1. 1. Question

A food company is building high availability application to collect customer feedback about its products, this application will be deployed on 3 EC2 instances and will run for one year (24/7) then be retired.  
What is the MOST cost-effective way to purchase compute for this platform?

* + Spot Instances
  + Scheduled Reserved Instances
  + ON-Demand Instances
  + **Standard Reserved Instances**

**Correct**

HA + one year (24/7) = Standard Reserved Instances. You can now purchase Amazon EC2 Scheduled Reserved Instances for applications that run on a part-time basis. Reserved Instances provide a capacity reservation so that you can have confidence in your ability to launch the number of instances you have reserved when you need them.  
Starting today, the new Scheduled Reserved Instances option allows you to reserve capacity on recurring daily, weekly, and monthly schedules. For example, you can purchase a daily reservation such as midnight to 6am every day, a weekly reservation such as 8am-5pm every weekday, or a monthly reservation such as the first five days of each month.  
With Reserved Instances, you can now choose the type of capacity reservation that best fits your needs:  
Standard Reserved Instances: The instances you reserved are available to launch any time, 24 hours/day x 7 days/week. This option provides the most flexibility to run instances whenever you need them, including steady state workloads.  
Scheduled Reserved Instances: Instances are available to launch within the time windows you reserved. This option allows you to match your capacity reservation to a predictable recurring schedule.  
Reference  
<https://aws.amazon.com/about-aws/whats-new/2016/01/announcing-amazon-ec2-reserved-instances-for-recurring-instances/>

1. 2. Question

You are a Solutions Architect at a travel agency and you need to give secure access for the development team to the web servers which reside in a private subnet and not accessible from the internet ,the web servers must be accessed via SSH connectivity originated from the corporate network only.  
What are the required steps to provide this secure access?(Choose TWO)

* + Configure inbound network ACL to accept all SSH traffic from the corporate network
  + Create IAM roles with least permission to access to web servers and assign to bastion host
  + Create IAM user with permission to access to web servers and assign to bastion host
  + **Create a bastion host with security group rules that only allow traffic from the corporate network**
  + **Open an SSH port on the security group for web servers and set the source to bastion host.**

**Incorrect**

Exam Tip  
Bastion Host = Secure remote access with Linux bastion hosts on the AWS Cloud  
Explanation  
This Quick Start adds Linux bastion hosts to your new or existing AWS infrastructure for your Linux-based deployments. The bastion hosts provide secure access to Linux instances located in the private and public subnets of your virtual private cloud (VPC).  
The Quick Start sets up a Multi-AZ environment and deploys Linux bastion host instances into the public subnets to provide readily available administrative access to the environment. You can specify the instance type for the bastion hosts and the number of instances you’d like to deploy (1-4).  
An Auto Scaling group ensures that the number of bastion host instances always matches the capacity you specify. The Quick Start also sets up Amazon CloudWatch Logs for remote storage of shell history logs, for added security. After you deploy this Quick Start, you can layer your cloud environment with additional AWS services, infrastructure components, and applications to complete your Linux environment in the AWS Cloud.  
Reference  
<https://aws.amazon.com/quickstart/architecture/linux-bastion/>

1. 3. Question

A company has VPC with private subnet, there are some services running inside the private subnet which needs to access the internet using IPv6 traffic.  
Which service can be used to deliver this solution in the MOST cost-effective && scalability manner?

* + **Egress-only internet gateway**
  + Proxy instance
  + **NAT instance**
  + NAT gateway

**Incorrect**

Exam Tip  
IPv6 traffic =Egress-only internet gateway  
Explanation  
This scenario can configured for IPv6—you can use the VPC wizard to create a VPC and subnets with associated IPv6 CIDR blocks. Instances launched into the subnets can receive IPv6 addresses, and communicate using IPv6. Instances in the private subnet can use an egress-only Internet gateway to connect to the Internet over IPv6, but the Internet cannot establish connections to the private instances over IPv6. For more information about IPv4 and IPv6 addressing  
Reference  
<https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html>

1. 4. Question

You are AWS Chief Architect in a startup company, the company has a legacy application which is running in AWS and connect to the on-premise data center through a VPN connection, you need to log all traffic over the VPN.  
Which AWS service can be used in this case?

* + **Amazon VPC flow logs**
  + ELB access logs
  + AWS CloudTrail logs
  + Amazon CloudWatch Logs

**Correct**

Exam Tip  
VPN Logs =VPC  Flow Logs  
Explanation  
VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs or Amazon S3. After you’ve created a flow log, you can retrieve and view its data in the chosen destination.  
Reference  
<https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html>

1. 5. Question

An governmental university has two-tier web site, each tier consists of Amazon EC2 instances behind an Application Load Balancer, all of EC2 instances run in Auto Scaling groups across two Availability Zones , the web server’s load balancer only will be exposed to the Internet.  
What is the best VPC subnet secure design in each Availability Zone?

* + One public subnet for the Application Load Balancer tier, one public subnet for the web server tier, and one private subnet for the backend tier.
  + One shared public subnet for all tiers
  + One shared private subnet for all tiers
  + **One public subnet for the Application Load Balancer tier, one shared private subnet for the web server and  backend tiers.**
  + One shared public subnet for all tiers

**Correct**

Exam Tip  
ELP only will be exposed over internet so it is the only service which needs to be in a public subnet  
Explanation  
A virtual private cloud (VPC) is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS Cloud. You can launch your AWS resources, such as Amazon EC2 instances, into your VPC.

Public subnet  
If a subnet’s default traffic is routed to an internet gateway, the subnet is known as a public subnet. For example, an instance launched in this subnet is publicly accessible if it has an Elastic IP address or a public IP address associated with it.  
Private subnet  
If a subnet’s default traffic is routed to a NAT instance/gateway or completely lacks a default route, the subnet is known as a private subnet. For example, an instance launched in this subnet is not publicly accessible even if it has an Elastic IP address or a public IP address associated with it.  
Reference  
<https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Subnets.html>  
<https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/>

1. 6. Question

The DevOps team working on designing an Amazon VPC. the applications in the VPC need to have private connection to Amazon Redshift in the same region. One member of the DevOps team consulted you about a the best AWS service to handle this requirement.  
What is your recommendation ?

* + AWS Direct Connect
  + **Amazon VPC endpoint**
  + Amazon egress-only internet gateway
  + Amazon NAT gateway

**Correct**

Exam Tip  
to provide VPC private connection to AWS services = Use VPC endpoint  
Explanation  
A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.  
Reference  
<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html>

1. 7. Question

You want to launch a managed Kubernetes cluster of serverless containers on AWS using open source framework.  
What AWS service can be used for this requirement?

* + SWF
  + **EKS**
  + Glue
  + ECS

**Correct**

Exam Tip  
EKS is open source framework which can be used to manage Kubernetes  cluster .  
Explanation  
Kubernetes is open source software that allows you to deploy and manage containerized applications at scale. Kubernetes manages clusters of Amazon EC2 compute instances and runs containers on those instances with processes for deployment, maintenance, and scaling. Using Kubernetes, you can run any type of containerized applications using the same toolset on-premises and in the cloud.  
AWS makes it easy to run Kubernetes in the cloud with scalable and highly-available virtual machine infrastructure, community-backed service integrations, and Amazon Elastic Kubernetes Service (EKS), a certified conformant, managed Kubernetes service.  
Reference  
<https://aws.amazon.com/kubernetes/>

1. 8. Question

One member of your DevOps team consulted you about the best storage which can handle the following requirements :-  
    – can be scaled automatically.  
    – can be accessed concurrently by multiple EC2 instances.  
    – support file-level locking.  
What is your recommendation?

* + **Amazon EFS**
  + Amazon Snowball
  + Amazon S3
  + Amazon EBS

**Correct**

Exam Tip  
File locking + concurrent access + auto scaling= EFS  
Explanation  
Amazon EFS is a fully-managed service that makes it easy to set up, scale, and cost-optimize file storage in the Amazon Cloud. With a few clicks in the AWS Management Console, you can create file systems that are accessible to Amazon EC2 instances via a file system interface (using standard operating system file I/O APIs) and support full file system access semantics (such as strong consistency and file locking).  
Amazon EFS file systems can automatically scale from gigabytes to petabytes of data without needing to provision storage. Tens, hundreds, or even thousands of Amazon EC2 instances can access an Amazon EFS file system at the same time, and Amazon EFS provides consistent performance to each Amazon EC2 instance. Amazon EFS is designed to be highly durable and highly available. With Amazon EFS, there is no minimum fee or setup costs, and you pay only for what you use.

Reference  
<https://aws.amazon.com/efs/faq/>

1. 9. Question

A petroleum company has a legacy application which currently uses on-premises Oracle database and need to migrate it to AWS.  
Which AWS database can be used to achieve this migration?

* + Amazon Redshift
  + Amazon DynmoDB
  + Amazon ElastiCache
  + **Amazon RDS**

**Correct**

Exam Tip  
Relational Database migration to AWS = Use Amazon RDS  
Reference  
<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-oracle-database-to-amazon-rds-for-oracle.html>

1. 10. Question

You are Solutions Architect in a governmental bank which currently has online transaction processing application and performs heavy read and write queries on Amazon RDS database, the operation team noticed throughput issues with the application.  
Which improvement can be done for the primary database to enhance the performance?

* + **Run SELECT queries for recent data to read replica**
  + Change standby replication mode from Sync to Async
  + Run UPDATE queries on read replica
  + **Run SELECT queries for stale data on read replica**

**Incorrect**

Exam Tip  
for performance enhancement = run SELECT queries on replicas for (Stale + Reporting ) data  
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.  
Reference  
<https://aws.amazon.com/rds/features/read-replicas/>

1. 11. Question

You are designing a food ordering two-tier application to be deployed on a fleet of EC2 instances with Auto Scaling Group ,the backend uses Amazon RDS MySQL database ,this application will be used by millions of users.  
What is the best solution to prevent losing orders and to provide optimum scaling mechanism?(Choose TWO)

* + Use Amazon ElastiCache to store the orders
  + Write the orders in Amazon Cloud Front
  + **Scale based on Number of waiting orders**
  + **Write the orders in Amazon SQS**
  + Scale based on order average processing time

**Incorrect**

Exam Tip  
   – SQS prevent losing orders  
   – Scaling based on the remaining number of orders = tracking scaling policy  
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 the 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 Elastic Load Balancing target group at 1000 for your Auto Scaling group.  
Reference  
<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html>

1. 12. Question

Which AWS service allow users to upload ,store and share millions of documents in a secure ,low cost and high performance way?

