements?

Reduce the concurrency rate for your Lambda Function.

Change the database to an Amazon DynamoDB database with on-demand scaling.

Correct answer

Enable an RDS Proxy instance on your RDS Database.

Change the class of the instance of your database to allow more connections.

Overall explanation

Amazon RDS Proxy is a fully managed, highly available database proxy for Amazon Relational Database Service (RDS) that makes applications more scalable, more resilient to database failures, and more secure. Amazon RDS Proxy allows applications to pool and share connections established with the database, improving database efficiency and application scalability.

Amazon RDS Proxy can be enabled for most applications with no code changes so this solution requires the least amount of code changes.

CORRECT: "Enable an RDS Proxy instance on your RDS Database" is the correct answer (as explained above.)

INCORRECT: "Reduce the concurrency rate for your Lambda Function" is incorrect. Concurrency is the number of requests that your function is serving at any given time. The errors are caused by an increase in connection timeouts, so editing the concurrency of your Lambda function would not solve the problem.

INCORRECT: "Change the class of the instance of your database to allow more connections" is incorrect. Resizing the instance might help, but there will be some inevitable downtime with a PostgreSQL database on RDS. RDS Proxy is specifically designed for this reason and would incur no downtime.

INCORRECT: "Change the database to an Amazon DynamoDB database with on-demand scaling" is incorrect as this would require significant application changes to accommodate the NoSQL database structure.

References:

https://aws.amazon.com/rds/proxy/

Save time with our AWS cheat sheets:

https://digitalcloud.training/category/aws-cheat-sheets/aws-database/

Domain

AWS Database

Question 52Skipped

An application stores transactional data in an Amazon S3 bucket. The data is analyzed for the first week and then must remain immediately available and highly available for occasional analysis.

What is the MOST cost-effective storage solution that meets the requirements?

Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 7 days.

Correct answer

Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.

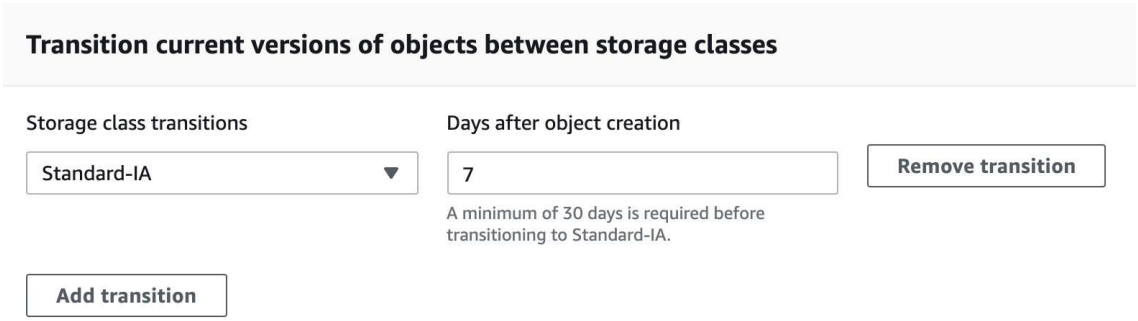
Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.

Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 7 days.

Overall explanation

The transition should be to Standard-IA rather than One Zone-IA. Though One Zone-IA would be cheaper, it also offers lower availability and the question states the objects “must remain immediately available”. Therefore the availability is a consideration.

Though there is no minimum duration when storing data in S3 Standard, you cannot transition to Standard IA within 30 days. This can be seen when trying to create a lifecycle rule:



Therefore, the best solution is to transition after 30 days.

CORRECT: "Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days" is the correct answer.

INCORRECT: "Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days" is incorrect as explained above.

INCORRECT: "Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 7 days" is incorrect as explained above.

INCORRECT: "Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 7 days" is incorrect as explained above.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 53Skipped

A gaming company uses a web application to display scores. An Application Load Balancer is used to distribute load across Amazon EC2 instances which run the application. The application stores data in an Amazon RDS for MySQL database. Users are experiencing long delays and interruptions due to poor database read performance. It is important for the company to improve the user experience while minimizing changes to the application's architecture.

What should a solutions architect do to meet these requirements?

Correct answer

Use Amazon ElastiCache to cache the database layer.

Use an Amazon DynamoDB table instead of RDS.

Connect the database and the application layer using RDS Proxy.

Use AWS Lambda instead of Amazon EC2 for the compute layer.

Overall explanation

Amazon ElastiCache is a fully managed, in-memory caching service supporting flexible, real-time use cases. You can use ElastiCache for caching, which accelerates application and database performance, or as a primary data store for use cases that don't require durability like session stores, gaming leaderboards, streaming, and analytics. ElastiCache is compatible with Redis and Memcached.

As the issues in this instance are caused by poor read performance, a caching solution would offload reads from the primary database instance and allow the application to perform better. **CORRECT:** "Use Amazon ElastiCache to cache the database layer" is the correct answer (as explained above.)

INCORRECT: "Connect the database and the application layer using RDS Proxy" is incorrect. RDS proxy allows applications to pool and share connections established with the database, improving database efficiency and application scalability. It does not however specifically improve read performance like a caching layer would.

