Exam Questions Export

Q1: A healthcare company has deployed its web application on Amazon Elastic Container Service (Amazon ECS) container instances running behind an Application Load Balancer. The website slows down when the traffic spikes and the website availability is also reduced. The development team has configured Amazon CloudWatch alarms to receive notifications whenever there is an availability constraint so the team can scale out resources. The company wants an automated solution to respond to such events. Which of the following addresses the given use case?

[ ] Configure AWS Auto Scaling to scale out the Amazon ECS cluster when the Application Load Balancer's target group's CPU utilization rises above a threshold

[ ] Configure AWS Auto Scaling to scale out the Amazon ECS cluster when the CloudWatch alarm's CPU utilization rises above a threshold

[ ] Configure AWS Auto Scaling to scale out the Amazon ECS cluster when the Application Load Balancer's CPU utilization rises above a threshold

[CORRECT] Configure AWS Auto Scaling to scale out the Amazon ECS cluster when the ECS service's CPU utilization rises above a threshold

Q2: A company has a hybrid cloud structure for its on-premises data center and AWS Cloud infrastructure. The company wants to build a web log archival solution such that only the most frequently accessed logs are available as cached data locally while backing up all logs on Amazon S3. As a solutions architect, which of the following solutions would you recommend for this use-case?

[ ] Use AWS Direct Connect to store the most frequently accessed logs locally for low-latency access while storing the full backup of logs in an Amazon S3 bucket

[CORRECT] Use AWS Volume Gateway - Cached Volume - to store the most frequently accessed logs locally for low-latency access while storing the full volume with all logs in its Amazon S3 service bucket

[ ] Use AWS Volume Gateway - Stored Volume - to store the most frequently accessed logs locally for low-latency access while storing the full volume with all logs in its Amazon S3 service bucket

[ ] Use AWS Snowball Edge Storage Optimized device to store the most frequently accessed logs locally for low-latency access while storing the full backup of logs in an Amazon S3 bucket

Q3: 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

[ ] 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

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

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

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

Q4: A retail company has connected its on-premises data center to the AWS Cloud via AWS Direct Connect. The company wants to be able to resolve Domain Name System (DNS) queries for any resources in the on-premises network from the AWS VPC and also resolve any DNS queries for resources in the AWS VPC from the on-premises network. As a solutions architect, which of the following solutions can be combined to address the given use case? (Select two)

[ ] Create a universal endpoint on Amazon Route 53 Resolver and then Amazon Route 53 Resolver can receive and forward queries to resolvers on the on-premises network via this endpoint

[ ] Create an outbound endpoint on Amazon Route 53 Resolver and then DNS resolvers on the on-premises network can forward DNS queries to Amazon Route 53 Resolver via this endpoint

[CORRECT] Create an inbound endpoint on Amazon Route 53 Resolver and then DNS resolvers on the on-premises network can forward DNS queries to Amazon Route 53 Resolver via this endpoint

[CORRECT] Create an outbound endpoint on Amazon Route 53 Resolver and then Amazon Route 53 Resolver can conditionally forward queries to resolvers on the on-premises network via this endpoint

[ ] Create an inbound endpoint on Amazon Route 53 Resolver and then Amazon Route 53 Resolver can conditionally forward queries to resolvers on the on-premises network via this endpoint

Q5: A financial services company has recently migrated from on-premises infrastructure to AWS Cloud. The DevOps team wants to implement a solution that allows all resource configurations to be reviewed and make sure that they meet compliance guidelines. Also, the solution should be able to offer the capability to look into the resource configuration history across the application stack. As a solutions architect, which of the following solutions would you recommend to the team?

[ ] Use Amazon CloudWatch to review resource configurations to meet compliance guidelines and maintain a history of resource configuration changes

[ ] Use AWS Systems Manager to review resource configurations to meet compliance guidelines and maintain a history of resource configuration changes

[ ] Use AWS CloudTrail to review resource configurations to meet compliance guidelines and maintain a history of resource configuration changes

[CORRECT] Use AWS Config to review resource configurations to meet compliance guidelines and maintain a history of resource configuration changes

Q6: An engineering team wants to orchestrate multiple Amazon ECS task types running on Amazon EC2 instances that are part of the Amazon ECS cluster. The output and state data for all tasks need to be stored. The amount of data output by each task is approximately 20 megabytes and there could be hundreds of tasks running at a time. As old outputs are archived, the storage size is not expected to exceed 1 terabyte. As a solutions architect, which of the following would you recommend as an optimized solution for high-frequency reading and writing?

[ ] Use Amazon EFS with Bursting Throughput mode

[CORRECT] Use Amazon EFS with Provisioned Throughput mode

[ ] Use Amazon DynamoDB table that is accessible by all ECS cluster instances

[ ] Use an Amazon EBS volume mounted to the Amazon ECS cluster instances

Q7: A company is transferring a significant volume of data from on-site storage to AWS, where it will be accessed by Windows, Mac, and Linux-based Amazon EC2 instances within the same AWS region using both SMB and NFS protocols. Part of this data will be accessed regularly, while the rest will be accessed less frequently. The company requires a hosting solution for this data that minimizes operational overhead. What solution would best meet these requirements?

[CORRECT] Set up an Amazon FSx for ONTAP instance. Configure an FSx for ONTAP file system on the root volume and migrate the data to the FSx for ONTAP volume

[ ] Set up an Amazon Elastic File System (Amazon EFS) volume that uses EFS Infrequent Access. Use AWS DataSync to migrate the data to the EFS volume

[ ] Set up an Amazon FSx for OpenZFS instance. Configure an FSx for OpenZFS file ystem on the root volume and migrate the data to the FSx for OpenZFS volume

[ ] Set up an Amazon Elastic File System (Amazon EFS) volume that uses EFS Intelligent-Tiering. Use AWS DataSync to migrate the data to the EFS volume

Q8: A company wants to improve its gaming application by adding a leaderboard that uses a complex proprietary algorithm based on the participating user's performance metrics to identify the top users on a real-time basis. The technical requirements mandate high elasticity, low latency, and real-time processing to deliver customizable user data for the community of users. The leaderboard would be accessed by millions of users simultaneously. Which of the following options support the case for using Amazon ElastiCache to meet the given requirements? (Select two)

[CORRECT] Use Amazon ElastiCache to improve latency and throughput for read-heavy application workloads

[CORRECT] Use Amazon ElastiCache to improve the performance of compute-intensive workloads

[ ] Use Amazon ElastiCache to improve latency and throughput for write-heavy application workloads

[ ] Use Amazon ElastiCache to run highly complex JOIN queries

[ ] Use Amazon ElastiCache to improve the performance of Extract-Transform-Load (ETL) workloads

Q9: The DevOps team at an IT company has recently migrated to AWS and they are configuring security groups for their two-tier application with public web servers and private database servers. The team wants to understand the allowed configuration options for an inbound rule for a security group. As a solutions architect, which of the following would you identify as an INVALID option for setting up such a configuration?

