

Exam Questions Export

Q1: An Internet of Things (IoT) company would like to have a streaming system that performs real-time analytics on the ingested IoT data. Once the analytics is done, the company would like to send notifications back to the mobile applications of the IoT device owners. As a solutions architect, which of the following AWS technologies would you recommend to send these notifications to the mobile applications?

☐ Amazon Simple Queue Service (Amazon SQS) with Amazon Simple Notification Service (Amazon SNS)

☐ Amazon Kinesis with Amazon Simple Email Service (Amazon SES)

☒ Amazon Kinesis with Amazon Simple Notification Service (Amazon SNS)

☐ Amazon Kinesis with Amazon Simple Queue Service (Amazon SQS)

Q2: A media agency stores its re-creatable assets on Amazon Simple Storage Service (Amazon S3) buckets. The assets are accessed by a large number of users for the first few days and the frequency of access falls down drastically after a week. Although the assets would be accessed occasionally after the first week, but they must continue to be immediately accessible when required. The cost of maintaining all the assets on Amazon S3 storage is turning out to be very expensive and the agency is looking at reducing costs as much as possible. As an AWS Certified Solutions Architect – Associate, can you suggest a way to lower the storage costs while fulfilling the business requirements?

☐ Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 7 days

☐ Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 7 days

☒ Configure a lifecycle policy to transition the objects to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days

☐ Configure a lifecycle policy to transition the objects to Amazon S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days

Q3: The engineering team at an e-commerce company is working on cost optimizations for Amazon Elastic Compute Cloud (Amazon EC2) instances. The team wants to manage the workload using a mix of on-demand and spot instances across multiple instance types. They would like to create an Auto Scaling group with a mix of these instances. Which of the following options would allow the engineering team to provision the instances for this use-case?

[CORRECT] You can only use a launch template to provision capacity across multiple instance types using both On-Demand Instances and Spot Instances to achieve the desired scale, performance, and cost

☐ You can neither use a launch configuration nor a launch template to provision capacity across multiple instance types using both On-Demand Instances and Spot Instances to achieve the desired scale, performance, and cost

☐ You can use a launch configuration or a launch template to provision capacity across multiple instance types using both On-Demand Instances and Spot Instances to achieve the desired scale, performance, and cost

☐ You can only use a launch configuration to provision capacity across multiple instance types using both On-Demand Instances and Spot Instances to achieve the desired scale, performance, and cost

Q4: A company has noticed that its application performance has deteriorated after a new Auto Scaling group was deployed a few days back. Upon investigation, the team found out that the Launch Configuration selected for the Auto Scaling group is using the incorrect instance type that is not optimized to handle the application workflow. As a solutions architect, what would you recommend to provide a long term resolution for this issue?

☐ No need to modify the launch configuration. Just modify the Auto Scaling group to use the correct instance type

[CORRECT] Create a new launch configuration to use the correct instance type. Modify the Auto Scaling group to use this new launch configuration. Delete the old launch configuration as it is no longer needed

☐ No need to modify the launch configuration. Just modify the Auto Scaling group to use more number of existing instance types. More instances may offset the loss of performance

☐ Modify the launch configuration to use the correct instance type and continue to use the existing Auto Scaling group

Q5: An e-commerce company has copied 1 petabyte of data from its on-premises data center to an Amazon S3 bucket in the us-west-1 Region 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 the us-east-1 Region. 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)

[CORRECT] Copy data from the source bucket to the destination bucket using the aws S3 sync command

☐ Set up Amazon S3 Transfer Acceleration (Amazon S3TA) to copy objects across Amazon S3 buckets in different Regions using 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

☐ 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

Q6: A cybersecurity company uses a fleet of Amazon EC2 instances to run a proprietary application. The infrastructure maintenance group at the company wants to be notified via an email whenever the CPU utilization for any of the Amazon EC2 instances breaches a certain threshold. Which of the following services would you use for building a solution with the LEAST amount of development effort? (Select two)

☐ AWS Lambda

☐ AWS Step Functions

[CORRECT] Amazon Simple Notification Service (Amazon SNS)

☐ Amazon Simple Queue Service (Amazon SQS)

[CORRECT] Amazon CloudWatch

Q7: A media company wants a low-latency way to distribute live sports results which are delivered via a proprietary application using UDP protocol. As a solutions architect, which of the following solutions would you recommend such that it offers the BEST performance for this use case?

- ☐ Use Auto Scaling group to provide a low latency way to distribute live sports results
- ☐ Use Elastic Load Balancing (ELB) to provide a low latency way to distribute live sports results
- ☐ Use Amazon CloudFront to provide a low latency way to distribute live sports results

[CORRECT] Use AWS Global Accelerator to provide a low latency way to distribute live sports results

Q8: A company has hired you as an AWS Certified Solutions Architect – Associate to help with redesigning a real-time data processor. The company wants to build custom applications that process and analyze the streaming data for its specialized needs. Which solution will you recommend to address this use-case?

[CORRECT] Use Amazon Kinesis Data Streams to process the data streams as well as decouple the producers and consumers for the real-time data processor

- ☐ Use Amazon Kinesis Data Firehose to process the data streams as well as decouple the producers and consumers for the real-time data processor
- ☐ Use Amazon Simple Queue Service (Amazon SQS) to process the data streams as well as decouple the producers and consumers for the real-time data processor
- ☐ Use Amazon Simple Notification Service (Amazon SNS) to process the data streams as well as decouple the producers and consumers for the real-time data processor

Q9: An IT company wants to review its security best-practices after an incident was reported where a new developer on the team was assigned full access to Amazon DynamoDB. The developer accidentally deleted a couple of tables from the production environment while building out a new feature. Which is the MOST effective way to address this issue so that such incidents do not recur?

