Amazon.SAA-C03.vNov-2023..by.Pen.212q

Number: Nov-2023
Passing Score: 800
Time Limit: 120
File Version: 13.0

Exam Code: SAA-C03

Exam Name: AWS Certified Solutions Architect – Associate

Exam A

QUESTION 1
A company is migrating its on-premises workload to the AWS Cloud. The company already uses several Amazon EC2 instances and Amazon RDS DB instances. The company wants a solution that automatically starts and stops the EC2 instances and D6 instances outside of business hours. The solution must minimize cost and infrastructure maintenance. Which solution will meet these requirement?

A. Scale the EC2 instances by using elastic resize Scale the DB instances to zero outside of business hours
B. Explore AWS Marketplace for partner solutions that will automatically start and stop the EC2 Instances and OB instances on a schedule
C. Launch another EC2 instance. Configure a crontab schedule to run shell scripts that will start and stop the existing EC2 instances and DB instances on a schedule.
D. Create an AWS Lambda function that will start and stop the EC2 instances and DB instances Configure Amazon EventBridge to invoke the Lambda function on a schedule

Correct Answer: D
Section:

QUESTION 2
A company hosts a three-tier ecommerce application on a fleet of Amazon EC2 instances. The instances run in an Auto Scaling group behind an Application Load Balancer (ALB) All ecommerce data is stored in an Amazon RDS for ManaDB Multi-AZ DB instance The company wants to optimize customer session management during transactions The application must store session data durably Which solutions will meet these requirements? (Select TWO)

A. Turn on the sticky sessions feature (session affinity) on the ALB
B. Use an Amazon DynamoOB table to store customer session information
C. Deploy an Amazon Cognito user pool to manage user session information
D. Deploy an Amazon ElastiCache for Redis cluster to store customer session information
E. Use AWS Systems Manager Application Manager in the application to manage user session information

Correct Answer: A, D
Section:
Explanation:
https://aws.amazon.com/caching/session-management/

QUESTION 3

A company is running a batch application on Amazon EC2 instances. The application consists of a backend with multiple Amazon RDS databases. The application is causing a high number of leads on the databases. A solutions architect must reduce the number of database reads while ensuring high availability.

What should the solutions architect do to meet this requirement?

A. Add Amazon RDS read replicas
B. Use Amazon ElasbCache for Redls
C. Use Amazon Route 53 DNS caching
D. Use Amazon ElastiCache for Memcached

Correct Answer: A
Section:

QUESTION 4
A company has a web application that is based on Java and PHP. The company plans to move the application from on premises to AWS. The company needs the ability to test new site features frequently. The company also needs a highly available and managed solution that requires minimum operational overhead.
Which solution will meet these requirements?

A. Create an Amazon S3 bucket Enable static web hosting on the S3 bucket Upload the static content to the S3 bucket Use AWS Lambda to process all dynamic content
B. Deploy the web application to an AWS Elastic Beanstalk environment Use URL swapping to switch between multiple Elastic Beanstalk environments for feature testing
C. Deploy the web application lo Amazon EC2 instances that are configured with Java and PHP Use Auto Scaling groups and an Application Load Balancer to manage the website's availability
D. Containerize the web application Deploy the web application to Amazon EC2 instances Use the AWS Load Balancer Controller to dynamically route traffic between containers thai contain the new site features for testing

Correct Answer: B
Section:

QUESTION 5
A telemarketing company is designing its customer call center functionality on AWS. The company needs a solution that provides multiple speaker recognition and generates transcript files. The company wants to query the transcript files to analyze the business patterns. The transcript files must be stored for 7 years for auditing purposes.
Which solution will meet these requirements?

A. Use Amazon Rekognition for multiple speaker recognition. Store the transcript files in Amazon S3. Use machine learning models for transcript file analysis.
B. Use Amazon Transcribe for multiple speaker recognition. Use Amazon Athena for transcript file analysis.
C. Use Amazon Translate for multiple speaker recognition. Store the transcript files in Amazon Redshift. Use SQL queries for transcript file analysis.
D. Use Amazon Rekognition for multiple speaker recognition. Store the transcript files in Amazon S3. Use Amazon Textract for transcript file analysis.

Correct Answer: B
Section:
Explanation:
Amazon Transcribe now supports speaker labeling for streaming transcription. Amazon Transcribe is an automatic speech recognition (ASR) service that makes it easy for you to convert speech-to-text.In live audio transcription, each stream of audio may contain multiple speakers. Now you can conveniently turn on the ability to label speakers, thus helping to identify who is saying what in theoutput transcript.
https://aws.amazon.com/about-aws/whats-new/2020/08/amazon-transcribe- supports-speaker-labeling-streaming-transcription/

QUESTION 6
A company is building a new dynamic ordering website. The company wants to minimize server maintenance and patching. The website must be highly available and must scale read and write capacity as quickly as possible to meet changes in user demand.
Which solution will meet these requirements?

A. Host static content in Amazon S3 Host dynamic content by using Amazon API Gateway and AWS Lambda Use Amazon DynamoDB with on-demand capacity for the database Configure Amazon CtoudFront to deliver the website content

B. Host static content in Amazon S3 Host dynamic content by using Amazon API Gateway and AWS Lambda Use Amazon Aurora with Aurora Auto Scaling for the database Configure Amazon CloudFront to deliver the website content
C. Host al the website content on Amazon EC2 instances Create an Auto Scaling group to scale the EC2 Instances Use an Application Load Balancer to distribute traffic Use Amazon DynamoDB with provisioned write capacity for the database
D. Host at the website content on Amazon EC2 instances Create an Auto Scaling group to scale the EC2 instances Use an Application Load Balancer to distribute traffic Use Amazon Aurora with Aurora Auto Scaling for the database

Correct Answer: A
Section:

QUESTION 7
A company hosts its application on AWS The company uses Amazon Cognito to manage users When users log in to the application the application fetches required data from Amazon DynamoOB by using a REST API that is hosted in Amazon API Gateway. The company wants an AWS managed solution that will control access to the REST API to reduce development efforts
Which solution will meet these requirements with the LEAST operational overhead?

A. Configure an AWS Lambda function to be an authorize! in API Gateway to validate which user made the request
B. For each user, create and assign an API key that must be sent with each request Validate the key by using an AWS Lambda function
C. Send the user's email address in the header with every request Invoke an AWS Lambda function to validate that the user with that email address has proper access
D. Configure an Amazon Cognito user pool authorizer in API Gateway to allow Amazon Cognito to validate each request

Correct Answer: D
Section:

QUESTION 8
A company must migrate 20 TB of data from a data center to the AWS Cloud within 30 days. The company's network bandwidth is limited to 15 Mbps and cannot exceed 70% utilization. What should a solutions architect do to meet these requirements?

A. Use AWS Snowball.
B. Use AWS DataSync.
C. Use a secure VPN connection.
D. Use Amazon S3 Transfer Acceleration.

Correct Answer: A
Section:
Explanation:
AWS Snowball is a secure data transport solution that accelerates moving large amounts of data into and out of the AWS cloud. It can move up to 80 TB of data at a time, and provides a network bandwidth of up to 50 Mbps, so it is well- suited for the task. Additionally, it is secure and easy to use, making it the ideal solution for this migration.

QUESTION 9
A company is experiencing sudden increases in demand. The company needs to provision large Amazon EC2 instances from an Amazon Machine image (AMI) The instances will run m an Auto Scaling group. The company needs a solution that provides minimum initialization latency to meet the demand.
Which solution meets these requirements?

A. Use the aws ec2 register-image command to create an AMI from a snapshot Use AWS Step Functions to replace the AMI in the Auto Scaling group
B. Enable Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot Provision an AMI by using the snapshot Replace the AMI m the Auto Scaling group with the new AMI
C. Enable AMI creation and define lifecycle rules in Amazon Data Lifecycle Manager (Amazon DLM) Create an AWS Lambda function that modifies the AMI in the Auto Scaling group
D. Use Amazon EventBridge (Amazon CloudWatch Events) to invoke AWS Backup lifecycle policies that provision AMIs Configure Auto Scaling group capacity limits as an event source in EventBridge

Correct Answer: B
Section:
Explanation:
Enabling Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot allows you to quickly create a new Amazon Machine Image (AMI) from a snapshot, which can help reduce the initialization latency when provisioning new instances. Once the AMI is provisioned, you can replace the AMI in the Auto Scaling group with the new AMI. This will ensure that new instances are launched from the updated AMI and are able to meet the increased demand quickly.

QUESTION 10
An ecommerce company needs to run a scheduled daily job to aggregate and filler sales records for analytics. The company stores the sales records in an Amazon S3 bucket. Each object can be up to 10 G6 in size Based on the number of sales events, the job can take up to an hour to complete. The CPU and memory usage of the fob are constant and are known in advance. A solutions architect needs to minimize the amount of operational effort that is needed for the job to run. Which solution meets these requirements?

A. Create an AWS Lambda function that has an Amazon EventBridge notification Schedule the EventBridge event to run once a day
B. Create an AWS Lambda function Create an Amazon API Gateway HTTP API, and integrate the APIwith the function Create an Amazon EventBridge scheduled avert that calls the API and invokes thefunction.
C. Create an Amazon Elastic Container Service (Amazon ECS) duster with an AWS Fargate launch type. Create an Amazon EventBridge scheduled event that launches an ECS task on the cluster to run the job.
D. Create an Amazon Elastic Container Service (Amazon ECS) duster with an Amazon EC2 launch type and an Auto Scaling group with at least one EC2 instance. Create an Amazon EventBridge scheduled event that launches an ECS task on the duster to run the job.

Correct Answer: C
Section:

QUESTION 11
A company runs an application on Amazon EC2 Linux instances across multiple Availability Zones. The application needs a storage layer that is highly available and Portable Operating System Interface (POSIX) compliant. The storage layer must provide maximum data durability and must be shareable across the EC2 instances. The data in the storage layer will be accessed frequency for the first 30 days and will be accessed infrequently alter that time. Which solution will meet these requirements MOST cost-effectively?

