1. 1. Question

You currently manage a set of web servers hosted on EC2 Servers with public IP addresses. These IP addresses are mapped to domain names. There was an urgent maintenance activity that had to be carried out on the servers and the servers had to be restarted. Now the web application hosted on these EC2 Instances is not accessible via the domain names configured earlier. Which of the following could be a reason for this.

* + A. The Route53 hosted zone needs to be restarted.
  + B. The network interfaces need to initialized again.
  + C. The public IP addresses need to associated to the ENI again.
  + **D. The public IP addresses have changed after the instance was stopped and started**

**Unattempted**

By default the public IP address of an EC2 Instance is released after the instance is stopped and started. Hence the earlier IP address which were mapped to the domain names would have become invalid now. For more information on public IP addressing, please visit the below URL: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html#concepts-public-addresses>

1. 2. Question

You are responsible to deploying a critical application onto AWS. Part of the requirements for this application is to ensure that the controls set for this application met PCI compliance. Also there is a need to monitor web application logs to identify any malicious activity. Which of the following services can be used to fulfil this requirement. Choose 2 answers from the options given below

* + **A. Amazon Cloudwatch Logs**
  + B. Amazon VPC Flow Logs
  + C. Amazon AWS Config
  + **D. Amazon Cloudtrail**

**Unattempted**

The AWS Documentation mentions the following about these services AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. For more information on Cloudtrail, please refer to below URL: <https://aws.amazon.com/cloudtrail/> You can use Amazon CloudWatch Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, Amazon Route 53, and other sources. You can then retrieve the associated log data from CloudWatch Logs. For more information on Cloudwatch logs, please refer to below URL: <http://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html>

1. 3. Question

There is a requirement to host a database server. This server should not be able to connect to the internet except in the case of downloading the required database patches. Which of the following solutions would be the best to satisfy all the above requirements? Choose the correct answer from the options below

* + A. Set up the database in a private subnet with a security group which only allows outbound traffic.
  + B. Set up the database in a public subnet with a security group which only allows inbound traffic.
  + C. Set up the database in a local data center and use a private gateway to connect the application to the database.
  + **D. Set up the database in a private subnet which connects to the Internet via a NAT instance.**

**Unattempted**

This sort of setup as per the aws documentation coincides with Scenario2 of setting up a VPC. For more information on the VPC Scenario for public and private subnets please see the below link: <http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html>

1. 4. Question

You have instances running on your VPC. You have both production and development based instances running in the VPC. You want to ensure that people who are responsible for the development instances don’t have the access to work on the production instances to ensure better security. Using policies, which of the following would be the best way to accomplish this? Choose the correct answer from the options given below

* + A. Launch the test and production instances in separate VPC's and use VPC peering
  + B. Create an IAM policy with a condition which allows access to only instances that are used for production or development
  + C. Launch the test and production instances in different Availability Zones and use Multi Factor Authentication
  + **D. Define the tags on the test and production servers and add a condition to the IAM policy which allows access to specific tags**

**Unattempted**

You can easily add tags which define which instances are production and which are development instances and then ensure these tags are used when controlling access via an IAM policy. For more information on tagging your resources, please refer to the below link: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html>

1. 5. Question

A company is planning on building a 2 tier architecture which consists of a web server and a database server. This will be hosted on EC2 Instances accordingly. The database server will experience a lot of read/write operations whereas the web server will have a standard workload. Which of the following underlying EBS volumes are optimum to use for the underlying EC2 Instances. Choose 2 answers from the options given below.

* + **A. General Purpose SSD for the web server**
  + B. Provisioned IOPS for the web server
  + C. General Purpose SSD for the database server
  + **D. Provisioned IOPS for the database server**

**Unattempted**

If the database is going to have a lot of read/write requests, then the ideal solution would be to have the underlying EBS volume as Provisioned IOPS. Whereas since the standard workload, General Purpose SSD should be sufficient enough. The below except from the documentation also shows the different types of EBS volumes for different workloads For more information on EBS Volume types, please visit the following URL: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html>

1. 6. Question

You are hosting a web server on an EC2 Instance. The number of requests are now consuming a large part of the CPU, and the response performance for the application is getting degraded. Which of the following would help alleviate the problem and provide a better response time.

* + A. Place the EC2 Instance behind a classic load balancer
  + B. Place the EC2 Instance behind an Application load balancer
  + C. Place the EC2 Instance in an Autoscaling Group with the max size as 1.
  + **D. Place a Cloudfront distribution in front of the EC2 Instance**

**Unattempted**

Since there is only a mention of one EC2 instance, placing it behind the ELB would not make much sense , hence Option A and B are invalid. Having it in an Autoscaling Group with just one instance would not make much sense. The Cloudfront distribution would help alleviate the load on the EC2 Instance because of its edge location and cache feature. For more information on Cloudfront, please visit the following URL: <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>

1. 7. Question

One is planning on using SQS queues and AWS Lambda to create a leverage the serverless aspects of the AWS Cloud. Each invocation to AWS Lambda will send a message to an SQS queue. In order for messages to be sent , which of the following must be in place

* + A. The queue must be a FIFO queue
  + **B. An IAM Role with the required permissions**
  + C. The code for Lambda must be written in C#
  + D. An IAM Group with the required permissions

**Unattempted**

When working with AWS Lambda functions, if there is a need to access other resources, then ensure that an IAM role is in place. The IAM role will have the required permissions to access the SQS queue. For more information on AWS IAM Roles, please visit the following URL: <https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html>

1. 8. Question

You have enabled Cloudtrail logs for your company’s AWS account. In addition the IT Security department has mentioned that the logs need to be encrypted. How can this be achieved.

* + A. Enable SSL certificates for the Cloudtrail logs
  + **B. There is no need to do anything since the logs will already be encrypted**
  + C. Enable Server side encryption for the trail
  + D. Enable Server side encryption for the destination S3 bucket

**Unattempted**

The AWS Documentation mentions the following By default, CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE). You can also choose to encrypt your log files with an AWS Key Management Service (AWS KMS) key. You can store your log files in your bucket for as long as you want. You can also define Amazon S3 lifecycle rules to archive or delete log files automatically. If you want notifications about log file delivery and validation, you can set up Amazon SNS notifications. For more information on how Cloudtrail works, please visit the following URL: <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/how-cloudtrail-works.html>

1. 9. Question

A company has setup their data layer in the Simple Storage service. There are a number of requests which include read/write and updates to objects in an S3 bucket. Users sometimes complain that updates to an object are not being reflected. Which of the following could be a reason for this

* + A. The versioning is not enable for the bucket , so the newer version is not reflecting the right data
  + **B. The updates are being made to the same key for the object**
  + C. Encryption is enabled for the bucket , hence it is taking time for the update to occur
  + D. The metadata for the S3 bucket is incorrectly configured

**Unattempted**

When updates are made to objects in S3, they have an eventual consistency model. Hence when objects updates are made to the same key, there can be a slight delay when the updated object is provided back to the user when the next read request is made. For more information on the various aspects for the Simple Storage service, please visit the following URL: <https://aws.amazon.com/s3/faqs/>

1. 10. Question

A company needs to have a fully managed NoSQL database on the AWS Cloud. The database should have the ability for backups and high availability. Which Amazon database meets these requirements?

* + A. MySQL
  + B. Microsoft SQL Server
  + **C. DynamoDB**
  + D. Amazon Aurora

**Unattempted**

The AWS Documentation mentions the following Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. DynamoDB lets you offload the administrative burdens of operating and scaling a distributed database, so that you don’t have to worry about hardware provisioning, setup and configuration, replication, software patching, or cluster scaling For more information on AWS DynamoDB, please visit the following URL: <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html>

1. 11. Question

A company is planning to move to the AWS Cloud. They want to leverage their existing Chef recipes for configuration management of their infrastructure. Which AWS service would be ideal for this requirement

* + A. AWS Elastic Load Balancer
  + B. AWS Elastic beanstalk
  + **C. AWS Opswork**
  + D. AWS Inspector

**Unattempted**

The AWS Documentation mentions the following which can support this requirement AWS OpsWorks is a configuration management service that helps you configure and operate applications in a cloud enterprise by using Puppet or Chef. AWS OpsWorks Stacks and AWS OpsWorks for Chef Automate let you use Chef cookbooks and solutions for configuration management, while AWS OpsWorks for Puppet Enterprise lets you configure a Puppet Enterprise master server in AWS. Puppet offers a set of tools for enforcing the desired state of your infrastructure, and automating on-demand tasks. For more information on AWS Opswork, please visit the following URL: <https://docs.aws.amazon.com/opsworks/latest/userguide/welcome.html>

1. 12. Question

An application consists of a web server and database server hosted on separate EC2 Instances. There are lot of read requests on the database which is degrading the performance of the application. Which of the following can help improve the performance of the database under the heavy load

* + A. Enable Multi-AZ for the database
  + **B. Put an Elastic Cache in front of the database**
  + C. Place another web server in the architecture to take the load
  + D. Place a CloudFront distribution in front of the database

**Unattempted**

The ideal solution would be to use Elastic Cache The AWS Documentation furthers mentions the following with respective to Elastic cache ElastiCache is a web service that makes it easy to set up, manage, and scale a distributed in-memory data store or cache environment in the cloud. It provides a high-performance, scalable, and cost-effective caching solution, while removing the complexity associated with deploying and managing a distributed cache environment. For more information on AWS Elastic Cache, please visit the following URL: <https://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/WhatIs.html>

1. 13. Question

You need to have the ability to store archive documents in AWS. This needs to be a COST-effective solution. Which of the following would you use to meet this requirement

* + **A. Amazon Glacier**
  + B. Amazon S3 Standard Infrequent Access
  + C. Amazon EFS
  + D. Amazon S3 Standard

**Unattempted**

The AWS Documentation mentions the following on Amazon Glacier Amazon Glacier is an extremely low-cost storage service that provides durable storage with security features for data archiving and backup. With Amazon Glacier, customers can store their data cost effectively for months, years, or even decades. Amazon Glacier enables customers to offload the administrative burdens of operating and scaling storage to AWS, so they don’t have to worry about capacity planning, hardware provisioning, data replication, hardware failure detection and recovery, or time-consuming hardware migrations. For more information on Amazon Glacier, please visit the following URL: <https://docs.aws.amazon.com/amazonglacier/latest/dev/introduction.html>

1. 14. Question

A company is hosting a MySQL database in AWS using the AWS RDS service. To offload the reads, a read replica has been created and reports are run off the read replica database. But at certain times, the reports are showing stale data. Why is this the case?

* + A. The Read replica has not been created properly
  + B. The backup of the original database has not been set properly
  + **C. This is due to the replication lag**
  + D. The Multi-AZ feature is not enable

**Unattempted**

An AWS Whitepaper on the caveat for Read Replica’s is given below which must be taken into consideration by designers Read replicas are separate database instances that are replicated asynchronously. As a result, they are subject to replication lag and might be missing some of the latest transactions. Application designers need to consider which queries have tolerance to slightly stale data. Those queries can be executed on a read replica, while the rest should run on the primary node. Read replicas can also not accept any write queries. For more information on AWS Cloud best practises, please visit the following URL: <https://d1.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf>

1. 15. Question

the sales team at a popular trading company must generate sales reports at the beginning of every month. this process launches 10 Amazon EC2 instances at the beginning of each month and takes 7 days without any interruption to complete the task.  
What is the best price model to use in order to minimize the cost?

