Q1. A solutions architect is designing a new service behind Amazon API Gateway. The request patterns for the service will be unpredictable and can change suddenly from 0 requests to over 500 per second.The total size of the data that needs to be persisted in a backend database is currently less than 1 GB with unpredictable future growth Data can be queried using simple key-value requests. Which combination of AWS services would meet these requirements? (Select TWO)

A.AWS Fargate

B.AWS Lambda

C.Amazon DynamoDB

D.Amazon EC2 Auto Scaling

E.MySQL-compatible Amazon Aurora

正确答案 B,C

解析:

In this case AWS Lambda can perform the computation and store the data in an Amazon DynamoDB table. Lambda can scale concurrent executions to meet demand easily and DynamoDB is built for key-value data storage requirements and is also serverless and easily scalable. This is therefore a cost effective solution for unpredictable workloads.CORRECT: "AWS Lambda" is a correct answer.CORRECT: "Amazon DynamoDB" is also a correct answer.INCORRECT: "AWS Fargate" is incorrect as containers run constantly and therefore incur costs even when no requests are being made.INCORRECT: "Amazon EC2 Auto Scaling" is incorrect as this uses EC2 instances which will incur costs even when no requests are being made.INCORRECT: "Amazon RDS" is incorrect as this is a relational database not a No-SQL database. It is therefore not suitable for key-value data storage requirements.References:https://aws.amazon.com/lambda/features/https://aws.amazon.com/dynamodb//

Q2. A solutions architect needs to design a managed storage solution for a company's application that includes high-performance machine learning.This application runs on AWS Fargate and the connected storage needs to have concurrent access to files and deliver high performance.Which storage option should the solutions architect recommend?

A. Create an Amazon S3 bucket for the application and establish an IAM role for Fargate to communicate with Amazon S3.

B. Create an Amazon FSx for Lustre file share and establish an IAM role that allows Fargate to communicate with FSx for Lustre.

C. Create an Amazon Elastic File System (Amazon EFS) file share and establish an IAM role that allows Fargate to communicate with Amazon EFS.

D. Create an Amazon Elastic Block Store (Amazon EBS) volume for the application and establish an IAM role that allows Fargate to communicate with Amazon EBS.

正确答案 B

解析:

https://aws.amazon.com/efs/Keyword: Concurrent Access to files + Deliver High Performance Amazon FSx -A high-performance file system optimized for fast processing of workloads. Lustre is a popular open-source parallel file system.Also supports concurrent access to the same file or directory from thousands of compute instances.Amazon IAM with FSx -?Amazon FSx is integrated with AWS Identity and Access Management (IAM). ?This integration means that you can control the actions your AWS IAM users and groups can take to manage your file systems (such as creating and deleting file systems). ?You can also tag your Amazon FSx resources and control the actions that your IAM users and groups can take based on those tags.Fargate Launch Type - So, Answer C & D Ruled-out as per Neal David Fargate automatically provisions resourcesFargate provisions and manages computeCharged for running tasksNo EFS and EBS

integrationFargate handles cluster optimizationLimited control, infrastructure is automated

Q3. A company has a multi-tier application that runs six front-end web servers in an Amazon EC2 Auto Scaling group in a single Availability Zone behind an Application Load Balancer (ALB). A solutions architect needs to modify the infrastructure to be highly available without modifying the application.Which architecture should the solutions architect choose that provides high availability?

A.Create an Auto Scaling group that uses three instances across each of two Regions

B.Modify the Auto Scaling group to use three instances across each of two Availability Zones

C.Create an Auto Scaling template that can be used to quickly create more instances in another Region

D.Change the ALB in front of the Amazon EC2 instances in a round-robin configuration to balance traffic to the web tier

正确答案 B

解析:

High availability can be enabled for this architecture quite simply by modifying the existing Auto Scaling group to use multiple availability zones. The ASG will automatically balance the load so you don't actually need to specify the instances per AZ. The architecture for the web tier will look like the one below:CORRECT: "Modify the Auto Scaling group to use four instances across each of two Availability Zones" is the correct answer.INCORRECT: "Create an Auto Scaling group that uses four instances across each of two Regions" is incorrect as EC2 Auto Scaling does not support multiple regions. INCORRECT: "Create an Auto Scaling template that can be used to quickly create more instances in another Region" is incorrect as EC2 Auto Scaling does not support multiple regions. INCORRECT: "Create an Auto Scaling group that uses four instances across each of two subnets" is incorrect as the subnets could be in the same

AZ.References:https://aws.amazon.com/ec2/autoscaling/Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws- auto-scaling/

Q4. A company runs an internal browser-based application The application runs on Amazon EC2 instances behind an Application Load Balancer.The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. The Auto Scaling group scales up to 20 instances during work hours, but scales down to 2 instances overnight Staff are complaining that the application is very slow when the day begins, although it runs well by mid-morning.How should the scaling be changed to address the staff complaints and keep costs to a minimum?

A. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens

B. Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period

C. Implement a target tracking action triggered at a lower CPU threshold and decrease the cooldown period

D. Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens

正确答案 C

解析:

Answers A & D are incorrect because the question states to keep costs to a minimum. This means, NOT running 20 instances from the start. Answers B & C are both a better options. The problem in the morning is not that there should have been 20 instances running and that they are not running. The problem is that the auto scaling is not responding fast enough to the increase in demand. That is why decreasing the cool down period will make the auto scaling more aggressive (and responsive) but

will still run less than 20 instances from the get go, and therefore will cost less money. Also, AWS recommends using target scaling as much as possible. ---------- 原始A答案解析

Though this sounds like a good use case for scheduled actions, both answers using scheduled actions will have 20 instances running regardless of actual demand. A better option to be more cost effective is to use a target tracking action that triggers at a lower CPU threshold. With this solution the scaling will occur before the CPU utilization gets to a point where performance is affected. This will result in resolving the performance issues whilst minimizing costs. Using a reduced cooldown period will also more quickly terminate unneeded instances, further reducing costs. CORRECT: "Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period" is the correct answer. INCORRECT: "Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens" is incorrect as this is not the most cost-effective option. Note you can choose min, max, or desired for a scheduled action. INCORRECT: "Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens" is incorrect as this is not the most cost-effective option. Note you can choose min, max, or desired for a scheduled action. INCORRECT: "Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period" is incorrect as AWS recommend you use target tracking in place of step scaling for most use cases. References: https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws- auto-scaling/

Q5. A solutions architect is designing a solution to access a catalog of images and provide users with the ability to submit requests to customize images.Image customization parameters will be in any request sent to an AWS API Gateway API. The customized image will be generated on demand, and users will receive a link they can click to view or download their customized image.The solution must be highly available

for viewing and customizing images What is the MOST cost-effective solution to meet these requirements?

A.Use Amazon EC2 instances to manipulate the original image into the requested customization.Store the original and manipulated images in Amazon S3.Configure an Elastic Load Balancer in front of the EC2 instances.

B.Use AWS Lambda to manipulate the original image to the requested customization.Store the original and manipulated images in Amazon S3.Configure an Amazon CloudFront distribution with the S3 bucket as the ongin.

C.Use AWS Lambda to manipulate the original image to the requested customization.Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB.Configure an Elastic Load Balancer in front of the Amazon EC2 instances.

D.Use Amazon EC2 instances to manipulate the original image into the requested customization.Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB.Configure an Amazon CloudFront distribution with the S3 bucket as the origin.

正确答案 B

解析:

All solutions presented are highly available. The key requirement that must be satisfied is that the solution should be cost-effective and you must choose the most cost-effective option. Therefore, it's best to eliminate services such as Amazon EC2 and ELB as these require ongoing costs even when they're not used. Instead, a fully serverless solution should be used. AWS Lambda, Amazon S3 and CloudFront are the best services to use for these requirements. CORRECT: "Use AWS Lambda to manipulate the original images to the requested customization. Store the original and manipulated images in Amazon S3. Configure an Amazon CloudFront distribution with the S3 bucket as the origin" is the correct answer. INCORRECT: "Use Amazon EC2 instances to manipulate the original

images into the requested customization. Store the original and manipulated images in Amazon S3. Configure an Elastic Load Balancer in front of the EC2 instances" is incorrect. This is not the most cost-effective option as the ELB and EC2 instances will incur costs even when not used. INCORRECT: "Use AWS Lambda to manipulate the original images to the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Elastic Load Balancer in front of the Amazon EC2 instances" is incorrect. This is not the most cost-effective option as the ELB will incur costs even when not used. Also, Amazon DynamoDB will incur RCU/WCUs when running and is not the best choice for storing images.INCORRECT: "Use Amazon EC2 instances to manipulate the original images into the requested customization. Store the original images in Amazon S3 and the manipulated images in Amazon DynamoDB. Configure an Amazon CloudFront distribution with the S3 bucket as the origin" is incorrect. This is not the most cost-effective option as the EC2 instances will incur costs even when not usedReferences:https://aws.amazon.com/serverless/Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/storage/amazon-s3/https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws-lambda/https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and- content-delivery/amazon-cloudfront/

Q6. A bicycle sharing company is developing a multi-tier architecture to track the location of its bicycles during peak operating hours.The company wants to use these data points in its existing analytics platform A solutions architect must determine the most viable multi-tier option to support this architecture. The data points must be accessible from the REST API. Which action meets these requirements for storing and retrieving location data?

A.Use Amazon Athena with Amazon S3

B.Use Amazon API Gateway with AWS Lambda

C.Use Amazon QuickSight with Amazon Redshift

D.Use Amazon API Gateway with Amazon Kinesis Data Analytics

正确答案 B

解析:

Keyword: Data points in its existing analytics platform + Data points must be accessible from the REST API + Track the location of its bicycles during peak operating hours They already have an analytics platform, A (Athena) and D (Kinesis Data Analytics) are out of the race even tough S3 & APT Gateway Support REST API. Now B and C are in Race. C will not support REST API. So answer should be B as per below details.Now if we talk about data type, we are talking about GEO location data for their bicycles. API Gateway will be support REST API. So, exact solution should be API Gateway with AWS Lambda along with Amazon Kinesis Data Analytics (Assume its used already).CORRECT: "Use Amazon API Gateway with AWS Lambda" is the correct answer. INCORRECT: "Use Amazon Athena with Amazon S3" is incorrect as they already have analytics platform.INCORRECT: "Use Amazon QuickSight with Amazon Redshift" is incorrect. This is not support REST API.INCORRECT: "Use Amazon API Gateway with Amazon Kinesis Data Analytics" is incorrect as they already have analytics platform.References:https://aws.amazon.com/api-gateway/https://aws.amazon.com/lambda/https://aws.amazon.com/kinesis/data-analytics/Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/analytics/amazon-athena/https://digitalcloud.training/certification-training/aws-solutions-architect- associate/storage/amazon-s3/https://digitalcloud.training/certification-training/aws-solutions-architect-associate/storage/aws- storage-gateway/

Q7. A solutions architect is deploying a distributed database on multiple Amazon EC2 instances. The database stores all data on multiple

instances so it can withstand the loss of an instance. The database requires block storage with latency and throughput to support several million transactions per second per server.Which storage solution should the solutions architect use?

A.Amazon EBS

B.Amazon EC2 instance store

C.Amazon EFS

D.Amazon S3

正确答案 B

解析:

An instance store provides temporary block-level storage for your instance. This storage is located on disks that are physically attached to the host computer. Instance store is ideal for temporary storage of information that changes frequently, such as buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as a load-balanced pool of web servers.Some instance types use NVMe or SATA-based solid state drives (SSD) to deliver high random I/O performance. This is a good option when you need storage with very low latency, but you don't need the data to persist when the instance terminates or you can take advantage of fault-tolerant architectures.In this scenario the data is replicated and fault tolerant so the best option to provide the level of performance required is to use instance store volumes. CORRECT: "Amazon EC2 instance store" is the correct answer. INCORRECT: "Amazon EBS " is incorrect. The Elastic Block Store (EBS) is a block storage device but as the data is distributed and fault tolerant a better option for performance would be to use instance stores.INCORRECT: "Amazon EFS " is incorrect as EFS is not a block device, it is a filesystem that is accessed using the NFS protocol.INCORRECT: "Amazon S3" is incorrect as S3 is an object-based storage system, not a block- based storage system.References:https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/In

stanceStorage.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/compute/amazon-ebs/

Q8. A solutions architect needs to ensure that API calls to Amazon DynamoDB from Amazon EC2 instances in a VPC do not traverse the internet.What should the solutions architect do to accomplish this? (Select TWO)

A.Create a route table entry for the endpoint

B.Create a gateway endpoint for DynamoDB

C.Create a new DynamoDB table that uses the endpoint

D.Create an ENI for the endpoint in each of the subnets of the VPC

E.Create a security group entry in the default security group to provide access

正确答案 A,B

解析:

Amazon DynamoDB and Amazon S3 support gateway endpoints, not interface endpoints. With a gateway endpoint you create the endpoint in the VPC, attach a policy allowing access to the service, and then specify the route table to create a route table entry in.CORRECT: "Create a route table entry for the endpoint" is a correct answer. CORRECT: "Create a gateway endpoint for DynamoDB" is also a correct answer. INCORRECT: "Create a new DynamoDB table that uses the endpoint" is incorrect as it is not necessary to create a new DynamoDB table.INCORRECT: "Create an ENI for the endpoint in each of the subnets of the VPC" is incorrect as an ENI is used by an interface endpoint, not a gateway endpoint. INCORRECT: "Create a VPC peering connection between the VPC and DynamoDB" is incorrect as you cannot create a VPC peering connection between a VPC and a public AWS service as public services are outside of VPCs.References:https://docs.aws.amazon.com/vpc/latest/userguide/vpce-

gateway.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and- content-delivery/amazon-vpc/

Q9. A solutions architect is designing a web application that will run on Amazon EC2 instances behind an Application Load Balancer (ALB).The company strictly requires that the application be resilient against malicious internet activity and attacks, and protect against new common vulnerabilities and exposures.What should the solutions architect recommend?

A.Leverage Amazon CloudFront with the ALB endpoint as the origin

B.Deploy an appropriate managed rule for AWS WAF and associate it with the ALB

C.Subscribe to AWS Shield Advanced and ensure common vulnerabilities and exposures are blocked

D.Configure network ACLs and security groups to allow only ports 80 and 443 to access the EC2 instances

正确答案 B

解析:

You can deploy AWS WAF on Amazon CloudFront as part of your CDN solution, the Application Load Balancer that fronts your web servers or origin servers running on EC2, or Amazon API Gateway for your APIs.Ease of deployment & maintenanceAWS WAF is easy to deploy and protect applications deployed on either Amazon CloudFront as part of your CDN solution, the Application Load Balancer that fronts all your origin servers, or Amazon API Gateway for your APIs. There is no additional software to deploy, DNS configuration, SSL/TLS certificate to manage, or need for a reverse proxy setup. With AWS Firewall Manager integration, you can centrally define and manage your rules, and reuse them across

all the web applications that you need to protect.CORRECT: "Deploy an appropriate managed rule for AWS WAF and associate it with the ALB" is a correct answer.INCORRECT: "Leverage Amazon CloudFront with the ALB endpoint as the origin" is incorrect as it is not fulfill the Security requirement.INCORRECT: "Subscribe to AWS Shield Advanced and ensure common vulnerabilities and exposures are blocked" is incorrect as this will Support ELB INCORRECT: "Configure network ACLs and security groups to allow only ports 80 and 443 to access the EC2 instances" is incorrect as "new common vulnerabilities & exposure"References:https://aws.amazon.com/waf/https://aws.amazon.com/shield/https://aws.amazon.com/shield/features/Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-waf-and-shield/

Q10. A company has been storing analytics data in an Amazon RDS instance for the past few years. The company asked a solutions architect to find a solution that allows users to access this data using an API.The expectation is that the application will experience periods of inactivity but could receive bursts of traffic within seconds.Which solution should the solutions architect suggest?