A. Use the Amazon S3 Standard storage class Create an S3 Lifecycle policy to move infrequently accessed data to S3 Glacier
B. Use the Amazon S3 Standard storage class. Create an S3 Lifecycle policy to move infrequently accessed data to S3 Standard-Infrequent Access (EF3 Standard-IA).
C. Use the Amazon Elastic File System (Amazon EFS) Standard storage class. Create a Lifecycle management policy to move infrequently accessed data to EFS Standard-Infrequent Access (EFS Standard-IA)
D. Use the Amazon Elastic File System (Amazon EFS) One Zone storage class. Create a Lifecycle management policy to move infrequently accessed data to EFS One Zone-Infrequent Access (EFS One Zone-IA).

Correct Answer: C
Section:
Explanation:

QUESTION 12
A company wants to migrate its 1 PB on-premises image repository to AWS. The images will be used by a serverless web application Images stored in the repository are rarely accessed, but they must be immediately available Additionally, the images must be encrypted at rest and protected from accidental deletion Which solution meets these requirements?

A. Implement client-side encryption and store the images in an Amazon S3 Glacier vault Set a vault lock to prevent accidental deletion
B. Store the images in an Amazon S3 bucket in the S3 Standard-Infrequent Access (S3 Standard-IA) storage class Enable versioning default encryption and MFA Delete on the S3 bucket.
C. Store the images in an Amazon FSx for Windows File Server file share Configure the Amazon FSx file share to use an AWS Key Management Service (AWS KMS) customer master key (CMK) to encrypt the images in the file share Use NTFS permission sets on the images to prevent accidental deletion
D. Store the images in an Amazon Elastic File System (Amazon EFS) file share in the Infrequent Access storage class Configure the EFS file share to use an AWS Key Management Service (AWS KMS) customer master key (CMK) to encrypt the images in the file share. Use NFS permission sets on the images to prevent accidental deletion

Correct Answer: B
Section:

QUESTION 13
A company runs an application that receives data from thousands of geographically dispersed remote devices that use UDP The application processes the data immediately and sends a message back to the device if necessary No data is stored.
The company needs a solution that minimizes latency for the data transmission from the devices. The solution also must provide rapid failover to another AWS Region Which solution will meet these requirements?

A. Configure an Amazon Route 53 failover routing policy Create a Network Load Balancer (NLB) in each of the two Regions Configure the NLB to invoke an AWS Lambda function to process the data
B. Use AWS Global Accelerator Create a Network Load Balancer (NLB) in each of the two Regions as an endpoint. Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type Create an ECS service on the cluster Set the ECS service as the target for the NLB Process the data in Amazon ECS.
C. Use AWS Global Accelerator Create an Application Load Balancer (ALB) in each of the two Regions as an endpoint Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type Create an ECS service on the cluster. Set the ECS service as the target for the ALB Process the data in Amazon ECS
D. Configure an Amazon Route 53 failover routing policy Create an Application Load Balancer (ALB) in each of the two Regions Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type Create an ECS service on the cluster Set the ECS service as the target for the ALB Process the data in Amazon ECS

Correct Answer: B
Section:
Explanation:
To meet the requirements of minimizing latency for data transmission from the devices and providing rapid failover to another AWS Region, the best solution would be to use AWS Global Accelerator in combination with a Network Load Balancer (NLB) and Amazon Elastic Container Service (Amazon ECS). AWS Global Accelerator is a service that improves the availability and performance of applications by using static IP addresses (Anycast) to route traffic to optimal AWS endpoints. With Global Accelerator,

QUESTION 14
A company is designing an application. The application uses an AWS Lambda function to receive information through Amazon API Gateway and to store the information in an Amazon Aurora PostgreSQL database. During the proof-of-concept stage, the company has to increase the Lambda quotas significantly to handle the high volumes of data that the company needs to load into the database. A solutions architect must recommend a new design to improve scalability and minimize the configuration effort.
Which solution will meet these requirements?

A. Refactor the Lambda function code to Apache Tomcat code that runs on Amazon EC2 instances.
Connect the database by using native Java Database Connectivity (JDBC) drivers.
B. Change the platform from Aurora to Amazon DynamoDB. Provision a DynamoDB Accelerator (DAX) cluster. Use the DAX client SDK to point the existing DynamoDB API calls at the DAX cluster.
C. Set up two Lambda functions. Configure one function to receive the information. Configure the other function to load the information into the database. Integrate the Lambda functions by using Amazon Simple Notification Service (Amazon SNS).
D. Set up two Lambda functions. Configure one function to receive the information. Configure the other function to load the information into the database. Integrate the Lambda functions by using an Amazon Simple Queue Service (Amazon SQS) queue.

Correct Answer: D
Section:
Explanation:

QUESTION 15
A company needs to review its AWS Cloud deployment to ensure that its Amazon S3 buckets do not have unauthorized configuration changes. What should a solutions architect do to accomplish this goal?

A. Turn on AWS Config with the appropriate rules.
B. Turn on AWS Trusted Advisor with the appropriate checks.
C. Turn on Amazon Inspector with the appropriate assessment template.
D. Turn on Amazon S3 server access logging. Configure Amazon EventBridge (Amazon Cloud Watch Events).

Correct Answer: A
Section:

Explanation:

QUESTION 16
A company is launching a new application and will display application metrics on an Amazon CloudWatch dashboard. The company's product manager needs to access this dashboard periodically. The product manager does not have an AWS account. A solution architect must provide access to the product manager by following the principle of least privilege. Which solution will meet these requirements?

A. Share the dashboard from the CloudWatch console. Enter the product manager's email address, and complete the sharing steps. Provide a shareable link for the dashboard to the product manager.
B. Create an IAM user specifically for the product manager. Attach the CloudWatch Read Only Access managed policy to the user. Share the new login credential with the product manager. Share the browser URL of the correct dashboard with the product manager.
C. Create an IAM user for the company's employees, Attach the View Only Access AWS managed policy to the IAM user. Share the new login credentials with the product manager. Ask the product manager to navigate to the CloudWatch console and locate the dashboard by name in the Dashboards section.
D. Deploy a bastion server in a public subnet. When the product manager requires access to the dashboard, start the server and share the RDP credentials. On the bastion server, ensure that the browser is configured to open the dashboard URL with cached AWS credentials that have appropriate permissions to view the dashboard.

Correct Answer: A
Section:
Explanation:

QUESTION 17
A company is migrating applications to AWS. The applications are deployed in different accounts. The company manages the accounts centrally by using AWS Organizations. The company's security team needs a single sign-on (SSO) solution across all the company's accounts. The company must continue managing the users and groups in its on-premises self-managed Microsoft Active Directory. Which solution will meet these requirements?

A. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console. Create a one-way forest trust or a one-way domain trust to connect the company's self-managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory.
B. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console. Create a two-way forest trust to connect the company's self-managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory.
C. Use AWS Directory Service. Create a two-way trust relationship with the company's self-managed Microsoft Active Directory.
D. Deploy an identity provider (IdP) on premises. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console.

Correct Answer: A
Section:
Explanation:
To provide single sign-on (SSO) across all the company's accounts while continuing to manage users and groups in its on-premises self-managed Microsoft Active Directory, the solution is to enable AWS Single Sign-On (SSO) from the AWS SSO console and create a one-way forest trust or a one-way domain trust to connect the company's self-managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory. This solution is described in the AWS documentation

QUESTION 18
A company provides a Voice over Internet Protocol (VoIP) service that uses UDP connections. The service consists of Amazon EC2 instances that run in an Auto Scaling group. The company has deployments across multiple AWS Regions. The company needs to route users to the Region with the lowest latency. The company also needs automated failover between Regions. Which solution will meet these requirements?

A. Deploy a Network Load Balancer (NLB) and an associated target group. Associate the target group with the Auto Scaling group. Use the NLB as an AWS Global Accelerator endpoint in each Region.
B. Deploy an Application Load Balancer (ALB) and an associated target group. Associate the target group with the Auto Scaling group. Use the ALB as an AWS Global Accelerator endpoint in each Region.
C. Deploy a Network Load Balancer (NLB) and an associated target group. Associate the target group with the Auto Scaling group. Create an Amazon Route 53 latency record that points to aliases for each NLB. Create an Amazon CloudFront distribution that uses the latency record as an origin.
D. Deploy an Application Load Balancer (ALB) and an associated target group. Associate the target group with the Auto Scaling group. Create an Amazon Route 53 weighted record that points to aliases for each ALB. Deploy an Amazon CloudFront distribution that uses the weighted record as an origin.

Correct Answer: A
Section:
Explanation:
https://aws.amazon.com/global-accelerator/faqs/

QUESTION 19
A development team runs monthly resource-intensive tests on its general purpose Amazon RDS for MySQL DB instance with Performance Insights enabled. The testing lasts for 48 hours once a month and is the only process that uses the database. The team wants to reduce the cost of running the tests without reducing the compute and memory attributes of the DB instance. Which solution meets these requirements MOST cost-effectively?

A. Stop the DB instance when tests are completed. Restart the DB instance when required.
B. Use an Auto Scaling policy with the DB instance to automatically scale when tests are completed.
C. Create a snapshot when tests are completed. Terminate the DB instance and restore the snapshot when required.
D. Modify the DB instance to a low-capacity instance when tests are completed. Modify the DB instance again when required.

Correct Answer: C
Section:
Explanation:
To reduce the cost of running the tests without reducing the compute and memory attributes of the Amazon RDS for MySQL DB instance, the development team can stop the instance when tests are completed and restart it when required. Stopping the DB instance when not in use can help save costs because customers are only charged for storage while the DB instance is stopped. During this time, automated backups and automated DB instance maintenance are suspended. When the instance is restarted, it retains the same configurations, security groups, and DB parameter groups as when it was stopped.Reference: Amazon RDS Documentation: Stopping and Starting a DB instance(https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_StopInstance.html)

QUESTION 20

A company that hosts its web application on AWS wants to ensure all Amazon EC2 instances. Amazon RDS DB instances. and Amazon Redshift clusters are configured with tags. The company wants to minimize the effort of configuring and operating this check.

What should a solutions architect do to accomplish this?

A. Use AWS Config rules to define and detect resources that are not properly tagged.
B. Use Cost Explorer to display resources that are not properly tagged. Tag those resources manually.
C. Write API calls to check all resources for proper tag allocation. Periodically run the code on an EC2 instance.
D. Write API calls to check all resources for proper tag allocation. Schedule an AWS Lambda function through Amazon CloudWatch to periodically run the code.

