

### Question 1Skipped

A retail organization sends coupons out twice a week and this results in a predictable surge in sales traffic. The application runs on Amazon EC2 instances behind an Elastic Load Balancer. The organization is looking for ways lower costs while ensuring they meet the demands of their customers.

How can they achieve this goal?

**Increase the instance size of the existing EC2 instances**

**Correct answer**

**Use capacity reservations with savings plans**

**Use a mixture of spot instances and on demand instances**

**Purchase Amazon EC2 dedicated hosts**

Overall explanation

On-Demand Capacity Reservations enable you to reserve compute capacity for your Amazon EC2 instances in a specific Availability Zone for any duration. By creating Capacity Reservations, you ensure that you always have access to EC2 capacity when you need it, for as long as you need it. When used in combination with savings plans, you can also gain the advantages of cost reduction.

**CORRECT:** " Use capacity reservations with savings plans" is the correct answer.

**INCORRECT:** "Use a mixture of spot instances and on demand instances" is incorrect. You can mix spot and on-demand in an auto scaling group. However, there's a risk the spot price may not be good, and this is a regular, predictable increase in traffic.

**INCORRECT:** "Increase the instance size of the existing EC2 instances" is incorrect. This would add more cost all the time rather than catering for the temporary increases in traffic.

**INCORRECT:** "Purchase Amazon EC2 dedicated hosts" is incorrect. This is not a way to save cost as dedicated hosts are much more expensive than shared hosts.

#### References:

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

**Save time with our AWS cheat sheets:**

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

#### Domain

AWS Compute

### Question 2Skipped

A company requires that IAM users must rotate their access keys every 60 days. If an access key is found to older it must be removed. A Solutions Architect must create an automated solution

that checks the age of access keys and removes any keys that exceed the maximum age defined.

Which solution meets these requirements?

**Create an Amazon EventBridge rule to check for the key age. Define an Amazon EventBridge rule to execute an AWS Lambda function that removes the key.**

**Create an AWS Config rule to check for the key age. Configure the AWS Config rule to trigger an Amazon SNS notification.**

**Correct answer**

**Create an AWS Config rule to check for the key age. Define an Amazon EventBridge rule to execute an AWS Lambda function that removes the key.**

**Create an Amazon EventBridge rule to check for the key age. Configure the rule to trigger an AWS Config remediation that removes the key.**

Overall explanation

Amazon EventBridge uses the same underlying service and API as Amazon CloudWatch Events. You can use EventBridge to detect and react to changes in the status of AWS Config events. You can create a rule that runs whenever there is a state transition, or when there is a transition to one or more states that are of interest. Then, based on rules you create, Amazon EventBridge invokes one or more target actions when an event matches the values you specify in a rule. Depending on the type of event, you might want to send notifications, capture event information, take corrective action, initiate events, or take other actions.

The AWS Config rule can be configured using the “access-keys-rotated” managed rule which checks if the active access keys are rotated within the number of days specified in `maxAccessKeyAge`. The rule is `NON_COMPLIANT` if the access keys have not been rotated for more than `maxAccessKeyAge` number of days.

Amazon EventBridge can react to the change of state to `NON_COMPLIANT` and trigger an AWS Lambda function that invalidates and removes the access key.

**CORRECT:** "Create an AWS Config rule to check for the key age. Define an Amazon EventBridge rule to execute an AWS Lambda function that removes the key" is the correct answer.

**INCORRECT:** "Create an AWS Config rule to check for the key age. Configure the AWS Config rule to trigger an Amazon SNS notification" is incorrect. This solution notifies the user or administrator but does not automatically remove the key.

**INCORRECT:** "Create an Amazon EventBridge rule to check for the key age. Configure the rule to trigger an AWS Config remediation that removes the key" is incorrect. Config rules will check the key age and then EventBridge should react to the state change, not the other way around.

**INCORRECT:** "Create an Amazon EventBridge rule to check for the key age. Define an Amazon EventBridge rule to execute an AWS Lambda function that removes the key" is incorrect. Again, EventBridge does not check the key age, AWS Config must be used for that purpose.

**References:**

<https://docs.aws.amazon.com/config/latest/developerguide/monitor-config-with-cloudwatchevents.html>

<https://docs.aws.amazon.com/config/latest/developerguide/access-keys-rotated.html>

**Save time with our AWS cheat sheets:**

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

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

## Domain

AWS Management & Governance

### Question 3Skipped

A financial institution with many departments wants to migrate to the AWS Cloud from their data center. Each department should have their own established AWS accounts with preconfigured, Limited access to authorized services, based on each team's needs, by the principle of least privilege.

What actions should be taken to ensure compliance with these security requirements?

**Configure AWS Organizations with SCPs and create new member accounts. Use AWS CloudFormation templates to configure the member account networking.**

### Correct answer

**Deploy a Landing Zone within AWS Control Tower. Allow department administrators to use the Landing Zone to create new member accounts and networking. Grant the department's AWS power user permissions on the created accounts.**

**Use AWS CloudFormation to create new member accounts and networking and use IAM roles to allow access to approved AWS services.**

**Deploy a Landing Zone within AWS Organizations. Allow department administrators to use the Landing Zone to create new member accounts and networking. Grant the department's AWS power user permissions on the created accounts.**

### Overall explanation

AWS Control Tower automates the setup of a new landing zone using best practices blueprints for identity, federated access, and account structure.

The account factory automates provisioning of new accounts in your organization. As a configurable account template, it helps you standardize the provisioning of new accounts with pre-approved account configurations. You can configure your account factory with pre-approved network configuration and region selections.

**CORRECT:** "Deploy a Landing Zone within AWS Control Tower. Allow department administrators to use the Landing Zone to create new member accounts and networking. Grant the department's AWS power user permissions on the created accounts" is the correct answer (as explained above.)

**INCORRECT:** "Use AWS CloudFormation to create new member accounts and networking and use IAM roles to allow access to approved AWS services" is incorrect. Although you could perhaps make new AWS Accounts with AWS CloudFormation, the easiest way to do that is by using AWS Control Tower.

**INCORRECT:** "Configure AWS Organizations with SCPs and create new member accounts. Use AWS CloudFormation templates to configure the member account networking" is incorrect. You can make new accounts using AWS Organizations however the easiest way to do this is by using the AWS Control Tower service.

**INCORRECT:** "Deploy a Landing Zone within AWS Organizations. Allow department administrators to use the Landing Zone to create new member accounts and networking. Grant the department's AWS power user permissions on the created accounts" is incorrect. Landing Zones do not get deployed within AWS Organizations.

#### **References:**

<https://aws.amazon.com/controltower/>

#### **Domain**

AWS Management & Governance

#### **Question 4Skipped**

A Solutions Architect has placed an Amazon CloudFront distribution in front of their web server, which is serving up a highly accessed website, serving content globally. The Solutions Architect needs to dynamically route the user to a new URL depending on where the user is accessing from, through running a particular script. This dynamic routing will happen on every request, and as a result requires the code to run at extremely low latency, and low cost.

What solution will best achieve this goal?

**Redirect traffic by running your code within a Lambda function using Lambda@Edge.**

#### **Correct answer**

**At the Edge Location, run your code with CloudFront Functions.**

**Use Path Based Routing to route each user to the appropriate webpage behind an Application Load Balancer.**

**Use Route 53 Geo Proximity Routing to route users' traffic to your resources based on their geographic location.**

Overall explanation

With CloudFront Functions in Amazon CloudFront, you can write lightweight functions in JavaScript for high-scale, latency-sensitive CDN customizations. Your functions can manipulate the requests and responses that flow through CloudFront, perform basic authentication and authorization, generate HTTP responses at the edge, and more. CloudFront Functions is approximately 1/6th the cost of Lambda@Edge and is extremely low latency as the functions are run on the host in the edge location, instead of the running on a Lambda function elsewhere.

**CORRECT:** "At the Edge Location, run your code with CloudFront Functions" is the correct answer (as explained above.)

**INCORRECT:** "Redirect traffic by running your code within a Lambda function using Lambda@Edge" is incorrect. Although you could achieve this using Lambda@Edge, the question states the need for the lowest latency possible, and comparatively the lowest latency option is CloudFront Functions.

**INCORRECT:** "Use Path Based Routing to route each user to the appropriate webpage behind an Application Load Balancer" is incorrect. This architecture does not account for the fact that custom code needs to be run to make this happen.

**INCORRECT:** "Use Route 53 Geo Proximity Routing to route users' traffic to your resources based on their geographic location." is incorrect. This may work, however again it does not account for the fact that custom code needs to be run to make this happen.

#### **References:**

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cloudfront-functions.html>

#### **Save time with our AWS cheat sheets:**

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

#### **Domain**

AWS Networking & Content Delivery

#### **Question 5Skipped**

A telecommunications company is looking to expand its 5G coverage nationwide, and as a result needs to provision and build their own private cellular network with the help of AWS.

Which solution does AWS provide to help with this?

#### **Correct answer**

**AWS Private 5G**

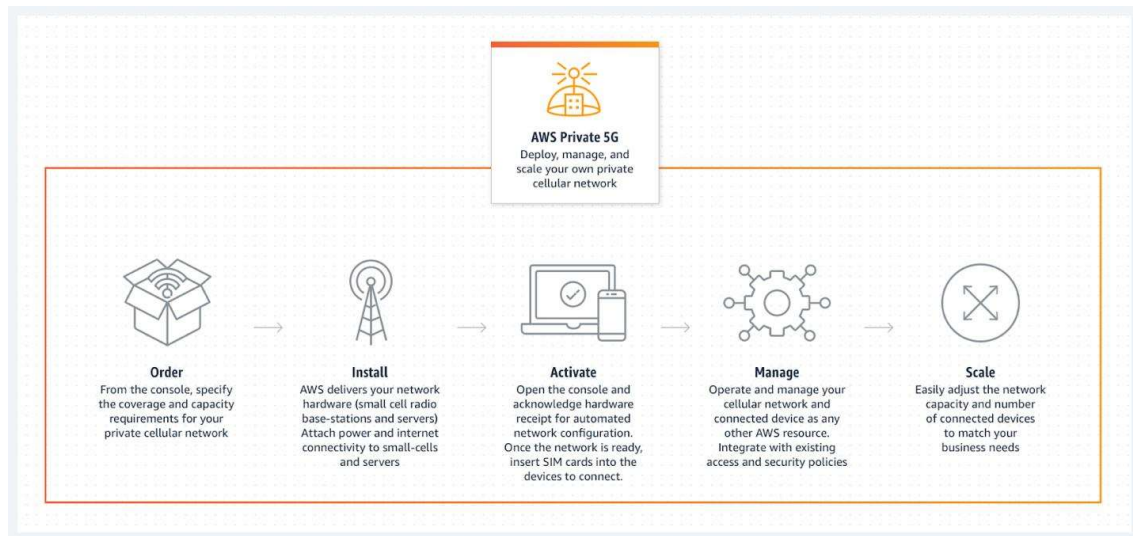
**AWS Wavelength**

**AWS Outposts**

**AWS CloudHSM**

Overall explanation

AWS Private 5G is a managed service that makes it easy to deploy, operate, and scale your own private cellular network, with all required hardware and software provided by AWS.



**CORRECT:** "AWS Private 5G" is the correct answer (as explained above.)

**INCORRECT:** "AWS Wavelength" is incorrect. AWS Wavelength embeds AWS compute and storage services within 5G networks, providing mobile edge computing infrastructure for developing, deploying, and scaling ultra-low-latency applications.

**INCORRECT:** "AWS CloudHSM" is incorrect. AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud and has nothing to do with 5G.

**INCORRECT:** "AWS Outposts" is incorrect. AWS Outposts is a family of fully managed solutions delivering AWS infrastructure and services to virtually any on-premises or edge location for a truly consistent hybrid experience. It is not related to 5G.

#### References:

<https://aws.amazon.com/private5g/>

#### Domain

AWS Networking & Content Delivery

#### Question 6Skipped

Every time an item in an Amazon DynamoDB table is modified a record must be retained for compliance reasons. What is the most efficient solution to recording this information?

**Enable Amazon CloudTrail. Configure an Amazon EC2 instance to monitor activity in the CloudTrail log files and record changed items in another DynamoDB table**

**Enable Amazon CloudWatch Logs. Configure an AWS Lambda function to monitor the log files and record deleted item data to an Amazon S3 bucket**

**Enable DynamoDB Global Tables. Enable DynamoDB streams on the multi-region table and save the output directly to an Amazon S3 bucket**

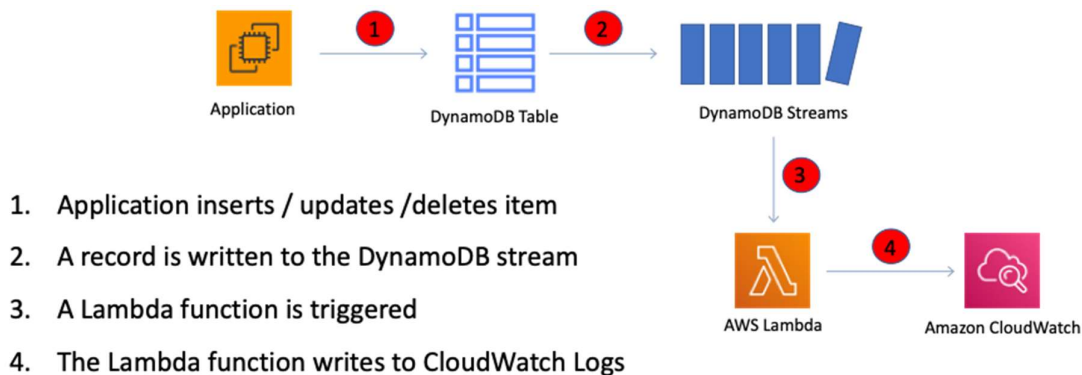
**Correct answer**

**Enable DynamoDB Streams. Configure an AWS Lambda function to poll the stream and record the modified item data to an Amazon S3 bucket**

Overall explanation

Amazon 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.

For example, in the diagram below a DynamoDB stream is being consumed by a Lambda function which processes the item data and records a record in CloudWatch Logs:



**CORRECT:** "Enable DynamoDB Streams. Configure an AWS Lambda function to poll the stream and record the modified item data to an Amazon S3 bucket" is the correct answer.

**INCORRECT:** "Enable Amazon CloudWatch Logs. Configure an AWS Lambda function to monitor the log files and record deleted item data to an Amazon S3 bucket" is incorrect. The deleted item data will not be recorded in CloudWatch Logs.

**INCORRECT:** "Enable Amazon CloudTrail. Configure an Amazon EC2 instance to monitor activity in the CloudTrail log files and record changed items in another DynamoDB table" is incorrect. CloudTrail records API actions so it will not record the data from the item that was modified.

**INCORRECT:** "Enable DynamoDB Global Tables. Enable DynamoDB streams on the multi-region table and save the output directly to an Amazon S3 bucket" is incorrect. Global Tables is used for creating a multi-region, multi-master database. It is of no additional value for this requirement as you could just enable DynamoDB streams on the main table. You also cannot save modified data straight to an S3 bucket.

**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 7Skipped

A company plans to provide developers with individual AWS accounts. The company will use AWS Organizations to provision the accounts. A Solutions Architect must implement secure auditing using AWS CloudTrail so that all events from all AWS accounts are logged. The developers must not be able to use root-level permissions to alter the AWS CloudTrail configuration in any way or access the log files in the S3 bucket. The auditing solution and security controls must automatically apply to all new developer accounts that are created.

Which action should the Solutions Architect take?

**Create a service-linked role for CloudTrail with a policy condition that allows changes only from an Amazon Resource Name (ARN) in the management account.**

**Correct answer**

**Create a new trail in CloudTrail from within the management account with the organization trails option enabled.**

**Create a service control policy (SCP) that prohibits changes to CloudTrail and attach it to the developer accounts.**

**Create an IAM policy that prohibits changes to CloudTrail and attach it to the root user.**

Overall explanation

You can create a CloudTrail trail in the management account with the organization trails option enabled and this will create the trail in all AWS accounts within the organization.

Member accounts can see the organization trail but can't modify or delete it. By default, member accounts don't have access to the log files for the organization trail in the Amazon S3 bucket.

**CORRECT:** "Create a new trail in CloudTrail from within the management account with the organization trails option enabled" is the correct answer.

**INCORRECT:** "Create an IAM policy that prohibits changes to CloudTrail and attach it to the root user" is incorrect. You cannot restrict the root user this way and should use the organization trails option or an SCP instead.

**INCORRECT:** "Create a service-linked role for CloudTrail with a policy condition that allows changes only from an Amazon Resource Name (ARN) in the management account" is incorrect. You cannot create service-linked roles, these are created by AWS for you.

**INCORRECT:** "Create a service control policy (SCP) that prohibits changes to CloudTrail and attach it to the developer accounts" is incorrect. An SCP can achieve the required outcome of limiting the ability to change the CloudTrail configuration, but the trail must still be created in each account and the SCP must be attached which is not automatic.

**References:**

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/creating-trail-organization.html>

**Save time with our AWS cheat sheets:**

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



## Domain

AWS Management & Governance

### Question 8Skipped

A Solutions Architect is rearchitecting an application with decoupling. The application will send batches of up to 1000 messages per second that must be received in the correct order by the consumers.

Which action should the Solutions Architect take?

**Create an Amazon SQS Standard queue**

**Correct answer**

**Create an Amazon SQS FIFO queue**

**Create an AWS Step Functions state machine**

**Create an Amazon SNS topic**

Overall explanation

Only FIFO queues guarantee the ordering of messages and therefore a standard queue would not work. The FIFO queue supports up to 3,000 messages per second with batching so this is a supported scenario.

Standard Queue	FIFO Queue
Unlimited Throughput: Standard queues support a nearly unlimited number of transactions per second (TPS) per API action.	High Throughput: FIFO queues support up to 300 messages per second (300 send, receive, or delete operations per second). When you batch 10 messages per operation (maximum), FIFO queues can support up to 3,000 messages per second
Best-Effort Ordering: Occasionally, messages might be delivered in an order different from which they were sent	First-In-First-out Delivery: The order in which messages are sent and received is strictly preserved
At-Least-Once Delivery: A message is delivered at least once, but occasionally more than one copy of a message is delivered	Exactly-Once Processing: A message is delivered once and remains available until a consumer processes and deletes it. Duplicates are not introduced into the queue

**CORRECT:** "Create an Amazon SQS FIFO queue" is the correct answer.

**INCORRECT:** "Create an Amazon SQS Standard queue" is incorrect as it does not guarantee ordering of messages.

**INCORRECT:** "Create an Amazon SNS topic" is incorrect. SNS is a notification service and a message queue is a better fit for this use case.