[ ] You can use an IP address as the custom source for the inbound rule

[ ] You can use a range of IP addresses in CIDR block notation as the custom source for the inbound rule

[CORRECT] You can use an Internet Gateway ID as the custom source for the inbound rule

[ ] You can use a security group as the custom source for the inbound rule

Q10: A national logistics company has a dedicated AWS Direct Connect connection from its corporate data center to AWS. Within its AWS account, the company operates 25 Amazon VPCs in the same Region, each supporting different regional distribution services. The VPCs were configured with non-overlapping CIDR blocks and currently use private VIFs for Direct Connect access to on-premises resources. As the architecture scales, the company wants to enable communication across all VPCs and the on-premises environment. The solution must scale efficiently, support full-mesh connectivity, and reduce the complexity of maintaining separate private VIFs for each VPC. Which combination of solutions will best fulfill these requirements with the least amount of operational overhead? (Select two)

[ ] Convert each existing private VIF into a new Direct Connect gateway association by attaching a virtual private gateway (VGW) to each VPC. Manually configure routing between VGWs

[ ] Reconfigure each VPC to connect through AWS PrivateLink endpoints to a central networking service VPC. Share the service with other VPCs using VPC endpoint services

[CORRECT] Create a transit virtual interface (VIF) from the Direct Connect connection and associate it with the transit gateway

[CORRECT] Create an AWS Transit Gateway and attach all 25 VPCs to it. Enable route propagation for each attachment to automatically manage inter-VPC routing

[ ] Create individual Site-to-Site VPN connections from the data center to each VPC. Set up BGP route propagation for every tunnel to facilitate on-premises-to-VPC routing

Q11: An e-commerce company has deployed its application on several Amazon EC2 instances that are configured in a private subnet using IPv4. These Amazon EC2 instances read and write a huge volume of data to and from Amazon S3 in the same AWS region. The company has set up subnet routing to direct all the internet-bound traffic through a Network Address Translation gateway (NAT gateway). The company wants to build the most cost-optimal solution without impacting the application's ability to communicate with Amazon S3 or the internet. As an AWS Certified Solutions Architect Associate, which of the following would you recommend?

[ ] Set up an egress-only internet gateway in the public subnet. Update the route table in the private subnet to route traffic to the internet gateway. Update the network ACL to allow the S3-bound traffic

[ ] Provision an internet gateway. Update the route table in the private subnet to route traffic to the internet gateway. Update the network ACL (NACL) to allow the S3-bound traffic

[CORRECT] Set up a VPC gateway endpoint for Amazon S3. Attach an endpoint policy to the endpoint. Update the route table to direct the S3-bound traffic to the VPC endpoint

[ ] Set up a Gateway Load Balancer (GWLB) endpoint for Amazon S3. Update the route table in the private subnet to direct the S3-bound traffic via the Gateway Load Balancer (GWLB) endpoint

Q12: A regional transportation authority operates a high-traffic public information portal hosted on AWS. The backend consists of Amazon EC2 instances behind an Application Load Balancer (ALB). In recent weeks, the operations team has observed intermittent slowdowns and performance issues. After investigation, the team suspect the application is being targeted by distributed denial-of-service (DDoS) attacks coming from a wide range of IP addresses. The team needs a solution that provides DDoS mitigation, detailed logs for audit purposes, and requires minimal changes to the existing architecture. Which solution best addresses these needs?

[ ] Enable Amazon Inspector for the EC2 instances. Use its vulnerability findings to detect potential DDoS attack vectors and patch the EC2 environments accordingly

[CORRECT] Subscribe to AWS Shield Advanced to gain proactive DDoS protection. Engage the AWS DDoS Response Team (DRT) to analyze traffic patterns and apply mitigations. Use the built-in logging and reporting to maintain an audit trail of detected events

[ ] Deploy Amazon GuardDuty and integrate with the EC2 environment. Use GuardDuty findings to manually block suspected IP addresses at the ALB level or within EC2 security groups

[ ] Create an Amazon CloudFront distribution in front of the ALB. Enable AWS WAF on the distribution and configure custom rules to filter traffic from known malicious IP ranges and geographies. Use CloudFront access logs for analysis

Q13: A media startup is looking at hosting their web application on AWS Cloud. The application will be accessed by users from different geographic regions of the world to upload and download video files that can reach a maximum size of 10 gigabytes. The startup wants the solution to be cost-effective and scalable with the lowest possible latency for a great user experience. As a Solutions Architect, which of the following will you suggest as an optimal solution to meet the given requirements?

[ ] Use Amazon EC2 with Amazon ElastiCache for faster distribution of content, while Amazon S3 can be used as a storage service

[ ] Use Amazon S3 for hosting the web application and use Amazon CloudFront for faster distribution of content to geographically dispersed users

[CORRECT] Use Amazon S3 for hosting the web application and use Amazon S3 Transfer Acceleration (Amazon S3TA) to reduce the latency that geographically dispersed users might face

[ ] Use Amazon EC2 with AWS Global Accelerator for faster distribution of content, while using Amazon S3 as storage service

Q14: A healthcare startup is modernizing its monolithic Python-based analytics application by transitioning to a microservices architecture on AWS. As a pilot, the team wants to refactor one module into a standalone microservice that can handle hundreds of requests per second. They are seeking an AWS-native solution that supports Python, scales automatically with traffic, and requires minimal infrastructure management and operational overhead to build, test, and deploy the service efficiently. Which AWS solution best meets these requirements?