* + Reserved Instances
  + Spot Block Instances
  + On-Demand Instances
  + **Scheduled Reserved Instances**

**Unattempted**

Exam Tip  
Scheduled Reserved Instances (Scheduled Instances) enable you to purchase capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term.  
Explanation  
Scheduled Reserved Instances (Scheduled Instances) enable you to purchase capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term. You reserve the capacity in advance, so that you know it is available when you need it. You pay for the time that the instances are scheduled, even if you do not use them.  
Scheduled Instances are a good choice for workloads that do not run continuously, but do run on a regular schedule. For example, you can use Scheduled Instances for an application that runs during business hours or for batch processing that runs at the end of the week.  
If you require a capacity reservation on a continuous basis, Reserved Instances might meet your needs and decrease costs. For more information, see Reserved Instances. If you are flexible about when your instances run, Spot Instances might meet your needs and decrease costs.  
Reference  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html>

1. 16. Question

A multimedia company want to transfer 720 TB of videos from a network-attached file system located at a branch office Amazon S3 Glacier with avoiding saturating the branch office’s low-bandwidth internet connection

What is the MOST cost-effective solution?

* + Mount the network-attached file system to Amazon S3 and copy the files directly. Create a lifecycle policy to S3 objects to Amazon S3 Glacier.
  + Order 10 AWS Snowball appliances and select an S3 Glacier vault as the destination. Create a bucket policy to enforce VPC endpoint.
  + Create a site-to-site VPN tunnel to an Amazon S3 bucket and transfer the files directly. Create a bucket VPC endpoint.
  + **Order 10 AWS Snowball appliances and select an Amazon S3 bucket as the destination. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.**

**Unattempted**

Exam Tip  
The solution must avoid saturating the branch office’s low-bandwidth internet connection = Use Snow Ball  
10 AWS snowball = 800 TB but you can use just 720 TB so you are missing 30 TB.  
Reference  
<https://docs.aws.amazon.com/snowball/latest/ug/specifications.html>

1. 17. Question

A multinational company will launch e-commerce multi-tier application and due to the big promotions , the company expects a huge traffic in the launching day.  
As solution architect, what is the best approach to prevent any potential failure in the database layer?

* + Create another DR site in case of failure
  + Migrate the database to NOSQL
  + Enable database auto Scaling feature.
  + **Migrate the database to Amazon RDS in multi AZ.**

**Unattempted**

Exam Tip  
to provide high availability in a database tier(the most critical tier) = use Multi-AZ RDS  
Explanation  
Amazon RDS Multi-AZ deployments provide enhanced availability and durability for RDS database (DB) instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby (or to a read replica in the case of Amazon Aurora), so that you can resume database operations as soon as the failover is complete. Since the endpoint for your DB Instance remains the same after a failover, your application can resume database operation without the need for manual administrative intervention.  
Reference  
<https://aws.amazon.com/rds/features/multi-az/>

1. 18. Question

A video streaming company is hosting a website behind multiple Application Load Balancers. The company has different distribution rights for its content around the world.  
Which configuration should the solutions architect choose to ensure that users are served the correct content without violating distribution rights.?

* + Configure Application Load Balancers with AWS WAF.
  + Configure Amazon Route 53 with a geoproximity routing policy.
  + Configure Amazon CloudFront with AWS WAF.
  + **Configure Amazon Route 53 with a geolocation policy.**

**Unattempted**

Exam Tip  
route traffic based on the location of your users. = Use Geolocation routing policy  
Explanation  
When you create a record, you choose a routing policy, which determines how Amazon Route 53 responds to queries:  
· Simple routing policy – Use for a single resource that performs a given function for your domain, for example, a web server that serves content for the example.com website.  
· Failover routing policy – Use when you want to configure active-passive failover.  
· Geolocation routing policy – Use when you want to route traffic based on the location of your users.  
· Geoproximity routing policy – Use when you want to route traffic based on the location of your resources and, optionally, shift traffic from resources in one location to resources in another.  
· Latency routing policy – Use when you have resources in multiple AWS Regions and you want to route traffic to the region that provides the best latency.  
· Multivalue answer routing policy – Use when you want Route 53 to respond to DNS queries with up to eight healthy records selected at random.  
· Weighted routing policy – Use to route traffic to multiple resources in proportions that you specify.

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

1. 19. Question

An e-commerce application is hosted in AWS which uses distributed database on multiple Amazon EC2 instances. The database stores all data on multiple instances to ensure that the operation is fault-tolerant up to the loss of an instance. The database requires block storage with latency and throughput to support several million transactions per second per server.  
Which storage solution should the solutions architect use?

* + **Amazon EBS**
  + Amazon EFS
  + Amazon EC2 instance store
  + Amazon S3

**Unattempted**

Exam Tip  
Block Storage +  fault-tolerant up to the loss of an instance = EBS  
Explanation  
Amazon Elastic Block Store (EBS) is an easy to use, high performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction intensive workloads at any scale. A broad range of workloads, such as relational and non-relational databases, enterprise applications, containerized applications, big data analytics engines, file systems, and media workflows are widely deployed on Amazon EBS.  
Reference  
<https://aws.amazon.com/ebs/?ebs-whats-new.sort-by=item.additionalFields.postDateTime&ebs-whats-new.sort-order=desc>

1. 20. Question

A startup company has application running on Amazon EC2 instances in a VPC. this application needs to call Amazon S3 API to store and read objects with restricting any internet-bound traffic from the application.  
What is the best solution to handle this requirement?

* + Use an S3 interface endpoint.
  + **Use an S3 gateway endpoint.**
  + Use an S3 bucket in the same Region as the EC2 instance.
  + Use an S3 bucket in a private subnet.

**Unattempted**

Exam Tip  
to integrate with S3 with  restricting any internet-bound traffic = Use A gateway endpoint.  
Explanation  
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.  
Endpoints are virtual devices. They are horizontally scaled, redundant, and highly available VPC components. They allow communication between instances in your VPC and services without imposing availability risks or bandwidth constraints on your network traffic.  
There are two types of VPC endpoints: interface endpoints and gateway endpoints. Create the type of VPC endpoint required by the supported service.  
An interface endpoint is an elastic network interface with a private IP address from the IP address range of your subnet that serves as an entry point for traffic destined to a supported service. Interface endpoints are powered by AWS PrivateLink, a technology that enables you to privately access services by using private IP addresses. AWS PrivateLink restricts all network traffic between your VPC and services to the Amazon network. You do not need an internet gateway, a NAT device, or a virtual private gateway. i.e all services excepts Amazon S3 and DynamoDB.

A gateway endpoint is a gateway that you specify as a target for a route in your route table for traffic destined to a supported AWS service. The following AWS services are supported:  
a – Amazon S3  
b -DynamoDB  
Reference  
<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html>

1. 21. Question

While performing PCI auditing on an existing workload deployed on AWS. The review identified a public-facing website running on the same Amazon EC2 instance as a Microsoft Active Directory domain controller that was install recently to support other AWS services.  
What should the solutions architect recommend for the new design that would improve the security of the architecture and minimize the administrative demand on IT staff?

* + **Use AWS Directory Service to create a managed Active Directory. Uninstall Active Directory on the current EC2 instance.**
  + Enable AWS Single Sign-On (AWS SSO) with Security Assertion Markup Language (SAML) 2.0 federation with the current Active Directory controller. Modify the EC2 instance's security group to deny public access to Active Directory.
  + Use AWS Directory Service to create an Active Directory connector. Proxy Active Directory requests to the Active domain controller running on the current EC2 instance.
  + Create another EC2 instance in the same subnet and reinstall Active Directory on it. Uninstall Active Directory.

**Unattempted**

Exam Tip  
migrate AD to AWS Managed AD and keep the webserver alone + improve the security of the architecture and minimize the administrative demand on IT staff = Use AWS Directory Service to create a managed Active Directory. Uninstall Active Directory on the current EC2 instance.  
You can use the Active Directory Migration Toolkit (ADMT) along with the Password Export Service (PES) to migrate users from your self-managed AD to your AWS Managed Microsoft AD directory. This enables you to migrate AD objects and encrypted passwords for your users more easily.  
Reference  
<https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_migrate_users.html>

1. 22. Question

A security team found database credentials stored in the source code of application which call AWS Lambda Functions. The database credentials need to be removed from the Lambda source code. The credentials must then be securely stored and rotated on an ongoing basis to meet security policy requirements.  
What should a solutions architect recommend to meet these requirements?

* + Store the password in AWS Key Management Service (AWS KMS). Associate the Lambda function with a role that can retrieve the password from AWS KMS given its key ID.
  + **Store the password in AWS Secrets Manager. Associate the Lambda function with a role that can retrieve the password from Secrets Manager given its secret ID.**
  + Store the password in AWS CloudHSM. Associate the Lambda function with a role that can retrieve the password from CloudHSM given its key ID.
  + Move the database password to an environment variable associated with the Lambda function. Retrieve the password from the environment variable upon execution.

**Unattempted**

Exam Tip  
You can configure Secrets Manager to automatically rotate your secrets without user intervention and on a specified schedule.  
Explanation  
AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text. Secrets Manager offers secret rotation with built-in integration for Amazon RDS, Amazon Redshift, and Amazon DocumentDB. Also, the service is extensible to other types of secrets, including API keys and OAuth tokens. In addition, Secrets Manager enables you to control access to secrets using fine-grained permissions and audit secret rotation centrally for resources in the AWS Cloud, third-party services, and on-premises.  
Reference  
<https://aws.amazon.com/secrets-manager/>

1. 23. Question

A customer owns a simple API in a VPC behind an internet-facing Application Load Balancer (ALB). a client application which consumes the API is deployed in a second account in private subnets behind a NAT gateway. When requests to the client application increase, the NAT gateway costs are higher than expected. A solutions architect has configured the ALB to be internal.

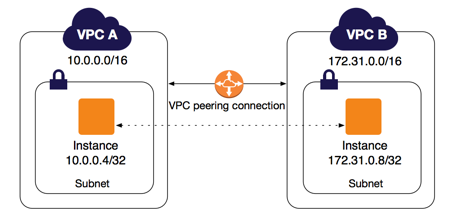
Which combination of architectural changes will reduce the NAT gateway costs? (Choose two.)

* + **Configure a VPC peering connection between the two VPCs. Access the API using the private address.**
  + Configure an AWS Resource Access Manager connection between the two accounts. Access the API using the private address.
  + Configure an AWS Direct Connect connection between the two VPCs. Access the API using the private address.
  + **Configure a PrivateLink connection for the API into the client VPC. Access the API using the PrivateLink address.**
  + Configure a ClassicLink connection for the API into the client VPC. Access the API using the ClassicLink address.

**Unattempted**

Exam Tip  
PrivateLink makes it easy to connect services across different accounts and VPCs to significantly simplify the network architecture.

Explanation  
AWS PrivateLink simplifies the security of data shared with cloud-based applications by eliminating the exposure of data to the public Internet. AWS PrivateLink provides private connectivity between VPCs, AWS services, and on-premises applications, securely on the Amazon network. AWS PrivateLink makes it easy to connect services across different accounts and VPCs to significantly simplify the network architecture.  
Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you’ve defined.  
A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection).