- ☐ Remove full database access for all IAM users in the organization

[CORRECT] Use permissions boundary to control the maximum permissions employees can grant to the IAM principals

- ☐ The CTO should review the permissions for each new developer's IAM user so that such incidents don't recur
- ☐ Only root user should have full database access in the organization

Q10: A company has grown from a small startup to an enterprise employing over 1000 people. As the team size has grown, the company has recently observed some strange behavior, with Amazon S3 buckets settings being changed regularly. How can you figure out what's happening without restricting the rights of the users?

[CORRECT] Use AWS CloudTrail to analyze API calls

- ☐ Implement an IAM policy to forbid users to change Amazon S3 bucket settings
- ☐ Implement a bucket policy requiring AWS Multi-Factor Authentication (AWS MFA) for all operations
- ☐ Use Amazon S3 access logs to analyze user access using Athena

Q11: A weather forecast agency collects key weather metrics across multiple cities in the US and sends this data in the form of key-value pairs to AWS Cloud at a one-minute frequency. As a solutions architect, which of the following AWS services would you use to build a solution for processing and then reliably storing this data with high availability? (Select two)

- ☐ Amazon Redshift
- ☐ Amazon RDS

[CORRECT] Amazon DynamoDB

- ☐ Amazon ElastiCache

[CORRECT] AWS Lambda

Q12: A retail company wants to rollout and test a blue-green deployment for its global application in the next 48 hours. Most of the customers use mobile phones which are prone to Domain Name System (DNS) caching. The company has only two days left for the annual Thanksgiving sale to commence. As a Solutions Architect, which of the following options would you recommend to test the deployment on as many users as possible in the given time frame?

- ☐ Use Amazon Route 53 weighted routing to spread traffic across different deployments
- ☐ Use AWS CodeDeploy deployment options to choose the right deployment
- [CORRECT] Use AWS Global Accelerator to distribute a portion of traffic to a particular deployment**
- ☐ Use Elastic Load Balancing (ELB) to distribute traffic across deployments

Q13: A healthcare startup needs to enforce compliance and regulatory guidelines for objects stored in Amazon S3. One of the key requirements is to provide adequate protection against accidental deletion of objects. As a solutions architect, what are your recommendations to address these guidelines? (Select two) ?

☐ Change the configuration on Amazon S3 console so that the user needs to provide additional confirmation while deleting any Amazon S3 object

☐ Create an event trigger on deleting any Amazon S3 object. The event invokes an Amazon Simple Notification Service (Amazon SNS) notification via email to the IT manager

☐ Establish a process to get managerial approval for deleting Amazon S3 objects

[CORRECT] Enable versioning on the Amazon S3 bucket

[CORRECT] Enable multi-factor authentication (MFA) delete on the Amazon S3 bucket

Q14: A social photo-sharing web application is hosted on Amazon Elastic Compute Cloud (Amazon EC2) instances behind an Elastic Load Balancer. The app gives the users the ability to upload their photos and also shows a leaderboard on the homepage of the app. The uploaded photos are stored in Amazon Simple Storage Service (Amazon S3) and the leaderboard data is maintained in Amazon DynamoDB. The Amazon EC2 instances need to access both Amazon S3 and Amazon DynamoDB for these features. As a solutions architect, which of the following solutions would you recommend as the MOST secure option?

[CORRECT] Attach the appropriate IAM role to the Amazon EC2 instance profile so that the instance can access Amazon S3 and Amazon DynamoDB

☐ Save the AWS credentials (access key Id and secret access token) in a configuration file within the application code on the Amazon EC2 instances. Amazon EC2 instances can use these credentials to access Amazon S3 and Amazon DynamoDB

☐ Encrypt the AWS credentials via a custom encryption library and save it in a secret directory on the Amazon EC2 instances. The application code can then safely decrypt the AWS credentials to make the API calls to Amazon S3 and Amazon DynamoDB

☐ Configure AWS CLI on the Amazon EC2 instances using a valid IAM user's credentials. The application code can then invoke shell scripts to access Amazon S3 and Amazon DynamoDB via AWS CLI

Q15: A healthcare company uses its on-premises infrastructure to run legacy applications that require specialized customizations to the underlying Oracle database as well as its host operating system (OS). The company also wants to improve the availability of the Oracle database layer. The company has hired you as an AWS Certified Solutions Architect – Associate to build a solution on AWS that meets these requirements while minimizing the underlying infrastructure maintenance effort. Which of the following options represents the best solution for this use case?

☐ Leverage cross AZ read-replica configuration of Amazon RDS for Oracle that allows the Database Administrator (DBA) to access and customize the database environment and the underlying operating system

☒ Leverage multi-AZ configuration of Amazon RDS Custom for Oracle that allows the Database Administrator (DBA) to access and customize the database environment and the underlying operating system

☐ Deploy the Oracle database layer on multiple Amazon EC2 instances spread across two Availability Zones (AZs). This deployment configuration guarantees high availability and also allows the Database Administrator (DBA) to access and customize the database environment and the underlying operating system

☐ Leverage multi-AZ configuration of Amazon RDS for Oracle that allows the Database Administrator (DBA) to access and customize the database environment and the underlying operating system

Q16: A mobile gaming company is experiencing heavy read traffic to its Amazon Relational Database Service (Amazon RDS) database that retrieves player's scores and stats. The company is using an Amazon RDS database instance type that is not cost-effective for their budget. The company would like to implement a strategy to deal with the high volume of read traffic, reduce latency, and also downsize the instance size to cut costs. Which of the following solutions do you recommend?