INCORRECT: "Use AWS Lambda instead of Amazon EC2 for the compute layer" is incorrect. AWS Lambda would not be a suitable use case for hosting leaderboards, as the maximum timeout is 15 minutes, and the issue lies with the database layer, not the compute later.

INCORRECT: "Use an Amazon DynamoDB table instead of RDS" is incorrect. Migrating to DynamoDB would not help the load of reads on the database and changing the schema of the database would cause massive changes to the application's architecture.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Database

Question 54Skipped

A company requires a solution to allow customers to customize images that are stored in an online catalog. The image customization parameters will be sent in requests to Amazon API Gateway. The customized image will then be generated on-demand and can be accessed online.

The solutions architect requires a highly available solution. Which solution will be MOST cost-effective?

Correct answer

Use AWS Lambda to manipulate the original images to the requested customization. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin

Use AWS Lambda to manipulate the original images to the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Elastic Load Balancer in front of the Amazon EC2 instances

Use Amazon EC2 instances to manipulate the original images into the requested customization. Store the original and manipulated images in Amazon S3. Configure an Elastic Load Balancer in front of the EC2 instances

Use Amazon EC2 instances to manipulate the original images into the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Amazon CloudFront distribution with the S3 bucket as the origin

Overall explanation

All solutions presented are highly available. The key requirement that must be satisfied is that the solution should be cost-effective and you must choose the most cost-effective option.

Therefore, it's best to eliminate services such as Amazon EC2 and ELB as these require ongoing costs even when they're not used. Instead, a fully serverless solution should be used. AWS Lambda, Amazon S3 and CloudFront are the best services to use for these requirements.

CORRECT: "Use AWS Lambda to manipulate the original images to the requested customization. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin" is the correct answer.

INCORRECT: "Use Amazon EC2 instances to manipulate the original images into the requested customization. Store the original and manipulated images in Amazon S3. Configure an Elastic Load Balancer in front of the EC2 instances" is incorrect. This is not the most cost-effective option as the ELB and EC2 instances will incur costs even when not used.

INCORRECT: "Use AWS Lambda to manipulate the original images to the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Elastic Load Balancer in front of the Amazon EC2 instances" is incorrect. This is not the most cost-effective option as the ELB will incur costs even when not used. Also, Amazon DynamoDB will incur RCU/WCUs when running and is not the best choice for storing images.

INCORRECT: "Use Amazon EC2 instances to manipulate the original images into the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon

DynamoDB. Configure an Amazon CloudFront distribution with the S3 bucket as the origin" is incorrect. This is not the most cost-effective option as the EC2 instances will incur costs even when not used

References:

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

Save time with our AWS cheat sheets:

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

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

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

Domain

AWS Compute

Question 55Skipped

A website runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The website has a mix of dynamic and static content. Customers around the world are reporting performance issues with the website.

Which set of actions will improve website performance for users worldwide?

Launch new EC2 instances hosting the same web application in different Regions closer to the users. Use an AWS Transit Gateway to connect customers to the closest region

Create a latency-based Amazon Route 53 record for the ALB. Then launch new EC2 instances with larger instance sizes and register the instances with the ALB

Correct answer

Create an Amazon CloudFront distribution and configure the ALB as an origin. Then update the Amazon Route 53 record to point to the CloudFront distribution

Migrate the website to an Amazon S3 bucket in the Regions closest to the users. Then create an Amazon Route 53 geolocation record to point to the S3 buckets

Overall explanation

Amazon CloudFront is a content delivery network (CDN) that improves website performance by caching content at edge locations around the world. It can serve both dynamic and static content. This is the best solution for improving the performance of the website.

CORRECT: "Create an Amazon CloudFront distribution and configure the ALB as an origin. Then update the Amazon Route 53 record to point to the CloudFront distribution" is the correct answer.

INCORRECT: "Create a latency-based Amazon Route 53 record for the ALB. Then launch new EC2 instances with larger instance sizes and register the instances with the ALB" is incorrect. Latency routing routes based on the latency between the client and AWS. There is no mention in the answer about creating the new instances in another region therefore the only advantage is in

using larger instance sizes. For a dynamic site this adds complexity in keeping the instances in sync.

INCORRECT: "Launch new EC2 instances hosting the same web application in different Regions closer to the users. Use an AWS Transit Gateway to connect customers to the closest region" is incorrect as Transit Gateway is a service for connecting on-premises networks and VPCs to a single gateway.

INCORRECT: "Migrate the website to an Amazon S3 bucket in the Regions closest to the users. Then create an Amazon Route 53 geolocation record to point to the S3 buckets" is incorrect as with S3 you can only host static websites, not dynamic websites.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Networking & Content Delivery

Question 56Skipped

A website runs on a Microsoft Windows server in an on-premises data center. The web server is being migrated to Amazon EC2 Windows instances in multiple Availability Zones on AWS. The web server currently uses data stored in an on-premises network-attached storage (NAS) device.

Which replacement to the NAS file share is MOST resilient and durable?

