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.

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.**

**Correct**

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).

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

**Correct**

Exam Tip  
IPv6 traffic =Egress-only internet gateway

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

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

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

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 .

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

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**

**Incorrect**

Exam Tip  
Relational Database migration to AWS = Use Amazon RDS

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**

**Correct**

Exam Tip  
for performance enhancement = run SELECT queries on replicas for (Stale + Reporting ) data

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

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

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

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.

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

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

**Correct**

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

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

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

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**

**Incorrect**

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

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

**Correct**

Exam Tip  
data in chunks + little latency = NoSQL DB = DynamoDB

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.

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

**Correct**

Exam Tip  
  ELB Application Load Balancer is cheaper than ELB Classic Load Balancer.

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

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.

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

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**

**Incorrect**

Exam Tip  
fully managed +  scalable + durable + flexible schema =Amazon DynamoDB

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

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

**Correct**

Exam Tip  
  Docker “Multi-Container” + Scaling +  path-based routing = Amazon ECS + Amazon ELB Application Load Balancer

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**

**Incorrect**

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

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

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

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.

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

**Correct**

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

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.

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.

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**

**Correct**

Exam Tip  
to manage Amazon Redshift cluster via commands = Use AWS CLI

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.

**Correct**

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

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.

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

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

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.

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

**Incorrect**

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.

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.

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

**Correct**

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

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.

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.

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.

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**

**Correct**

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.

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.

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

**Correct**

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.

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.

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

**Correct**

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.

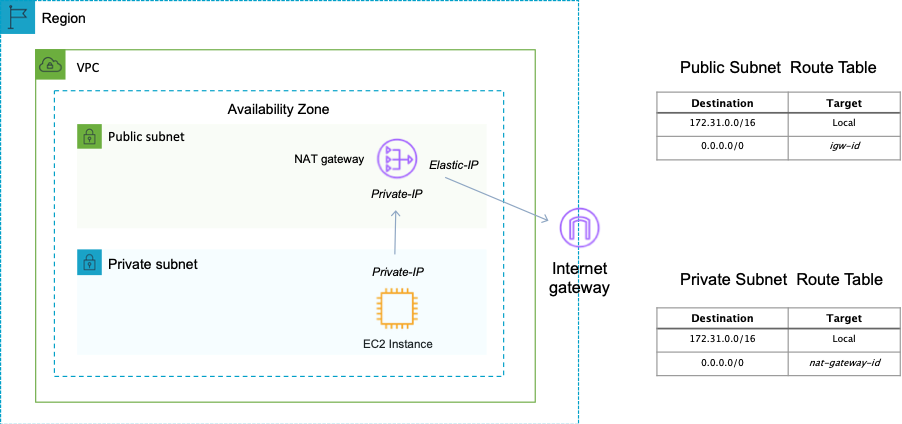
53. Question

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.

[](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.

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

**Incorrect**

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

**Correct**

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.

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.