A.Set up an Amazon API Gateway and use Amazon ECS.

B.Set up an Amazon API Gateway and use AWS Elastic Beanstalk.

C.Set up an Amazon API Gateway and use AWS Lambda functions

D.Set up an Amazon API Gateway and use Amazon EC2 with Auto Scaling

正确答案 C

解析:

This question is simply asking you to work out the best compute service for the stated requirements. The key requirements are that the compute service should be suitable for a workload that can range quite broadly

in demand from no requests to large bursts of traffic. AWS Lambda is an ideal solution as you pay only when requests are made and it can easily scale to accommodate the large bursts in traffic. Lambda works well with both API Gateway and Amazon RDS.CORRECT: "Set up an Amazon API Gateway and use AWS Lambda functions" is the correct answer.INCORRECT: "Set up an Amazon API Gateway and use Amazon ECS" is incorrect as Lambda is a better fit for this use case as the traffic patterns are highly dynamic. INCORRECT: "Set up an Amazon API Gateway and use AWS Elastic Beanstalk" is incorrect as Lambda is a better fit for this use case as the traffic patterns are highly dynamic. INCORRECT: "Set up an Amazon API Gateway and use Amazon EC2 with Auto Scaling" is incorrect as Lambda is a better fit for this use case as the traffic patterns are highly dynamic.References:https://docs.aws.amazon.com/lambda/latest/dg/invocation-scaling.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws- lambda/

Q11. A company's web application is using multiple Linux Amazon EC2 instances and storing data on Amazon EBS volumes.The company is looking for a solution to increase the resiliency of the application in case of a failure and to provide storage that complies with atomicity, consistency, isolation, and durability (ACID).What should a solutions architect do to meet these requirements?

A.Launch the application on EC2 instances in each Availability Zone.Attach EBS volumes to each EC2 instance.

B.Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones.Mount an instance store on each EC2 instance.

C.Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones.Store data on Amazon EFS and mount a target on each instance.

D.Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones.Store data using Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).

正确答案 C

解析:

To increase the resiliency of the application the solutions architect can use Auto Scaling groups to launch and terminate instances across multiple availability zones based on demand. An application load balancer (ALB) can be used to direct traffic to the web application running on the EC2 instances.Lastly, the Amazon Elastic File System (EFS) can assist with increasing the resilience of the application by providing a shared file system that can be mounted by multiple EC2 instances from multiple availability zones.CORRECT: "Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data on Amazon EFS and mount a target on each instance" is the correct answer.INCORRECT: "Launch the application on EC2 instances in each Availability Zone. Attach EBS volumes to each EC2 instance" is incorrect as the EBS volumes are single points of failure which are not shared with other instances.INCORRECT: "Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Mount an instance store on each EC2 instance" is incorrect as instance stores are ephemeral data stores which means data is lost when powered down. Also, instance stores cannot be shared between instances.INCORRECT: "Create an Application Load Balancer with Auto Scaling groups across multiple Availability Zones. Store data using Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)" is incorrect as there are data retrieval charges associated with this S3 tier. It is not a suitable storage tier for application files.References:https://docs.aws.amazon.com/efs/Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/storage/amazon-efs/

Q12. A company has an application that calls AWS Lambda functions. A recent code review found database credentials stored in the source code. The database credentials need to be removed from the Lambda source code. The credentials must then be securely stored and rotated on an ongoing basis to meet security policy requirements.What should a solutions architect recommend to meet these requirements?

A. Store the password in AWS CloudHSM.Associate the Lambda function with a role that can retrieve the password from CloudHSM given its key ID.

B. Store the password in AWS Secrets Manager.Associate the Lambda function with a role that can retrieve the password from Secrets Manager given its secret ID.

C. Move the database password to an environment variable associated with the Lambda function.Retrieve the password from the environment variable upon execution.

D. Store the password in AWS Key Management Service (AWS KMS).Associate the Lambda function with a role that can retrieve the password from AWS KMS given its key ID.

正确答案 B

解析:

AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.
https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html

Q13. A solutions architect needs the static website within an Amazon S3 bucket. A solutions architect needs to ensure that data can be recovered in case of accidental deletion.Which action will accomplish this?

A.Enable Amazon S3 versioning

B.Enable Amazon S3 Intelligent-Tiering.

C.Enable an Amazon S3 lifecycle policy

D.Enable Amazon S3 cross-Region replication.

正确答案 A

解析:

Object versioning is a means of keeping multiple variants of an object in the same Amazon S3 bucket. Versioning provides the ability to recover from both unintended user actions and application failures. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket.CORRECT: "Enable Amazon S3 versioning" is the correct answer. INCORRECT: "Enable Amazon S3 Intelligent-Tiering" is incorrect. This is a storage class that automatically moves data between frequent access and infrequent access classes based on usage patterns.INCORRECT: "Enable an Amazon S3 lifecycle policy" is incorrect. An S3 lifecycle policy is a set of rules that define actions that apply to groups of S3 objects such as transitioning objects to another storage class.INCORRECT: "Enable Amazon S3 cross-Region replication" is incorrect as this is used to copy objects to different regions. CRR relies on versioning which is the feature that is required for protecting against accidental deletion.References:https://d0.awsstatic.com/whitepapers/protecting-s3-against-object-deletion.pdf Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/storage/amazon-s3/

Q14. A company is managing health records on-premises.The company must keep these records indefinitely, disable any modifications to the records once they are stored, and granularly audit access at all levels. The chief technology officer (CTO) is concerned because there are already millions of records not being used by any application, and the current infrastructure is running out of space. The CTO has requested a

solutions architect design a solution to move existing data and support future records.Which services can the solutions architect recommend to meet these requirements'?

A.Use AWS DataSync to move existing data to AWS.Use Amazon S3 to store existing and new data.Enable Amazon S3 object lock and enable AWS CloudTrail with data events.

B.Use AWS Storage Gateway to move existing data to AWS.Use Amazon S3 to store existing and new data.Enable Amazon S3 object lock and enable AWS CloudTrail with management events.

C.Use AWS DataSync to move existing data to AWS.Use Amazon S3 to store existing and new data.Enable Amazon S3 object lock and enable AWS CloudTrail with management events.

D.Use AWS Storage Gateway to move existing data to AWS.Use Amazon Elastic Block Store (Amazon EBS) to store existing and new data.Enable Amazon S3 object lock and enable Amazon S3 server access logging.

正确答案 A

解析:

原始答案 B,现更正为 AKeyword: Move existing data and support future records + Granular audit access at all levelsUse AWS DataSync to migrate existing data to Amazon S3, and then use the File Gateway configuration of AWS Storage Gateway to retain access to the migrated data and for ongoing updates from your on-premises file-based applications.Need a solution to move existing data and support future records = AWS DataSync should be used for migration.Need granular audit access at all levels = Data Events should be used in CloudTrail, Management Events is enabled by default.CORRECT: "Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with data events" is the correct answer.INCORRECT: "Use AWS Storage Gateway to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events" is incorrect as

"current infrastructure is running out of space" INCORRECT: "Use AWS DataSync to move existing data to AWS. Use Amazon S3 to store existing and new data. Enable Amazon S3 object lock and enable AWS CloudTrail with management events." is incorrect as "Management Events is enabled by default" INCORRECT: "Use AWS Storage Gateway to move existing data to AWS. Use Amazon Elastic Block Store (Amazon EBS) to store existing and new data. Enable Amazon S3 object lock and enable Amazon S3 server access logging." is incorrect as "current infrastructure is running out of space"How AWS DataSync WorksHow AWS CloudTrail worksReferences:https://aws.amazon.com/datasync/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc https://aws.amazon.com/cloudtrail/https://aws.amazon.com/storagegateway/?whats-new-cards.sort- by=item.additionalFields.postDateTime&whats-new-cards.sort-order=descSave time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/storage/amazon-s3/

Q15. A company currently operates a web application backed by an Amazon RDS MySQL database. It has automated backups that are run daily and are not encrypted. A security audit requires future backups to be encrypted and the unencrypted backups to be destroyed.The company will make at least one encrypted backup before destroying the old backups What should be done to enable encryption for future backups?

A.Enable default encryption for the Amazon S3 bucket where backups are stored

B.Modify the backup section of the database configuration to toggle the Enable encryption check box.

C.Create a snapshot of the database.Copy it to an encrypted snapshot.Restore the database from the encrypted snapshot.

D.Enable an encrypted read replica on RDS for MySQL.Promote the encrypted read replica to primary.Remove the original database instance.

正确答案 C

解析:

Amazon RDS uses snapshots for backup. Snapshots are encrypted when created only if the database is encrypted and you can only select encryption for the database when you first create it. In this case the database, and hence the snapshots, ad unencrypted. However, you can create an encrypted copy of a snapshot. You can restore using that snapshot which creates a new DB instance that has encryption enabled. From that point on encryption will be enabled for all snapshots.CORRECT: "Create a snapshot of the database. Copy it to an encrypted snapshot. Restore the database from the encrypted snapshot" is the correct answer. INCORRECT: "Enable an encrypted read replica on RDS for MySQL. Promote the encrypted read replica to primary. Remove the original database instance" is incorrect as you cannot create an encrypted read replica from an unencrypted master.INCORRECT: "Modify the backup section of the database configuration to toggle the Enable encryption check box" is incorrect as you cannot add encryption for an existing database. INCORRECT: "Enable default encryption for the Amazon S3 bucket where backups are stored" is incorrect because you do not have access to the S3 bucket in which snapshots are stored.References:https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/database/amazon-rds/

Q16. A client reports that they want see an audit log of any changes made to AWS resources in their account.What can the client do to achieve this?

A. Set up Amazon CloudWatch monitors on services they own

B. Enable AWS CloudTrail logs to be delivered to an Amazon S3 bucket

C. Use Amazon CloudWatch Events to parse logs

D. Use AWS OpsWorks to manage their resources

正确答案 B

解析:

A CloudTrail trail can be created which delivers log files to an Amazon S3 bucket.

Q17. An application running in a private subnet accesses an Amazon DynamoDB table. There is a security requirement that the data never leave the AWS network.How should this requirement be met?

A.Configure a network ACL on DynamoDB to limit traffic to the private subnet

B.Enable DynamoDB encryption at rest using an AWS KMS key

C.Add a NAT gateway and configure the route table on the private subnet

D.Create a VPC endpoint for DynamoDB and configure the endpoint policy

正确答案 D

解析:

Hint: Private Subnet = VPC Endpoint

Q18. A three-tier application is being created to host small news articles. The application is expected to serve millions of users. When breaking news occurs, the site must handle very large spikes in traffic without significantly impacting database performance.Which design meets these requirements while minimizing costs?

A.Use Auto Scaling groups to increase the number of Amazon EC2 instances delivering the web application

B.Use Auto Scaling groups to increase the size of the Amazon RDS instances delivering the database

C.Use Amazon DynamoDB strongly consistent reads to adjust for the increase in traffic

D.Use Amazon DynamoDB Accelerator (DAX) to cache read operations to the database

正确答案 D

解析:

DAX has in memory cache. If breaking news happens, majority of the users searching will look for the exact same thing. That being said, requests will query the Memory Cache first and will not need to fetch the data from the DB directly.

Q19. During a review of business applications, a Solutions Architect identifies a critical application with a relational database that was built by a business user and is running on the user's desktop. To reduce the risk of a business interruption, the Solutions Architect wants to migrate the application to a highly available, multi-tiered solution in AWS.What should the Solutions Architect do to accomplish this with the LEAST amount of disruption to the business?

A. Create an import package of the application code for upload to AWS Lambda, and include a function to create another Lambda function to migrate data into an Amazon RDS database

B. Create an image of the user's desktop, migrate it to Amazon EC2 using VM Import, and place the EC2 instance in an Auto Scaling group

C. Pre-stage new Amazon EC2 instances running the application code on AWS behind an Application Load Balancer and an Amazon RDS Multi-AZ DB instance

D. Use AWS DMS to migrate the backend database to an Amazon RDS Multi-AZ DB instance.Migrate the application code to AWS Elastic Beanstalk

正确答案 D

解析:

We migrate the DB to RDS using AWS DMS. The code can be serverless in ElasticBeanstalk. Multi tier, HA is mentioned. So backend DB layer should run RDS Multi - AZ front end app layer should in BeanStalk. Focus on ques - least amount of disruption - DMS (easy data migration) and BeanStalk (easy mgmt of code/compute)

Q20. A company has thousands of files stored in an Amazon S3 bucket that has a well-defined access pattern. The files are accessed by an application multiple times a day for the first 30 days. Files are rarely accessed within the next 90 days. After that, the files are never accessed again. During the first 120 days, accessing these files should never take more than a few seconds.Which lifecycle policy should be used for the S3 objects to minimize costs based on the access pattern?

A.Use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) storage for the first 30 days. Then move the files to the GLACIER storage class for the next 90 days. Allow the data to expire after that.

B.Use Amazon S3 Standard storage for the first 30 days. Then move the files to Amazon S3 Standard- Infrequent Access (S3 Standard-IA) for the next 90 days. Allow the data to expire after that.

C.Use Amazon S3 Standard storage for first 30 days. Then move the files to the GLACIER storage class for the next 90 days. Allow the data to expire after that.

D.Use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) for the first 30 days. After that, move the data to the GLACIER storage class, where is will be deleted automatically.

正确答案 B

解析:

It is mentioned that they need to access data in few seconds during the 120 days.

Q21. A company creates business-critical 3D images every night. The images are batch-processed every Friday and require an uninterrupted 48 hours to complete.What is the MOST cost-effective Amazon EC2 pricing model for this scenario?

A.On-Demand Instances

B.Scheduled Reserved Instances

C.Reserved Instances

D.Spot Instances

正确答案 B

解析:

Scheduled Reserved Instances (Scheduled Instances) enable you to purchase capacity reservations that recur on a daily, weekly, or monthly basis, with a specified start time and duration, for a one-year term. You reserve the capacity in advance, so that you know it is available when you need it. You pay for the time that the instances are scheduled, even if you do not use them.Scheduled Instances are a good choice for workloads that do not run continuously, but do run on a regular schedule. For example, you can use Scheduled Instances for an application that runs during business hours or for batch processing that runs at the end of the week. CORRECT: "Scheduled Reserved Instances" is the correct answer. INCORRECT: "Standard Reserved Instances" is incorrect as the workload only runs for 4 hours a day this would be more expensive.INCORRECT: "On-Demand Instances" is incorrect as this would be much more expensive as there is no discount applied.INCORRECT: "Spot Instances" is incorrect as the workload cannot be interrupted once started. With Spot instances workloads can be terminated if the Spot price changes or capacity is

required.References:https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/compute/amazon-ec2/

Q22. An application generates audit logs of operational activities. Compliance requirements mandate that the application retain the logs for 5 years.How can these requirements be met?

A.Save the logs in an Amazon S3 bucket and enable Multi-Factor Authentication Delete (MFA Delete) on the bucket.

B.Save the logs in an Amazon EFS volume and use Network File System version 4 (NFSv4) locking with the volume.

C.Save the logs in an Amazon Glacier vault and use the Vault Lock feature.

D.Save the logs in an Amazon EBS volume and take monthly snapshots.

正确答案 C

解析:

Amazon Glacier, which enables long-term storage of mission-critical data, has added Vault Lock. This new feature allows you to lock your vault with a variety of compliance controls that are designed to support such long-term records retention.