Correct Answer: A
Section:
Explanation:
To ensure all Amazon EC2 instances, Amazon RDS DB instances, and Amazon Redshift clusters are configured with tags, a solutions architect should use AWS Config rules to define and detect resources that are not properly tagged. AWS Config rules are a set of customizable rules that AWS Config uses to evaluate AWS resource configurations for compliance with best practices and company policies. Using AWS Config rules can minimize the effort of configuring and operating this check because it automates the process of identifying non-compliant resources and notifying the responsible teams.Reference: AWS Config Developer Guide: AWS Config Rules(https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_use-managed- rules.html)

QUESTION 21
A development team needs to host a website that will be accessed by other teams. The website contents consist of HTML, CSS, client-side JavaScript, and images Which method is the MOST costeffective for hosting the website?

A. Containerize the website and host it in AWS Fargate.
B. Create an Amazon S3 bucket and host the website there
C. Deploy a web server on an Amazon EC2 instance to host the website.
D. Configure an Application Loa d Balancer with an AWS Lambda target that uses the Express js framework.

Correct Answer: B
Section:
Explanation:
In Static Websites, Web pages are returned by the server which are prebuilt.
They use simple languages such as HTML, CSS, or JavaScript.
There is no processing of content on the server (according to the user) in Static Websites. Web pages are returned by the server with no change therefore, static Websites are fast. There is no interaction with databases.
Also, they are less costly as the host does not need to support server-side processing with different languages. ==========
In Dynamic Websites, Web pages are returned by the server which are processed during runtime means they are not prebuilt web pages but they are built during runtime according to the user's demand. These use server-side scripting languages such as PHP, Node.js, ASP.NET and many more supported by the server. So, they are slower than static websites but updates and interaction with databases are possible.

QUESTION 22
A company runs an online marketplace web application on AWS. The application serves hundreds of thousands of users during peak hours. The company needs a scalable, near-real-time solution to share the details of millions of financial transactions with several other internal applications Transactions also need to be processed to remove sensitive data before being stored in a document database for low-latency retrieval. What should a solutions architect recommend to meet these requirements?

A. Store the transactions data into Amazon DynamoDB Set up a rule in DynamoDB to remove sensitive data from every transaction upon write Use DynamoDB Streams to share the transactions data with other applications
B. Stream the transactions data into Amazon Kinesis Data Firehose to store data in Amazon DynamoDB and Amazon S3 Use AWS Lambda integration with Kinesis Data Firehose to remove sensitive data. Other applications can consume the data stored in Amazon S3
C. Stream the transactions data into Amazon Kinesis Data Streams Use AWS Lambda integration to remove sensitive data from every transaction and then store the transactions data in Amazon DynamoDB Other applications can consume the transactions data off the Kinesis data stream.
D. Store the batched transactions data in Amazon S3 as files. Use AWS Lambda to process every file and remove sensitive data before updating the files in Amazon S3 The Lambda function then stores the data in Amazon DynamoDB Other applications can consume transaction files stored in Amazon S3.

Correct Answer: C

Section:
Explanation:
The destination of your Kinesis Data Firehose delivery stream. Kinesis Data Firehose can send data records to various destinations, including Amazon Simple Storage Service (Amazon S3), Amazon Redshift, Amazon OpenSearch Service, and any HTTP endpoint that is owned by you or any of your third-party service providers. The following are the supported destinations:
* Amazon OpenSearch Service
* Amazon S3
* Datadog
* Dynatrace
* Honeycomb
* HTTP Endpoint
* Logic Monitor
* MongoDB Cloud
* New Relic
* Splunk
* Sumo Logic
https://docs.aws.amazon.com/firehose/latest/dev/create-name.html
https://aws.amazon.com/kinesis/data-streams/
Amazon Kinesis Data Streams (KDS) is a massively scalable and durable real-time data streaming service. KDS can continuously capture gigabytes of data per second from hundreds of thousands of sources such as website clickstreams, database event streams, financial transactions, social media feeds, IT logs, and location-tracking events.

QUESTION 23
A company hosts its multi-tier applications on AWS. For compliance, governance, auditing, and security, the company must track configuration changes on its AWS resources and record a history of API calls made to these resources. What should a solutions architect do to meet these requirements?

A. Use AWS CloudTrail to track configuration changes and AWS Config to record API calls
B. Use AWS Config to track configuration changes and AWS CloudTrail to record API calls
C. Use AWS Config to track configuration changes and Amazon CloudWatch to record API calls
D. Use AWS CloudTrail to track configuration changes and Amazon CloudWatch to record API calls

Correct Answer: B
Section:
Explanation:
AWS Config is a fully managed service that allows the company to assess, audit, and evaluate the configurations of its AWS resources. It provides a detailed inventory of the resources in use and tracks changes to resource configurations. AWS Config can detect configuration changes and alert the company when changes occur. It also provides a historical view of changes, which is essential for compliance and governance purposes. AWS CloudTrail is a fully managed service that provides a detailed history of API calls made to the company's AWS resources. It records all API activity in the AWS account, including who made the API call, when the call was made, and what resources were affected by the call. This information is critical for security and auditing purposes, as it allows the company to investigate any suspicious activity that might occur on its AWS resources.

QUESTION 24
A company is preparing to launch a public-facing web application in the AWS Cloud. The architecture consists of Amazon EC2 instances within a VPC behind an Elastic Load Balancer (ELB). A third-party service is used for the DNS. The company's solutions architect must recommend a solution to detect and protect against large-scale DDoS attacks. Which solution meets these requirements?

A. Enable Amazon GuardDuty on the account.
B. Enable Amazon Inspector on the EC2 instances.
C. Enable AWS Shield and assign Amazon Route 53 to it.
D. Enable AWS Shield Advanced and assign the ELB to it.

Correct Answer: D
Section:
Explanation:

https://aws.amazon.com/shield/faqs/

QUESTION 25
A company is building an application in the AWS Cloud. The application will store data in Amazon S3 buckets in two AWS Regions. The company must use an AWS Key Management Service (AWS KMS) customer managed key to encrypt all data that is stored in the S3 buckets. The data in both S3 buckets must be encrypted and decrypted with the same KMS key. The data and the key must be stored in each of the two Regions. Which solution will meet these requirements with the LEAST operational overhead?

A. Create an S3 bucket in each Region Configure the S3 buckets to use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) Configure replication between the S3 buckets.
B. Create a customer managed multi-Region KMS key. Create an S3 bucket in each Region. Configure replication between the S3 buckets. Configure the application to use the KMS key with client-side encryption.
C. Create a customer managed KMS key and an S3 bucket in each Region Configure the S3 buckets to use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) Configure replication between the S3 buckets.
D. Create a customer managed KMS key and an S3 bucket m each Region Configure the S3 buckets to use server-side encryption with AWS KMS keys (SSE-KMS) Configure replication between the S3 buckets.

Correct Answer: B
Section:
Explanation:
From https://docs.aws.amazon.com/kms/latest/developerguide/custom-key-store-overview.htmlFor most users, the default AWS KMS key store, which is protected by FIPS 140-2 validatedcryptographic modules, fulfills their security requirements. There is no need to add an extra layer ofmaintenance responsibility or a dependency on an additional service. However, you might considercreating a custom key store if your organization has any of the following requirements: Key materialcannot be stored in a shared environment. Key material must be subject to a secondary, independentaudit path. The HSMs that generate and store key material must be certified at FIPS 140-2 Level 3. https://docs.aws.amazon.com/kms/latest/developerguide/custom-key-store-overview.html

QUESTION 26
A company recently launched a variety of new workloads on Amazon EC2 instances in its AWS account. The company needs to create a strategy to access and administer the instances remotely and securely. The company needs to implement a repeatable process that works with native AWS services and follows the AWS Well-Architected Framework. Which solution will meet these requirements with the LEAST operational overhead?

A. Use the EC2 serial console to directly access the terminal interface of each instance for administration.
B. Attach the appropriate IAM role to each existing instance and new instance. Use AWS Systems Manager Session Manager to establish a remote SSH session.
C. Create an administrative SSH key pair. Load the public key into each EC2 instance. Deploy a bastion host in a public subnet to provide a tunnel for administration of each instance.
D. Establish an AWS Site-to-Site VPN connection. Instruct administrators to use their local onpremises machines to connect directly to the instances by using SSH keys across the VPN tunnel.

Correct Answer: B
Section:
Explanation:
https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-launch-managedinstance. html

QUESTION 27
A company is hosting a static website on Amazon S3 and is using Amazon Route 53 for DNS. The website is experiencing increased demand from around the world. The company must decrease latency for users who access the website. Which solution meets these requirements MOST cost-effectively?

A. Replicate the S3 bucket that contains the website to all AWS Regions. Add Route 53 geolocation routing entries.
B. Provision accelerators in AWS Global Accelerator. Associate the supplied IP addresses with the S3 bucket. Edit the Route 53 entries to point to the IP addresses of the accelerators.
C. Add an Amazon CloudFront distribution in front of the S3 bucket. Edit the Route 53 entries to point to the CloudFront distribution.
D. Enable S3 Transfer Acceleration on the bucket. Edit the Route 53 entries to point to the new endpoint.

Correct Answer: C
Section:
Explanation:
Amazon CloudFront is a content delivery network (CDN) that caches content at edge locations around the world, providing low latency and high transfer speeds to users accessing the content.Adding a CloudFront distribution

in front of the S3 bucket will cache the static website's content at edge locations around the world, decreasing latency for users accessing the website. This solution is

QUESTION 28
A company maintains a searchable repository of items on its website. The data is stored in an Amazon RDS for MySQL database table that contains more than 10 million rows The database has 2 TB of General Purpose SSD storage There are millions of updates against this data every day through the company's website The company has noticed that some insert operations are taking 10 seconds or longer The company has determined that the database storage performance is the problem Which solution addresses this performance issue?

A. Change the storage type to Provisioned IOPS SSD
B. Change the DB instance to a memory optimized instance class
C. Change the DB instance to a burstable performance instance class
D. Enable Multi-AZ RDS read replicas with MySQL native asynchronous replication.

