

Exam Questions Export

Q1: Your company is deploying a website running on AWS Elastic Beanstalk. The website takes over 45 minutes for the installation and contains both static as well as dynamic files that must be generated during the installation process. As a Solutions Architect, you would like to bring the time to create a new instance in your AWS Elastic Beanstalk deployment to be less than 2 minutes. Which of the following options should be combined to build a solution for this requirement? (Select two)

- [CORRECT] Create a Golden Amazon Machine Image (AMI) with the static installation components already setup
- [CORRECT] Use Amazon EC2 user data to customize the dynamic installation parts at boot time
- Store the installation files in Amazon S3 so they can be quickly retrieved
- Use AWS Elastic Beanstalk deployment caching feature
- Use Amazon EC2 user data to install the application at boot time

Q2: The engineering team at a global e-commerce company is currently reviewing their disaster recovery strategy. The team has outlined that they need to be able to quickly recover their application stack with a Recovery Time Objective (RTO) of 5 minutes, in all of the AWS Regions that the application runs. The application stack currently takes over 45 minutes to install on a Linux system. As a Solutions architect, which of the following options would you recommend as the disaster recovery strategy?

- Create an Amazon Machine Image (AMI) after installing the software and use this AMI to run the recovery process in other Regions
- [CORRECT] Create an Amazon Machine Image (AMI) after installing the software and copy the AMI across all Regions. Use this Region-specific AMI to run the recovery process in the respective Regions
- Use Amazon EC2 user data to speed up the installation process
- Store the installation files in Amazon S3 for quicker retrieval

Q3: A ride-sharing company wants to use an Amazon DynamoDB table for data storage. The table will not be used during the night hours whereas the read and write traffic will often be unpredictable during day hours. When traffic spikes occur they will happen very quickly. Which of the following will you recommend as the best-fit solution?

- Set up Amazon DynamoDB table with a global secondary index
- [CORRECT] Set up Amazon DynamoDB table in the on-demand capacity mode**
- Set up Amazon DynamoDB table in the provisioned capacity mode with auto-scaling enabled
- Set up Amazon DynamoDB global table in the provisioned capacity mode

Q4: A development team has configured Elastic Load Balancing for host-based routing. The idea is to support multiple subdomains and different top-level domains. The rule *.example.com matches which of the following?

- EXAMPLE.COM
- example.test.com
- [CORRECT] test.example.com**
- example.com

Q5: A startup's cloud infrastructure consists of a few Amazon EC2 instances, Amazon RDS instances and Amazon S3 storage. A year into their business operations, the startup is incurring costs that seem too high for their business requirements. Which of the following options represents a valid cost-optimization solution?

- Use AWS Compute Optimizer recommendations to help you choose the optimal Amazon EC2 purchasing options and help reserve your instance capacities at reduced costs
- [CORRECT] Use AWS Cost Optimization Hub to get a report of Amazon EC2 instances that are either idle or have low utilization and use AWS Compute Optimizer to look at instance type recommendations**
- Use Amazon S3 Storage class analysis to get recommendations for transitions of objects to Amazon S3 Glacier storage classes to reduce storage costs. You can also automate moving these objects into lower-cost storage tier using Lifecycle Policies
- Use AWS Trusted Advisor checks on Amazon EC2 Reserved Instances to automatically renew reserved instances (RI). AWS Trusted advisor also suggests Amazon RDS idle database instances

Q6: A retail company is using AWS Site-to-Site VPN connections for secure connectivity to its AWS cloud resources from its on-premises data center. Due to a surge in traffic across the VPN connections to the AWS cloud, users are experiencing slower VPN connectivity. Which of the following options will maximize the VPN throughput?

[CORRECT] Create an AWS Transit Gateway with equal cost multipath routing and add additional VPN tunnels

- Use AWS Global Accelerator for the VPN connection to maximize the throughput
- Use Transfer Acceleration for the VPN connection to maximize the throughput
- Create a virtual private gateway with equal cost multipath routing and multiple channels

Q7: As an e-sport tournament hosting company, you have servers that need to scale and be highly available. Therefore you have deployed an Elastic Load Balancing (ELB) with an Auto Scaling group (ASG) across 3 Availability Zones (AZs). When e-sport tournaments are running, the servers need to scale quickly. And when tournaments are done, the servers can be idle. As a general rule, you would like to be highly available, have the capacity to scale and optimize your costs. What do you recommend? (Select two)

- Use Dedicated hosts for the minimum capacity
- Set the minimum capacity to 3

[CORRECT] Use Reserved Instances (RIs) for the minimum capacity

[CORRECT] Set the minimum capacity to 2

- Set the minimum capacity to 1

Q8: A CRM web application was written as a monolith in PHP and is facing scaling issues because of performance bottlenecks. The CTO wants to re-engineer towards microservices architecture and expose their application from the same load balancer, linked to different target groups with different URLs: checkout.mycorp.com, www.mycorp.com, yourcorp.com/profile and yourcorp.com/search. The CTO would like to expose all these URLs as HTTPS endpoints for security purposes. As a solutions architect, which of the following would you recommend as a solution that requires MINIMAL configuration effort?

- Use a wildcard Secure Sockets Layer certificate (SSL certificate)
- [CORRECT] Use Secure Sockets Layer certificate (SSL certificate) with SNI**
- Change the Elastic Load Balancing (ELB) SSL Security Policy
- Use an HTTP to HTTPS redirect

Q9: You are working as a Solutions Architect for a photo processing company that has a proprietary algorithm to compress an image without any loss in quality. Because of the efficiency of the algorithm, your clients are willing to wait for a response that carries their compressed images back. You also want to process these jobs asynchronously and scale quickly, to cater to the high demand. Additionally, you also want the job to be retried in case of failures. Which combination of choices do you recommend to minimize cost and comply with the requirements? (Select two)

[CORRECT] Amazon EC2 Spot Instances

[CORRECT] Amazon Simple Queue Service (Amazon SQS)

- Amazon Simple Notification Service (Amazon SNS)
- Amazon EC2 Reserved Instances (RIs)
- Amazon EC2 On-Demand Instances

Q10: A company has migrated its application from a monolith architecture to a microservices based architecture. The development team has updated the Amazon Route 53 simple record to point "myapp.mydomain.com" from the old Load Balancer to the new one. The users are still not redirected to the new Load Balancer. What has gone wrong in the configuration?