**INCORRECT:** "Create an AWS Step Functions state machine" is incorrect. Step Functions is a workflow orchestration service and is not useful for this scenario.

**References:**

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-quotas.html>

**Save time with our AWS cheat sheets:**

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

## Domain

AWS Application Integration

### Question 9Skipped

A company has 200 TB of video files stored in an on-premises data center that must be moved to the AWS Cloud within the next four weeks. The company has around 50 Mbps of available bandwidth on an Internet connection for performing the transfer.

What is the MOST cost-effective solution for moving the data within the required timeframe?

#### Correct answer

**Order multiple AWS Snowball devices to migrate the data to AWS.**

**Use AWS Snowmobile to migrate the data to AWS.**

**Use Amazon S3 Transfer Acceleration to securely upload the data.**

**Create a virtual private gateway and connect a VPN to upload the data.**

Overall explanation

To move 200 TB of data over a 50 Mbps link would take over 300 days. Therefore, the solution must avoid the Internet link. The most cost-effective solution is to use multiple AWS Snowball devices to migrate the data to AWS.

Snowball devices are shipped to your data center where you can load the data and then ship it back to AWS. This avoids the Internet connection and utilizes local high-bandwidth network connections to load the data.

**CORRECT:** "Order multiple AWS Snowball devices to migrate the data to AWS" is the correct answer.

**INCORRECT:** "Use Amazon S3 Transfer Acceleration to securely upload the data" is incorrect. This would use the Internet link and would not meet the required timeframe.

**INCORRECT:** "Create a virtual private gateway and connect a VPN to upload the data" is incorrect. This would also use the Internet link and would not meet the required timeframe.

**INCORRECT:** "Use AWS Snowmobile to migrate the data to AWS" is incorrect. This is a very large device on the back of a truck that is used for moving huge quantities of data. It would be very expensive for moving just 200 TB of data.

#### References:

<https://aws.amazon.com/snowball/features/>

**Save time with our AWS cheat sheets:**

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

## Domain

AWS Storage

### Question 10Skipped

Over 500 TB of data must be analyzed using standard SQL business intelligence tools. The dataset consists of a combination of structured data and unstructured data. The unstructured data is small and stored on Amazon S3. Which AWS services are most suitable for performing analytics on the data?

**Amazon RDS MariaDB with Amazon Athena**

**Amazon ElastiCache for Redis with cluster mode enabled**

**Amazon DynamoDB with Amazon DynamoDB Accelerator (DAX)**

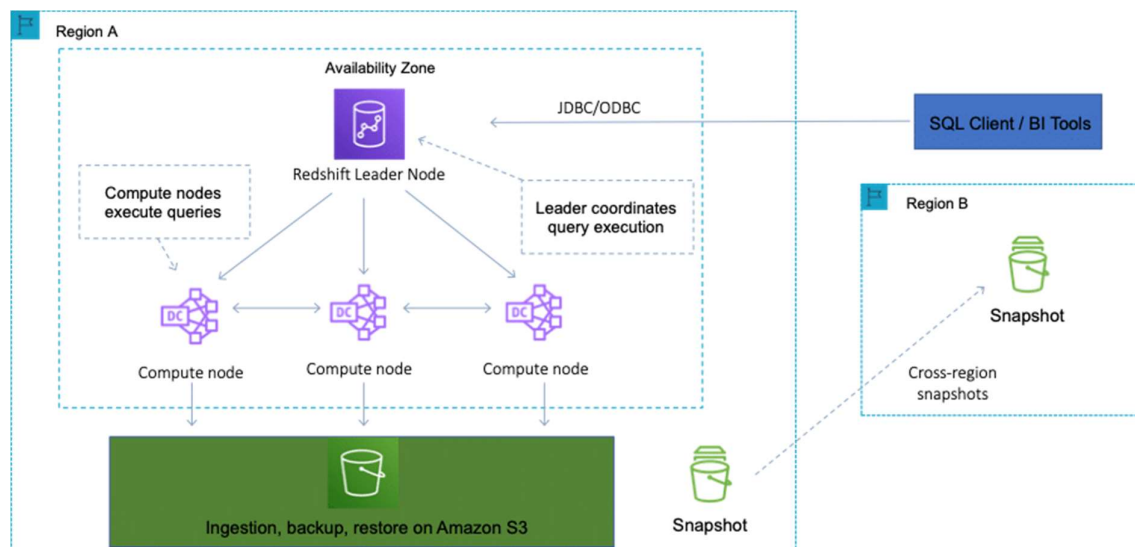
**Correct answer**

**Amazon Redshift with Amazon Redshift Spectrum**

Overall explanation

Amazon Redshift is an enterprise-level, petabyte scale, fully managed data warehousing service. An Amazon Redshift data warehouse is an enterprise-class relational database query and management system. Redshift supports client connections with many types of applications, including business intelligence (BI), reporting, data, and analytics tools.

Using Amazon Redshift Spectrum, you can efficiently query and retrieve structured and semistructured data from files in Amazon S3 without having to load the data into Amazon Redshift tables. Redshift Spectrum queries employ massive parallelism to execute very fast against large datasets.



Used together, RedShift and RedShift spectrum are suitable for running massive analytics jobs on both the structured (RedShift data warehouse) and unstructured (Amazon S3) data.

**CORRECT:** "Amazon Redshift with Amazon Redshift Spectrum" is the correct answer.

**INCORRECT:** "Amazon RDS MariaDB with Amazon Athena" is incorrect. Amazon RDS is not suitable for analytics (OLAP) use cases as it is designed for transactional (OLTP) use cases. Athena can however be used for running SQL queries on data on S3.

**INCORRECT:** "Amazon DynamoDB with Amazon DynamoDB Accelerator (DAX)" is incorrect. This is an example of a non-relational DB with a caching layer and is not suitable for an OLAP use case.

**INCORRECT:** "Amazon ElastiCache for Redis with cluster mode enabled" is incorrect. This is an example of an in-memory caching service. It is good for performance for transactional use cases.

#### **References:**

[https://docs.aws.amazon.com/redshift/latest/dg/c\\_redshift\\_system\\_overview.html](https://docs.aws.amazon.com/redshift/latest/dg/c_redshift_system_overview.html)

<https://docs.aws.amazon.com/redshift/latest/dg/c-using-spectrum.html>

#### **Save time with our AWS cheat sheets:**

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

#### **Domain**

AWS Database

#### **Question 11Skipped**

An eCommerce company has a very popular web application that receives a large amount of traffic. The application must store customer profile data and shopping cart information in a database. A Solutions Architect must design the database solution to support peak loads of several million requests per second and millisecond response times. Operational overhead must be minimized, and scaling should not cause downtime.

Which database solution should the Solutions Architect recommend?

#### **Correct answer**

**Amazon DynamoDB**

**Amazon Athena**

**Amazon Aurora**

**Amazon RDS**

Overall explanation

Amazon DynamoDB is a non-relational database that is managed for you. It can scale without downtime and with minimal operational overhead. DynamoDB can support the request rates and response times required by this solution and is often used in eCommerce solutions and for session state use cases.

**CORRECT:** "Amazon DynamoDB" is the correct answer.

**INCORRECT:** "Amazon Aurora" is incorrect. Aurora will require downtime to scale as you must change the instance type.

**INCORRECT:** "Amazon RDS" is incorrect. RDS will require downtime to scale as you must change the instance type.

**INCORRECT:** "Amazon Athena" is incorrect. Athena is used for querying data in a data lake, it is not used for storing this type of information in a transactional database model.

**References:**

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AutoScaling.html>

**Save time with our AWS cheat sheets:**

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

**Domain**

AWS Database

**Question 12Skipped**

The Chief Financial Officer of a large corporation is looking for an AWS native tool which will help reduce their cloud spend. After receiving a budget alarm, the company has decided that they need to reduce their spend across their different areas of compute and need insights into their spend to decide where they can reduce cost.

What is the easiest way to achieve this goal?

**Correct answer**

**AWS Compute Optimizer**

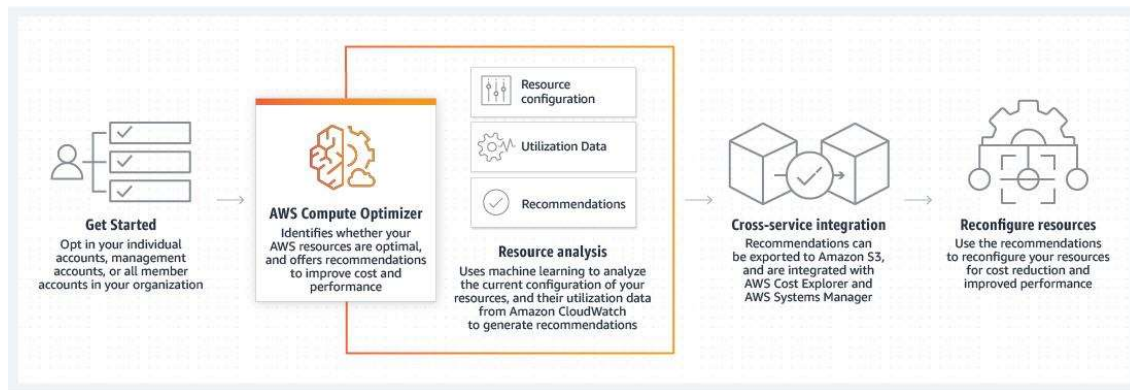
**Cost and Usage Reports**

**AWS Trusted Advisor**

**AWS Cost Explorer**

Overall explanation

AWS Compute Optimizer helps you identify the optimal AWS resource configurations, such as Amazon Elastic Compute Cloud (EC2) instance types, Amazon Elastic Block Store (EBS) volume configurations, and AWS Lambda function memory sizes, using machine learning to analyze historical utilization metrics. AWS Compute Optimizer provides a set of APIs and a console experience to help you reduce costs and increase workload performance by recommending the optimal AWS resources for your AWS workloads.



**CORRECT:** "AWS Compute Optimizer" is the correct answer (as explained above.)

**INCORRECT:** "AWS Trusted Advisor" is incorrect. Whilst you will get some cost recommendations using Trusted Advisor, when working with reducing cost for compute specifically, AWS Compute Optimizer is a better choice.

**INCORRECT:** "Cost and Usage Reports" is incorrect. Cost and Usage Reports are a highly detailed report of your spend and usage across your entire AWS Environment. Whilst it can be used to understand cost, it does not make recommendations.

**INCORRECT:** "AWS Cost Explorer" is incorrect. Cost Explorer gives you insight into your spend and usage in a graphical format, which can be filtered and grouped by parameters like Region, instance type and can use Tags to further group resources. It does not however make any recommendations on how to reduce spend.

#### References:

<https://aws.amazon.com/compute-optimizer/faqs/>

#### Save time with our AWS cheat sheets:

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

#### Domain

AWS Compute

#### Question 13Skipped

A Solutions Architect for a large banking company is configuring access control within the organization for an Amazon S3 bucket containing thousands of financial records. There are 20 different teams which need to have access to this bucket, however they all need different permissions. These 20 teams correspond to 20 accounts within the banking company who are currently using AWS Organizations.

What is the simplest way to achieve this, whilst adhering to the principle of least privilege?

#### Correct answer

**Use S3 Access points to administer different access policies to each team, and control access points using Service Control Policies within AWS Organizations.**

**Create the S3 Bucket in an individual account. Configure an IAM Role for each user to enable cross account access for the S3 Bucket with a permissions policy to only access the appropriate items within the bucket.**

**Create a new AWS Organizations. Assign each team to a different Organizational Unit and apply to appropriate permissions granting access to the appropriate resources in the bucket.**

**Copy the items from the bucket to create separate versions of each Separate the items in the bucket into new buckets. Administer Bucket policies to allow each account to access the appropriate bucket.**

Overall explanation

Amazon S3 Access Points, a feature of S3, simplify data access for any AWS service or customer application that stores data in S3. With S3 Access Points, customers can create unique access control policies for each access point to easily control access to shared datasets. You can also control access point usage using AWS Organizations support for AWS SCPs.

**CORRECT:** "Use S3 Access points to administer different access policies to each team, and control access points using Service Control Policies within AWS Organizations" is the correct answer (as explained above.)

**INCORRECT:** "Create a new AWS Organizations. Assign each team to a different Organizational Unit and apply to appropriate permissions granting access to the appropriate resources in the bucket" is incorrect. This would not only be incredibly time consuming but totally unnecessary as you can use the preexisting AWS Organizations and the Service Control policies to control access via S3 Access Points.

**INCORRECT:** "Copy the items from the bucket to create separate versions of each Separate the items in the bucket into new buckets. Administer Bucket policies to allow each account to access the appropriate bucket" is incorrect. This involves a lot of operational overhead and would be prone to significant error when administering the correct permissions to each account.

**INCORRECT:** "Create the S3 Bucket in an individual account. Configure an IAM Role for each user to enable cross account access for the S3 Bucket with a permissions policy to only access the appropriate items within the bucket" is incorrect. This is an unnecessary complexity as it would be much easier to provision separate policies per team using S3 Access Points.

**References:**

<https://aws.amazon.com/s3/features/access-points/>

**Save time with our AWS cheat sheets:**

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

**Domain**

AWS Security, Identity, & Compliance

**Question 14**Skipped

A team of scientists are collecting environmental data to assess the impact of pollution in a small regional town. The scientists collect data from various sensors and cameras. The data must be immediately processed to validate its accuracy, but the scientists have limited local storage space on their laptops and intermittent and unreliable connectivity to their Amazon EC2 instances and S3 buckets.

What should a Solutions Architect recommend?

**Configure Amazon Kinesis Data Firehose to load data directly to a Snowball device and process locally with Lambda@Edge.**

**Correct answer**

**Use AWS Snowball Edge devices to process the data locally.**

**Use AWS DataSync on the scientists' laptops to synchronize the data to Amazon S3. Process the data with Amazon EC2 instances.**

**Upload the data to Amazon SQS in batches and process the messages using Amazon EC2 instances.**

Overall explanation

AWS Snowball Edge is a type of Snowball device with on-board storage and compute power for select AWS capabilities. Snowball Edge can do local processing and edge-computing workloads in addition to transferring data between your local environment and the AWS Cloud.

You can run Amazon EC2 compute instances on a Snowball Edge device using the Amazon EC2 compatible endpoint, which supports a subset of the Amazon EC2 API operations. Data can subsequently be transferred to Amazon S3 for storage and additional processing.

**CORRECT:** "Use AWS Snowball Edge devices to process the data locally" is the correct answer.

**INCORRECT:** "Upload the data to Amazon SQS in batches and process the messages using Amazon EC2 instances" is incorrect. The internet connectivity is unreliable so this could result in data loss and delays for the team.

**INCORRECT:** "Configure Amazon Kinesis Data Firehose to load data directly to a Snowball device and process locally with Lambda@Edge" is incorrect. KDF cannot load data to Snowball devices and Lambda@Edge is used with CloudFront for processing data.

**INCORRECT:** "Use AWS DataSync on the scientists' laptops to synchronize the data to Amazon S3. Process the data with Amazon EC2 instances" is incorrect. Due to the unreliable connectivity this does not solve the problem.

**References:**

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

**Save time with our AWS cheat sheets:**

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

**Domain**

AWS Storage



## Question 15Skipped

A company has over 200 TB of log files in an Amazon S3 bucket. The company must process the files using a Linux-based software application that will extract and summarize data from the log files and store the output in a separate Amazon S3 bucket. The company needs to minimize data transfer charges associated with the processing of this data.

How can a Solutions Architect meet these requirements?

**Launch an Amazon EC2 instance in the same Region as the S3 bucket. Process the log files and upload the output to another S3 bucket in a different Region.**

**Correct answer**

**Launch an Amazon EC2 instance in the same Region as the S3 bucket. Process the log files and upload the output to another S3 bucket in the same Region.**

**Use an on-premises virtual machine for processing the data. Retrieve the log files from the S3 bucket and upload the output to another S3 bucket in the same Region.**

**Connect an AWS Lambda function to the S3 bucket via a VPC endpoint. Process the log files and store the output to another S3 bucket in the same Region.**

Overall explanation

The software application must be installed on a Linux operating system so we must use Amazon EC2 or an on-premises VM. To avoid data charges however, we must ensure that the data does not egress the AWS Region. The best solution to avoid the egress data charges is to use an Amazon EC2 instance in the same Region as the S3 bucket that contains the log files. The processed output files must also be stored in a bucket in the same Region to avoid any data going out from EC2 to another Region.

**CORRECT:** "Launch an Amazon EC2 instance in the same Region as the S3 bucket. Process the log files and upload the output to another S3 bucket in the same Region" is the correct answer.

**INCORRECT:** "Use an on-premises virtual machine for processing the data. Retrieve the log files from the S3 bucket and upload the output to another S3 bucket in the same Region" is incorrect. The data would need to egress the AWS Region incurring data transfer charges in this configuration.

**INCORRECT:** "Launch an Amazon EC2 instance in the same Region as the S3 bucket. Process the log files and upload the output to another S3 bucket in a different Region" is incorrect. The processed data would be going from the EC2 instance to a bucket in a different Region which would incur data transfer charges.

**INCORRECT:** "Connect an AWS Lambda function to the S3 bucket via a VPC endpoint. Process the log files and store the output to another S3 bucket in the same Region" is incorrect. You cannot install a Linux-based software application on AWS Lambda.

**References:**

<https://aws.amazon.com/s3/pricing/>

**Save time with our AWS cheat sheets:**

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

## Domain

AWS Storage

### Question 16Skipped

A Solutions Architect needs to design a solution for providing a shared file system for company users in the AWS Cloud. The solution must be fault tolerant and should integrate with the company's Microsoft Active Directory for access control.

Which storage solution meets these requirements?

### Correct answer

**Create a file system with Amazon FSx for Windows File Server and enable Multi-AZ. Join Amazon FSx to Active Directory.**

**Create an Amazon EFS file system and configure AWS Single Sign-On with Active Directory.**

**Use Amazon S3 for storing the data and configure AWS Cognito to connect S3 to Active Directory for access control.**

**Use an Amazon EC2 Windows instance to create a file share. Attach Amazon EBS volumes in different Availability Zones.**

Overall explanation

Amazon FSx for Windows File Server provides fully managed Microsoft Windows file servers, backed by a fully native Windows file system. Multi-AZ file systems provide high availability and failover support across multiple Availability Zones by provisioning and maintaining a standby file server in a separate Availability Zone within an AWS Region.