Correct Answer: A
Section:
Explanation:
https://aws.amazon.com/ebs/features/
"Provisioned IOPS volumes are backed by solid-state drives (SSDs) and are the highest performance EBS volumes designed for your critical, I/O intensive database applications. These volumes are ideal for both IOPS-intensive and throughput-intensive workloads that require extremely low latency."

QUESTION 29
A company has thousands of edge devices that collectively generate 1 TB of status alerts each day.
Each alert is approximately 2 KB in size. A solutions architect needs to implement a solution to ingest and store the alerts for future analysis. The company wants a highly available solution. However, the company needs to minimize costs and does not want to manage additional infrastructure. Additionally, the company wants to keep 14 days of data available for immediate analysis and archive any data older than 14 days.
What is the MOST operationally efficient solution that meets these requirements?

A. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon S3 bucket Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days
B. Launch Amazon EC2 instances across two Availability Zones and place them behind an Elastic Load Balancer to ingest the alerts Create a script on the EC2 instances that will store tne alerts m an Amazon S3 bucket Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days
C. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon Elasticsearch Service (Amazon ES) duster Set up the Amazon ES cluster to take manual snapshots every day and delete data from the duster that is older than 14 days
D. Create an Amazon Simple Queue Service (Amazon SQS i standard queue to ingest the alerts and set the message retention period to 14 days Configure consumers to poll the SQS queue check the age of the message and analyze the message data as needed If the message is 14 days old the consumer should copy the message to an Amazon S3 bucket and delete the message from the SQS queue

Correct Answer: A
Section:
Explanation:
https://aws.amazon.com/kinesis/datafirehose/ features/?nc=sn&loc=2#:~:text=into%20Amazon%20S3%2C%20Amazon%20Redshift%2C%20Amazon%20OpenSearch%20Service%2C%20Kinesis,Delivery%20streams

QUESTION 30
A company's application integrates with multiple software-as-a-service (SaaS) sources for data collection. The company runs Amazon EC2 instances to receive the data and to upload the data to an Amazon S3 bucket for analysis. The same EC2 instance that receives and uploads the data also sends a notification to the user when an upload is complete. The company has noticed slow application performance and wants to improve the performance as much as possible. Which solution will meet these requirements with the LEAST operational overhead?

A. Create an Auto Scaling group so that EC2 instances can scale out. Configure an S3 event notification to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.
B. Create an Amazon AppFlow flow to transfer data between each SaaS source and the S3 bucket.
Configure an S3 event notification to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.

C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for each SaaS source to send output data. Configure the S3 bucket as the rule's target. Create a second EventBridge (CloudWatch Events) rule to send events when the upload to the S3 bucket is complete. Configure an Amazon Simple Notification Service (Amazon SNS) topic as the second rule's target.

D. Create a Docker container to use instead of an EC2 instance. Host the containerized application on Amazon Elastic Container Service (Amazon ECS). Configure Amazon CloudWatch Container Insights to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.

Correct Answer: B
Section:
Explanation:
Amazon AppFlow is a fully managed integration service that enables you to securely transfer data between Software-as-a-Service (SaaS) applications like Salesforce, SAP, Zendesk, Slack, and ServiceNow, and AWS services like Amazon S3 and Amazon Redshift, in just a few clicks.https://aws.amazon.com/appflow/

QUESTION 31
A company runs a highly available image-processing application on Amazon EC2 instances in a single VPC The EC2 instances run inside several subnets across multiple Availability Zones. The EC2 instances do not communicate with each other However, the EC2 instances download images from Amazon S3 and upload images to Amazon S3 through a single NAT gateway The company is concerned about data transfer charges What is the MOST cost-effective way for the company to avoid Regional data transfer charges?

A. Launch the NAT gateway in each Availability Zone
B. Replace the NAT gateway with a NAT instance
C. Deploy a gateway VPC endpoint for Amazon S3
D. Provision an EC2 Dedicated Host to run the EC2 instances

Correct Answer: C
Section:
Explanation:

QUESTION 32
A company has an on-premises application that generates a large amount of time-sensitive data that is backed up to Amazon S3. The application has grown and there are user complaints about internet bandwidth limitations. A solutions architect needs to design a long-term solution that allows for both timely backups to Amazon S3 and with minimal impact on internet connectivity for internal users. Which solution meets these requirements?

A. Establish AWS VPN connections and proxy all traffic through a VPC gateway endpoint
B. Establish a new AWS Direct Connect connection and direct backup traffic through this new connection.
C. Order daily AWS Snowball devices Load the data onto the Snowball devices and return the devices to AWS each day.
D. Submit a support ticket through the AWS Management Console Request the removal of S3 service limits from the account.

Correct Answer: B
Section:
Explanation:
To address the issue of bandwidth limitations on the company's on-premises application, and to minimize the impact on internal user connectivity, a new AWS Direct Connect connection should be established to direct backup traffic through this new connection. This solution will offer a secure, high-speed connection between the company's data center and AWS, which will allow the company to transfer data quickly without consuming internet bandwidth.
Reference:AWS Direct Connect documentation: https://aws.amazon.com/directconnect/

QUESTION 33
A company has an Amazon S3 bucket that contains critical dat a. The company must protect the data from accidental deletion. Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

A. Enable versioning on the S3 bucket.

B. Enable MFA Delete on the S3 bucket.
C. Create a bucket policy on the S3 bucket.
D. Enable default encryption on the S3 bucket.
E. Create a lifecycle policy for the objects in the S3 bucket.

Correct Answer: A, B
Section:
Explanation:
To protect data in an S3 bucket from accidental deletion, versioning should be enabled, which enables you to preserve, retrieve, and restore every version of every object in an S3 bucket.Additionally, enabling MFA (multi-factor authentication) Delete on the S3 bucket adds an extra layer of protection by requiring an authentication token in addition to the user's access keys to delete objects in the bucket.Reference: AWS S3 Versioning documentation:https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html
AWS S3 MFA Delete documentation:https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMFADelete.html

QUESTION 34
A company has a data ingestion workflow that consists the following:
An Amazon Simple Notification Service (Amazon SNS) topic for notifications about new data deliveries An AWS Lambda function to process the data and record metadata The company observes that the ingestion workflow fails occasionally because of network connectivity issues. When such a failure occurs, the Lambda function does not ingest the corresponding data unless the company manually reruns the job. Which combination of actions should a solutions architect take to ensure that the Lambda function ingests all data in the future? (Select TWO.)

A. Configure the Lambda function In multiple Availability Zones.
B. Create an Amazon Simple Queue Service (Amazon SQS) queue, and subscribe It to me SNS topic.
C. Increase the CPU and memory that are allocated to the Lambda function.
D. Increase provisioned throughput for the Lambda function.
E. Modify the Lambda function to read from an Amazon Simple Queue Service (Amazon SQS) queue

Correct Answer: B, E
Section:
Explanation:
To ensure that the Lambda function ingests all data in the future despite occasional network connectivity issues, the following actions should be taken: Create an Amazon Simple Queue Service (SQS) queue and subscribe it to the SNS topic. This allows

QUESTION 35
A company has an application that provides marketing services to stores. The services are based on previous purchases by store customers. The stores upload transaction data to the company through SFTP, and the data is processed and analyzed to generate new marketing offers. Some of the files can exceed 200 GB in size.
Recently, the company discovered that some of the stores have uploaded files that contain personally identifiable information (PII) that should not have been included. The company wants administrators to be alerted if PII is shared again. The company also wants to automate remediation.
What should a solutions architect do to meet these requirements with the LEAST development effort?

A. Use an Amazon S3 bucket as a secure transfer point. Use Amazon Inspector to scan me objects in the bucket. If objects contain Pll. trigger an S3 Lifecycle policy to remove the objects that contain Pll.
B. Use an Amazon S3 bucket as a secure transfer point. Use Amazon Macie to scan the objects in the bucket. If objects contain Pll. Use Amazon Simple Notification Service (Amazon SNS) to trigger a notification to the administrators to remove the objects mat contain Pll.
C. Implement custom scanning algorithms in an AWS Lambda function. Trigger the function when objects are loaded into the bucket. It objects contain Rll. use Amazon Simple Notification Service (Amazon SNS) to trigger a notification to the administrators to remove the objects that contain Pll.
D. Implement custom scanning algorithms in an AWS Lambda function. Trigger the function when objects are loaded into the bucket. If objects contain Pll. use Amazon Simple Email Service (Amazon STS) to trigger a notification to the administrators and trigger on S3 Lifecycle policy to remove the objects mot contain PII.

Correct Answer: A

Section:
Explanation:

QUESTION 36
A company needs guaranteed Amazon EC2 capacity in three specific Availability Zones in a specific AWS Region for an upcoming event that will last 1 week. What should the company do to guarantee the EC2 capacity?

A. Purchase Reserved instances that specify the Region needed
B. Create an On Demand Capacity Reservation that specifies the Region needed
C. Purchase Reserved instances that specify the Region and three Availability Zones needed
D. Create an On-Demand Capacity Reservation that specifies the Region and three Availability Zones needed

Correct Answer: D
Section:
Explanation:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-capacity-reservations.html
Reserve instances: You will have to pay for the whole term (1 year or 3years) which is not cost effective

QUESTION 37
A company's website uses an Amazon EC2 instance store for its catalog of items. The company wants to make sure that the catalog is highly available and that the catalog is stored in a durable location. What should a solutions architect do to meet these requirements?

A. Move the catalog to Amazon ElastiCache for Redis.
B. Deploy a larger EC2 instance with a larger instance store.
C. Move the catalog from the instance store to Amazon S3 Glacier Deep Archive.
D. Move the catalog to an Amazon Elastic File System (Amazon EFS) file system.

Correct Answer: D
Section:
Explanation:
Moving the catalog to an Amazon Elastic File System (Amazon EFS) file system provides both high availability and durability. Amazon EFS is a fully-managed, highly-available, and durable file system that is built to scale on demand. With Amazon EFS, the catalog data can be stored and accessed from multiple EC2 instances in different availability zones, ensuring high availability. Also, Amazon EFS automatically stores files redundantly within and across multiple availability zones, making it a durable storage option.