Q23. A Solutions Architect is creating an application running in an Amazon VPC that needs to access AWS Systems Manager Parameter Store. Network security rules prohibit any route table entry with a 0.0.0.0/0 destination.What infrastructure addition will allow access to the AWS service while meeting the requirements?

A.VPC peering

B.NAT instance

C.NAT gateway

D.AWS PrivateLink

正确答案 D

解析:

To publish messages to Amazon SNS topics from an Amazon VPC, create an interface VPC endpoint. Then, you can publish messages to SNS topics while keeping the traffic within the network that you manage with the VPC. This is the most secure option as traffic does not need to traverse the Internet.CORRECT: "Use AWS PrivateLink" is the correct answer. INCORRECT: "Use an Internet Gateway" is incorrect. Internet Gateways are used by instances in public subnets to access the Internet and this is less secure than an VPC endpoint. INCORRECT: "Use a proxy instance" is incorrect. A proxy instance will also use the public Internet and so is less secure than a VPC endpoint.INCORRECT: "Use a NAT gateway" is incorrect. A NAT Gateway is used by instances in private subnets to access the Internet and this is less secure than an VPC endpoint.References:https://docs.aws.amazon.com/sns/latest/dg/sns-vpc-endpoint.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and- content-delivery/amazon-vpc/

Q24. A photo-sharing website running on AWS allows users to generate thumbnail images of photos stored in Amazon S3. An Amazon DynamoDB table maintains the locations of photos, and thumbnails are easily re- created from the originals if they are accidentally deleted.How should the thumbnail images be stored to ensure the LOWEST cost?

A. Amazon S3 Standard-Infrequent Access (S3 Standard-IA) with cross-region replication

B. Amazon S3

C. Amazon Glacier

D. Amazon S3 with cross-region replication

正确答案 B

解析:

This is a tricky question. They are already stored on S3. The "easily re-created if deleted" doesn't say much. Would need versioning with that. LOWEST-Cost could imply S3-IA and would be less than S3 Standard. Sticking with S3. straight S3, with no CRR or versioning so less cost, if deleted can be recreated easy this statement suggests, that thumbnails are used very often and that's why if they are deleted because they are needed they are re created, that takes away Glacier. Using for website so must be accessed frequently and quickly, access cost + storage cost = S3 is cost effective.

Q25. A company is implementing a data lake solution on Amazon S3. Its security policy mandates that the data stored in Amazon S3 should be encrypted at rest.Which options can achieve this? (Select TWO.)

A. Use S3 server-side encryption with an Amazon EC2 key pair.

B. Use S3 server-side encryption with customer-provided keys (SSE-C).

C. Use S3 bucket policies to restrict access to the data at rest.

D. Use client-side encryption before ingesting the data to Amazon S3 using encryption keys.

E. Use SSL to encrypt the data while in transit to Amazon S3.

正确答案 B,D

解析:

Data lakes built on AWS primarily use two types of encryption: Server-side encryption (SSE) and client-side encryption. SSE provides data-at-rest encryption for data written to Amazon S3. With SSE, Amazon S3 encrypts user data assets at the object level, stores the encrypted objects, and then decrypts them as they are accessed and retrieved. With client-side encryption, data objects are encrypted before they written into Amazon S3. Pay close attention to the question about "options". Those are obviously: either the customer encrypts the data or the server does it.
https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html

Q26. A solutions architect has created a new AWS account and must secure AWS account root user access.Which combination of actions will accomplish this? (Select TWO.)

A.Ensure the root user uses a strong password

B.Enable multi-factor authentication to the root user

C.Store root user access keys in an encrypted Amazon S3 bucket

D.Add the root user to a group containing administrative permissions.

E.Apply the required permissions to the root user with an inline policy document

正确答案 A,B

解析:

There are several security best practices for securing the root user account:Lock away root user access keys OR delete them if possibleUse a strong passwordEnable multi-factor authentication (MFA)The root user automatically has full privileges to the account and these privileges cannot be restricted so it is extremely important to follow best practice advice about securing the root user account.CORRECT: "Ensure the root user uses a strong password" is the correct answer. CORRECT: "Enable multi-factor authentication to the root user" is the correct

answer. INCORRECT: "Store root user access keys in an encrypted Amazon S3 bucket" is incorrect as the best practice is to lock away or delete the root user access keys. An S3 bucket is not a suitable location for storing them, even if encrypted. INCORRECT: "Add the root user to a group containing administrative permissions" is incorrect as this does not restrict access and is unnecessary.INCORRECT: "Delete the root user account" is incorrect as you cannot delete the root user account.References:https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity- compliance/aws-iam/

Q27. A company's application runs on Amazon EC2 instances behind an Application Load Balancer (ALB).The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. On the first day of every month at midnight the application becomes much slower when the month-end financial calculation batch executes.This causes the CPU utilization of the EC2 instances to immediately peak to 100% which disrupts the application.What should a solutions architect recommend to ensure the application is able to handle the workload and avoid downtime?

A.Configure an Amazon CloudFront distribution in front of the ALB

B.Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization

C.Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule.

D.Configure Amazon ElastiCache to remove some of the workload from the EC2 instances

正确答案 C

解析:

Scheduled scaling allows you to set your own scaling schedule. In this case the scaling action can be scheduled to occur just prior to the time that the reports will be run each month. Scaling actions are performed automatically as a function of time and date. This will ensure that there are enough EC2 instances to serve the demand and prevent the application from slowing down. CORRECT: "Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule" is the correct answer.INCORRECT: "Configure an Amazon CloudFront distribution in front of the ALB" is incorrect as this would be more suitable for providing access to global users by caching content. INCORRECT: "Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization" is incorrect as this would not prevent the slow-down from occurring as there would be a delay between when the CPU hits 100% and the metric being reported and additional instances being launched.INCORRECT: "Configure Amazon ElastiCache to remove some of the workload from the EC2 instances" is incorrect as ElastiCache is a database cache, it cannot replace the compute functions of an EC2 instance.References:https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws- auto-scaling/

Q28. A company is migrating from an on-premises infrastructure to the AWS Cloud. One of the company's applications stores files on a Windows file server farm that uses Distributed File System Replication (DFSR) to keep data in sync.A solutions architect needs to replace the file server farm.Which service should the solutions architect use?

A.Amazon EFS

B.Amazon FSx

C.Amazon S3

D.AWS Storage Gateway

正确答案 B

解析:

Amazon FSx for Windows File Server provides fully managed, highly reliable file storage that is accessible over the industry-standard Server Message Block (SMB) protocol. Amazon FSx is built on Windows Server and provides a rich set of administrative features that include end-user file restore, user quotas, and Access Control Lists (ACLs). Additionally, Amazon FSX for Windows File Server supports Distributed File System Replication (DFSR) in both Single-AZ and Multi-AZ deployments as can be seen in the feature comparison table below.CORRECT: "Amazon FSx" is the correct answer.INCORRECT: "Amazon EFS" is incorrect as EFS only supports Linux systems. INCORRECT: "Amazon S3" is incorrect as this is not a suitable replacement for a Microsoft filesystem.INCORRECT: "AWS Storage Gateway" is incorrect as this service is primarily used for connecting on-premises storage to cloud storage. It consists of a software device installed on- premises and can be used with SMB shares but it actually stores the data on S3. It is also used for migration. However, in this case the company need to replace the file server farm and Amazon FSx is the best choice for this job.References:https://docs.aws.amazon.com/fsx/latest/WindowsGuide/high-availability-multiAZ.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/storage/amazon-fsx/

Q29. A company's website is used to sell products to the public. The site runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB).There is also an Amazon CloudFront distribution and AWS WAF is being used to protect against SQL injection attacks.The ALB is the origin for the CloudFront distribution. A recent review of security logs revealed an external malicious IP that needs to be blocked from accessing the website.What should a solutions architect do to protect the application?

A.Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address

B.Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address

C.Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address

D.Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address

正确答案 B

解析:

A new version of the AWS Web Application Firewall was released in November 2019. With AWS WAF classic you create "IP match conditions", whereas with AWS WAF (new version) you create "IP set match statements". Look out for wording on the exam. The IP match condition / IP set match statement inspects the IP address of a web request's origin against a set of IP addresses and address ranges.Use this to allow or block web requests based on the IP addresses that the requests originate from.AWS WAF supports all IPv4 and IPv6 address ranges. An IP set can hold up to 10,000 IP addresses or IP address ranges to check.CORRECT: "Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address" is the correct answer.INCORRECT: "Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address" is incorrect as CloudFront does not sit within a subnet so network ACLs do not apply to it.INCORRECT: "Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address" is incorrect as the source IP addresses of the data in the EC2 instances' subnets will be the ELB IP addresses.INCORRECT: "Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address." is incorrect as you cannot create deny rules with security groups.References:https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-ipset- match.html Save time with our exam-

specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-waf-and-shield/

Q30. A marketing company is storing CSV files in an Amazon S3 bucket for statistical analysis. An application on an Amazon EC2 instance needs permission to efficiently process the CSV data stored in the S3 bucket.Which action will MOST securely grant the EC2 instance access to the S3 bucket?

A.Attach a resource-based policy to the S3 bucket

B.Create an IAM user for the application with specific permissions to the S3 bucket

C.Associate an IAM role with least privilege permissions to the EC2 instance profile

D.Store AWS credentials directly on the EC2 instance for applications on the instance to use for API calls

正确答案C

解析:

Keyword: Privilege Permission + IAM RoleAWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.IAM is a feature of your AWS account offered at no additional charge. You will be charged only for use of other AWS services by your users.IAM roles for Amazon EC2Applications must sign their API requests with AWS credentials. Therefore, if you are an application developer, you need a strategy for managing credentials for your applications that run on EC2 instances. For example, you can securely distribute your AWS credentials to the instances, enabling the applications on those instances to use your credentials to sign requests, while protecting

your credentials from other users. However, it's challenging to securely distribute credentials to each instance, especially those that AWS creates on your behalf, such as Spot Instances or instances in Auto Scaling groups. You must also be able to update the credentials on each instance when you rotate your AWS credentials.We designed IAM roles so that your applications can securely make API requests from your instances, without requiring you to manage the security credentials that the applications use.Instead of creating and distributing your AWS credentials, you can delegate permission to make API requests using IAM roles as follows:Create an IAM role.Define which accounts or AWS services can assume the role.Define which API actions and resources the application can use after assuming the role.Specify the role when you launch your instance, or attach the role to an existing instance.Have the application retrieve a set of temporary credentials and use them.For example, you can use IAM roles to grant permissions to applications running on your instances that need to use a bucket in Amazon S3. You can specify permissions for IAM roles by creating a policy in JSON format. These are similar to the policies that you create for IAM users. If you change a role, the change is propagated to all instances.When creating IAM roles, associate least privilege IAM policies that restrict access to the specific API calls the application requires.IAM RolesReferences:https://aws.amazon.com/iam/faqs/https://youtu.be/YQsK4MtsELUhttps://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.htmlSave time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity- compliance/aws-iam/https://digitalcloud.training/certification-training/aws-solutions-architect- associate/compute/amazon-ec2/

Q31. A solutions architect is designing a solution where users will De directed to a backup static error page it the primary website is unavailable.The primary website's DNS records are hosted in Amazon Route 53 where their domain is pointing to an Application Load Balancer (ALB).Which configuration should the solutions architect use to meet the company's needs while minimizing changes and infrastructure overhead?

A. Point a Route 53 alias record to an Amazon CloudFront distribution with the ALB as one of its origins.Then, create custom error pages for the distribution.

B. Set up a Route 53 active-passive failover configuration.Direct traffic to a static error page hosted within an Amazon S3 bucket when Route 53 health checks determine that the ALB endpoint is unhealthy.

C. Update the Route 53 record to use a latency-based routing policy.Add the backup static error page hosted within an Amazon S3 bucket to the record so the traffic is sent to the most responsive endpoints.

D. Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance hosting a static error page as endpoints.Route 53 will only send requests to the instance if the health checks fail for the ALB.

正确答案 B

解析:

Answer is A Using Amazon CloudFront as the front-end provides the option to specify a custom message instead of the default message. To specify the specific file that you want to return and the errors for which the file should be returned, you update your CloudFront distribution to specify those values. The CloudFront distribution can use the ALB as the origin, which will cause the website content to be cached on the CloudFront edge caches. This solution represents the most operationally efficient choice as no action is required in the event of an issue, other than troubleshooting the root cause.
Answer is B. active-passive configuration introduces minimum changes and infrastructure overhead. A is incorrect for the usecase "directed to a backup static error page if the primary website is unavailable" Using A will route the traffic to static error page not just when the primary website is unavailable but even in scenarios in 404 (i.e. website available, but invalid resource requested) and this option does not fit the usecase description. Also, introducing CF distribution is costlier than hosting a static error page in S3.

Using Amazon CloudFront as the front-end provides the option to specify a custom message instead of the default message. To specify the specific file that you want to return and the errors for which the file should be returned, you update your CloudFront distribution to specify those values.For example, the following is a customized error message:The CloudFront distribution can use the ALB as the origin, which will cause the website content to be cached on the CloudFront edge caches.This solution represents the most operationally efficient choice as no action is required in the event of an issue, other than troubleshooting the root cause. CORRECT: "Create a Route 53 alias record for an Amazon CloudFront distribution and specify the ALB as the origin. Create custom error pages for the distribution" is the correct answer. INCORRECT: "Create a Route 53 active-passive failover configuration. Create a static website using an Amazon S3 bucket that hosts a static error page. Configure the static website as the passive record for failover" is incorrect. This option does not represent the lowest operational overhead as manual intervention would be required to cause a fail-back to the main website. INCORRECT: "Create a Route 53 weighted routing policy. Create a static website using an Amazon S3 bucket that hosts a static error page. Configure the record for the S3 static website with a weighting of zero. When an issue occurs increase the weighting" is incorrect. This option requires manual intervention and there would be a delay from the issue arising before an administrative action could make the changes.INCORRECT: "Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance hosting a static error page as endpoints. Route 53 will only send requests to the instance if the health checks fail for the ALB" is incorrect. With an active-active configuration traffic would be split between the website and the error page.References:https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/custom-error- pages.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and- content-delivery/amazon-cloudfront/

Q32. A solutions architect is designing the cloud architecture for a new application being deployed on AWS.The process should run in parallel

while adding and removing application nodes as needed based on the number of jobs to be processed.The processor application is stateless.The solutions architect must ensure that the application is loosely coupled and the job items are durably stored.Which design should the solutions architect use?

A.Create an Amazon SNS topic to send the jobs that need to be processed.Create an Amazon Machine Image (AMI) that consists of the processor application.Create a launch configuration that uses the AMI.Create an Auto Scaling group using the launch configuration.Set the scaling policy for the Auto Scaling group to add and remove nodes based on CPU usage

B.Create an Amazon SQS queue to hold the jobs that need to be processed.Create an Amazon Machine Image (AMI) that consists of the processor application.Create a launch configuration that uses the AMI.Create an Auto Scaling group using the launch configuration.Set the scaling policy for the Auto Scaling group to add and remove nodes based on network usage

C.Create an Amazon SQS queue to hold the jobs that needs to be processed.Create an Amazon Machine Image (AMI) that consists of the processor application.Create a launch template that uses the AMI.Create an Auto Scaling group using the launch template.Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue

D.Create an Amazon SNS topic to send the jobs that need to be processed.Create an Amazon Machine Image (AMI) that consists of the processor application.Create a launch template that uses the AMI.Create an Auto Scaling group using the launch template.Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of messages published to the SNS topic.