Amazon FSx works with Microsoft Active Directory (AD) to integrate with your existing Microsoft Windows environments. Active Directory is the Microsoft directory service used to store information about objects on the network and make this information easy for administrators and users to find and use.

**CORRECT:** "Create a file system with Amazon FSx for Windows File Server and enable Multi-AZ. Join Amazon FSx to Active Directory" is the correct answer.

**INCORRECT:** "Create an Amazon EFS file system and configure AWS Single Sign-On with Active Directory" is incorrect. You cannot configure AWS SSO for an EFS file system with Active Directory.

**INCORRECT:** "Use an Amazon EC2 Windows instance to create a file share. Attach Amazon EBS volumes in different Availability Zones" is incorrect. You cannot attach EBS volumes in different AZs to an instance.

**INCORRECT:** "Use Amazon S3 for storing the data and configure AWS Cognito to connect S3 to Active Directory for access control" is incorrect. You cannot use Cognito to connect S3 to Active Directory.

**References:**

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/what-is.html>

**Save time with our AWS cheat sheets:**

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

## Domain

AWS Storage

### Question 17Skipped

An application runs on Amazon EC2 instances. The application reads data from Amazon S3, performs processing on the data, and then writes the results to an Amazon DynamoDB table.

The application writes many temporary files during the data processing. The application requires a high-performance storage solution for the temporary files.

What would be the fastest storage option for this solution?

**Multiple Amazon EFS volumes in Max I/O performance mode.**

**Multiple Amazon EBS volumes with Provisioned IOPS.**

**Correct answer**

**Multiple instance store volumes with software RAID 0.**

**Multiple Amazon S3 buckets with Transfer Acceleration.**

Overall explanation

As the data is only temporary it can be stored on an instance store volume which is a volume that is physically attached to the host computer on which the EC2 instance is running.

To increase aggregate IOPS, or to improve sequential disk throughput, multiple instance store volumes can be grouped together using RAID 0 (disk striping) software. This can improve the aggregate performance of the volume.

**CORRECT:** "Multiple instance store volumes with software RAID 0" is the correct answer.

**INCORRECT:** "Multiple Amazon EBS volumes with Provisioned IOPS" is incorrect. Multiple volumes will not provide better performance unless you can aggregate the performance across them which is what the correct answer offers with instance store volumes.

**INCORRECT:** "Multiple Amazon EFS volumes in Max I/O performance mode" is incorrect. You cannot aggregate the performance of multiple EFS volumes.

**INCORRECT:** "Multiple Amazon S3 buckets with Transfer Acceleration" is incorrect. Amazon S3 will not provide the best performance for this use case and transfer acceleration is used more for the upload of data.

## References:

<https://docs.aws.amazon.com/whitepapers/latest/aws-storage-services-overview/performance-4.html>

**Save time with our AWS cheat sheets:**

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

## Domain

AWS Compute

### Question 18Skipped

A web application hosts static and dynamic content. The application runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). The database tier runs on an Amazon Aurora database. A Solutions Architect needs to make the application more resilient to periodic increases in request rates.

Which architecture should the Solutions Architect implement? (Select TWO.)

#### Correct selection

**Add an Amazon CloudFront distribution.**

**Add an AWS Transit Gateway.**

#### Correct selection

**Add Aurora Replicas.**

**Add an AWS Direct Connect link.**

**Add an AWS Global Accelerator.**

Overall explanation

Using an Amazon CloudFront distribution can help reduce the impact of increases in requests rates as content is cached at edge locations and delivered via the AWS global network. For the database layer, Aurora Replicas will assist with serving read requests which reduces the load on the main database instance.

**CORRECT:** "Add Aurora Replicas" is a correct answer.

**CORRECT:** "Add an Amazon CloudFront distribution" is also a correct answer.

**INCORRECT:** "Add an AWS Transit Gateway" is incorrect. This service offers no value in this situation.

**INCORRECT:** "Add an AWS Direct Connect link" is incorrect. This would only improve network performance for users connecting from an on-premises location.

**INCORRECT:** "Add an AWS Global Accelerator" is incorrect. CloudFront is better suited to this use case as it caches static content and improves performance for dynamic content.

#### References:

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

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

**Save time with our AWS cheat sheets:**

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

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

## Domain

AWS Networking & Content Delivery

### Question 19Skipped

A Solutions Architect is designing an application that consists of AWS Lambda and Amazon RDS Aurora MySQL. The Lambda function must use database credentials to authenticate to MySQL and security policy mandates that these credentials must not be stored in the function code.

How can the Solutions Architect securely store the database credentials and make them available to the function?

**Store the credentials in AWS Key Management Service and use environment variables in the function code pointing to KMS**

**Use the AWSAuthenticationPlugin and associate an IAM user account in the MySQL database**

**Correct answer**

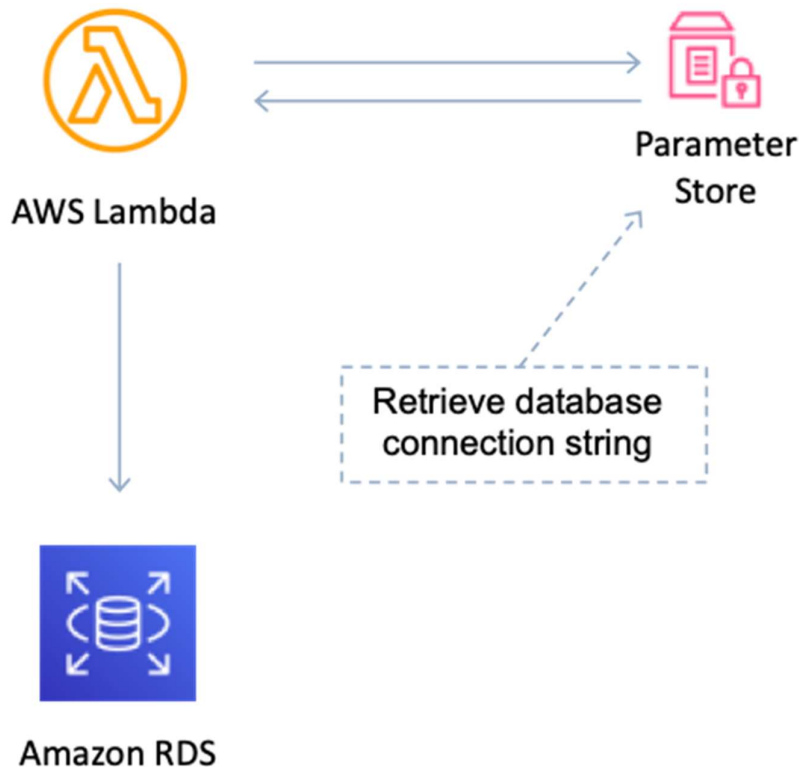
**Store the credentials in Systems Manager Parameter Store and update the function code and execution role**

**Create an IAM policy and store the credentials in the policy. Attach the policy to the Lambda function execution role**

Overall explanation

In this case the scenario requires that credentials are used for authenticating to MySQL. The credentials need to be securely stored outside of the function code. Systems Manager Parameter Store provides secure, hierarchical storage for configuration data management and secrets management.

You can easily reference the parameters from services including AWS Lambda as depicted in the diagram below:



**CORRECT:** "Store the credentials in Systems Manager Parameter Store and update the function code and execution role" is the correct answer.

**INCORRECT:** "Store the credentials in AWS Key Management Service and use environment variables in the function code pointing to KMS" is incorrect. You cannot store credentials in KMS, it is used for creating and managing encryption keys

**INCORRECT:** "Use the AWSAuthenticationPlugin and associate an IAM user account in the MySQL database" is incorrect. This is a great way to securely authenticate to RDS using IAM users or roles. However, in this case the scenario requires database credentials to be used by the function.

**INCORRECT:** "Create an IAM policy and store the credentials in the policy. Attach the policy to the Lambda function execution role" is incorrect. You cannot store credentials in IAM policies.

**References:**

<https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-parameter-store.html>

**Domain**

AWS Compute

**Question 20**Skipped

A large financial services company currently has an SMB file server in its on-premises environment. After a large file is created, it is accessed frequently by the file server for the first few days. It is rare for the files to be accessed after 30 days.

Data sizes are increasing and are approaching the company's storage capacity. Increasing a company's storage space without sacrificing access to recent files is the task of the solutions architect. The solutions architect must also provide file lifecycle management to avoid future storage issues from recurring.

Which solution will meet these requirements?

**Create an Amazon FSx for Windows File Server file system to extend the file space.**

**Install a custom program on each user's computer which will grant them access to Amazon S3. Create an S3 Lifecycle policy to transition the data to S3 Glacier Flexible Retrieval after 30 days.**

**Correct answer**

**Create an Amazon S3 File Gateway, extending the company's storage space into the cloud. Create an S3 Lifecycle policy to transition the data to S3 Glacier Deep Archive after 30 days.**

**Use AWS DataSync to take data older than 30 days from the SMB file server to AWS.**

Overall explanation

Amazon S3 File Gateway provides a seamless way to connect to the cloud to store application data files and backup images as durable objects in Amazon S3 cloud storage. Amazon S3 File Gateway offers SMB or NFS-based access to data in Amazon S3 with local caching.

It can be used for on-premises data-intensive Amazon EC2-based applications that need file protocol access to S3 object storage. Lifecycle policies can then transition the data to S3 Glacier Deep Archive after 30 days.

**CORRECT:** "Create an Amazon S3 File Gateway, extending the company's storage space into the cloud. Create an S3 Lifecycle policy to transition the data to S3 Glacier Deep Archive after 30 days" is the correct answer (as explained above.)

**INCORRECT:** "Use AWS DataSync to take data older than 30 days from the SMB file server to AWS" is incorrect. This solution would not distinguish between more and less frequently accessed data.

**INCORRECT:** "Create an Amazon FSx for Windows File Server file system to extend the file space" is incorrect. Amazon FSx for Windows File Server is not a hybrid service and is only suitable for cloud-based deployments of Windows File Server.

**INCORRECT:** "Install a custom program on each user's computer which will grant them access to Amazon S3. Create an S3 Lifecycle policy to transition the data to S3 Glacier Flexible Retrieval after 30 days" is incorrect. This involves too much extra configuration which is unnecessary.

**References:**

<https://aws.amazon.com/storagegateway/file/s3/>

**Save time with our AWS cheat sheets:**

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

## Domain

AWS Storage

### Question 21Skipped

An application is deployed using Amazon EC2 instances behind an Application Load Balancer running in an Auto Scaling group. The EC2 instances connect to an Amazon RDS database. When running performance testing on the application latency was experienced when performing queries on the database. The Amazon CloudWatch metrics for the EC2 instances do not show any performance issues.

How can a Solutions Architect resolve the application latency issues?

**Replace the EC2 instances with AWS Lambda functions.**

**Correct answer**

**Add read replicas for the RDS database and direct read traffic to the replicas.**

**Replace the Application Load Balancer with a Network Load Balancer.**

**Enable Multi-AZ for the RDS database and direct read traffic to the standby.**

Overall explanation

The latency is most likely due to the RDS database having insufficient resources to handle the load. This can be resolved by deploying a read replica and directing queries to the replica endpoint. This offloads the performance hit of the queries from the master database which will improve overall performance and reduce the latency associated with database queries.

**CORRECT:** "Add read replicas for the RDS database and direct read traffic to the replicas" is the correct answer.

**INCORRECT:** "Replace the EC2 instances with AWS Lambda functions" is incorrect. If the latency is being caused by the database layer, then this will not resolve the issues.

**INCORRECT:** "Replace the Application Load Balancer with a Network Load Balancer" is incorrect. If the latency is being caused by the database layer, then this will not resolve the issues.

**INCORRECT:** "Enable Multi-AZ for the RDS database and direct read traffic to the standby" is incorrect. You cannot read from the standby in an Amazon RDS database cluster (you can with Aurora though).

### References:

<https://aws.amazon.com/rds/features/read-replicas/>

**Save time with our AWS cheat sheets:**

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

## Domain

AWS Database

### Question 22Skipped



A company has two accounts in an AWS Organization. The accounts are: Prod1 and Prod2. An Amazon RDS database runs in the Prod1 account. Amazon EC2 instances run in the Prod2 account. The EC2 instances in the Prod2 account must access the RDS database.

How can a Solutions Architect meet this requirement MOST cost-effectively?

**Create a cross-Region Replica of the Amazon RD database in the Prod2 account. Point the EC2 instances to the Replica endpoint.**

**Take a snapshot of the Amazon RDS database and share it with the Prod2 account. In the Prod2 account, restore the cluster using the shared snapshot.**

**Correct answer**

**Set up VPC sharing with the Prod1 account as the owner and the Prod2 account as the participant to transfer the data.**

**Create an AWS Lambda function in the Prod1 account to transfer data to the Amazon EC2 instances in the Prod2 account.**

Overall explanation

VPC sharing makes use of the AWS Resource Access Manager (AWS RAM) service. It enables the sharing of VPCs across accounts. In this model, the account that owns the VPC (owner) shares one or more subnets with other accounts (participants) that belong to the same organization from AWS Organizations.

This scenario could be implemented with Prod1 account as the VPC owner and the Prod2 account as a VPC participant. This would allow the central control of the shared resource whilst enabling the EC2 instances in Prod2 to access the database.

**CORRECT:** "Set up VPC sharing with the Prod1 account as the owner and the Prod2 account as the participant to transfer the data" is the correct answer.

**INCORRECT:** "Create an AWS Lambda function in the Prod1 account to transfer data to the Amazon EC2 instances in the Prod2 account" is incorrect. The question is not asking for transfer of data; the EC2 instances need to access the database. Therefore, a method of connecting to a database endpoint is required.

**INCORRECT:** "Create a cross-Region Replica of the Amazon RD database in the Prod2 account. Point the EC2 instances to the Replica endpoint" is incorrect. You cannot create cross-Region replicas of RDS databases in different accounts.

**INCORRECT:** "Take a snapshot of the Amazon RDS database and share it with the Prod2 account. In the Prod2 account, restore the cluster using the shared snapshot" is incorrect. This is less cost-effective as there is now a second RDS database running.

**References:**

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-sharing.html>

**Save time with our AWS cheat sheets:**

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

**Domain**

**Question 23**Skipped

A Solutions Architect is designing an application that will run on an Amazon EC2 instance. The application must asynchronously invoke an AWS Lambda function to analyze thousands of .CSV files. The services should be decoupled.

Which service can be used to decouple the compute services?

**Amazon OpsWorks**

**Correct answer**

**Amazon SNS**

**Amazon SWF**

**Amazon Kinesis**

Overall explanation

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

**CORRECT:** "Amazon SNS" is the correct answer.

**INCORRECT:** "Amazon SWF" is incorrect. The Simple Workflow Service (SWF) is used for process automation. It is not well suited to this requirement.

**INCORRECT:** "Amazon Kinesis" is incorrect as this service is used for ingesting and processing real time streaming data, it is not a suitable service to be used solely for invoking a Lambda function.

**INCORRECT:** "Amazon OpsWorks" is incorrect as this service is used for configuration management of systems using Chef or Puppet.

**References:**

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

**Save time with our AWS cheat sheets:**

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

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

**Domain**

AWS Application Integration

**Question 24**Skipped

As part of a company's shift to the AWS cloud, they need to gain an insight into their total on-premises footprint. They have discovered that they are currently struggling with managing their

software licenses. They would like to maintain a hybrid cloud setup, with some of their licenses stored in the cloud with some stored on-premises.

What actions should be taken to ensure they are managing the licenses appropriately going forward?

**Use the AWS Key Management Service to treat the license key safely and store it securely**

**Correct answer**

**Use AWS License Manager to manage the software licenses**

**Use Amazon S3 with governance lock to manage the storage of the licenses**

**Use AWS Secrets Manager to store the licenses as secrets to ensure they are stored securely**

Overall explanation

AWS License Manager makes it easier to manage your software licenses from vendors such as Microsoft, SAP, Oracle, and IBM across AWS and on-premises environments. AWS License Manager lets administrators create customized licensing rules that mirror the terms of their licensing agreements.

**CORRECT:** "Use AWS License Manager to manage the software licenses" is the correct answer (as explained above.)

**INCORRECT:** "Use AWS Secrets Manager to store the licenses as secrets to ensure they are stored securely" is incorrect. AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. This does not include license keys.

**INCORRECT:** "Use the AWS Key Management Service to treat the license key safely and store it securely" is incorrect. AWS Key Management Service (AWS KMS) makes it easy for you to create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications, not license keys.

**INCORRECT:** "Use Amazon S3 with governance lock to manage the storage of the licenses" is incorrect. Amazon S3 is not designed to store software licenses.

**References:**

<https://aws.amazon.com/license-manager/>

**Domain**

AWS Management & Governance

**Question 25**Skipped

A company runs a streaming application on AWS that ingests data in near real-time and then processes the data. The data processing takes 30 minutes to complete. As the volume of data being ingested by the application has increased, high latency has occurred. A Solutions Architect needs to design a scalable and serverless solution to improve performance.

Which combination of steps should the Solutions Architect take? (Select TWO.)

**Use Amazon EC2 instances in a placement group to process the data.**

**Use Amazon Simple Queue Service (SQS) to ingest the data.**

**Use AWS Lambda with AWS Step Functions to process the data.**

**Correct selection**

**Use Amazon Kinesis Data Firehose to ingest the data.**

**Correct selection**

**Use containers running on AWS Fargate to process the data.**

Overall explanation

The application is a streaming application that ingests near real time data. This is a good fit for Amazon Kinesis Data Firehose which can ingest data and load it directly to a data store where it can be subsequently processed. We then need a serverless solution for processing the data. AWS Fargate is a serverless service that uses Amazon ECS for running Docker containers on AWS.

This solution will seamlessly scale for the data ingestion and processing. It is also fully serverless.

**CORRECT:** "Use Amazon Kinesis Data Firehose to ingest the data" is a correct answer.

**CORRECT:** "Use containers running on AWS Fargate to process the data" is also a correct answer.

**INCORRECT:** "Use AWS Lambda with AWS Step Functions to process the data" is incorrect. Lambda has a maximum execution time of 900 seconds (15 minutes), so it is not possible to use AWS Lambda functions for processing the data.

**INCORRECT:** "Use Amazon Simple Queue Service (SQS) to ingest the data" is incorrect. SQS does not ingest data, you must use an application process to place messages in the queue and then another process to consumer and process the messages from the queue.