QUESTION 38
A company stores call transcript files on a monthly basis. Users access the files randomly within 1 year of the call, but users access the files infrequently after 1 year. The company wants to optimize its solution by giving users the ability to query and retrieve files that are less than 1-year-old as quickly as possible. A delay in retrieving older files is acceptable. Which solution will meet these requirements MOST cost-effectively?

A. Store individual files with tags in Amazon S3 Glacier Instant Retrieval. Query the tags to retrieve the files from S3 Glacier Instant Retrieval.
B. Store individual files in Amazon S3 Intelligent-Tiering. Use S3 Lifecycle policies to move the files to S3 Glacier Flexible Retrieval after 1 year. Query and retrieve the files that are in Amazon S3 by using Amazon Athena. Query and retrieve the files that are in S3 Glacier by using S3 Glacier Select.
C. Store individual files with tags in Amazon S3 Standard storage. Store search metadata for each archive in Amazon S3 Standard storage. Use S3 Lifecycle policies to move the files to S3 Glacier Instant Retrieval after 1 year. Query and retrieve the files by searching for metadata from Amazon S3.
D. Store individual files in Amazon S3 Standard storage. Use S3 Lifecycle policies to move the files to S3 Glacier Deep Archive after 1 year. Store search metadata in Amazon RDS. Query the files from Amazon RDS. Retrieve the files from S3 Glacier Deep Archive.

Correct Answer: B
Section:

Explanation:
"For archive data that needs immediate access, such as medical images, news media assets, or genomics data, choose the S3 Glacier Instant Retrieval storage class, an archive storage class that delivers the lowest cost storage with milliseconds retrieval. For archive data that does not require immediate access but needs the flexibility to retrieve large sets of data at no cost, such as backup or disaster recovery use cases, choose S3 Glacier Flexible Retrieval (formerly S3 Glacier), with retrieval in minutes or free bulk retrievals in 5-12 hours." https://aws.amazon.com/about-aws/whats-new/2021/11/amazon-s3-glacier-instant-retrieval-storage-class/

QUESTION 39
A company has a production workload that runs on 1,000 Amazon EC2 Linux instances. The workload is powered by third-party software. The company needs to patch the third-party software on all EC2 instances as quickly as possible to remediate a critical security vulnerability.
What should a solutions architect do to meet these requirements?

A. Create an AWS Lambda function to apply the patch to all EC2 instances.
B. Configure AWS Systems Manager Patch Manager to apply the patch to all EC2 instances.
C. Schedule an AWS Systems Manager maintenance window to apply the patch to all EC2 instances.
D. Use AWS Systems Manager Run Command to run a custom command that applies the patch to all EC2 instances.

Correct Answer: D
Section:
Explanation:

QUESTION 40
A company is developing an application that provides order shipping statistics for retrieval by a REST API. The company wants to extract the shipping statistics, organize the data into an easy-to-read HTML format, and send the report to several email addresses at the same time every morning.
Which combination of steps should a solutions architect take to meet these requirements? (Choose two.)

A. Configure the application to send the data to Amazon Kinesis Data Firehose.
B. Use Amazon Simple Email Service (Amazon SES) to format the data and to send the report by email.
C. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that invokes an AWS Glue job to query the application's API for the data.
D. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that invokes an AWS Lambda function to query the application's API for the data.
E. Store the application data in Amazon S3. Create an Amazon Simple Notification Service (Amazon SNS) topic as an S3 event destination to send the report by

Correct Answer: B, D
Section:
Explanation:
https://docs.aws.amazon.com/ses/latest/dg/send-email-formatted.html D. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that invokes an AWS Lambda function to query the application's API for the data. This step can be done using AWS Lambda to extract the shipping statistics and organize the data into an HTML format.B. Use Amazon Simple Email Service (Amazon SES) to format the data and send the report by email.This step can be done by using Amazon SES to send the report to multiple email addresses at the same time every morning.
Therefore, options D and B are the correct choices for this question. Option A is incorrect because Kinesis Data Firehose is not necessary for this use case. Option C is incorrect because AWS Glue is not required to query the application's API. Option E is incorrect because S3 event notifications cannot be used to send the report by email.

QUESTION 41
A company wants to migrate its on-premises application to AWS. The application produces output files that vary in size from tens of gigabytes to hundreds of terabytes The application data must be stored in a standard file system structure The company wants a solution that scales automatically, is highly available, and requires minimum operational overhead. Which solution will meet these requirements?

A. Migrate the application to run as containers on Amazon Elastic Container Service (Amazon ECS) Use Amazon S3 for storage
B. Migrate the application to run as containers on Amazon Elastic Kubernetes Service (Amazon EKS) Use Amazon Elastic Block Store (Amazon EBS) for storage
C. Migrate the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group. Use Amazon Elastic File System (Amazon EFS) for storage.
D. Migrate the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group. Use Amazon Elastic Block Store (Amazon EBS) for storage.

Correct Answer: C
Section:
Explanation:
EFS is a standard file system, it scales automatically and is highly available.

QUESTION 42
A company needs to store its accounting records in Amazon S3. The records must be immediately accessible for 1 year and then must be archived for an additional 9 years. No one at the company, including administrative users and root users, can be able to delete the records during the entire 10- year period. The records must be stored with maximum resiliency. Which solution will meet these requirements?

A. Store the records in S3 Glacier for the entire 10-year period. Use an access control policy to deny deletion of the records for a period of 10 years.
B. Store the records by using S3 Intelligent-Tiering. Use an IAM policy to deny deletion of the records. After 10 years, change the IAM policy to allow deletion.
C. Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 Glacier Deep Archive after 1 year. Use S3 Object Lock in compliance mode for a period of 10 years.
D. Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 1 year. Use S3 Object Lock in governance mode for a period of 10 years.

Correct Answer: C
Section:
Explanation:
To meet the requirements of immediately accessible records for 1 year and then archived for an additional 9 years with maximum resiliency, we can use S3 Lifecycle policy to transition records from S3 Standard to S3 Glacier Deep Archive after 1 year. And to ensure that the records cannot be deleted by anyone, including administrative and root users, we can use S3 Object Lock in compliance mode for a period of 10 years. Therefore, the correct answer is option C.Reference: https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.htmls

QUESTION 43
A company runs multiple Windows workloads on AWS. The company's employees use Windows file shares that are hosted on two Amazon EC2 instances. The file shares synchronize data between themselves and maintain duplicate copies. The company wants a highly available and durable storage solution that preserves how users currently access the files. What should a solutions architect do to meet these requirements?

A. Migrate all the data to Amazon S3 Set up IAM authentication for users to access files
B. Set up an Amazon S3 File Gateway. Mount the S3 File Gateway on the existing EC2 Instances.
C. Extend the file share environment to Amazon FSx for Windows File Server with a Multi-AZ configuration. Migrate all the data to FSx for Windows File Server.
D. Extend the file share environment to Amazon Elastic File System (Amazon EFS) with a Multi-AZ configuration. Migrate all the data to Amazon EFS.

Correct Answer: C
Section:
Explanation:
https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/AmazonEFS.html Amazon FSx for Windows File Server provides fully managed Microsoft Windows file servers, backed by a fully nativeWindows file system.
https://docs.aws.amazon.com/fsx/latest/WindowsGuide/what-is.html

QUESTION 44
A solutions architect is developing a multiple-subnet VPC architecture. The solution will consist of six subnets in two Availability Zones. The subnets are defined as public, private and dedicated for databases. Only the Amazon EC2 instances running in the private subnets should be able to access a database.
Which solution meets these requirements?

A. Create a now route table that excludes the route to the public subnets' CIDR blocks. Associate the route table to the database subnets.
B. Create a security group that denies ingress from the security group used by instances in the public subnets. Attach the security group to an Amazon RDS DB instance.
C. Create a security group that allows ingress from the security group used by instances in the private subnets. Attach the security group to an Amazon RDS DB instance.
D. Create a new peering connection between the public subnets and the private subnets. Create a different peering connection between the private subnets and the database subnets.

Correct Answer: C
Section:

Explanation:
Security groups are stateful. All inbound traffic is blocked by default. If you create an inbound rule allowing traffic in, that traffic is automatically allowed back out again. You cannot block specific IP address using Security groups (instead use Network Access Control Lists).
"You can specify allow rules, but not deny rules." "When you first create a security group, it has no inbound rules. Therefore, no inbound traffic originating from another host to your instance is allowed until you add inbound rules to the security group." Source:
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html#VPCSecurityGroups

QUESTION 45
A company has registered its domain name with Amazon Route 53. The company uses Amazon API Gateway in the ca-central-1 Region as a public interface for its backend microservice APIs. Thirdparty services consume the APIs securely. The company wants to design its API Gateway URL with the company's domain name and corresponding certificate so that the third-party services can use HTTPS. Which solution will meet these requirements?

A. Create stage variables in API Gateway with Name="Endpoint-URL" and Value="Company Domain Name" to overwrite the default URL. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM).
B. Create Route 53 DNS records with the company's domain name. Point the alias record to the Regional API Gateway stage endpoint. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the us-east-1 Region.
C. Create a Regional API Gateway endpoint. Associate the API Gateway endpoint with the company's domain name. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the same Region. Attach the certificate to the API Gateway endpoint.
Configure Route 53 to route traffic to the API Gateway endpoint.
D. Create a Regional API Gateway endpoint. Associate the API Gateway endpoint with the company's domain name. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the us- east-1 Region. Attach the certificate to the API Gateway APIs.
Create Route 53 DNS records with the company's domain name. Point an A record to the company's domain name.

Correct Answer: C
Section:
Explanation:
To design the API Gateway URL with the company's domain name and corresponding certificate, the company needs to do the following: 1. Create a Regional API Gateway endpoint: This will allow the company to create an endpoint that is specific to a region. 2. Associate the API Gateway endpoint with the company's domain name: This will allow the company to use its own domain name for the API Gateway URL. 3. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the same Region: This will allow the company to use HTTPS for secure communication with its APIs. 4. Attach the certificate to the API Gateway endpoint: This will allow the company to use the certificate for securing the API Gateway URL. 5. Configure Route 53 to route traffic to the API Gateway endpoint: This will allow the company to use Route 53 to route traffic to the API Gateway URL using the company's domain name.