* + Amazon EFS
  + AWS lambda function
  + Amazon CloudFront.
  + **Amazon S3**

**Correct**

Exam Tip  
S3 = Secure + Salable + High available  
Explanation  
Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Amazon S3 provides easy-to-use management features so you can organize your data and configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements. Amazon S3 is designed for 99.999999999% (11 9’s) of durability, and stores data for millions of applications for companies all around the world.  
Reference  
<https://aws.amazon.com/s3/>

1. 13. Question

A company is designing bidding application which will receive 1000 bids per second, these bids will be processed in order without losing any bid. there will be multiple services to process each bid.  
What is the best AWS service to handle this requirement?

* + Amazon CloudFront.
  + Amazon SNS
  + **Amazon Kinesis Data Stream**
  + **Amazon SQS**

**Incorrect**

Exam Tip  
1000 bid per second + process in order + no losing messages + multiple services to process each bid= Amazon Kinesis Data Streams  
Explanation  
Amazon Kinesis Data Streams enables real-time processing of streaming big data. It provides ordering of records, as well as the ability to read and/or replay records in the same order to multiple Amazon Kinesis Applications. The Amazon Kinesis Client Library (KCL) delivers all records for a given partition key to the same record processor, making it easier to build multiple applications reading from the same Amazon Kinesis data stream (for example, to perform counting, aggregation, and filtering).  
Amazon Simple Queue Service (Amazon SQS) offers a reliable, highly scalable hosted queue for storing messages as they travel between computers. Amazon SQS lets you easily move data between distributed application components and helps you build applications in which messages are processed independently (with message-level ack/fail semantics), such as automated workflows.

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

1. 14. Question

A company has e-commerce two-tier web application, Application’s front end is deployed on a fleet of EC2 instances with auto scaling group and Application’s backend use Amazon RDS MySql database, the traffic to the application spikes during the promotion periods especially in the black friday,The database is unable to keep up with the front-end connection requests.  
What is the best cost-optimized solution to handle this issue?

* + **Re-design the current architecture using Amazon API gateway with AWS Lambda.**
  + change the instance types to c4.large instances
  + **Decouple the two tiers using Amazon SQS.**
  + Re-design the current architecture using the API using Amazon API Gateway and integrate the new API with the existing backend service.

**Incorrect**

Exam Tip  
MOST efficient + cost-effective = Decouple the two tiers using Amazon SQS.  
Explanation  
Amazon Simple Queue Service (Amazon SQS) offers a secure, durable, and available hosted queue that lets you integrate and decouple distributed software systems and components. Amazon SQS offers common constructs such as dead-letter queues and cost allocation tags. It provides a generic web services API and it can be accessed by any programming language that the AWS SDK supports.  
Reference  
<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html>

1. 15. Question

A trading platform is using AWS Lambda with Amazon RDS database to perform simple data processing, the security team has a lot of concerns about storing passwords in Lambda functions due to compliance requirements.  
What is the most secure method to enable the Lambda function to retrieve the database password?(Choose TWO)

* + **AWS Secrets Manager**
  + **AWS Parameter Store**
  + replace the encrypted password with hashed password
  + **Create IAM roles with Database access permissions and assign it to Lambda function**

**Incorrect**

Exam Tip  
to store database password and access it by lambda you can use both AWS Parameter Store and AWS Secrets Manager  
Explanation  
Secrets Manager helps you organize and manage important configuration data such as credentials, passwords, and license keys. Parameter Store is now integrated with Secrets Manager so that you can retrieve Secrets Manager secrets when using other AWS services that already support references to Parameter Store parameters. These services include Amazon EC2, Amazon Elastic Container Service, AWS Lambda, AWS CloudFormation, AWS CodeBuild, AWS CodeDeploy, and other Systems Manager capabilities. By using Parameter Store to reference Secrets Manager secrets, you create a consistent and secure process for calling and using secrets and reference data in your code and configuration scripts.  
Reference  
<https://docs.aws.amazon.com/systems-manager/latest/userguide/integration-ps-secretsmanager.html>

1. 16. Question

A research company wants to securely share its scientific data stored in Amazon S3 bucket to other company’s AWS accounts.  
As a solution architect, Which S3 feature can achieve this requirement?

* + Lifecycle policy
  + AWS DataSync
  + **Bucket policy**
  + **Bucket Replication**

**Incorrect**

Exam Tip  
  bucket policy is a secure way to share S3 files

Explanation  
A bucket policy is a resource-based AWS Identity and Access Management (IAM) policy. You add a bucket policy to a bucket to grant other AWS accounts or IAM users access permissions for the bucket and the objects in it. Object permissions apply only to the objects that the bucket owner creates.  
Reference  
<https://docs.aws.amazon.com/AmazonS3/latest/user-guide/add-bucket-policy.html>

1. 17. Question

Your company has a multi-tier online book store application deployed on a fleet of EC2 instances behind ELB with Auto Scaling Group ,the back end use Amazon DynamoDB. to minimize access to the web servers you added Amazon CloudFront to serve the static data but still the dynamic requests will go to the web server.  
the company decide to make a weekly promotions every Monday (From 8 AM to 11 AM) which will cause a traffic increasing during.  
What is the cost optimized solution can be done with the web tier to handle this requirement?

* + **Use Schedule reserved EC2 instances**
  + Use Convertible  EC2 instances
  + Add additional caching layer using DAX in front of the database.
  + Replace the Cloud Front with Amazon API Gateway.

**Correct**

Exam Tip  
since the promotion is schedule and we need cost optimized solution = use Scheduled Reserved Instances  
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.  
Reference  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html>

1. 18. Question

You works in digital media company , the company has more than 200 TB of videos are infrequently accessed but when accessed ,it is acceptable to be retrieved within 1 hour.  
Which low-cost AWS Service can handle this requirement?

* + **Amazon S3 Standard Infrequent Access**
  + Amazon Glacier Expedited retrievals
  + Amazon Glacier standard retrievals
  + Amazon Glacier bulk retrievals

**Correct**

Exam Tip  
Infrequent Access +1 hour retrieval = Amazon S3 Standard Infrequent Access  
Explanation  
S3 Standard-IA is for data that is accessed less frequently, but requires rapid access when needed. S3 Standard-IA offers the high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval fee. This combination of low cost and high performance make S3 Standard-IA ideal for long-term storage, backups, and as a data store for disaster recovery files. S3 Storage Classes can be configured at the object level and a single bucket can contain objects stored across S3 Standard, S3 Intelligent-Tiering, S3 Standard-IA, and S3 One Zone-IA. You can also use S3 Lifecycle policies to automatically transition objects between storage classes without any application changes.  
S3 Glacier Archives  
Expedited — Expedited retrievals allow you to quickly access your data when occasional urgent requests for a subset of archives are required. For all but the largest archives (250 MB+), data accessed using Expedited retrievals are typically made available within 1–5 minutes. Provisioned Capacity ensures that retrieval capacity for Expedited retrievals is available when you need it. For more information, see Provisioned Capacity.

Standard — Standard retrievals allow you to access any of your archives within several hours. Standard retrievals typically complete within 3–5 hours. This is the default option for retrieval requests that do not specify the retrieval option.

Bulk — Bulk retrievals are S3 Glacier’s lowest-cost retrieval option, which you can use to retrieve large amounts, even petabytes, of data inexpensively in a day. Bulk retrievals typically complete within 5–12 hours.  
Reference  
<https://aws.amazon.com/s3/storage-classes/>

1. 19. Question

A company has social-web application which attracts a millions of users around the world, the management team needs to generate different types reports from its data warehouse which exceeds 1 TB . the reports varies between fast and long running SQL queries.  
Which lowest cost solution can be used to achieve this requirement?

* + Configure replication between Amazon ElastiCache and Amazon Redshift, for fast reports , run it on Amazon ElastiCache and for long running reports ,run it on Amazon Redshift.
  + Configure replication between Amazon RDS and Amazon Redshift, for fast reports , run it on Amazon RDS and for long running reports ,run it on Amazon Redshift.
  + Use multi Amazon Lambda functions to handle each type of report , the lambda function will use Amazon Redshift to retrieve the data.
  + **Enable Amazon Redshift workload management (WLM) to run both types of reports on Amazon Redshift**

**Unattempted**

Exam Tip  
to run different queries types on big data =Amazon Redshift workload management (WLM)

Explanation  
Amazon Redshift workload management (WLM) enables users to flexibly manage priorities within workloads so that short, fast-running queries won’t get stuck in queues behind long-running queries.  
Amazon Redshift WLM creates query queues at runtime according to service classes, which define the configuration parameters for various types of queues, including internal system queues and user-accessible queues. From a user perspective, a user-accessible service class and a queue are functionally equivalent. For consistency, this documentation uses the term queue to mean a user-accessible service class as well as a runtime queue.  
When you run a query, WLM assigns the query to a queue according to the user’s user group or by matching a query group that is listed in the queue configuration with a query group label that the user sets at runtime.  
Reference  
<https://docs.aws.amazon.com/redshift/latest/dg/c_workload_mngmt_classification.html>

1. 20. Question

You work for a leading leading airline company as an AWS Infrastructure Engineer and you are designing application which store data in chunks with little latency in data retrieval.  
What is the optimum AWS storage can achieve this requirement?

* + **Amazon EBS Throughput Optimized HDD Volumes**
  + Amazon EBS Cold HDD Volumes
  + **Amazon DynamoDB**
  + Amazon EFS

**Incorrect**

Exam Tip  
data in chunks + little latency = NoSQL DB = 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.  
Reference: <https://aws.amazon.com/dynamodb/>

1. 21. Question

A startup company has issue-tracking web application , the web servers and RDS database are hosted on multiple EC2 instances in a single availability zone , the web servers require Internet access to perform periodically OS updates but it have not been given public addresses.  
What is the best solution to provide high availability to this architecture?