**INCORRECT:** "Use Amazon EC2 instances in a placement group to process the data" is incorrect. A placement group with EC2 instances is not a serverless solution as you must manage the EC2 instances.

**References:**

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

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

**Save time with our AWS cheat sheets:**

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

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

**Domain**

AWS Analytics

### Question 26Skipped

To increase performance and redundancy for an application a company has decided to run multiple implementations in different AWS Regions behind network load balancers. The company currently advertise the application using two public IP addresses from separate /24 address ranges and would prefer not to change these. Users should be directed to the closest available application endpoint.

Which actions should a solutions architect take? (Select TWO.)

#### Correct selection

**Migrate both public IP addresses to the AWS Global Accelerator**

**Create PTR records to map existing public IP addresses to an Alias**

**Assign new static anycast IP addresses and modify any existing pointers**

#### Correct selection

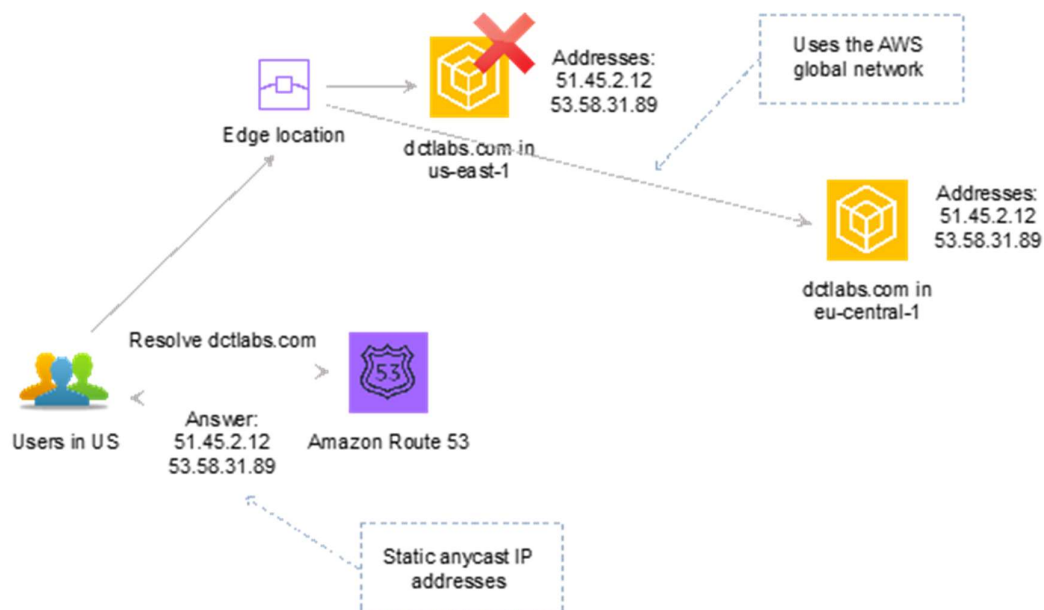
**Create an AWS Global Accelerator and attach endpoints in each AWS Region**

**Create an Amazon Route 53 geolocation based routing policy**

Overall explanation

AWS Global Accelerator uses static IP addresses as fixed entry points for your application. You can migrate up to two /24 IPv4 address ranges and choose which /32 IP addresses to use when you create your accelerator.

This solution ensures the company can continue using the same IP addresses and they are able to direct traffic to the application endpoint in the AWS Region closest to the end user. Traffic is sent over the AWS global network for consistent performance.



**CORRECT:** "Create an AWS Global Accelerator and attach endpoints in each AWS Region" is a correct answer.

**CORRECT:** "Migrate both public IP addresses to the AWS Global Accelerator" is also a correct answer.

**INCORRECT:** "Create an Amazon Route 53 geolocation based routing policy" is incorrect. With this solution new IP addresses will be required as there will be application endpoints in different regions.

**INCORRECT:** "Assign new static anycast IP addresses and modify any existing pointers" is incorrect. This is unnecessary as you can bring your own IP addresses to AWS Global Accelerator and this is preferred in this scenario.

**INCORRECT:** "Create PTR records to map existing public IP addresses to an Alias" is incorrect. This is not a workable solution for mapping existing IP addresses to an Amazon Route 53 Alias.

#### **References:**

<https://aws.amazon.com/global-accelerator/features/>

#### **Save time with our AWS cheat sheets:**

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

#### **Domain**

AWS Networking & Content Delivery

#### **Question 27Skipped**

A large manufacturing company needs to store data in Amazon S3 and prevent the data from being modified. The company requires that all new objects uploaded to Amazon S3 should remain unchangeable for an unspecified period until the company decides to modify the objects. Only specific users within the company's AWS account should have the ability to delete the objects.

What should a solutions architect do to meet these requirements?

**Create an S3 bucket. Use AWS CloudTrail to track S3 all actions to the resources within S3. Upon notification, restore the modified objects from any backup versions that the company has if a delete action has taken place.**

#### **Correct answer**

**Create an S3 bucket with S3 Object Lock enabled. Enable versioning. Add a legal hold to the objects. Add the s3:PutObjectLegalHold permission to the IAM policies of users who need to delete the objects.**

**Create an S3 Glacier vault. Apply a vault lock policy to the objects to prevent modification of the objects.**

**Create a new S3 bucket with S3 Object Lock enabled. Enable versioning on your bucket and set a retention period of 50 years. Use governance mode as the S3 bucket's default retention mode for new objects.**

Overall explanation

With S3 Object Lock, you can store objects using a write-once-read-many (WORM) model. Object Lock can help prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. You can use Object Lock to help meet regulatory requirements that require WORM storage, or to simply add another layer of protection against object changes and deletion. Governance mode also renders the objects to be immutable.

**CORRECT:** "Create an S3 bucket with S3 Object Lock enabled. Enable versioning. Add a legal hold to the objects. Add the s3:PutObjectLegalHold permission to the IAM policies of users who need to delete the objects" is the correct answer (as explained above.)

**INCORRECT:** "Create an S3 Glacier vault. Apply a vault lock policy to the objects to prevent modification of the objects" is incorrect as this would not make the objects immutable.

**INCORRECT:** "Create an S3 bucket. Use AWS CloudTrail to track S3 all actions to the resources within S3. Upon notification, restore the modified objects from any backup versions that the company has if a delete action has taken place" is incorrect as this would not make the objects immutable.

**INCORRECT:** "Create a new S3 bucket with S3 Object Lock enabled. Enable versioning on your bucket and set a retention period of 50 years. Use governance mode as the S3 bucket's default retention mode for new objects" is incorrect as using governance mode would not allow the files to be changed at all for the duration of this being enabled.

#### References:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html>

#### Save time with our AWS cheat sheets:

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

#### Domain

AWS Storage

#### Question 28Skipped

A company is migrating a decoupled application to AWS. The application uses a message broker based on the MQTT protocol. The application will be migrated to Amazon EC2 instances and the solution for the message broker must not require rewriting application code.

Which AWS service can be used for the migrated message broker?

#### AWS Step Functions

#### Amazon SQS

#### Correct answer

#### Amazon MQ

#### Amazon SNS

#### Overall explanation

Amazon MQ is a managed message broker service for Apache ActiveMQ that makes it easy to set up and operate message brokers in the cloud. Connecting current applications to Amazon

MQ is easy because it uses industry-standard APIs and protocols for messaging, including JMS, NMS, AMQP, STOMP, MQTT, and WebSocket. Using standards means that in most cases, there's no need to rewrite any messaging code when you migrate to AWS.

**CORRECT:** "Amazon MQ" is the correct answer.

**INCORRECT:** "Amazon SQS" is incorrect. This is an Amazon proprietary service and does not support industry-standard messaging APIs and protocols.

**INCORRECT:** "Amazon SNS" is incorrect. This is a notification service not a message bus.

**INCORRECT:** "AWS Step Functions" is incorrect. This is a workflow orchestration service, not a message bus.

#### References:

<https://aws.amazon.com/amazon-mq/>

#### Save time with our AWS cheat sheets:

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

#### Domain

AWS Application Integration

#### Question 29Skipped

A financial services company provides users with downloadable reports in PDF format. The company requires a solution that can seamlessly scale to meet the demands of a growing, global user base. The solution must be cost-effective and minimize operational overhead.

Which combination of services should a Solutions Architect recommend to meet these requirements?

**AWS Lambda and Amazon DynamoDB.**

**Application Load Balancer with AWS Auto Scaling.**

**Correct answer**

**Amazon CloudFront and Amazon S3.**

**Amazon Route 53 with Network Load Balancers.**

Overall explanation

The most cost-effective option is to use Amazon S3 for storing the PDF files and Amazon CloudFront for caching the files around the world in edge locations. This combination of services will provide seamless scalability and is cost-effective. This is also a serverless solution so operational overhead is minimized.

**CORRECT:** "Amazon CloudFront and Amazon S3" is the correct answer.

**INCORRECT:** "AWS Lambda and Amazon DynamoDB" is incorrect. AWS Lambda can be used to process requests and serve traffic from DynamoDB. However, a front end like API Gateway may be required and DynamoDB would be less cost-effective compared to using S3.



**INCORRECT:** "Application Load Balancer with AWS Auto Scaling" is incorrect. This would use Amazon EC2 instances and load balancers which is more expensive.

**INCORRECT:** "Amazon Route 53 with Network Load Balancers" is incorrect. This would use Amazon EC2 instances and load balancers which is more expensive.

**References:**

<https://aws.amazon.com/blogs/networking-and-content-delivery/amazon-s3-amazon-cloudfront-a-match-made-in-the-cloud/>

**Save time with our AWS cheat sheets:**

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

**Domain**

AWS Networking & Content Delivery

**Question 30**Skipped

The log files of a proprietary application must be analyzed. The log files are stored in an Amazon S3 bucket in JSON format. Query execution will be on-demand and simple. It is essential for a solutions architect to perform the analysis with minimal changes to the existing architecture.

How can a solutions architect meet these requirements with the LOWEST amount of operational overhead?

**Use Amazon Redshift to place all the content in one place and run the SQL queries as and when required.**

**Correct answer**

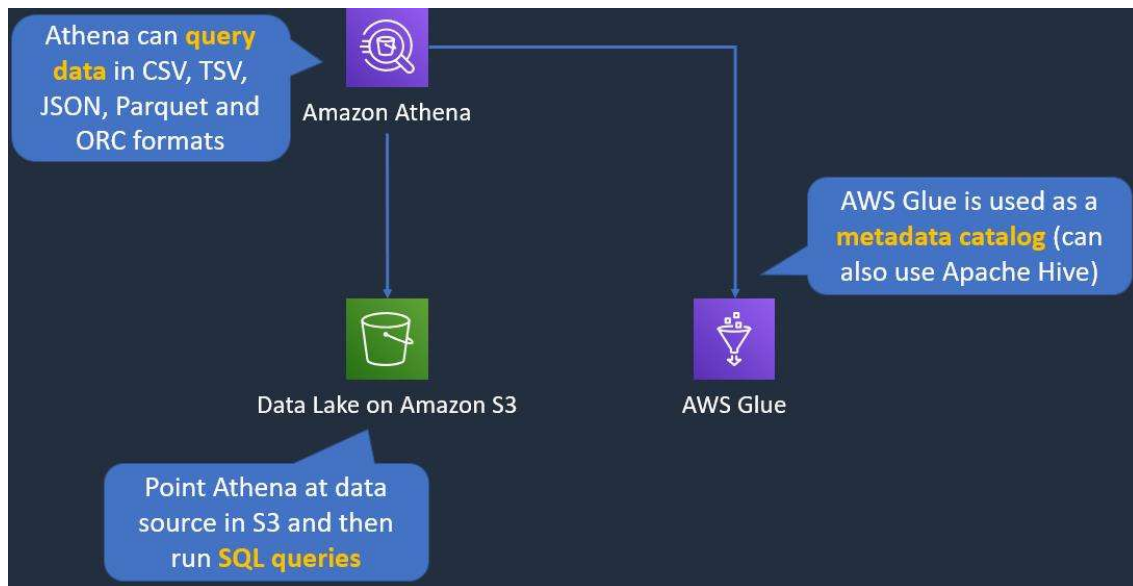
**Use Amazon Athena to query and analyze the data in Amazon S3 using standard SQL queries on demand.**

**Use Amazon CloudWatch Logs for log storage. Run SQL queries on demand from the Amazon CloudWatch console.**

**Use AWS Glue to catalog the logs. Use a transient Apache Spark cluster on Amazon EMR to run the SQL queries on demand.**

**Overall explanation**

Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run. The Solutions Architect could easily use Amazon Athena to query the logs on demand without refactoring any other parts of the application.



**CORRECT:** "Use Amazon Athena to query and analyze the data in Amazon S3 using standard SQL queries on demand" is the correct answer (as explained above.)

**INCORRECT:** "Use Amazon Redshift to place all the content in one place and run the SQL queries as and when required" is incorrect. This would take a significant amount of refactoring by moving all the application log data into Amazon RedShift.

**INCORRECT:** "Use Amazon CloudWatch Logs for log storage. Run SQL queries on demand from the Amazon CloudWatch console" is incorrect. Though you can use CloudWatch Logs Insights to run queries on log files, these are not SQL queries, and this is not an efficient solution as it will require a lot of refactoring.

**INCORRECT:** "Use AWS Glue to catalog the logs. Use a transient Apache Spark cluster on Amazon EMR to run the SQL queries on demand" is incorrect. This would take a significant amount of refactoring by moving all the application log data into AWS Glue and using an EMR cluster to analyze the logs.

#### References:

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

#### Save time with our AWS cheat sheets:

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

#### Domain

AWS Analytics

#### Question 31Skipped

A company is deploying an Amazon ElastiCache for Redis cluster. To enhance security a password should be required to access the database. What should the solutions architect use?

#### VPC Security Group

#### AWS IAM Policy

## **AWS Directory Service**

### **Correct answer**

#### **Redis AUTH command**

Overall explanation

Redis authentication tokens enable Redis to require a token (password) before allowing clients to execute commands, thereby improving data security.

You can require that users enter a token on a token-protected Redis server. To do this, include the parameter `--auth-token` (API: `AuthToken`) with the correct token when you create your replication group or cluster. Also include it in all subsequent commands to the replication group or cluster.

**CORRECT:** "Redis AUTH command" is the correct answer.

**INCORRECT:** "AWS Directory Service" is incorrect. This is a managed Microsoft Active Directory service and cannot add password protection to Redis.

**INCORRECT:** "AWS IAM Policy" is incorrect. You cannot use an IAM policy to enforce a password on Redis.

**INCORRECT:** "VPC Security Group" is incorrect. A security group protects at the network layer, it does not affect application authentication.

### **References:**

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/auth.html>

### **Save time with our AWS cheat sheets:**

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

## **Domain**

AWS Database

### **Question 32Skipped**

An application that runs a computational fluid dynamics workload uses a tightly-coupled HPC architecture that uses the MPI protocol and runs across many nodes. A service-managed deployment is required to minimize operational overhead.

Which deployment option is MOST suitable for provisioning and managing the resources required for this use case?

### **Correct answer**

**Use AWS Batch to deploy a multi-node parallel job**

**Use Amazon EC2 Auto Scaling to deploy instances in multiple subnets**

**Use AWS Elastic Beanstalk to provision and manage the EC2 instances**

**Use AWS CloudFormation to deploy a Cluster Placement Group on EC2**

Overall explanation

AWS Batch Multi-node parallel jobs enable you to run single jobs that span multiple Amazon EC2 instances. With AWS Batch multi-node parallel jobs, you can run large-scale, tightly coupled, high performance computing applications and distributed GPU model training without the need to launch, configure, and manage Amazon EC2 resources directly.

An AWS Batch multi-node parallel job is compatible with any framework that supports IP-based, internode communication, such as Apache MXNet, TensorFlow, Caffe2, or Message Passing Interface (MPI).

This is the most efficient approach to deploy the resources required and supports the application requirements most effectively.

**CORRECT:** "Use AWS Batch to deploy a multi-node parallel job" is the correct answer.

**INCORRECT:** "Use Amazon EC2 Auto Scaling to deploy instances in multiple subnets " is incorrect. This is not the best solution for a tightly-coupled HPC workload with specific requirements such as MPI support.

**INCORRECT:** "Use AWS CloudFormation to deploy a Cluster Placement Group on EC2" is incorrect. This would deploy a cluster placement group but not manage it. AWS Batch is a better fit for large scale workloads such as this.

**INCORRECT:** "Use AWS Elastic Beanstalk to provision and manage the EC2 instances" is incorrect. You can certainly provision and manage EC2 instances with Elastic Beanstalk but this scenario is for a specific workload that requires MPI support and managing a HPC deployment across a large number of nodes. AWS Batch is more suitable.

**References:**

<https://d1.awsstatic.com/whitepapers/architecture/AWS-HPC-Lens.pdf>

<https://docs.aws.amazon.com/batch/latest/userguide/multi-node-parallel-jobs.html>

**Domain**

AWS Compute

**Question 33**Skipped

A Solutions Architect needs to select a low-cost, short-term option for adding resilience to an AWS Direct Connect connection. What is the MOST cost-effective solution to provide a backup for the Direct Connect connection?

**Configure an IPSec VPN connection over the Direct Connect link**

**Implement a second AWS Direct Connection**

**Configure AWS Transit Gateway with an IPSec VPN backup**

**Correct answer**

**Implement an IPSec VPN connection and use the same BGP prefix**

Overall explanation

This is the most cost-effective solution. With this option both the Direct Connect connection and IPsec VPN are active and being advertised using the Border Gateway Protocol (BGP). The Direct Connect link will always be preferred unless it is unavailable.

**CORRECT:** "Implement an IPsec VPN connection and use the same BGP prefix" is the correct answer.

**INCORRECT:** "Implement a second AWS Direct Connection" is incorrect. This is not a short-term or low-cost option as it takes time to implement and is costly.

**INCORRECT:** "Configure AWS Transit Gateway with an IPsec VPN backup" is incorrect. This is a workable solution and provides some advantages. However, you do need to pay for the Transit Gateway so it is not the most cost-effective option and probably not suitable for a short-term need.

**INCORRECT:** "Configure an IPsec VPN connection over the Direct Connect link" is incorrect. This is not a solution to the problem as the VPN connection is going over the Direct Connect link. This is something you might do to add encryption to Direct Connect but it doesn't make it more resilient.