QUESTION 46
A company is running a popular social media website. The website gives users the ability to upload images to share with other users. The company wants to make sure that the images do not contain inappropriate content. The company needs a solution that minimizes development effort.
What should a solutions architect do to meet these requirements?

A. Use Amazon Comprehend to detect inappropriate content. Use human review for low-confidence predictions.
B. Use Amazon Rekognition to detect inappropriate content. Use human review for low-confidence predictions.
C. Use Amazon SageMaker to detect inappropriate content. Use ground truth to label low-confidence predictions.
D. Use AWS Fargate to deploy a custom machine learning model to detect inappropriate content.
Use ground truth to label low-confidence predictions.

Correct Answer: B
Section:
Explanation:
https://docs.aws.amazon.com/rekognition/latest/dg/moderation.html?pg=ln&sec=fthttps://docs.aws.amazon.com/rekognition/latest/dg/a2i-rekognition.html

QUESTION 47
A company wants to run its critical applications in containers to meet requirements tor scalability and availability The company prefers to focus on maintenance of the critical applications The company does not want to be

responsible for provisioning and managing the underlying infrastructure that runs the containerized workload What should a solutions architect do to meet those requirements?

A. Use Amazon EC2 Instances, and Install Docker on the Instances
B. Use Amazon Elastic Container Service (Amazon ECS) on Amazon EC2 worker nodes
C. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate
D. Use Amazon EC2 instances from an Amazon Elastic Container Service (Amazon ECS)-op6mized Amazon Machine Image (AMI).

Correct Answer: C
Section:
Explanation:
Explanation: using AWS ECS on AWS Fargate since they requirements are for scalability and availability without having to provision and manage the underlying infrastructure to run the containerized workload.
https://docs.aws.amazon.com/AmazonECS/latest/userguide/what-is-fargate.html

QUESTION 48
A company hosts more than 300 global websites and applications. The company requires a platform to analyze more than 30 TB of clickstream data each day. What should a solutions architect do to transmit and process the clickstream data?

A. Design an AWS Data Pipeline to archive the data to an Amazon S3 bucket and run an Amazon EMR duster with the data to generate analytics
B. Create an Auto Scaling group of Amazon EC2 instances to process the data and send it to an Amazon S3 data lake for Amazon Redshift to use tor analysis
C. Cache the data to Amazon CloudFron: Store the data in an Amazon S3 bucket When an object is added to the S3 bucket, run an AWS Lambda function to process the data tor analysis.
D. Collect the data from Amazon Kinesis Data Streams. Use Amazon Kinesis Data Firehose to transmit the data to an Amazon S3 data lake Load the data in Amazon Redshift for analysis

Correct Answer: D
Section:
Explanation:
https://aws.amazon.com/es/blogs/big-data/real-time-analytics-with-amazon-redshift-streaming- ingestion/

QUESTION 49
A company has a website hosted on AWS The website is behind an Application Load Balancer (ALB) that is configured to handle HTTP and HTTPS separately. The company wants to forward all requests to the website so that the requests will use HTTPS.
What should a solutions architect do to meet this requirement?

A. Update the ALB's network ACL to accept only HTTPS traffic
B. Create a rule that replaces the HTTP in the URL with HTTPS.
C. Create a listener rule on the ALB to redirect HTTP traffic to HTTPS.
D. Replace the ALB with a Network Load Balancer configured to use Server Name Indication (SNI).

Correct Answer: C
Section:
Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/elb-redirect-http-to-https-using-alb/How can I redirect HTTP requests to HTTPS using an Application Load Balancer? Last updated: 2020-10-30 I want to redirect HTTP requests to HTTPS using Application Load Balancer listener rules. Howcan I do this? Resolution Reference: https://aws.amazon.com/premiumsupport/knowledgecenter/elb-redirect-http-to-https-using-alb/

QUESTION 50
A company is developing a two-tier web application on AWS. The company's developers have deployed the application on an Amazon EC2 instance that connects directly to a backend Amazon RDS database. The company must not hardcode database credentials in the application. The company must also implement a solution to automatically rotate the database credentials on a regular basis. Which solution will meet these requirements with the LEAST operational overhead?

A. Store the database credentials in the instance metadata. Use Amazon EventBridge (Amazon CloudWatch Events) rules to run a scheduled AWS Lambda function that updates the RDS credentials and instance metadata at the same time.
B. Store the database credentials in a configuration file in an encrypted Amazon S3 bucket. Use Amazon EventBridge (Amazon CloudWatch Events) rules to run a scheduled AWS Lambda function that updates the RDS credentials and the credentials in the configuration file at the same time. Use S3 Versioning to ensure the ability to fall back to previous values.
C. Store the database credentials as a secret in AWS Secrets Manager. Turn on automatic rotation for the secret. Attach the required permission to the EC2 role to grant access to the secret.
D. Store the database credentials as encrypted parameters in AWS Systems Manager Parameter Store. Turn on automatic rotation for the encrypted parameters. Attach the required permission to the EC2 role to grant access to the encrypted parameters.

Correct Answer: C
Section:
Explanation:
https://docs.aws.amazon.com/secretsmanager/latest/userguide/create_database_secret.html

QUESTION 51
A company is deploying a new public web application to AWS. The application will run behind an Application Load Balancer (ALB). The application needs to be encrypted at the edge with an SSL/TLS certificate that is issued by an external certificate authority (CA). The certificate must be rotated each year before the certificate expires. What should a solutions architect do to meet these requirements?

A. Use AWS Certificate Manager (ACM) to issue an SSL/TLS certificate. Apply the certificate to the ALB. Use the managed renewal feature to automatically rotate the certificate.
B. Use AWS Certificate Manager (ACM) to issue an SSL/TLS certificate. Import the key material from the certificate. Apply the certificate to the ALB. Use the managed renewal feature to automatically rotate the certificate.
C. Use AWS Certificate Manager (ACM) Private Certificate Authority to issue an SSL/TLS certificate from the root CA. Apply the certificate to the ALB. Use the managed renewal feature to automatically rotate the certificate.
D. Use AWS Certificate Manager (ACM) to import an SSL/TLS certificate. Apply the certificate to the ALB. Use Amazon EventBridge (Amazon CloudWatch Events) to send a notification when the certificate is nearing expiration. Rotate the certificate manually.

Correct Answer: D
Section:
Explanation:

QUESTION 52
A company runs its Infrastructure on AWS and has a registered base of 700.000 users for res document management application The company intends to create a product that converts large pdf files to jpg Imago files. The .pdf files average 5 MB in size. The company needs to store the original files and the converted files. A solutions architect must design a scalable solution to accommodate demand that will grow rapidly over lime. Which solution meets these requirements MOST cost-effectively?

A. Save the pdf files to Amazon S3 Configure an S3 PUT event to invoke an AWS Lambda function to convert the files to jpg format and store them back in Amazon S3
B. Save the pdf files to Amazon DynamoDB. Use the DynamoDB Streams feature to invoke an AWS Lambda function to convert the files to jpg format and store them hack in DynamoDB
C. Upload the pdf files to an AWS Elastic Beanstalk application that includes Amazon EC2 instances. Amazon Elastic Block Store (Amazon EBS) storage and an Auto Scaling group. Use a program In the EC2 instances to convert the files to jpg format Save the .pdf files and the .jpg files In the EBS store.
D. Upload the .pdf files to an AWS Elastic Beanstalk application that includes Amazon EC2 instances, Amazon Elastic File System (Amazon EPS) storage, and an Auto Scaling group. Use a program in the EC2 instances to convert the file to jpg format Save the pdf files and the jpg files in the EBS store.

Correct Answer: A
Section:
Explanation:
Elastic BeanStalk is expensive, and DocumentDB has a 400KB max to upload files. So Lambda and S3 should be the one.

QUESTION 53
A company has more than 5 TB of file data on Windows file servers that run on premises Users and applications interact with the data each day The company is moving its Windows workloads to AWS. As the company

continues this process, the company requires access to AWS and on-premises file storage with minimum latency The company needs a solution that minimizes operational overhead and requires no significant changes to the existing file access patterns. The company uses an AWS Site-to-Site VPN connection for connectivity to AWS What should a solutions architect do to meet these requirements?

A. Deploy and configure Amazon FSx for Windows File Server on AWS. Move the on-premises file data to FSx for Windows File Server. Reconfigure the workloads to use FSx for Windows File Server on AWS.
B. Deploy and configure an Amazon S3 File Gateway on premises Move the on-premises file data to the S3 File Gateway Reconfigure the on-premises workloads and the cloud workloads to use the S3 File Gateway
C. Deploy and configure an Amazon S3 File Gateway on premises Move the on-premises file data to Amazon S3 Reconfigure the workloads to use either Amazon S3 directly or the S3 File Gateway, depending on each workload's location
D. Deploy and configure Amazon FSx for Windows File Server on AWS Deploy and configure an Amazon FSx File Gateway on premises Move the on-premises file data to the FSx File Gateway Configure the cloud workloads to use FSx for Windows File Server on AWS Configure the on-premises workloads to use the FSx File Gateway

Correct Answer: D
Section:
Explanation:

QUESTION 54
A hospital recently deployed a RESTful API with Amazon API Gateway and AWS Lambda The hospital uses API Gateway and Lambda to upload reports that are in PDF format and JPEG format The hospital needs to modify the Lambda code to identify protected health information (PHI) in the reports Which solution will meet these requirements with the LEAST operational overhead?

A. Use existing Python libraries to extract the text from the reports and to identify the PHI from the extracted text.
B. Use Amazon Textract to extract the text from the reports Use Amazon SageMaker to identify the PHI from the extracted text.
C. Use Amazon Textract to extract the text from the reports Use Amazon Comprehend Medical to identify the PHI from the extracted text
D. Use Amazon Rekognition to extract the text from the reports Use Amazon Comprehend Medical to identify the PHI from the extracted text

Correct Answer: C
Section:
Explanation:
To meet the requirements of the company to have access to both AWS and on-premises file storage with minimum latency, a hybrid cloud architecture can be used. One solution is to deploy and configure Amazon FSx for Windows File Server on AWS, which provides fully managed Windows file servers. The on-premises file data can be moved to the FSx File Gateway, which can act as a bridge between on-premises and AWS file storage. The cloud workloads can be configured to use FSx for Windows File Server on AWS, while the on-premises workloads can be configured to use the FSx File Gateway. This solution minimizes operational overhead and requires no significant changes to the existing file access patterns. The connectivity between on-premises and AWS can be established using an AWS Site-to-Site VPN connection.Reference:AWS FSx for Windows File Server: https://aws.amazon.com/fsx/windows/ AWS FSx File Gateway: https://aws.amazon.com/fsx/file-gateway/ AWS Site-to-Site VPN: https://aws.amazon.com/vpn/site-to-site-vpn/

QUESTION 55
A company has an application that generates a large number of files, each approximately 5 MB in size. The files are stored in Amazon S3. Company policy requires the files to be stored for 4 years before they can be deleted Immediate accessibility is always required as the files contain critical business data that is not easy to reproduce. The files are frequently accessed in the first 30 days of the object creation but are rarely accessed after the first 30 days Which storage solution is MOST cost-effective?