* + **Deploy EC2 instances in two Availability Zones and enable Multi-AZ RDS. Deploy NAT gateways in both Availability Zones and put web servers behind ELB Application load balancer.**
  + Deploy EC2 instances in two Availability Zones and enable Multi-AZ RDS. Deploy NAT gateways in both Availability Zones and put database servers behind ELB Application load balancer.
  + **Deploy EC2 instances in two Availability Zones and enable Multi-AZ RDS. Deploy NAT gateways in shared subnet between Availability Zones and put web servers behind ELB Application load balancer.**
  + Deploy EC2 instances in two Availability Zones and enable Multi-AZ RDS. Deploy NAT gateways in shared subnet between Availability Zones and put Database behind ELB Application load balancer.

**Incorrect**

Exam Tip  
high availability + internet accessing without having public IP = multi AZ with NAT gateway in each one , and put ELB in front of web servers.  
Explanation  
Amazon RDS provides high availability and failover support for DB instances using Multi-AZ deployments. Amazon RDS uses several different technologies to provide failover support. Multi-AZ deployments for MariaDB, MySQL, Oracle, and PostgreSQL DB instances use Amazon’s failover technology. SQL Server DB instances use SQL Server Database Mirroring (DBM) or Always On Availability Groups (AGs).  
In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. Running a DB instance with high availability can enhance availability during planned system maintenance, and help protect your databases against DB instance failure and Availability Zone disruption.  
Reference

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html>

1. 22. Question

A Docker critical application consists of 20 micro-services on multiple EC2 instances behind a ELB classic load balancer with auto scaling group. the company decide to make cost reduction without impacting the performance the architecture of the current application.  
What is the best option to handle this requirement?

* + **ELB Application Load Balancer instead of ELB Classic Load Balancer**
  + Recreate the API using Amazon API Gateway and use AWS Lambda as the service backend.
  + Create an Auto Scaling group with a minimum of one instance and a maximum of two instances,
  + **Recreate the API using Amazon API Gateway and integrate the new API with the existing backend service**

**Incorrect**

Exam Tip  
  ELB Application Load Balancer is cheaper than ELB Classic Load Balancer.  
Explanation  
Application Load Balancer : You are charged for each hour or partial hour that an Application Load Balancer is running and the number of Load Balancer Capacity Units (LCU) used per hour.  
Network Load Balancer : You are charged for each hour or partial hour that a Network Load Balancer is running and the number of Load Balancer Capacity Units (LCU) used by Network Load Balancer per hour.  
Classic Load Balancer : You are charged for each hour or partial hour that a Classic Load Balancer is running and for each GB of data transferred through your load balancer.  
Reference  
<https://aws.amazon.com/elasticloadbalancing/pricing/>

1. 23. Question

You are designing a Retail website which will use EBS volumes as primary storage, these EBS volumes are attached to multiple EC2 instances at the same time.  
What is the best solution to backup these EBS volumes in another Region ?

* + Use Lambda function copy data from the current Amazon EBS volumes to the Amazon EBS volume in the other region.
  + **Create point-in-time snapshots of volumes then copy it from the current AWS Region to the other region.**
  + Store the data in Amazon S3 then enable cross-region replication.
  + Enable Cross region replication in the current Amazon EBS volumes

**Correct**

Exam Tip  
to copy Amazon EBS volumes to another/same region = Create snapshots  
Explanation  
With Amazon EBS, you can create point-in-time snapshots of volumes, which we store for you in Amazon S3. After you create a snapshot and it has finished copying to Amazon S3 (when the snapshot status is completed), you can copy it from one AWS Region to another, or within the same Region. Amazon S3 server-side encryption (256-bit AES) protects a snapshot’s data in transit during a copy operation. The snapshot copy receives an ID that is different from the ID of the original snapshot.  
To copy multi-volume snapshots to another AWS Region, retrieve the snapshots using the tag you applied to the multi-volume snapshots group when you created it. Then individually copy the snapshots to another Region.

[A screenshot of a computer

Description automatically generated](https://skillcertpro.com/wp-content/uploads/2020/08/a18.png)

Reference  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-copy-snapshot.html>

1. 24. Question

A scientific magazine has a web application which allows the users around the world to upload their recent researches ,these file are saved into Amazon S3 bucket located in eu-east-1 , during the peak times the users in united states suffer from slow performance in downloading the files and sometimes they are receiving HTTP 500 errors.  
What is the best solution to handle this problem?

* + **Use Amazon CloudFront with all Edge locations to cache and deliver the contents.**
  + Create ELB in front of Amazon S3 bucket to distribute the load .
  + Use EBS instead of Amazon S3 buckets
  + **Enable Amazon S3 cross-region in another region and use an Amazon Route 53 failover routing policy to determine which bucket it should serve the request to.**

**Incorrect**

Exam Tip  
to increase the performance of loading cached data around the world = Use Amazon CloudFront with Edge locations.  
Explanation  
Amazon CloudFront can speed up the delivery of your static content (e.g., images, style sheets, JavaScript, etc.) to viewers across the globe. The Content Delivery Network (CDN) offers a multi-tier cache by default, with regional Edge caches that improve latency and lower the load on your origin servers when the object is not already cached at the Edge. Caching static content gives you the performance and scale you need to give your viewers a fast and reliable experience when visiting your website.

[A diagram of a diagram of a diagram

Description automatically generated with medium confidence](https://skillcertpro.com/wp-content/uploads/2020/08/a19.jpg)

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

1. 25. Question

A telecom company has Amazon RDS in a private subnet , you are designing a new application which will depend on Lambda function to execute queries against the RDS database.  
What is the best solution to allow Lambda function to Access Amazon RDS database?

* + Create Lambda function in the VPC of the RDS database and configure the Network ACL for the private subnet to allow Lambda port.
  + **Create Lambda function in the VPC of the RDS database and enable the inbound rule of Amazon RDS security group to allow Lambda security group.**
  + Create Lambda function in the VPC of the RDS database and enable the outbound rule of Lambda security group to allow Amazon RDS security group.
  + Create Lambda function in the private subnet of the RDS database in another region then create a direct connection between two regions.

**Correct**

Exam Tip  
To allow Lambda function to access Amazon RDS in private subnet  = Create the lambda in same VPC + configure the security group of RDS

[A diagram of a computer security system

Description automatically generated](https://skillcertpro.com/wp-content/uploads/2020/08/a21.png)  
Explanation  
You can configure a function to connect to private subnets in a virtual private cloud (VPC) in your account. Use Amazon Virtual Private Cloud (Amazon VPC) to create a private network for resources such as databases, cache instances, or internal services. Connect your function to the VPC to access private resources during execution.

To connect a function to a VPC  
Open the Lambda console.  
Choose a function.  
Under VPC, choose Edit.  
Choose Custom VPC.  
Choose a VPC, subnets, and security groups.  
Note  
Connect your function to private subnets to access private resources. If your function needs internet access, use NAT. Connecting a function to a public subnet does not give it internet access or a public IP address.  
To connect a function to a VPC  
1. Open the Lambda console.  
2. Choose a function.  
3. Under VPC, choose Edit.  
4. Choose Custom VPC.  
5. Choose a VPC, subnets, and security groups.  
Note  
Connect your function to private subnets to access private resources. If your function needs internet access, use NAT. Connecting a function to a public subnet does not give it internet access or a public IP address.  
6. Choose Save.  
7 .Choose Save.

Creating a Security Group for our AWS Lambda Function  
You can use an existing VPC security group for your Lambda function. However, I recommend to create a separate Security Group in your VPC to separate its security from others. Therefore, we go to VPC dashboard and create a Security Group with no ingress rules because there will be no incoming connection to our Lambda function. We give a name like my-lambda-sg and note its security group name.  
Make sure to select the VPC that your RDS instance were launched into. We will use this security group when we create our Lambda function.

[A screenshot of a computer

Description automatically generated](https://skillcertpro.com/wp-content/uploads/2020/08/a23.png)  
Granting access to Lambda function’s Security Group in RDS instance’s Security Group  
To grant access to RDS instance for the members of our Lambda function’s Security Group; we need to define ingress rules for our RDS instance database port in our RDS instance’s Security Group. Here, be sure that you selected your Lambda function’s security group in the Source field.

[A screenshot of a computer

Description automatically generated](https://skillcertpro.com/wp-content/uploads/2020/08/a22.png)  
Reference  
<https://docs.aws.amazon.com/lambda/latest/dg/services-rds-tutorial.html>  
<https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html>  
<https://blog.shikisoft.com/running-aws-lambda-in-vpc-accessing-rds/>

1. 26. Question

A telecom company is designing a call management application which will be integrated with fully managed, scalable, durable database with flexible schema.  
Which database service should the Solutions Architect use to meet these requirements?

* + **Amazon DynamoDB**
  + Amazon Redshift
  + Amazon S3
  + Amazon Aurora

**Correct**

Exam Tip  
fully managed +  scalable + durable + flexible schema =Amazon 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.  
Reference  
<https://aws.amazon.com/dynamodb/>

1. 27. Question

An e-commerce application is hosted in AWS, the web servers run in a public subnet and RDS database instances run in a private subnet, the operation team needs to provide internet connectivity to the private subnet to receive updates.  
What is the most secure solution to handle this requirement?

* + Launch a NAT gateway in the public subnet and update the public subnet route table.
  + Open the outbound port on the security group of RDS and set to 0.0.0.0/0
  + **Launch a NAT gateway in the public subnet and update the private subnet route table.**
  + Launch a NAT gateway in the private subnet and update the public subnet route table.

**Correct**

Exam Tip  
to enable instances in a private subnet to connect to the internet = Use NAT Gateway  
Explanation  
To create a NAT gateway, you must specify the public subnet in which the NAT gateway should reside. For more information about public and private subnets, see Subnet routing. You must also specify an Elastic IP address to associate with the NAT gateway when you create it. The Elastic IP address cannot be changed after you associate it with the NAT Gateway. After you’ve created a NAT gateway, you must update the route table associated with one or more of your private subnets to point internet-bound traffic to the NAT gateway. This enables instances in your private subnets to communicate with the internet.  
Each NAT gateway is created in a specific Availability Zone and implemented with redundancy in that zone. You have a quota on the number of NAT gateways you can create in an Availability Zone.  
If you no longer need a NAT gateway, you can delete it. Deleting a NAT gateway disassociates its Elastic IP address, but does not release the address from your account.  
The following diagram illustrates the architecture of a VPC with a NAT gateway. The main route table sends internet traffic from the instances in the private subnet to the NAT gateway. The NAT gateway sends the traffic to the internet gateway using the NAT gateway’s Elastic IP address as the source IP address.