[ ] Use Amazon EC2 Spot Instances in an Auto Scaling group. Launch the Python application as a background service and install all required dependencies at instance startup

[CORRECT] Use AWS Lambda to run the Python-based microservice. Integrate it with Amazon API Gateway for HTTP access and enable provisioned concurrency for performance during peak loads

[ ] Use AWS App Runner to build and deploy the Python application directly from a GitHub repository. Allow App Runner to manage traffic scaling and deployments

[ ] Deploy the microservice in an AWS Fargate task using Amazon ECS. Package the code in a Docker container image with a Python runtime and configure ECS Service Auto Scaling to respond to CPU utilization metrics

Q15: A company has its application servers in the public subnet that connect to the database instances in the private subnet. For regular maintenance, the database instances need patch fixes that need to be downloaded from the internet. Considering the company uses only IPv4 addressing and is looking for a fully managed service, which of the following would you suggest as an optimal solution?

[ ] Configure a Network Address Translation instance (NAT instance) in the public subnet of the VPC

[ ] Configure the Internet Gateway of the VPC to be accessible to the private subnet resources by changing the route tables

[ ] Configure an Egress-only internet gateway for the resources in the private subnet of the VPC

[CORRECT] Configure a Network Address Translation gateway (NAT gateway) in the public subnet of the VPC

Q16: A big data analytics company is working on a real-time vehicle tracking solution. The data processing workflow involves both I/O intensive and throughput intensive database workloads. The development team needs to store this real-time data in a NoSQL database hosted on an Amazon EC2 instance and needs to support up to 25,000 IOPS per volume. As a solutions architect, which of the following Amazon Elastic Block Store (Amazon EBS) volume types would you recommend for this use-case?

[ ] General Purpose SSD (gp2)

[CORRECT] Provisioned IOPS SSD (io1)

[ ] Throughput Optimized HDD (st1)

[ ] Cold HDD (sc1)

Q17: 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?

[ ] 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

[ ] 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

[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

Q18: A gaming company uses Application Load Balancers in front of Amazon EC2 instances for different services and microservices. The architecture has now become complex with too many Application Load Balancers in multiple AWS Regions. Security updates, firewall configurations, and traffic routing logic have become complex with too many IP addresses and configurations. The company is looking at an easy and effective way to bring down the number of IP addresses allowed by the firewall and easily manage the entire network infrastructure. Which of these options represents an appropriate solution for this requirement?

[ ] Set up a Network Load Balancer with elastic IP address. Register the private IPs of all the Application Load Balancers as targets of this Network Load Balancer

[ ] Assign an Elastic IP to an Auto Scaling Group (ASG), and set up multiple Amazon EC2 instances to run behind the Auto Scaling Groups, for each of the Regions

[CORRECT] Launch AWS Global Accelerator and create endpoints for all the Regions. Register the Application Load Balancers of each Region to the corresponding endpoints

[ ] Configure Elastic IPs for each of the Application Load Balancers in each Region

Q19: An application running on an Amazon EC2 instance needs to access a Amazon DynamoDB table in the same AWS account. Which of the following solutions should a solutions architect configure for the necessary permissions?

[ ] Set up an IAM user with the appropriate permissions to allow access to the Amazon DynamoDB table. Store the access credentials in an Amazon S3 bucket and read them from within the application code directly

[ ] Set up an IAM user with the appropriate permissions to allow access to the Amazon DynamoDB table. Store the access credentials in the local storage and read them from within the application code directly

[ ] Set up an IAM service role with the appropriate permissions to allow access to the Amazon DynamoDB table. Add the Amazon EC2 instance to the trust relationship policy document so that the instance can assume the role

[CORRECT] Set up an IAM service role with the appropriate permissions to allow access to the Amazon DynamoDB table. Configure an instance profile to assign this IAM role to the Amazon EC2 instance

Q20: Your application is hosted by a provider on yourapp.provider.com. You would like to have your users access your application using www.your-domain.com, which you own and manage under Amazon Route 53. Which Amazon Route 53 record should you create?

[CORRECT] Create a CNAME record

[ ] Create an A record

[ ] Create a PTR record

[ ] Create an Alias Record

Q21: An online gaming application has a large chunk of its traffic coming from users who download static assets such as historic leaderboard reports and the game tactics for various games. The current infrastructure and design are unable to cope up with the traffic and application freezes on most of the pages. Which of the following is a cost-optimal solution that does not need provisioning of infrastructure?

[ ] Use Amazon CloudFront with Amazon DynamoDB for greater speed and low latency access to static assets

[CORRECT] Use Amazon CloudFront with Amazon S3 as the storage solution for the static assets

[ ] Configure AWS Lambda with an Amazon RDS database to provide a serverless architecture

[ ] Use AWS Lambda with Amazon ElastiCache and Amazon RDS for serving static assets at high speed and low latency

Q22: An e-commerce company is using Elastic Load Balancing (ELB) for its fleet of Amazon EC2 instances spread across two Availability Zones (AZs), with one instance as a target in Availability Zone A and four instances as targets in Availability Zone B. The company is doing benchmarking for server performance when cross-zone load balancing is enabled compared to the case when cross-zone load balancing is disabled. As a solutions architect, which of the following traffic distribution outcomes would you identify as correct?

[ ] With cross-zone load balancing enabled, one instance in Availability Zone A receives no traffic and four instances in Availability Zone B receive 25% traffic each. With cross-zone load balancing disabled, one instance in Availability Zone A receives 50% traffic and four instances in Availability Zone B receive 12.5% traffic each

[ ] With cross-zone load balancing enabled, one instance in Availability Zone A receives 20% traffic and four instances in Availability Zone B receive 20% traffic each. With cross-zone load balancing disabled, one instance in Availability Zone A receives no traffic and four instances in Availability Zone B receive 25% traffic each

[ ] With cross-zone load balancing enabled, one instance in Availability Zone A receives 50% traffic and four instances in Availability Zone B receive 12.5% traffic each. With cross-zone load balancing disabled, one instance in Availability Zone A receives 20% traffic and four instances in Availability Zone B receive 20% traffic each

[CORRECT] With cross-zone load balancing enabled, one instance in Availability Zone A receives 20% traffic and four instances in Availability Zone B receive 20% traffic each. With cross-zone load balancing disabled, one instance in Availability Zone A receives 50% traffic and four instances in Availability Zone B receive 12.5% traffic each

Q23: A financial services firm runs a containerized risk analytics tool in its on-premises data center using Docker. The tool depends on persistent data storage for maintaining customer simulation results and operates on a single host machine where the volume is locally mounted. The infrastructure team is looking to replatform the tool to AWS using a fully managed service because they want to avoid managing EC2 instances, volumes, or underlying servers. Which AWS solution best meets these requirements?