正确答案 C

解析:

In this case we need to find a durable and loosely coupled solution for storing jobs. Amazon SQS is ideal for this use case and can be configured to use dynamic scaling based on the number of jobs waiting in the queue.To configure this scaling you can use the backlog per instance metric with the target value being the acceptable backlog per instance to maintain. You can calculate these numbers as follows:Backlog per instance: To calculate your backlog per instance, start with the ApproximateNumberOfMessages queue attribute to determine the length of the SQS queue (number of messages available for retrieval from the queue). Divide that number by the fleet's running capacity, which for an Auto Scaling group is the number of instances in the InService state, to get the backlog per instance.Acceptable backlog per instance: To calculate your target value, first determine what your application can accept in terms of latency. Then, take the acceptable latency value and divide it by the average time that an EC2 instance takes to process a message. This solution will scale EC2 instances using Auto Scaling based on the number of jobs waiting in the SQS queue.CORRECT: "Create an Amazon SQS queue to hold the jobs that needs to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue" is the correct answer.INCORRECT: "Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the Auto Scaling group to add and remove nodes based on network usage" is incorrect as scaling on network usage does not relate to the number of jobs waiting to be processed. INCORRECT: "Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling policy for the Auto Scaling group to add and remove nodes based on CPU usage" is incorrect. Amazon SNS is a notification service so it delivers notifications to subscribers. It does store data durably but is less suitable than SQS for this use case. Scaling on CPU usage is not the best solution as it does not relate to the number of jobs waiting to be processed. INCORRECT: "Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon EC2 Auto Scaling group for the compute application. Set the scaling

policy for the Auto Scaling group to add and remove nodes based on the number of messages published to the SNS topic" is incorrect. Amazon SNS is a notification service so it delivers notifications to subscribers. It does store data durably but is less suitable than SQS for this use case. Scaling on the number of notifications in SNS is not possible.References:https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws- auto-scaling/ https://digitalcloud.training/certification-training/aws-solutions-architect- associate/application-integration/amazon-sqs/

Q33. A company has a legacy application that processes data in two parts. The second part of the process takes longer than the first, so the company has decided to rewrite the application as two microservices running on Amazon ECS that can scale independently. How should a solutions architect integrate the microservices?

A.Implement code in microservice 1 to send data to an Amazon S3 bucket.Use S3 event notifications to invoke microservice 2.

B.Implement code in microservice 1 to publish data to an Amazon SNS topic.Implement code in microservice 2 to subscribe to this topic.

C.Implement code in microservice 1 to send data to Amazon Kinesis Data Firehose.Implement code in microservice 2 to read from Kinesis Data Firehose.

D.Implement code in microservice 1 to send data to an Amazon SQS queue.Implement code in microservice 2 to process messages from the queue.

正确答案 D

解析:

This is a good use case for Amazon SQS. The microservices must be decoupled so they can scale independently. An Amazon SQS queue will enable microservice 1 to add messages to the queue. Microservice 2 can then pick up the messages and process them. This ensures that if there's a spike in traffic on the frontend, messages do not get lost due to the backend process not being ready to process them.CORRECT: "Implement code in microservice 1 to send data to an Amazon SQS queue. Implement code in microservice 2 to process messages from the queue" is the correct answer. INCORRECT: "Implement code in microservice 1 to send data to an Amazon S3 bucket. Use S3 event notifications to invoke microservice 2" is incorrect as a message queue would be preferable to an S3 bucket.INCORRECT: "Implement code in microservice 1 to publish data to an Amazon SNS topic. Implement code in microservice 2 to subscribe to this topic" is incorrect as notifications to topics are pushed to subscribers. In this case we want the second microservice to pickup the messages when ready (pull them).INCORRECT: "Implement code in microservice 1 to send data to Amazon Kinesis Data Firehose. Implement code in microservice 2 to read from Kinesis Data Firehose" is incorrect as this is not how Firehose works. Firehose sends data directly to destinations, it is not a message queue.References:https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.ht ml Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application- integration/amazon-sqs/

Q34. A solutions architect at an ecommerce company wants to back up application log data to Amazon S3.The solutions architect is unsure how frequently the logs will be accessed or which logs will be accessed the most.The company wants to keep costs as low as possible by using the appropriate S3 storage class. Which S3 storage class should be implemented to meet these requirements?

A.S3 Glacier

B.S3 Intelligent-Tiering

C.S3 Standard-Infrequent Access (S3 Standard-IA)

D.S3 One Zone-Infrequent Access (S3 One Zone-IA)

正确答案 B

解析:

The S3 Intelligent-Tiering storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead. It works by storing objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequent access. This is an ideal use case for intelligent-tiering as the access patterns for the log files are not known. CORRECT: "S3 Intelligent-Tiering" is the correct answer. INCORRECT: "S3 Standard-Infrequent Access (S3 Standard-IA)" is incorrect as if the data is accessed often retrieval fees could become expensive. INCORRECT: "S3 One Zone-Infrequent Access (S3 One Zone-IA)" is incorrect as if the data is accessed often retrieval fees could become expensive. INCORRECT: "S3 Glacier" is incorrect as if the data is accessed often retrieval fees could become expensive. Glacier also requires more work in retrieving the data from the archive and quick access requirements can add further costs.References:https://aws.amazon.com/s3/storage-classes/#Unknown_or_changing_access Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/storage/amazon-s3/

Q35. A security team wants to limit access to specific services or actions in all of the team's AWS accounts.All accounts belong to a large organization in AWS Organizations. The solution must be scalable and there must be a single point where permissions can be maintained.What should a solutions architect do to accomplish this?

A.Create an ACL to provide access to the services or actions.

B.Create a security group to allow accounts and attach it to user groups

C.Create cross-account roles in each account to deny access to the services or actions.

D.Create a service control policy in the root organizational unit to deny access to the services or actions

正确答案 D

解析:

Service control policies (SCPs) offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization's access control guidelines.SCPs alone are not sufficient for allowing access in the accounts in your organization. Attaching an SCP to an AWS Organizations entity (root, OU, or account) defines a guardrail for what actions the principals can perform. You still need to attach identity-based or resource-based policies to principals or resources in your organization's accounts to actually grant permissions to them.CORRECT: "Create a service control policy in the root organizational unit to deny access to the services or actions" is the correct answer.INCORRECT: "Create an ACL to provide access to the services or actions" is incorrect as access control lists are not used for permissions associated with IAM. Permissions policies are used with IAM.INCORRECT: "Create a security group to allow accounts and attach it to user groups" is incorrect as security groups are instance level firewalls. They do not limit service actions. INCORRECT: "Create cross-account roles in each account to deny access to the services or actions" is incorrect as this is a complex solution and does not provide centralized control References:https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management- tools/aws-organizations/

Q36. You are trying to launch an EC2 instance, however the instance seems to go into a terminated status immediately. What would probably not be a reason that this is happening?

A.The AMI is missing a required part.

B.The snapshot is corrupt.

C.You need to create storage in EBS first.

D.You've reached your volume limit.

正确答案 C

解析:

Amazon EC2 provides a virtual computing environments, known as an instance. After you launch an instance, AWS recommends that you check its status to confirm that it goes from the pending status to the running status, the not terminated status. The following are a few reasons why an Amazon EBS-backed instance might immediately terminate:You've reached your volume limit.The AMI is missing a required part.The snapshot is corrupt.Reference:http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_InstanceStraightToTerminated.ht ml

Q37. You have set up an Auto Scaling group. The cool down period for the Auto Scaling group is 7 minutes. The first instance is launched after 3 minutes, while the second instance is launched after 4 minutes. How many minutes after the first instance is launched will Auto Scaling accept another scaling activity request?

A.11 minutes

B.7 minutes

C.10 minutes

D.14 minutes

正确答案 A

解析:

If an Auto Scaling group is launching more than one instance, the cool down period for each instance starts after that instance is launched. The group remains locked until the last instance that was launched has completed its cool down period. In this case the cool down period for the first instance starts after 3 minutes and finishes at the 10th minute (3+7 cool down), while for the second instance it starts at the 4th minute and finishes at the 11th minute (4+7 cool down). Thus, the Auto Scaling group will receive another request only after 11 minutes.
Reference:
http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/AS_Concepts.html

Q38. In Amazon EC2 Container Service components, what is the name of a logical grouping of container instances on which you can place tasks?

A.A cluster

B.A container instance

C.A container

D.A task definition

正确答案 A

解析:

Amazon ECS contains the following components:A Cluster is a logical grouping of container instances that you can place tasks on. A Container instance is an Amazon EC2 instance that is running the Amazon ECS agent and has been registered into a cluster.A Task definition is a description of an application that contains one or more container definitions. A Scheduler is the method used for placing tasks on container instances. A Service is an Amazon ECS service that allows you to run and maintain a specified number of instances of a task definition simultaneously.A Task is an instantiation of a task definition that is running on a container instance. A Container is a Linux container that

was created as part of a task. Reference: http://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcome.html

Q39. In the context of AWS support, why must an EC2 instance be unreachable for 20 minutes rather than allowing customers to open tickets immediately?

A.Because most reachability issues are resolved by automated processes in less than 20 minutes

B.Because all EC2 instances are unreachable for 20 minutes every day when AWS does routine maintenance

C.Because all EC2 instances are unreachable for 20 minutes when first launched

D.Because of all the reasons listed here

正确答案 A

解析:

An EC2 instance must be unreachable for 20 minutes before opening a ticket, because most reachability issues are resolved by automated processes in less than 20 minutes and will not require any action on the part of the customer. If the instance is still unreachable after this time frame has passed, then you should open a case with support. Reference: https://aws.amazon.com/premiumsupport/faqs/

Q40. Can a user get a notification of each instance start / terminate configured with Auto Scaling?

A.Yes, if configured with the Launch Config

B.Yes, always

C.Yes, if configured with the Auto Scaling group

D.No

正确答案 C

解析:

The user can get notifications using SNS if he has configured the notifications while creating the Auto Scaling group.Reference:http://docs.aws.amazon.com/AutoScaling/latest/DeveloperGuide/GettingStartedTutorial.html

Q41. Amazon EBS provides the ability to create backups of any Amazon EC2 volume into what is known as _____.

A.snapshots

B.images

C.instance backups

D.mirrors

正确答案 A

解析:

Amazon allows you to make backups of the data stored in your EBS volumes through snapshots that can later be used to create a new EBS volume.Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/Storage.html

Q42. To specify a resource in a policy statement, in Amazon EC2, can you use its Amazon Resource Name (ARN)?

A.Yes, you can.

B.No, you can't because EC2 is not related to ARN.

C.No, you can't because you can't specify a particular Amazon EC2 resource in an IAM policy.

D.Yes, you can but only for the resources that are not affected by the action.

正确答案 A

解析:

Some Amazon EC2 API actions allow you to include specific resources in your policy that can be created or modified by the action. To specify a resource in the statement, you need to use its Amazon Resource Name (ARN).Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-ug.pdf

Q43. After you recommend Amazon Redshift to a client as an alternative solution to paying data warehouses to analyze his data, your client asks you to explain why you are recommending Redshift. Which of the following would be a reasonable response to his request?

A.It has high performance at scale as data and query complexity grows.

B.It prevents reporting and analytic processing from interfering with the performance of OLTP workloads.

C.You don't have the administrative burden of running your own data warehouse and dealing with setup, durability, monitoring, scaling, and patching.

D.All answers listed are a reasonable response to his question

正确答案 D

解析:

Amazon Redshift delivers fast query performance by using columnar storage technology to improve I/O efficiency and parallelizing queries across multiple nodes. Redshift uses standard PostgreSQL JDBC and ODBC

drivers, allowing you to use a wide range of familiar SQL clients. Data load speed scales linearly with cluster size, with integrations to Amazon S3, Amazon DynamoDB, Amazon Elastic MapReduce, Amazon Kinesis or any SSH-enabled host. AWS recommends Amazon Redshift for customers who have a combination of needs, such as:High performance at scale as data and query complexity grows Desire to prevent reporting and analytic processing from interfering with the performance of OLTP workloads Large volumes of structured data to persist and query using standard SQL and existing BI tools Desire to the administrative burden of running one's own data warehouse and dealing with setup, durability, monitoring, scaling and patchingReference:
https://aws.amazon.com/running_databases/#redshift_anchor

Q44. One of the criteria for a new deployment is that the customer wants to use AWS Storage Gateway. However you are not sure whether you should use gateway-cached volumes or gateway-stored volumes or even what the differences are. Which statement below best describes those differences?

A.Gateway-cached lets you store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally.Gateway-stored enables you to configure your on-premises gateway to store all your data locally and then asynchronously back up point-in-time snapshots of this data to Amazon S3.

B.Gateway-cached is free whilst gateway-stored is not.

C.Gateway-cached is up to 10 times faster than gateway-stored.

D.Gateway-stored lets you store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally.Gateway-cached enables you to configure your on-premises gateway to store all your data locally and then asynchronously back up point-in-time snapshots of this data to Amazon S3.

正确答案 A

解析:

Volume gateways provide cloud-backed storage volumes that you can mount as Internet Small Computer System Interface (iSCSI) devices from your on-premises application servers. The gateway supports the following volume configurations:Gateway-cached volumes ?You store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally. Gateway-cached volumes offer a substantial cost savings on primary storage and minimize the need to scale your storage on- premises. You also retain low-latency access to your frequently accessed data. Gateway-stored volumes ?If you need low-latency access to your entire data set, you can configure your on-premises gateway to store all your data locally and then asynchronously back up point-in-time snapshots of this data to Amazon S3. This configuration provides durable and inexpensive off-site backups that you can recover to your local data center or Amazon EC2. For example, if you need replacement capacity for disaster recovery, you can recover the backups to Amazon EC2. Reference: http://docs.aws.amazon.com/storagegateway/latest/userguide/volume-gateway.html

Q45. A user is launching an EC2 instance in the US East region. Which of the below mentioned options is recommended by AWS with respect to the selection of the availability zone?

A.Always select the AZ while launching an instance

B.Always select the US-East-1-a zone for HA

C.Do not select the AZ; instead let AWS select the AZ

D.The user can never select the availability zone while launching an instance

正确答案 C

解析:

When launching an instance with EC2, AWS recommends not to select the availability zone (AZ). AWS specifies that the default Availability Zone should be accepted. This is because it enables AWS to select the best Availability Zone based on the system health and available capacity. If the user launches additional instances, only then an Availability Zone should be specified. This is to specify the same or different AZ from the running instances. Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability- zones.html

Q46. A company's website runs on Amazon EC2 instances behind an Application Load Balancer (ALB).The website has a mix of dynamic and static content Users around the globe are reporting that the website is slow.Which set of actions will improve website performance for users worldwide?

A.Create an Amazon CloudFront distribution and configure the ALB as an origin.Then update the Amazon Route 53 record to point to the CloudFront distribution.

B.Create a latency-based Amazon Route 53 record for the ALB.Then launch new EC2 instances with larger instance sizes and register the instances with the ALB.

C.Launch nev. EC2 instances hosting the same web application in different Regions closer to the users.Then register the instances with the same ALB using cross-Region VPC peering.

D.Host the website in an Amazon S3 bucket in the Regions closest to the users and delete the ALB and EC2 instances.Then update an Amazon Route 53 record to point to the S3 buckets.