[](https://skillcertpro.com/wp-content/uploads/2020/08/a59.png)  
AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.  
A VPC peering connection helps you to facilitate the transfer of data. For example, if you have more than one AWS account, you can peer the VPCs across those accounts to create a file sharing network. You can also use a VPC peering connection to allow other VPCs to access resources you have in one of your VPCs.  
You can establish peering relationships between VPCs across different AWS Regions (also called Inter-Region VPC Peering). This allows VPC resources including EC2 instances, Amazon RDS databases and Lambda functions that run in different AWS Regions to communicate with each other using private IP addresses, without requiring gateways, VPN connections, or separate network appliances. The traffic remains in the private IP space. All inter-region traffic is encrypted with no single point of failure, or bandwidth bottleneck. Traffic always stays on the global AWS backbone, and never traverses the public internet, which reduces threats, such as common exploits, and DDoS attacks. Inter-Region VPC Peering provides a simple and cost-effective way to share resources between regions or replicate data for geographic redundancy.

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

1. 24. Question

“A trading company is about to release a new online transaction processing (OLTP) application using Amazon RDS MySQL DB instance.  
The company needs to create another highly available reporting tool which will access the same data without impacting the performance of the production application.  
”  
What is the best solution to achieve this goal?

* + Create hourly snapshots of the production RDS DB instance.
  + Create a Single-AZ RDS Read Replica of the production RDS DB instance. Create a second Single-AZ RDS Read Replica from the replica.
  + **Create a Multi-AZ RDS Read Replica of the production RDS DB instance.**
  + Create multiple ROS Read Replicas of the production RDS DB instance. Place the Read Replicas in an Auto Scaling group.

**Unattempted**

Exam Tip  
for better performance, run the reports on the read replicas.  
Explanation  
Amazon RDS Read Replicas provide enhanced performance and durability for RDS database (DB) instances. They make it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances. Read replicas are available in Amazon RDS for MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server as well as Amazon Aurora.

For the MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server database engines, Amazon RDS creates a second DB instance using a snapshot of the source DB instance. It then uses the engines’ native asynchronous replication to update the read replica whenever there is a change to the source DB instance. The read replica operates as a DB instance that allows only read-only connections; applications can connect to a read replica just as they would to any DB instance. Amazon RDS replicates all databases in the source DB instance.

Amazon Aurora futher extends the benefits of read replicas by employing an SSD-backed virtualized storage layer purpose-built for database workloads. Amazon Aurora replicas share the same underlying storage as the source instance, lowering costs and avoiding the need to copy data to the replica nodes.  
Reference  
<https://aws.amazon.com/rds/features/read-replicas/>

1. 25. Question

A start-up company that offers an intuitive financial data analytics service behind Amazon API Gateway.  the traffic to this service is  unpredictable and varies from 0 requests to over 500 per second. The data size which needs to be persisted in a database is currently less than 1 GB with unpredictable future growth and can be queried using simple key-value requests.

Which combination of AWS services would meet these requirements? (Choose two.)

* + **AWS Lambda**
  + AWS Fargate
  + Amazon EC2 Auto Scaling
  + **Amazon DynamoDB**
  + MySQL-compatible Amazon Aurora

**Unattempted**

Exam Tip  
DynamoDB is noSQL (key – value based),Lambda works out of the box can handle request also both are serverless.  
Lambda autoscale and can handle 500 requests per second and integrates with API Gateway and DynamoDB.  
Explanation

Amazon DynamoDB is a key-value and document database that delivers single-digit millisecond performance at any scale. It’s a fully managed, multiregion, multimaster, durable database with built-in security, backup and restore, and in-memory caching for internet-scale applications. DynamoDB can handle more than 10 trillion requests per day and can support peaks of more than 20 million requests per second.

Lambda  
the first time you invoke your function, AWS Lambda creates an instance of the function and runs its handler method to process the event. When the function returns a response, it stays active and waits to process additional events. If you invoke the function again while the first event is being processed, Lambda initializes another instance, and the function processes the two events concurrently. As more events come in, Lambda routes them to available instances and creates new instances as needed. When the number of requests decreases, Lambda stops unused instances to free up scaling capacity for other functions.  
Your functions’ concurrency is the number of instances that serve requests at a given time. For an initial burst of traffic, your functions’ cumulative concurrency in a Region can reach an initial level of between 500 and 3000, which varies per Region.  
Burst concurrency limits  
3000 – US West (Oregon), US East (N. Virginia), Europe (Ireland)  
1000 – Asia Pacific (Tokyo), Europe (Frankfurt)  
500 – Other Regions  
After the initial burst, your functions’ concurrency can scale by an additional 500 instances each minute. This continues until there are enough instances to serve all requests, or until a concurrency limit is reached. When requests come in faster than your function can scale, or when your function is at maximum concurrency, additional requests fail with a throttling error (429 status code).  
The following example shows a function processing a spike in traffic. As invocations increase exponentially, the function scales up. It initializes a new instance for any request that can’t be routed to an available instance. When the burst concurrency limit is reached, the function starts to scale linearly. If this isn’t enough concurrency to serve all requests, additional requests are throttled and should be retried.

[A diagram of a curve

Description automatically generated](https://skillcertpro.com/wp-content/uploads/2020/08/a60.png)  
Legend

 Function instances

 Open requests

 Throttling possible

The function continues to scale until the account’s concurrency limit for the function’s Region is reached. The function catches up to demand, requests subside, and unused instances of the function are stopped after being idle for some time. Unused instances are frozen while they’re waiting for requests and don’t incur any charges.

Reference  
<https://docs.aws.amazon.com/lambda/latest/dg/invocation-scaling.html>  
<https://aws.amazon.com/dynamodb/>

1. 26. Question

An application runs on Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones behind Application Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 30 %.  
What should a solutions architect do to maintain the desired performance across all instances in the group?

* + Use an AWS Lambda function to update the desired Auto Scaling group capacity.
  + Use a simple scaling policy to dynamically scale the Auto Scaling group.
  + Use scheduled scaling actions to scale up and scale down the Auto Scaling group.
  + **Use a target tracking policy to dynamically scale the Auto Scaling group.**

**Unattempted**

Exam Tip  
because a target tracking scaling policy assumes that it should scale out your Auto Scaling group when the specified metric is above the target value. You cannot use a target tracking scaling policy to scale out your Auto Scaling group when the specified metric is below the target value  
Explanation  
With target tracking scaling policies, you select a scaling metric and set a target value. Amazon EC2 Auto Scaling creates and manages the CloudWatch alarms that trigger the scaling policy and calculates the scaling adjustment based on the metric and the target value. The scaling policy adds or removes capacity as required to keep the metric at, or close to, the specified target value. In addition to keeping the metric close to the target value, a target tracking scaling policy also adjusts to changes in the metric due to a changing load pattern.  
For example, you can use target tracking scaling to:  
Configure a target tracking scaling policy to keep the average aggregate CPU utilization of your Auto Scaling group at 40 percent.  
Configure a target tracking scaling policy to keep the request count per target of your Application Load Balancer target group at 1000 for your Auto Scaling group.  
Depending on your application needs, you might find that one of these popular scaling metrics works best for you when using target tracking, or you might find that a combination of these metrics or a different metric meets your needs better.  
Reference  
<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html>

1. 27. Question

A popular bank has a high available critical application which currently uses oracle database backed by SAN disc. the company decided to move it to the cloud.  
What is the best AWS storage to handle this requirement ?

* + AWS Storage Gateway
  + Amazon EFS
  + **Amazon EBS**
  + Amazon S3

**Unattempted**

Exam Tip  
SAN disc = Object Store = EBS  
Explanation  
Amazon Elastic Block Store (EBS) is an easy to use, high performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction intensive workloads at any scale. A broad range of workloads, such as relational and non-relational databases, enterprise applications, containerized applications, big data analytics engines, file systems, and media workflows are widely deployed on Amazon EBS.  
You can choose from four different volume types to balance optimal price and performance. You can achieve single digit-millisecond latency for high performance database workloads such as SAP HANA or gigabyte per second throughput for large, sequential workloads such as Hadoop. You can change volume types, tune performance, or increase volume size without disrupting your critical applications, so you have cost-effective storage when you need it.  
Reference  
<https://aws.amazon.com/ebs/?ebs-whats-new.sort-by=item.additionalFields.postDateTime&ebs-whats-new.sort-order=desc>

1. 28. Question

You are a Solutions architect in a news agency which has a multi-tier web application  The application runs on Amazon EC2 instances behind an Application Load Balancer with Auto Scaling group across multiple Availability Zones and use an Amazon Aurora database.  
What are the best options to make the application more resilient to periodic increases in request rates? (Choose two.)

* + **Add Aurora Replica.**
  + **Configure an Amazon CloudFront distribution as first layer.**
  + Configure AWS WAF.
  + Configure AWS Global Accelerator.
  + Configure AWS Direct Connect.

**Unattempted**

Explanation:  
The architecture is already highly resilient but the may be subject to performance degradation if there are sudden increases in request rates. To resolve this situation Amazon Aurora Read Replicas can be used to serve read traffic which offloads requests from the main database. On the frontend an Amazon CloudFront distribution can be placed in front of the ALB and this will cache content for better performance and also offloads requests from the backend. References: <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html>  
https:// docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html

1. 29. Question

A Solutions Architect needs to run a production batch process quickly that will use several EC2 instances. The process cannot be interrupted and must be completed within a short time period.  
What is likely to be the MOST cost-effective choice of EC2 instance type to use for this requirement?

* + **On-demand instances**
  + Flexible instances
  + Spot instances
  + Reserved instances

**Unattempted**

The key requirements here are that you need to deploy several EC2 instances quickly to run the batch process and you must ensure that the job completes. The on-demand pricing model is the best for this ad-hoc requirement as though spot pricing may be cheaper you cannot afford to risk that the instances are terminated by AWS when the market price increases.  
CORRECT: “On-demand instances” is the correct answer.  
INCORRECT: “Reserved instances” is incorrect. Reserved instances are used for longer more stable requirements where you can get a discount for a fixed 1 or 3 year term. This pricing model is not good for temporary requirements.  
INCORRECT: “Spot instances” is incorrect. Spot instances provide a very low hourly compute cost and are good when you have flexible start and end times. They are often used for use cases such as grid computing and high-performance computing (HPC).  
INCORRECT: “Flexible instances” is incorrect. There is no such thing as a “flexible instance”.  
References:  
<https://aws.amazon.com/ec2/pricing/>

References:  
Topic: aws-solutions-architect-associate/compute/amazon-ec2/

1. 30. Question

A Solutions Architect regularly launches EC2 instances manually from the console and wants to streamline the process to reduce administrative overhead. Which feature of EC2 enables storing of settings such as AMI ID, instance type, key pairs and Security Groups?

* + Launch Configurations
  + Run Command
  + Placement Groups
  + **Launch Templates**

**Unattempted**

Launch templates enable you to store launch parameters so that you do not have to specify them every time you launch an instance. When you launch an instance using the Amazon EC2 console, an AWS SDK, or a command line tool, you can specify the launch template to use.  
CORRECT: “Launch Templates” is the correct answer.  
INCORRECT: “Placement Groups” is incorrect. You can launch or start instances in a placement group, which determines how instances are placed on underlying hardware.  
INCORRECT: “Run Command” is incorrect. Run Command automates common administrative tasks, and lets you perform ad hoc configuration changes at scale.  
INCORRECT: “Launch Configurations” is incorrect. Launch Configurations are used with Auto Scaling Groups.  
References:  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-launch-templates.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-launch-templates.html>

1. 31. Question

An application uses a combination of Reserved and On-Demand instances to handle typical load. The application involves performing analytics on a set of data. A Solutions Architect needs to temporarily deploy a large number of EC2 instances. The instances must be available for a short period of time until the analytics job is completed.  
If job completion is not time-critical, what is likely to be the MOST cost-effective choice of EC2 instance type to use for this requirement?