Migrate the file share to Amazon Elastic File System (Amazon EFS)

Migrate the file share to AWS Storage Gateway

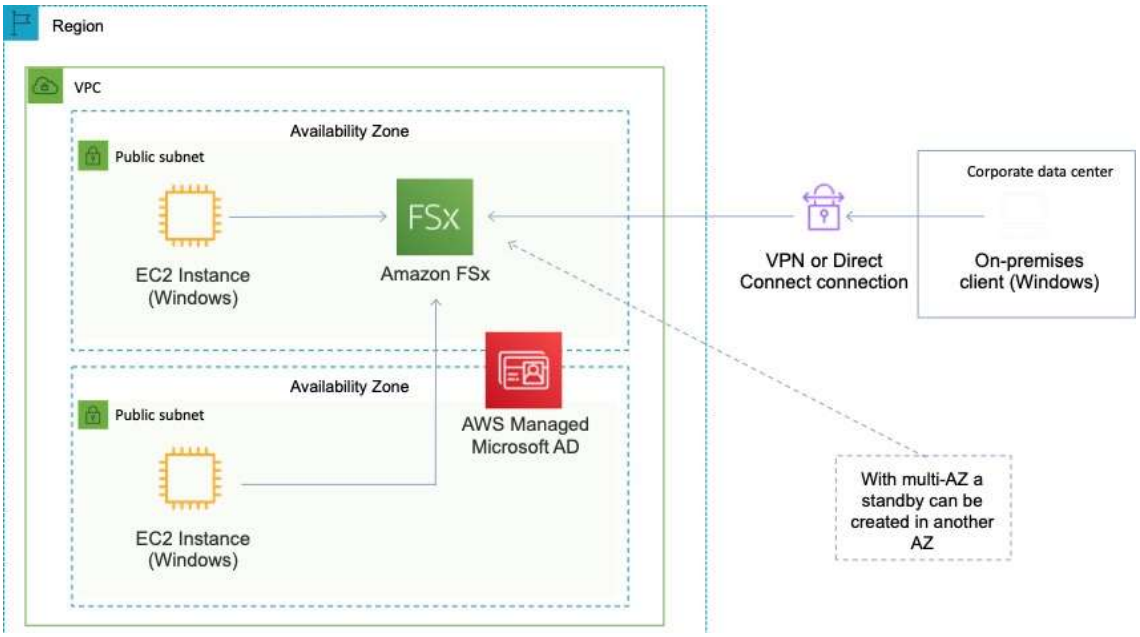
Migrate the file share to Amazon EBS

Correct answer

Migrate the file share to Amazon FSx for Windows File Server

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. It is built on Windows Server, delivering a wide range of administrative features such as user quotas, end-user file restore, and Microsoft Active Directory (AD) integration. It offers single-AZ and multi-AZ deployment options, fully managed backups, and encryption of data at rest and in transit.



This is the only solution presented that provides resilient storage for Windows instances.

CORRECT: "Migrate the file share to Amazon FSx for Windows File Server" is the correct answer.

INCORRECT: "Migrate the file share to Amazon Elastic File System (Amazon EFS)" is incorrect as you cannot use Windows instances with Amazon EFS.

INCORRECT: "Migrate the file share to Amazon EBS" is incorrect as this is not a shared storage solution for multi-AZ deployments.

INCORRECT: "Migrate the file share to AWS Storage Gateway" is incorrect as with Storage Gateway replicated files end up on Amazon S3. The replacement storage solution should be a file share, not an object-based storage system.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 57Skipped

Data from 45 TB of data is used for reporting by a company. The company wants to move this data from on premises into the AWS cloud. A custom application in the company's data center runs a weekly data transformation job and the company plans to pause the application until the data transfer is complete and needs to begin the transfer process as soon as possible.

The data center bandwidth is saturated, and a solutions architect has been tasked to transfer the data and must configure the transformation job to continue to run in the AWS Cloud.

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

The data will be moved using an AWS Snowcone device. The transformation application should be deployed to the device.

The data can be moved using AWS DataSync. Using AWS Glue, create a custom transformation job.

Order an AWS Snowball Edge Storage Optimized device that includes Amazon EC2 compute. Transfer the data to the device. Launch a new EC2 instance to run the transformation application.

Correct answer

Order an AWS Snowball Edge Storage Optimized device. Copy the data to the device. and create a custom transformation job by using AWS Glue.

Overall explanation

As the network is saturated, the solutions architect will have to use a physical solution, i.e. a member of the snow family to achieve this requirement quickly. As the data transformation job needs to be completed in the cloud, using AWS Glue will suit this requirement also. AWS Glue is a managed data transformation service.

CORRECT: "Order an AWS Snowball Edge Storage Optimized device. Copy the data to the device. and create a custom transformation job by using AWS Glue" is the correct answer (as explained above.)

INCORRECT: "The data can be moved using AWS DataSync. Using AWS Glue, create a custom transformation job" is incorrect. As the network is saturated, AWS DataSync will not work as it is primarily an online data transfer service to transfer data between a data center and AWS.