正确答案 A

解析:

Amazon CloudFront is a content delivery network (CDN) that improves website performance by caching content at edge locations around the world. It can serve both dynamic and static content. This is the best solution for improving the performance of the website. CORRECT: "Create an Amazon CloudFront distribution and configure the ALB as an origin. Then update the Amazon Route 53 record to point to the CloudFront distribution" is the correct answer. INCORRECT: "Create a latency-based Amazon Route 53 record for the ALB. Then launch new EC2 instances with larger instance sizes and register the instances with the ALB" is incorrect. Latency routing routes based on the latency between the client and AWS. There is no mention in the answer about creating the new instances in another region therefore the only advantage is in using larger instance sizes. For a dynamic site this adds complexity in keeping the instances in sync.INCORRECT: "Launch new EC2 instances hosting the same web application in different Regions closer to the users. Use an AWS Transit Gateway to connect customers to the closest region" is incorrect as Transit Gateway is a service for connecting on-premises networks and VPCs to a single gateway.INCORRECT: "Migrate the website to an Amazon S3 bucket in the Regions closest to the users. Then create an Amazon Route 53 geolocation record to point to the S3 buckets" is incorrect as with S3 you can only host static websites, not dynamic websites.References:https://aws.amazon.com/cloudfront/dynamic-content/Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and- content-delivery/amazon-cloudfront/

Q47. A company wants to migrate a high performance computing (HPC) application and data from on- premises to the AWS Cloud.The company uses tiered storage on premises with hot high-performance parallel storage to support the application during periodic runs of the application and more economical cold storage to hold the data when the application is not actively running. Which combination of solutions should a solutions architect recommend to support the storage needs of the application? (Select TWO)

A.Amazon S3 for cold data storage

B.Amazon EFS for cold data storage

C.Amazon S3 for high-performance parallel storage

D.Amazon FSx for Lustre for high-performance parallel storage

E.Amazon FSx for Windows for high-performance parallel storage

正确答案 A,D

解析:

Amazon FSx for Lustre provides a high-performance file system optimized for fast processing of workloads such as machine learning, high-performance computing (HPC), video processing, financial modeling, and electronic design automation (EDA). These workloads commonly require data to be presented via a fast and scalable file system interface, and typically have data sets stored on long-term data stores like Amazon S3.Amazon FSx works natively with Amazon S3, making it easy to access your S3 data to run data processing workloads. Your S3 objects are presented as files in your file system, and you can write your results back to S3. This lets you run data processing workloads on FSx for Lustre and store your long- term data on S3 or on-premises data stores. Therefore, the best combination for this scenario is to use S3 for cold data and FSx for Lustre for the parallel HPC job.CORRECT: "Amazon S3 for cold data storage" is the correct answer. CORRECT: "Amazon FSx for Lustre for high-performance parallel storage" is the correct answer. INCORRECT: "Amazon EFS for cold data storage" is incorrect as FSx works natively with S3 which is also more economical.INCORRECT: "Amazon S3 for high-performance parallel storage" is incorrect as S3 is not suitable for running high-performance computing jobs. INCORRECT: "Amazon FSx for Windows for high-performance parallel storage" is incorrect as FSx for Lustre should be used for HPC use cases and use cases that require storing data on S3.References:https://aws.amazon.com/fsx/lustre/Save time with our exam-specific cheat

sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/storage/amazon-fsx/

Q48. A company has on-premises servers running a relational database. The current database serves high read traffic for users in different locations. The company wants to migrate to AWS with the least amount of effort. The database solution should support disaster recovery and not affect the company's current traffic flow.Which solution meets these requirements?

A.Use a database in Amazon RDS with Multi-AZ and at least one read replica

B.Use a database in Amazon RDS with Multi-AZ and at least one standby replica

C.Use databases hosted on multiple Amazon EC2 instances in different AWS Regions

D.Use databases hosted on Amazon EC2 instances behind an Application Load Balancer in different Availability Zones

正确答案 A

解析:

https://aws.amazon.com/blogs/database/implementing-a-disaster-recovery-strategy-with-amazon- rds/

Q49. A media streaming company collects real-time data and stores it in a disk-optimized database system.The company is not getting the expected throughput and wants an in-memory database storage solution that performs faster and provides high availability using data replication. Which database should a solutions architect recommend'?

A.Amazon RDS for MySQL

B.Amazon RDS for PostgreSQL

C.Amazon ElastiCache for Redis

D.Amazon ElastiCache for Memcached

正确答案C

解析:

Amazon ElastiCache is an in-memory database. With ElastiCache Memcached there is no data replication or high availability. As you can see in the diagram, each node is a separate partition of data:Therefore, the Redis engine must be used which does support both data replication and clustering. The following diagram shows a Redis architecture with cluster mode enabled:CORRECT: "Amazon ElastiCache for Redis" is the correct answer. INCORRECT: "Amazon ElastiCache for Memcached" is incorrect as Memcached does not support data replication or high availability.INCORRECT: "Amazon RDS for MySQL" is incorrect as this is not an in-memory database. INCORRECT: "Amazon RDS for PostgreSQL" is incorrect as this is not an in-memory database.References:https://aws.amazon.com/elasticache/redis/Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/database/amazon-elasticache/

Q50. A company's application is running on Amazon EC2 instances within an Auto Scaling group behind an Elastic Load Balancer.Based on the application's history, the company anticipates a spike in traffic during a holiday each year.A solutions architect must design a strategy to ensure that the Auto Scaling group proactively increases capacity to minimize any performance impact on application users. Which solution will meet these requirements?

A. Create an Amazon CloudWatch alarm to scale up the EC2 instances when CPU utilization exceeds 90%

B. Create a recurring scheduled action to scale up the Auto Scaling group before the expected period of peak demand

C. Increase the minimum and maximum number of EC2 instances in the Auto Scaling group during the peak demand period

D. Configure an Amazon Simple Notification Service (Amazon SNS) notification to send alerts when there are auto scaling EC2_INSTANCE_LAUNCH events

正确答案 B

解析:

AWS Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. AWS Auto Scaling refers to a collection of Auto Scaling capabilities across several AWS services. The services within the AWS Auto Scaling family include:Amazon EC2 (known as Amazon EC2 Auto Scaling).Amazon ECS.Amazon DynamoDB.Amazon Aurora.The scaling options define the triggers and when instances should be provisioned/de-provisioned.There are four scaling options:keep a specific or minimum number of instances running.Maintainuse maximum, minimum, or a specific number of instances.Manualincrease or decrease the number of instances based on a schedule.Scheduledscale based on real-time system metrics (e.g. CloudWatch metrics).DynamicThe following table describes the scaling options available and when to use them:The scaling options are configured through Scaling Policies which determine when, if, and how the ASG scales and shrinks.The following table describes the scaling policy types available for dynamic scaling policies and when to use them (more detail further down the page):The diagram below depicts an Auto Scaling group with a Scaling policy set to a minimum size of 1 instance,

a desired capacity of 2 instances, and a maximum size of 4 instances:Amazon EC2 Auto Scaling supports sending Amazon SNS notifications when the following events occur.References:Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws- auto-scaling/https://digitalcloud.training/certification-training/aws-solutions-architect-associate/management- tools/amazon-cloudwatch/https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application- integration/amazon-sns/

Q51. A company has a two-tier application architecture that runs in public and private subnets Amazon EC2 instances running the web application are in the public subnet and a database runs on the private subnet.The web application instances and the database are running in a single Availability Zone (AZ). Which combination of steps should a solutions architect take to provide high availability for this architecture? (Select TWO.)

A.Create new public and private subnets in the same AZ for high availability

B.Create an Amazon EC2 Auto Scaling group and Application Load Balancer spanning multiple AZs

C.Add the existing web application instances to an Auto Scaling group behind an Application Load Balancer

D.Create new public and private subnets in a new AZ Create a database using Amazon EC2 in one AZ

E.Create new public and private subnets in the same VPC each in a new AZ Migrate the database to an Amazon RDS multi-AZ deployment

正确答案 B,E

解析:

You would the EC2 instances to have high availability by placing them in multiple AZs.

Q52. A financial services company has a web application that serves users in the United States and Europe.The application consists of a database tier and a web server tier. The database tier consists of a MySQL database hosted in us-east-1 Amazon Route 53 geoproximity routing is used to direct traffic to instances in the closest Region. A performance review of the system reveals that European users are not receiving the same level of query performance as those in the United States.Which changes should be made to the database tier to improve performance?

A.Migrate the database to Amazon RDS for MySQL.Configure Multi-AZ in one of the European Regions.

B.Migrate the database to Amazon DynamoDB.Use DynamoDB global tables to enable replication to additional Regions.

C.Deploy MySQL instances in each Region.Deploy an Application Load Balancer in front of MySQL to reduce the load on the primary instance.

D.Migrate the database to an Amazon Aurora global database in MySQL compatibility mode.Configure read replicas in one of the European Regions.

正确答案 D

解析:

The issue here is latency with read queries being directed from Australia to UK which is great physical distance. A solution is required for improving read performance in Australia. An Aurora global database consists of one primary AWS Region where your data is mastered, and up to five read-only, secondary AWS Regions.Aurora replicates data to the secondary AWS Regions with typical latency of under a second. You issue write operations directly to the primary DB instance in the primary AWS

Region.This solution will provide better performance for users in the Australia Region for queries. Writes must still take place in the UK Region but read performance will be greatly improved. CORRECT: "Migrate the database to an Amazon Aurora global database in MySQL compatibility mode. Configure read replicas in ap-southeast-2" is the correct answer. INCORRECT: "Migrate the database to Amazon RDS for MySQL. Configure Multi-AZ in the Australian Region" is incorrect. The database is located in UK. If the database is migrated to Australia then the reverse problem will occur. Multi-AZ does not assist with improving query performance across Regions.INCORRECT: "Migrate the database to Amazon DynamoDB. Use DynamoDB global tables to enable replication to additional Regions" is incorrect as a relational database running on MySQL is unlikely to be compatible with DynamoDB.INCORRECT: "Deploy MySQL instances in each Region. Deploy an Application Load Balancer in front of MySQL to reduce the load on the primary instance" is incorrect as you can only put ALBs in front of the web tier, not the DB tier.References:https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/database/amazon-aurora/

Q53. A solutions architect is tasked with transferring 750 TB of data from a network-attached file system located at a branch office to Amazon S3 Glacier. The solution must avoid saturating the branch office's low-bandwidth internet connection.What is the MOST cost-effective solution1?

A.Create a site-to-site VPN tunnel to an Amazon S3 bucket and transfer the files directly.Create a bucket policy to enforce a VPC endpoint.

B.Order 10 AWS Snowball appliances and select an S3 Glacier vault as the destination.Create a bucket policy to enforce a VPC endpoint.

C.Mount the network-attached file system to Amazon S3 and copy the files directly.Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.

D.Order 10 AWS Snowball appliances and select an Amazon S3 bucket as the destination.Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier.

正确答案 D

解析:

As the company's internet link is low-bandwidth uploading directly to Amazon S3 (ready for transition to Glacier) would saturate the link. The best alternative is to use AWS Snowball appliances. The Snowball edge appliance can hold up to 75 TB of data so 10 devices would be required to migrate 750 TB of data.Snowball moves data into AWS using a hardware device and the data is then copied into an Amazon S3 bucket of your choice. From there, lifecycle policies can transition the S3 objects to Amazon S3 Glacier.CORRECT: "Order 10 AWS Snowball appliances and select an Amazon S3 bucket as the destination. Create a lifecycle policy to transition the S3 objects to Amazon S3 Glacier" is the correct answer.INCORRECT: "Order 10 AWS Snowball appliances and select an S3 Glacier vault as the destination. Create a bucket policy to enforce a VPC endpoint" is incorrect as you cannot set a Glacier vault as the destination, it must be an S3 bucket. You also can't enforce a VPC endpoint using a bucket policy.INCORRECT: "Create an AWS Direct Connect connection and migrate the data straight into Amazon Glacier" is incorrect as this is not the most cost- effective option and takes time to setup. INCORRECT: "Use AWS Global Accelerator to accelerate upload and optimize usage of the available bandwidth" is incorrect as this service is not used for accelerating or optimizing the upload of data from on-premises networks.References:https://docs.aws.amazon.com/snowball/latest/developer-guide/specifications.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/storage/amazon-s3/

Q54. A company's production application runs online transaction processing (OLTP) transactions on an Amazon RDS MySQL DB instance.The company is launching a new reporting tool that will access the same

data. The reporting tool must be highly available and not impact the performance of the production applicationHow can this be achieved'?

A.Create hourly snapshots of the production RDS DB instance.

B.Create a Multi-AZ RDS Read Replica of the production RDS DB instance.

C.Create multiple RDS Read Replicas of the production RDS DB instance.Place the Read Replicas in an Auto Scaling group.

D.Create a Single-AZ RDS Read Replica of the production RDS DB instance.Create a second Single-AZ RDS Read Replica from the replica.

正确答案 B

解析:

You can create a read replica as a Multi-AZ DB instance. Amazon RDS creates a standby of your replica in another Availability Zone for failover support for the replica. Creating your read replica as a Multi-AZ DB instance is independent of whether the source database is a Multi-AZ DB instance.CORRECT: "Create a Multi-AZ RDS Read Replica of the production RDS DB instance" is the correct answer.INCORRECT: "Create a Single-AZ RDS Read Replica of the production RDS DB instance. Create a second Single-AZ RDS Read Replica from the replica" is incorrect. Read replicas are primarily used for horizontal scaling. The best solution for high availability is to use a Multi-AZ read replica.INCORRECT: "Create a cross-region Multi-AZ deployment and create a read replica in the second region" is incorrect as you cannot create a cross- region Multi-AZ deployment with RDS. INCORRECT: "Use Amazon Data Lifecycle Manager to automatically create and manage snapshots" is incorrect as using snapshots is not the best solution for high availability.References:https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/
USER_MySQL.Replication.ReadReplicas.html#USER_MySQL.Replication.ReadReplicas.MultiAZ Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/database/amazon-rds/

Q55. A company allows its developers to attach existing IAM policies to existing IAM roles to enable faster experimentation and agility.However the security operations team is concerned that the developers could attach the existing administrator policy, which would allow the developers to circumvent any other security policies.How should a solutions architect address this issue?

A. Create an Amazon SNS topic to send an alert every time a developer creates a new policy

B. Use service control policies to disable IAM activity across all accounts in the organizational unit

C. Prevent the developers from attaching any policies and assign all IAM duties to the security operations team

D. Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy

正确答案 D

解析:

The permissions boundary for an IAM entity (user or role) sets the maximum permissions that the entity can have. This can change the effective permissions for that user or role. The effective permissions for an entity are the permissions that are granted by all the policies that affect the user or role. Within an account, the permissions for an entity can be affected by identity-based policies, resource-based policies, permissions boundaries, Organizations SCPs, or session policies.Therefore, the solutions architect can set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy. CORRECT: "Set an IAM permissions boundary on the developer IAM role that explicitly denies attaching the administrator policy" is the correct answer. INCORRECT: "Create an Amazon SNS topic to send an alert every time a developer creates a new policy" is incorrect as this would mean investigating every incident which is not an

efficient solution.INCORRECT: "Use service control policies to disable IAM activity across all accounts in the organizational unit" is incorrect as this would prevent the developers from being able to work with IAM completely.INCORRECT: "Prevent the developers from attaching any policies and assign all IAM duties to the security operations team" is incorrect as this is not necessary. The requirement is to allow developers to work with policies, the solution needs to find a secure way of achieving this.References:https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity- compliance/aws-iam/

Q56. A user is storing a large number of objects on AWS S3. The user wants to implement the search functionality among the objects. How can the user achieve this?

A.Use the indexing feature of S3.

B.Tag the objects with the metadata to search on that.

C.Use the query functionality of S3.

D.Make your own DB system which stores the S3 metadata for the search functionality.

正确答案 D

解析:

In Amazon Web Services, AWS S3 does not provide any query facility. To retrieve a specific object the user needs to know the exact bucket / object key. In this case it is recommended to have an own DB system which manages the S3 metadata and key mapping. Reference: http://media.amazonwebservices.com/AWS_Storage_Options.pdf

Q57. After setting up a Virtual Private Cloud (VPC) network, a more experienced cloud engineer suggests that to achieve low network latency and high network throughput you should look into setting up a placement group. You know nothing about this, but begin to do some research about it and are especially curious about its limitations. Which of the below statements is wrong in describing the limitations of a placement group?