[A diagram of a route

Description automatically generated](https://skillcertpro.com/wp-content/uploads/2020/08/a24.png)  
Reference  
<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>

1. 28. Question

You are designing a Docker based web application for e-commerce company, you need to scale some modules of the web application independently to support path-based routing while maintaining a single Fully Qualified Domain Name.  
Which AWS services are suitable for this application? (Select TWO.)

* + **Amazon ELB Application Load Balancer**
  + Amazon ELB Classic Load Balancer
  + **Amazon ECS**
  + Amazon MQ
  + Amazon RDS

**Incorrect**

Exam Tip  
  Docker “Multi-Container” + Scaling +  path-based routing = Amazon ECS + Amazon ELB Application Load Balancer  
Explanation  
Your Amazon ECS service can optionally be configured to use Elastic Load Balancing to distribute traffic evenly across the tasks in your service.  
Amazon ECS services support the Application Load Balancer, Network Load Balancer, and Classic Load Balancer load balancer types. Application Load Balancers are used to route HTTP/HTTPS (or Layer 7) traffic. Network Load Balancers and Classic Load Balancers are used to route TCP (or Layer 4) traffic.  
Application Load Balancers offer several features that make them attractive for use with Amazon ECS services:  
  – Each service can serve traffic from multiple load balancers and expose multiple load balanced ports by specifying multiple target groups.  
  – They are supported by tasks using both the Fargate and EC2 launch types.  
  – Application Load Balancers allow containers to use dynamic host port mapping (so that multiple tasks from the same service are allowed per container instance).  
  – Application Load Balancers support path-based routing and priority rules (so that multiple services can use the same listener port on a single Application Load Balancer).  
We recommend that you use Application Load Balancers for your Amazon ECS services so that you can take advantage of these latest features, unless your service requires a feature that is only available with Network Load Balancers or Classic Load Balancers. For more information about Elastic Load Balancing and the differences between the load balancer types

Reference  
<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/service-load-balancing.html>

1. 29. Question

A travel company has image viewer web application which contains millions of images. both the web site and the images are hosted within an Amazon S3 bucket to serve users globally.  
What is the best option can be done to minimize the cost of data transfer?

* + **Create an Amazon CloudFront distribution with S3 bucket as the origin server**
  + Enable Amazon S3 cross region replicaton.
  + Use Amazon EBS to host the images with keeping the web site hosted in Amazon S3 bucket
  + Create an Amazon API Gateway distribution, with the S3 bucket as the origin server

**Correct**

Exam Tip  
   store + scale + secure + low cost = Amazon S3 + Amazon Cloud Front

Explanation  
If you have a website, application, or another web resource, you probably have static content. Static content includes files like images, videos, or music, or even scripts like .css or js. In the pre-cloud era, you would put those files on a standard server, and then serve them on the internet to all of your viewers, across the globe, from one specific geo location. But with cloud services, there’s a solution that provides faster delivery and better scalability. In this blog post, you’ll learn how to use Amazon Simple Storage Service (S3) and Amazon CloudFront to store, secure, and deliver your static content at scale. And to help you get started with just a few clicks, we’ve included a CloudFormation template that can quickly provision these services for you.  
Reference  
<https://aws.amazon.com/blogs/networking-and-content-delivery/amazon-s3-amazon-cloudfront-a-match-made-in-the-cloud/>

1. 30. Question

A trading company has a back end API service to serve multiple clients, this service is running on multiple EC2 instances behind Application Load Balancer. most of the client requests finish very quickly but some requests takes a longer time to complete which causes client timeouts and increasing overall system latency.  
How can this issue be corrected?

* + Use Compute optimized EC2 instances i.e  c5.12xlarge
  + **Write the long running requests on Amazon SQS to be processed asynchronous**
  + Use Caching layer to handle the long running requests
  + Add more EC2 instances to distribute the workload.

**Correct**

Exam Tip  
for long running requests = Use Amazon SQS

Explanation  
Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message oriented middleware, and empowers developers to focus on differentiating work. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available. Get started with SQS in minutes using the AWS console, Command Line Interface or SDK of your choice, and three simple commands.  
Reference  
<https://aws.amazon.com/sqs/>

1. 31. Question

You are working as Solutions Architect in popular software company , one of the clients asked you to recommend the simplest way to administrate VPCs with all needed security aspects?  
What is your recommendation?

* + Create AWS Elastic Beanstalk and define all needed VPC resources
  + Manually create all needed VPC components and resources.
  + Create a user script to deploy the VPC
  + **Create AWS CloudFormation template and define all needed VPC resources**

**Correct**

Exam Tip  
keyword “administrate VPCs” = Use AWS CloudFormation  
Explanation  
AWS CloudFormation simplifies provisioning and management on AWS. You can create templates for the service or application architectures you want and have AWS CloudFormation use those templates for quick and reliable provisioning of the services or applications (called “stacks”). You can also easily update or replicate the stacks as needed.  
This collection of sample templates will help you get started with AWS CloudFormation and quickly build your own templates  
Reference  
<https://aws.amazon.com/cloudformation/resources/templates/>

1. 32. Question

A travel photo sharing website is deployed on a multiple EC2 instances with auto scaling group behind application load balancer in a multiple Availability zone. the operation team noticed that every night , the EC2 instances are scaling out due to the high traffic from specific region to request some static content stored in EC2 instances.  
What is the best solution to resolve this issue?

* + Store the contents on Amazon EFS instead of the EC2 root volume.
  + Change the Auto Scaling group's scale out event to scale based on network utilization.
  + **Create an Amazon CloudFront distribution for the site and redirect traffic it.**
  + **Create an Auto Scaling scheduled action to scale IN the necessary resources at every morning.**

**Incorrect**

Exam Tip  
for better performance = Use CloudFront with EC2 as origin.  
Explanation  
Amazon CloudFront works seamlessly with Amazon EC2 to accelerate the delivery of your dynamic content. In addition, if you use AWS origins such as Amazon S3, Amazon EC2 or Elastic Load Balancing, you don’t pay for any data transferred between these services and CloudFront.  
Reference  
<https://aws.amazon.com/cloudfront/getting-started/EC2/>

1. 33. Question

A Global news agency has an application deployed on multiple EC2 instances in a private subnet within a VPC. this application uses Amazon SNS for sending news to users .  
What is the MOST secure way to allow the application to access service endpoints in the same region?

* + **Use AWS PrivateLink.**
  + Use an egress-only Internet Gateway.
  + **Use a NAT gateway.**
  + Use a NAT instance

**Incorrect**

Exam Tip  
keyword “allow the application to access service endpoints in the same region” =  Use AWS PrivateLink.  
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.

[A diagram of a diagram

Description automatically generated](https://skillcertpro.com/wp-content/uploads/2020/08/a13-1.png)

AWS PrivateLink enables you to securely connect your VPCs to supported AWS services: to your own services on AWS, to services hosted by other AWS accounts, and to third-party services on AWS Marketplace. Since traffic between your VPC and any one of these services does not leave the Amazon network, an Internet gateway, NAT device, public IP address, or VPN connection is no longer needed to communicate with the service.

To use AWS PrivateLink, create an interface VPC endpoint for a service in your VPC. This creates an Elastic Network Interface (ENI) in your subnet with a private IP address that serves as an entry point for traffic destined to the service. Service endpoints available over AWS PrivateLink will appear as ENIs with private IPs in your VPCs.

Reference  
<https://aws.amazon.com/privatelink/>

1. 34. Question

Your company has a critical application which runs in the VPC on an Amazon EC2 instances and use Amazon S3 for storage. while PCI auditing, the security team found that some traffic is going through the internet.  
Which enhancement can be applied in the VPC before updating the route table to resolve this security issue?

* + **Create a VPC endpoint for Amazon S3 access**
  + Create a NAT gateway for Amazon EC2 access
  + Create a VPC endpoint for Amazon EC2 access
  + Create a NAT gateway for Amazon S3 access

**Correct**

Exam Tip  
the idea being that you will modify the route table to remove internet access. Thus the S3 VPC endpoint is needed.  
Explanation  
A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.  
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.

Gateway endpoints  
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

Interface endpoints (powered by AWS PrivateLink)  
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.

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

1. 35. Question

You are designing a application which needs to connect to Amazon RDS PostgreSQL.  
Which port can be used?

* + 443
  + **5432**
  + 3306
  + 1521

**Correct**

Exam Tip  
the default PostgreSQL port is 5432.  
Reference  
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ConnectToPostgreSQLInstance.html>

1. 36. Question

Which management interface can be used to create, manage, and delete Amazon Redshift clusters via list of commands?

* + **The Amazon Redshift API**
  + AWS Terraform
  + AWS SDKs
  + **AWS CLI**

**Incorrect**

Exam Tip  
to manage Amazon Redshift cluster via commands = Use AWS CLI  
Explanation  
Amazon Redshift supports several management interfaces that you can use to create, manage, and delete Amazon Redshift clusters: the AWS SDKs, the AWS Command Line Interface (AWS CLI), and the Amazon Redshift management API.  
The Amazon Redshift API – You can call this Amazon Redshift management API by submitting a request. Requests are HTTP or HTTPS requests that use the HTTP verbs GET or POST with a parameter named Action. Calling the Amazon Redshift API is the most direct way to access the Amazon Redshift service. However, it requires that your application handle low-level details such as error handling and generating a hash to sign the request.  
AWS SDKs – You can use the AWS SDKs to perform Amazon Redshift cluster-related operations. Several of the SDK libraries wrap the underlying Amazon Redshift API. They integrate the API functionality into the specific programming language and handle many of the low-level details, such as calculating signatures, handling request retries, and error handling. Calling the wrapper functions in the SDK libraries can greatly simplify the process of writing an application to manage an Amazon Redshift cluster.  
AWS CLI – The CLI provides a set of command line tools that you can use to manage AWS services from Windows, Mac, and Linux computers. The AWS CLI includes commands based on the Amazon Redshift API actions.  
Reference  
<https://docs.aws.amazon.com/redshift/latest/mgmt/using-aws-sdk.html>

1. 37. Question

A social media website runs on Amazon EC2 instances in a single Availability zone using Amazon S3 for storage.  
What should the Architect do in the current architecture to optimize transfer costs?