☐ Move to Amazon Redshift

☐ Switch application code to AWS Lambda for better performance

☒ Setup Amazon ElastiCache in front of Amazon RDS

☐ Setup Amazon RDS Read Replicas

Q17: A financial services company wants to identify any sensitive data stored on its Amazon S3 buckets. The company also wants to monitor and protect all data stored on Amazon S3 against any malicious activity. As a solutions architect, which of the following solutions would you recommend to help address the given requirements?

[CORRECT] Use Amazon GuardDuty to monitor any malicious activity on data stored in Amazon S3. Use Amazon Macie to identify any sensitive data stored on Amazon S3

☐ Use Amazon GuardDuty to monitor any malicious activity on data stored in Amazon S3 as well as to identify any sensitive data stored on Amazon S3

☐ Use Amazon Macie to monitor any malicious activity on data stored in Amazon S3 as well as to identify any sensitive data stored on Amazon S3

☐ Use Amazon Macie to monitor any malicious activity on data stored in Amazon S3. Use Amazon GuardDuty to identify any sensitive data stored on Amazon S3

Q18: A retail company uses AWS Cloud to manage its IT infrastructure. The company has set up AWS Organizations to manage several departments running their AWS accounts and using resources such as Amazon EC2 instances and Amazon RDS databases. The company wants to provide shared and centrally-managed VPCs to all departments using applications that need a high degree of interconnectivity. As a solutions architect, which of the following options would you choose to facilitate this use-case?

☐ Use VPC peering to share one or more subnets with other AWS accounts belonging to the same parent organization from AWS Organizations

[CORRECT] Use VPC sharing to share one or more subnets with other AWS accounts belonging to the same parent organization from AWS Organizations

☐ Use VPC peering to share a VPC with other AWS accounts belonging to the same parent organization from AWS Organizations

☐ Use VPC sharing to share a VPC with other AWS accounts belonging to the same parent organization from AWS Organizations

Q19: A pharma company is working on developing a vaccine for the COVID-19 virus. The researchers at the company want to process the reference healthcare data in a highly available as well as HIPAA compliant in-memory database that supports caching results of SQL queries. As a solutions architect, which of the following AWS services would you recommend for this task?

[CORRECT] Amazon ElastiCache for Redis/Memcached

- ☐ Amazon DynamoDB Accelerator (DAX)
- ☐ Amazon DynamoDB
- ☐ Amazon DocumentDB

Q20: 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?

- ☐ 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

[CORRECT] Leverage AWS Database Migration Service (AWS DMS) as a bridge between Amazon S3 and 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
- ☐ 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

Q21: A developer needs to implement an AWS Lambda function in AWS account A that accesses an Amazon Simple Storage Service (Amazon S3) bucket in AWS account B. As a Solutions Architect, which of the following will you recommend to meet this requirement?

[CORRECT] Create an IAM role for the AWS Lambda function that grants access to the Amazon S3 bucket. Set the IAM role as the AWS Lambda function's execution role. Make sure that the bucket policy also grants access to the AWS Lambda function's execution role

☐ The Amazon S3 bucket owner should make the bucket public so that it can be accessed by the AWS Lambda function in the other AWS account

☐ Create an IAM role for the AWS Lambda function that grants access to the Amazon S3 bucket. Set the IAM role as the Lambda function's execution role and that would give the AWS Lambda function cross-account access to the Amazon S3 bucket

☐ AWS Lambda cannot access resources across AWS accounts. Use Identity federation to work around this limitation of Lambda

Q22: A media company wants to get out of the business of owning and maintaining its own IT infrastructure. As part of this digital transformation, the media company wants to archive about 5 petabytes of data in its on-premises data center to durable long term storage. As a solutions architect, what is your recommendation to migrate this data in the MOST cost-optimal way?

☐ Setup AWS direct connect between the on-premises data center and AWS Cloud. Use this connection to transfer the data into Amazon S3 Glacier

☐ Setup AWS Site-to-Site VPN connection between the on-premises data center and AWS Cloud. Use this connection to transfer the data into Amazon S3 Glacier

[CORRECT] Transfer the on-premises data into multiple AWS Snowball Edge Storage Optimized devices. Copy the AWS Snowball Edge data into Amazon S3 and create a lifecycle policy to transition the data into Amazon S3 Glacier

☐ Transfer the on-premises data into multiple AWS Snowball Edge Storage Optimized devices. Copy the AWS Snowball Edge data into Amazon S3 Glacier

Q23: 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)

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

[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

☐ 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] 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

[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

Q24: A company manages a multi-tier social media application that runs on Amazon Elastic Compute Cloud (Amazon EC2) instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones (AZs) and use an Amazon Aurora database. As an AWS Certified Solutions Architect – Associate, you have been tasked to make the application more resilient to periodic spikes in request rates. Which of the following solutions would you recommend for the given use-case? (Select two)

☐ Use AWS Global Accelerator

☐ Use AWS Direct Connect

☐ Use AWS Shield

[CORRECT] Use Amazon CloudFront distribution in front of the Application Load Balancer

[CORRECT] Use Amazon Aurora Replica

Q25: 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)

[CORRECT] Amazon S3

- ☐ Amazon Kinesis
- ☐ Amazon Simple Queue Service (Amazon SQS)
- ☐ Amazon Simple Notification Service (Amazon SNS)

[CORRECT] Amazon DynamoDB

Q26: An e-commerce application uses an Amazon Aurora Multi-AZ deployment for its database. While analyzing the performance metrics, the engineering team has found that the database reads are causing high input/output (I/O) and adding latency to the write requests against the database. As an AWS Certified Solutions Architect Associate, what would you recommend to separate the read requests from the write requests?