INCORRECT: "The data will be moved using an AWS Snowcone device. The transformation application should be deployed to the device" is incorrect. You would not be able to deploy a transformation service locally to the Snowcone device as it is not optimized for compute operations.

INCORRECT: "Order an AWS Snowball Edge Storage Optimized device that includes Amazon EC2 compute. Transfer the data to the device. Launch a new EC2 instance to run the transformation application" is incorrect. Using an EC2 instance instead of a managed service like AWS Glue will include more operational overhead for the organization.

References:

https://aws.amazon.com/glue/

Save time with our AWS cheat sheets:

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

Domain

AWS Migration & Transfer

Question 58Skipped

An application is running on Amazon EC2 behind an Elastic Load Balancer (ELB). Content is being published using Amazon CloudFront and you need to restrict the ability for users to circumvent CloudFront and access the content directly through the ELB.

How can you configure this solution?

Use a Network ACL to restrict access to the ELB

Use signed URLs or signed cookies to limit access to the content

Create an Origin Access Identity (OAI) and associate it with the distribution

Correct answer

Create a VPC Security Group for the ELB and use AWS Lambda to automatically update the CloudFront internal service IP addresses when they change

Overall explanation

The only way to get this working is by using a VPC Security Group for the ELB that is configured to allow only the internal service IP ranges associated with CloudFront. As these are updated from time to time, you can use AWS Lambda to automatically update the addresses. This is done using a trigger that is triggered when AWS issues an SNS topic update when the addresses are changed.

CORRECT: "Create a VPC Security Group for the ELB and use AWS Lambda to automatically update the CloudFront internal service IP addresses when they change" is the correct answer.

INCORRECT: "Create an Origin Access Identity (OAI) and associate it with the distribution" is incorrect. You can use an OAI to restrict access to content in Amazon S3 but not on EC2 or ELB.

INCORRECT: "Use signed URLs or signed cookies to limit access to the content" is incorrect. Signed cookies and URLs are used to limit access to files but this does not stop people from circumventing CloudFront and accessing the ELB directly.

INCORRECT: "Use a Network ACL to restrict access to the ELB" is incorrect. A Network ACL can be used to restrict access to an ELB but it is recommended to use security groups and this solution is incomplete as it does not account for the fact that the internal service IP ranges change over time.

References:

https://aws.amazon.com/blogs/security/how-to-automatically-update-your-security-groups-for-amazon-cloudfront-and-aws-waf-by-using-aws-lambda/

Save time with our AWS cheat sheets:

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

Domain

AWS Networking & Content Delivery

Question 59Skipped

A company has divested a single business unit and needs to move the AWS account owned by the business unit to another AWS Organization. How can this be achieved?

Migrate the account using AWS CloudFormation

Correct answer

Migrate the account using the AWS Organizations console

Create a new account in the destination AWS Organization and share the original resources using AWS Resource Access Manager

Create a new account in the destination AWS Organization and migrate resources

Overall explanation

Accounts can be migrated between organizations. To do this you must have root or IAM access to both the member and master accounts. Resources will remain under the control of the migrated account.

CORRECT: "Migrate the account using the AWS Organizations console" is the correct answer.

INCORRECT: "Create a new account in the destination AWS Organization and migrate resources" is incorrect. You do not need to create a new account in the destination AWS Organization as you can just migrate the existing account.

INCORRECT: "Create a new account in the destination AWS Organization and share the original resources using AWS Resource Access Manager" is incorrect. You do not need to create a new account in the destination AWS Organization as you can just migrate the existing account.

INCORRECT: "Migrate the account using AWS CloudFormation" is incorrect. You do not need to use AWS CloudFormation. You can use the Organizations API or AWS CLI for when there are many accounts to migrate and therefore you could use CloudFormation for any additional automation but it is not necessary for this scenario.

References:

https://aws.amazon.com/premiumsupport/knowledge-center/organizations-move-accounts/

Save time with our AWS cheat sheets:

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

Domain

AWS Management & Governance

Question 60Skipped

A company requires a solution for replicating data to AWS for disaster recovery. Currently, the company uses scripts to copy data from various sources to a Microsoft Windows file server in the on-premises data center. The company also requires that a small amount of recent files are accessible to administrators with low latency.

What should a Solutions Architect recommend to meet these requirements?

Correct answer

Update the script to copy data to an AWS Storage Gateway for File Gateway virtual appliance instead of the on-premises file server.

Update the script to copy data to an Amazon EFS volume instead of the on-premises file server.