A. Although launching multiple instance types into a placement group is possible, this reduces the likelihood that the required capacity will be available for your launch to succeed.

B. A placement group can span multiple Availability Zones.

C. You can't move an existing instance into a placement group.

D. A placement group can span peered VPCs

正确答案 B

解析:

这题从 wording 上看恐怕是 2018 年以前版本,彼时 placement group 应指 cluster placement group,因为另外两种还没有发布;因此在当时版本下,正确的选项应该是 B; 当然如果你强行认为该题适合当前服务的版本,那么其实 B 与 C 都可能是错误答案,因为在当前版本下,泛称的 placement group 不好说指的是哪一种,因为泛泛说 placement group can span multiple AZ 应该是不对的; 就按原始答案 B 吧 A placement group is a logical grouping of instances within a single Availability Zone. Using placement groups enables applications to participate in a low-latency, 10 Gbps network. Placement groups are recommended for applications that benefit from low network latency, high network throughput, or both. To provide the lowest latency, and the highest packet-per-second network performance for your placement group, choose an instance type that supports enhanced networking.Placement groups have the following limitations:The name you specify for a placement group a name must be unique within your AWS account. A placement group can't span multiple Availability Zones. Although launching multiple instance types into a placement group is possible, this reduces the likelihood that the required capacity will be available

for your launch to succeed. We recommend using the same instance type for all instances in a placement group. You can't merge placement groups. Instead, you must terminate the instances in one placement group, and then relaunch those instances into the other placement group. A placement group can span peered VPCs; however, you will not get full-bisection bandwidth between instances in peered VPCs. For more information about VPC peering connections, see VPC Peering in the Amazon VPC User Guide. You can't move an existing instance into a placement group. You can create an AMI from your existing instance, and then launch a new instance from the AMI into a placement group. Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

Q58. What is a placement group in Amazon EC2?

A.It is a group of EC2 instances within a single Availability Zone.

B.It the edge location of your web content.

C.It is the AWS region where you run the EC2 instance of your web content.

D.It is a group used to span multiple Availability Zones.

正确答案 A

解析:

A placement group is a logical grouping of instances within a single Availability Zone. Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

Q59. You are migrating an internal server on your DC to an EC2 instance with EBS volume. Your server disk usage is around 500GB so you just copied all your data to a 2TB disk to be used with AWS Import/Export. Where will the data be imported once it arrives at Amazon?

A.to a 2TB EBS volume

B.to an S3 bucket with 2 objects of 1TB

C.to an 500GB EBS volume

D.to an S3 bucket as a 2TB snapshot

正确答案 B

解析:

An import to Amazon EBS will have different results depending on whether the capacity of your storage device is less than or equal to 1 TB or greater than 1 TB. The maximum size of an Amazon EBS snapshot is 1 TB, so if the device image is larger than 1 TB, the image is chunked and stored on Amazon S3. The target location is determined based on the total capacity of the device, not the amount of data on the device.Reference:
http://docs.aws.amazon.com/AWSImportExport/latest/DG/Concepts.html

Q60. A client needs you to import some existing infrastructure from a dedicated hosting provider to AWS to try and save on the cost of running his current website. He also needs an automated process that manages backups, software patching, automatic failure detection, and recovery. You are aware that his existing set up currently uses an Oracle database. Which of the following AWS databases would be best for accomplishing this task?

A.Amazon RDS

B.Amazon Redshift

C.Amazon SimpleDB

D.Amazon ElastiCache

正确答案 A

解析:

Amazon RDS gives you access to the capabilities of a familiar MySQL, Oracle, SQL Server, or PostgreSQL database engine. This means that the code, applications, and tools you already use today with your existing databases can be used with Amazon RDS. Amazon RDS automatically patches the database software and backs up your database, storing the backups for a user- defined retention period and enabling point-in-time recovery. Reference: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html

Q61. True or false: A VPC contains multiple subnets, where each subnet can span multiple Availability Zones.

A.This is true only if requested during the set-up of VPC.

B.This is true.

C.This is false.

D.This is true only for US regions.

正确答案 C

解析:

A VPC can span several Availability Zones. In contrast, a subnet must reside within a single Availability Zone.Reference: https://aws.amazon.com/vpc/faqs/

Q62. An edge location refers to which Amazon Web Service?

A.An edge location is refered to the network configured within a Zone or Region

B.An edge location is an AWS Region

C.An edge location is the location of the data center used for Amazon CloudFront.

D.An edge location is a Zone within an AWS Region

正确答案C

解析:

Amazon CloudFront is a content distribution network. A content delivery network or content distribution network (CDN) is a large distributed system of servers deployed in multiple data centers across the world. The location of the data center used for CDN is called edge location. Amazon CloudFront can cache static content at each edge location. This means that your popular static content (e.g., your site's logo, navigational images, cascading style sheets, JavaScript code, etc.) will be available at a nearby edge location for the browsers to download with low latency and improved performance for viewers. Caching popular static content with Amazon CloudFront also helps you offload requests for such files from your origin sever - CloudFront serves the cached copy when available and only makes a request to your origin server if the edge location receiving the browser's request does not have a copy of the file.Reference: http://aws.amazon.com/cloudfront/

Q63. You are looking at ways to improve some existing infrastructure as it seems a lot of engineering resources are being taken up with basic management and monitoring tasks and the costs seem to be excessive. You are thinking of deploying Amazon ElasticCache to help. Which of the following statements is true in regards to ElasticCache?

A.You can improve load and response times to user actions and queries however the cost associated with scaling web applications will be more.

B.You can't improve load and response times to user actions and queries but you can reduce the cost associated with scaling web applications.

C.You can improve load and response times to user actions and queries however the cost associated with scaling web applications will remain the same.

D.You can improve load and response times to user actions and queries and also reduce the cost associated with scaling web applications.

正确答案 D

解析:

Amazon ElastiCache is a web service that makes it easy to deploy and run Memcached or Redis protocol-compliant server nodes in the cloud. Amazon ElastiCache improves the performance of web applications by allowing you to retrieve information from a fast, managed, in-memory caching system, instead of relying entirely on slower disk-based databases. The service simplifies and offloads the management, monitoring and operation of in-memory cache environments, enabling your engineering resources to focus on developing applications. Using Amazon ElastiCache, you can not only improve load and response times to user actions and queries, but also reduce the cost associated with scaling web applications.Reference: https://aws.amazon.com/elasticache/faqs/

Q64. Do Amazon EBS volumes persist independently from the running life of an Amazon EC2 instance?

A.Yes, they do but only if they are detached from the instance.

B.No, you cannot attach EBS volumes to an instance.

C.No, they are dependent.

D.Yes, they do.

正确答案 D

解析:

An Amazon EBS volume behaves like a raw, unformatted, external block device that you can attach to a single instance. The volume persists independently from the running life of an Amazon EC2 instance.Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/Storage.html

Q65. Your supervisor has asked you to build a simple file synchronization service for your department. He doesn't want to spend too much money and he wants to be notified of any changes to files by email. What do you think would be the best Amazon service to use for the email solution?

A.Amazon SES

B.Amazon CloudSearch

C.Amazon SWF

D.Amazon AppStream

正确答案 A

解析:

File change notifications can be sent via email to users following the resource with Amazon Simple Email Service (Amazon SES), an easy-to-use, cost-effective email solution.Reference:http://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_filesync_08.pdf

Q66. A product team is creating a new application that will store a large amount of data. The data will be analyzed hourly and modified by multiple Amazon EC2 Linux instances. The application team believes the amount of space needed will continue to grow for the next 6 months.Which set of actions should a solutions architect take to support these needs'?

A.Store the data in an Amazon EBS volume.Mount the EBS volume on the application instances

B.Store the data in an Amazon EFS file system.Mount the file system on the application instances.

C.Store the data in Amazon S3 Glacier.Update the vault policy to allow access to the application instances.

D.Store the data in Amazon S3 Standard-Infrequent Access (S3 Standard-IA).Update the bucket policy to allow access to the application instances.

正确答案 B

解析:

Amazon Elastic File System (Amazon EFS) provides a simple, scalable, fully managed elastic NFS file system for use with AWS Cloud services and on- premises resources. "It is built to scale on demand to petabytes without disrupting applications", "growing and shrinking automatically as you add and remove files", eliminating the need to provision and manage capacity to accommodate growth."The data will be analyzed hourly and modified by multiple Amazon EC2 Linux instances."

Q67. A gaming company has multiple Amazon EC2 instances in a single Availability Zone for its multiplayer game that communicates with users on Layer 4. The chief technology officer (CTO) wants to make the architecture highly available and cost- effective.What should a solutions architect do to meet these requirements? (Select TWO.)

A.Increase the number of EC2 instances.

B.Decrease the number of EC2 instances

C.Configure a Network Load Balancer in front of the EC2 instances.

D.Configure an Application Load Balancer in front of the EC2 instances

E.Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically.

正确答案 C,E

解析:

The solutions architect must enable high availability for the architecture and ensure it is cost- effective. To enable high availability an Amazon EC2 Auto Scaling group should be created to add and remove instances across multiple availability zones. In order to distribute the traffic to the instances the architecture should use a Network Load Balancer which operates at Layer 4. This architecture will also be cost-effective as the Auto Scaling group will ensure the right number of instances are running based on demand. CORRECT: "Configure a Network Load Balancer in front of the EC2 instances" is a correct answer.CORRECT: "Configure an Auto Scaling group to add or remove instances in multiple Availability Zones automatically" is also a correct answer.INCORRECT: "Increase the number of instances and use smaller EC2 instance types" is incorrect as this is not the most cost-effective option. Auto Scaling should be used to maintain the right number of active instances.INCORRECT: "Configure an Auto Scaling group to add or remove instances in the Availability Zone automatically" is incorrect as this is not highly available as it's a single AZ. INCORRECT: "Configure an Application Load Balancer in front of the EC2 instances" is incorrect as an ALB operates at Layer 7 rather than Layer 4.References:https://docsaws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/compute/amazon-ec2/ https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/elastic-load-balancing/

Q68. A company hosts an application on multiple Amazon EC2 instances. The application processes messages from an Amazon SQS queue writes to an Amazon RDS table and deletes the message from the queue Occasional duplicate records are found in the RDS table.The SQS queue does not contain any duplicate messages. What should a solutions archived do to ensure messages are being processed once only?

A.Use the CreateQueue API call to create a new queue

B.Use the AddPermission API call to add appropriate permissions

C.Use the ReceiveMessage API call to set an appropriate wait time.

D.Use the ChangeMessageVisibility API call to increase the visibility timeout

正确答案 D

解析:

Keyword: SQS queue writes to an Amazon RDSFrom this, Option D best suite & other Options ruled out [Option A - You can't intruduce one more Queue in the existing one; Option B - only Permission & Option C - Only Retrieves Messages]FIFO queues are designed to never introduce duplicate messages. However, your message producer might introduce duplicates in certain scenarios: for example, if the producer sends a message, does not receive a response, and then resends the same message. Amazon SQS APIs provide deduplication functionality that prevents your message producer from sending duplicates. Any duplicates introduced by the message producer are removed within a 5-minute deduplication interval.For standard queues, you might occasionally receive a duplicate copy of a message (at-least- once delivery). If you use a standard queue, you must design your applications to be idempotent (that is, they must not be affected adversely when processing the same message more than once).CreateQueue - You can't change the queue type after you create it and you can't convert an existing standard queue into a FIFO queue. You must either create a new FIFO queue for your application or delete your existing standard queue and recreate it as a FIFO queue.AddPermission - You create a queue, you have full control access rights for the queue. Only you, the owner of the queue, can grant or deny permissions to the queue.ReceiveMessage - Retrieves one or more messages (up to 10), from the specified queue.FIFO queues provide exactly-once processing, which means that each message is delivered once and remains available until a consumer processes it and deletes it.Visibility TimeoutAmazon SQSReferences:https://aws.amazon.com/sqs/?nc2=h_ql_prod_ap_sqshttps://aws.amazon.com/sqs/faqs/https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO- queues.html#FIFO-queues-exactly-once-

processinghttps://youtu.be/XrX7rb6M3jwhttps://docs.aws.amazon.com/AWSSimpleQueueService/latest/APIReference/API_ChangeMessageVisibility.htmlSave time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/application- integration/amazon-sqs/

Q69. A solutions architect is designing an application for a two-step order process. The first step is synchronous and must return to the user with little latency. The second step takes longer, so it will be implemented in a separate component Orders must be processed exactly once and in the order in which they are received. How should the solutions architect integrate these components?

A.Use Amazon SQS FIFO queues.

B.Use an AWS Lambda function along with Amazon SQS standard queues

C.Create an SNS topic and subscribe an Amazon SQS FIFO queue to that topic

D.Create an SNS topic and subscribe an Amazon SQS Standard queue to that topic.

正确答案 A

解析:

https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO- queues.html "Standard queues provide at-least-once delivery, which means that each message is delivered at least once.FIFO queues provide exactly-once processing, which means that each message is delivered once and remains available until a consumer processes it and deletes it. Duplicates are not introduced into the queue."

Q70. A solutions architect is designing a high performance computing (HPC) workload on Amazon EC2.The EC2 instances need to communicate to

each other frequently and require network performance with low latency and high throughput.Which EC2 configuration meets these requirements?

A.Launch the EC2 instances in a cluster placement group in one Availability Zone

B.Launch the EC2 instances in a spread placement group in one Availability Zone

C.Launch the EC2 instances in an Auto Scaling group in two Regions and peer the VPCs

D.Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones

正确答案 A

解析:

When you launch a new EC2 instance, the EC2 service attempts to place the instance in such a way that all of your instances are spread out across underlying hardware to minimize correlated failures. You can use placement groups to influence the placement of a group of interdependent instances to meet the needs of your workload.Depending on the type of workload, you can create a placement group using one of the following placement strategies:Cluster -packs instances close together inside an Availability Zone. This strategy enables workloads to achieve the low-latency network performance necessary for tightly-coupled node-to- node communication that is typical of HPC applications. Partition -spreads your instances across logical partitions such that groups of instances in one partition do not share the underlying hardware with groups of instances in different partitions. This strategy is typically used by large distributed and replicated workloads, such as Hadoop, Cassandra, and Kafka.Spread -strictly places a small group of instances across distinct underlying hardware to reduce correlated failures.For this scenario, a cluster placement group should be used as this is the best option for providing low-latency network performance for a HPC application. CORRECT: "Launch the EC2 instances in a cluster placement

group in one Availability Zone" is the correct answer.INCORRECT: "Launch the EC2 instances in a spread placement group in one Availability Zone" is incorrect as the spread placement group is used to spread instances across distinct underlying hardware.INCORRECT: "Launch the EC2 instances in an Auto Scaling group in two Regions. Place a Network Load Balancer in front of the instances" is incorrect as this does not achieve the stated requirement to provide low-latency, high throughput network performance between instances.Also, you cannot use an ELB across Regions.INCORRECT: "Launch the EC2 instances in an Auto Scaling group spanning multiple Availability Zones" is incorrect as this does not reduce network latency or improve performance.References:https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/compute/amazon-ec2/

Q71. A company is planning to use Amazon S3 lo store images uploaded by its users.The images must be encrypted at rest in Amazon S3.The company does not want to spend time managing and rotating the keys, but it does want to control who can access those keys.What should a solutions architect use to accomplish this?