A. Create an S3 bucket lifecycle policy to move Mm from S3 Standard to S3 Glacier 30 days from object creation. Delete the Tiles 4 years after object creation
B. Create an S3 bucket lifecycle policy to move tiles from S3 Standard to S3 One Zone-infrequent Access (S3 One Zone-IA] 30 days from object creation. Delete the fees 4 years after object creation
C. Create an S3 bucket lifecycle policy to move files from S3 Standard-infrequent Access (S3 Standard -lA) 30 from object creation. Delete the ties 4 years after object creation
D. Create an S3 bucket Lifecycle policy to move files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 30 days from object creation. Move the files to S3 Glacier 4 years after object carton.

Correct Answer: C
Section:

QUESTION 56
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 architect do to ensure messages are being processed once only?

A. Use the CreateQueue API call to create a new queue
B. Use the Add Permission API call to add appropriate permissions
C. Use the ReceiveMessage API call to set an appropriate wail time
D. Use the ChangeMessageVisibility APi call to increase the visibility timeout

Correct Answer: D
Section:
Explanation:
The visibility timeout begins when Amazon SQS returns a message. During this time, the consumer processes and deletes the message. However, if the consumer fails before deleting the message and your system doesn't call the DeleteMessage action for that message before the visibility timeout expires, the message becomes visible to other consumers and the message is received again. If a message must be received only once, your consumer should delete it within the duration of the visibility timeout.
https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibilitytimeout. html Keyword: SQS queue writes to an Amazon RDS From 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] FIF O 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).

QUESTION 57
A solutions architect is designing a new hybrid architecture to extend a company s on-premises infrastructure to AWS The company requires a highly available connection with consistent low latency to an AWS Region. The company needs to minimize costs and is willing to accept slower traffic if the primary connection fails.
What should the solutions architect do to meet these requirements?

A. Provision an AWS Direct Connect connection to a Region Provision a VPN connection as a backup if the primary Direct Connect connection fails.
B. Provision a VPN tunnel connection to a Region for private connectivity. Provision a second VPN tunnel for private connectivity and as a backup if the primary VPN connection fails.
C. Provision an AWS Direct Connect connection to a Region Provision a second Direct Connect connection to the same Region as a backup if the primary Direct Connect connection fails.
D. Provision an AWS Direct Connect connection to a Region Use the Direct Connect failover attribute from the AWS CLI to automatically create a backup connection if the primary Direct Connect connection fails.

Correct Answer: A
Section:
Explanation:
"In some cases, this connection alone is not enough. It is always better to guarantee a fallback connection as the backup of DX. There are several options, but implementing it with an AWS Site-To- Site VPN is a real cost-effective solution that can be exploited to reduce costs or, in the meantime, wait for the setup of a second DX." https://www.proud2becloud.com/hybrid-cloud-networking-backup-aws-direct-connect-networkconnection- with-aws-site-to-site-vpn/

QUESTION 58
A company is running a business-critical web application on Amazon EC2 instances behind an Application Load Balancer. The EC2 instances are in an Auto Scaling group. The application uses an Amazon Aurora PostgreSQL database that is deployed in a single Availability Zone. The company wants the application to be highly available with minimum downtime and minimum loss of data. Which solution will meet these requirements with the LEAST operational effort?

A. Place the EC2 instances in different AWS Regions. Use Amazon Route 53 health checks to redirect traffic. Use Aurora PostgreSQL Cross-Region Replication.
B. Configure the Auto Scaling group to use multiple Availability Zones. Configure the database as Multi-AZ. Configure an Amazon RDS Proxy instance for the database.
C. Configure the Auto Scaling group to use one Availability Zone. Generate hourly snapshots of the database. Recover the database from the snapshots in the event of a failure.
D. Configure the Auto Scaling group to use multiple AWS Regions. Write the data from the application to Amazon S3. Use S3 Event Notifications to launch an AWS Lambda function to write the data to the database.

Correct Answer: B
Section:
Explanation:

QUESTION 59
A company's HTTP application is behind a Network Load Balancer (NLB). The NLB's target group isconfigured to use an Amazon EC2 Auto Scaling group with multiple EC2 instances that run the webservice. The company notices that the NLB is not detecting HTTP errors for the application. These errorsrequire a manual restart of the EC2 instances that run the web service. The company needs toimprove the application's availability without writing custom scripts or code.
What should a solutions architect do to meet these requirements?

A. Enable HTTP health checks on the NLB. supplying the URL of the company's application.
B. Add a cron job to the EC2 instances to check the local application's logs once each minute. If HTTPerrors are detected, the application will restart.
C. Replace the NLB with an Application Load Balancer. Enable HTTP health checks by supplying theURL of the company's application. Configure an Auto Scaling action to replace unhealthy instances.
D. Create an Amazon Cloud Watch alarm that monitors the UnhealthyHostCount metric for the NLB.
Configure an Auto Scaling action to replace unhealthy instances when the alarm is in the ALARM state.

Correct Answer: C
Section:
Explanation:
Application availability: NLB cannot assure the availability of the application. This is because it bases its decisions solely on network and TCP-layer variables and has no awareness of the application at all.Generally, NLB determines availability based on the ability of a server to respond to ICMP ping or to correctly complete the three-way TCP handshake. ALB goes much deeper and is capable of determining availability based on not only a successful HTTP GET of a particular page but also the verification that the content is as was expected based on the input parameters.

QUESTION 60
A company runs a shopping application that uses Amazon DynamoDB to store customer information.
In case of data corruption, a solutions architect needs to design a solution that meets a recovery point objective (RPO) of 15 minutes and a recovery time objective (RTO) of 1 hour. What should the solutions architect recommend to meet these requirements?

A. Configure DynamoDB global tables. For RPO recovery, point the application to a different AWS Region.
B. Configure DynamoDB point-in-time recovery. For RPO recovery, restore to the desired point in time.
C. Export the DynamoDB data to Amazon S3 Glacier on a daily basis. For RPO recovery, import the data from S3 Glacier to DynamoDB.
D. Schedule Amazon Elastic Block Store (Amazon EBS) snapshots for the DynamoDB table every 15 minutes. For RPO recovery, restore the DynamoDB table by using the EBS snapshot.

Correct Answer: B
Section:
Explanation:
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/PointInTimeRecovery.html

QUESTION 61
A company runs a photo processing application that needs to frequently upload and download pictures from Amazon S3 buckets that are located in the same AWS Region. A solutions architect has noticed an increased cost in data transfer fees and needs to implement a solution to reduce these costs.
How can the solutions architect meet this requirement?

A. Deploy Amazon API Gateway into a public subnet and adjust the route table to route S3 calls through It.
B. Deploy a NAT gateway into a public subnet and attach an end point policy that allows access to the S3 buckets.
C. Deploy the application Into a public subnet and allow it to route through an internet gateway to access the S3 Buckets
D. Deploy an S3 VPC gateway endpoint into the VPC and attach an endpoint policy that allows access to the S3 buckets.

Correct Answer: D
Section:
Explanation:

QUESTION 62
A company recently launched Linux-based application instances on Amazon EC2 in a private subnet and launched a Linux-based bastion host on an Amazon EC2 instance in a public subnet of a VPC A solutions architect needs to connect from the on-premises network, through the company's internet connection to the bastion host and to the application servers The solutions architect must make sure that the security groups of all the EC2 instances will allow that access Which combination of steps should the solutions architect take to meet these requirements? (Select TWO)

A. Replace the current security group of the bastion host with one that only allows inbound access from the application instances
B. Replace the current security group of the bastion host with one that only allows inbound access from the internal IP range for the company
C. Replace the current security group of the bastion host with one that only allows inbound access from the external IP range for the company
D. Replace the current security group of the application instances with one that allows inbound SSH access from only the private IP address of the bastion host
E. Replace the current security group of the application instances with one that allows inbound SSH access from only the public IP address of the bastion host

Correct Answer: C, D
Section:
Explanation:
https://digitalcloud.training/ssh-into-ec2-in-private-subnet/

QUESTION 63
A solutions architect is designing a two-tier web application The application consists of a publicfacing web tier hosted on Amazon EC2 in public subnets The database tier consists of Microsoft SQL Server running on Amazon EC2 in a private subnet Security is a high priority for the company How should security groups be configured in this situation? (Select TWO)

A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0.
B. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0.
C. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier.
D. Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier.
E. Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier.

Correct Answer: A, B
Section:
Explanation:

QUESTION 64
A company wants to move a multi-tiered application from on premises to the AWS Cloud to improve the application's performance. The application consists of application tiers that communicate with each other by way of RESTful services. Transactions are dropped when one tier becomes overloaded.
A solutions architect must design a solution that resolves these issues and modernizes the application. Which solution meets these requirements and is the MOST operationally efficient?

A. Use Amazon API Gateway and direct transactions to the AWS Lambda functions as the application layer. Use Amazon Simple Queue Service (Amazon SQS) as the communication layer between application services. Most Voted
B. Use Amazon CloudWatch metrics to analyze the application performance history to determine the server's peak utilization during the performance failures. Increase the size of the application server's Amazon EC2 instances to meet the peak requirements.
C. Use Amazon Simple Notification Service (Amazon SNS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SNS queue length and scale up and down as required.
D. Use Amazon Simple Queue Service (Amazon SQS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SQS queue length and scale up when communication failures are detected.