#### References:

<https://docs.aws.amazon.com/whitepapers/latest/hybrid-connectivity/vpn-connection-as-a-backup-to-aws-dx-connection-example.html>

#### Save time with our AWS cheat sheets:

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

#### Domain

AWS Networking & Content Delivery

#### Question 34Skipped

A large financial services organization has a workflow for ingesting data. It currently consists of an Amazon Simple Notification Service (Amazon SNS) topic for receiving notifications about new deliveries of data, and an AWS Lambda function to process the data and record metadata.

Network connectivity issues occasionally cause the ingestion workflow to fail. When such a failure occurs, the Lambda function does not ingest the corresponding data and the team must manually re-run the Lambda function.

Which combination of actions should a solutions architect take to ensure that the data is ingested even if there is a network outage. (Select TWO.)

#### Correct selection

**Modify the Lambda function so it reads from an Amazon SQS queue.**

**Deploy the Lambda function across multiple Availability Zones within the Region.**

**Increase throughput for the Lambda function and increase the provisioned CPU and memory.**

#### Correct selection

**Set up an Amazon SQS queue and subscribe it to the SNS topic.**

**Attach the Lambda function to an Amazon VPC and deploy a NAT gateway. Enable multi-AZ for the VPC.**

Overall explanation

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message-oriented middleware and empowers developers to focus on differentiating work. Using Amazon SQS here will allow us to decouple the different parts of our architecture to ensure that even if there is a network outage, the Lambda function will not have to be retried, as the SQS queue will persistently store the request.

**CORRECT:** "Set up an Amazon SQS queue and subscribe it to the SNS topic" is the correct answer (as explained above.)

**CORRECT:** "Modify the Lambda function so it reads from an Amazon SQS queue" is also the correct answer (as explained above.)

**INCORRECT:** "Deploy the Lambda function across multiple Availability Zones within the Region" is incorrect. AWS Lambda automatically maintains compute capacity across multiple Availability Zones (AZs) in each AWS Region to help protect your code against individual machine or data center facility failures.

**INCORRECT:** "Attach the Lambda function to an Amazon VPC and deploy a NAT gateway. Enable multi-AZ for the VPC" is incorrect. There is no such thing as enabling multi-AZ for a VPC and attaching the function to a VPC does not assist with solving the issue in this case.

**INCORRECT:** "Increase throughput for the Lambda function and increase the provisioned CPU and memory" is incorrect. This will increase the performance of the function but will not help if there is a network outage.

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

**Save time with our AWS cheat sheets:**

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

**Domain**

AWS Application Integration

**Question 35**Skipped

A computer scientist working for a university is looking to build a machine learning application which will use telemetry data to predict weather for a given area at a given time. This application would benefit from using managed services and will need to find a solution which uses third party data within the application.

Which of the following combinations of services will deliver the best solution?

**Use a TensorFlow AMI from the AWS Marketplace to build the machine learning part of the application and use AWS Data Exchange to gain access to the third-party telemetry data.**

**Use Amazon SageMaker to build the machine learning part of the application and use AWS DataSync to gain access to the third-party telemetry data.**

**Correct answer**

**Use Amazon SageMaker to build the machine learning part of the application and use AWS Data Exchange to gain access to the third-party telemetry data.**

**Use a TensorFlow AMI from the AWS Marketplace to build the machine learning part of the application and use AWS DataSync to gain access to the third-party telemetry data.**

Overall explanation

Amazon SageMaker allows you to build, train, and deploy machine learning models for any use case with fully managed infrastructure, tools, and workflows. AWS Data Exchange allows you to gain access to third party data sets across Automotive, Financial Services, Gaming, Healthcare & Life Sciences, Manufacturing, Marketing, Media & Entertainment, Retail, and many more industries.

**CORRECT:** "Use Amazon SageMaker to build the machine learning part of the application and use AWS Data Exchange to gain access to the third-party telemetry data" is the correct answer (as explained above.)

**INCORRECT:** "Use Amazon SageMaker to build the machine learning part of the application and use AWS DataSync to gain access to the third-party telemetry data" is incorrect. AWS DataSync is a secure, online service that automates and accelerates moving data between on-premises and AWS storage services. It does not give access to third party data.

**INCORRECT:** "Use a TensorFlow AMI from the AWS Marketplace to build the machine learning part of the application and use AWS DataSync to gain access to the third-party telemetry data" is incorrect. Building an EC2 instance from a TensorFlow AMI would not involve using managed services and AWS DataSync is a secure, online service that automates and accelerates moving data between on-premises and AWS storage services. It does not give access to third party data.

**INCORRECT:** "Use a TensorFlow AMI from the AWS Marketplace to build the machine learning part of the application and use AWS Data Exchange to gain access to the third-party telemetry data" is incorrect. Building an EC2 instance from a TensorFlow AMI would not involve using managed services.

**References:**

<https://aws.amazon.com/data-exchange/>

**Domain**

AWS Machine Learning

**Question 36**Skipped

A highly elastic application consists of three tiers. The application tier runs in an Auto Scaling group and processes data and writes it to an Amazon RDS MySQL database. The Solutions Architect wants to restrict access to the database tier to only accept traffic from the instances

in the application tier. However, instances in the application tier are being constantly launched and terminated.

How can the Solutions Architect configure secure access to the database tier?

**Correct answer**

**Configure the database security group to allow traffic only from the application security group**

**Configure a Network ACL on the database subnet to deny all traffic to ports other than 3306**

**Configure the database security group to allow traffic only from port 3306**

**Configure a Network ACL on the database subnet to allow all traffic from the application subnet**

Overall explanation

The best option is to configure the database security group to only allow traffic that originates from the application security group. You can also define the destination port as the database port. This setup will allow any instance that is launched and attached to this security group to connect to the database.

**CORRECT:** "Configure the database security group to allow traffic only from the application security group" is the correct answer.

**INCORRECT:** "Configure the database security group to allow traffic only from port 3306" is incorrect. Port 3306 for MySQL should be the destination port, not the source.

**INCORRECT:** "Configure a Network ACL on the database subnet to deny all traffic to ports other than 3306" is incorrect. This does not restrict access specifically to the application instances.

**INCORRECT:** "Configure a Network ACL on the database subnet to allow all traffic from the application subnet" is incorrect. This does not restrict access specifically to the application instances.

**References:**

[https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_SecurityGroups.html](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 37Skipped**

Several workloads are being run in one AWS region by a rapidly growing retail company. A solutions architect must create disaster recovery plans that include different AWS regions. In the DR Region, the company needs its database to be kept up to date with the lowest latency possible. Infrastructure in the DR Region must run at reduced capacity and be capable of handling traffic immediately.



Which solution will meet these requirements with the LOWEST possible recovery time objective (RTO)?

**Correct answer**

**Use an Amazon Aurora global database with a warm standby disaster recovery strategy.**

**Use an Amazon Aurora global database with a pilot light disaster recovery strategy.**

**Use an Amazon RDS Multi-AZ DB instance with a warm standby disaster recovery strategy.**

**Use an Amazon RDS Multi-AZ DB instance with a pilot light disaster recovery strategy.**

**Overall explanation**

Amazon Aurora global databases span multiple AWS Regions, enabling low latency global reads and providing fast recovery from the rare outage that might affect an entire AWS Region. An Aurora global database has a primary DB cluster in one Region, and up to five secondary DB clusters in different Regions.

With the warm standby strategy the application can handle traffic (at reduced capacity levels) immediately so this will reduce the RTO.

**CORRECT:** "Use an Amazon Aurora global database with a warm standby disaster recovery strategy" is the correct answer (as explained above.)

**INCORRECT:** "Use an Amazon Aurora global database with a pilot light disaster recovery strategy" is incorrect. With a pilot light strategy the application in the DR site may not be able to accept traffic immediately, and may need intervention and time to get the resources running.

**INCORRECT:** "Use an Amazon RDS Multi-AZ DB instance with a pilot light disaster recovery strategy" is incorrect as an Amazon RDS Multi-AZ DB instance will not be suitable for a multi-region disaster recovery scenario.

**INCORRECT:** "Use an Amazon RDS Multi-AZ DB instance with a warm standby disaster recovery strategy" is incorrect as an Amazon RDS Multi-AZ DB instance will not be suitable for a multi-region disaster recovery scenario.

**References:**

<https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html>

**Domain**

AWS Database

**Question 38**Skipped

A large accounting company needs to store all its accounting records in Amazon S3. The records must be accessible for 1 year with immediate notice, and then must be archived for a further 9 years due to compliance requirements. No one at the company, under any circumstances, should be able to delete the records over the entire 10-year period. The records must be stored with maximum resiliency to prevent data loss.

Which solution will most elegantly meet these requirements?

**Store the records exclusively in S3 Glacier Deep Archive for the entire 10-year period. Use an access control policy to prevent deletion of the records for 10 years.**

**Store the records within S3 Intelligent-Tiering. Use a Bucket policy to deny deletion of the records, and after 10 years, change the Bucket policy to allow deletion manually.**

**Correct answer**

**Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 Glacier Deep Archive after 1 year. Use S3 Object Lock in compliance mode for a period of 10 years.**

**Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 1 year. Use S3 Object Lock in governance mode for a period of 10 years.**

Overall explanation

Using an S3 Lifecycle policy is the easiest way to transition your storage class to an archival tier after one year, with no manual intervention. S3 Standard is suitable for the first year as the customer requires maximum resiliency and immediate retrieval for the first year.

Secondly the customer requires the data to be deleted at no point, and under no circumstances. With S3 Object Lock, you can store objects using a *write-once-read-many* (WORM) model. In *compliance* mode, a protected object version can't be overwritten or deleted by any user, including the root user in your AWS account.

**CORRECT:** "Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 Glacier Deep Archive after 1 year. Use S3 Object Lock in compliance mode for a period of 10 years" is the correct answer (as explained above.)

**INCORRECT:** "Store the records exclusively in S3 Glacier Deep Archive for the entire 10-year period. Use an access control policy to prevent deletion of the records for 10 years" is incorrect as the customer needs to have the data immediately retrievable for the first year. This is not possible with S3 Glacier Deep Archive.

**INCORRECT:** "Store the records within S3 Intelligent-Tiering. Use a Bucket policy to deny deletion of the records, and after 10 years, change the Bucket policy to allow deletion manually" is incorrect. A Bucket policy can be easily changed to allow deletion of the resources within the S3 Bucket, so this is not suitable.

**INCORRECT:** "Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 1 year. Use S3 Object Lock in governance mode for a period of 10 years" is incorrect. S3 One-Zone-IA is not a suitable storage class as the customer requires as much redundancy and possible, which will not be achieved through a single AZ. Secondly, Governance mode can be overturned with certain permissions, unlike Compliance mode.

**References:**

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html>

**Save time with our AWS cheat sheets:**

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

## Domain

AWS Storage

### Question 39Skipped

A company is planning to use an Amazon S3 bucket to store a large volume of customer transaction data. The data will be structured into a hierarchy of objects, and they require a solution for running complex queries as quickly as possible. The solution must minimize operational overhead.

Which solution meets these requirements?

**Use AWS Glue to transform the data into Amazon Redshift tables and then perform the queries.**

**Use AWS Elasticsearch on Amazon S3 to perform the queries.**

**Use AWS Data Pipeline to process and move the data to Amazon EMR and then perform the queries.**

**Correct answer**

**Use Amazon Athena on Amazon S3 to perform the queries.**

Overall explanation

Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to setup or manage, and you can start analyzing data immediately. While Amazon Athena is ideal for quick, ad-hoc querying, it can also handle complex analysis, including large joins, window functions, and arrays.

Athena is the fastest way to query the data in Amazon S3 and offers the lowest operational overhead as it is a fully serverless solution.

**CORRECT:** "Use Amazon Athena on Amazon S3 to perform the queries" is the correct answer.

**INCORRECT:** "Use AWS Data Pipeline to process and move the data to Amazon EMR and then perform the queries" is incorrect. Amazon EMR is not required and would represent a more operationally costly solution.

**INCORRECT:** "Use AWS Elasticsearch on Amazon S3 to perform the queries" is incorrect. Elasticsearch cannot perform SQL queries and join tables for data in Amazon S3.

**INCORRECT:** "Use AWS Glue to transform the data into Amazon Redshift tables and then perform the queries" is incorrect. RedShift is not required and would represent a more operationally costly solution.

**References:**

<https://aws.amazon.com/athena/faqs/>

**Save time with our AWS cheat sheets:**

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

## Domain

AWS Analytics

### Question 40Skipped

A Solutions Architect is tasked with designing a fully Serverless, Microservices based web application which requires the use of a GraphQL API to provide a single entry point to the application.

Which AWS managed service could the Solutions Architect use?

**Amazon Athena**

**Correct answer**

**AWS AppSync**

**API Gateway**

**AWS Lambda**

Overall explanation

AWS AppSync is a serverless GraphQL and Pub/Sub API service that simplifies building modern web and mobile applications.

AWS AppSync GraphQL APIs simplify application development by providing a single endpoint to securely query or update data from multiple databases, microservices, and APIs.

**CORRECT:** "AWS AppSync" is the correct answer (as explained above.)

**INCORRECT:** "API Gateway" is incorrect. You cannot create GraphQL APIs on API Gateway.

**INCORRECT:** "Amazon Athena" is incorrect. Amazon Athena is a Serverless query service where you can query S3 using SQL statements.

**INCORRECT:** "AWS Lambda" is incorrect. AWS Lambda is a serverless compute service and is not designed to build APIs.

### References:

<https://aws.amazon.com/appsync/>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/category/aws-cheat-sheets/aws-networking-content-delivery/>

## Domain

AWS Networking & Content Delivery

### Question 41Skipped

A large MongoDB database running on-premises must be migrated to Amazon DynamoDB within the next few weeks. The database is too large to migrate over the company's limited internet bandwidth so an alternative solution must be used. What should a Solutions Architect recommend?

**Setup an AWS Direct Connect and migrate the database to Amazon DynamoDB using the AWS Database Migration Service (DMS)**

**Use the AWS Database Migration Service (DMS) to extract and load the data to an AWS Snowball Edge device. Complete the migration to Amazon DynamoDB using AWS DMS in the AWS Cloud**

**Enable compression on the MongoDB database and use the AWS Database Migration Service (DMS) to directly migrate the database to Amazon DynamoDB**

**Correct answer**

**Use the Schema Conversion Tool (SCT) to extract and load the data to an AWS Snowball Edge device. Use the AWS Database Migration Service (DMS) to migrate the data to Amazon DynamoDB**

Overall explanation

Larger data migrations with AWS DMS can include many terabytes of information. This process can be cumbersome due to network bandwidth limits or just the sheer amount of data. AWS DMS can use Snowball Edge and Amazon S3 to migrate large databases more quickly than by other methods.

When you're using an Edge device, the data migration process has the following stages:

1. You use the AWS Schema Conversion Tool (AWS SCT) to extract the data locally and move it to an Edge device.
2. You ship the Edge device or devices back to AWS.
3. After AWS receives your shipment, the Edge device automatically loads its data into an Amazon S3 bucket.
4. AWS DMS takes the files and migrates the data to the target data store. If you are using change data capture (CDC), those updates are written to the Amazon S3 bucket and then applied to the target data store.

**CORRECT:** "Use the Schema Conversion Tool (SCT) to extract and load the data to an AWS Snowball Edge device. Use the AWS Database Migration Service (DMS) to migrate the data to Amazon DynamoDB" is the correct answer.

**INCORRECT:** "Setup an AWS Direct Connect and migrate the database to Amazon DynamoDB using the AWS Database Migration Service (DMS)" is incorrect as Direct Connect connections can take several weeks to implement.

**INCORRECT:** "Enable compression on the MongoDB database and use the AWS Database Migration Service (DMS) to directly migrate the database to Amazon DynamoDB" is incorrect. It's unlikely that compression is going to make the difference and the company want to avoid the internet link as stated in the scenario.

**INCORRECT:** "Use the AWS Database Migration Service (DMS) to extract and load the data to an AWS Snowball Edge device. Complete the migration to Amazon DynamoDB using AWS DMS in the AWS Cloud" is incorrect. This is the wrong method, the Solutions Architect should use the SCT to extract and load to Snowball Edge and then AWS DMS in the AWS Cloud.

## References:

[https://docs.aws.amazon.com/dms/latest/userguide/CHAP\\_LargeDBs.html](https://docs.aws.amazon.com/dms/latest/userguide/CHAP_LargeDBs.html)

[https://docs.aws.amazon.com/dms/latest/userguide/CHAP\\_Target.DynamoDB.html](https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Target.DynamoDB.html)

## Save time with our AWS cheat sheets:

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

## Domain

AWS Migration & Transfer

### Question 42Skipped

A DevOps team uses an Amazon RDS MySQL database running for running resource-intensive tests each month. The instance has Performance Insights enabled and is only used once a month for up to 48 hours. As part of an effort to reduce AWS spend, the team wants to reduce the cost of running the tests without reducing the memory and compute attributes of the DB instance.

Which solution meets these requirements MOST cost-effectively?

### Correct answer

**Create a snapshot of the database when the tests are completed. Terminate the DB instance. Create a new DB instance from the snapshot when required.**

**Create an Auto Scaling group for the DB instance and reduce the desired capacity to 0 once the tests are completed.**

**Stop the DB instance once all tests are completed. Start the DB instance again when required.**

**Modify the DB instance size to a smaller capacity instance when all the tests have been completed. Scale up again when required.**

Overall explanation

Taking a snapshot of the instance and storing the snapshot is the most cost-effective solution. When needed, a new database can be created from the snapshot. Performance Insights can be enabled on the new instance if needed. Note that the previous data from Performance Insights will not be associated with the new instance, however this was not a requirement.

**CORRECT:** "Create a snapshot of the database when the tests are completed. Terminate the DB instance. Create a new DB instance from the snapshot when required" is the correct answer (as explained above.)

**INCORRECT:** "Stop the DB instance once all tests are completed. Start the DB instance again when required" is incorrect. You will be charged when your instance is stopped. When an instance is stopped you are charged for provisioned storage, manual snapshots, and automated backup storage within your specified retention window, but not for database instance hours. This is more costly compared to using snapshots.

**INCORRECT:** "Create an Auto Scaling group for the DB instance and reduce the desired capacity to 0 once the tests are completed" is incorrect. You cannot use Auto Scaling groups with Amazon RDS instances.

**INCORRECT:** "Modify the DB instance size to a smaller capacity instance when all the tests have been completed. Scale up again when required" is incorrect. This will reduce compute and memory capacity and will be more costly than taking a snapshot and terminating the DB.