- ☐ Provision another Amazon Aurora database and link it to the primary database as a read replica
- [CORRECT] Set up a read replica and modify the application to use the appropriate endpoint**
- ☐ Activate read-through caching on the Amazon Aurora database
- ☐ Configure the application to read from the Multi-AZ standby instance

Q27: 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)

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

- ☐ The Amazon Elastic Block Store (Amazon EBS) volumes have been improperly mounted
- ☐ You need to attach elastic IP address (EIP) to the Amazon EC2 instances
- ☐ Your web-app has a runtime that is not supported by the Application Load Balancer

[CORRECT] The route for the health check is misconfigured

Q28: A company wants to store business-critical data on Amazon Elastic Block Store (Amazon EBS) volumes which provide persistent storage independent of Amazon EC2 instances. During a test run, the development team found that on terminating an Amazon EC2 instance, the attached Amazon EBS volume was also lost, which was contrary to their assumptions. As a solutions architect, could you explain this issue?

☐ On termination of an Amazon EC2 instance, all the attached Amazon EBS volumes are always terminated

[CORRECT] The Amazon EBS volume was configured as the root volume of Amazon EC2 instance. On termination of the instance, the default behavior is to also terminate the attached root volume

☐ The Amazon EBS volumes were not backed up on Amazon S3 storage, resulting in the loss of volume

☐ The Amazon EBS volumes were not backed up on Amazon EFS file system storage, resulting in the loss of volume

Q29: 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?

☐ Use Spot Instances

[CORRECT] Use a Cluster placement group

☐ Optimize the Amazon EC2 kernel using EC2 User Data

☐ Use a Spread placement group

Q30: An IT company has an Access Control Management (ACM) application that uses Amazon RDS for MySQL but is running into performance issues despite using Read Replicas. The company has hired you as a solutions architect to address these performance-related challenges without moving away from the underlying relational database schema. The company has branch offices across the world, and it needs the solution to work on a global scale. Which of the following will you recommend as the MOST cost-effective and high-performance solution?

☐ Use Amazon DynamoDB Global Tables to provide fast, local, read and write performance in each region

[CORRECT] Use Amazon Aurora Global Database to enable fast local reads with low latency in each region

☐ Spin up Amazon EC2 instances in each AWS region, install MySQL databases and migrate the existing data into these new databases

☐ Spin up a Amazon Redshift cluster in each AWS region. Migrate the existing data into Redshift clusters

Q31: A financial services firm uses a high-frequency trading system and wants to write the log files into Amazon S3. The system will also read these log files in parallel on a near real-time basis. The engineering team wants to address any data discrepancies that might arise when the trading system overwrites an existing log file and then tries to read that specific log file. Which of the following options BEST describes the capabilities of Amazon S3 relevant to this scenario?

☐ A process replaces an existing object and immediately tries to read it. Until the change is fully propagated, Amazon S3 might return the previous data

[CORRECT] A process replaces an existing object and immediately tries to read it. Amazon S3 always returns the latest version of the object

☐ A process replaces an existing object and immediately tries to read it. Until the change is fully propagated, Amazon S3 might return the new data

☐ A process replaces an existing object and immediately tries to read it. Until the change is fully propagated, Amazon S3 does not return any data

Q32: A media company has created an AWS Direct Connect connection for migrating its flagship application to the AWS Cloud. The on-premises application writes hundreds of video files into a mounted NFS file system daily. Post-migration, the company will host the application on an Amazon EC2 instance with a mounted Amazon Elastic File System (Amazon EFS) file system. Before the migration cutover, the company must build a process that will replicate the newly created on-premises video files to the Amazon EFS file system. Which of the following represents the MOST operationally efficient way to meet this requirement?

☐ Configure an AWS DataSync agent on the on-premises server that has access to the NFS file system. Transfer data over the AWS Direct Connect connection to an AWS VPC peering endpoint for Amazon EFS by using a private VIF. Set up an AWS DataSync scheduled task to send the video files to the Amazon EFS file system every 24 hours

☒ [CORRECT] Configure an AWS DataSync agent on the on-premises server that has access to the NFS file system. Transfer data over the AWS Direct Connect connection to an AWS PrivateLink interface VPC endpoint for Amazon EFS by using a private VIF. Set up an AWS DataSync scheduled task to send the video files to the Amazon EFS file system every 24 hours

☐ Configure an AWS DataSync agent on the on-premises server that has access to the NFS file system. Transfer data over the AWS Direct Connect connection to an Amazon S3 bucket by using a VPC gateway endpoint for Amazon S3. Set up an AWS Lambda function to process event notifications from Amazon S3 and copy the video files from Amazon S3 to the Amazon EFS file system

☐ Configure an AWS DataSync agent on the on-premises server that has access to the NFS file system. Transfer data over the AWS Direct Connect connection to an Amazon S3 bucket by using public VIF. Set up an AWS Lambda function to process event notifications from Amazon S3 and copy the video files from Amazon S3 to the Amazon EFS file system

Q33: A leading social media analytics company is contemplating moving its dockerized application stack into AWS Cloud. The company is not sure about the pricing for using Amazon Elastic Container Service (Amazon ECS) with the EC2 launch type compared to the Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type. Which of the following is correct regarding the pricing for these two services?