* + Use dedicated hosts
  + Use Reserved instances
  + **Use Spot instances**
  + Use On-Demand instances

**Unattempted**

The key requirements here are that you need to temporarily deploy a large number of instances, can tolerate an delay (not time-critical), and need the most economical solution. In this case Spot instances are likely to be the most economical solution.  
You must be able to tolerate delays if using Spot instances as if the market price increases your instances will be terminated and you may have to wait for the price to lower back to your budgeted allowance.  
CORRECT: “Use Spot instances” is the correct answer.  
INCORRECT: “Use dedicated hosts” is incorrect. An EC2 Dedicated Host is a physical server with EC2 instance capacity fully dedicated to your use. They are much more expensive than on-demand or Spot instances and are used for use cases such as bringing your own socket-based software licences to AWS or for compliance reasons.  
INCORRECT: “Use On-Demand instances” is incorrect. On-demand is good for temporary deployments when you cannot tolerate any delays (instances being terminated by AWS). It is likely to be more expensive than Spot however so if delays can be tolerated it is not the best solution.  
INCORRECT: “Use Reserved instances” is incorrect. Reserved instances are used for longer more stable requirements where you can get a discount for a fixed 1 or 3 year term. This pricing model is not good for temporary requirements.  
References:  
<https://aws.amazon.com/ec2/pricing/>

Topic: aws-solutions-architect-associate/compute/amazon-ec2/

1. 32. Question

A Solutions Architect would like to implement a method of automating the creation, retention, and deletion of backups for the Amazon EBS volumes in an Amazon VPC. What is the easiest way to automate these tasks using AWS tools?

* + **Use the EBS Data Lifecycle Manager (DLM) to manage snapshots of the volumes**
  + Create a scheduled job and run the AWS CLI command “create-backup”
  + Configure EBS volume replication to create a backup on Amazon S3
  + Create a scheduled job and run the AWS CLI command “create-snapshot”

**Unattempted**

You backup EBS volumes by taking snapshots. This can be automated via the AWS CLI command “create-snapshot”. However the question is asking for a way to automate not just the creation of the snapshot but the retention and deletion too.  
The EBS Data Lifecycle Manager (DLM) can automate all of these actions for you and this can be performed centrally from within the management console.  
CORRECT: “Use the EBS Data Lifecycle Manager (DLM) to manage snapshots of the volumes” is the correct answer.  
INCORRECT: “Configure EBS volume replication to create a backup on S3” is incorrect. You cannot configure volume replication for EBS volumes using AWS tools.  
INCORRECT: “Create a scheduled job and run the AWS CLI command “create-backup” to take backups of the EBS volumes” is incorrect. This is the wrong command (use create-snapshot) and is not the easiest method.  
INCORRECT: “Create a scheduled job and run the AWS CLI command “create-snapshot” to take backups of the EBS volumes” is incorrect. This is not the easiest method, DLM would be a much better solution.  
References:  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-lifecycle.html>  
<https://docs.aws.amazon.com/cli/latest/reference/ec2/create-snapshot.html>

Topic: aws-solutions-architect-associate/compute/amazon-ebs/

1. 33. Question

The disk configuration for an Amazon EC2 instance must be finalized. The instance will be running an application that requires heavy read/write IOPS. A single volume is required that is 500 GiB in size and needs to support 20,000 IOPS.  
What EBS volume type should be selected?

* + EBS General Purpose SSD
  + **EBS Provisioned IOPS SSD**
  + EBS General Purpose SSD in a RAID 1 configuration
  + EBS Throughput Optimized HDD

**Unattempted**

This is simply about understanding the performance characteristics of the different EBS volume types. The only EBS volume type that supports over 16,000 IOPS per volume is Provisioned IOPS SSD.  
SSD, General Purpose – gp2  
– Volume size 1 GiB – 16 TiB.  
– Max IOPS/volume 16,000.  
SSD, Provisioned IOPS – i01  
– Volume size 4 GiB – 16 TiB.  
– Max IOPS/volume 64,000.  
– HDD, Throughput Optimized – (st1)  
– Volume size 500 GiB – 16 TiB.  
Throughput measured in MB/s, and includes the ability to burst up to 250 MB/s per TB, with a baseline throughput of 40 MB/s per TB and a maximum throughput of 500 MB/s per volume.  
HDD, Cold – (sc1)  
– Volume size 500 GiB – 16 TiB.  
Lowest cost storage – cannot be a boot volume.  
– These volumes can burst up to 80 MB/s per TB, with a baseline throughput of 12 MB/s per TB and a maximum throughput of 250 MB/s per volume  
HDD, Magnetic – Standard – cheap, infrequently accessed storage – lowest cost storage that can be a boot volume.  
CORRECT: “EBS Provisioned IOPS SSD” is the correct answer.  
INCORRECT: “EBS General Purpose SSD” is incorrect as the max IOPS is 16,000.  
INCORRECT: “EBS General Purpose SSD in a RAID 1 configuration” is incorrect. RAID 1 is mirroring and does not increase the amount of IOPS you can generate.  
INCORRECT: “EBS Throughput Optimized HDD” is incorrect as this type of disk does not support the IOPS requirement.  
References:  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html>

Topic: aws-solutions-architect-associate/compute/amazon-ebs/

1. 34. Question

Health related data in Amazon S3 needs to be frequently accessed for up to 90 days. After that time the data must be retained for compliance reasons for seven years and is rarely accessed.  
Which storage classes should be used?

* + Store data in INTELLIGENT\_TIERING for 90 days then transition to STANDARD\_IA
  + **Store data in STANDARD for 90 days then transition the data to DEEP\_ARCHIVE**
  + Store data in STANDARD for 90 days then expire the data
  + Store data in STANDARD for 90 days then transition to REDUCED\_REDUNDANCY

**Unattempted**

In this case the data is frequently accessed so must be stored in standard for the first 90 days. After that the data is still to be kept for compliance reasons but is rarely accessed so is a good use case for DEEP\_ARCHIVE.  
CORRECT: “Store data in STANDARD for 90 days then transition the data to DEEP\_ARCHIVE” is the correct answer.  
INCORRECT: “Store data in INTELLIGENT\_TIERING for 90 days then transition to STANDARD\_IA” is incorrect. You cannot transition from INTELLIGENT\_TIERING to STANDARD\_IA.  
INCORRECT: “Store data in STANDARD for 90 days then expire the data” is incorrect. Expiring the data is not possible as it must be retained for compliance.  
INCORRECT: “Store data in STANDARD for 90 days then transition to REDUCED\_REDUNDANCY” is incorrect. You cannot transition from any storage class to REDUCED\_REDUNDANCY.  
References:  
<https://docs.aws.amazon.com/AmazonS3/latest/dev/lifecycle-transition-general-considerations.html>

Topic: aws-solutions-architect-associate/storage/amazon-s3/

1. 35. Question

A high-performance file system is required for a financial modelling application. The data set will be stored on Amazon S3 and the storage solution must have seamless integration so objects can be accessed as files.  
Which storage solution should be used?

* + **Amazon FSx for Lustre**
  + Amazon Elastic File System (EFS)
  + Amazon Elastic Block Store (EBS)
  + Amazon FSx for Windows File Server

**Unattempted**

Amazon FSx for Lustre provides a high-performance file system optimized for fast processing of workloads such as machine learning, high performance computing (HPC), video processing, financial modeling, and electronic design automation (EDA). Amazon FSx works natively with Amazon S3, letting you transparently access your S3 objects as files on Amazon FSx to run analyses for hours to months.

[A diagram of a network

Description automatically generated](https://skillcertpro.com/wp-content/uploads/2020/08/a46.jpg)  
CORRECT: “Amazon FSx for Lustre” is the correct answer.  
INCORRECT: “Amazon FSx for Windows File Server” is incorrect. Amazon FSx for Windows File Server provides a fully managed native Microsoft Windows file system so you can easily move your Windows-based applications that require shared file storage to AWS. This solution integrates with Windows file shares, not with Amazon S3.  
INCORRECT: “Amazon Elastic File System (EFS)” is incorrect. EFS and EBS are not good use cases for this solution. Neither storage solution is capable of presenting Amazon S3 objects as files to the application.  
INCORRECT: “Amazon Elastic Block Store (EBS)” is incorrect. EFS and EBS are not good use cases for this solution. Neither storage solution is capable of presenting Amazon S3 objects as files to the application.  
References:  
<https://aws.amazon.com/fsx/>

Topic: aws-solutions-architect-associate/storage/amazon-fsx/

1. 36. Question

A new security mandate requires that all personnel data held in the cloud is encrypted at rest. Which two methods allow you to encrypt data stored in S3 buckets at rest cost-efficiently? (choose 2)

* + Use CloudHSM
  + Use Multipart upload with SSL
  + **Encrypt the data at the source using the client's CMK keys before transferring it to S3**
  + **Use AWS S3 server-side encryption with Key Management Service keys or Customer-provided keys**
  + Make use of AWS S3 bucket policies to control access to the data at rest

**Unattempted**

When using S3 encryption your data is always encrypted at rest and you can choose to use KMS managed keys or customer-provided keys. If you encrypt the data at the source and transfer it in an encrypted state it will also be encrypted in-transit.  
With client side encryption data is encrypted on the client side and transferred in an encrypted state and with server-side encryption data is encrypted by S3 before it is written to disk (data is decrypted when it is downloaded).  
CORRECT: “Use AWS S3 server-side encryption with Key Management Service keys or Customer-provided keys” is the correct answer.  
CORRECT: “Encrypt the data at the source using the client’s CMK keys before transferring it to S3” is the correct answer.  
INCORRECT: “Make use of AWS S3 bucket policies to control access to the data at rest” is incorrect. You can use bucket policies to control encryption of data that is uploaded but use of encryption is not stated in the answer given. Simply using bucket policies to control access to the data does not meet the security mandate that data must be encrypted.  
INCORRECT: “Use CloudHSM” is incorrect. CloudHSM can be used to encrypt data but as a dedicated service it is charged on an hourly basis and is less cost-efficient compared to S3 encryption or encrypting the data at the source.  
INCORRECT: “Use Multipart upload with SSL” is incorrect. Multipart upload helps with uploading large files but does not encrypt your data.  
References:  
<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html>

Topic: aws-solutions-architect-associate/storage/amazon-s3/

1. 37. Question

A Solutions Architect is designing a web page for event registrations, and needs a managed service to send a text message to users every time users sign up for an event.  
Which AWS service should the Architect use to achieve this?

* + Amazon SQS
  + **Amazon SNS**
  + Amazon STS
  + AWS Lambda

**Unattempted**

Amazon Simple Notification Service (SNS) is a web service that makes it easy to set up, operate, and send notifications from the cloud and supports notifications over multiple transports including HTTP/HTTPS, Email/Email-JSON, SQS and SMS.