[ ] Use Amazon EKS with managed node groups. Provision an Amazon EBS volume and mount it inside the container by creating a Kubernetes persistent volume and claim. Manage storage lifecycle manually

[ ] Use AWS Lambda with a container image runtime. Store stateful data in temporary local storage (/tmp) and sync with Amazon S3 periodically

[ ] Use Amazon ECS with Fargate launch type. Attach an Amazon S3 bucket using a shared access script that mounts the S3 bucket into the container for data storage

[CORRECT] Use Amazon ECS with Fargate launch type. Provision an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS volume inside the container at runtime to provide persistent storage access

Q24: 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

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

Q25: A global pharmaceutical company wants to move most of the on-premises data into Amazon S3, Amazon Elastic File System (Amazon EFS), and Amazon FSx for Windows File Server easily, quickly, and cost-effectively. As a solutions architect, which of the following solutions would you recommend as the BEST fit to automate and accelerate online data transfers to these AWS storage services?

[ ] Use AWS Transfer Family to automate and accelerate online data transfers to the given AWS storage services

[ ] Use File Gateway to automate and accelerate online data transfers to the given AWS storage services

[CORRECT] Use AWS DataSync to automate and accelerate online data transfers to the given AWS storage services

[ ] Use AWS Snowball Edge Storage Optimized device to automate and accelerate online data transfers to the given AWS storage services

Q26: A financial services company is modernizing its analytics platform on AWS. Their legacy data processing scripts, built for both Windows and Linux environments, require shared access to a file system that supports Windows ACLs and SMB protocol for compatibility with existing Windows workloads. At the same time, their Linux-based applications need to read from and write to the same shared storage to maintain cross-platform consistency. The solutions architect needs to design a storage solution that allows both Windows and Linux EC2 instances to access the shared file system simultaneously, while preserving Windows-specific features like NTFS permissions and Active Directory (AD) integration. Which solution will best meet these requirements?

[ ] Deploy Amazon FSx for Lustre and mount the file system using a POSIX-compliant client from both platforms

[ ] Use Amazon EFS with the Standard storage class and mount the file system using NFS from both Windows and Linux instances

[ ] Create an S3 bucket and mount it on EC2 instances using Mountpoint for Amazon S3, managing access through IAM policies to support both Windows and Linux workloads

[CORRECT] Deploy Amazon FSx for Windows File Server and mount it using the SMB protocol from both Windows and Linux EC2 instances

Q27: A startup has recently moved their monolithic web application to AWS Cloud. The application runs on a single Amazon EC2 instance. Currently, the user base is small and the startup does not want to spend effort on elaborate disaster recovery strategies or Auto Scaling Group. The application can afford a maximum downtime of 10 minutes. In case of a failure, which of these options would you suggest as a cost-effective and automatic recovery procedure for the instance?

[CORRECT] Configure an Amazon CloudWatch alarm that triggers the recovery of the Amazon EC2 instance, in case the instance fails. The instance, however, should only be configured with an Amazon EBS volume

[ ] Configure AWS Trusted Advisor to monitor the health check of Amazon EC2 instance and provide a remedial action in case an unhealthy flag is detected

[ ] Configure an Amazon CloudWatch alarm that triggers the recovery of the Amazon EC2 instance, in case the instance fails. The instance can be configured with Amazon Elastic Block Store (Amazon EBS) or with instance store volumes

[ ] Configure Amazon EventBridge events that can trigger the recovery of the Amazon EC2 instance, in case the instance or the application fails

Q28: 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?

[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 one or more subnets 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

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

Q29: An IT training company hosted its website on Amazon S3 a couple of years ago. Due to COVID-19 related travel restrictions, the training website has suddenly gained traction. With an almost 300% increase in the requests served per day, the company's AWS costs have sky-rocketed for just the Amazon S3 outbound data costs. As a Solutions Architect, can you suggest an alternate method to reduce costs while keeping the latency low?

[ ] Configure Amazon S3 Batch Operations to read data in bulk at one go, to reduce the number of calls made to Amazon S3 buckets

[ ] Use Amazon EFS service, as it provides a shared, scalable, fully managed elastic NFS file system for storing AWS Cloud or on-premises data

[CORRECT] Configure Amazon CloudFront to distribute the data hosted on Amazon S3 cost-effectively

[ ] To reduce Amazon S3 cost, the data can be saved on an Amazon EBS volume connected to an Amazon EC2 instance that can host the application

Q30: An IT consultant is helping a small business revamp their technology infrastructure on the AWS Cloud. The business has two AWS accounts and all resources are provisioned in theus-west-2region. The IT consultant is trying to launch an Amazon EC2 instance in each of the two AWS accounts such that the instances are in the same Availability Zone (AZ) of theus-west-2region. Even after selecting the same default subnet (us-west-2a) while launching the instances in each of the AWS accounts, the IT consultant notices that the Availability Zones (AZs) are still different. As a solutions architect, which of the following would you suggest resolving this issue?

[ ] Reach out to AWS Support for creating the Amazon EC2 instances in the same Availability Zone (AZ) across the two AWS accounts

[ ] Use the default subnet to uniquely identify the Availability Zones across the two AWS Accounts

[ ] Use the default VPC to uniquely identify the Availability Zones across the two AWS Accounts

[CORRECT] Use Availability Zone (AZ) ID to uniquely identify the Availability Zones across the two AWS Accounts

Q31: A small business has been running its IT systems on the on-premises infrastructure but the business now plans to migrate to AWS Cloud for operational efficiencies. As a Solutions Architect, can you suggest a cost-effective serverless solution for its flagship application that has both static and dynamic content?