[CORRECT] The Time To Live (TTL) is still in effect

- The health checks are failing
- The Alias Record is misconfigured
- The CNAME Record is misconfigured

Q11: A developer in your company has set up a classic 2 tier architecture consisting of an Application Load Balancer and an Auto Scaling group (ASG) managing a fleet of Amazon EC2 instances. The Application Load Balancer is deployed in a subnet of size 10.0.1.0/24 and the Auto Scaling group is deployed in a subnet of size 10.0.4.0/22. As a solutions architect, you would like to adhere to the security pillar of the well-architected framework. How do you configure the security group of the Amazon EC2 instances to only allow traffic coming from the Application Load Balancer?

[CORRECT] Add a rule to authorize the security group of the Application Load Balancer

- Add a rule to authorize the CIDR 10.0.1.0/24
- Add a rule to authorize the security group of the Auto Scaling group
- Add a rule to authorize the CIDR 10.0.4.0/22

Q12: A fintech startup hosts its real-time transaction metadata in Amazon DynamoDB tables. During a recent system maintenance event, a junior engineer accidentally deleted a production table, resulting in major service downtime and irreversible data loss. Leadership has mandated an immediate solution that prevents future data loss from human error, while requiring minimal ongoing maintenance or manual effort from the engineering team. Which approach best addresses these requirements with the least operational overhead?

[CORRECT] Enable deletion protection on DynamoDB tables

- Configure AWS CloudTrail to monitor DynamoDB API calls. Set up an Amazon EventBridge rule to detect DeleteTable events and trigger a Lambda function that recreates the deleted table using backup data stored in Amazon S3
- Enable point-in-time recovery (PITR) on each DynamoDB table
- Manually export each table as a full backup to Amazon S3 on a weekly basis. Use the DynamoDB export to S3 feature and rely on manual recovery if tables are deleted

Q13: A healthcare provider is experiencing rapid data growth in its on-premises servers due to increased patient imaging and record retention requirements. The organization wants to extend its storage capacity to AWS in a way that preserves quick access to critical records, including from its local file systems. The company must optimize bandwidth usage during migration and avoid any retrieval fees or delays when accessing the data in the cloud. The provider wants a hybrid cloud solution that requires minimal application reconfiguration, allows frequent local access to key datasets, and ensures that cloud storage costs remain predictable without paying extra for data retrieval. Which AWS solution best meets these requirements?

- Set up Amazon S3 Standard-Infrequent Access (S3 Standard-IA) as the primary storage tier. Configure the on-premises file server to replicate changes to the S3 bucket using AWS DataSync for asynchronous updates
- Implement Amazon FSx for Windows File Server and configure on-premises servers to mount the file system using a VPN connection. Store all primary data in FSx and use it as the central NAS replacement

[CORRECT] Deploy AWS Storage Gateway using cached volumes. Store frequently accessed data locally, while writing all primary data asynchronously to Amazon S3

- Deploy AWS Storage Gateway using stored volumes. Retain the full dataset on-premises and asynchronously back up point-in-time snapshots to Amazon S3. Configure applications to read from the local volume and recover data from the cloud if needed

Q14: A genomics research firm is processing sporadic bursts of data-intensive workloads using Amazon EC2 instances. The shared storage must support unpredictable spikes in file operations, but the average daily throughput demand remains relatively low. The team has selected Amazon Elastic File System (EFS) for its scalability and wants to ensure optimal cost and performance during bursts without provisioning throughput manually. Which approach should the team take to best meet these requirements?

[] Change the throughput mode to provisioned and configure the desired throughput value to support burst workloads

[CORRECT] Enable EFS burst throughput mode on the file system using the General Purpose performance mode and EFS Standard storage class

[] Enable EFS Infrequent Access (IA) storage class to reduce storage cost while continuing to benefit from burst throughput mode

[] Switch the EFS storage class to EFS One Zone to reduce cost, which will automatically enable burst throughput mode

Q15: A Big Data processing company has created a distributed data processing framework that performs best if the network performance between the processing machines is high. The application has to be deployed on AWS, and the company is only looking at performance as the key measure. As a Solutions Architect, which deployment do you recommend?

[CORRECT] Use a Cluster placement group

[] Optimize the Amazon EC2 kernel using EC2 User Data

[] Use Spot Instances

[] Use a Spread placement group

Q16: An e-commerce company wants to migrate its on-premises application to AWS. The application consists of application servers and a Microsoft SQL Server database. The solution should result in the maximum possible availability for the database layer while minimizing operational and management overhead. As a solutions architect, which of the following would you recommend to meet the given requirements?

[CORRECT] Migrate the data to Amazon RDS for SQL Server database in a Multi-AZ deployment

- Migrate the data to Amazon RDS for SQL Server database in a cross-region read-replica configuration
- Migrate the data to Amazon EC2 instance hosted SQL Server database. Deploy the Amazon EC2 instances in a Multi-AZ configuration
- Migrate the data to Amazon RDS for SQL Server database in a cross-region Multi-AZ deployment

Q17: A small rental company had 5 employees, all working under the same AWS cloud account. These employees deployed their applications built for various functions- including billing, operations, finance, etc. Each of these employees has been operating in their own VPC. Now, there is a need to connect these VPCs so that the applications can communicate with each other. Which of the following is the MOST cost-effective solution for this use-case?

- Use a Network Address Translation gateway (NAT gateway)

[CORRECT] Use a VPC peering connection

- Use an AWS Direct Connect connection
- Use an Internet Gateway

Q18: A transportation logistics company runs a shipment tracking application on Amazon EC2 instances with an Amazon Aurora MySQL database cluster. The application is experiencing rapid growth due to increased demand from mobile app users querying package delivery statuses. Although the compute layer (EC2) has remained stable, the Aurora DB cluster is under growing read pressure, especially from frequent repeated queries about package locations and delivery history. The company added an Aurora read replica, which temporarily alleviated the load, but read traffic continues to spike as user queries grow. The company wants to reduce the repeated reads pressure on the DB cluster. Which solution will best meet these requirements in a cost-effective manner?