[A diagram of a service

Description automatically generated](https://skillcertpro.com/wp-content/uploads/2020/08/a47.jpg)  
CORRECT: “Amazon SNS” is the correct answer.  
INCORRECT: “Amazon STS” is incorrect. Amazon Security Token Service (STS) is used for requesting temporary credentials.  
INCORRECT: “Amazon SQS” is incorrect. Amazon Simple Queue Service (SQS) is a message queue used for decoupling application components.  
INCORRECT: “AWS Lambda” is incorrect. Lambda is a serverless service that runs code in response to events/triggers.  
References:  
<https://docs.aws.amazon.com/sns/latest/dg/welcome.html>

Topic: aws-solutions-architect-associate/application-integration/amazon-sns/

1. 38. Question

You need to scale read operations for your Amazon Aurora DB within a region. To increase availability you also need to be able to failover if the primary instance fails.  
What should you implement?

* + Aurora Global Database
  + An Aurora Cluster Volume
  + **Aurora Replicas**
  + A DB cluster

**Unattempted**

Aurora Replicas are independent endpoints in an Aurora DB cluster, best used for scaling read operations and increasing availability. Up to 15 Aurora Replicas can be distributed across the Availability Zones that a DB cluster spans within an AWS Region. To increase availability, you can use Aurora Replicas as failover targets. That is, if the primary instance fails, an Aurora Replica is promoted to the primary instance.  
The graphic below provides an overview of Aurora Replicas:

[A diagram of data processing

Description automatically generated](https://skillcertpro.com/wp-content/uploads/2020/08/a48.jpg)  
CORRECT: “Aurora Replicas” is the correct answer.  
INCORRECT: “A DB cluster” is incorrect. An Amazon Aurora DB cluster consists of a DB instance, compatible with either MySQL or PostgreSQL, and a cluster volume that represents the data for the DB cluster, copied across three Availability Zones as a single, virtual volume. The DB cluster contains a primary instance and, optionally, up to 15 Aurora Replicas. A DB cluster does not necessarily scale read operations as it is optional to deploy Aurora Replicas, therefore it can be thought of as more of a storage level availability feature in this case and is not the best answer.  
INCORRECT: “An Aurora Cluster Volume” is incorrect. A cluster volume manages the data for DB instances in a DB cluster and does not provide read scaling.  
INCORRECT: “Aurora Global Database” is incorrect. Amazon Aurora Global Database is not suitable for scaling read operations within a region. It is a new feature in the MySQL-compatible edition of Amazon Aurora, designed for applications with a global footprint. It allows a single Aurora database to span multiple AWS regions, with fast replication to enable low-latency global reads and disaster recovery from region-wide outages.  
References:  
<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html>

Topic: aws-solutions-architect-associate/database/amazon-aurora/

1. 39. Question

You are planning to deploy a number of EC2 instances in your VPC. The EC2 instances will be deployed across several subnets and multiple AZs. What AWS feature can act as an instance-level firewall to control traffic between your EC2 instances?

* + **Security Group**
  + Route table
  + AWS WAF
  + Network ACL

**Unattempted**

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC can be assigned to a different set of security groups.  
CORRECT: “Security group” is the correct answer.  
INCORRECT: “AWS WAF” is incorrect. AWS WAF is a web application firewall and does not work at the instance level.  
INCORRECT: “Route table” is incorrect. Route tables are not firewalls.  
INCORRECT: “Network ACL” is incorrect. Network ACL’s function at the subnet level.  
References:  
<https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html>

Topic: aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

1. 40. Question

An Architect needs to find a way to automatically and repeatably create many member accounts within an AWS Organization. The accounts also need to be moved into an OU and have VPCs and subnets created.  
What is the best way to achieve this?

* + Use the AWS CLI
  + Use the AWS Organizations API
  + **Use CloudFormation with scripts**
  + Use the AWS Management Console

**Unattempted**

The best solution is to use a combination of scripts and AWS CloudFormation. You will also leverage the AWS Organizations API. This solution can provide all of the requirements.  
CORRECT: “Use CloudFormation with scripts” is the correct answer.  
INCORRECT: “Use the AWS Organizations API” is incorrect. You can create member accounts with the AWS Organizations API. However, you cannot use that API to configure the account and create VPCs and subnets.  
INCORRECT: “Use the AWS Management Console” is incorrect. Using the AWS Management Console is not a method of automatically creating the resources.  
INCORRECT: “Use the AWS CLI” is incorrect. You can do all tasks using the AWS CLI but it is better to automate the process using AWS CloudFormation.  
References:  
<https://aws.amazon.com/blogs/security/how-to-use-aws-organizations-to-automate-end-to-end-account-creation/>

Topic: aws-solutions-architect-associate/management-tools/aws-organizations/

1. 41. Question

An online store uses an Amazon Aurora database. The database is deployed as a Multi-AZ deployment. Recently, metrics have shown that database read requests are high and causing performance issues which result in latency for write requests.  
What should the solutions architect do to separate the read requests from the write requests?

* + **Create a read replica and modify the application to use the appropriate endpoint.**
  + Create a second Amazon Aurora database and link it to the primary database as a read replica
  + Enable read through caching on the Amazon Aurora database
  + Update the application to read from the Multi-AZ standby instance

**Unattempted**

The best solution for the solutions architect to separate read requests from write requests in this scenario is:

**A. Create a read replica and modify the application to use the appropriate endpoint.**

Here’s why this option is the most suitable:

* + **Read replicas in Aurora:** Aurora allows creating read replicas, which are read-only copies of the primary database. This means read requests can be directed to the replica, offloading the load from the primary database and improving write performance.
  + **Modifying the application:** The application needs to be modified to connect to the read replica endpoint specifically for read requests. This can be done through configuration changes or introducing logic to differentiate between read and write operations.
  + **Ineffectiveness of other options:**
    - **Creating a second database (B):** This would be unnecessary and wouldn’t address the issue of separating read and write traffic within the same application.
    - **Read through caching (C):** While caching can improve read performance to some extent, it’s not a substitute for separating read and write workloads. Writes still need to be directed to the primary database, and maintaining cache coherence adds complexity.
    - **Using the standby instance (D):** The Multi-AZ standby in Aurora is intended for automatic failover if the primary instance becomes unavailable. It’s not designed for routine read operations and might have higher latency due to its asynchronous nature.

Therefore, creating a read replica and adapting the application is the most efficient and cost-effective solution to address the high read traffic impacting write performance in this scenario.

1. 42. Question

A production application runs on an Amazon RDS MySQL DB instance. A solutions architect is building a new reporting tool that will access the same data. The reporting tool must be highly available and not impact the performance of the production application.  
How can this be achieved?

* + Use Amazon Data Lifecycle Manager to automatically create and manage snapshots
  + Create a Single-AZ RDS Read Replica of the production RDS DB instance. Create a second Single-AZ RDS Read Replica from the replica
  + Create a cross-region Multi-AZ deployment and create a read replica in the second region
  + **Create a Multi-AZ RDS Read Replica of the production RDS DB instance**

**Unattempted**

You can create a read replica as a Multi-AZ DB instance. Amazon RDS creates a standby of your replica in another Availability Zone for failover support for the replica. Creating your read replica as a Multi-AZ DB instance is independent of whether the source database is a Multi-AZ DB instance.  
CORRECT: “Create a Multi-AZ RDS Read Replica of the production RDS DB instance” is the correct answer.  
INCORRECT: “Create a Single-AZ RDS Read Replica of the production RDS DB instance. Create a second Single-AZ RDS Read Replica from the replica” is incorrect. Read replicas are primarily used for horizontal scaling. The best solution for high availability is to use a Multi-AZ read replica.  
INCORRECT: “Create a cross-region Multi-AZ deployment and create a read replica in the second region” is incorrect as you cannot create a cross-region Multi-AZ deployment with RDS.  
INCORRECT: “Use Amazon Data Lifecycle Manager to automatically create and manage snapshots” is incorrect as using snapshots is not the best solution for high availability.  
References:  
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_MySQL.Replication.ReadReplicas.html#USER_MySQL.Replication.ReadReplicas.MultiAZ>

Topic: aws-solutions-architect-associate/database/amazon-rds/

1. 43. Question

You have created an application in a VPC that uses a Network Load Balancer (NLB). The application will be offered in a service provider model for AWS principals in other accounts within the region to consume. Based on this model, what AWS service will be used to offer the service for consumption?

* + API Gateway
  + IAM Role Based Access Control
  + Route 53
  + **VPC Endpoint Services using AWS PrivateLink**

**Unattempted**

An Interface endpoint uses AWS PrivateLink and is an elastic network interface (ENI) with a private IP address that serves as an entry point for traffic destined to a supported service.  
Using PrivateLink you can connect your VPC to supported AWS services, services hosted by other AWS accounts (VPC endpoint services), and supported AWS Marketplace partner services.  
CORRECT: “VPC Endpoint Services using AWS PrivateLink” is the correct answer.  
INCORRECT: “IAM Role Based Access Control” is incorrect as this provides authorization.  
INCORRECT: “Route 53” is incorrect as this service provides DNS resolution.  
INCORRECT: “API Gateway” is incorrect as this service is used for hosting REST and Websocket APIs.  
References:  
<https://docs.aws.amazon.com/vpc/latest/userguide/endpoint-service.html>

Topic: aws-solutions-architect-associate/networking-and-content-delivery/amazon-vpc/

1. 44. Question

A company allows its developers to attach existing IAM policies to existing IAM roles to enable faster experimentation and agility. However, the security operations team is concerned that the developers could attach the existing administrator policy, which would allow the developers to circumvent any other security policies.  
How should a solutions architect address this issue?

* + Prevent the developers from attaching any policies and assign all IAM duties to the security operations team
  + Use service control policies to disable IAM activity across all accounts in the organizational unit
  + **Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy.**
  + Create an Amazon SNS topic to send an alert every time a developer creates a new policy

**Unattempted**

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

[A diagram of a policy

Description automatically generated](https://skillcertpro.com/wp-content/uploads/2020/08/a24.jpg)  
Therefore, the solutions architect can set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy.  
CORRECT: “Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy” is the correct answer.  
INCORRECT: “Create an Amazon SNS topic to send an alert every time a developer creates a new policy” is incorrect as this would mean investigating every incident which is not an efficient solution.  
INCORRECT: “Use service control policies to disable IAM activity across all accounts in the organizational unit” is incorrect as this would prevent the developers from being able to work with IAM completely.  
INCORRECT: “Prevent the developers from attaching any policies and assign all IAM duties to the security operations team” is incorrect as this is not necessary. The requirement is to allow developers to work with policies, the solution needs to find a secure way of achieving this.  
References:  
<https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html>

Topic: aws-solutions-architect-associate/security-identity-compliance/aws-iam/

1. 45. Question

A client needs to implement a shared directory system. Requirements are that it should provide a hierarchical structure, support strong data consistency, and be accessible from multiple accounts, regions and on-premises servers using their AWS Direct Connect link.  
Which storage service would you recommend to the client?