[ ] Host both the static and dynamic content of the web application on Amazon EC2 with Amazon RDS as database. Amazon CloudFront should be configured to distribute the content across geographically disperse regions

[CORRECT] Host the static content on Amazon S3 and use AWS Lambda with Amazon DynamoDB for the serverless web application that handles dynamic content. Amazon CloudFront will sit in front of AWS Lambda for distribution across diverse regions

[ ] Host the static content on Amazon S3 and use Amazon EC2 with Amazon RDS for generating the dynamic content. Amazon CloudFront can be configured in front of Amazon EC2 instance, to make global distribution easy

[ ] Host both the static and dynamic content of the web application on Amazon S3 and use Amazon CloudFront for distribution across diverse regions/countries

Q32: An e-commerce company runs its web application on Amazon EC2 instances in an Auto Scaling group and it's configured to handle consumer orders in an Amazon Simple Queue Service (Amazon SQS) queue for downstream processing. The DevOps team has observed that the performance of the application goes down in case of a sudden spike in orders received. As a solutions architect, which of the following solutions would you recommend to address this use-case?

[ ] Use a simple scaling policy based on a custom Amazon SQS queue metric

[CORRECT] Use a target tracking scaling policy based on a custom Amazon SQS queue metric

[ ] Use a step scaling policy based on a custom Amazon SQS queue metric

[ ] Use a scheduled scaling policy based on a custom Amazon SQS queue metric

Q33: 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?

[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 primary elastic 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

Q34: 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 Elastic Load Balancing (ELB) 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

[ ] Use Auto Scaling group 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

Q35: A financial services company is migrating their messaging queues from self-managed message-oriented middleware systems to Amazon Simple Queue Service (Amazon SQS). The development team at the company wants to minimize the costs of using Amazon SQS. As a solutions architect, which of the following options would you recommend for the given use-case?

[ ] Use SQS message timer to retrieve messages from your Amazon SQS queues

[CORRECT] Use SQS long polling to retrieve messages from your Amazon SQS queues

[ ] Use SQS visibility timeout to retrieve messages from your Amazon SQS queues

[ ] Use SQS short polling to retrieve messages from your Amazon SQS queues

Q36: An AWS Organization is using Service Control Policies (SCPs) for central control over the maximum available permissions for all accounts in their organization. This allows the organization to ensure that all accounts stay within the organization's access control guidelines. Which of the given scenarios are correct regarding the permissions described below? (Select three)

[ ] Service control policy (SCP) affects service-linked roles

[CORRECT] Service control policy (SCP) does not affect service-linked role

[ ] If a user or role has an IAM permission policy that grants access to an action that is either not allowed or explicitly denied by the applicable service control policy (SCP), the user or role can still perform that action

[CORRECT] If a user or role has an IAM permission policy that grants access to an action that is either not allowed or explicitly denied by the applicable service control policy (SCP), the user or role can't perform that action

[CORRECT] Service control policy (SCP) affects all users and roles in the member accounts, including root user of the member accounts

[ ] Service control policy (SCP) affects all users and roles in the member accounts, excluding root user of the member accounts

Q37: An engineering lead is designing a VPC with public and private subnets. The VPC and subnets use IPv4 CIDR blocks. There is one public subnet and one private subnet in each of three Availability Zones (AZs) for high availability. An internet gateway is used to provide internet access for the public subnets. The private subnets require access to the internet to allow Amazon EC2 instances to download software updates. Which of the following options represents the correct solution to set up internet access for the private subnets?

[ ] Set up three NAT gateways, one in each private subnet in each AZ. Create a custom route table for each AZ that forwards non-local traffic to the NAT gateway in its AZ

[ ] Set up three egress-only internet gateways, one in each public subnet in each AZ. Create a custom route table for each AZ that forwards non-local traffic to the egress-only internet gateway in its AZ

[CORRECT] Set up three NAT gateways, one in each public subnet in each AZ. Create a custom route table for each AZ that forwards non-local traffic to the NAT gateway in its AZ

[ ] Set up three Internet gateways, one in each private subnet in each AZ. Create a custom route table for each AZ that forwards non-local traffic to the Internet gateway in its AZ

Q38: The DevOps team at a multi-national company is helping its subsidiaries standardize Amazon EC2 instances by using the same Amazon Machine Image (AMI). Some of these subsidiaries are in the same AWS region but use different AWS accounts whereas others are in different AWS regions but use the same AWS account as the parent company. The DevOps team has hired you as a solutions architect for this project. Which of the following would you identify as CORRECT regarding the capabilities of an Amazon Machine Image (AMI)? (Select three)

[ ] Copying an Amazon Machine Image (AMI) backed by an encrypted snapshot results in an unencrypted target snapshot

[ ] You cannot share an Amazon Machine Image (AMI) with another AWS account

[CORRECT] Copying an Amazon Machine Image (AMI) backed by an encrypted snapshot cannot result in an unencrypted target snapshot

[CORRECT] You can share an Amazon Machine Image (AMI) with another AWS account

[ ] You cannot copy an Amazon Machine Image (AMI) across AWS Regions

[CORRECT] You can copy an Amazon Machine Image (AMI) across AWS Regions

Q39: A video conferencing application is hosted on a fleet of EC2 instances which are part of an Auto Scaling group. The Auto Scaling group uses a Launch Template (LT1) with "dedicated" instance tenancy but the VPC (V1) used by the Launch Template LT1 has the instance tenancy set to default. Later the DevOps team creates a new Launch Template (LT2) with shared (default) instance tenancy but the VPC (V2) used by the Launch Template LT2 has the instance tenancy set to dedicated. Which of the following is correct regarding the instances launched via Launch Template LT1 and Launch Template LT2?

[ ] The instances launched by both Launch Template LT1 and Launch Template LT2 will have default instance tenancy

[CORRECT] The instances launched by both Launch Template LT1 and Launch Template LT2 will have dedicated instance tenancy

[ ] The instances launched by Launch Template LT1 will have default instance tenancy while the instances launched by the Launch Template LT2 will have dedicated instance tenancy

[ ] The instances launched by Launch Template LT1 will have dedicated instance tenancy while the instances launched by the Launch Template LT2 will have shared (default) instance tenancy

Q40: 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] Security Groups can be associated with a NAT instance

[ ] Security Groups can be associated with a NAT gateway

[ ] NAT gateway supports port forwarding

[ ] NAT gateway can be used as a bastion server

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

[CORRECT] NAT instance supports port forwarding

Q41: A legacy application is built using a tightly-coupled monolithic architecture. Due to a sharp increase in the number of users, the application performance has degraded. The company now wants to decouple the architecture and adopt AWS microservices architecture. Some of these microservices need to handle fast running processes whereas other microservices need to handle slower processes. Which of these options would you identify as the right way of connecting these microservices?