☐ Both Amazon ECS with EC2 launch type and Amazon ECS with Fargate launch type are charged based on Amazon EC2 instances and Amazon EBS Elastic Volumes used

☐ Both Amazon ECS with EC2 launch type and Amazon ECS with Fargate launch type are charged based on vCPU and memory resources that the containerized application requests

☐ Both Amazon ECS with EC2 launch type and Amazon ECS with Fargate launch type are just charged based on Elastic Container Service used per hour

[CORRECT] Amazon ECS with EC2 launch type is charged based on EC2 instances and EBS volumes used. Amazon ECS with Fargate launch type is charged based on vCPU and memory resources that the containerized application requests

Q34: 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?

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

☐ 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

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

Q35: A news network uses Amazon Simple Storage Service (Amazon S3) to aggregate the raw video footage from its reporting teams across the US. The news network has recently expanded into new geographies in Europe and Asia. The technical teams at the overseas branch offices have reported huge delays in uploading large video files to the destination Amazon S3 bucket. Which of the following are the MOST cost-effective options to improve the file upload speed into Amazon S3 (Select two)

[CORRECT] Use Amazon S3 Transfer Acceleration (Amazon S3TA) to enable faster file uploads into the destination S3 bucket

[CORRECT] Use multipart uploads for faster file uploads into the destination Amazon S3 bucket

☐ Create multiple AWS Direct Connect connections between the AWS Cloud and branch offices in Europe and Asia. Use the direct connect connections for faster file uploads into Amazon S3

☐ Use AWS Global Accelerator for faster file uploads into the destination Amazon S3 bucket

☐ Create multiple AWS Site-to-Site VPN connections between the AWS Cloud and branch offices in Europe and Asia. Use these VPN connections for faster file uploads into Amazon S3

Q36: A financial services company recently launched an initiative to improve the security of its AWS resources and it had enabled AWS Shield Advanced across multiple AWS accounts owned by the company. Upon analysis, the company has found that the costs incurred are much higher than expected. Which of the following would you attribute as the underlying reason for the unexpectedly high costs for AWS Shield Advanced service?

[CORRECT] Consolidated billing has not been enabled. All the AWS accounts should fall under a single consolidated billing for the monthly fee to be charged only once

☐ Savings Plans has not been enabled for the AWS Shield Advanced service across all the AWS accounts

☐ AWS Shield Advanced also covers AWS Shield Standard plan, thereby resulting in increased costs

☐ AWS Shield Advanced is being used for custom servers, that are not part of AWS Cloud, thereby resulting in increased costs

Q37: A Big Data analytics company wants to set up an AWS cloud architecture that throttles requests in case of sudden traffic spikes. The company is looking for AWS services that can be used for buffering or throttling to handle such traffic variations. Which of the following services can be used to support this requirement?

☐ Amazon Simple Queue Service (Amazon SQS), Amazon Simple Notification Service (Amazon SNS) and AWS Lambda

☐ Amazon Gateway Endpoints, Amazon Simple Queue Service (Amazon SQS) and Amazon Kinesis

☐ Elastic Load Balancer, Amazon Simple Queue Service (Amazon SQS), AWS Lambda

[CORRECT] Amazon API Gateway, Amazon Simple Queue Service (Amazon SQS) and Amazon Kinesis

Q38: 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?

[CORRECT] Amazon Neptune

☐ Amazon OpenSearch Service

☐ Amazon Aurora

☐ Amazon Redshift

Q39: 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 Trusted Advisor checks on Amazon EC2 Reserved Instances to automatically renew reserved instances (RI). AWS Trusted advisor also suggests Amazon RDS idle database instances

[CORRECT] Use AWS Cost Explorer Resource Optimization 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 AWS Compute Optimizer recommendations to help you choose the optimal Amazon EC2 purchasing options and help reserve your instance capacities at reduced costs

☐ 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

Q40: An engineering team wants to examine the feasibility of the user data feature of Amazon EC2 for an upcoming project. Which of the following are true about the Amazon EC2 user data configuration? (Select two)

[CORRECT] By default, scripts entered as user data are executed with root user privileges

[CORRECT] By default, user data runs only during the boot cycle when you first launch an instance

☐ When an instance is running, you can update user data by using root user credentials

☐ By default, user data is executed every time an Amazon EC2 instance is re-started

☐ By default, scripts entered as user data do not have root user privileges for executing

Q41: An Electronic Design Automation (EDA) application produces massive volumes of data that can be divided into two categories. The 'hot data' needs to be both processed and stored quickly in a parallel and distributed fashion. The 'cold data' needs to be kept for reference with quick access for reads and updates at a low cost. Which of the following AWS services is BEST suited to accelerate the aforementioned chip design process?

☐ AWS Glue

☐ Amazon EMR

[CORRECT] Amazon FSx for Lustre

☐ Amazon FSx for Windows File Server

Q42: 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

☐ Store the installation files in Amazon S3 so they can be quickly retrieved

[CORRECT] Use Amazon EC2 user data to customize the dynamic installation parts at boot time

☐ Use Amazon EC2 user data to install the application at boot time

☐ Use AWS Elastic Beanstalk deployment caching feature

Q43: An IT company provides Amazon Simple Storage Service (Amazon S3) bucket access to specific users within the same account for completing project specific work. With changing business requirements, cross-account S3 access requests are also growing every month. The company is looking for a solution that can offer user level as well as account-level access permissions for the data stored in Amazon S3 buckets. As a Solutions Architect, which of the following would you suggest as the MOST optimized way of controlling access for this use-case?