[] Add another Aurora read replica to distribute the increasing read load across more read nodes.
Adjust the application to perform client-side load balancing across the read replicas

[CORRECT] Integrate Amazon ElastiCache for Redis between the application and Aurora. Cache frequently accessed query results in Redis to reduce the number of identical read requests hitting the database

[] Convert the Aurora MySQL DB cluster into a multi-writer setup using Aurora global database.
Allow concurrent writes from multiple application nodes across Regions

[] Enable Aurora Serverless v2 for the DB cluster to automatically scale read and write capacity in response to usage spikes. Route all traffic through the cluster endpoint

Q19: The engineering team at a social media company has recently migrated to AWS Cloud from its on-premises data center. The team is evaluating Amazon CloudFront to be used as a CDN for its flagship application. The team has hired you as an AWS Certified Solutions Architect – Associate to advise on Amazon CloudFront capabilities on routing, security, and high availability. Which of the following would you identify as correct regarding Amazon CloudFront? (Select three)

[CORRECT] Use field level encryption in Amazon CloudFront to protect sensitive data for specific content

[] Amazon CloudFront can route to multiple origins based on the price class

[] Use geo restriction to configure Amazon CloudFront for high-availability and failover

[CORRECT] Amazon CloudFront can route to multiple origins based on the content type

[] Use AWS Key Management Service (AWS KMS) encryption in Amazon CloudFront to protect sensitive data for specific content

[CORRECT] Use an origin group with primary and secondary origins to configure Amazon CloudFront for high-availability and failover

Q20: A ride-sharing company wants to improve the ride-tracking system that stores GPS coordinates for all rides. The engineering team at the company is looking for a NoSQL database that has single-digit millisecond latency, can scale horizontally, and is serverless, so that they can perform high-frequency lookups reliably. As a Solutions Architect, which database do you recommend for their requirements?

- Amazon ElastiCache
- [CORRECT] Amazon DynamoDB**
- Amazon Relational Database Service (Amazon RDS)
- Amazon Neptune

Q21: A Big Data analytics company writes data and log files in Amazon S3 buckets. The company now wants to stream the existing data files as well as any ongoing file updates from Amazon S3 to Amazon Kinesis Data Streams. As a Solutions Architect, which of the following would you suggest as the fastest possible way of building a solution for this requirement?

- Configure Amazon EventBridge events for the bucket actions on Amazon S3. An AWS Lambda function can then be triggered from the Amazon EventBridge event that will send the necessary data to Amazon Kinesis Data Streams
- [CORRECT] Leverage AWS Database Migration Service (AWS DMS) as a bridge between Amazon S3 and Amazon Kinesis Data Streams**
- Leverage Amazon S3 event notification to trigger an AWS Lambda function for the file create event. The AWS Lambda function will then send the necessary data to Amazon Kinesis Data Streams
- Amazon S3 bucket actions can be directly configured to write data into Amazon Simple Notification Service (Amazon SNS). Amazon SNS can then be used to send the updates to Amazon Kinesis Data Streams

Q22: A financial services firm has traditionally operated with an on-premise data center and would like to create a disaster recovery strategy leveraging the AWS Cloud. As a Solutions Architect, you would like to ensure that a scaled-down version of a fully functional environment is always running in the AWS cloud, and in case of a disaster, the recovery time is kept to a minimum. Which disaster recovery strategy is that?

- Pilot Light
- [CORRECT] Warm Standby**
- Multi Site
- Backup and Restore

Q23: A systems administrator is creating IAM policies and attaching them to IAM identities. After creating the necessary identity-based policies, the administrator is now creating resource-based policies. Which is the only resource-based policy that the IAM service supports?

- Access control list (ACL)
- [CORRECT] Trust policy**
- Permissions boundary
- AWS Organizations Service Control Policies (SCP)

Q24: For security purposes, a development team has decided to deploy the Amazon EC2 instances in a private subnet. The team plans to use VPC endpoints so that the instances can access some AWS services securely. The members of the team would like to know about the two AWS services that support Gateway Endpoints. As a solutions architect, which of the following services would you suggest for this requirement? (Select two)

- Amazon Kinesis
- [CORRECT] Amazon DynamoDB**
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Queue Service (Amazon SQS)
- [CORRECT] Amazon S3**

Q25: The engineering team at an e-commerce company has been tasked with migrating to a serverless architecture. The team wants to focus on the key points of consideration when using AWS Lambda as a backbone for this architecture. As a Solutions Architect, which of the following options would you identify as correct for the given requirement? (Select three)

[CORRECT] Since AWS Lambda functions can scale extremely quickly, it's a good idea to deploy a Amazon CloudWatch Alarm that notifies your team when function metrics such as ConcurrentExecutions or Invocations exceeds the expected threshold

[] AWS Lambda allocates compute power in proportion to the memory you allocate to your function. AWS, thus recommends to over provision your function time out settings for the proper performance of AWS Lambda functions

[CORRECT] By default, AWS Lambda functions always operate from an AWS-owned VPC and hence have access to any public internet address or public AWS APIs. Once an AWS Lambda function is VPC-enabled, it will need a route through a Network Address Translation gateway (NAT gateway) in a public subnet to access public resources

[] Serverless architecture and containers complement each other but you cannot package and deploy AWS Lambda functions as container images

[CORRECT] If you intend to reuse code in more than one AWS Lambda function, you should consider creating an AWS Lambda Layer for the reusable code

[] The bigger your deployment package, the slower your AWS Lambda function will cold-start. Hence, AWS suggests packaging dependencies as a separate package from the actual AWS Lambda package

Q26: An enterprise has decided to move its secondary workloads such as backups and archives to AWS cloud. The CTO wishes to move the data stored on physical tapes to Cloud, without changing their current tape backup workflows. The company holds petabytes of data on tapes and needs a cost-optimized solution to move this data to cloud. What is an optimal solution that meets these requirements while keeping the costs to a minimum?