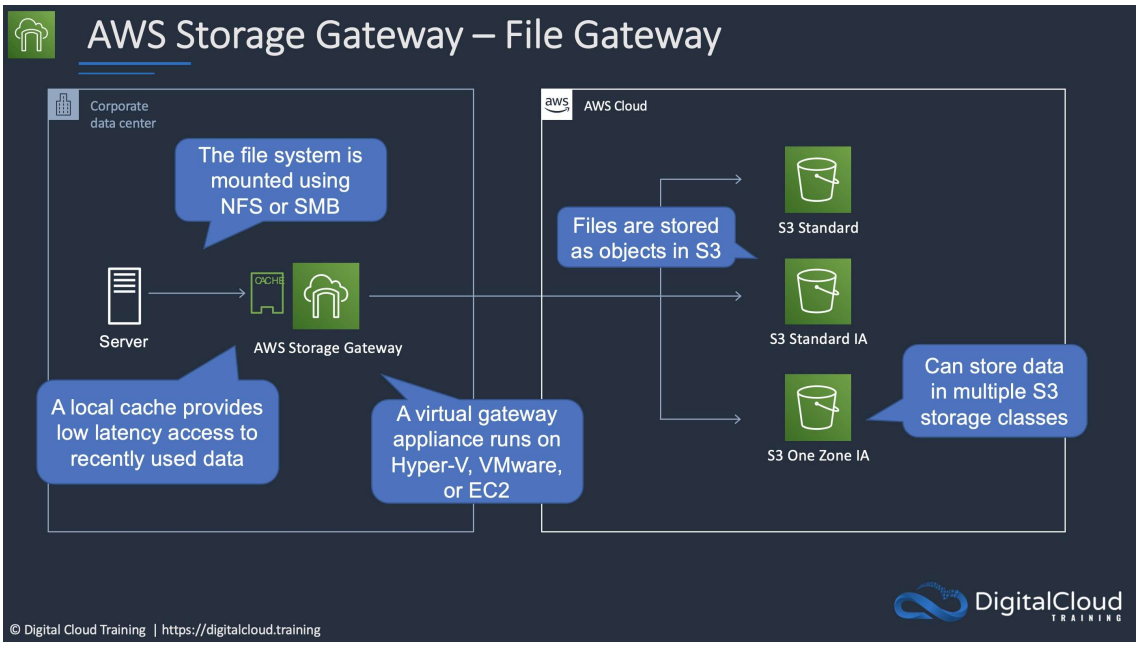
Update the script to copy data to an Amazon S3 Glacier archive instead of the on-premises file server.

Update the script to copy data to an Amazon EBS volume instead of the on-premises file server.

Overall explanation

The best solution here is to use an AWS Storage Gateway File Gateway virtual appliance in the on-premises data center. This can be accessed the same protocols as the existing Microsoft Windows File Server (SMB/CIFS). Therefore, the script simply needs to be updated to point to the gateway.

The file gateway will then store data on Amazon S3 and has a local cache for data that can be accessed at low latency. The file gateway provides an excellent method of enabling file protocol access to low cost S3 object storage.



CORRECT: "Update the script to copy data to an AWS Storage Gateway for File Gateway virtual appliance instead of the on-premises file server" is the correct answer.

INCORRECT: "Update the script to copy data to an Amazon EBS volume instead of the on-premises file server" is incorrect. This would also need an attached EC2 instance running Windows to be able to mount using the same protocols and would not offer any local low-latency access.

INCORRECT: "Update the script to copy data to an Amazon EFS volume instead of the on-premises file server" is incorrect. This solution would not provide a local cache.

INCORRECT: "Update the script to copy data to an Amazon S3 Glacier archive instead of the on-premises file server" is incorrect. This would not provide any immediate access with low-latency.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 61Skipped

A web application is being deployed on an Amazon ECS cluster using the Fargate launch type. The application is expected to receive a large volume of traffic initially. The company wishes to ensure that performance is good for the launch and that costs reduce as demand decreases

What should a solutions architect recommend?

Use Amazon EC2 Auto Scaling to scale out on a schedule and back in once the load decreases.

Use Amazon EC2 Auto Scaling with simple scaling policies to scale when an Amazon CloudWatch alarm is breached.

Use an AWS Lambda function to scale Amazon ECS based on metric breaches that trigger an Amazon CloudWatch alarm.