* + **Use Amazon CloudFront distribution with Amazon S3 as the origin**
  + Enable S3 cross region replication.
  + Use Lambda@Edge
  + **Deploy the web site in another region near to the customers.**

**Incorrect**

Exam Tip  
– to enhance the transfer performance with Amazon S3 = Use CloudFront.  
– single availability zone means single region so we can not use Lambda@Edge in this case.  
Explanation  
if you want higher transfer rates over a single HTTP connection or single-digit millisecond latencies, use Amazon CloudFront or Amazon ElastiCache for caching with Amazon S3.  
Reference  
<https://docs.aws.amazon.com/AmazonS3/latest/dev/optimizing-performance.html>

1. 38. Question

You need to share some video files that are stored in a private S3 bucket for a short period of time with your friends using Amazon CloudFront?  
What is the best solution to handle this requirement?

* + Use EBS volumes instead of Amazon S3
  + **Use CloudFront Signed Cookies.**
  + **Use CloudFront Signed URL.**
  + Use IAM policies.
  + Using Bucket Policy.

**Incorrect**

Exam Tip  
– Use CloudFront Signed Cookies restrict access to multiple files.  
– Use CloudFront Signed URL restrict access to a Single file.  
Explanation  
CloudFront signed cookies allow you to control who can access your content when you don’t want to change your current URLs or when you want to provide access to multiple restricted files, for example, all of the files in the subscribers’ area of a website. This topic explains the considerations when using signed cookies and describes how to set signed cookies using canned and custom policies.  
Reference  
<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-cookies.html>

1. 39. Question

A Solutions Architect is designing a mobile gaming application. it is expected to be very popular. the application will use Amazon DynamoDB table to store the data. the operation team asked you to ensure that you must take daily backup for the database and each backup must be kept for one year.  
What is the best solution to handle this requirement without affecting the application performance?

* + Configure DynamoDB replication to be daily basis
  + Create a scheduled job to back up the DynamoDB table daily.
  + **Create Lambda function to export data from DynamoDB and store in Amazon S3.**
  + **Create Lambda function to trigger On-demand backup based on Amazon CloudWatch Events.**

**Incorrect**

Exam Tip  
  backup DynamoDB  + without affecting the application performance= Use On-demand backup  
Explanation  
On-demand backup allows you to create full backups of your Amazon DynamoDB table for data archiving, helping you meet your corporate and governmental regulatory requirements. You can back up tables from a few megabytes to hundreds of terabytes of data, with no impact on performance and availability to your production applications. Backups process in seconds regardless of the size of your tables, so you do not have to worry about backup schedules or long-running processes. In addition, all backups are automatically encrypted, cataloged, easily discoverable, and retained until explicitly deleted.  
Point-in-time recovery (PITR) provides continuous backups of your DynamoDB table data. When enabled, DynamoDB maintains incremental backups of your table for the last 35 days until you explicitly turn it off.  
Reference  
<https://aws.amazon.com/dynamodb/backup-restore/>

1. 40. Question

A multimedia company has a application running on Amazon EC2 which creates water marked images of millions of images stored in Amazon S3 then store the locations of the new images in Amazon DynamoDB table, and water marked images are easily re-created from the originals if they are accidentally deleted.  
Which cost-optimized storage can be used to store water marked images with taking into consideration the immediate retrieval?

* + Amazon EBS
  + **Amazon S3**
  + Amazon Glacier
  + S3 Standard-IA with cross-region replication

**Correct**

Exam Tip  
–  Immediate Retrieval + Cost optimized =Amazon S3  
–  No Cross region replication for S3 Standard-IA  
Explanation  
Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Amazon S3 provides easy-to-use management features so you can organize your data and configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements. Amazon S3 is designed for 99.999999999% (11 9’s) of durability, and stores data for millions of applications for companies all around the world.  
Reference  
<https://aws.amazon.com/s3/>

1. 41. Question

A fleet of Amazon EC2 instances running Linux will be launched in an Amazon VPC. An application development framework and some custom software must be installed on the instances. The installation will be initiated using some scripts. What feature enables a Solutions Architect to specify the scripts the software can be installed during the EC2 instance launch?

* + AWS Config
  + Metadata
  + **User data**
  + Run command

**Correct**

When you launch an instance in Amazon EC2, you have the option of passing user data to the instance that can be used to perform common automated configuration tasks and even run scripts after the instance starts. You can pass two types of user data to Amazon EC2: shell scripts and cloud-init directives  
User data is data that is supplied by the user at instance launch in the form of a script and is limited to 16KB.  
CORRECT: “User Data” is the correct answer.  
INCORRECT: “Metadata” is incorrect. Instance metadata is data about your instance that you can use to configure or manage the running instance. Instance metadata is divided into categories, for example, host name, events, and security groups.  
INCORRECT: “Run Command” is incorrect. The AWS Systems Manager run command is used to manage the configuration of existing instances by using remotely executed commands. User data is better for specifying scripts to run at startup.  
INCORRECT: “AWS Config” is incorrect. This service is used to manage the configuration of AWS resources, it does not run scripts on instances.  
References:  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/user-data.html>

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

1. 42. Question

Several Amazon EC2 Spot instances are being used to process messages from an Amazon SQS queue and store results in an Amazon DynamoDB table. Shortly after picking up a message from the queue AWS terminated the Spot instance. The Spot instance had not finished processing the message. What will happen to the message?

* + The message will remain in the queue and be immediately picked up by another instance
  + **The message will become available for processing again after the visibility timeout expires**
  + The message will be lost as it would have been deleted from the queue when processed
  + The results may be duplicated in DynamoDB as the message will likely be processed multiple times

**Correct**

The visibility timeout is the amount of time a message is invisible in the queue after a reader picks up the message. If a job is processed within the visibility timeout the message will be deleted. If a job is not processed within the visibility timeout the message will become visible again (could be delivered twice). The maximum visibility timeout for an Amazon SQS message is 12 hours.

[A screenshot of a computer

Description automatically generated](https://skillcertpro.com/wp-content/uploads/2020/08/b35-1.png)  
CORRECT: “The message will become available for processing again after the visibility timeout expires” is the correct answer.  
INCORRECT: “The message will be lost as it would have been deleted from the queue when processed” is incorrect. The message will not be lost and will not be immediately picked up by another instance.  
INCORRECT: “The message will remain in the queue and be immediately picked up by another instance” is incorrect. As mentioned above it will be available for processing in the queue again after the timeout expires.  
INCORRECT: “The results may be duplicated in DynamoDB as the message will likely be processed multiple times” is incorrect. As the instance had not finished processing the message it should only be fully processed once. Depending on your application process however it is possible some data was written to DynamoDB.  
References:  
<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html>

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

1. 43. Question

A company has launched a multi-tier application architecture. The web tier and database tier run on Amazon EC2 instances in private subnets within the same Availability Zone.  
Which combination of steps should a Solutions Architect take to add high availability to this architecture? (Select TWO.)

* + **Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer (ALB)**
  + **Create new private subnets in the same VPC but in a different 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 subnets in the same AZ for high availability and move the web tier to the public subnets
  + Create new private subnets in the same VPC but in a different AZ. Create a database using Amazon EC2 in one AZ

**Incorrect**

The Solutions Architect can use Auto Scaling group across multiple AZs with an ALB in front to create an elastic and highly available architecture. Then, migrate the database to an Amazon RDS multi-AZ deployment to create HA for the database tier. This results in a fully redundant architecture that can withstand the failure of an availability zone.  
CORRECT: “Create an Amazon EC2 Auto Scaling group and Application Load Balancer (ALB) spanning multiple AZs” is a correct answer.  
CORRECT: “Create new private subnets in the same VPC but in a different AZ. Migrate the database to an Amazon RDS multi-AZ deployment” is also a correct answer.  
INCORRECT: “Create new public subnets in the same AZ for high availability and move the web tier to the public subnets” is incorrect. If subnets share the same AZ they are not suitable for splitting your tier across them for HA as the failure of a an AZ will take out both subnets.  
INCORRECT: “Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer (ALB)” is incorrect. The instances are in a single AZ so the Solutions Architect should create a new auto scaling group and launch instances across multiple AZs.  
INCORRECT: “Create new private subnets in the same VPC but in a different AZ. Create a database using Amazon EC2 in one AZ” is incorrect. A database in a single AZ will not be highly available.  
References:  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-increase-availability.html>  
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html>

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

1. 44. Question

A company has multiple Amazon VPCs that are peered with each other. The company would like to use a single Elastic Load Balancer (ELB) to route traffic to multiple EC2 instances in peered VPCs within the same region. How can this be achieved?

* + This is possible using the Classic Load Balancer (CLB) if using Instance IDs
  + **This is possible using the Network Load Balancer (NLB) and Application Load Balancer (ALB) if using IP addresses as targets**
  + **This is not possible, the instances that an ELB routes traffic to must be in the same VPC**
  + This is not possible with ELB, you would need to use Route 53

**Incorrect**

With ALB and NLB IP addresses can be used to register:  
– Instances in a peered VPC.  
– AWS resources that are addressable by IP address and port.  
– On-premises resources linked to AWS through Direct Connect or a VPN connection.  
CORRECT: “This is possible using the Network Load Balancer (NLB) and Application Load Balancer (ALB) if using IP addresses as targets” is the correct answer.  
INCORRECT: “This is not possible, the instances that an ELB routes traffic to must be in the same VPC” is incorrect. Instances can be in peered VPCs.  
INCORRECT: “This is possible using the Classic Load Balancer (CLB) if using Instance IDs” is incorrect. This is not possible with the CLB.  
INCORRECT: “This is not possible with ELB, you would need to use Route 53” is incorrect. This is not true, as detailed above.  
References:  
<https://aws.amazon.com/blogs/aws/new-application-load-balancing-via-ip-address-to-aws-on-premises-resources/>

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

1. 45. Question

An Auto Scaling group of Amazon EC2 instances behind an Elastic Load Balancer (ELB) is running in an Amazon VPC. Health checks are configured on the ASG to use EC2 status checks. The ELB has determined that an EC2 instance is unhealthy and has removed it from service. A Solutions Architect noticed that the instance is still running and has not been terminated by EC2 Auto Scaling.  
What would be an explanation for this behavior?