[CORRECT] Use Tape Gateway, which can be used to move on-premises tape data onto AWS Cloud. Then, Amazon S3 archiving storage classes can be used to store data cost-effectively for years

[] Use AWS DataSync, which makes it simple and fast to move large amounts of data online between on-premises storage and AWS Cloud. Data moved to Cloud can then be stored cost-effectively in Amazon S3 archiving storage classes

[] Use AWS Direct Connect, a cloud service solution that makes it easy to establish a dedicated network connection from on-premises to AWS to transfer data. Once this is done, Amazon S3 can be used to store data at lesser costs

[] Use AWS VPN connection between the on-premises datacenter and your Amazon VPC. Once this is established, you can use Amazon Elastic File System (Amazon EFS) to get a scalable, fully managed elastic NFS file system for use with AWS Cloud services and on-premises resources

Q27: You started a new job as a solutions architect at a company that has both AWS experts and people learning AWS. Recently, a developer misconfigured a newly created Amazon RDS database which resulted in a production outage. How can you ensure that Amazon RDS specific best practices are incorporated into a reusable infrastructure template to be used by all your AWS users?

- Create an AWS Lambda function which sends emails when it finds misconfigured Amazon RDS databases

[CORRECT] Use AWS CloudFormation to manage Amazon RDS databases

- Attach an IAM policy to interns preventing them from creating an Amazon RDS database
- Store your recommendations in a custom AWS Trusted Advisor rule

Q28: A company uses Application Load Balancers in multiple AWS Regions. The Application Load Balancers receive inconsistent traffic that varies throughout the year. The engineering team at the company needs to allow the IP addresses of the Application Load Balancers in the on-premises firewall to enable connectivity. Which of the following represents the MOST scalable solution with minimal configuration changes?

[CORRECT] Set up AWS Global Accelerator. Register the Application Load Balancers in different Regions to the AWS Global Accelerator. Configure the on-premises firewall's rule to allow static IP addresses associated with the AWS Global Accelerator

- Develop an AWS Lambda script to get the IP addresses of the Application Load Balancers in different Regions. Configure the on-premises firewall's rule to allow the IP addresses of the Application Load Balancers
- Set up a Network Load Balancer in one Region. Register the private IP addresses of the Application Load Balancers in different Regions with the Network Load Balancer. Configure the on-premises firewall's rule to allow the Elastic IP address attached to the Network Load Balancer
- Migrate all Application Load Balancers in different Regions to the Network Load Balancers. Configure the on-premises firewall's rule to allow the Elastic IP addresses of all the Network Load Balancers

Q29: Amazon Route 53 is configured to route traffic to two Network Load Balancer nodes belonging to two Availability Zones (AZs): AZ-A and AZ-B. Cross-zone load balancing is disabled. AZ-A has four targets and AZ-B has six targets. Which of the below statements is true about traffic distribution to the target instances from Amazon Route 53?

[CORRECT] Each of the four targets in AZ-A receives 12.5% of the traffic

- Each of the six targets in AZ-B receives 10% of the traffic
- Each of the four targets in AZ-A receives 10% of the traffic
- Each of the four targets in AZ-A receives 8% of the traffic

Q30: A company has developed a popular photo-sharing website using a serverless pattern on the AWS Cloud using Amazon API Gateway and AWS Lambda. The backend uses an Amazon RDS PostgreSQL database. The website is experiencing high read traffic and the AWS Lambda functions are putting an increased read load on the Amazon RDS database. The architecture team is planning to increase the read throughput of the database, without changing the application's core logic. As a Solutions Architect, what do you recommend?

[CORRECT] Use Amazon RDS Read Replicas

- Use Amazon DynamoDB
- Use Amazon ElastiCache
- Use Amazon RDS Multi-AZ feature

Q31: A global pharmaceutical company operates a hybrid cloud network. Its primary AWS workloads run in the us-west-2 Region, connected to its on-premises data center via an AWS Direct Connect connection. After acquiring a biotech firm headquartered in Europe, the company must integrate the biotech's workloads, which are hosted in several VPCs in the eu-central-1 Region and connected to the biotech's on-premises facility through a separate Direct Connect link. All CIDR blocks are non-overlapping, and the business requires full connectivity between both data centers and all VPCs across the two Regions. The company also wants a scalable solution that minimizes manual network configuration and long-term operational overhead. Which solution will best meet these requirements?

- Establish inter-Region VPC peering between each VPC in the us-west-2 and eu-central-1 Regions. Use static routing tables in each VPC to define peer relationships and enable cross-Region communication
- [CORRECT] Connect both Direct Connect links to a shared Direct Connect gateway. Attach each Region's virtual private gateway (VGW) to the Direct Connect gateway, enabling transitive routing between the VPCs and the on-premises networks across Regions**
- Create private VIFs (virtual interfaces) in each Region and associate them directly with foreign-region VPCs using routing table entries and BGP. Use VPC endpoints in each account to forward cross-Region traffic
- Deploy EC2-based VPN appliances in each VPC. Configure a full mesh VPN topology between all VPCs and data centers using CloudHub-style routing across Regions

Q32: The development team at a social media company wants to handle some complicated queries such as "What are the number of likes on the videos that have been posted by friends of a user A?". As a solutions architect, which of the following AWS database services would you suggest as the BEST fit to handle such use cases?

- Amazon OpenSearch Service
- Amazon Redshift
- [CORRECT] Amazon Neptune**
- Amazon Aurora

Q33: A company has noticed that its Amazon EBS Elastic Volume (io1) accounts for 90% of the cost and the remaining 10% cost can be attributed to the Amazon EC2 instance. The Amazon CloudWatch metrics report that both the Amazon EC2 instance and the Amazon EBS volume are under-utilized. The Amazon CloudWatch metrics also show that the Amazon EBS volume has occasional I/O bursts. The entire infrastructure is managed by AWS CloudFormation. As a Solutions Architect, what do you propose to reduce the costs?

[] Change the Amazon EC2 instance type to something much smaller

[] Keep the Amazon EBS volume to io1 and reduce the IOPS

[CORRECT] Convert the Amazon EC2 instance EBS volume to gp2

[] Don't use a AWS CloudFormation template to create the database as the AWS CloudFormation service incurs greater service charges

Q34: As a solutions architect, you have created a solution that utilizes an Application Load Balancer with stickiness and an Auto Scaling Group (ASG). The Auto Scaling Group spans across 2 Availability Zones (AZs). AZ-A has 3 Amazon EC2 instances and AZ-B has 4 Amazon EC2 instances. The Auto Scaling Group is about to go into a scale-in event due to the triggering of a Amazon CloudWatch alarm. What will happen under the default Auto Scaling Group configuration?