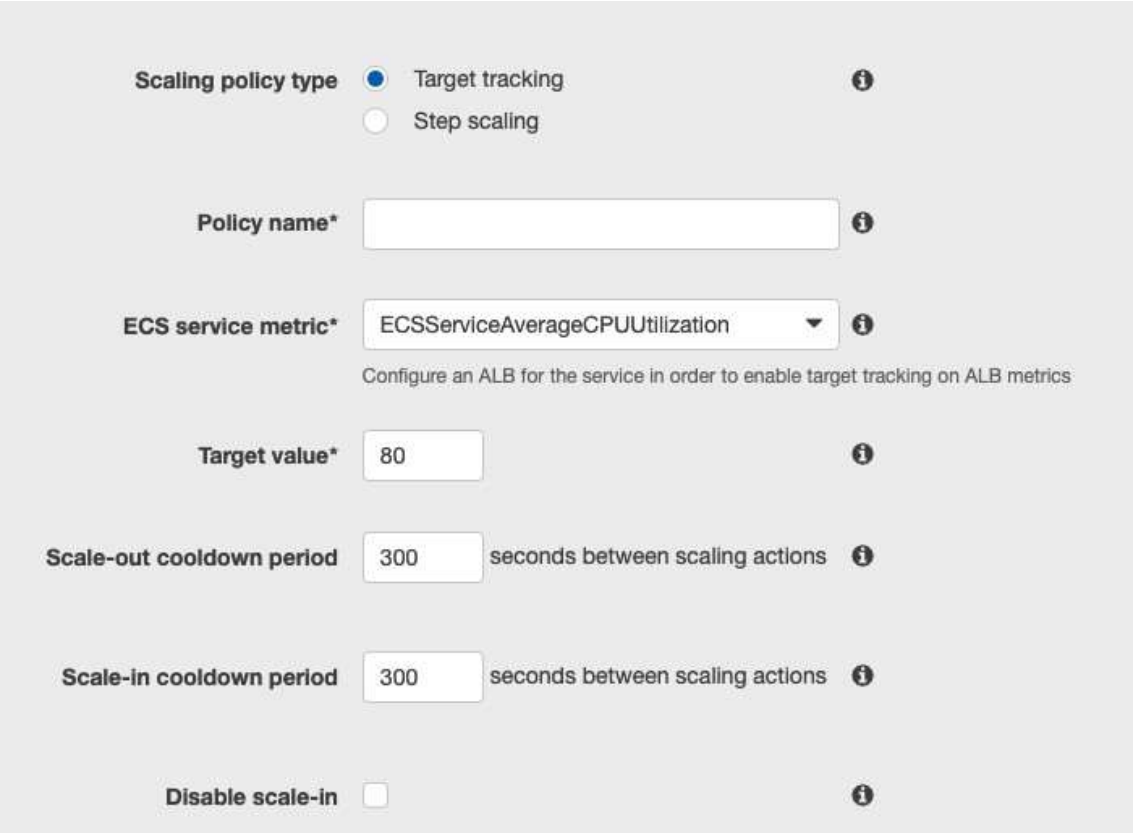
Correct answer

Use Amazon ECS Service Auto Scaling with target tracking policies to scale when an Amazon CloudWatch alarm is breached.

Overall explanation

Amazon ECS uses the AWS Application Auto Scaling service to scales tasks. This is configured through Amazon ECS using Amazon ECS Service Auto Scaling.

A Target Tracking Scaling policy increases or decreases the number of tasks that your service runs based on a target value for a specific metric. For example, in the image below the tasks will be scaled when the average CPU breaches 80% (as reported by CloudWatch):



CORRECT: "Use Amazon ECS Service Auto Scaling with target tracking policies to scale when an Amazon CloudWatch alarm is breached" is the correct answer.

INCORRECT: "Use Amazon EC2 Auto Scaling with simple scaling policies to scale when an Amazon CloudWatch alarm is breached" is incorrect

INCORRECT: "Use Amazon EC2 Auto Scaling to scale out on a schedule and back in once the load decreases" is incorrect

INCORRECT: "Use an AWS Lambda function to scale Amazon ECS based on metric breaches that trigger an Amazon CloudWatch alarm" is incorrect

References:

https://docs.aws.amazon.com/AmazonECS/latest/developerguide/service-auto-scaling.html

Save time with our AWS cheat sheets:

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

Domain

AWS Compute

Question 62Skipped

A multi-tier application runs with eight front-end web servers in an Amazon EC2 Auto Scaling group in a single Availability Zone behind an Application Load Balancer. A solutions architect needs to modify the infrastructure to be highly available without modifying the application.

Which architecture should the solutions architect choose that provides high availability?

Create an Auto Scaling group that uses four instances across each of two subnets

Create an Auto Scaling template that can be used to quickly create more instances in another Region