[ ] Use Amazon Simple Notification Service (Amazon SNS) to decouple microservices running faster processes from the microservices running slower ones

[CORRECT] Configure Amazon Simple Queue Service (Amazon SQS) queue to decouple microservices running faster processes from the microservices running slower ones

[ ] Configure Amazon Kinesis Data Streams to decouple microservices running faster processes from the microservices running slower ones

[ ] Add Amazon EventBridge to decouple the complex architecture

Q42: 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

[ ] AWS Glue

[ ] AWS Snowball Edge

[CORRECT] AWS Database Migration Service (AWS DMS)

Q43: A startup has created a new web application for users to complete a risk assessment survey for COVID-19 symptoms via a self-administered questionnaire. The startup has purchased the domain covid19survey.com using Amazon Route 53. The web development team would like to create Amazon Route 53 record so that all traffic for covid19survey.com is routed to www.covid19survey.com. As a solutions architect, which of the following is the MOST cost-effective solution that you would recommend to the web development team?

[ ] Create an NS record for covid19survey.com that routes traffic to www.covid19survey.com

[ ] Create a CNAME record for covid19survey.com that routes traffic to www.covid19survey.com

[ ] Create an MX record for covid19survey.com that routes traffic to www.covid19survey.com

[CORRECT] Create an alias record for covid19survey.com that routes traffic to www.covid19survey.com

Q44: A developer has configured inbound traffic for the relevant ports in both the Security Group of the Amazon EC2 instance as well as the Network Access Control List (Network ACL) of the subnet for the Amazon EC2 instance. The developer is, however, unable to connect to the service running on the Amazon EC2 instance. As a solutions architect, how will you fix this issue?

[ ] Network ACLs are stateful, so allowing inbound traffic to the necessary ports enables the connection. Security Groups are stateless, so you must allow both inbound and outbound traffic

[ ] IAM Role defined in the Security Group is different from the IAM Role that is given access in the Network ACLs

[ ] Rules associated with Network ACLs should never be modified from command line. An attempt to modify rules from command line blocks the rule and results in an erratic behavior

[CORRECT] Security Groups are stateful, so allowing inbound traffic to the necessary ports enables the connection. Network ACLs are stateless, so you must allow both inbound and outbound traffic

Q45: A company maintains its business-critical customer data on an on-premises system in an encrypted format. Over the years, the company has transitioned from using a single encryption key to multiple encryption keys by dividing the data into logical chunks. With the decision to move all the data to an Amazon S3 bucket, the company is now looking for a technique to encrypt each file with a different encryption key to provide maximum security to the migrated on-premises data. How will you implement this requirement without adding the overhead of splitting the data into logical groups?

[CORRECT] Configure a single Amazon S3 bucket to hold all data. Use server-side encryption with Amazon S3 managed keys (SSE-S3) to encrypt the data

[ ] Use Multi-Region keys for client-side encryption in the AWS S3 Encryption Client to generate unique keys for each file of data

[ ] Store the logically divided data into different Amazon S3 buckets. Use server-side encryption with Amazon S3 managed keys (SSE-S3) to encrypt the data

[ ] Configure a single Amazon S3 bucket to hold all data. Use server-side encryption with AWS KMS (SSE-KMS) and use encryption context to generate a different key for each file/object that you store in the S3 bucket

Q46: A company recently experienced a database outage in its on-premises data center. The company now wants to migrate to a reliable database solution on AWS that minimizes data loss and stores every transaction on at least two nodes. Which of the following solutions meets these requirements?

[ ] Set up an Amazon RDS MySQL DB instance and then create a read replica in another Availability Zone that synchronously replicates the data

[CORRECT] Set up an Amazon RDS MySQL DB instance with Multi-AZ functionality enabled to synchronously replicate the data

[ ] Set up an Amazon RDS MySQL DB instance and then create a read replica in a separate AWS Region that synchronously replicates the data

[ ] Set up an Amazon EC2 instance with a MySQL DB engine installed that triggers an AWS Lambda function to synchronously replicate the data to an Amazon RDS MySQL DB instance

Q47: An e-commerce company uses Microsoft Active Directory to provide users and groups with access to resources on the on-premises infrastructure. The company has extended its IT infrastructure to AWS in the form of a hybrid cloud. The engineering team at the company wants to run directory-aware workloads on AWS for a SQL Server-based application. The team also wants to configure a trust relationship to enable single sign-on (SSO) for its users to access resources in either domain. As a solutions architect, which of the following AWS services would you recommend for this use-case?

[ ] Amazon Cloud Directory

[ ] Simple Active Directory (Simple AD)

[CORRECT] AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD)

[ ] Active Directory Connector

Q48: A financial services company wants to move the Windows file server clusters out of their datacenters. They are looking for cloud file storage offerings that provide full Windows compatibility. Can you identify the AWS storage services that provide highly reliable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol compatible with Windows systems? (Select two)

[CORRECT] Amazon FSx for Windows File Server

[ ] Amazon Elastic File System (Amazon EFS)

[ ] Amazon Simple Storage Service (Amazon S3)

[CORRECT] File Gateway Configuration of AWS Storage Gateway

[ ] Amazon Elastic Block Store (Amazon EBS)

Q49: A startup is building a serverless microservices architecture where client applications (web and mobile) authenticate users via a third-party OIDC-compliant identity provider. The backend APIs must validate JSON Web Tokens (JWTs) issued by this provider, enforce scope-based access control, and be cost-effective with minimal latency. The development team wants to use a fully managed service that supports JWT validation natively, without writing custom authentication logic. Which solution should the team implement to meet these requirements?