[] A random instance in the AZ-A will be terminated

[] A random instance will be terminated in AZ-B

[] An instance in the AZ-A will be created

[CORRECT] The instance with the oldest launch template or launch configuration will be terminated in AZ-B

Q35: You are working for a software as a service (SaaS) company as a solutions architect and help design solutions for the company's customers. One of the customers is a bank and has a requirement to whitelist a public IP when the bank is accessing external services across the internet. Which architectural choice do you recommend to maintain high availability, support scaling-up to 10 instances and comply with the bank's requirements?

[] Use a Classic Load Balancer with an Auto Scaling Group

[] Use an Application Load Balancer with an Auto Scaling Group

[CORRECT] Use a Network Load Balancer with an Auto Scaling Group

[] Use an Auto Scaling Group with Dynamic Elastic IPs attachment

Q36: A company wants to grant access to an Amazon S3 bucket to users in its own AWS account as well as to users in another AWS account. Which of the following options can be used to meet this requirement?

- Use a user policy to grant permission to users in its account as well as to users in another account
 - Use either a bucket policy or a user policy to grant permission to users in its account as well as to users in another account
 - Use permissions boundary to grant permission to users in its account as well as to users in another account
- [CORRECT] Use a bucket policy to grant permission to users in its account as well as to users in another account**

Q37: You have an Amazon S3 bucket that contains files in two different folders -s3://my-bucket/images and s3://my-bucket-thumbnails. When an image is first uploaded and new, it is viewed several times. But after 45 days, analytics prove that image files are on average rarely requested, but the thumbnails still are. After 180 days, you would like to archive the image files and the thumbnails. Overall you would like the solution to remain highly available to prevent disasters happening against a whole Availability Zone (AZ). How can you implement an efficient cost strategy for your Amazon S3 bucket? (Select two)

- Create a Lifecycle Policy to transition all objects to Amazon S3 Standard IA after 45 days
 - Create a Lifecycle Policy to transition objects to Amazon S3 One Zone IA using a prefix after 45 days
 - Create a Lifecycle Policy to transition objects to Amazon S3 Glacier using a prefix after 180 days
- [CORRECT] Create a Lifecycle Policy to transition all objects to Amazon S3 Glacier after 180 days**
- [CORRECT] Create a Lifecycle Policy to transition objects to Amazon S3 Standard IA using a prefix after 45 days**

Q38: A company runs a popular dating website on the AWS Cloud. As a Solutions Architect, you've designed the architecture of the website to follow a serverless pattern on the AWS Cloud using Amazon API Gateway and AWS Lambda. The backend uses an Amazon RDS PostgreSQL database. Currently, the application uses a username and password combination to connect the AWS Lambda function to the Amazon RDS database. You would like to improve the security at the authentication level by leveraging short-lived credentials. What will you choose? (Select two)

- Deploy AWS Lambda in a VPC
- [CORRECT] Attach an AWS Identity and Access Management (IAM) role to AWS Lambda**
- [CORRECT] Use IAM authentication from AWS Lambda to Amazon RDS PostgreSQL**
- Restrict the Amazon RDS database security group to the AWS Lambda's security group
- Embed a credential rotation logic in the AWS Lambda, retrieving them from SSM

Q39: A ride-hailing startup has launched a mobile app that matches passengers with nearby drivers based on real-time GPS coordinates. The application backend uses an Amazon RDS for PostgreSQL instance with read replicas to store the latitude and longitude of drivers and passengers. As the service scales, the backend experiences performance bottlenecks during peak hours, especially when thousands of updates and reads occur per second to keep location data current. The company expects its user base to double in the next few months and needs a high-performance, scalable solution that can handle frequent write and read operations with minimal latency. What do you recommend?

- Create a read-replica Auto Scaling policy for the PostgreSQL database to dynamically add replicas during peak load. Distribute traffic evenly using an RDS proxy with failover configuration
- Migrate the location data to Amazon OpenSearch Service and use its geospatial indexing features to retrieve and store coordinates in near real-time. Visualize tracking data using OpenSearch Dashboards
- [CORRECT] Place an Amazon ElastiCache for Redis cluster in front of the PostgreSQL database. Modify the application to cache recent location reads and updates in Redis, using a TTL-based eviction strategy**
- Enable Multi-AZ deployment for the primary RDS instance to improve write resilience and fault tolerance. Use Multi-AZ standby failover to distribute reads during peak hours

Q40: An Elastic Load Balancer has marked all the Amazon EC2 instances in the target group as unhealthy. Surprisingly, when a developer enters the IP address of the Amazon EC2 instances in the web browser, he can access the website. What could be the reason the instances are being marked as unhealthy? (Select two)

[] You need to attach elastic IP address (EIP) to the Amazon EC2 instances

[CORRECT] The route for the health check is misconfigured

[] Your web-app has a runtime that is not supported by the Application Load Balancer

[] The Amazon Elastic Block Store (Amazon EBS) volumes have been improperly mounted

[CORRECT] The security group of the Amazon EC2 instance does not allow for traffic from the security group of the Application Load Balancer

Q41: A digital media platform is preparing to launch a new interactive content service that is expected to receive sudden spikes in user engagement, especially during live events and media releases. The backend uses an Amazon Aurora PostgreSQL Serverless v2 cluster to handle dynamic workloads. The architecture must be capable of scaling both compute and storage performance to maintain low latency and avoid bottlenecks under load. The engineering team is evaluating storage configuration options and wants a solution that will scale automatically with traffic, optimize I/O performance, and remain cost-effective without manual provisioning or tuning. Which configuration will best meet these requirements?