* + AWS Storage Gateway
  + **Amazon EFS**
  + Amazon EBS
  + Amazon S3

**Unattempted**

Amazon EFS provides high-performance, secure access for thousands of connections to a shared file system using a traditional file permissions model, file locking, and hierarchical directory structure via the NFSv4 protocol.  
It allows you to simultaneously share files between multiple Amazon EC2 instances across multiple AZs, regions, VPCs, and accounts as well as on-premises servers via AWS Direct Connect or AWS VPN.  
This is ideal for your business applications that need to share a common data source. For application workloads with many instances accessing the same set of files, Amazon EFS provides strong data consistency helping to ensure that any file read will reflect the last write of the file.  
CORRECT: “Amazon EFS” is the correct answer.  
INCORRECT: “AWS Storage Gateway” is incorrect. AWS Storage Gateway supports multiple modes of operation but none of them provide a single shared storage location that is accessible from multiple accounts, regions and on-premise servers simultaneously.  
INCORRECT: “Amazon EBS” is incorrect. Amazon EBS is a block-storage device that is attached to an individual instance and cannot be shared between multiple instances. EBS does not support multiple requirements in this scenario.  
INCORRECT: “Amazon S3” is incorrect. Amazon S3 does not support a hierarchical structure. Though you can create folders within buckets, these are actually just pointers to groups of objects. The structure is flat in Amazon S3. Also, the consistency model of Amazon S3 is read-after-write for PUTS of new objects, but only eventual consistency for overwrite PUTS and DELETES. This does not support the requirement for strong consistency.  
References:  
<https://aws.amazon.com/efs/features/>

Topic: aws-solutions-architect-associate/storage/amazon-efs/

1. 46. Question

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

* + **Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period.**
  + Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens
  + Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period
  + Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens

**Unattempted**

Though this sounds like a good use case for scheduled actions, both answers using scheduled actions will have 20 instances running regardless of actual demand. A better option to be more cost effective is to use a target tracking action that triggers at a lower CPU threshold.  
With this solution the scaling will occur before the CPU utilization gets to a point where performance is affected. This will result in resolving the performance issues whilst minimizing costs. Using a reduced cooldown period will also more quickly terminate unneeded instances, further reducing costs.  
CORRECT: “Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period” is the correct answer.  
INCORRECT: “Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens” is incorrect as this is not the most cost-effective option. Note you can choose min, max, or desired for a scheduled action.  
INCORRECT: “Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens” is incorrect as this is not the most cost-effective option. Note you can choose min, max, or desired for a scheduled action.  
INCORRECT: “Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period” is incorrect as AWS recommend you use target tracking in place of step scaling for most use cases.  
References:  
<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html>

Topic: aws-solutions-architect-associate/compute/aws-auto-scaling/

1. 47. Question

A company’s Amazon EC2 instances were terminated or stopped, resulting in a loss of important data that was stored on attached EC2 instance stores. They want to avoid this happening in the future and need a solution that can scale as data volumes increase with the LEAST amount of management and configuration.  
Which storage is most appropriate?

* + Amazon RDS
  + Amazon EBS
  + Amazon S3
  + **Amazon EFS**

**Unattempted**

Amazon EFS is a fully managed service that requires no changes to your existing applications and tools, providing access through a standard file system interface for seamless integration. It is built to scale on demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files. This is an easy solution to implement and the option that requires the least management and configuration.  
An instance store provides temporary block-level storage for an EC2 instance. If you terminate the instance you lose all data. The alternative is to use Elastic Block Store volumes which are also block-level storage devices but the data is persistent. However, EBS is not a fully managed solution and doesn’t grow automatically as your data requirements increase – you would need to increase the volume size and then extend your filesystem.  
CORRECT: “Amazon EFS” is the correct answer.  
INCORRECT: “Amazon S3” is incorrect. Amazon S3 is an object storage solution and as the data is currently sitting on a block storage you would need to develop some way to use the REST API to upload/manage data on S3 – this is not the easiest solution to implement.  
INCORRECT: “Amazon EBS” is incorrect as EBS is not a fully managed solution and doesn’t grow automatically as your data requirements increase – you would need to increase the volume size and then extend your filesystem.  
INCORRECT: “Amazon RDS” is incorrect. Amazon RDS is a relational database service, the question is not looking for a database, just a way of storing data.  
References:  
<https://aws.amazon.com/efs/>

Topic: aws-solutions-architect-associate/storage/amazon-efs/

1. 48. Question

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

* + **Use AWS Lambda to manipulate the original images to the requested customization.Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin**
  + Use AWS Lambda to manipulate the original images to the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Elastic Load Balancer in front of the Amazon EC2 instances
  + Use Amazon EC2 instances to manipulate the original images into the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Amazon CloudFront distribution with the S3 bucket as the origin
  + Use Amazon EC2 instances to manipulate the original images into the requested customization. Store the original and manipulated images in Amazon S3. Configure an Elastic Load Balancer in front of the EC2 instances

**Unattempted**

All solutions presented are highly available. The key requirement that must be satisfied is that the solution should be cost-effective and you must choose the most cost-effective option.  
Therefore, it’s best to eliminate services such as Amazon EC2 and ELB as these require ongoing costs even when they’re not used. Instead, a fully serverless solution should be used. AWS Lambda, Amazon S3 and CloudFront are the best services to use for these requirements.  
CORRECT: “Use AWS Lambda to manipulate the original images to the requested customization. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin” is the correct answer.  
INCORRECT: “Use Amazon EC2 instances to manipulate the original images into the requested customization. Store the original and manipulated images in Amazon S3. Configure an Elastic Load Balancer in front of the EC2 instances” is incorrect. This is not the most cost-effective option as the ELB and EC2 instances will incur costs even when not used.  
INCORRECT: “Use AWS Lambda to manipulate the original images to the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Elastic Load Balancer in front of the Amazon EC2 instances” is incorrect. This is not the most cost-effective option as the ELB will incur costs even when not used. Also, Amazon DynamoDB will incur RCU/WCUs when running and is not the best choice for storing images.  
INCORRECT: “Use Amazon EC2 instances to manipulate the original images into the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Amazon CloudFront distribution with the S3 bucket as the origin” is incorrect. This is not the most cost-effective option as the EC2 instances will incur costs even when not used  
References:  
<https://aws.amazon.com/serverless/>

Topic: aws-solutions-architect-associate/storage/amazon-s3/  
Topic: aws-solutions-architect-associate/compute/aws-lambda/  
Topic: aws-solutions-architect-associate/networking-and-content-delivery/amazon-cloudfront/

1. 49. Question

Developers regularly create and update CloudFormation stacks using API calls. For security reasons you need to ensure that users are restricted to a specified template. How can this be achieved?

* + Create an IAM policy with a Condition: ResourceTypes parameter
  + Create an IAM policy with a Condition: StackPolicyURL parameter
  + **Create an IAM policy with a Condition: TemplateURL parameter**
  + Store the template on Amazon S3 and use a bucket policy to restrict access

**Unattempted**

The cloudformation:TemplateURL, lets you specify where the CloudFormation template for a stack action, such as create or update, resides and enforce that it be used.  
CORRECT: “Create an IAM policy with a Condition: TemplateURL parameter” is the correct answer.  
INCORRECT: “Store the template on Amazon S3 and use a bucket policy to restrict access” is incorrect. Configuring a bucket policy on the Amazon S3 bucket where you place your templates is a good idea, but it does not enforce CloudFormation create and update API requests to use the templates in the bucket.  
INCORRECT: “Create an IAM policy with a Condition: ResourceTypes parameter” is incorrect. The CloudFormation API accepts a ResourceTypes parameter. In your API call, you specify which types of resources can be created or updated. This does not control which template is used.  
INCORRECT: “Create an IAM policy with a Condition: StackPolicyURL parameter” is incorrect. You can ensure that every CloudFormation stack has a stack policy associated with it upon creation with the StackPolicyURL condition. However, this parameter itself is not used to specify the template to use.  
References:  
<https://aws.amazon.com/blogs/devops/aws-cloudformation-security-best-practices/>  
<https://aws.amazon.com/cloudformation/aws-cloudformation-templates/>

Topic: aws-solutions-architect-associate/management-tools/aws-cloudformation/

1. 50. Question

A High Performance Computing (HPC) application will be migrated to AWS. The application requires low network latency and high throughput between nodes and will be deployed in a single AZ.  
How should the application be deployed for best inter-node performance?

* + In a spread placement group
  + **In a cluster placement group**
  + In a partition placement group
  + Behind a Network Load Balancer (NLB)

**Unattempted**

A cluster placement group provides low latency and high throughput for instances deployed in a single AZ. It is the best way to provide the performance required for this application.  
CORRECT: “In a cluster placement group” is the correct answer.  
INCORRECT: “In a partition placement group” is incorrect. A partition placement group is used for grouping instances into logical segments. It provides control and visibility into instance placement but is not the best option for performance.  
INCORRECT: “In a spread placement group” is incorrect. A spread placement group is used to spread instances across underlying hardware. It is not the best option for performance.  
INCORRECT: “Behind a Network Load Balancer (NLB)” is incorrect. A network load balancer is used for distributing incoming connections, this does assist with inter-node performance.  
References:  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

Topic: aws-solutions-architect-associate/compute/amazon-ec2/

1. 51. Question

A Solutions Architect is designing a web application that runs on Amazon EC2 instances behind an Elastic Load Balancer. All data in transit must be encrypted.  
Which solution options meet the encryption requirement? (choose 2)

* + Use an Application Load Balancer (ALB) in passthrough mode, then terminate SSL on EC2 instances
  + Use an Application Load Balancer (ALB) with a TCP listener, then terminate SSL on EC2 instances
  + **Use a Network Load Balancer (NLB) with a TCP listener, then terminate SSL on EC2 instances**
  + **Use an Application Load Balancer (ALB) with an HTTPS listener, then install SSL certificates on the ALB and EC2 instances**
  + Use a Network Load Balancer (NLB) with an HTTPS listener, then install SSL certificates on the NLB and EC2 instances

**Unattempted**

You can passthrough encrypted traffic with an NLB and terminate the SSL on the EC2 instances, so this is a valid answer.  
You can use a HTTPS listener with an ALB and install certificates on both the ALB and EC2 instances. This does not use passthrough, instead it will terminate the first SSL connection on the ALB and then re-encrypt the traffic and connect to the EC2 instances.  
CORRECT: “Use a Network Load Balancer (NLB) with a TCP listener, then terminate SSL on EC2 instances” is the correct answer.  
CORRECT: “Use an Application Load Balancer (ALB) with an HTTPS listener, then install SSL certificates on the ALB and EC2 instances” is the correct answer.  
INCORRECT: “Use an Application Load Balancer (ALB) in passthrough mode, then terminate SSL on EC2 instances” is incorrect. You cannot use passthrough mode with an ALB and terminate SSL on the EC2 instances.  
INCORRECT: “Use a Network Load Balancer (NLB) with an HTTPS listener, then install SSL certificates on the NLB and EC2 instances” is incorrect. You cannot use a HTTPS listener with an NLB.  
INCORRECT: “Use an Application Load Balancer (ALB) with a TCP listener, then terminate SSL on EC2 instances” is incorrect. You cannot use a TCP listener with an ALB.  
References:  
<https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/what-is-load-balancing.html>

Topic: aws-solutions-architect-associate/compute/elastic-load-balancing/

1. 52. Question

The security team in your company is defining new policies for enabling security analysis, resource change tracking, and compliance auditing. They would like to gain visibility into user activity by recording API calls made within the company’s AWS account. The information that is logged must be encrypted. This requirement applies to all AWS regions in which your company has services running.  
How will you implement this request? (choose 2)

* + **Create a CloudTrail trail and apply it to all regions**
  + Use CloudWatch to monitor API calls
  + Create a CloudTrail trail in each region in which you have services
  + **Enable encryption with a single KMS key**
  + Enable encryption with multiple KMS keys

**Unattempted**

CloudTrail is used for recording API calls (auditing) whereas CloudWatch is used for recording metrics (performance monitoring). The solution can be deployed with a single trail that is applied to all regions. A single KMS key can be used to encrypt log files for trails applied to all regions. CloudTrail log files are encrypted using S3 Server Side Encryption (SSE) and you can also enable encryption SSE KMS for additional security.  
CORRECT: “Enable encryption with a single KMS key” is the correct answer.  
CORRECT: “Create a CloudTrail trail and apply it to all regions” is the correct answer.  
INCORRECT: “Create a CloudTrail trail in each region in which you have services” is incorrect. You do not need to create a separate trail in each region.  
INCORRECT: “Enable encryption with multiple KMS keys” is incorrect. You do not need to use multiple KMS keys.  
INCORRECT: “Use CloudWatch to monitor API calls” is incorrect. CloudWatch is not used for monitoring API calls (use CloudTrail).  
References:  
<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/receive-cloudtrail-log-files-from-multiple-regions.html>

Topic: aws-solutions-architect-associate/management-tools/aws-cloudtrail/

1. 53. Question

A solutions architect is finalizing the architecture for a distributed database that will run across multiple Amazon EC2 instances. Data will be replicated across all instances so the loss of an instance will not cause loss of data. The database requires block storage with low latency and throughput that supports up to several million transactions per second per server.  
Which storage solution should the solutions architect use?