[CORRECT] Use Amazon API Gateway HTTP API with a native JWT authorizer configured to validate tokens from the OIDC provider

[ ] Use Amazon API Gateway WebSocket API with JWT claims validated by a Lambda authorizer

[ ] Use Amazon API Gateway REST API with a Lambda function that manually validates JWT tokens

[ ] Deploy a gRPC backend on Amazon ECS Fargate and expose it through AWS App Runner, handling JWT validation inside the containerized services

Q50: The engineering team at a company is moving the static content from the company's logistics website hosted on Amazon EC2 instances to an Amazon S3 bucket. The team wants to use an Amazon CloudFront distribution to deliver the static content. The security group used by the Amazon EC2 instances allows the website to be accessed by a limited set of IP ranges from the company's suppliers. Post-migration to Amazon CloudFront, access to the static content should only be allowed from the aforementioned IP addresses. Which options would you combine to build a solution to meet these requirements? (Select two)

[ ] Create a new NACL that allows traffic from the same IPs as specified in the current Amazon EC2 security group. Associate this new NACL with the Amazon CloudFront distribution

[CORRECT] Configure an origin access identity (OAI) and associate it with the Amazon CloudFront distribution. Set up the permissions in the Amazon S3 bucket policy so that only the OAI can read the objects

[ ] Create a new security group that allows traffic from the same IPs as specified in the current Amazon EC2 security group. Associate this new security group with the Amazon CloudFront distribution

[ ] Create an AWS Web Application Firewall (AWS WAF) ACL and use an IP match condition to allow traffic only from those IPs that are allowed in the Amazon EC2 security group. Associate this new AWS WAF ACL with the Amazon S3 bucket policy

[CORRECT] Create an AWS WAF ACL and use an IP match condition to allow traffic only from those IPs that are allowed in the Amazon EC2 security group. Associate this new AWS WAF ACL with the Amazon CloudFront distribution

Q51: A media streaming startup is building a set of backend APIs that will be consumed by external mobile applications. To prevent API abuse, protect downstream resources, and ensure fair usage across clients, the architecture must enforce rate limiting and throttling on a per-client basis. The team also wants to define usage quotas and apply different limits to different API consumers. Which solution should the team implement to enforce rate limiting and usage quotas at the API layer?

[ ] Use a Gateway Load Balancer to inspect and control incoming HTTP traffic and throttle requests by integrating with third-party firewall appliances

[ ] Use an Application Load Balancer (ALB) with path-based routing and configure listener rules to enforce request limits

[CORRECT] Use Amazon API Gateway and configure usage plans with API keys to apply rate limits and quotas per client

[ ] Use a Network Load Balancer (NLB) to terminate TLS and apply rate-limiting logic within backend EC2 instances

Q52: The database backend for a retail company's website is hosted on Amazon RDS for MySQL having a primary instance and three read replicas to support read scalability. The company has mandated that the read replicas should lag no more than 1 second behind the primary instance to provide the best possible user experience. The read replicas are falling further behind during periods of peak traffic spikes, resulting in a bad user experience as the searches produce inconsistent results. You have been hired as an AWS Certified Solutions Architect - Associate to reduce the replication lag as much as possible with minimal changes to the application code or the effort required to manage the underlying resources. Which of the following will you recommend?

[CORRECT] Set up database migration from Amazon RDS MySQL to Amazon Aurora MySQL. Swap out the MySQL read replicas with Aurora Replicas. Configure Aurora Auto Scaling

[ ] Host the MySQL primary database on a memory-optimized Amazon EC2 instance. Spin up additional compute-optimized Amazon EC2 instances to host the read replicas

[ ] Set up database migration from Amazon RDS MySQL to Amazon DynamoDB. Provision a large number of read capacity units (RCUs) to support the required throughput and enable Auto-Scaling

[ ] Set up an Amazon ElastiCache for Redis cluster in front of the MySQL database. Update the website to check the cache before querying the read replicas

Q53: 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?

[ ] 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

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

Q54: A geospatial analytics firm recently completed a large-scale seafloor imaging project and used AWS Snowball Edge Storage Optimized devices to collect and transfer over 150 TB of raw sonar data. The firm uses a high-performance computing (HPC) cluster on AWS to process and analyze massive datasets to identify natural resource formations. The processing workloads require sub-millisecond latency, high-throughput, fast and parallel file access to the imported dataset once the Snowball Edge devices are returned to AWS and the data is ingested. Which solution best meets these requirements?

[ ] Copy the data into Amazon S3. Transfer the contents to an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system on the HPC cluster nodes to access the data in parallel

[CORRECT] Create an Amazon FSx for Lustre file system and import the 150 TB of data directly into the Lustre file system. Mount the FSx file system on the HPC cluster instances to enable low-latency, high-throughput access to the data

[ ] Import the data into Amazon S3. Set up an Amazon FSx for NetApp ONTAP file system and configure the FSx volume to sync with the S3 bucket. Mount the FSx volume on the HPC nodes for shared access

[ ] Import the data into an Amazon S3 bucket. Create an Amazon FSx for Lustre file system, and link it to the S3 bucket. Mount the FSx for Lustre file system on the HPC nodes to access the data with high throughput and low latency

Q55: An IT company hosts windows based applications on its on-premises data center. The company is looking at moving the business to the AWS Cloud. The cloud solution should offer shared storage space that multiple applications can access without a need for replication. Also, the solution should integrate with the company's self-managed Active Directory domain. Which of the following solutions addresses these requirements with the minimal integration effort?

[CORRECT] Use Amazon FSx for Windows File Server as a shared storage solution

[ ] Use Amazon FSx for Lustre as a shared storage solution with millisecond latencies

[ ] Use Amazon Elastic File System (Amazon EFS) as a shared storage solution

[ ] Use File Gateway of AWS Storage Gateway to create a hybrid storage solution

Q56: 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 VPN connection to access Amazon SQS

[ ] Use Internet Gateway to access Amazon SQS

[CORRECT] Use VPC endpoint to access Amazon SQS

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

Q57: The engineering team at a social media company wants to use Amazon CloudWatch alarms to automatically recover Amazon EC2 instances if they become impaired. The team has hired you as a solutions architect to provide subject matter expertise. As a solutions architect, which of the following statements would you identify as CORRECT regarding this automatic recovery process? (Select two)

[ ] If your instance has a public IPv4 address, it does not retain the public IPv4 address after recovery

[ ] Terminated Amazon EC2 instances can be recovered if they are configured at the launch of instance

[ ] During instance recovery, the instance is migrated during an instance reboot, and any data that is in-memory is retained

[CORRECT] If your instance has a public IPv4 address, it retains the public IPv4 address after recovery

[CORRECT] A recovered instance is identical to the original instance, including the instance ID, private IP addresses, Elastic IP addresses, and all instance metadata

Q58: A software company manages a fleet of Amazon EC2 instances that support internal analytics applications. These instances use an IAM role with custom policies to connect to Amazon RDS and AWS Secrets Manager for secure access to credentials and database endpoints. The IT operations team wants to implement a centralized patch management solution that simplifies compliance and security tasks. Their goal is to automate OS patching across EC2 instances without disrupting the running applications. Which approach will allow the company to meet these goals with the least administrative overhead?