[] Select Provisioned IOPS (io1) as the storage type for the Aurora cluster. Manually adjust IOPS based on expected traffic during peak usage

[] Configure the cluster with Magnetic (Standard) storage to minimize baseline storage costs and rely on Aurora's autoscaling to handle demand spikes

[] Configure the Aurora cluster to use General Purpose SSD (gp2) storage. Increase performance by scaling database compute capacity to reduce IOPS bottlenecks

[CORRECT] Configure the Aurora cluster to use Aurora I/O-Optimized storage. This configuration delivers high throughput and low-latency I/O performance with predictable pricing and no I/O-based charges

Q42: A company's business logic is built on several microservices that are running in the on-premises data center. They currently communicate using a message broker that supports the MQTT protocol. The company is looking at migrating these applications and the message broker to AWS Cloud without changing the application logic. Which technology allows you to get a managed message broker that supports the MQTT protocol?

- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Queue Service (Amazon SQS)
- Amazon Kinesis Data Streams

[CORRECT] Amazon MQ

Q43: An e-commerce company tracks user clicks on its flagship website and performs analytics to provide near-real-time product recommendations. An Amazon EC2 instance receives data from the website and sends the data to an Amazon Aurora Database instance. Another Amazon EC2 instance continuously checks the changes in the database and executes SQL queries to provide recommendations. Now, the company wants a redesign to decouple and scale the infrastructure. The solution must ensure that data can be analyzed in real-time without any data loss even when the company sees huge traffic spikes. What would you recommend as an AWS Certified Solutions Architect - Associate?

- Leverage Amazon Kinesis Data Streams to capture the data from the website and feed it into Amazon Kinesis Data Firehose to persist the data on Amazon S3. Lastly, use Amazon Athena to analyze the data in real time

[CORRECT] Leverage Amazon Kinesis Data Streams to capture the data from the website and feed it into Amazon Kinesis Data Analytics which can query the data in real time. Lastly, the analyzed feed is output into Amazon Kinesis Data Firehose to persist the data on Amazon S3

- Leverage Amazon Kinesis Data Streams to capture the data from the website and feed it into Amazon QuickSight which can query the data in real time. Lastly, the analyzed feed is output into Kinesis Data Firehose to persist the data on Amazon S3

- Leverage Amazon SQS to capture the data from the website. Configure a fleet of Amazon EC2 instances under an Auto scaling group to process messages from the Amazon SQS queue and trigger the scaling policy based on the number of pending messages in the queue. Perform real-time analytics using a third-party library on the Amazon EC2 instances

Q44: A social media company wants the capability to dynamically alter the size of a geographic area from which traffic is routed to a specific server resource. Which feature of Amazon Route 53 can help achieve this functionality?

- Latency-based routing
- Geolocation routing
- [CORRECT] Geoproximity routing**
- Weighted routing

Q45: A financial services company is implementing two separate data retention policies to comply with regulatory standards: Policy A: Critical transaction records must be immediately available for audit and must not be deleted or overwritten for 7 years. Policy B: Archived compliance data must be stored in a low-cost, long-term storage solution and locked from deletion or modification for at least 10 years. As a solutions architect, which combination of AWS features should you recommend to enforce these policies effectively?

- Use Amazon S3 Standard storage class with S3 Lifecycle policies for Policy A, and S3 Glacier Flexible Retrieval for Policy B
- [CORRECT] Use Amazon S3 Object Lock in Compliance mode for Policy A, and S3 Glacier Vault Lock for Policy B**
- Use Amazon S3 Glacier Vault Lock for both policies to reduce storage costs while enforcing retention
- Use Amazon S3 Object Lock in Governance mode for both policies to ensure data cannot be deleted prematurely

Q46: A company has recently created a new department to handle their services workload. An IT team has been asked to create a custom VPC to isolate the resources created in this new department. They have set up the public subnet and internet gateway (IGW). However, they are not able to ping the Amazon EC2 instances with elastic IP address (EIP) launched in the newly created VPC. As a Solutions Architect, the team has requested your help. How will you troubleshoot this scenario? (Select two)

- Create a secondary internet gateway to attach with public subnet and move the current internet gateway to private and write route tables
- Contact AWS support to map your VPC with subnet
- [CORRECT] Check if the security groups allow ping from the source**
- Disable Source / Destination check on the Amazon EC2 instance
- [CORRECT] Check if the route table is configured with internet gateway**

Q47: You have developed a new REST API leveraging the Amazon API Gateway, AWS Lambda and Amazon Aurora database services. Most of the workload on the website is read-heavy. The data rarely changes and it is acceptable to serve users outdated data for about 24 hours. Recently, the website has been experiencing high load and the costs incurred on the Aurora database have been very high. How can you easily reduce the costs while improving performance, with minimal changes?

[CORRECT] Enable Amazon API Gateway Caching

- Switch to using an Application Load Balancer
- Add Amazon Aurora Read Replicas
- Enable AWS Lambda In Memory Caching

Q48: A junior developer has downloaded a sample Amazon S3 bucket policy to make changes to it based on new company-wide access policies. He has requested your help in understanding this bucket policy. As a Solutions Architect, which of the following would you identify as the correct description for the given policy?

- It authorizes an IP address and a Classless Inter-Domain Routing (CIDR) to access the S3 bucket
- [CORRECT] It authorizes an entire Classless Inter-Domain Routing (CIDR) except one IP address to access the Amazon S3 bucket**
- It ensures Amazon EC2 instances that have inherited a security group can access the bucket
- It ensures the Amazon S3 bucket is exposing an external IP within the Classless Inter-Domain Routing (CIDR) range specified, except one IP

Q49: A company wants to adopt a hybrid cloud infrastructure where it uses some AWS services such as Amazon S3 alongside its on-premises data center. The company wants a dedicated private connection between the on-premise data center and AWS. In case of failures though, the company needs to guarantee uptime and is willing to use the public internet for an encrypted connection. What do you recommend? (Select two)

- Use Egress Only Internet Gateway as a backup connection
- [CORRECT] Use AWS Site-to-Site VPN as a backup connection**
- [CORRECT] Use AWS Direct Connect connection as a primary connection**
- Use AWS Site-to-Site VPN as a primary connection
- Use AWS Direct Connect connection as a backup connection

Q50: What does this AWS CloudFormation snippet do? (Select three)

[CORRECT] It lets traffic flow from one IP on port 22

It configures a security group's outbound rules

[CORRECT] It configures a security group's inbound rules

It configures the inbound rules of a network access control list (network ACL)

It only allows the IP 0.0.0.0 to reach HTTP

[CORRECT] It allows any IP to pass through on the HTTP port

It prevents traffic from reaching on HTTP unless from the IP 192.168.1.1

Q51: An e-commerce analytics company is preparing to archive several years of transaction records and customer analytics reports in Amazon S3 for long-term storage. To meet compliance requirements, the archived data must be encrypted at rest. Additionally, the solution must be cost-effective and ensure that key rotation occurs automatically every 12 months to comply with the company's internal data governance policy. Which solution will meet these requirements with the least operational overhead?