Create an Auto Scaling group that uses four instances across each of two Regions

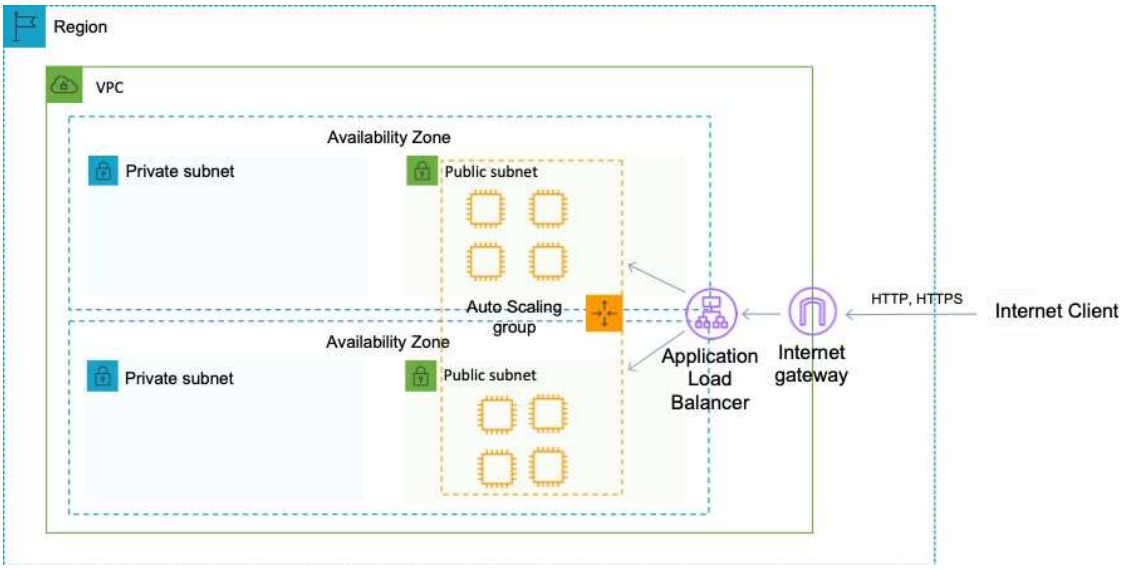
Correct answer

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

Overall explanation

High availability can be enabled for this architecture quite simply by modifying the existing Auto Scaling group to use multiple availability zones. The ASG will automatically balance the load so you don't actually need to specify the instances per AZ.

The architecture for the web tier will look like the one below:



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

INCORRECT: "Create an Auto Scaling group that uses four instances across each of two Regions" is incorrect as EC2 Auto Scaling does not support multiple regions.

INCORRECT: "Create an Auto Scaling template that can be used to quickly create more instances in another Region" is incorrect as EC2 Auto Scaling does not support multiple regions.

INCORRECT: "Create an Auto Scaling group that uses four instances across each of two subnets" is incorrect as the subnets could be in the same AZ.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Compute

Question 63Skipped

There are badge readers located at every entrance of an organization's warehouses. A message is sent over HTTPS when badges are scanned to indicate who tried to access the entrance.

A solutions architect must design a system to process these messages. A highly available solution is required. The solution must store results in a durable data store for later analysis.

Which system architecture should the solutions architect recommend?

Correct answer

Set up an HTTPS endpoint in Amazon API Gateway. To process the messages and save the results to Amazon DynamoDB, configure an API Gateway endpoint to invoke an AWS Lambda function.

Create an Amazon EC2 instance to serve as the HTTPS endpoint and to process messages. An Amazon S3 bucket should be configured for the EC2 instance to save the results.

Direct incoming messages from the sensor to an AWS Lambda function using Amazon Route 53. Create a Lambda function that processes messages and saves results to Amazon DynamoDB.

Set up an Amazon S3 gateway endpoint in your VPC. Connect the facility network to the VPC via a Site-to-Site VPN connection so that sensor data can be written directly to an S3 bucket.

Overall explanation

Amazon API Gateway would be ideal for providing a secure entry point for your application, and for traffic to be sent via HTTPS. AWS Lambda would integrate seamlessly with API Gateway to process the data, as an event-driven solution like this would be perfect when designing a scalable system based on sporadic use. Finally, DynamoDB is highly scalable and is a perfect repository for data to be stored for future analysis.

CORRECT: "Set up an HTTPS endpoint in Amazon API Gateway. To process the messages and save the results to Amazon DynamoDB, configure an API Gateway endpoint to invoke an AWS Lambda function" is the correct answer (as explained above.)

INCORRECT: "Create an Amazon EC2 instance to serve as the HTTPS endpoint and to process messages. An Amazon S3 bucket should be configured for the EC2 instance to save the results" is incorrect. As the action of a badge being read to initiate access to a warehouse should only take a few seconds, spinning up an EC2 instance to serve as a HTTPS endpoint would take minutes, and is not suitable for this use case.

INCORRECT: "Direct incoming messages from the sensor to an AWS Lambda function using Amazon Route 53. Create a Lambda function that processes messages and saves results to

Amazon DynamoDB” is incorrect. Amazon Route 53 is a managed DNS service, and DNS is not required in this instance as the badge reader does not have a DNS name.

INCORRECT: "Set up an Amazon S3 gateway endpoint in your VPC. Connect the facility network to the VPC via a Site-to-Site VPN connection so that sensor data can be written directly to an S3 bucket" is incorrect. VPC endpoints are designed to facilitate traffic across the AWS backbone network between AWS services and are not used to create connections between external endpoints outside of the AWS network and an Amazon S3 bucket.

References:

https://docs.aws.amazon.com/lambda/latest/dg/services-apigateway.html

Save time with our AWS cheat sheets:

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

Domain

AWS Networking & Content Delivery

Question 64Skipped

An organization plans to deploy a higher performance computing (HPC) workload on AWS using Linux. The HPC workload will use many Amazon EC2 instances and will generate a large quantity of small output files that must be stored in persistent storage for future use.

A Solutions Architect must design a solution that will enable the EC2 instances to access data using native file system interfaces and to store output files in cost-effective long-term storage.

Which combination of AWS services meets these requirements?

Correct answer

Amazon FSx for Lustre with Amazon S3.

Amazon EBS volumes with Amazon S3 Glacier.

AWS DataSync with Amazon S3 Intelligent tiering.