**References:**

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_StopInstance.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_StopInstance.html)

**Save time with our AWS cheat sheets:**

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

**Domain**

AWS Database

**Question 43Skipped**

An application in a private subnet needs to query data in an Amazon DynamoDB table. Use of the DynamoDB public endpoints must be avoided. What is the most EFFICIENT and secure method of enabling access to the table?

**Create a private Amazon DynamoDB endpoint and connect to it using an AWS VPN**

**Create a software VPN between DynamoDB and the application in the private subnet**

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

**Correct answer**

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

Overall explanation

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection.

Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

With a gateway endpoint you configure your route table to point to the endpoint. Amazon S3 and DynamoDB use gateway endpoints.

The table below helps you to understand the key differences between the two different types of VPC endpoint:

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

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

**INCORRECT:** "Create an interface VPC endpoint in the VPC with an Elastic Network Interface (ENI)" is incorrect. This would be used for services that are supported by interface endpoints, not gateway endpoints.

**INCORRECT:** "Create a private Amazon DynamoDB endpoint and connect to it using an AWS VPN" is incorrect. You cannot create an Amazon DynamoDB private endpoint and connect to it over VPN. Private endpoints are VPC endpoints and are connected to by instances in subnets via route table entries or via ENIs (depending on which service).

**INCORRECT:** "Create a software VPN between DynamoDB and the application in the private subnet" is incorrect. You cannot create a software VPN between DynamoDB and an application.

#### References:

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

#### Save time with our AWS cheat sheets:

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

#### Domain

AWS Database

#### Question 44Skipped

A company needs to transfer data from an Amazon EC2 instance to an Amazon S3 bucket. The company must prevent API calls and data from being routed over the public internet and must use a private connection. Only the single EC2 instance can have access to upload data to the S3 bucket.

Which solution will meet these requirements?

#### Correct answer

**Create an Amazon S3 interface VPC endpoint in the subnet where the EC2 instance is located. Add a resource policy to the S3 bucket to allow only the EC2 instance's IAM role access.**



**Run the nslookup tool from inside your EC2 instance to obtain the private IP address of the S3 bucket's service API endpoint. Create a route in your VPCs route table to provide the EC2 instance with direct access to the S3 bucket. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.**

**Attach the appropriate security groups to the endpoint and use an S3 Bucket Policy on your S3 bucket to only allow the EC2 instance's IAM role access to the bucket.**

**Obtain the private IP address of the S3 bucket's service API endpoint through the management console. Create a route in the VPC route table to provide the EC2 instance with access to the S3 bucket. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.**

Overall explanation

You can use two types of VPC endpoints to access Amazon S3: *gateway endpoints* and *interface endpoints* (using AWS PrivateLink). A *gateway endpoint* is a gateway that you specify in your route table to access Amazon S3 from your VPC over the AWS network. *Interface endpoints* extend the functionality of gateway endpoints by using private IP addresses to route requests to Amazon S3 from within your VPC, on premises, or from a VPC in another AWS Region using VPC peering or AWS Transit Gateway.

Using an Interface endpoint to grant access to your S3 bucket from your EC2 instance is a safe and reliable way of traversing the AWS Global Backbone, instead of moving data over the public internet. Adding a resource policy to only allow the EC2 instance IAM role will lockdown the access to this EC2 instance only.

**CORRECT:** "Create an Amazon S3 interface VPC endpoint in the subnet where the EC2 instance is located. Add a resource policy to the S3 bucket to allow only the EC2 instance's IAM role access" is the correct answer (as explained above.)

**INCORRECT:** "Attach the appropriate security groups to the endpoint and use an S3 Bucket Policy on your S3 bucket to only allow the EC2 instance's IAM role access to the bucket" is incorrect. This would not prevent you from sending your traffic over the public internet, and you would not meet the requirements.

**INCORRECT:** "Run the nslookup tool from inside your EC2 instance to obtain the private IP address of the S3 bucket's service API endpoint. Create a route in your VPCs route table to provide the EC2 instance with direct access to the S3 bucket. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access" is incorrect also. You would not need to use nslookup - as using an interface endpoint manages all of this for you.

**INCORRECT:** "Obtain the private IP address of the S3 bucket's service API endpoint through the management console. Create a route in the VPC route table to provide the EC2 instance with access to the S3 bucket. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access" is incorrect. Finding the private IP address of the S3 bucket's service API endpoint is not possible through the console. Also this would not prevent you from sending your traffic over the public internet, and you would not meet the requirements.

**References:**

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html>

**Save time with our AWS cheat sheets:**

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

## **Domain**

AWS Networking & Content Delivery

### **Question 45Skipped**

A critical web application that runs on a fleet of Amazon EC2 Linux instances has experienced issues due to failing EC2 instances. The operations team have investigated and determined that insufficient swap space is a likely cause. The operations team require a method of monitoring the swap space on the EC2 instances.

What should a Solutions Architect recommend?

**Use EC2 metadata to collect information, then publish it to Amazon CloudWatch custom metrics. Monitor Swap Usage metrics in CloudWatch.**

### **Correct answer**

**Install and configure the unified CloudWatch agent on the EC2 instances. Monitor Swap Utilization metrics in CloudWatch.**

**Create a custom metric in Amazon CloudWatch that monitors Swap Usage. Monitor Swap Usage metrics in CloudWatch.**

**Enable detailed monitoring in the EC2 console. Create an Amazon CloudWatch SwapUtilization custom metric and monitor the metric in CloudWatch.**

Overall explanation

The unified CloudWatch agent enables you to collect internal system-level metrics from Amazon EC2 instances across operating systems. The metrics can include in-guest metrics, in addition to the metrics for EC2 instances. The metrics that are collected include swap\_free, swap\_used, and swap\_used\_percent.

**CORRECT:** "Install and configure the unified CloudWatch agent on the EC2 instances. Monitor Swap Utilization metrics in CloudWatch" is the correct answer.

**INCORRECT:** "Create a custom metric in Amazon CloudWatch that monitors Swap Usage. Monitor Swap Usage metrics in CloudWatch" is incorrect. You cannot create a custom metric for swap utilization as this data is not collected without the CloudWatch agent.

**INCORRECT:** "Use EC2 metadata to collect information, then publish it to Amazon CloudWatch custom metrics. Monitor Swap Usage metrics in CloudWatch" is incorrect. You cannot collect performance metrics with EC2 metadata.

**INCORRECT:** "Enable detailed monitoring in the EC2 console. Create an Amazon CloudWatch SwapUtilization custom metric and monitor the metric in CloudWatch" is incorrect. Detailed monitoring changes the frequency of metric reporting but does not include the swap utilization data as you must install the CloudWatch agent to collect that info.

**References:**

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

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/metrics-collected-by-CloudWatch-agent.html>

**Save time with our AWS cheat sheets:**

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

## Domain

AWS Management & Governance

### Question 46Skipped

An Amazon S3 bucket is going to be used by a company to store sensitive data. A Solutions Architect needs to ensure that all objects uploaded to an Amazon S3 bucket are encrypted. How can this be achieved?

**Create a bucket policy that denies Put requests that do not have an s3:x-amz-acl header set.**

**Create a bucket policy that denies Put requests that do not have an aws:Secure Transport header set to true.**

### Correct answer

**Create a bucket policy that denies Put requests that do not have an x-amz-server-side-encryption header set.**

**Create a bucket policy that denies Put requests that do not have an s3:x-amz-acl header set to private.**

### Overall explanation

To encrypt an object at the time of upload, you need to add a header called x-amz-server-side-encryption to the request to tell S3 to encrypt the object using SSE-C, SSE-S3, or SSE-KMS.

To enforce object encryption, create an S3 bucket policy that denies any S3 Put request that does not include the x-amz-server-side-encryption header. There are two possible values for the x-amz-server-side-encryption header: AES256, which tells S3 to use S3-managed keys, and aws:kms, which tells S3 to use AWS KMS-managed keys.

The example policy below denies Put requests that do not have the correct encryption header set:

```

{
  "Version": "2012-10-17",
  "Id": "PutObjPolicy",
  "Statement": [
    {
      "Sid": "DenyIncorrectEncryptionHeader",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::<bucket_name>/*",
      "Condition": {
        "StringNotEquals": {
          "s3:x-amz-server-side-encryption": "AES256"
        }
      }
    },
    {
      "Sid": "DenyUnEncryptedObjectUploads",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::<bucket_name>/*",
      "Condition": {
        "Null": {
          "s3:x-amz-server-side-encryption": true
        }
      }
    }
  ]
}

```

**CORRECT:** "Create a bucket policy that denies Put requests that do not have an x-amz-server-side-encryption header set" is the correct answer.

**INCORRECT:** "Create a bucket policy that denies Put requests that do not have an s3:x-amz-acl header set" is incorrect. This header is not for encryption.

**INCORRECT:** "Create a bucket policy that denies Put requests that do not have an s3:x-amz-acl header set to private" is incorrect. This header is not for encryption.

**INCORRECT:** "Create a bucket policy that denies Put requests that do not have an aws:Secure Transport header set to true" is incorrect. This header is used for SSL/TLS.

#### References:

<https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/>

#### Save time with our AWS cheat sheets:

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

#### Domain

AWS Storage

#### Question 47Skipped

A company is migrating an eCommerce application into the AWS Cloud. The application uses an SQL database, and the database will be migrated to Amazon RDS. A Solutions Architect has

been asked to recommend a method to attain sub-millisecond responses to common read requests.

What should the solutions architect recommend?

**Correct answer**

**Deploy a database cache using Amazon ElastiCache.**

**Deploy Amazon RDS read replicas.**

**Deploy a database cache using Amazon DynamoDB Accelerator.**

**Use Amazon EBS Provisioned IOPS volumes.**

Overall explanation

Amazon ElastiCache is a fully managed in-memory data store and cache service. ElastiCache can be used to cache requests to an Amazon RDS database through application configuration. This can greatly improve performance as ElastiCache can return responses to queries with sub-millisecond latency.

**CORRECT:** "Deploy a database cache using Amazon ElastiCache" is the correct answer.

**INCORRECT:** "Deploy a database cache using Amazon DynamoDB Accelerator" is incorrect. DynamoDB DAX cannot be used with RDS or SQL databases.

**INCORRECT:** "Deploy Amazon RDS read replicas" is incorrect. Read replicas will not provide sub-millisecond response times to queries.

**INCORRECT:** "Use Amazon EBS Provisioned IOPS volumes" is incorrect. This will not improve response times for queries to the database to the level required.

**References:**

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

**Save time with our AWS cheat sheets:**

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

**Domain**

AWS Database

**Question 48Skipped**

A company is testing a new web application that runs on Amazon EC2 instances. A Solutions Architect is performing load testing and must be able to analyze the performance of the web application with a granularity of 1 minute.

What should the Solutions Architect do to meet this requirement?

**Send Amazon CloudWatch logs to Amazon S3. Use Amazon Athena to perform the analysis.**

**Create an AWS CloudTrail trail and log data events. Use Amazon Athena to query the CloudTrail logs.**

**Create an AWS Lambda function to fetch EC2 logs from Amazon CloudWatch Logs. Use Amazon CloudWatch metrics to perform the analysis.**

**Correct answer**

**Enable detailed monitoring on all EC2 instances. Use Amazon CloudWatch metrics to perform the analysis.**

Overall explanation

By default, your instance is enabled for basic monitoring. You can optionally enable detailed monitoring. After you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period for the instance.

The following describes the data interval and charge for basic and detailed monitoring for instances:

Monitoring type	Description	Charges
Basic monitoring	Data is available automatically in 5-minute periods.	No charge
Detailed monitoring	Data is available in 1-minute periods. To get this level of data, you must specifically enable it for the instance. For the instances where you've enabled detailed monitoring, you can also get aggregated data across groups of similar instances.	You are charged per metric that is sent to CloudWatch. You are not charged for data storage. For more information, see <b>Paid tier</b> and <b>Example 1 - EC2 Detailed Monitoring</b> on the <a href="#">Amazon CloudWatch pricing page</a> .

**CORRECT:** "Enable detailed monitoring on all EC2 instances. Use Amazon CloudWatch metrics to perform the analysis" is the correct answer.

**INCORRECT:** "Send Amazon CloudWatch logs to Amazon S3. Use Amazon Athena to perform the analysis" is incorrect. You must enable detailed monitoring to get data in 1-minute periods.

**INCORRECT:** "Create an AWS Lambda function to fetch EC2 logs from Amazon CloudWatch Logs. Use Amazon CloudWatch metrics to perform the analysis" is incorrect. There is no need to use a Lambda function to retrieve the logs and detailed monitoring must still be enabled.

**INCORRECT:** "Create an AWS CloudTrail trail and log data events. Use Amazon Athena to query the CloudTrail logs" is incorrect. This will not assist with gathering the required data from EC2 instances. Detailed monitoring must be enabled instead.

**References:**

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-cloudwatch-new.html>

**Save time with our AWS cheat sheets:**

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

**Domain**

AWS Compute

**Question 49**Skipped

A storage company creates and emails PDF statements to their customers at the end of each month. Customers must be able to download their statements from the company website for

up to 30 days from when the statements were generated. When customers close their accounts, they are emailed a ZIP file that contains all the statements.

What is the MOST cost-effective storage solution for this situation?

**Store the statements using the Amazon S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Create a lifecycle policy to move the statements to Amazon S3 Intelligent Tiering storage after 30 days.**

**Store the statements using the Amazon S3 Standard storage class. Create a lifecycle policy to move the statements to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) storage after 30 days.**

**Store the statements using the Amazon S3 Glacier storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier Deep Archive storage after 30 days.**

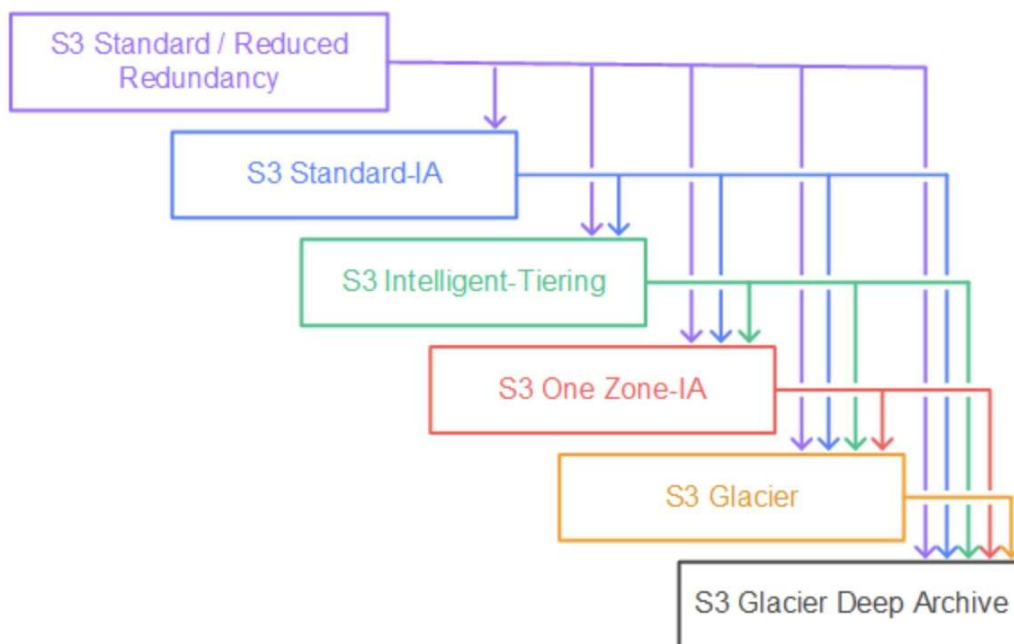
**Correct answer**

**Store the statements using the Amazon S3 Standard storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 30 days.**

Overall explanation

The most cost-effective option is to store the PDF files in S3 Standard for 30 days where they can be easily downloaded by customers. Then, transition the objects to Amazon S3 Glacier which will reduce the storage costs. When a customer closes their account, the objects can be retrieved from S3 Glacier and provided to the customer as a ZIP file.

Be cautious of subtle changes to the answer options in questions like these as you may see several variations of similar questions on the exam. Also, be aware of the supported transitions (below) and minimum storage durations.



**CORRECT:** "Store the statements using the Amazon S3 Standard storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier storage after 30 days" is the correct answer.

**INCORRECT:** "Store the statements using the Amazon S3 Glacier storage class. Create a lifecycle policy to move the statements to Amazon S3 Glacier Deep Archive storage after 30 days" is incorrect. Using Glacier will not allow customers to download their statements as the files would need to be restored. Also, the minimum storage duration before you can transition from Glacier is 90 days.

**INCORRECT:** "Store the statements using the Amazon S3 Standard storage class. Create a lifecycle policy to move the statements to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) storage after 30 days" is incorrect. This would work but is not as cost-effective as using Glacier for the longer-term storage.

**INCORRECT:** "Store the statements using the Amazon S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Create a lifecycle policy to move the statements to Amazon S3 Intelligent Tiering storage after 30 days" is incorrect. This would work but is not as cost-effective as using Glacier for the longer-term storage.

#### **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 50Skipped**

A company are finalizing their disaster recovery plan. A limited set of core services will be replicated to the DR site ready to seamlessly take over the in the event of a disaster. All other services will be switched off.

Which DR strategy is the company using?

#### **Backup and restore**

#### **Correct answer**

#### **Pilot light**

#### **Warm standby**

#### **Multi-site**

Overall explanation

In this DR approach, you simply replicate part of your IT structure for a limited set of core services so that the AWS cloud environment seamlessly takes over in the event of a disaster.



A small part of your infrastructure is always running simultaneously syncing mutable data (as databases or documents), while other parts of your infrastructure are switched off and used only during testing.

Unlike a backup and recovery approach, you must ensure that your most critical core elements are already configured and running in AWS (the pilot light). When the time comes for recovery, you can rapidly provision a full-scale production environment around the critical core.

**CORRECT:** "Pilot light" is the correct answer.

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

**INCORRECT:** "Warm standby" is incorrect. The term warm standby is used to describe a DR scenario in which a scaled-down version of a fully functional environment is always running in the cloud.

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

#### **References:**

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

#### **Domain**

AWS Cloud Architecture & Design

#### **Question 51 Skipped**

An application is being monitored using Amazon GuardDuty. A Solutions Architect needs to be notified by email of medium to high severity events. How can this be achieved?