[ ] Manually install the Systems Manager Agent (SSM Agent) on each EC2 instance. Schedule daily patch jobs using cron scripts

[CORRECT] Enable Default Host Management Configuration in AWS Systems Manager Quick Setup

[ ] Detach the existing IAM role from all EC2 instances. Replace it with a new role that has both the original permissions and the AmazonSSMManagedInstanceCore policy to enable Systems Manager features

[ ] Create a second IAM role with the AmazonSSMManagedInstanceCore policy and attach both the new and the existing IAM roles to each EC2 instance using Systems Manager Hybrid Activation

Q59: The development team at a retail company wants to optimize the cost of Amazon EC2 instances. The team wants to move certain nightly batch jobs to spot instances. The team has hired you as a solutions architect to provide the initial guidance. Which of the following would you identify as CORRECT regarding the capabilities of spot instances? (Select three)

[CORRECT] If a spot request is persistent, then it is opened again after your Spot Instance is interrupted

[CORRECT] Spot Fleets can maintain target capacity by launching replacement instances after Spot Instances in the fleet are terminated

[ ] When you cancel an active spot request, it terminates the associated instance as well

[ ] Spot Fleets cannot maintain target capacity by launching replacement instances after Spot Instances in the fleet are terminated

[ ] If a spot request is persistent, then it is opened again after you stop the Spot Instance

[CORRECT] When you cancel an active spot request, it does not terminate the associated instance

Q60: The DevOps team at an IT company has created a custom VPC (V1) and attached an Internet Gateway (I1) to the VPC. The team has also created a subnet (S1) in this custom VPC and added a route to this subnet's route table (R1) that directs internet-bound traffic to the Internet Gateway. Now the team launches an Amazon EC2 instance (E1) in the subnet S1 and assigns a public IPv4 address to this instance. Next the team also launches a Network Address Translation (NAT) instance (N1) in the subnet S1. Under the given infrastructure setup, which of the following entities is doing the Network Address Translation for the Amazon EC2 instance E1?

[CORRECT] Internet Gateway (I1)

[ ] Route Table (R1)

[ ] Subnet (S1)

[ ] Network Address Translation (NAT) instance (N1)

Q61: A health care application processes the real-time health data of the patients into an analytics workflow. With a sharp increase in the number of users, the system has become slow and sometimes even unresponsive as it does not have a retry mechanism. The startup is looking at a scalable solution that has minimal implementation overhead. Which of the following would you recommend as a scalable alternative to the current solution?

[ ] Use Amazon Simple Notification Service (Amazon SNS) for data ingestion and configure AWS Lambda to trigger logic for downstream processing

[CORRECT] Use Amazon Kinesis Data Streams to ingest the data, process it using AWS Lambda or run analytics using Amazon Kinesis Data Analytics

[ ] Use Amazon Simple Queue Service (Amazon SQS) for data ingestion and configure AWS Lambda to trigger logic for downstream processing

[ ] Use Amazon API Gateway with the existing REST-based interface to create a high performing architecture

Q62: A social media startup uses AWS Cloud to manage its IT infrastructure. The engineering team at the startup wants to perform weekly database rollovers for a MySQL database server using a serverless cron job that typically takes about 5 minutes to execute the database rollover script written in Python. The database rollover will archive the past week's data from the production database to keep the database small while still keeping its data accessible. As a solutions architect, which of the following would you recommend as the MOST cost-efficient and reliable solution?

[CORRECT] Schedule a weekly Amazon EventBridge event cron expression to invoke an AWS Lambda function that runs the database rollover job

[ ] Create a time-based schedule option within an AWS Glue job to invoke itself every week and run the database rollover script

[ ] Provision an Amazon EC2 spot instance to run the database rollover script to be run via an OS-based weekly cron expression

[ ] Provision an Amazon EC2 scheduled reserved instance to run the database rollover script to be run via an OS-based weekly cron expression

Q63: A company has set up AWS Organizations to manage several departments running their own AWS accounts. The departments operate from different countries and are spread across various AWS Regions. The company wants to set up a consistent resource provisioning process across departments so that each resource follows pre-defined configurations such as using a specific type of Amazon EC2 instances, specific IAM roles for AWS Lambda functions, etc. As a solutions architect, which of the following options would you recommend for this use-case?

[ ] Use AWS CloudFormation stacks to deploy the same template across AWS accounts and regions

[CORRECT] Use AWS CloudFormation StackSets to deploy the same template across AWS accounts and regions

[ ] Use AWS CloudFormation templates to deploy the same template across AWS accounts and regions

[ ] Use AWS Resource Access Manager (AWS RAM) to deploy the same template across AWS accounts and regions

Q64: A data analytics company manages an application that stores user data in a Amazon DynamoDB table. The development team has observed that once in a while, the application writes corrupted data in the Amazon DynamoDB table. As soon as the issue is detected, the team needs to remove the corrupted data at the earliest. What do you recommend?

[ ] Configure the Amazon DynamoDB table as a global table and point the application to use the table from another AWS region that has no corrupted data

[ ] Use Amazon DynamoDB Streams to restore the table to the state just before corrupted data was written

[ ] Use Amazon DynamoDB on-demand backup to restore the table to the state just before corrupted data was written

[CORRECT] Use Amazon DynamoDB point in time recovery to restore the table to the state just before corrupted data was written

Q65: The application maintenance team at a company has noticed that the production application is very slow when the business reports are run on the Amazon RDS database. These reports fetch a large amount of data and have complex queries with multiple joins, spanning across multiple business-critical core tables. CPU, memory, and storage metrics are around 50% of the total capacity. Can you recommend an improved and cost-effective way of generating the business reports while keeping the production application unaffected?

[ ] Configure the Amazon RDS instance to be Multi-AZ DB instance, and connect the report generation tool to the DB instance in a different AZ

[CORRECT] Create a read replica and connect the report generation tool/application to it

[ ] Migrate from General Purpose SSD to magnetic storage to enhance IOPS

[ ] Increase the size of Amazon RDS instance