A.Server-Side Encryption with keys stored in an S3 bucket

B.Server-Side Encryption with Customer-Provided Keys (SSE-C)

C.Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

D.Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

正确答案 D

解析:

SSE-KMS requires that AWS manage the data key but you manage the customer master key (CMK) in AWS KMS. You can choose a customer managed CMK or the AWS managed CMK for Amazon S3 in your account.Customer

managed CMKs are CMKs in your AWS account that you create, own, and manage. You have full control over these CMKs, including establishing and maintaining their key policies, IAM policies, and grants, enabling and disabling them, rotating their cryptographic material, adding tags, creating aliases that refer to the CMK, and scheduling the CMKs for deletion. For this scenario, the solutions architect should use SSE-KMS with a customer managed CMK. That way KMS will manage the data key but the company can configure key policies defining who can access the keys.CORRECT: "Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)" is the correct answer.INCORRECT: "Server-Side Encryption with keys stored in an S3 bucket" is incorrect as you cannot store your keys in a bucket with server-side encryption INCORRECT: "Server-Side Encryption with Customer-Provided Keys (SSE-C)" is incorrect as the company does not want to manage the keys.INCORRECT: "Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)" is incorrect as the company needs to manage access control for the keys which is not possible when they're managed by
Amazon.References:https://docs.aws.amazon.com/kms/latest/developerguide/services-s3.html#sse
https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#master_keys Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/storage/amazon-s3/
https://digitalcloud.training/certification-training/aws-solutions-architect-associate/security-identity-compliance/aws-kms/

Q72. An Amazon EC2 administrator created the following policy associated with an IAM group containing several users. What is the effect of this policy?