☐ Use Identity and Access Management (IAM) policies

[CORRECT] Use Amazon S3 Bucket Policies

☐ Use Security Groups

☐ Use Access Control Lists (ACLs)

Q44: The engineering team at a company wants to use Amazon Simple Queue Service (Amazon SQS) to decouple components of the underlying application architecture. However, the team is concerned about the VPC-bound components accessing Amazon Simple Queue Service (Amazon SQS) over the public internet. As a solutions architect, which of the following solutions would you recommend to address this use-case?

☐ Use Internet Gateway to access Amazon SQS

☐ Use VPN connection to access Amazon SQS

[CORRECT] Use VPC endpoint to access Amazon SQS

☐ Use Network Address Translation (NAT) instance to access Amazon SQS

Q45: A retail company maintains an AWS Direct Connect connection to AWS and has recently migrated its data warehouse to AWS. The data analysts at the company query the data warehouse using a visualization tool. The average size of a query returned by the data warehouse is 60 megabytes and the query responses returned by the data warehouse are not cached in the visualization tool. Each webpage returned by the visualization tool is approximately 600 kilobytes. Which of the following options offers the LOWEST data transfer egress cost for the company?

☐ Deploy the visualization tool on-premises. Query the data warehouse directly over an AWS Direct Connect connection at a location in the same AWS region

[CORRECT] Deploy the visualization tool in the same AWS region as the data warehouse. Access the visualization tool over a Direct Connect connection at a location in the same region

☐ Deploy the visualization tool on-premises. Query the data warehouse over the internet at a location in the same AWS region

☐ Deploy the visualization tool in the same AWS region as the data warehouse. Access the visualization tool over the internet at a location in the same region

Q46: The engineering team at an e-commerce company wants to migrate from Amazon Simple Queue Service (Amazon SQS) Standard queues to FIFO (First-In-First-Out) queues with batching. As a solutions architect, which of the following steps would you have in the migration checklist? (Select three)

☐ Make sure that the name of the FIFO (First-In-First-Out) queue is the same as the standard queue

[CORRECT] Make sure that the throughput for the target FIFO (First-In-First-Out) queue does not exceed 3,000 messages per second

[CORRECT] Make sure that the name of the FIFO (First-In-First-Out) queue ends with the .fifo suffix

☐ Make sure that the throughput for the target FIFO (First-In-First-Out) queue does not exceed 300 messages per second

[CORRECT] Delete the existing standard queue and recreate it as a FIFO (First-In-First-Out) queue

☐ Convert the existing standard queue into a FIFO (First-In-First-Out) queue

Q47: The business analytics team at a company has been running ad-hoc queries on Oracle and PostgreSQL services on Amazon RDS to prepare daily reports for senior management. To facilitate the business analytics reporting, the engineering team now wants to continuously replicate this data and consolidate these databases into a petabyte-scale data warehouse by streaming data to Amazon Redshift. As a solutions architect, which of the following would you recommend as the MOST resource-efficient solution that requires the LEAST amount of development time without the need to manage the underlying infrastructure?

☐ Use Amazon Kinesis Data Streams to replicate the data from the databases into Amazon Redshift

☐ Use AWS Glue to replicate the data from the databases into Amazon Redshift

☐ Use AWS EMR to replicate the data from the databases into Amazon Redshift

[CORRECT] Use AWS Database Migration Service (AWS DMS) to replicate the data from the databases into Amazon Redshift

Q48: A retail organization is moving some of its on-premises data to AWS Cloud. The DevOps team at the organization has set up an AWS Managed IPSec VPN Connection between their remote on-premises network and their Amazon VPC over the internet. Which of the following represents the correct configuration for the IPSec VPN Connection?

☐ Create a virtual private gateway (VGW) on the on-premises side of the VPN and a Customer Gateway on the AWS side of the VPN

[CORRECT] Create a virtual private gateway (VGW) on the AWS side of the VPN and a Customer Gateway on the on-premises side of the VPN

☐ Create a Customer Gateway on both the AWS side of the VPN as well as the on-premises side of the VPN

☐ Create a virtual private gateway (VGW) on both the AWS side of the VPN as well as the on-premises side of the VPN

Q49: A financial services company has deployed its flagship application on Amazon EC2 instances. Since the application handles sensitive customer data, the security team at the company wants to ensure that any third-party Secure Sockets Layer certificate (SSL certificate) SSL/Transport Layer Security (TLS) certificates configured on Amazon EC2 instances via the AWS Certificate Manager (ACM) are renewed before their expiry date. The company has hired you as an AWS Certified Solutions Architect Associate to build a solution that notifies the security team 30 days before the certificate expiration. The solution should require the least amount of scripting and maintenance effort. What will you recommend?

☐ Monitor the days to expiry Amazon CloudWatch metric for certificates created via ACM. Create a CloudWatch alarm to monitor such certificates based on the days to expiry metric and then trigger a custom action of notifying the security team

[CORRECT] Leverage AWS Config managed rule to check if any third-party SSL/TLS certificates imported into ACM are marked for expiration within 30 days. Configure the rule to trigger an Amazon SNS notification to the security team if any certificate expires within 30 days

☐ Leverage AWS Config managed rule to check if any SSL/TLS certificates created via ACM are marked for expiration within 30 days. Configure the rule to trigger an Amazon SNS notification to the security team if any certificate expires within 30 days

☐ Monitor the days to expiry Amazon CloudWatch metric for certificates imported into ACM. Create a CloudWatch alarm to monitor such certificates based on the days to expiry metric and then trigger a custom action of notifying the security team

Q50: A retail company uses Amazon Elastic Compute Cloud (Amazon EC2) instances, Amazon API Gateway, Amazon RDS, Elastic Load Balancer and Amazon CloudFront services. To improve the security of these services, the Risk Advisory group has suggested a feasibility check for using the Amazon GuardDuty service. Which of the following would you identify as data sources supported by Amazon GuardDuty?