* + Connection draining is enabled and the ASG is waiting for in-flight requests to complete
  + The health check grace period has not yet expired
  + The ASG is waiting for the cooldown timer to expire before terminating the instance
  + **The ELB health check type has not been selected for the ASG and so it is unaware that the instance has been determined to be unhealthy by the ELB and has been removed from service**

**Correct**

If using an ELB it is best to enable ELB health checks as otherwise EC2 status checks may show an instance as being healthy that the ELB has determined is unhealthy. In this case the instance will be removed from service by the ELB but will not be terminated by Auto Scaling  
More information on ASG health checks:  
– By default uses EC2 status checks.  
– Can also use ELB health checks and custom health checks.  
– ELB health checks are in addition to the EC2 status checks.  
– If any health check returns an unhealthy status the instance will be terminated.  
– With ELB an instance is marked as unhealthy if ELB reports it as OutOfService  
– A healthy instance enters the InService state.  
– If an instance is marked as unhealthy it will be scheduled for replacement.  
– If connection draining is enabled, Auto Scaling waits for in-flight requests to complete or timeout before terminating instances.  
– The health check grace period allows a period of time for a new instance to warm up before performing a health check (300 seconds by default).  
CORRECT: “The ELB health check type has not been selected for the ASG and so it is unaware that the instance has been determined to be unhealthy by the ELB and has been removed from service” is the correct answer.  
INCORRECT: “The ASG is waiting for the cooldown timer to expire before terminating the instance” is incorrect as the ASG does not wait for the cooldown time to expire.  
INCORRECT: “Connection draining is enabled and the ASG is waiting for in-flight requests to complete” is incorrect. Connection draining is not the correct answer as the ELB has taken the instance out of service so there are no active connections.  
INCORRECT: “The health check grace period has not yet expired” is incorrect. The health check grace period allows a period of time for a new instance to warm up before performing a health check.  
References:  
<https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroupLifecycle.html>

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

1. 46. Question

A large multi-national client has requested a design for a multi-region database. The master database will be in the EU (Frankfurt) region and databases will be located in 4 other regions to service local read traffic. The database should be a managed service including the replication.  
The solution should be cost-effective and secure. Which AWS service can deliver these requirements?

* + **RDS with cross-region Read Replicas**
  + ElastiCache with Redis and clustering mode enabled
  + **RDS with Multi-AZ**
  + EC2 instances with EBS replication

**Incorrect**

Amazon RDS Read replicas are used for read heavy DBs and replication is asynchronous. Read replicas are for workload sharing and offloading. Read replicas can be in another region (uses asynchronous replication). This solution will enable better performance for users in the other AWS regions for database queries and is a managed service.  
CORRECT: “RDS with cross-region Read Replicas” is the correct answer.  
INCORRECT: “RDS with Multi-AZ” is incorrect. RDS with Multi-AZ is within a region only  
INCORRECT: “EC2 instances with EBS replication” is incorrect. EC2 instances with EBS replication is not a suitable solution.  
INCORRECT: “ElastiCache with Redis and clustering mode enabled” is incorrect. ElastiCache is an in-memory key/value store database (more OLAP than OLTP) and is not suitable for this scenario. Clustering mod is only available within the same region.  
References:  
<https://aws.amazon.com/blogs/aws/cross-region-read-replicas-for-amazon-rds-for-mysql/>

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

1. 47. Question

An on-premise data center will be connected to an Amazon VPC by a hardware VPN that has public and VPN-only subnets. The security team has requested that traffic hitting public subnets on AWS that’s destined to on-premise applications must be directed over the VPN to the corporate firewall.  
How can this be achieved?

* + **In the public subnet route table, add a route for your remote network and specify the virtual private gateway as the target**
  + Configure a NAT Gateway and configure all traffic to be directed via the virtual private gateway
  + In the public subnet route table, add a route for your remote network and specify the customer gateway as the target
  + **In the VPN-only subnet route table, add a route that directs all Internet traffic to the virtual private gateway**

**Incorrect**

Route tables determine where network traffic is directed. In your route table, you must add a route for your remote network and specify the virtual private gateway as the target. This enables traffic from your VPC that’s destined for your remote network to route via the virtual private gateway and over one of the VPN tunnels. You can enable route propagation for your route table to automatically propagate your network routes to the table for you.  
CORRECT: “In the public subnet route table, add a route for your remote network and specify the virtual private gateway as the target” is the correct answer.  
INCORRECT: “In the VPN-only subnet route table, add a route that directs all Internet traffic to the virtual private gateway” is incorrect. You must create the route table rule in the route table attached to the public subnet, not the VPN-only subnet.  
INCORRECT: “In the public subnet route table, add a route for your remote network and specify the customer gateway as the target” is incorrect. You must select the virtual private gateway (AWS side of the VPN) not the customer gateway (customer side of the VPN) in the target in the route table.  
INCORRECT: “Configure a NAT Gateway and configure all traffic to be directed via the virtual private gateway” is incorrect. NAT Gateways are used to enable Internet access for EC2 instances in private subnets, they cannot be used to direct traffic to VPG.  
References:  
<https://docs.aws.amazon.com/vpc/latest/userguide/VPC_VPN.html>  
<https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario3.html>

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

1. 48. Question

A Solutions Architect has created a new security group in an Amazon VPC. No rules have been created. Which of the statements below are correct regarding the default state of the security group? (choose 2)

* + There is an inbound rule allowing traffic from the Internet to port 22 for management
  + **There are no inbound rules and traffic will be implicitly denied**
  + There is an outbound rule allowing traffic to the Internet Gateway
  + There are is an inbound rule that allows traffic from the Internet Gateway
  + **There is an outbound rule that allows all traffic to all IP addresses**

**Incorrect**

Custom security groups do not have inbound allow rules (all inbound traffic is denied by default) whereas default security groups do have inbound allow rules (allowing traffic from within the group). All outbound traffic is allowed by default in both custom and default security groups.  
Security groups act like a stateful firewall at the instance level. Specifically security groups operate at the network interface level of an EC2 instance. You can only assign permit rules in a security group, you cannot assign deny rules and there is an implicit deny rule at the end of the security group. All rules are evaluated until a permit is encountered or continues until the implicit deny. You can create ingress and egress rules.  
CORRECT: “There is an outbound rule that allows all traffic to all IP addresses” is the correct answer.  
CORRECT: “There are no inbound rules and traffic will be implicitly denied” is the correct answer.  
INCORRECT: “There is an inbound rule allowing traffic from the Internet to port 22 for management” is incorrect. This is not true.  
INCORRECT: “There are is an inbound rule that allows traffic from the Internet Gateway” is incorrect. There are no inbound allow rules by default.  
INCORRECT: “There is an outbound rule allowing traffic to the Internet Gateway” is incorrect. There is an outbound allow rule but it allows traffic to anywhere, it does not specify the internet gateway.  
References:  
<https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html>

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

1. 49. Question

A Solutions Architect created a new IAM user account for a temporary employee who recently joined the company. The user does not have permissions to perform any actions, which statement is true about newly created users in IAM?

* + They are created with user privileges
  + They are created with full permissions
  + They are created with limited permissions
  + **They are created with no permissions**

**Correct**

Every IAM user starts with no permissions.. In other words, by default, users can do nothing, not even view their own access keys. To give a user permission to do something, you can add the permission to the user (that is, attach a policy to the user). Or you can add the user to a group that has the intended permission.  
CORRECT: “They are created with no permissions” is the correct answer.  
INCORRECT: “They are created with limited permissions” is incorrect as they are created with no permissions.  
INCORRECT: “They are created with full permissions” is incorrect as they are created with no permissions.  
INCORRECT: “They are created with user privileges” is incorrect as they are created with no permissions.  
References:  
<https://docs.aws.amazon.com/IAM/latest/UserGuide/access_controlling.html>

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

1. 50. Question

A financial services company regularly runs an analysis of the day’s transaction costs, execution reporting, and market performance. The company currently uses third-party commercial software for provisioning, managing, monitoring, and scaling the computing jobs which utilize a large fleet of EC2 instances.  
The company is seeking to reduce costs and utilize AWS services. Which AWS service could be used in place of the third-party software?

* + Amazon Lex
  + **AWS Batch**
  + AWS Systems Manager
  + **Amazon Athena**

**Incorrect**

AWS Batch eliminates the need to operate third-party commercial or open source batch processing solutions. There is no batch software or servers to install or manage. AWS Batch manages all the infrastructure for you, avoiding the complexities of provisioning, managing, monitoring, and scaling your batch computing jobs.  
CORRECT: “AWS Batch” is the correct answer.  
INCORRECT: “Amazon Athena” is incorrect. Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL.  
INCORRECT: “AWS Systems Manager” is incorrect. AWS Systems Manager gives you visibility and control of your infrastructure on AWS.  
INCORRECT: “Amazon Lex” is incorrect. Amazon Lex is a service for building conversational interfaces into any application using voice and text.  
References:  
<https://aws.amazon.com/batch/>

1. 51. Question

A Solutions Architect is creating a design for a two-tier application with a MySQL RDS back-end. The performance requirements of the database tier are hard to quantify until the application is running and the Architect is concerned about right-sizing the database.  
What methods of scaling are possible after the MySQL RDS database is deployed? (choose 2)

* + Horizontal scaling for write capacity by enabling Multi-AZ
  + Vertical scaling for read and write by using Transfer Acceleration
  + **Vertical scaling for read and write by choosing a larger instance size**
  + **Horizontal scaling for read and write by enabling Multi-Master RDS DB**
  + **Horizontal scaling for read capacity by creating a read-replica**

**Incorrect**

To handle a higher load in your database, you can vertically scale up your master database with a simple push of a button. In addition to scaling your master database vertically, you can also improve the performance of a read-heavy database by using read replicas to horizontally scale your database.  
CORRECT: “Vertical scaling for read and write by choosing a larger instance size” is a correct answer.  
CORRECT: “Horizontal scaling for read capacity by creating a read-replica” is also a correct answer.  
INCORRECT: “Horizontal scaling for write capacity by enabling Multi-AZ” is incorrect. You cannot scale write capacity by enabling Multi-AZ as only one DB is active and can be written to.  
INCORRECT: “Vertical scaling for read and write by using Transfer Acceleration” is incorrect. Transfer Acceleration is a feature of S3 for fast uploads of objects.  
INCORRECT: “Horizontal scaling for read and write by enabling Multi-Master RDS DB” is incorrect. There is no such thing as a Multi-Master MySQL RDS DB (there is for Aurora).  
References:  
<https://aws.amazon.com/blogs/database/scaling-your-amazon-rds-instance-vertically-and-horizontally/>

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

1. 52. Question

The database layer of an on-premises web application is being migrated to AWS. The database uses a multi-threaded, in-memory caching layer to improve performance for repeated queries. Which service would be the most suitable replacement for the database cache?