* + Amazon S3
  + Amazon EFS
  + Amazon EBS
  + **Amazon EC2 instance store**

**Unattempted**

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

[A close-up of a computer store

Description automatically generated](https://skillcertpro.com/wp-content/uploads/2020/08/a27.jpg)  
Some instance types use NVMe or SATA-based solid state drives (SSD) to deliver high random I/O performance. This is a good option when you need storage with very low latency, but you don’t need the data to persist when the instance terminates or you can take advantage of fault-tolerant architectures.  
In this scenario the data is replicated and fault tolerant so the best option to provide the level of performance required is to use instance store volumes.  
CORRECT: “Amazon EC2 instance store” is the correct answer.  
INCORRECT: “Amazon EBS ” is incorrect. The Elastic Block Store (EBS) is a block storage device but as the data is distributed and fault tolerant a better option for performance would be to use instance stores.  
INCORRECT: “Amazon EFS ” is incorrect as EFS is not a block device, it is a filesystem that is accessed using the NFS protocol.  
INCORRECT: “Amazon S3” is incorrect as S3 is an object-based storage system, not a block-based storage system.  
References:  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html>

Topic: aws-solutions-architect-associate/compute/amazon-ebs/

1. 54. Question

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

* + Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)
  + Amazon S3 Intelligent-Tiering
  + Amazon S3 Glacier Deep Archive
  + **Amazon S3 Standard**

**Unattempted**

S3 standard is the best choice in this scenario for a short term storage solution. In this case the size and number of logs is unknown and it would be difficult to fully assess the access patterns at this stage. Therefore, using S3 standard is best as it is cost-effective, provides immediate access, and there are no retrieval fees or minimum capacity charge per object.  
CORRECT: “Amazon S3 Standard” is the correct answer.  
INCORRECT: “Amazon S3 Intelligent-Tiering” is incorrect as there is an additional fee for using this service and for a short-term requirement it may not be beneficial.  
INCORRECT: “Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)” is incorrect as this storage class has a minimum capacity charge per object (128 KB) and a per GB retrieval fee.  
INCORRECT: “Amazon S3 Glacier Deep Archive” is incorrect as this storage class is used for archiving data. There are retrieval fees and it take hours to retrieve data from an archive.  
References:  
<https://aws.amazon.com/s3/storage-classes/>

Topic: aws-solutions-architect-associate/storage/amazon-s3/

1. 55. Question

You are a Solutions Architect at SkillCertPro Training. One of your clients runs an application that writes data to a DynamoDB table. The client has asked how they can implement a function that runs code in response to item level changes that take place in the DynamoDB table. What would you suggest to the client?

* + Enable server access logging and create an event source mapping between AWS Lambda and the S3 bucket to which the logs are written
  + Use Kinesis Data Streams and configure DynamoDB as a producer
  + **Enable DynamoDB Streams and create an event source mapping between AWS Lambda and the relevant stream**
  + Create a local secondary index that records item level changes and write some custom code that responds to updates to the index

**Unattempted**

DynamoDB Streams help you to keep a list of item level changes or provide a list of item level changes that have taken place in the last 24hrs. Amazon DynamoDB is integrated with AWS Lambda so that you can create triggers—pieces of code that automatically respond to events in DynamoDB Streams.  
If you enable DynamoDB Streams on a table, you can associate the stream ARN with a Lambda function that you write. Immediately after an item in the table is modified, a new record appears in the table’s stream. AWS Lambda polls the stream and invokes your Lambda function synchronously when it detects new stream records.  
An event source mapping identifies a poll-based event source for a Lambda function. It can be either an Amazon Kinesis or DynamoDB stream. Event sources maintain the mapping configuration except for stream-based services (e.g. DynamoDB, Kinesis) for which the configuration is made on the Lambda side and Lambda performs the polling.  
CORRECT: “Enable DynamoDB Streams and create an event source mapping between AWS Lambda and the relevant stream” is the correct answer.  
INCORRECT: “Enable server access logging and create an event source mapping between AWS Lambda and the S3 bucket to which the logs are written” is incorrect. The questions asks for a solution that runs code in response to changes in a DynamoDB table, not an S3 bucket.  
INCORRECT: “Create a local secondary index that records item level changes and write some custom code that responds to updates to the index” is incorrect. A local secondary index maintains an alternate sort key for a given partition key value, it does not record item level changes.  
INCORRECT: “Use Kinesis Data Streams and configure DynamoDB as a producer” is incorrect. You cannot configure DynamoDB as a Kinesis Data Streams producer.  
References:  
<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.Lambda.html>

Topic: aws-solutions-architect-associate/database/amazon-dynamodb/  
Topic: aws-solutions-architect-associate/compute/aws-lambda/

1. 56. Question

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

* + Amazon RDS
  + Amazon EC2 Auto Scaling
  + **Amazon DynamoDB**
  + AWS Fargate
  + **AWS Lambda**

**Unattempted**

In this case AWS Lambda can perform the computation and store the data in an Amazon DynamoDB table. Lambda can scale concurrent executions to meet demand easily and DynamoDB is built for key-value data storage requirements and is also serverless and easily scalable. This is therefore a cost effective solution for unpredictable workloads.  
CORRECT: “AWS Lambda” is a correct answer.  
CORRECT: “Amazon DynamoDB” is also a correct answer.  
INCORRECT: “AWS Fargate” is incorrect as containers run constantly and therefore incur costs even when no requests are being made.  
INCORRECT: “Amazon EC2 Auto Scaling” is incorrect as this uses EC2 instances which will incur costs even when no requests are being made.  
INCORRECT: “Amazon RDS” is incorrect as this is a relational database not a No-SQL database. It is therefore not suitable for key-value data storage requirements.  
References:  
<https://aws.amazon.com/lambda/features/>  
<https://aws.amazon.com/dynamodb/>

Topic: aws-solutions-architect-associate/compute/aws-lambda/  
Topic: aws-solutions-architect-associate/database/amazon-dynamodb/

1. 57. Question

A web application runs in public and private subnets. The application architecture consists of a web tier and database tier running on Amazon EC2 instances. Both tiers run in a single Availability Zone (AZ).  
Which combination of steps should a solutions architect take to provide high availability for this architecture? (Select TWO.)

* + **Create new public and private subnets in the same VPC, each in a new AZ. Migrate the database to an Amazon RDS multi-AZ deployment**
  + **Create an Amazon EC2 Auto Scaling group and Application Load Balancer (ALB) spanning multiple AZs**
  + Create new public and private subnets in a new AZ. Create a database using Amazon EC2 in one AZ
  + Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer (ALB)
  + Create new public and private subnets in the same AZ for high availability

**Unattempted**

To add high availability to this architecture both the web tier and database tier require changes. For the web tier an Auto Scaling group across multiple AZs with an ALB will ensure there are always instances running and traffic is being distributed to them.  
The database tier should be migrated from the EC2 instances to Amazon RDS to take advantage of a managed database with Multi-AZ functionality. This will ensure that if there is an issue preventing access to the primary database a secondary database can take over.  
CORRECT: “Create an Amazon EC2 Auto Scaling group and Application Load Balancer (ALB) spanning multiple AZs” is the correct answer.  
CORRECT: “Create new public and private subnets in the same VPC, each in a new AZ. Migrate the database to an Amazon RDS multi-AZ deployment” is the correct answer.  
INCORRECT: “Create new public and private subnets in the same AZ for high availability” is incorrect as this would not add high availability.  
INCORRECT: “Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer (ALB)” is incorrect because the existing servers are in a single subnet. For HA we need to instances in multiple subnets.  
INCORRECT: “Create new public and private subnets in a new AZ. Create a database using Amazon EC2 in one AZ” is incorrect because we also need HA for the database layer.  
References:  
<https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html>  
<https://aws.amazon.com/rds/features/multi-az/>

Topic: aws-solutions-architect-associate/compute/elastic-load-balancing/  
Topic: aws-solutions-architect-associate/compute/aws-auto-scaling/  
Topic: aws-solutions-architect-associate/database/amazon-rds/

1. 58. Question

A solutions architect is creating a document submission application for a school. The application will use an Amazon S3 bucket for storage. The solution must prevent accidental deletion of the documents and ensure that all versions of the documents are available. Users must be able to upload and modify the documents.  
Which combination of actions should be taken to meet these requirements? (Select TWO.)

* + Encrypt the bucket using AWS SSE-S3
  + Attach an IAM policy to the bucket
  + **Enable versioning on the bucket**
  + Set read-only permissions on the bucket
  + **Enable MFA Delete on the bucket**

**Unattempted**

None of the options present a good solution for specifying permissions required to write and modify objects so that requirement needs to be taken care of separately. The other requirements are to prevent accidental deletion and the ensure that all versions of the document are available.  
The two solutions for these requirements are versioning and MFA delete. Versioning will retain a copy of each version of the document and multi-factor authentication delete (MFA delete) will prevent any accidental deletion as you need to supply a second factor when attempting a delete.  
CORRECT: “Enable versioning on the bucket” is a correct answer.  
CORRECT: “Enable MFA Delete on the bucket” is also a correct answer.  
INCORRECT: “Set read-only permissions on the bucket” is incorrect as this will also prevent any writing to the bucket which is not desired.  
INCORRECT: “Attach an IAM policy to the bucket” is incorrect as users need to modify documents which will also allow delete. Therefore, a method must be implemented to just control deletes.  
INCORRECT: “Encrypt the bucket using AWS SSE-S3” is incorrect as encryption doesn’t stop you from deleting an object.References:  
<https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html>  
<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMFADelete.html>

Topic: aws-solutions-architect-associate/storage/amazon-s3/

1. 59. Question

An application receives images uploaded by customers and stores them on Amazon S3. An AWS Lambda function then processes the images to add graphical elements. The processed images need to be available for users to download for 30 days, after which time they can be deleted. Processed images can be easily recreated from original images. The Original images need to be immediately available for 30 days and be accessible within 24 hours for another 90 days.  
Which combination of Amazon S3 storage classes is most cost-effective for the original and processed images? (choose 2)

* + Store the processed images in STANDARD and then transition to GLACIER after 30 days
  + Store the original images in STANDARD\_IA for 30 days and then transition to DEEP\_ARCHIVE
  + **Store the original images in STANDARD for 30 days, transition to GLACIER for 90 days, then expire the data**
  + **Store the processed images in ONEZONE\_IA and then expire the data after 30 days**
  + Store the original images in STANDARD for 30 days, transition to DEEP\_ARCHIVE for 90 days, then expire the data

**Unattempted**

The key requirements for the original images are that they are immediately available for 30 days (STANDARD), available within 24 hours for 90 days (GLACIER) and then they are not needed (expire them).  
The key requirements for the processed images are that they are immediately available for 30 days (ONEZONE\_IA as they can be recreated from the originals), and then are not needed (expire them).