[CORRECT] Use AWS Key Management Service (KMS) to create a customer managed key with automatic rotation enabled. Configure the S3 bucket's default encryption to use the customer managed key. Migrate the data to the S3 bucket

Use AWS CloudHSM to generate encryption keys. Configure S3 to use these custom encryption keys via client-side encryption and rotate the keys annually using an on-premises key management workflow

Encrypt the data locally using client-side encryption libraries and upload the encrypted files to S3. Create a KMS key with imported key material and configure key rotation settings

Use Amazon S3 server-side encryption with S3-managed keys (SSE-S3). Upload data with default encryption enabled. Rely on the built-in key management and rotation behavior of SSE-S3

Q52: An e-commerce company has copied 1 petabyte of data from its on-premises data center to an Amazon S3 bucket in theus-west-1Region using an AWS Direct Connect link. The company now wants to set up a one-time copy of the data to another Amazon S3 bucket in theus-east-1Region. The on-premises data center does not allow the use of AWS Snowball. As a Solutions Architect, which of the following options can be used to accomplish this goal? (Select two)

- Set up Amazon S3 Transfer Acceleration (Amazon S3TA) to copy objects across Amazon S3 buckets in different Regions using S3 console
- [CORRECT] Copy data from the source bucket to the destination bucket using the aws S3 sync command**
- Use AWS Snowball Edge device to copy the data from one Region to another Region
- Copy data from the source Amazon S3 bucket to a target Amazon S3 bucket using the S3 console
- [CORRECT] Set up Amazon S3 batch replication to copy objects across Amazon S3 buckets in another Region using S3 console and then delete the replication configuration**

Q53: An IT company runs a high-performance computing (HPC) workload on AWS. The workload requires high network throughput and low-latency network performance along with tightly coupled node-to-node communications. The Amazon EC2 instances are properly sized for compute and storage capacity and are launched using default options. Which of the following solutions can be used to improve the performance of the workload?

- Select an Elastic Inference accelerator while launching Amazon EC2 instances
- Select the appropriate capacity reservation while launching Amazon EC2 instances
- Select dedicated instance tenancy while launching Amazon EC2 instances
- [CORRECT] Select a cluster placement group while launching Amazon EC2 instances**

Q54: A media company uses Amazon ElastiCache Redis to enhance the performance of its Amazon RDS database layer. The company wants a robust disaster recovery strategy for its caching layer that guarantees minimal downtime as well as minimal data loss while ensuring good application performance. Which of the following solutions will you recommend to address the given use-case?

[CORRECT] Opt for Multi-AZ configuration with automatic failover functionality to help mitigate failure

- Schedule manual backups using Redis append-only file (AOF)
- Add read-replicas across multiple availability zones (AZs) to reduce the risk of potential data loss because of failure
- Schedule daily automatic backups at a time when you expect low resource utilization for your cluster

Q55: A Pharmaceuticals company is looking for a simple solution to connect its VPCs and on-premises networks through a central hub. As a Solutions Architect, which of the following would you suggest as the solution that requires the LEAST operational overhead?

- Use Transit VPC Solution to connect the Amazon VPCs to the on-premises networks

[CORRECT] Use AWS Transit Gateway to connect the Amazon VPCs to the on-premises networks

- Fully meshed VPC peering can be used to connect the Amazon VPCs to the on-premises networks
- Partially meshed VPC peering can be used to connect the Amazon VPCs to the on-premises networks

Q56: A digital media company needs to manage uploads of around 1 terabyte each from an application being used by a partner company. As a Solutions Architect, how will you handle the upload of these files to Amazon S3?

- Use AWS Snowball

[CORRECT] Use multi-part upload feature of Amazon S3

- Use AWS Direct Connect to provide extra bandwidth
- Use Amazon S3 Versioning

Q57: A media company operates a video rendering pipeline on Amazon EKS, where containerized jobs are scheduled using Kubernetes deployments. The application experiences bursty traffic patterns, particularly during peak streaming hours. The platform uses the Kubernetes Horizontal Pod Autoscaler (HPA) to scale pods based on CPU utilization. A solutions architect observes that the total number of EC2 worker nodes remains constant during traffic spikes, even when all nodes are at maximum resource utilization. The company needs a solution that enables automatic scaling of the underlying compute infrastructure when pod demand exceeds cluster capacity. Which solution should the architect implement to resolve this issue with the least operational overhead?

[] Use AWS Fargate to replace the EKS worker nodes with serverless compute profiles, allowing Fargate to scale pods automatically without managing EC2 infrastructure

[CORRECT] Deploy the Kubernetes Cluster Autoscaler to the EKS cluster. Configure it to integrate with the existing EC2 Auto Scaling group to automatically launch or terminate nodes based on pending pod demands

[] Enable Amazon EC2 Auto Scaling with custom CloudWatch alarms based on cluster-wide CPU and memory usage to dynamically adjust node count in the EKS worker node group

[] Implement an AWS Lambda function that runs every 10 minutes and checks EKS pod scheduling status. Trigger node scaling manually using the eksctl CLI or AWS SDK if unschedulable pods are detected

Q58: A retail company uses AWS Cloud to manage its technology infrastructure. The company has deployed its consumer-focused web application on Amazon EC2-based web servers and uses Amazon RDS PostgreSQL database as the data store. The PostgreSQL database is set up in a private subnet that allows inbound traffic from selected Amazon EC2 instances. The database also uses AWS Key Management Service (AWS KMS) for encrypting data at rest. Which of the following steps would you recommend to facilitate end-to-end security for the data-in-transit while accessing the database?