**Create an Amazon CloudWatch Logs rule that triggers an AWS Lambda function**

**Correct answer**

**Create an Amazon CloudWatch events rule that triggers an Amazon SNS topic**

**Configure an Amazon CloudWatch alarm that triggers based on a GuardDuty metric**

**Configure an Amazon CloudTrail alarm the triggers based on GuardDuty API activity**

Overall explanation

A CloudWatch Events rule can be used to set up automatic email notifications for Medium to High Severity findings to the email address of your choice. You simply create an Amazon SNS topic and then associate it with an Amazon CloudWatch events rule.

Note: step by step procedures for how to set this up can be found in the article linked in the references below.

**CORRECT:** "Create an Amazon CloudWatch events rule that triggers an Amazon SNS topic" is the correct answer.

**INCORRECT:** "Configure an Amazon CloudWatch alarm that triggers based on a GuardDuty metric" is incorrect. There is no metric for GuardDuty that can be used for specific findings.

**INCORRECT:** "Create an Amazon CloudWatch Logs rule that triggers an AWS Lambda function" is incorrect. CloudWatch logs is not the right CloudWatch service to use. CloudWatch events is used for reacting to changes in service state.

**INCORRECT:** "Configure an Amazon CloudTrail alarm the triggers based on GuardDuty API activity" is incorrect. CloudTrail cannot be used to trigger alarms based on GuardDuty API activity.

#### References:

[https://docs.aws.amazon.com/guardduty/latest/ug/guardduty\\_findings\\_cloudwatch.html](https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings_cloudwatch.html)

#### Save time with our AWS cheat sheets:

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

#### Domain

AWS Application Integration

#### Question 52Skipped

A company runs a legacy application that uses an Amazon RDS MySQL database without encryption. The security team has instructed a Solutions Architect to encrypt the database due to new compliance requirements.

How can the Solutions Architect encrypt all existing and new data in the database?

**Add an RDS read replica with encryption at rest enabled. Promote the read replica to master and then delete the original database instance.**

#### Correct answer

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

**Enable Multi-AZ mode for the database and enable encryption at rest. Perform a manual failover to the standby and delete the original database instance.**

**Create an Amazon S3 bucket with server-side encryption enabled. Move all the data to Amazon S3. Delete the RDS instance.**

#### Overall explanation

This comes up on almost every exam so be prepared! The key fact to remember is that you cannot alter the encryption state of an RDS database after you have deployed it. You also cannot create encrypted replicas from unencrypted instances.

The only solution is to create a snapshot (which will be unencrypted) and subsequently create an encrypted copy of the snapshot. You can then create a new database instance from the encrypted snapshot. The new database will be encrypted and will have a new endpoint address.

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

**INCORRECT:** "Create an Amazon S3 bucket with server-side encryption enabled. Move all the data to Amazon S3. Delete the RDS instance" is incorrect. S3 is an object storage system and not a replacement for a relational MySQL database.

**INCORRECT:** "Enable Multi-AZ mode for the database and enable encryption at rest. Perform a manual failover to the standby and delete the original database instance" is incorrect. You cannot enable encryption after creation of the database, and this includes for any instances created from the database such as replicas and multi-AZ standby instances.

**INCORRECT:** "Add an RDS read replica with encryption at rest enabled. Promote the read replica to master and then delete the original database instance" is incorrect. You cannot enable encryption on a read replica when the primary database is unencrypted.

#### References:

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

#### Save time with our AWS cheat sheets:

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

#### Domain

AWS Database

#### Question 53Skipped

A social media company has a Microsoft .NET application that currently runs on an on-premises Windows Server. The application uses an Oracle Database Standard Edition server for its database layer.

The company is planning to migrate this application to AWS and wants to minimize development changes while moving the application, due to limited staff resources. The AWS application environment should however not compromise on being highly available.

Which two actions should the company take to meet these requirements? (Select TWO.)

**Use the AWS Database Migration Service (AWS DMS) to migrate the database from the Oracle database to an Amazon DynamoDB table in a Multi-AZ configuration.**

**Refactor the application into a serverless solution with multiple Lambda functions running .NET Core.**

#### Correct selection

**Redeploy the application in Elastic Beanstalk with the .NET platform provisioned in a Multi-AZ configuration.**

#### Correct selection

**Migrate from Oracle to Oracle on Amazon RDS using the AWS Database Migration Service (AWS DMS).**

**Migrate the server to Amazon EC2 using an Amazon Linux Amazon Machine Image (AMI).**

Overall explanation

AWS Elastic Beanstalk in a multi-AZ configuration is an ideal platform for running the application. This is a PaaS service, and the developers only need to add the code. The deployment also provides the required high availability as a multi-AZ deployment will include Auto Scaling and Load Balancing.

For the database tier, AWS DMS can be used to migrate the database to an Amazon RDS managed database service using the Oracle DB engine. This requires a minimum of changes and provides high availability.

**CORRECT:** "Redeploy the application in Elastic Beanstalk with the .NET platform provisioned in a Multi-AZ configuration" is the correct answer (as explained above.)

**CORRECT:** "Migrate from Oracle to Oracle on Amazon RDS using the AWS Database Migration Service (AWS DMS)" is also the correct answer (as explained above.)

**INCORRECT:** "Refactor the application into a serverless solution with multiple Lambda functions running .NET Core" is incorrect. This would involve substantial application changes and would not meet the specific requirements of the migration.

**INCORRECT:** "Migrate the server to Amazon EC2 using an Amazon Linux Amazon Machine Image (AMI)" is incorrect. There is no high availability in this solution unless deployed using Auto Scaling and a Load Balancer.

**INCORRECT:** "Use the AWS Database Migration Service (AWS DMS) to migrate the database from the Oracle database to an Amazon DynamoDB table in a Multi-AZ configuration" is incorrect. DynamoDB is a NoSQL Database whereas Oracle is a SQL based database, meaning that the database's schema would have to be radically changed to accommodate the DynamoDB database. DynamoDB also does not have a feature known as multi-AZ.

#### References:

<https://aws.amazon.com/dms/>

#### Save time with our AWS cheat sheets:

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

#### Domain

AWS Compute

#### Question 54Skipped

A HR application stores employment records on Amazon S3. Regulations mandate the records are retained for seven years. Once created the records are accessed infrequently for the first three months and then must be available within 10 minutes if required thereafter.

Which lifecycle action meets the requirements whilst MINIMIZING cost?

**Store the data in S3 Standard for 3 months, then transition to S3 Glacier**

**Store the data in S3 Standard for 3 months, then transition to S3 Standard-IA**

**Store the data in S3 Intelligent Tiering for 3 months, then transition to S3 Standard-IA**

**Correct answer**

### **Store the data in S3 Standard-IA for 3 months, then transition to S3 Glacier**

Overall explanation

The most cost-effective solution is to first store the data in S3 Standard-IA where it will be infrequently accessed for the first three months. Then, after three months expires, transition the data to S3 Glacier where it can be stored at lower cost for the remainder of the seven year period. Expedited retrieval can bring retrieval times down to 1-5 minutes.

**CORRECT:** "Store the data in S3 Standard-IA for 3 months, then transition to S3 Glacier" is the correct answer.

**INCORRECT:** "Store the data in S3 Standard for 3 months, then transition to S3 Glacier" is incorrect. S3 Standard is more costly than S3 Standard-IA and the data is only accessed infrequently.

**INCORRECT:** "Store the data in S3 Standard for 3 months, then transition to S3 Standard-IA" is incorrect. Neither storage class in this answer is the most cost-effective option.

**INCORRECT:** "Store the data in S3 Intelligent Tiering for 3 months, then transition to S3 Standard-IA" is incorrect. Intelligent tiering moves data between tiers based on access patterns, this is more costly and better suited to use cases that are unknown or unpredictable.

#### **References:**

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

<https://docs.aws.amazon.com/amazonglacier/latest/dev/downloading-an-archive-two-steps.html#api-downloading-an-archive-two-steps-retrieval-options>

#### **Save time with our AWS cheat sheets:**

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

#### **Domain**

AWS Storage

#### **Question 55Skipped**

Three Amazon VPCs are used by a company in the same region. The company has two AWS Direct Connect connections to two separate company offices and wishes to share these with all three VPCs. A Solutions Architect has created an AWS Direct Connect gateway. How can the required connectivity be configured?

#### **Correct answer**

**Associate the Direct Connect gateway to a transit gateway**

**Associate the Direct Connect gateway to a virtual private gateway in each VPC**

**Create a transit virtual interface between the Direct Connect gateway and each VPC**

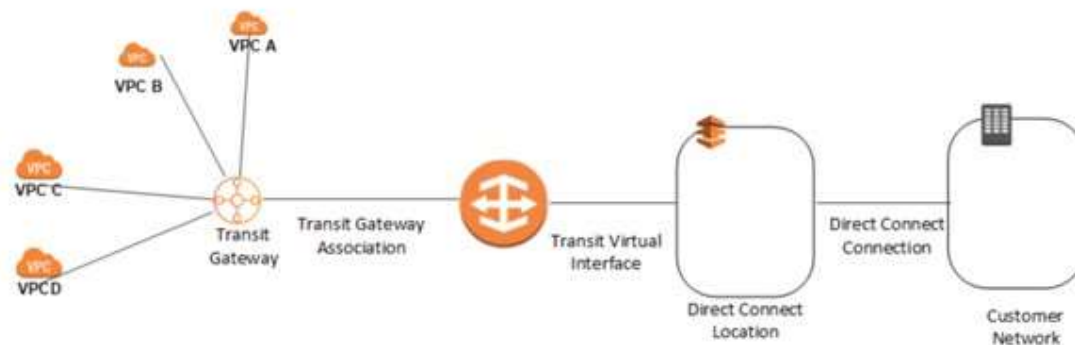
**Create a VPC peering connection between the VPCs and route entries for the Direct Connect Gateway**

Overall explanation

You can manage a single connection for multiple VPCs or VPNs that are in the same Region by associating a Direct Connect gateway to a transit gateway. The solution involves the following components:

- A transit gateway that has VPC attachments.
- A Direct Connect gateway.
- An association between the Direct Connect gateway and the transit gateway.
- A transit virtual interface that is attached to the Direct Connect gateway.

The following diagram depicts this configuration:



**CORRECT:** "Associate the Direct Connect gateway to a transit gateway" is the correct answer.

**INCORRECT:** "Associate the Direct Connect gateway to a virtual private gateway in each VPC" is incorrect. For VPCs in the same region a VPG is not necessary. A transit gateway can instead be configured.

**INCORRECT:** "Create a VPC peering connection between the VPCs and route entries for the Direct Connect Gateway" is incorrect. You cannot add route entries for a Direct Connect gateway to each VPC and enable routing. Use a transit gateway instead.

**INCORRECT:** "Create a transit virtual interface between the Direct Connect gateway and each VPC" is incorrect. The transit virtual interface is attached to the Direct Connect gateway on the connection side, not the VPC/transit gateway side.

#### References:

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

Save time with our AWS cheat sheets:

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

#### Domain

AWS Networking & Content Delivery

Question 56Skipped

A company runs a legacy application on an Amazon EC2 Linux instance. The application code cannot be modified, and the system cannot run on more than one instance. A Solutions Architect must design a resilient solution that can improve the recovery time for the system.

What should the Solutions Architect recommend to meet these requirements?

**Launch the EC2 instance with two Amazon EBS volumes and configure RAID 0.**

**Deploy the EC2 instance in a cluster placement group in an Availability Zone.**

**Create an Amazon CloudWatch alarm to recover the EC2 instance in case of failure.**

**Correct answer**

**Launch the EC2 instance with two Amazon EBS volumes and configure RAID 1.**

Overall explanation

A RAID array uses multiple EBS volumes to improve performance or redundancy. When fault tolerance is more important than I/O performance a RAID 1 array should be used which creates a mirror of your data for extra redundancy.

The following table summarizes the differences between RAID 0 and RAID 1:

Configuration	Use	Advantages	Disadvantages
RAID 0	When I/O performance is more important than fault tolerance; for example, as in a heavily used database (where data replication is already set up separately).	I/O is distributed across the volumes in a stripe. If you add a volume, you get the straight addition of throughput and IOPS.	Performance of the stripe is limited to the worst performing volume in the set. Loss of a single volume results in a complete data loss for the array.
RAID 1	When fault tolerance is more important than I/O performance; for example, as in a critical application.	Safer from the standpoint of data durability.	Does not provide a write performance improvement; requires more Amazon EC2 to Amazon EBS bandwidth than non-RAID configurations because the data is written to multiple volumes simultaneously.

**CORRECT:** Launch the EC2 instance with two Amazon EBS volumes and configure RAID 1 is the correct answer.

**INCORRECT:** "Launch the EC2 instance with two Amazon EBS volumes and configure RAID 0" is incorrect. RAID 0 is used for striping which improves performance but not redundancy.

**INCORRECT:** "Create an Amazon CloudWatch alarm to recover the EC2 instance in case of failure" is incorrect. This does not improve recovery time it just attempts to fix issues relating to the underlying hardware.

**INCORRECT:** "Deploy the EC2 instance in a cluster placement group in an Availability Zone" is incorrect. You cannot gain any advantages by deploying a single instance into a cluster placement group.

**References:**

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/raid-config.html>

**Save time with our AWS cheat sheets:**

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

## Domain

AWS Compute

### Question 57Skipped

A Solutions Architect is migrating a distributed application from their on-premises environment into AWS. This application consists of an Apache Cassandra NoSQL database, with a containerized SUSE Linux compute layer with an additional storage layer made up of multiple Microsoft SQL Server databases. Once in the cloud the company wants to have as little operational overhead as possible, with no schema conversion during the migration and the company wants to host the architecture in a highly available and durable way.

Which of the following groups of services will provide the solutions architect with the best solution ?

**Run the NoSQL database on DynamoDB, and the compute layer on Amazon ECS on Fargate. Use Amazon RDS for Microsoft SQL Server to host the second storage layer.**

**Run the NoSQL database on Amazon Keyspaces, and the compute layer on Amazon ECS on Fargate. Use Amazon Aurora to host the second storage layer.**

**Run the NoSQL database on DynamoDB, and the compute layer on Amazon ECS on EC2. Use Amazon RDS for Microsoft SQL Server to host the second storage layer.**

### Correct answer

**Run the NoSQL database on Amazon Keyspaces, and the compute layer on Amazon ECS on Fargate. Use Amazon RDS for Microsoft SQL Server to host the second storage layer.**

### Overall explanation

Amazon Keyspaces (for Apache Cassandra) is a scalable, highly available, and managed Apache Cassandra-compatible database service. This combined with a containerized, serverless compute layer on Amazon ECS for Fargate and a RDS for Microsoft SQL Server database layer is a fully managed version of what currently exists on premises.

**CORRECT:** "Run the NoSQL database on Amazon Keyspaces, and the compute layer on Amazon ECS on Fargate. Use Amazon RDS for Microsoft SQL Server to host the second storage layer" is the correct answer (as explained above.)

**INCORRECT:** "Run the NoSQL database on DynamoDB, and the compute layer on Amazon ECS on EC2. Use Amazon RDS for Microsoft SQL Server to host the second storage layer" is incorrect. DynamoDB is not a managed version of DynamoDB therefore it is not the correct answer.

**INCORRECT:** "Run the NoSQL database on DynamoDB, and the compute layer on Amazon ECS on Fargate. Use Amazon RDS for Microsoft SQL Server to host the second storage layer" is incorrect. DynamoDB is not a managed version of DynamoDB therefore it is not the correct answer.

**INCORRECT:** "Run the NoSQL database on Amazon Keyspaces, and the compute layer on Amazon ECS on Fargate. Use Amazon Aurora to host the second storage layer" is incorrect.



Amazon Aurora does not have an option to run a Microsoft SQL Server database, therefore this answer is not correct.

**References:**

<https://aws.amazon.com/keyspaces/>

**Save time with our AWS cheat sheets:**

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

**Domain**

AWS Database

**Question 58**Skipped

A large customer services company is planning to build a highly scalable and durable application designed to aggregate data across their support communications, and extract sentiment on how successfully they are helping their customers. These communications are generated across chat, social media, emails and more. They need a solution which stores output from these communication channels, which then processes the text for sentiment analysis. The outputs must then be stored in a data warehouse for future use.

Which series of AWS services will provide the functionality the company is looking for?

**Use DynamoDB as the original data store for the output from the support communications. Use Amazon Kendra to process the text for sentiment analysis. Then store the outputs in Amazon RedShift.**

**Correct answer**

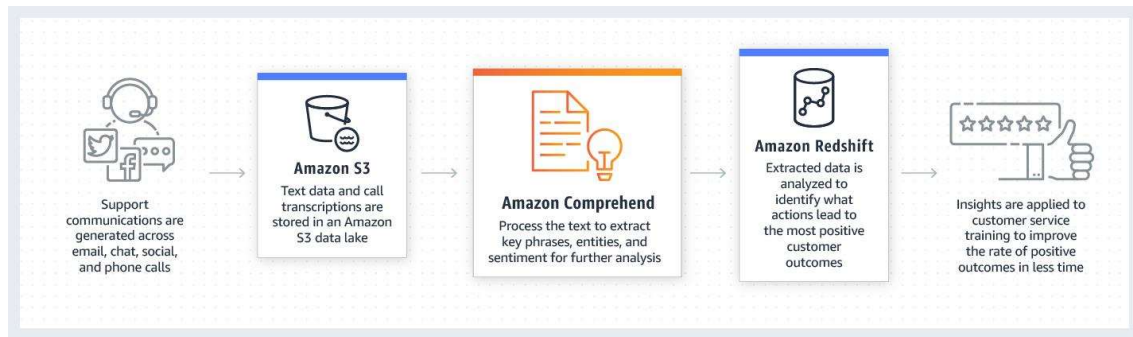
**Use an Amazon S3 Data Lake as the original date store for the output from the support communications. Use Amazon Comprehend to process the text for sentiment analysis. Then store the outputs in Amazon RedShift.**

**Use DynamoDB as the original data store for the output from the support communications. Use Amazon Comprehend to process the text for sentiment analysis. Then store the outputs in Amazon RedShift.**

**Use an Amazon S3 Data Lake as the original date store for the output from the support communications. Use Amazon Textract to process the text for sentiment analysis. Then store the outputs in Amazon RedShift.**

**Overall explanation**

Amazon Comprehend is a natural-language processing (NLP) service that uses machine learning to uncover valuable insights and connections in text.



You could easily use Amazon Comprehend to detect customer sentiment and analyze customer interactions and automatically extract insights from customer surveys to improve your products. An S3 Data Lake also acts as an ideal data repository for Machine Learning data used by many different business units and applications.