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:TerminateInstances",
            "Resources": "*",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "10.100.100.0/24"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "ec2:*",
            "Resources": "*",
            "Condition": {
                "StringNotEquals": {
                    "ec2:Region": "us-east-1"
                }
            }
        }
    ]
}
```

A. Users can terminate an EC2 instance in any AWS Region except us-east-1.

B. Users can terminate an EC2 instance with the IP address 10.100. 1001 in the us-east-1 Region.

C. Users can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.

D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.

正确答案 C

解析:

1. deny policy always overrides allow policy according to AWS 2. first statement says allow ec2 termination action coming from a IP address range (condiiton is the IP range) 3. second statement, deny all action on ec2 (now the condition is StringNotEquals, which means negated matching according to AWS), which implies deny all actions on ec2 so far as the request is not coming from us-east-1, that is allow actions only from us-east-1 (negate matching). 3. this would help you eliminate option A and D. now you are left with B and C 4. now remember deny rule takes effect before allow rule. 5. now users can terminate instances in us-east-1 as far as the IP range 10....whatever the range is.
Actually as per the policy both B and C are correct. But the IP 10.100.100.1 is the Reserved AWS IP and cannot be used by EC2 instance. What the policy means: 1. Allow termination of any instance if user's source ip address is 10.100. 100.254. 2. Deny termination of instances that are not in the us-east-1 region. Combining this two, you get: "Allow instance termination in the us-east-1 region if the user's source ip address is 10.100. 100.254. Deny termination operation on other regions."

Q73. A company is running an ecommerce application on Amazon EC2. The application consists of a stateless web tier that requires a minimum of 10 instances, and a peak of 250 instances to support the application's

usage. The application requires 50 instances 80% of the time.Which solution should be used to minimize costs?

A. Purchase Reserved Instances to cover 250 instances

B. Purchase Reserved Instances to cover 80 instances.Use Spot Instances to cover the remaining instances

C. Purchase On-Demand Instances to cover 40 instances.Use Spot Instances to cover the remaining instances

D. Purchase Reserved Instances to cover 50 instances.Use On-Demand and Spot Instances to cover the remaining instances

正确答案 D

解析:

On-Demand is default and really very expensive. Spot instance is like a bidding you can bid and use but if some one else bid more than you he will get the opportunity to grab the instance. Dedicated Host is for private and expensive. Reserved the instances for the particular time period and you will get the discount and it is some where near 60% (tentative) cheaper then the On-demand instance Discount for reserved instances goes from 40% to 60% for 1 year and 3 years commitment. In this scenario: 1 year of 50 Reserved instances is around the same price of 30 On-demand instances. https://aws.amazon.com/ec2/pricing/reserved-instances/ https://aws.amazon.com/ec2/pricing/on-demand/ https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html

Reserved Instances -

Having 50 EC2 RIs provide a discounted hourly rate and an optional capacity reservation for EC2 instances. AWS Billing automatically applies your RI's discounted rate when attributes of EC2 instance usage match attributes of an active RI.

If an Availability Zone is specified, EC2 reserves capacity matching the attributes of the RI. The capacity reservation of an RI is automatically utilized by running instances matching these attributes.

You can also choose to forego the capacity reservation and purchase an RI that is scoped to a region. RIs that are scoped to a region automatically apply the RI's discount to instance usage across AZs and instance sizes in a region, making it easier for you to take advantage of the RI's discounted rate.

On-Demand Instance -

On-Demand instances let you pay for compute capacity by the hour or second (minimum of 60 seconds) with no long-term commitments. This frees you from the costs and complexities of planning, purchasing, and maintaining hardware and transforms what are commonly large fixed costs into much smaller variable costs.

The pricing below includes the cost to run private and public AMIs on the specified operating system ("Windows Usage" prices apply to Windows Server 2003 R2,

2008, 2008 R2, 2012, 2012 R2, 2016, and 2019). Amazon also provides you with additional instances for Amazon EC2 running Microsoft Windows with SQL

Server, Amazon EC2 running SUSE Linux Enterprise Server, Amazon EC2 running Red Hat Enterprise Linux and Amazon EC2 running IBM that are priced differently.

Spot Instances -

A Spot Instance is an unused EC2 instance that is available for less than the On-Demand price. Because Spot Instances enable you to request unused EC2 instances at steep discounts, you can lower your Amazon EC2 costs significantly. The hourly price for a Spot Instance is called a Spot price. The Spot price of each instance type in each Availability Zone is set by Amazon EC2, and adjusted gradually based on the long-term supply of and demand for Spot Instances. Your

Spot Instance runs whenever capacity is available and the maximum price per hour for your request exceeds the Spot price.

Q74. Does DynamoDB support in-place atomic updates?

A.Yes

B.No

C.It does support in-place non-atomic updates

D.It is not defined

正确答案 A

解析:

DynamoDB supports in-place atomic updates.Reference:http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/WorkingWithItems.html#W orkingWithItems.AtomicCounters

Q75. Your manager has just given you access to multiple VPN connections that someone else has recently set up between all your company's offices. She needs you to make sure that the communication between the VPNs is secure. Which of the following services would be best for providing a low-cost hub-and-spoke model for primary or backup connectivity between these remote offices?

A.Amazon CloudFront

B.AWS Direct Connect

C.AWS CloudHSM

D.AWS VPN CloudHub

正确答案 D

解析:

If you have multiple VPN connections, you can provide secure communication between sites using the AWS VPN CloudHub. The VPN CloudHub operates on a simple hub-and-spoke model that you can use with or without a VPC. This design is suitable for customers with multiple branch offices and existing Internet connections who would like to implement a convenient, potentially low-cost hub-and-spoke model for

primary or backup connectivity between these remote offices. Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPN_CloudHub.html

Q76. Amazon EC2 provides a ____. It is an HTTP or HTTPS request that uses the HTTP verbs GET or POST.

A.web database

B..net framework

C.Query API

D.C library

正确答案C

解析:

Amazon EC2 provides a Query API. These requests are HTTP or HTTPS requests that use the HTTP verbs GET or POST and a Query parameter named Action. Reference: http://docs.aws.amazon.com/AWSEC2/latest/APIReference/making-api-requests.html

Q77. In Amazon AWS, which of the following statements is true of key pairs?

A.Key pairs are used only for Amazon SDKs.

B.Key pairs are used only for Amazon EC2 and Amazon CloudFront.

C.Key pairs are used only for Elastic Load Balancing and AWS IAM.

D.Key pairs are used for all Amazon services.

正确答案B

解析:

Key pairs consist of a public and private key, where you use the private key to create a digital signature, and then AWS uses the corresponding public key to validate the signature. Key pairs are used only for Amazon EC2 and Amazon CloudFront.Reference: http://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html

Q78. Does Amazon DynamoDB support both increment and decrement atomic operations?

A.Only increment, since decrement are inherently impossible with DynamoDB's data model.

B.No, neither increment nor decrement operations.

C.Yes, both increment and decrement operations.

D.Only decrement, since increment are inherently impossible with DynamoDB's data model.

正确答案 C

解析:

Amazon DynamoDB supports increment and decrement atomic operations.Reference:http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/APISummary.html

Q79. An organization has three separate AWS accounts, one each for development, testing, and production. The organization wants the testing team to have access to certain AWS resources in the production account. How can the organization achieve this?

A.It is not possible to access resources of one account with another account.

B.Create the IAM roles with cross account access.

C.Create the IAM user in a test account, and allow it access to the production environment with the IAM policy.

D.Create the IAM users with cross account access.

正确答案 B

解析:

An organization has multiple AWS accounts to isolate a development environment from a testing or production environment. At times the users from one account need to access resources in the other account, such as promoting an update from the development environment to the production environment. In this case the IAM role with cross account access will provide a solution. Cross account access lets one account share access to their resources with users in the other AWS accounts.Reference: http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf

Q80. You need to import several hundred megabytes of data from a local Oracle database to an Amazon RDS DB instance. What does AWS recommend you use to accomplish this?

A.Oracle export/import utilities

B.Oracle SQL Developer

C.Oracle Data Pump

D.DBMS_FILE_TRANSFER

正确答案 C

解析:

How you import data into an Amazon RDS DB instance depends on the amount of data you have and the number and variety of database objects in your database. For example, you can use Oracle SQL Developer to import a simple, 20 MB database; you want to use Oracle Data Pump to import complex databases or databases that are several hundred megabytes or

several terabytes in size.Reference:http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Oracle.Procedural.Importing.html

Q81. A user has created an EBS volume with 1000 IOPS. What is the average IOPS that the user will get for most of the year as per EC2 SLA if the instance is attached to the EBS optimized instance?

A.950

B.990

C.1000

D.900

正确答案 D

解析:

As per AWS SLA if the instance is attached to an EBS-Optimized instance, then the Provisioned IOPS volumes are designed to deliver within 10% of the provisioned IOPS performance 99.9% of the time in a given year. Thus, if the user has created a volume of 1000 IOPS, the user will get a minimum 900 IOPS 99.9% time of the year.Reference: http://aws.amazon.com/ec2/faqs/

Q82. You need to migrate a large amount of data into the cloud that you have stored on a hard disk and you decide that the best way to accomplish this is with AWS Import/Export and you mail the hard disk to AWS. Which of the following statements is incorrect in regards to AWS Import/Export?

A.It can export from Amazon S3

B.It can Import to Amazon Glacier

C.It can export from Amazon Glacier.

D.It can Import to Amazon EBS

正确答案C

解析:

AWS Import/Export supports:Import to Amazon S3Export from Amazon S3Import to Amazon EBSImport to Amazon GlacierAWS Import/Export does not currently support export from Amazon EBS or Amazon Glacier. Reference: https://docs.aws.amazon.com/AWSImportExport/latest/DG/whatisdisk.html

Q83. You are in the process of creating a Route 53 DNS failover to direct traffic to two EC2 zones. Obviously, if one fails, you would like Route 53 to direct traffic to the other region. Each region has an ELB with some instances being distributed. What is the best way for you to configure the Route 53 health check?

A.Route 53 doesn't support ELB with an internal health check.You need to create your own Route 53 health check of the ELB

B.Route 53 natively supports ELB with an internal health check. Turn "Evaluate target health" off and "Associate with Health Check" on and R53 will use the ELB's internal health check.

C.Route 53 doesn't support ELB with an internal health check. You need to associate your resource record set for the ELB with your own health check

D.Route 53 natively supports ELB with an internal health check. Turn "Evaluate target health" on and "Associate with Health Check" off and R53 will use the ELB's internal health check.

正确答案D

解析:

With DNS Failover, Amazon Route 53 can help detect an outage of your website and redirect your end users to alternate locations where your

application is operating properly. When you enable this feature, Route 53 uses health checks--regularly making Internet requests to your application's endpoints from multiple locations around the world--to determine whether each endpoint of your application is up or down. To enable DNS Failover for an ELB endpoint, create an Alias record pointing to the ELB and set the "Evaluate Target Health" parameter to true. Route 53 creates and manages the health checks for your ELB automatically. You do not need to create your own Route 53 health check of the ELB. You also do not need to associate your resource record set for the ELB with your own health check, because Route 53 automatically associates it with the health checks that Route 53 manages on your behalf. The ELB health check will also inherit the health of your backend instances behind that ELB. Reference: http://aws.amazon.com/about-aws/whats-new/2013/05/30/amazon-route-53-adds-elb- integration-for-dns- failover/

Q84. A user wants to use an EBS-backed Amazon EC2 instance for a temporary job. Based on the input data, the job is most likely to finish within a week. Which of the following steps should be followed to terminate the instance automatically once the job is finished?

A.Configure the EC2 instance with a stop instance to terminate it.

B.Configure the EC2 instance with ELB to terminate the instance when it remains idle.

C.Configure the CloudWatch alarm on the instance that should perform the termination action once the instance is idle.

D.Configure the Auto Scaling schedule activity that terminates the instance after 7 days.

正确答案C

解析:

Auto Scaling can start and stop the instance at a pre-defined time. Here, the total running time is unknown. Thus, the user has to use the

CloudWatch alarm, which monitors the CPU utilization. The user can create an alarm that is triggered when the average CPU utilization percentage has been lower than 10 percent for 24 hours, signaling that it is idle and no longer in use. When the utilization is below the threshold limit, it will terminate the instance as a part of the instance
action.Reference:http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/UsingAlarmActions.html

Q85. Which of the following is true of Amazon EC2 security group?

A.You can modify the outbound rules for EC2-Classic.

B.You can modify the rules for a security group only if the security group controls the traffic for just one instance.

C.You can modify the rules for a security group only when a new instance is created.

D.You can modify the rules for a security group at any time.

正确答案 D

解析:

A security group acts as a virtual firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances. You can modify the rules for a security group at any time; the new rules are automatically applied to all instances that are associated with the security group.Reference:
http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/using-network-security.html

Q86. An Elastic IP address (EIP) is a static IP address designed for dynamic cloud computing. With an EIP, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account. Your EIP is associated with your AWS account, not a particular EC2 instance, and it remains associated with your account until you choose to explicitly release it. By default how many EIPs is each AWS account limited to on a per region basis?

A.1

B.5

C.Unlimited

D.10

正确答案 B

解析:

By default, all AWS accounts are limited to 5 Elastic IP addresses per region for each AWS account, because public (IPv4) Internet addresses are a scarce public resource. AWS strongly encourages you to use an EIP primarily for load balancing use cases, and use DNS hostnames for all other inter-node communication.If you feel your architecture warrants additional EIPs, you would need to complete the Amazon EC2 Elastic IP Address Request Form and give reasons as to your need for additional addresses. Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html#using-instance-ad dressing-limit

Q87. An application running on AWS uses an Amazon Aurora Multi-AZ deployment for its database. When evaluating performance metrics, a solutions architect discovered that the database reads are causing high I/O and adding latency to the write requests against the database. What should the solutions architect do to separate the read requests from the write requests?

A. Enable read-through caching on the Amazon Aurora database

B. Update the application to read from the Multi-AZ standby instance

C. Create a read replica and modify the application to use the appropriate endpoint

D. Create a second Amazon Aurora database and link it to the primary database as a read replica.

正确答案 C

解析:

争议题，B 或者 C 都有道理 The primary DB instance is synchronously replicated across Availability Zones to a standby replica. So they use *SYNC* pattern to replicate data, if you push workload to standby instance, standby instance will run slow, and because primary need wait standby instance to commit data, the primary will get affected as well, the cost is even higher than request to primary directly.

Read replica pull data from primary instance in *async* way, so it doesn't effect primary's performance and availability. Well, the drawback is read replica may have a few seconds delay, so you cannot use read replica for any transactional work.

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

Aurora Replicas are independent endpoints in an Aurora DB cluster, best used for scaling read operations and increasing availability. Up to 15 Aurora Replicas can be distributed across the Availability Zones that a DB cluster spans within an AWS Region. The DB cluster volume is made up of multiple copies of the data for the DB cluster. However, the data in the cluster volume is represented as a single, logical volume to the primary instance and to Aurora Replicas in the DB cluster.As well as providing scaling for reads, Aurora Replicas are also targets for multi-AZ. In this case the solutions architect can update the application to read from the Multi-AZ standby instance. CORRECT: "Update the

application to read from the Multi-AZ standby instance" is the correct answer.INCORRECT: "Create a read replica and modify the application to use the appropriate endpoint" is incorrect. An Aurora Replica is both a standby in a Multi-AZ configuration and a target for read traffic. The architect simply needs to direct traffic to the Aurora Replica. INCORRECT: "Enable read through caching on the Amazon Aurora database." is incorrect as this is not a feature of Amazon Aurora.INCORRECT: "Create a second Amazon Aurora database and link it to the primary database as a read replica" is incorrect as an Aurora Replica already exists as this is a Multi-AZ configuration and the standby is an Aurora Replica that can be used for read traffic.References:https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/database/amazon-aurora/

Q88. An application runs on Amazon EC2 instances across multiple Availability Zones. The instances run in an Amazon EC2 Auto Scaling group behind an Application Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 40%. What should a solutions architect do to maintain the desired performance across all instances m the group?

A.Use a simple scaling policy to dynamically scale the Auto Scaling group

B.Use a target tracking policy to dynamically scale the Auto Scaling group

C.Use an AWS Lambda function to update the desired Auto Scaling group capacity

D.Use scheduled scaling actions to scale up and scale down the Auto Scaling group

正确答案 B

解析:

With target tracking scaling policies, you select a scaling metric and set a target value. Amazon EC2 Auto Scaling creates and manages the CloudWatch alarms that trigger the scaling policy and calculates the scaling adjustment based on the metric and the target value. The scaling policy adds or removes capacity as required to keep the metric at, or close to, the specified target value. In addition to keeping the metric close to the target value, a target tracking scaling policy also adjusts to the changes in the metric due to a changing load pattern. CORRECT: "Use a target tracking policy to dynamically scale the Auto Scaling group" is the correct answer.INCORRECT: "Use a simple scaling policy to dynamically scale the Auto Scaling group" is incorrect as target tracking is a better way to keep the aggregate CPU usage at around 40% INCORRECT: "Use an AWS Lambda function to update the desired Auto Scaling group capacity" is incorrect as this can be done automatically.INCORRECT: "Use scheduled scaling actions to scale up and scale down the Auto Scaling group" is incorrect as dynamic scaling is required to respond to changes in utilization.References:https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/compute/aws- auto-scaling/

Q89. A company runs a multi-tier web application that hosts news content. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an EC2 Auto Scaling group across multiple Availability Zones and use an Amazon Aurora database.A solutions architect needs to make the application more resilient to periodic increases in request rates.Which architecture should the solutions architect implement? (Select TWO)

A. Add AWS Shield.

B. Add Aurora Replicas

C. Add AWS Direct Connect

D. Add AWS Global Accelerator.

E. Add an Amazon CloudFront distribution in front of the Application Load Balancer

正确答案 B,E

解析:

ExplanationThe architecture is already highly resilient but the may be subject to performance degradation if there are sudden increases in request rates. To resolve this situation Amazon Aurora Read Replicas can be used to serve read traffic which offloads requests from the main database. On the frontend an Amazon CloudFront distribution can be placed in front of the ALB and this will cache content for better performance and also offloads requests from the backend. CORRECT: "Add Amazon Aurora Replicas" is the correct answer.
CORRECT: "Add an Amazon CloudFront distribution in front of the ALB" is the correct answer. INCORRECT: "Add and Amazon WAF in front of the ALB" is incorrect. A web application firewall protects applications from malicious attacks. It does not improve performance. INCORRECT: "Add an Amazon Transit Gateway to the Availability Zones" is incorrect as this is used to connect on-premises networks to VPCs. INCORRECT: "Add an Amazon Global Accelerator endpoint" is incorrect as this service is used for directing users to different instances of the application in different regions based on latency.
References:https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.
htmlSave time with our exam-specific cheat sheets:
https://digitalcloud.training/certification-training/aws-solutions-architect- associate/database/amazon-aurora/

https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and- content-delivery/amazon-cloudfront/

Q90. A solutions architect is optimizing a website for an upcoming musical event Videos of the performances will be streamed in real time and then will be available on demand. The event is expected to attract a global online audience. Which service will improve the performance of both the real-time and on-demand streaming?

A.Amazon CloudFront

B.AWS Global Accelerator

C.Amazon Route 53

D.Amazon S3 Transfer Acceleration

正确答案 A

解析:

Amazon CloudFront can be used to stream video to users across the globe using a wide variety of protocols that are layered on top of HTTP. This can include both on-demand video as well as real time streaming video.CORRECT: "Amazon CloudFront" is the correct answer.INCORRECT: "AWS Global Accelerator" is incorrect as this would be an expensive way of getting the content closer to users compared to using CloudFront. As this is a use case for CloudFront and there are so many edge locations it is the better option. INCORRECT: "Amazon Route 53" is incorrect as you still need a solution for getting the content closer to users.INCORRECT: "Amazon S3 Transfer Acceleration" is incorrect as this is used to accelerate uploads of data to Amazon S3 buckets.References:https://aws.amazon.com/cloudfront/streaming/https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/on-demand-streaming- video.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-

solutions-architect-associate/networking-and- content-delivery/amazon-cloudfront/

Q91. A company serves content to its subscribers across the world using an application running on AWS.The application has several Amazon EC2 instances in a private subnet behind an Application Load Balancer (ALB).Due to a recent change in copyright restrictions the chief information officer (CIO) wants to block access for certain countries.Which action will meet these requirements?

A.Modify the ALB security group to deny incoming traffic from blocked countries

B.Modify the security group for EC2 instances to deny incoming traffic from blocked countries

C.Use Amazon CloudFront to serve the application and deny access to blocked countries

D.Use ALB listener rules to return access denied responses to incoming traffic from blocked countries

正确答案 C

解析:

When a user requests your content, CloudFront typically serves the requested content regardless of where the user is located. If you need to prevent users in specific countries from accessing your content, you can use the CloudFront geo restriction feature to do one of the following:Allow your users to access your content only if they're in one of the countries on a whitelist of approved countries.Prevent your users from accessing your content if they're in one of the countries on a blacklist of banned countries.For example, if a request comes from a country where, for copyright reasons, you are not authorized to distribute your content, you can use CloudFront geo restriction to block the request. This is the easiest and most effective way to implement a

geographic restriction for the delivery of content.CORRECT: "Use Amazon CloudFront to serve the application and deny access to blocked countries" is the correct answer.INCORRECT: "Use a Network ACL to block the IP address ranges associated with the specific countries" is incorrect as this would be extremely difficult to manage. INCORRECT: "Modify the ALB security group to deny incoming traffic from blocked countries" is incorrect as security groups cannot block traffic by country. INCORRECT: "Modify the security group for EC2 instances to deny incoming traffic from blocked countries" is incorrect as security groups cannot block traffic by country.References:https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and- content-delivery/amazon-cloudfront/

Q92. A manufacturing company wants to implement predictive maintenance on its machinery equipment.The company will install thousands of loT sensors that will send data to AWS in real time. A solutions architect is tasked with implementing a solution that will receive events in an ordered manner for each machinery asset and ensure that data is saved for further processing at a later time.Which solution would be MOST efficient?

A.Use Amazon Kinesis Data Streams for real-time events with a partition for each equipment asset.Use Amazon Kinesis Data Firehose to save data to Amazon S3.

B.Use Amazon Kinesis Data Streams for real-time events with a shard for each equipment asset.Use Amazon Kinesis Data Firehose to save data to Amazon EBS.

C.Use an Amazon SQS FIFO queue for real-time events with one queue for each equipment asset.Trigger an AWS Lambda function for the SQS queue to save data to Amazon EFS.

D.Use an Amazon SQS standard queue for real-time events with one queue for each equipment asset.Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3.

正确答案 A

解析:

Amazon Kinesis Data Streams collect and process data in real time. A Kinesis data stream is a set of shards. Each shard has a sequence of data records. Each data record has a sequence number that is assigned by Kinesis Data Streams. A shard is a uniquely identified sequence of data records in a stream.A partition key is used to group data by shard within a stream. Kinesis Data Streams segregates the data records belonging to a stream into multiple shards. It uses the partition key that is associated with each data record to determine which shard a given data record belongs to.For this scenario, the solutions architect can use a partition key for each device. This will ensure the records for that device are grouped by shard and the shard will ensure ordering. Amazon S3 is a valid destination for saving the data records.CORRECT: "Use Amazon Kinesis Data Streams for real-time events with a partition key for each device. Use Amazon Kinesis Data Firehose to save data to Amazon S3" is the correct answer. INCORRECT: "Use Amazon Kinesis Data Streams for real-time events with a shard for each device. Use Amazon Kinesis Data Firehose to save data to Amazon EBS" is incorrect as you cannot save data to EBS from Kinesis.INCORRECT: "Use an Amazon SQS FIFO queue for real-time events with one queue for each device. Trigger an AWS Lambda function for the SQS queue to save data to Amazon EFS" is incorrect as SQS is not the most efficient service for streaming, real time data. INCORRECT: "Use an Amazon SQS standard queue for real-time events with one queue for each device. Trigger an AWS Lambda function from the SQS queue to save data to Amazon S3" is incorrect as SQS is not the most efficient service for streaming, real time data.References:https://docs.aws.amazon.com/streams/latest/dev/key-concepts.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect- associate/analytics/amazon-kinesis/

Q93. A company has deployed an API in a VPC behind an internet-facing Application Load Balancer (ALB).An application that consumes the API as a client is deployed in a second account in private subnets behind a NAT gateway.When requests to the client application increase, the NAT gateway costs are higher than expected.A solutions architect has configured the ALB to be internal. Which combination of architectural changes will reduce the NAT gateway costs'? (Select TWO)

A.Configure a VPC peering connection between the two VPCs.Access the API using the private address

B.Configure an AWS Direct Connect connection between the two VPCs.Access the API using the private address.

C.Configure a ClassicLink connection for the API into the client VPC.Access the API using the ClassicLink address.

D.Configure a PrivateLink connection for the API into the client VPC.Access the API using the PrivateLink address.

E.Configure an AWS Resource Access Manager connection between the two accounts.Access the API using the private address

正确答案 A,D

解析:

You can create your own application in your VPC and configure it as an AWS PrivateLink- powered service (referred to as an endpoint service). Other AWS principals can create a connection from their VPC to your endpoint service using an interface VPC endpoint. You are the service provider, and the AWS principals that create connections to your service are service consumers.This configuration is powered by AWS PrivateLink and clients do not need to use an internet gateway, NAT device, VPN connection or AWS Direct Connect connection, nor do they require public IP addresses.Another option is to use a VPC Peering connection. A VPC peering connection is a networking connection between two VPCs that

enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account.CORRECT: "Configure a VPC peering connection between the two VPCs. Access the API using the private address" is a correct answer.CORRECT: "Configure a PrivateLink connection for the API into the client VPC. Access the API using the PrivateLink address" is also a correct answer. INCORRECT: "Configure an AWS Direct Connect connection between the two VPCs. Access the API using the private address" is incorrect. Direct Connect is used for connecting from on- premises data centers into AWS. It is not used from one VPC to another. INCORRECT: "Configure a ClassicLink connection for the API into the client VPC. Access the API using the ClassicLink address" is incorrect.ClassicLink allows you to link EC2-Classic instances to a VPC in your account, within the same Region. This is not relevant to sending data between two VPCs. INCORRECT: "Configure an AWS Resource Access Manager connection between the two accounts. Access the API using the private address" is incorrect. AWS RAM lets you share resources that are provisioned and managed in other AWS services. However, APIs are not shareable resources with AWS
RAM.References:https://docs.aws.amazon.com/vpc/latest/userguide/endpoint-service.html https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html Save time with our exam-specific cheat sheets:https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and- content-delivery/amazon-vpc/

Q94. In Amazon EC2, partial instance-hours are billed _____.

A.per second used in the hour

B.per minute used

C.by combining partial segments into full hours

D.as full hours

正确答案 D

解析:

Partial instance-hours are billed to the next hour.Reference: http://aws.amazon.com/ec2/faqs/

Q95. In EC2, what happens to the data in an instance store if an instance reboots (either intentionally or unintentionally)?

A.Data is deleted from the instance store for security reasons.

B.Data persists in the instance store.

C.Data is partially present in the instance store.

D.Data in the instance store will be lost.

正确答案 B

解析:

The data in an instance store persists only during the lifetime of its associated instance. If an instance reboots (intentionally or unintentionally), data in the instance store persists. However, data on instance store volumes is lost under the following circumstances.Failure of an underlying driveStopping an Amazon EBS-backed instanceTerminating an instanceReference:http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/InstanceStorage.html

Q96. You are setting up a VPC and you need to set up a public subnet within that VPC. Which following requirement must be met for this subnet to be considered a public subnet?

A.Subnet's traffic is not routed to an internet gateway but has its traffic routed to a virtual private gateway.

B.Subnet's traffic is routed to an internet gateway.

C.Subnet's traffic is not routed to an internet gateway.

D.None of these answers can be considered a public subnet.

正确答案 B

解析:

A virtual private cloud (VPC) is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS cloud. You can launch your AWS resources, such as Amazon EC2 instances, into your VPC. You can configure your VPC: you can select its IP address range, create subnets, and configure route tables, network gateways, and security settings. A subnet is a range of IP addresses in your VPC. You can launch AWS resources into a subnet that you select. Use a public subnet for resources that must be connected to the internet, and a private subnet for resources that won't be connected to the Internet. If a subnet's traffic is routed to an internet gateway, the subnet is known as a public subnet. If a subnet doesn't have a route to the internet gateway, the subnet is known as a private subnet. If a subnet doesn't have a route to the internet gateway, but has its traffic routed to a virtual private gateway, the subnet is known as a VPN-only subnet.Reference:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html

Q97. Can you specify the security group that you created for a VPC when you launch an instance in EC2-Classic?

A.No, you can specify the security group created for EC2-Classic when you launch a VPC instance.

B.No

C.Yes

D.No, you can specify the security group created for EC2-Classic to a non-VPC based instance only.

正确答案 B

解析:

If you're using EC2-Classic, you must use security groups created specifically for EC2-Classic. When you launch an instance in EC2-Classic, you must specify a security group in the same region as the instance. You can't specify a security group that you created for a VPC when you launch an instance in EC2-Classic.Reference:http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html#ec2-classic- securit y-groups

Q98. While using the EC2 GET requests as URLs, the _____ is the URL that serves as the entry point for the web service.

A.token

B.endpoint

C.action

D.None of these

正确答案 B

解析:

The endpoint is the URL that serves as the entry point for the web service. Reference: http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/using-query-api.html