* + **Amazon ElastiCache Memcached**
  + Amazon RDS MySQL
  + **Amazon DynamoDB DAX**
  + Amazon ElastiCache Redis

**Incorrect**

Amazon ElastiCache with the Memcached engine is an in-memory database that can be used as a database caching layer. The memached engine supports multiple cores and threads and large nodes.

[A black and white table with white text

Description automatically generated](https://skillcertpro.com/wp-content/uploads/2020/08/b21-1.png)  
CORRECT: “Amazon ElastiCache Memcached” is the correct answer.  
INCORRECT: “Amazon ElastiCache Redis” is incorrect. The Redis engine does not support multiple CPU cores or threads.  
INCORRECT: “Amazon DynamoDB DAX” is incorrect. Amazon DynamoDB Accelerator (DAX) is a database cache that should be used with DynamoDB only.  
INCORRECT: “Amazon RDS MySQL” is incorrect as this is not an example of an in-memory database that can be used as a database caching layer.  
References:  
<https://aws.amazon.com/elasticache/redis-vs-memcached/>

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

1. 53. Question

An application running a private subnet of an Amazon VPC must have outbound internet access for downloading updates. The Solutions Architect does not want the application exposed to inbound connection attempts. Which steps should be taken?

* + **Create a NAT gateway and attach an internet gateway to the VPC**
  + Attach an internet gateway to the private subnet and create a NAT gateway
  + Create a NAT gateway but do not create attach an internet gateway to the VPC
  + **Attach an internet gateway to the VPC but do not create a NAT gateway**

**Incorrect**

To enable outbound connectivity for instances in private subnets a NAT gateway can be created. The NAT gateway is created in a public subnet and a route must be created in the private subnet pointing to the NAT gateway for internet-bound traffic. An internet gateway must be attached to the VPC to facilitate outbound connections.

[A screenshot of a computer

Description automatically generated](https://skillcertpro.com/wp-content/uploads/2020/08/b22-1.png)  
You cannot directly connect to an instance in a private subnet from the internet. You would need to use a bastion/jump host. Therefore, the application will not be exposed to inbound connection attempts.  
CORRECT: “Create a NAT gateway and attach an internet gateway to the VPC” is the correct answer.  
INCORRECT: “Create a NAT gateway but do not create attach an internet gateway to the VPC” is incorrect. An internet gateway must be attached to the VPC for any outbound connections to work.  
INCORRECT: “Attach an internet gateway to the private subnet and create a NAT gateway” is incorrect. You do not attach internet gateways to subnets, you attach them to VPCs.  
INCORRECT: “Attach an internet gateway to the VPC but do not create a NAT gateway” is incorrect. Without a NAT gateway the instances in the private subnet will not be able to download updates from the internet.  
References:  
<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>

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

1. 54. Question

The AWS Acceptable Use Policy describes permitted and prohibited behavior on AWS and includes descriptions of prohibited security violations and network abuse. According to the policy, what is AWS’s position on penetration testing?

* + AWS do not allow any form of penetration testing
  + AWS allow penetration testing by customers on their own VPC resources
  + **AWS allow penetration for some resources without prior authorization**
  + AWS allow penetration testing for all resources

**Correct**

AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for 8 services. Please check the AWS link below for the latest information.  
CORRECT: “AWS allow penetration for some resources without prior authorization” is the correct answer.  
INCORRECT: “AWS do not allow any form of penetration testing” is incorrect as explained above.  
INCORRECT: “AWS allow penetration testing by customers on their own VPC resources” is incorrect as explained above.  
INCORRECT: “AWS allow penetration testing for all resources” is incorrect as explained above.  
References:  
<https://aws.amazon.com/security/penetration-testing/>

Topic: aws-certified-cloud-practitioner/cloud-security/

1. 55. Question

A Solutions Architect is designing the compute layer of a serverless application. The compute layer will manage requests from external systems, orchestrate serverless workflows, and execute the business logic.  
The Architect needs to select the most appropriate AWS services for these functions. Which services should be used for the compute layer? (choose 2)

* + **Use AWS Step Functions for orchestrating serverless workflows**
  + Use AWS Elastic Beanstalk for executing the business logic
  + Use Amazon ECS for executing the business logic
  + **Use AWS CloudFormation for orchestrating serverless workflows**
  + **Use Amazon API Gateway with AWS Lambda for executing the business logic**

**Incorrect**

With Amazon API Gateway, you can run a fully managed REST API that integrates with Lambda to execute your business logic and includes traffic management, authorization and access control, monitoring, and API versioning.  
AWS Step Functions orchestrates serverless workflows including coordination, state, and function chaining as well as combining long-running executions not supported within Lambda execution limits by breaking into multiple steps or by calling workers running on Amazon Elastic Compute Cloud (Amazon EC2) instances or on-premises.  
CORRECT: “Use AWS Step Functions for orchestrating serverless workflows” is the correct answer.  
CORRECT: “Use Amazon API Gateway with AWS Lambda for executing the business logics” is the correct answer.  
INCORRECT: “Use Amazon ECS for executing the business logic” is incorrect. The Amazon Elastic Container Service (ECS) is not a serverless application stack, containers run on EC2 instances.  
INCORRECT: “Use AWS CloudFormation for orchestrating serverless workflows” is incorrect. AWS CloudFormation is used for describing and provisioning resources not actually performing workflow functions within the application.  
INCORRECT: “Use AWS Elastic Beanstalk for executing the business logic” is incorrect. AWS Elastic Beanstalk is used for describing and provisioning resources not actually performing workflow functions within the application.  
References:  
<https://aws.amazon.com/step-functions/>

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

1. 56. Question

A company runs an application on-premises that must consume a REST API running on Amazon API Gateway. The company has an AWS Direct Connect connection to their Amazon VPC. The solutions architect wants all API calls to use private addressing only and avoid the internet. How can this be achieved?

* + **Use a private virtual interface and create a VPC Endpoint for Amazon API Gateway**
  + **Use a transit virtual interface and an AWS VPN to create a secure tunnel to Amazon API Gateway**
  + Use a public virtual interface and an AWS VPN to create a secure tunnel to Amazon API Gateway
  + Use a hosted virtual interface and create a VPC Endpoint for Amazon API Gateway

**Incorrect**

The requirements are to avoid the internet and use private IP addresses only. The best solution is to use a private virtual interface across the Direct Connect connection to connect to the VPC using private IP addresses. A VPC endpoint for Amazon API Gateway can be created and this will provide access to API Gateway using private IP addresses and avoids the internet completely.  
CORRECT: “Use a private virtual interface and create a VPC Endpoint for Amazon API Gateway” is the correct answer.  
INCORRECT: “Use a hosted virtual interface and create a VPC Endpoint for Amazon API Gateway” is incorrect. A hosted virtual interface is used to allow another account to access your Direct Connect link.  
INCORRECT: “Use a transit virtual interface and an AWS VPN to create a secure tunnel to Amazon API Gateway” is incorrect. A transit virtual interface is used to access Amazon VPC Transit Gateways which are not included in the solution.  
INCORRECT: “Use a public virtual interface and an AWS VPN to create a secure tunnel to Amazon API Gateway” is incorrect. This will use the public internet so it is not allowed in this scenario.  
References:  
<https://docs.aws.amazon.com/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.html>  
<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html>

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

1. 57. Question

Amazon CloudWatch is being used to monitor the performance of AWS Lambda. Which metrics does Lambda track? (choose 2)

* + Number of users
  + **Latency per request**
  + Total number of transactions
  + Total number of connections
  + **Total number of requests**

**Incorrect**

AWS Lambda automatically monitors Lambda functions and reports metrics through Amazon CloudWatch. Lambda tracks the number of requests, the latency per request, and the number of requests resulting in an error. You can view the request rates and error rates using the AWS Lambda Console, the CloudWatch console, and other AWS resources.  
CORRECT: “Total number of requests” is a correct answer.  
CORRECT: “Latency per request” is also a correct answer.  
INCORRECT: “Number of users” is incorrect as this is not returned.  
INCORRECT: “Total number of connections” is incorrect as this is not returned.  
INCORRECT: “Total number of transactions” is incorrect as this is not returned.  
References:  
<https://docs.aws.amazon.com/lambda/latest/dg/monitoring-metrics.html>

Topic: aws-solutions-architect-associate/compute/aws-lambda/

1. 58. Question

A Solutions Architect is creating an application design with several components that will be publicly addressable. The Architect would like to use Alias records. Using Route 53 Alias records what targets can you specify? (choose 2)

* + EFS filesystem
  + **ElastiCache cluster**
  + On-premise web server
  + **CloudFront distribution**
  + **Elastic BeanStalk environment**

**Incorrect**

Alias records are used to map resource record sets in your hosted zone to Amazon Elastic Load Balancing load balancers, API Gateway custom regional APIs and edge-optimized APIs, CloudFront Distributions, AWS Elastic Beanstalk environments, Amazon S3 buckets that are configured as website endpoints, Amazon VPC interface endpoints, and to other records in the same Hosted Zone.  
CORRECT: “CloudFront distribution” is the correct answer.  
CORRECT: “Elastic Beanstalk environment” is the correct answer.  
INCORRECT: “ElastiCache cluster” is incorrect. You cannot use an Alias to point at an ElastiCache cluster or VPC endpoint.  
INCORRECT: “EFS filesystems” is incorrect. You cannot use an Alias to point to an EFS filesystem.  
INCORRECT: “On-premise web server” is incorrect. You cannot point an Alias record directly at an on-premises web server (you can point to another record in a hosted zone, which could point to an on-premises web server though I’m not sure if this is supported).  
References:  
<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html>

Topic: aws-solutions-architect-associate/networking-and-content-delivery/amazon-route-53/