- ☐ VPC Flow Logs, Amazon API Gateway logs, Amazon S3 access logs
- ☒ VPC Flow Logs, Domain Name System (DNS) logs, AWS CloudTrail events**
- ☐ Elastic Load Balancing logs, Domain Name System (DNS) logs, AWS CloudTrail events
- ☐ Amazon CloudFront logs, Amazon API Gateway logs, AWS CloudTrail events

Q51: You have been hired as a Solutions Architect to advise a company on the various authentication/authorization mechanisms that AWS offers to authorize an API call within the Amazon API Gateway. The company would prefer a solution that offers built-in user management. Which of the following solutions would you suggest as the best fit for the given use-case?

- ☐ Use AWS_IAM authorization
- ☒ Use Amazon Cognito User Pools**
- ☐ Use Amazon Cognito Identity Pools
- ☐ Use AWS Lambda authorizer for Amazon API Gateway

Q52: A financial services company is looking to move its on-premises IT infrastructure to AWS Cloud. The company has multiple long-term server bound licenses across the application stack and the CTO wants to continue to utilize those licenses while moving to AWS. As a solutions architect, which of the following would you recommend as the MOST cost-effective solution?

- ☒ Use Amazon EC2 dedicated hosts**
- ☐ Use Amazon EC2 dedicated instances
- ☐ Use Amazon EC2 on-demand instances
- ☐ Use Amazon EC2 reserved instances (RI)

Q53: The DevOps team at an IT company is provisioning a two-tier application in a VPC with a public subnet and a private subnet. The team wants to use either a Network Address Translation (NAT) instance or a Network Address Translation (NAT) gateway in the public subnet to enable instances in the private subnet to initiate outbound IPv4 traffic to the internet but needs some technical assistance in terms of the configuration options available for the Network Address Translation (NAT) instance and the Network Address Translation (NAT) gateway. As a solutions architect, which of the following options would you identify as CORRECT? (Select three)

[CORRECT] NAT instance can be used as a bastion server

☐ NAT gateway can be used as a bastion server

[CORRECT] NAT instance supports port forwarding

☐ NAT gateway supports port forwarding

[CORRECT] Security Groups can be associated with a NAT instance

☐ Security Groups can be associated with a NAT gateway

Q54: An organization wants to delegate access to a set of users from the development environment so that they can access some resources in the production environment which is managed under another AWS account. As a solutions architect, which of the following steps would you recommend?

☐ Both IAM roles and IAM users can be used interchangeably for cross-account access

[CORRECT] Create a new IAM role with the required permissions to access the resources in the production environment. The users can then assume this IAM role while accessing the resources from the production environment

☐ It is not possible to access cross-account resources

☐ Create new IAM user credentials for the production environment and share these credentials with the set of users from the development environment

Q55: A cyber security company is running a mission critical application using a single Spread placement group of Amazon EC2 instances. The company needs 15 Amazon EC2 instances for optimal performance. How many Availability Zones (AZs) will the company need to deploy these Amazon EC2 instances per the given use-case?

☐ 7

[CORRECT] 3

☐ 14

☐ 15

Q56: A retail company has developed a REST API which is deployed in an Auto Scaling group behind an Application Load Balancer. The REST API stores the user data in Amazon DynamoDB and any static content, such as images, are served via Amazon Simple Storage Service (Amazon S3). On analyzing the usage trends, it is found that 90% of the read requests are for commonly accessed data across all users. As a Solutions Architect, which of the following would you suggest as the MOST efficient solution to improve the application performance?

☐ Enable ElastiCache Redis for DynamoDB and Amazon CloudFront for Amazon S3

[CORRECT] Enable Amazon DynamoDB Accelerator (DAX) for Amazon DynamoDB and Amazon CloudFront for Amazon S3

☐ Enable Amazon DynamoDB Accelerator (DAX) for Amazon DynamoDB and ElastiCache Memcached for Amazon S3

☐ Enable ElastiCache Redis for DynamoDB and ElastiCache Memcached for Amazon S3

Q57: The infrastructure team at a company maintains 5 different VPCs (let's call these VPCs A, B, C, D, E) for resource isolation. Due to the changed organizational structure, the team wants to interconnect all VPCs together. To facilitate this, the team has set up VPC peering connection between VPC A and all other VPCs in a hub and spoke model with VPC A at the center. However, the team has still failed to establish connectivity between all VPCs. As a solutions architect, which of the following would you recommend as the MOST resource-efficient and scalable solution?

☐ Establish VPC peering connections between all VPCs

☐ Use an internet gateway to interconnect the VPCs

☐ Use a VPC endpoint to interconnect the VPCs

[CORRECT] Use AWS transit gateway to interconnect the VPCs

Q58: A development team has deployed a microservice to the Amazon Elastic Container Service (Amazon ECS). The application layer is in a Docker container that provides both static and dynamic content through an Application Load Balancer. With increasing load, the Amazon ECS cluster is experiencing higher network usage. The development team has looked into the network usage and found that 90% of it is due to distributing static content of the application. As a Solutions Architect, what do you recommend to improve the application's network usage and decrease costs?