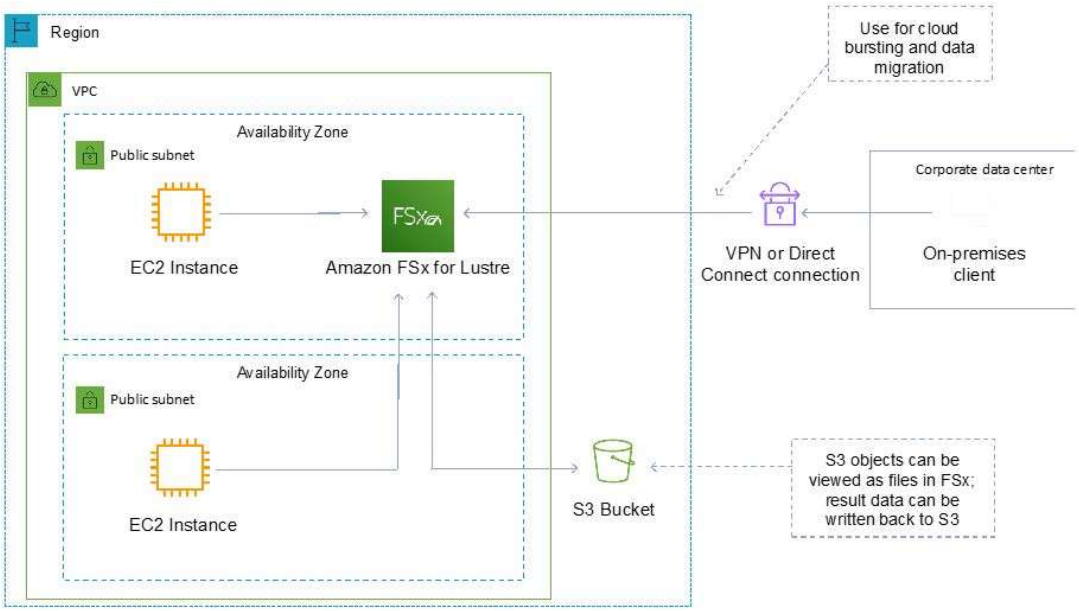
Amazon FSx for Windows File Server with Amazon S3.

Overall explanation

Amazon FSx for Lustre is ideal for high performance computing (HPC) workloads running on Linux instances. FSx for Lustre provides a native file system interface and works as any file system does with your Linux operating system.

When linked to an Amazon S3 bucket, FSx for Lustre transparently presents objects as files, allowing you to run your workload without managing data transfer from S3.

This solution provides all requirements as it enables Linux workloads to use the native file system interfaces and to use S3 for long-term and cost-effective storage of output files.



CORRECT: "Amazon FSx for Lustre with Amazon S3" is the correct answer.

INCORRECT: "Amazon FSx for Windows File Server with Amazon S3" is incorrect. This service should be used with Windows instances and does not integrate with S3.

INCORRECT: "Amazon EBS volumes with Amazon S3 Glacier" is incorrect. EBS volumes do not provide the shared, high performance storage solution using file system interfaces.

INCORRECT: "AWS DataSync with Amazon S3 Intelligent tiering" is incorrect. AWS DataSync is used for migrating / synchronizing data.

References:

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

Save time with our AWS cheat sheets:

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

Domain

AWS Storage

Question 65Skipped

A web application has recently been launched on AWS. The architecture includes two tier with a web layer and a database layer. It has been identified that the web server layer may be vulnerable to cross-site scripting (XSS) attacks.

What should a solutions architect do to remediate the vulnerability?

Correct answer

Create an Application Load Balancer. Put the web layer behind the load balancer and enable AWS WAF

Create a Classic Load Balancer. Put the web layer behind the load balancer and enable AWS WAF

Create a Network Load Balancer. Put the web layer behind the load balancer and enable AWS WAF

Create an Application Load Balancer. Put the web layer behind the load balancer and use AWS Shield Standard

Overall explanation

The AWS Web Application Firewall (WAF) is available on the Application Load Balancer (ALB). You can use AWS WAF directly on Application Load Balancers (both internal and external) in a VPC, to protect your websites and web services.

Attackers sometimes insert scripts into web requests in an effort to exploit vulnerabilities in web applications. You can create one or more cross-site scripting match conditions to identify the parts of web requests, such as the URI or the query string, that you want AWS WAF to inspect for possible malicious scripts.

CORRECT: "Create an Application Load Balancer. Put the web layer behind the load balancer and enable AWS WAF" is the correct answer.

INCORRECT: "Create a Classic Load Balancer. Put the web layer behind the load balancer and enable AWS WAF" is incorrect as you cannot use AWS WAF with a classic load balancer.

INCORRECT: "Create a Network Load Balancer. Put the web layer behind the load balancer and enable AWS WAF" is incorrect as you cannot use AWS WAF with a network load balancer.

INCORRECT: "Create an Application Load Balancer. Put the web layer behind the load balancer and use AWS Shield Standard" is incorrect as you cannot use AWS Shield to protect against XSS attacks. Shield is used to protect against DDoS attacks.

References:

https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-xss-conditions.html

Save time with our AWS cheat sheets:

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

Domain

AWS Security, Identity, & Compliance