[CORRECT] Configure Amazon RDS to use SSL for data in transit

[] Create a new network access control list (network ACL) that blocks SSH from the entire Amazon EC2 subnet into the database

[] Use IAM authentication to access the database instead of the database user's access credentials

[] Create a new security group that blocks SSH from the selected Amazon EC2 instances into the database

Q59: An IT company has a large number of clients opting to build their application programming interface (API) using Docker containers. To facilitate the hosting of these containers, the company is looking at various orchestration services available with AWS. As a Solutions Architect, which of the following solutions will you suggest? (Select two)

- Use Amazon EMR for serverless orchestration of the containerized services
- [CORRECT] Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate for serverless orchestration of the containerized services**
- [CORRECT] Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate for serverless orchestration of the containerized services**
- Use Amazon SageMaker for serverless orchestration of the containerized services
- Use Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 for serverless orchestration of the containerized services

Q60: The engineering team at a leading e-commerce company is anticipating a surge in the traffic because of a flash sale planned for the weekend. You have estimated the web traffic to be 10x. The content of your website is highly dynamic and changes very often. As a Solutions Architect, which of the following options would you recommend to make sure your infrastructure scales for that day?

- Use an Amazon CloudFront distribution in front of your website
- [CORRECT] Use an Auto Scaling Group**
- Use an Amazon Route 53 Multi Value record
- Deploy the website on Amazon S3

Q61: A streaming media company operates a high-traffic content delivery platform on AWS. The application backend is deployed on Amazon EC2 instances within an Auto Scaling group across multiple Availability Zones in a VPC. The team has observed that workloads follow predictable usage patterns, such as higher viewership on weekends and in the evenings, along with occasional real-time spikes due to viral content. To reduce cost and improve responsiveness, the team wants an automated scaling approach that can forecast future demand using historical usage patterns, scale in advance based on those predictions, and react quickly to unplanned usage surges in real time. Which scaling strategy should a solutions architect recommend to meet these requirements?

[] Configure step scaling policies based on EC2 CPU utilization. Use CloudWatch alarms to trigger scaling actions when utilization crosses defined thresholds with incremental adjustments

[CORRECT] Use predictive scaling for the Auto Scaling group to analyze daily and weekly patterns, and configure dynamic scaling with target tracking policies to respond to real-time traffic changes

[] Implement scheduled scaling actions based on pre-defined time windows from historical traffic data. Adjust instance count manually for known high-traffic hours

[] Set up simple scaling policies with longer cooldown periods to avoid rapid scaling. Trigger scale-out events based on average network throughput

Q62: A CRM company has a software as a service (SaaS) application that feeds updates to other in-house and third-party applications. The SaaS application and the in-house applications are being migrated to use AWS services for this inter-application communication. As a Solutions Architect, which of the following would you suggest to asynchronously decouple the architecture?

[] Use Elastic Load Balancing (ELB) for effective decoupling of system architecture

[] Use Amazon Simple Queue Service (Amazon SQS) to decouple the architecture

[] Use Amazon Simple Notification Service (Amazon SNS) to communicate between systems and decouple the architecture

[CORRECT] Use Amazon EventBridge to decouple the system architecture

Q63: A research organization is running a high-performance computing (HPC) workload using Amazon EC2 instances that are distributed across multiple Availability Zones (AZs) within a single AWS Region. The workload requires access to a shared file system with the lowest possible latency for frequent reads and writes. The team decides to use Amazon Elastic File System (Amazon EFS) for its scalability and simplicity. To ensure optimal performance and reduce network latency, the solution architect must design the architecture so that each EC2 instance can access the file system with the least possible delay. Which of the following is the most appropriate solution to meet these requirements?

- [] Use Mountpoint for Amazon S3 to mount an S3 bucket on each EC2 instance and use it as a shared storage layer across Availability Zones
 - [] Create a single EFS mount target in one AZ and allow all EC2 instances in other AZs to access it using the default mount target
 - [] Create mount targets for Amazon EFS on an EC2 instance in each AZ and use them to serve as access points for other instances
- [CORRECT] Create EFS mount targets in each AZ and mount the EFS file system to EC2 instances in the same AZ as the mount target**

Q64: A global insurance company is modernizing its infrastructure by migrating multiple line-of-business applications from its on-premises data centers to AWS. These applications will be deployed across several AWS accounts, all governed under a centralized AWS Organizations structure. The company manages all user identities, groups, and access policies within its on-premises Microsoft Active Directory and wants to continue doing so. The goal is to enable seamless single sign-in across all AWS accounts without duplicating user identity stores or manually provisioning accounts. Which solution best meets these requirements in the most operationally efficient manner?

- [] Enable AWS IAM Identity Center and manually create user accounts and groups within it. Assign these users permission sets in each AWS account. Manage synchronization with on-premises Active Directory using custom PowerShell scripts
 - [] Deploy an OpenLDAP server on Amazon EC2, sync it with the on-premises Active Directory, and integrate it with each AWS account by creating IAM roles that trust the EC2-hosted LDAP server as a SAML provider
- [CORRECT] Deploy AWS IAM Identity Center and configure it to use AWS Directory Service for Microsoft Active Directory (Enterprise Edition). Establish a two-way trust relationship between the managed directory and the on-premises Active Directory to enable federated authentication across all AWS accounts**
- [] Use Amazon Cognito as the primary identity store and create a custom OpenID Connect (OIDC) federation with the on-premises Active Directory. Assign IAM roles using Cognito identity pools and propagate access to multiple AWS accounts using resource policies

Q65: A niche social media application allows users to connect with sports athletes. As a solutions architect, you've designed the architecture of the application to be fully serverless using Amazon API Gateway and AWS Lambda. The backend uses an Amazon DynamoDB table. Some of the star athletes using the application are highly popular, and therefore Amazon DynamoDB has increased the read capacity units (RCUs). Still, the application is experiencing a hot partition problem. What can you do to improve the performance of Amazon DynamoDB and eliminate the hot partition problem without a lot of application refactoring?

- Use Amazon DynamoDB Streams
- [CORRECT] Use Amazon DynamoDB DAX**
- Use Amazon DynamoDB Global Tables
- Use Amazon ElastiCache