[A diagram of different colored rectangular shapes

Description automatically generated](https://skillcertpro.com/wp-content/uploads/2020/08/a1-1.jpg)  
CORRECT: “Store the original images in STANDARD for 30 days, transition to GLACIER for 90 days, then expire the data” is a correct answer.  
CORRECT: “Store the processed images in ONEZONE\_IA and then expire the data after 30 days” is also a correct answer.  
INCORRECT: “Store the original images in STANDARD\_IA for 30 days and then transition to DEEP\_ARCHIVE” is incorrect. DEEP\_ARCHIVE has a minimum storage duration of 180 days.  
INCORRECT: “Store the processed images in STANDARD and then transition to GLACIER after 30 days” is incorrect. There is no need to transition the processed images to GLACIER as are not needed after 30 days as they can be recreated if needed from the originals.  
INCORRECT: “Store the original images in STANDARD for 30 days, transition to DEEP\_ARCHIVE for 90 days, then expire the data” is incorrect. DEEP\_ARCHIVE has a minimum storage duration of 180 days.  
References:  
<https://docs.aws.amazon.com/AmazonS3/latest/dev/lifecycle-transition-general-considerations.html>  
<https://aws.amazon.com/s3/storage-classes/>

Topic: aws-solutions-architect-associate/storage/amazon-s3/

1. 60. Question

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

* + **Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure read replicas in ap-southeast-2**
  + Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in the Australian Region
  + Migrate the database to Amazon DynamoDB. Use DynamoDB global tables to enable replication to additional Regions
  + Deploy MySQL instances in each Region. Deploy an Application Load Balancer in front of MySQL to reduce the load on the primary instance

**Unattempted**

The issue here is latency with read queries being directed from Australia to UK which is great physical distance. A solution is required for improving read performance in Australia.  
An Aurora global database consists of one primary AWS Region where your data is mastered, and up to five read-only, secondary AWS Regions. Aurora replicates data to the secondary AWS Regions with typical latency of under a second. You issue write operations directly to the primary DB instance in the primary AWS Region.

[A diagram of a diagram showing the different types of data

Description automatically generated with medium confidence](https://skillcertpro.com/wp-content/uploads/2020/08/a2.jpg)  
This solution will provide better performance for users in the Australia Region for queries. Writes must still take place in the UK Region but read performance will be greatly improved.  
CORRECT: “Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure read replicas in ap-southeast-2” is the correct answer.  
INCORRECT: “Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in the Australian Region” is incorrect. The database is located in UK. If the database is migrated to Australia then the reverse problem will occur. Multi-AZ does not assist with improving query performance across Regions.  
INCORRECT: “Migrate the database to Amazon DynamoDB. Use DynamoDB global tables to enable replication to additional Regions” is incorrect as a relational database running on MySQL is unlikely to be compatible with DynamoDB.  
INCORRECT: “Deploy MySQL instances in each Region. Deploy an Application Load Balancer in front of MySQL to reduce the load on the primary instance” is incorrect as you can only put ALBs in front of the web tier, not the DB tier.  
References:  
<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database.html>

Topic: aws-solutions-architect-associate/database/amazon-aurora/

1. 61. Question

You are a receive significant load that could scale to millions of messages within a short space of time following high-profile matches. As you are unsure of the load required for the database layer what is the most cost-effective way to ensure that the messages are not dropped?

* + Use DynamoDB and provision enough write capacity to handle the highest expected load
  + **Create an SQS queue and modify the application to write to the SQS queue. Launch another application instance the polls the queue and writes messages to the database**
  + Write the data to an S3 bucket, configure RDS to poll the bucket for new messages
  + Use RDS Auto Scaling for the database layer which will automatically scale as required

**Unattempted**

Amazon Simple Queue Service (Amazon SQS) is a web service that gives you access to message queues that store messages waiting to be processed. SQS offers a reliable, highly-scalable, hosted queue for storing messages in transit between computers and is used for distributed/decoupled applications.  
The following diagram depicts a decoupled application using an Amazon SQS queue:

[A diagram of a process

Description automatically generated](https://skillcertpro.com/wp-content/uploads/2020/08/a3-1.jpg)

This is a great use case for SQS as the messages you don’t have to over-provision the database layer or worry about messages being dropped.  
CORRECT: “Create an SQS queue and modify the application to write to the SQS queue. Launch another application instance the polls the queue and writes messages to the database” is the correct answer.  
INCORRECT: “Use DynamoDB and provision enough write capacity to handle the highest expected load” is incorrect. With DynamoDB there are 2 pricing options:  
– Provisioned capacity has been around forever and is one of the incorrect answers to this question. With provisioned capacity you have to specify the number of read/write capacity units to provision and pay for these regardless of the load on the database.  
– With the On-demand capacity mode DynamoDB is charged based on the data reads and writes your application performs on your tables. You do not need to specify how much read and write throughput you expect your application to perform because DynamoDB instantly accommodates your workloads as they ramp up or down. it might be a good solution to this question but is not an available option.  
INCORRECT: “Write the data to an S3 bucket, configure RDS to poll the bucket for new messages” is incorrect.  
INCORRECT: “Use RDS Auto Scaling for the database layer which will automatically scale as required” is incorrect. RDS Auto Scaling does not exist. With RDS you have to select the underlying EC2 instance type to use and pay for that regardless of the actual load on the DB. Note that a new feature released in June 2019 does allow Auto Scaling for the RDS storage, but not the compute layer.  
References:  
<https://aws.amazon.com/sqs/faqs/>

Topic: aws-solutions-architect-associate/application-integration/amazon-sqs/

1. 62. Question

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

* + Enable encryption using Key Management Service (KMS) when creating the cross-region Read Replica
  + Enable encryption on the master DB instance, then create an encrypted cross-region Read Replica
  + Encrypt a snapshot from the master DB instance, create an encrypted cross-region Read Replica from the snapshot
  + **Encrypt a snapshot from the master DB instance, create a new encrypted master DB instance, and then create an encrypted cross-region Read Replica**

**Unattempted**

You cannot create an encrypted Read Replica from an unencrypted master DB instance. You also cannot enable encryption after launch time for the master DB instance. Therefore, you must create a new master DB by taking a snapshot of the existing DB, encrypting it, and then creating the new DB from the snapshot. You can then create the encrypted cross-region Read Replica of the master DB.  
CORRECT: “Encrypt a snapshot from the master DB instance, create a new encrypted master DB instance, and then create an encrypted cross-region Read Replica” is the correct answer.  
INCORRECT: “Enable encryption using Key Management Service (KMS) when creating the cross-region Read Replica” is incorrect. All other options will not work due to the limitations explained above.  
INCORRECT: “Encrypt a snapshot from the master DB instance, create an encrypted cross-region Read Replica from the snapshot” is incorrect. All other options will not work due to the limitations explained above.  
INCORRECT: “Enabled encryption on the master DB instance, then create an encrypted cross-region Read Replica” is incorrect. All other options will not work due to the limitations explained above.  
References:  
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html>  
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html>

Topic: aws-solutions-architect-associate/database/amazon-rds/

1. 63. Question

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

* + Create an IAM policy to deny launching all but the specific instance types
  + Use AWS Resource Access Manager to control which launch types can be used
  + **Create an SCP with a deny rule that denies all but the specific instance types**
  + Create an SCP with an allow rule that allows launching the specific instance types

**Unattempted**

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

[A diagram of a service

Description automatically generated](https://skillcertpro.com/wp-content/uploads/2020/08/a4-1.jpg)  
CORRECT: “Create an SCP with a deny rule that denies all but the specific instance types” is the correct answer.  
INCORRECT: “Create an SCP with an allow rule that allows launching the specific instance types” is incorrect as a deny rule is required.  
INCORRECT: “Create an IAM policy to deny launching all but the specific instance types” is incorrect. With IAM you need to apply the policy within each account rather than centrally so this would require much more effort.  
INCORRECT: “Use AWS Resource Access Manager to control which launch types can be used” is incorrect. AWS Resource Access Manager (RAM) is a service that enables you to easily and securely share AWS resources with any AWS account or within your AWS Organization. It is not used for restricting access or permissions.  
References:  
<https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_example-scps.html#example-ec2-instances>

Topic: aws-solutions-architect-associate/management-tools/aws-organizations/

1. 64. Question

An organization plans to deploy a higher performance computing (HPC) workload on AWS using Linux. The HPC workload will use many Amazon EC2 instances and will generate a large quantity of small output files that must be stored in persistent storage for future use.  
A Solutions Architect must design a solution that will enable the EC2 instances to access data using native file system interfaces and to store output files in cost-effective long-term storage.  
Which combination of AWS services meets these requirements?

* + Amazon EBS volumes with Amazon S3 Glacier.
  + AWS DataSync with Amazon S3 Intelligent tiering.
  + Amazon FSx for Windows File Server with Amazon S3.
  + **Amazon FSx for Lustre with Amazon S3.**

**Unattempted**

Amazon FSx for Lustre is ideal for high performance computing (HPC) workloads running on Linux instances. FSx for Lustre provides a native file system interface and works as any file system does with your Linux operating system.  
When linked to an Amazon S3 bucket, FSx for Lustre transparently presents objects as files, allowing you to run your workload without managing data transfer from S3.  
This solution provides all requirements as it enables Linux workloads to use the native file system interfaces and to use S3 for long-term and cost-effective storage of output files.

A diagram of a software application

Description automatically generated with medium confidence  
CORRECT: “Amazon FSx for Lustre with Amazon S3“ is the correct answer.  
INCORRECT: “Amazon FSx for Windows File Server with Amazon S3“ is incorrect. This service should be used with Windows instances and does not integrate with S3.  
INCORRECT: “Amazon EBS volumes with Amazon S3 Glacier“ is incorrect. EBS volumes do not provide the shared, high performance storage solution using file system interfaces.  
INCORRECT: “AWS DataSync with Amazon S3 Intelligent tiering“ is incorrect. AWS DataSync is used for migrating / synchronizing data.  
References:  
<https://aws.amazon.com/fsx/lustre/>

Topic: amazon-fsx/

1. 65. Question

A company has a web application running on a fleet of EC2 instances configured in an auto-scaling group and behind an Application Load Balancer. Users reported 5XX errors during peak hours because of high traffic spikes. The instances were terminated due to scaling activities, resulting in the 5XX errors. In order to understand the issue, you need to look at the logs for those terminated instances.  
Which of the following helps with the investigation?

* + Use AWS system manager logs to help find the logs for the terminated instances.
  + **Use Application load balancer access logs to get the logs of terminated instances.**
  + Reach out to AWS support, they can retrieve the logs of a terminated instance.
  + Use AWS cloud trail to get the terminated instance logs

**Unattempted**

Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer. Each log contains information such as the time the request was received, the client‘s IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and troubleshoot issues.