**CORRECT:** "Use an Amazon S3 Data Lake as the original data store for the output from the support communications. Use Amazon Comprehend to process the text for sentiment analysis. Then store the outputs in Amazon RedShift" is the correct answer (as explained above.)

**INCORRECT:** "Use an Amazon S3 Data Lake as the original data store for the output from the support communications. Use Amazon Textract to process the text for sentiment analysis. Then store the outputs in Amazon RedShift" is incorrect. Amazon Textract is a machine learning (ML) service that automatically extracts text, handwriting, and data from scanned documents, and does not output any sentiment.

**INCORRECT:** "Use DynamoDB as the original data store for the output from the support communications. Use Amazon Comprehend to process the text for sentiment analysis. Then store the outputs in Amazon RedShift" is incorrect. DynamoDB is not as suitable of a data repository for machine learning data like an Amazon S3 Data Lake would be.

**INCORRECT:** "Use DynamoDB as the original data store for the output from the support communications. Use Amazon Kendra to process the text for sentiment analysis. Then store the outputs in Amazon RedShift" is incorrect. DynamoDB is not as suitable of a data repository for machine learning data like an Amazon S3 Data Lake would be, and Amazon Kendra is a highly accurate intelligent search service powered by machine learning and does not work to understand sentiment.

#### References:

<https://aws.amazon.com/comprehend/>

#### Domain

AWS Storage

#### Question 59Skipped

A dynamic website runs on Amazon EC2 instances behind an Application Load Balancer (ALB). Users are distributed around the world, and many are reporting poor website performance. The company uses Amazon Route 53 for DNS.

Which set of actions will improve website performance while minimizing cost?

**Launch new EC2 instances running the website and ALBs in different Regions. Use AWS Global Accelerator to direct connections 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.**

**Host the website in an Amazon S3 bucket and delete the ALB and EC2 instances. Enable transfer acceleration and update the Amazon Route 53 record to point to the S3 bucket.**

**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.**

Overall explanation

The most cost-effective option for improving performance is to create an Amazon CloudFront distribution. CloudFront can be used to serve both static and dynamic content. This solution will ensure that wherever users are located they will experience improved performance due to the caching of content and the usage of the AWS global network.

**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:** "Launch new EC2 instances running the website and ALBs in different Regions. Use AWS Global Accelerator to direct connections to the closest Region" is incorrect. This is a more costly solution as there are more EC2 instances, ALBs, and Global Accelerator. Using CloudFront would be a better solution for this use case.

**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. With only one ALB latency-based record serves no purpose. Additionally, using larger instances sizes may not assist as it does not reduce latency for global users.

**INCORRECT:** "Host the website in an Amazon S3 bucket and delete the ALB and EC2 instances. Enable transfer acceleration and update the Amazon Route 53 record to point to the S3 bucket" is incorrect. Transfer acceleration offers performance benefits for uploading and downloading content to/from S3 buckets but the S3 bucket can only serve static content, not a dynamic website.

**References:**

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

**Save time with our AWS cheat sheets:**

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

**Domain**

AWS Networking & Content Delivery

**Question 60**Skipped

A company runs a containerized application on a Kubernetes cluster in an on-premises data center. The application uses a MongoDB Database to store data. The application will be migrated to AWS, but no code changes or deployment method changes are possible at this time due to a constraint in time and resources. Operational efficiency is critical.

Which solution meets these requirements?

**Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate for compute and Amazon DynamoDB for the data storage.**

**Correct answer**

**Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate for compute and Amazon DocumentDB (with MongoDB compatibility) for data storage.**

**Use Amazon Elastic Container Service (Amazon ECS) with worker nodes on Amazon EC2 for compute, as well as and MongoDB on EC2 for data storage.**

**Use Amazon Elastic Kubernetes Service (Amazon EKS) with worker nodes on Amazon EC2 for compute and Amazon DynamoDB for data storage.**

Overall explanation

The easiest way to lift this application out of the data center with minimal code changes is to use the Elastic Kubernetes Service (Amazon EKS) on Fargate for the compute tier and Amazon DocumentDB (with MongoDB compatibility) for data storage.

**CORRECT:** "Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate for compute and Amazon DocumentDB (with MongoDB compatibility) for data storage" is the correct answer (as explained above.)

**INCORRECT:** "Use Amazon Elastic Container Service (Amazon ECS) with worker nodes on Amazon EC2 for compute, as well as and MongoDB on EC2 for data storage" is incorrect. Using Amazon ECS will take some application refactoring, so it involves code changes and is not operationally efficient.

**INCORRECT:** "Use Amazon Elastic Kubernetes Service (Amazon EKS) with worker nodes on Amazon EC2 for compute and Amazon DynamoDB for data storage" is incorrect. Using DynamoDB would take a refactoring of the application code and is not operationally efficient.

**INCORRECT:** "Use Amazon Elastic Container Service (Amazon ECS) with worker nodes on Amazon EC2 for compute, as well as and MongoDB on EC2 for data storage" Using Amazon ECS will take some application refactoring, so it is not operationally efficient.

**References:**

<https://aws.amazon.com/ecs/>

**Save time with our AWS cheat sheets:**

<https://digitalcloud.training/category/aws-cheat-sheets/aws-compute/>

**Domain**

AWS Compute

## Question 61Skipped

An application runs across a fleet of Amazon EC2 instances and uses a shared file system hosted on Amazon EFS. The file system is used for storing many files that are generated by the application. The files are only accessed for the first few days after creation but must be retained.

How can a Solutions Architect optimize storage costs for the application?

### Correct answer

**Configure a lifecycle policy to move the files to the EFS Infrequent Access (IA) storage class after 7 days.**

**Move the files to an instance store on each Amazon EC2 instance after 7 days.**

**Implement AWS Storage Gateway and transition files to Amazon S3 after 7 days.**

**Configure a lifecycle policy to move the files to the S3 Standard-IA storage class after 7 days.**

Overall explanation

The solution uses Amazon EFS, and the files are only accessed for a few days. To reduce storage costs the Solutions Architect can configure the AFTER\_7\_DAYS lifecycle policy to transition the files to the IA storage class 7 days after the files are last accessed.

You define when Amazon EFS transitions files an IA storage class by setting a lifecycle policy. A file system has one lifecycle policy that applies to the entire file system. If a file is not accessed for the period of time defined by the lifecycle policy that you choose, Amazon EFS transitions the file to the IA storage class that is applicable to your file system.

**CORRECT:** "Configure a lifecycle policy to move the files to the EFS Infrequent Access (IA) storage class after 7 days" is the correct answer.

**INCORRECT:** "Implement AWS Storage Gateway and transition files to Amazon S3 after 7 days" is incorrect. Storage Gateway is used for using cloud storage from on-premises systems. It is not used for transitioning data from EFS.

**INCORRECT:** "Move the files to an instance store on each Amazon EC2 instance after 7 days" is incorrect. This would put the files at risk of loss as instance stores are ephemeral.

**INCORRECT:** "Configure a lifecycle policy to move the files to the S3 Standard-IA storage class after 7 days" is incorrect. You cannot create a lifecycle policy in EFS that transitions files to Amazon S3.

### References:

<https://docs.aws.amazon.com/efs/latest/ug/lifecycle-management-efs.html>

**Save time with our AWS cheat sheets:**

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

### Domain

AWS Storage

## Question 62Skipped

A large online retail company manages and runs an online e-commerce web application on AWS. This application serves hundreds of thousands of concurrent users during their peak operating hours, and as a result the company needs a highly scalable, near-real-time solution to share the order details with several other internal applications for order processing. Some additional processing to remove sensitive data also needs to occur before being stored in a document database for low-latency retrieval.

What should a solutions architect recommend to meet these requirements?

**Store the batched transactions data in Amazon S3 as files. Use AWS Lambda to process every file and remove sensitive data before updating the files in Amazon S3. The Lambda function then stores the data in Amazon DynamoDB. Other applications can consume transaction files stored in Amazon S3.**

**Stream the transactions data into Amazon Kinesis Data Firehose to store data in Amazon DynamoDB and Amazon S3. Use AWS Lambda integration with Kinesis Data Firehose to remove sensitive data. Other applications can consume the data stored in Amazon S3.**

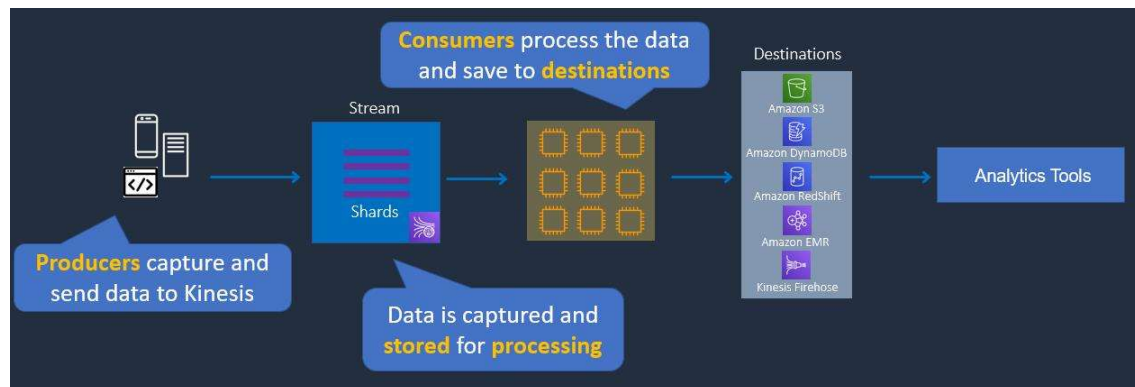
**Store the transaction data in Amazon DynamoDB. Set up a rule in DynamoDB to remove sensitive data from every transaction upon writing. Use DynamoDB Streams to share the transaction data with other applications.**

### Correct answer

**Stream the transactions data into Amazon Kinesis Data Streams. Use AWS Lambda integration to remove sensitive data from every transaction and then store the transactions data in Amazon DynamoDB. Other applications can consume the transactions data off the Kinesis data stream.**

### Overall explanation

Amazon Kinesis Data Streams is a serverless streaming data service that makes it easy to capture, process, and store data streams at any scale. When connected to Amazon DynamoDB



as an output the customer is able to scale to hundreds of thousands of concurrent users during their peak operating hours. KDS stores records for 24 hours by default so other applications can read the data.

**CORRECT:** "Stream the transactions data into Amazon Kinesis Data Streams. Use AWS Lambda integration to remove sensitive data from every transaction and then store the transactions data in Amazon DynamoDB. Other applications can consume the transactions data off the Kinesis data stream" is the correct answer (as explained above.)

**INCORRECT:** "Store the transaction data in Amazon DynamoDB. Set up a rule in DynamoDB to remove sensitive data from every transaction upon writing. Use DynamoDB Streams to share the transaction data with other applications" is incorrect. There's no capability to write rules that remove sensitive data in DynamoDB.

**INCORRECT:** "Stream the transactions data into Amazon Kinesis Data Firehose to store data in Amazon DynamoDB and Amazon S3. Use AWS Lambda integration with Kinesis Data Firehose to remove sensitive data. Other applications can consume the data stored in Amazon S3" is incorrect. Amazon Kinesis Data Firehose cannot load data directly to Amazon DynamoDB as it is not a supported destination.

**INCORRECT:** "Store the batched transactions data in Amazon S3 as files. Use AWS Lambda to process every file and remove sensitive data before updating the files in Amazon S3. The Lambda function then stores the data in Amazon DynamoDB. Other applications can consume transaction files stored in Amazon S3" is incorrect. This is highly inefficient and storing data in a DynamoDB table would be a much better solution.

#### References:

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

#### Save time with our AWS cheat sheets:

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

#### Domain

AWS Analytics

#### Question 63Skipped

A Solutions Architect has been tasked with building an application which stores images to be used for a website. The website will be accessed by thousands of customers. The images within the application need to be able to be transformed and processed as they are being retrieved. The solutions architect would prefer to use managed services to achieve this, and the solution should be highly available and scalable, and be able to serve users from around the world with low latency.

Which scenario represents the easiest solution for this task?

#### Correct answer

**Store the images in Amazon S3, behind a CloudFront distribution. Use S3 Object Lambda to transform and process the images whenever a GET request is initiated on an object.**

**Store the images in Amazon S3, behind a CloudFront distribution. Use S3 Event Notifications to connect to a Lambda function to process and transform the images when a GET request is initiated on an object.**

**Store the images in a DynamoDB table, with DynamoDB Accelerator enabled. Use Amazon EventBridge to pass the data into an event bus as it is retrieved from DynamoDB and use AWS Lambda to process the data.**

**Store the images in a DynamoDB table, with DynamoDB Global Tables enabled. Provision a Lambda function to process the data on demand as it leaves the table.**

Overall explanation

With S3 Object Lambda you can add your own code to S3 GET requests to modify and process data as it is returned to an application. For the first time, you can use custom code to modify the data returned by standard S3 GET requests to filter rows, dynamically resize images, redact confidential data, and much more. Powered by AWS Lambda functions, your code runs on infrastructure that is fully managed by AWS, eliminating the need to create and store derivative copies of your data or to run expensive proxies, all with no changes required to your applications.

**CORRECT:** "Store the images in Amazon S3, behind a CloudFront distribution. Use S3 Object Lambda to transform and process the images whenever a GET request is initiated on an object" is the correct answer (as explained above.)

**INCORRECT:** "Store the images in a DynamoDB table, with DynamoDB Global Tables enabled. Provision a Lambda function to process the data on demand as it leaves the table" is incorrect. DynamoDB is not as well designed for Write Once Read Many workloads and adding a Lambda function to the DynamoDB table takes more manual provisioning of resources than using S3 Object Lambda.

**INCORRECT:** "Store the images in Amazon S3, behind a CloudFront distribution. Use S3 Event Notifications to connect to a Lambda function to process and transform the images when a GET request is initiated on an object" is incorrect. This would work; however it is easier to use S3 Object Lambda as this manages the Lambda function for you.

**INCORRECT:** "Store the images in a DynamoDB table, with DynamoDB Accelerator enabled. Use Amazon EventBridge to pass the data into an event bus as it is retrieved from DynamoDB and use AWS Lambda to process the data" is incorrect. DynamoDB is not as well designed for Write Once Read Many workloads and adding a Lambda function to the DynamoDB table takes more manual provisioning of resources than using S3 Object Lambda.

#### **References:**

<https://aws.amazon.com/s3/features/object-lambda/>

**Save time with our AWS cheat sheets:**

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

#### **Domain**

AWS Compute

#### **Question 64Skipped**

A company is using Amazon Aurora as the database for an online retail application. Data analysts run reports every fortnight that take a long time to process and cause performance



degradation for the database. A Solutions Architect has reviewed performance metrics in Amazon CloudWatch and noticed that the ReadIOPS and CPUUtilization metrics are spiking when the reports run.

What is the MOST cost-effective solution to resolve the performance issues?

**Migrate the Aurora database to a larger instance class.**

**Increase the Provisioned IOPS on the Aurora instance.**

**Migrate the fortnightly reporting to Amazon EMR.**

**Correct answer**

**Migrate the fortnightly reporting to an Aurora Replica.**

Overall explanation

You can issue queries to the Aurora Replicas to scale the read operations for your application. You typically do so by connecting to the reader endpoint of the cluster. That way, Aurora can spread the load for read-only connections across as many Aurora Replicas as you have in the cluster.

This solution is the most cost-effective method of scaling the database for reads for the regular reporting job. The reporting job will be run against the read endpoint and will not cause performance issues for the main database.

**CORRECT:** "Migrate the fortnightly reporting to an Aurora Replica" is the correct answer.

**INCORRECT:** "Migrate the fortnightly reporting to Amazon EMR" is incorrect. There is no need to load data into EMR to run reports, simply offloading to an Aurora Replica will suffice.

**INCORRECT:** "Migrate the Aurora database to a larger instance class" is incorrect. This may be a more costly solution and may not be as effective as the long-running reporting job may just complete faster with more resources whilst still causing performance degradation.

**INCORRECT:** "Increase the Provisioned IOPS on the Aurora instance" is incorrect. This will improve the storage throughput but not the CPU.

**References:**

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

**Save time with our AWS cheat sheets:**

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

**Domain**

AWS Database

**Question 65Skipped**

A company is migrating an application that comprises a web tier and a MySQL database into the AWS Cloud. The web tier will run on EC2 instances, and the database tier will run on an Amazon RDS for MySQL DB instance. Customers access the application via the Internet using dynamic IP addresses.

How should the Solutions Architect configure the security groups to enable connectivity to the application?

**Configure the security group for the web tier to allow inbound traffic on port 443 from the IP addresses of the customers. Configure the security group for the DB tier to allow inbound traffic on port 3306 from the web tier security group.**

**Correct answer**

**Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0. Configure the security group for the DB tier to allow inbound traffic on port 3306 from the web tier security group.**

**Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0. Configure the security group for the DB tier to allow inbound traffic on port 3306 from 0.0.0.0/0.**

**Configure the security group for the web tier to allow inbound traffic on port 443 from the IP addresses of the customers. Configure the security group for the DB tier to allow inbound traffic on port 3306 from the IP addresses of the customers.**

Overall explanation

The customers are connecting from dynamic IP addresses so we must assume they will be changing regularly. Therefore, it is not possible to restrict access from the IP addresses of the customers. The security group for the web tier must allow 443 (HTTPS) from 0.0.0.0/0, which means any IP source IP address.

For the database tier, this can best be secured by restricting access to the web tier security group. The port required to be opened is 3306 for MySQL.

**CORRECT:** "Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0. Configure the security group for the DB tier to allow inbound traffic on port 3306 from the web tier security group" is the correct answer.

**INCORRECT:** "Configure the security group for the web tier to allow inbound traffic on port 443 from the IP addresses of the customers. Configure the security group for the DB tier to allow inbound traffic on port 3306 from the IP addresses of the customers" is incorrect.

The customer IP addresses are dynamic, so it is not possible to restrict access using IP addresses. Access to the DB tier should be restricted to the web tier, there is no need to enable end-user access.

**INCORRECT:** "Configure the security group for the web tier to allow inbound traffic on port 443 from the IP addresses of the customers. Configure the security group for the DB tier to allow inbound traffic on port 3306 from the web tier security group" is incorrect.

The customer IP addresses are dynamic, so it is not possible to restrict access using IP addresses.

**INCORRECT:** "Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0. Configure the security group for the DB tier to allow inbound traffic on port 3306 from 0.0.0.0/0" is incorrect.

Access to the DB tier should be restricted to the web tier, there is no need to enable access from the internet.

**References:**

[https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_SecurityGroups.html](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 Networking & Content Delivery