1. 59. Question

A Solutions Architect is designing the messaging and streaming layers of a serverless application. The messaging layer will manage communications between components and the streaming layer will manage real-time analysis and processing of streaming data.  
The Architect needs to select the most appropriate AWS services for these functions. Which services should be used for the messaging and streaming layers? (choose 2)

* + Use Amazon EMR for collecting, processing and analyzing real-time streaming data
  + Use Amazon SWF for providing a fully managed messaging service
  + **Use Amazon Kinesis for collecting, processing and analyzing real-time streaming data**
  + **Use Amazon SNS for providing a fully managed messaging service**
  + Use AWS CloudTrail for collecting, processing and analyzing real-time streaming data

**Incorrect**

Amazon Kinesis makes it easy to collect, process, and analyze real-time streaming data. With Amazon Kinesis Analytics, you can run standard SQL or build entire streaming applications using SQL  
Amazon Simple Notification Service (Amazon SNS) provides a fully managed messaging service for pub/sub patterns using asynchronous event notifications and mobile push notifications for microservices, distributed systems, and serverless applications.  
CORRECT: “Use Amazon Kinesis for collecting, processing and analyzing real-time streaming data” is the correct answer.  
CORRECT: “Use Amazon SNS for providing a fully managed messaging service” is the correct answer.  
INCORRECT: “Use Amazon SWF for providing a fully managed messaging service” is incorrect. Amazon Simple Workflow Service is used for executing tasks not sending messages.  
INCORRECT: “Use Amazon EMR for collecting, processing and analyzing real-time streaming data” is incorrect. Amazon Elastic Map Reduce runs on EC2 instances so is not serverless.  
INCORRECT: “Use AWS CloudTrail for collecting, processing and analyzing real-time streaming data” is incorrect. AWS CloudTrail is used for recording API activity on your account.  
References:  
<https://aws.amazon.com/kinesis/>  
<https://aws.amazon.com/sns/>

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

1. 60. Question

The development team in a media organization is moving their SDLC processes into the AWS Cloud. Which AWS service can a Solutions Architect recommend that is primarily used for software version control?

* + CodeStar
  + Step Functions
  + CloudHSM
  + **CodeCommit**

**Correct**

AWS CodeCommit is a fully-managed source control service that hosts secure Git-based repositories. It makes it easy for teams to collaborate on code in a secure and highly scalable ecosystem. CodeCommit eliminates the need to operate your own source control system or worry about scaling its infrastructure. You can use CodeCommit to securely store anything from source code to binaries, and it works seamlessly with your existing Git tools.  
CORRECT: “CodeCommit” is the correct answer.  
INCORRECT: “CloudHSM” is incorrect. AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud  
INCORRECT: “CodeStar” is incorrect. AWS CodeStar enables you to quickly develop, build, and deploy applications on AWS..  
INCORRECT: “Step Functions” is incorrect. AWS Step Functions lets you coordinate multiple AWS services into serverless workflows so you can build and update apps quickly.  
References:  
<https://aws.amazon.com/codecommit/>

1. 61. Question

Several environments are being created in a single Amazon VPC. The Solutions Architect needs to implement a system of categorization that allows for identification of Amazon EC2 resources by business unit, owner, or environment.  
Which AWS feature can be used?

* + **Tags**
  + Parameters
  + Metadata
  + Custom filters

**Correct**

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value, both of which you define. Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment.  
CORRECT: “Tags” is the correct answer.  
INCORRECT: “Parameters” is incorrect. Parameters are not used for categorization  
INCORRECT: “Metadata” is incorrect. Instance metadata is data about your instance that you can use to configure or manage the running instance.  
INCORRECT: “Custom filters” is incorrect. Custom filters are not used for categorization.  
References:  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html>

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

1. 62. Question

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

* + **Amazon ElastiCache for Redis with cluster mode enabled**
  + Amazon RDS MariaDB with Amazon Athena
  + **Amazon Redshift with Amazon Redshift Spectrum**
  + Amazon DynamoDB with Amazon DynamoDB Accelerator (DAX)

**Incorrect**

Amazon Redshift is an enterprise-level, petabyte scale, fully managed data warehousing service. An Amazon Redshift data warehouse is an enterprise-class relational database query and management system. Redshift supports client connections with many types of applications, including business intelligence (BI), reporting, data, and analytics tools.  
Using Amazon Redshift Spectrum, you can efficiently query and retrieve structured and semistructured data from files in Amazon S3 without having to load the data into Amazon Redshift tables. Redshift Spectrum queries employ massive parallelism to execute very fast against large datasets.

[A screenshot of a computer

Description automatically generated](https://skillcertpro.com/wp-content/uploads/2020/08/b6.png)  
Used together, RedShift and RedShift spectrum are suitable for running massive analytics jobs on both the structured (RedShift data warehouse) and unstructured (Amazon S3) data.  
CORRECT: “Amazon Redshift with Amazon Redshift Spectrum” is the correct answer.  
INCORRECT: “Amazon RDS MariaDB with Amazon Athena” is incorrect. Amazon RDS is not suitable for analytics (OLAP) use cases as it is designed for transactional (OLTP) use cases. Athena can however be used for running SQL queries on data on S3.  
INCORRECT: “Amazon DynamoDB with Amazon DynamoDB Accelerator (DAX)” is incorrect. This is an example of a non-relational DB with a caching layer and is not suitable for an OLAP use case.  
INCORRECT: “Amazon ElastiCache for Redis with cluster mode enabled” is incorrect. This is an example of an in-memory caching service. It is good for performance for transactional use cases.  
References:  
<https://docs.aws.amazon.com/redshift/latest/dg/c_redshift_system_overview.html>  
<https://docs.aws.amazon.com/redshift/latest/dg/c-using-spectrum.html>

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

1. 63. Question

A membership website has become quite popular and is gaining members quickly. The website currently runs on Amazon EC2 instances with one web server instance and one database instance running MySQL. A Solutions Architect is concerned about the lack of high-availability in the current architecture.  
What can the Solutions Architect do to easily enable high availability without making major changes to the architecture?

* + **Install MySQL on an EC2 instance in another availability zone and enable replication**
  + **Enable Multi-AZ for the MySQL instance**
  + Install MySQL on an EC2 instance in the same availability zone and enable replication
  + Create a Read Replica in another availability zone

**Incorrect**

If you are installing MySQL on an EC2 instance you cannot enable read replicas or multi-AZ. Instead you would need to use Amazon RDS with a MySQL DB engine to use these features.  
In this example a good solution is to use the native HA features of MySQL. You would want to place the second MySQL DB instance in another AZ to enable high availability and fault tolerance.  
Migrating to Amazon RDS may be a good solution but is not presented as an option.  
CORRECT: “Install MySQL on an EC2 instance in another availability zone and enable replication” is the correct answer.  
INCORRECT: “Create a Read Replica in another availability zone” is incorrect as described above.  
INCORRECT: “Enable Multi-AZ for the MySQL instance” is incorrect as described above.  
INCORRECT: “Install MySQL on an EC2 instance in the same availability zone and enable replication” is incorrect as described above.  
References:  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-increase-availability.html>

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

1. 64. Question

An application running AWS uses an Elastic Load Balancer (ELB) to distribute connections between EC2 instances. A Solutions Architect needs to record information on the requester, IP, and request type for connections made to the ELB. Additionally, the Architect will also need to perform some analysis on the log files.  
Which AWS services and configuration options can be used to collect and then analyze the logs? (choose 2)

* + **Use EMR for analyzing the log files**
  + **Update the application to use DynamoDB for storing log files**
  + **Enable Access Logs on the ELB and store the log files on S3**
  + Enable Access Logs on the EC2 instances and store the log files on S3
  + Use Elastic Transcoder to analyze the log files

**Incorrect**

The best way to deliver these requirements is to enable access logs on the ELB and then use EMR for analyzing the log files  
Access Logs on ELB are disabled by default. Information includes information about the clients (not included in CloudWatch metrics) such as the identity of the requester, IP, request type etc. Logs can be optionally stored and retained in S3  
Amazon EMR is a web service that enables businesses, researchers, data analysts, and developers to easily and cost-effectively process vast amounts of data. EMR utilizes a hosted Hadoop framework running on Amazon EC2 and Amazon S3.  
CORRECT: “Use EMR for analyzing the log files” is the correct answer.  
CORRECT: “Enable Access Logs on the ELB and store the log files on S3” is the correct answer.  
INCORRECT: “Update the application to use DynamoDB for storing log files” is incorrect. The information recorded by ELB access logs is exactly what you require so there is no need to get the application to record the information into DynamoDB.  
INCORRECT: “Use Elastic Transcoder to analyze the log files” is incorrect. Elastic Transcoder is used for converting media file formats not analyzing files.  
INCORRECT: “Enable Access Logs on the EC2 instances and store the log files on S3” is incorrect as the access logs on the ELB should be enabled.  
References:  
<https://aws.amazon.com/blogs/aws/access-logs-for-elastic-load-balancers/>

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

1. 65. Question

A Solutions Architect must design a solution for providing single sign-on to existing staff in a company. The staff manage on-premise web applications and also need access to the AWS management console to manage resources in the AWS cloud.  
Which combination of services are BEST suited to delivering these requirements?

* + Use IAM and Amazon Cognito
  + **Use your on-premise LDAP directory with IAM**
  + Use IAM and MFA
  + **Use the AWS Secure Token Service (STS) and SAML**

**Incorrect**

Single sign-on using federation allows users to login to the AWS console without assigning IAM credentials. The AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for IAM users or for users that you authenticate (such as federated users from an on-premise directory).  
Federation (typically Active Directory) uses SAML 2.0 for authentication and grants temporary access based on the users AD credentials. The user does not need to be a user in IAM.  
CORRECT: “Use the AWS Secure Token Service (STS) and SAML” is the correct answer.  
INCORRECT: “Use IAM and Amazon Cognito” is incorrect. Amazon Cognito is used for authenticating users to web and mobile apps not for providing single sign-on between on-premises directories and the AWS management console.  
INCORRECT: “Use your on-premise LDAP directory with IAM” is incorrect. You cannot use your on-premise LDAP directory with IAM, you must use federation.  
INCORRECT: “Use IAM and MFA” is incorrect. Enabling multi-factor authentication (MFA) for IAM is not a federation solution..