☐ Distribute the static content through Amazon EFS

☐ Distribute the dynamic content through Amazon EFS

[CORRECT] Distribute the static content through Amazon S3

☐ Distribute the dynamic content through Amazon S3

Q59: A company has a license-based, expensive, legacy commercial database solution deployed at its on-premises data center. The company wants to migrate this database to a more efficient, open-source, and cost-effective option on AWS Cloud. The CTO at the company wants a solution that can handle complex database configurations such as secondary indexes, foreign keys, and stored procedures. As a solutions architect, which of the following AWS services should be combined to handle this use-case? (Select two)

[CORRECT] AWS Schema Conversion Tool (AWS SCT)

☐ Basic Schema Copy

[CORRECT] AWS Database Migration Service (AWS DMS)

☐ AWS Snowball Edge

☐ AWS Glue

Q60: A leading online gaming company is migrating its flagship application to AWS Cloud for delivering its online games to users across the world. The company would like to use a Network Load Balancer to handle millions of requests per second. The engineering team has provisioned multiple instances in a public subnet and specified these instance IDs as the targets for the NLB. As a solutions architect, can you help the engineering team understand the correct routing mechanism for these target instances?

☐ Traffic is routed to instances using the primary elastic IP address specified in the primary network interface for the instance

[CORRECT] Traffic is routed to instances using the primary private IP address specified in the primary network interface for the instance

☐ Traffic is routed to instances using the instance ID specified in the primary network interface for the instance

☐ Traffic is routed to instances using the primary public IP address specified in the primary network interface for the instance

Q61: A pharmaceutical company is considering moving to AWS Cloud to accelerate the research and development process. Most of the daily workflows would be centered around running batch jobs on Amazon EC2 instances with storage on Amazon Elastic Block Store (Amazon EBS) volumes. The CTO is concerned about meeting HIPAA compliance norms for sensitive data stored on Amazon EBS. Which of the following options outline the correct capabilities of an encrypted Amazon EBS volume? (Select three)

☐ Data moving between the volume and the instance is NOT encrypted

[CORRECT] Any snapshot created from the volume is encrypted

☐ Any snapshot created from the volume is NOT encrypted

[CORRECT] Data moving between the volume and the instance is encrypted

☐ Data at rest inside the volume is NOT encrypted

[CORRECT] Data at rest inside the volume is encrypted

Q62: A media company has its corporate headquarters in Los Angeles with an on-premises data center using an AWS Direct Connect connection to the AWS VPC. The branch offices in San Francisco and Miami use AWS Site-to-Site VPN connections to connect to the AWS VPC. The company is looking for a solution to have the branch offices send and receive data with each other as well as with their corporate headquarters. As a solutions architect, which of the following AWS services would you recommend addressing this use-case?

☐ Software VPN

☐ VPC Peering connection

☐ VPC Endpoint

[CORRECT] AWS VPN CloudHub

Q63: An IT company has built a custom data warehousing solution for a retail organization by using Amazon Redshift. As part of the cost optimizations, the company wants to move any historical data (any data older than a year) into Amazon S3, as the daily analytical reports consume data for just the last one year. However the analysts want to retain the ability to cross-reference this historical data along with the daily reports. The company wants to develop a solution with the LEAST amount of effort and MINIMUM cost. As a solutions architect, which option would you recommend to facilitate this use-case?

☐ Use the Amazon Redshift COPY command to load the Amazon S3 based historical data into Amazon Redshift. Once the ad-hoc queries are run for the historic data, it can be removed from Amazon Redshift

☐ Setup access to the historical data via Amazon Athena. The analytics team can run historical data queries on Amazon Athena and continue the daily reporting on Amazon Redshift. In case the reports need to be cross-referenced, the analytics team need to export these in flat files and then do further analysis

[CORRECT] Use Amazon Redshift Spectrum to create Amazon Redshift cluster tables pointing to the underlying historical data in Amazon S3. The analytics team can then query this historical data to cross-reference with the daily reports from Redshift

☐ Use AWS Glue ETL job to load the Amazon S3 based historical data into Redshift. Once the ad-hoc queries are run for the historic data, it can be removed from Amazon Redshift

Q64: A big data analytics company is using Amazon Kinesis Data Streams (KDS) to process IoT data from the field devices of an agricultural sciences company. Multiple consumer applications are using the incoming data streams and the engineers have noticed a performance lag for the data delivery speed between producers and consumers of the data streams. As a solutions architect, which of the following would you recommend for improving the performance for the given use-case?

☐ Swap out Amazon Kinesis Data Streams with Amazon SQS Standard queues

☐ Swap out Amazon Kinesis Data Streams with Amazon SQS FIFO queues

☐ Swap out Amazon Kinesis Data Streams with Amazon Kinesis Data Firehose

[CORRECT] Use Enhanced Fanout feature of Amazon Kinesis Data Streams

Q65: A medium-sized business has a taxi dispatch application deployed on an Amazon EC2 instance. Because of an unknown bug, the application causes the instance to freeze regularly. Then, the instance has to be manually restarted via the AWS management console. Which of the following is the MOST cost-optimal and resource-efficient way to implement an automated solution until a permanent fix is delivered by the development team?

☐ Use Amazon EventBridge events to trigger an AWS Lambda function to check the instance status every 5 minutes. In the case of Instance Health Check failure, the AWS lambda function can use Amazon EC2 API to reboot the instance

[CORRECT] Setup an Amazon CloudWatch alarm to monitor the health status of the instance. In case of an Instance Health Check failure, an EC2 Reboot CloudWatch Alarm Action can be used to reboot the instance

☐ Setup an Amazon CloudWatch alarm to monitor the health status of the instance. In case of an Instance Health Check failure, Amazon CloudWatch Alarm can publish to an Amazon Simple Notification Service (Amazon SNS) event which can then trigger an AWS lambda function. The AWS lambda function can use Amazon EC2 API to reboot the instance

☐ Use Amazon EventBridge events to trigger an AWS Lambda function to reboot the instance status every 5 minutes