Correct Answer: A
Section:
Explanation:
https://aws.amazon.com/getting-started/hands-on/build-serverless-web-app-lambda-apigateways3- dynamodb-cognito/module-4/ Build a Serverless Web Application with AWS Lambda, Amazon API Gateway, AWS Amplify, Amazon DynamoDB, and Amazon Cognito. This example showed similar setup as question: Build a Serverless Web Application with AWS Lambda, Amazon API Gateway, AWS Amplify, Amazon DynamoDB, and Amazon Cognito

QUESTION 65
A company receives 10 TB of instrumentation data each day from several machines located at a single factory. The data consists of JSON files stored on a storage area network (SAN) in an onpremises data center located within the factory. The company wants to send this data to Amazon S3 where it can be accessed by several additional systems that provide critical near-real-lime analytics. A secure transfer is important because the data is considered sensitive.
Which solution offers the MOST reliable data transfer?

A. AWS DataSync over public internet
B. AWS DataSync over AWS Direct Connect
C. AWS Database Migration Service (AWS DMS) over public internet
D. AWS Database Migration Service (AWS DMS) over AWS Direct Connect

Correct Answer: B
Section:
Explanation:
These are some of the main use cases for AWS DataSync: • Data migration – Move active datasets rapidly over the network into Amazon S3, Amazon EFS, or FSx for Windows File Server. DataSync includes automatic encryption and data integrity validation to help make sure that your data arrives securely, intact, and ready to use. "DataSync includes encryption and integrity validation to help make sure your data arrives securely, intact, and ready to use." https://aws.amazon.com/datasync/faqs/

QUESTION 66
A company needs to configure a real-time data ingestion architecture for its application. The company needs an API, a process that transforms data as the data is streamed, and a storage solution for the data. Which solution will meet these requirements with the LEAST operational overhead?

A. Deploy an Amazon EC2 instance to host an API that sends data to an Amazon Kinesis data stream.
Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source. Use AWS Lambda functions to transform the data. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.
B. Deploy an Amazon EC2 instance to host an API that sends data to AWS Glue. Stop source/destination checking on the EC2 instance. Use AWS Glue to transform the data and to send the data to Amazon S3.
C. Configure an Amazon API Gateway API to send data to an Amazon Kinesis data stream. Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source. Use AWS Lambda functions to transform the data. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.
D. Configure an Amazon API Gateway API to send data to AWS Glue. Use AWS Lambda functions to transform the data. Use AWS Glue to send the data to Amazon S3.

Correct Answer: C
Section:

QUESTION 67
A company needs to keep user transaction data in an Amazon DynamoDB table.
The company must retain the data for 7 years.
What is the MOST operationally efficient solution that meets these requirements?

A. Use DynamoDB point-in-time recovery to back up the table continuously.
B. Use AWS Backup to create backup schedules and retention policies for the table.
C. Create an on-demand backup of the table by using the DynamoDB console. Store the backup in an Amazon S3 bucket. Set an S3 Lifecycle configuration for the S3 bucket.
D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function. Configure the Lambda function to back up the table and to store the backup in an Amazon S3 bucket. Set an S3

Lifecycle configuration for the S3 bucket.

Correct Answer: B
Section:

QUESTION 68
A company is planning to use an Amazon DynamoDB table for data storage. The company is concerned about cost optimization. The table will not be used on most mornings. In the evenings, the read and write traffic will often be unpredictable. When traffic spikes occur, they will happen very quickly.
What should a solutions architect recommend?

A. Create a DynamoDB table in on-demand capacity mode.
B. Create a DynamoDB table with a global secondary index.
C. Create a DynamoDB table with provisioned capacity and auto scaling.
D. Create a DynamoDB table in provisioned capacity mode, and configure it as a global table.

Correct Answer: A
Section:

QUESTION 69
A solutions architect must design a highly available infrastructure for a website. The website is powered by Windows web servers that run on Amazon EC2 instances. The solutions architect must implement a solution that can mitigate a large-scale DDoS attack that originates from thousands of IP addresses. Downtime is not acceptable for the website. Which actions should the solutions architect take to protect the website from such an attack? (Select TWO.)

A. Use AWS Shield Advanced to stop the DDoS attack.
B. Configure Amazon GuardDuty to automatically block the attackers.
C. Configure the website to use Amazon CloudFront for both static and dynamic content.
D. Use an AWS Lambda function to automatically add attacker IP addresses to VPC network ACLs.
E. Use EC2 Spot Instances in an Auto Scaling group with a target tracking scaling policy that is set to 80% CPU utilization

Correct Answer: A, C
Section:
Explanation:
https://aws.amazon.com/cloudfron

QUESTION 70
A company is preparing to deploy a new serverless workload. A solutions architect must use the principle of least privilege to configure permissions that will be used to run an AWS Lambda function. An Amazon EventBridge (Amazon CloudWatch Events) rule will invoke the function.
Which solution meets these requirements?

A. Add an execution role to the function with lambda:InvokeFunction as the action and * as the principal.
B. Add an execution role to the function with lambda:InvokeFunction as the action and Service:amazonaws.com as the principal.
C. Add a resource-based policy to the function with lambda:'* as the action and Service:events.amazonaws.com as the principal.
D. Add a resource-based policy to the function with lambda:InvokeFunction as the action and Service:events.amazonaws.com as the principal.

Correct Answer: D
Section:
Explanation:
https://docs.aws.amazon.com/eventbridge/latest/userguide/resource-based-policieseventbridge. html#lambda-permissions

QUESTION 71
A company is preparing to store confidential data in Amazon S3 For compliance reasons the data must be encrypted at rest Encryption key usage must be logged tor auditing purposes. Keys must be rotated every year. Which solution meets these requirements and «the MOST operationally efferent?

A. Server-side encryption with customer-provided keys (SSE-C)
B. Server-side encryption with Amazon S3 managed keys (SSE-S3)
C. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with manual rotation
D. Server-side encryption with AWS KMS (SSE-KMS) customer master keys (CMKs) with automate rotation

Correct Answer: D
Section:
Explanation:
https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html When you enable automatic key rotation for a customer managed key, AWS KMS generates new cryptographic material for the KMS key every year. AWS KMS also saves the KMS key's older cryptographic material in perpetuity so it can be used to decrypt data that the KMS key encrypted. Key rotation in AWS KMS is a cryptographic best practice that is designed to be transparent and easy to use. AWS KMS supports optional automatic key rotation only for customer managed CMKs. Enable and disable key rotation. Automatic key rotation is disabled by default on customer managed CMKs.
When you enable (or re-enable) key rotation, AWS KMS automatically rotates the CMK 365 days after the enable date and every 365 days thereafter.

QUESTION 72
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

Correct Answer: B
Section:
Explanation:

QUESTION 73
A company has an automobile sales website that stores its listings in a database on Amazon RDS When an automobile is sold the listing needs to be removed from the website and the data must be sent to multiple target systems. Which design should a solutions architect recommend?

A. Create an AWS Lambda function triggered when the database on Amazon RDS is updated to send the information to an Amazon Simple Queue Service (Amazon SQS> queue for the targets to consume
B. Create an AWS Lambda function triggered when the database on Amazon RDS is updated to send the information to an Amazon Simple Queue Service (Amazon SQS) FIFO queue for the targets to consume
C. Subscribe to an RDS event notification and send an Amazon Simple Queue Service (Amazon SQS) queue fanned out to multiple Amazon Simple Notification Service (Amazon SNS) topics Use AWS Lambda functions to update the targets
D. Subscribe to an RDS event notification and send an Amazon Simple Notification Service (Amazon SNS) topic fanned out to multiple Amazon Simple Queue Service (Amazon SQS) queues Use AWS Lambda functions to update the targets

Correct Answer: D
Section:
Explanation:
https://docs.aws.amazon.com/lambda/latest/dg/services-rds.html
https://docs.aws.amazon.com/lambda/latest/dg/with-sns.html

QUESTION 74
A company needs to store data in Amazon S3 and must prevent the data from being changed. The company wants new objects that are uploaded to Amazon S3 to remain unchangeable for a nonspecific amount of time until the company decides to modify the objects. Only specific users in the company's AWS account can have the ability to delete the objects. What should a solutions architect do to meet these requirements?

A. Create an S3 Glacier vault Apply a write-once, read-many (WORM) vault lock policy to the objects
B. Create an S3 bucket with S3 Object Lock enabled Enable versioning Set a retention period of 100 years Use governance mode as the S3 bucket's default retention mode for new objects
C. Create an S3 bucket Use AWS CloudTrail to (rack any S3 API events that modify the objects Upon notification, restore the modified objects from any backup versions that the company has
D. Create an S3 bucket with S3 Object Lock enabled Enable versioning Add a legal hold to the objects Add the s3 PutObjectLegalHold permission to the IAM policies of users who need to delete the objects

Correct Answer: D
Section:
Explanation:
"The Object Lock legal hold operation enables you to place a legal hold on an object version. Like setting a retention period, a legal hold prevents an object version from being overwritten or deleted.However, a legal hold doesn't have an associated retention period and remains in effect untilremoved." https://docs.aws.amazon.com/AmazonS3/latest/userguide/batch-ops-legal-hold.html

QUESTION 75
A social media company allows users to upload images to its website. The website runs on Amazon EC2 instances. During upload requests, the website resizes the images to a standard size and stores the resized images in Amazon S3. Users are experiencing slow upload requests to the website.
The company needs to reduce coupling within the application and improve website performance. A solutions architect must design the most operationally efficient process for image uploads. Which combination of actions should the solutions architect take to meet these requirements?
(Choose two.)

A. Configure the application to upload images to S3 Glacier.
B. Configure the web server to upload the original images to Amazon S3.
C. Configure the application to upload images directly from each user's browser to Amazon S3 through the use of a presigned URL.
D. Configure S3 Event Notifications to invoke an AWS Lambda function when an image is uploaded.
Use the function to resize the image
E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function on a schedule to resize uploaded images.

Correct Answer: B, D
Section:
Explanation:

QUESTION 76
A company recently migrated a message processing system to AWS. The system receives messages into an ActiveMQ queue running on an Amazon EC2 instance. Messages are processed by a consumer application running on Amazon EC2. The consumer application processes the messages and writes results to a MySQL database funning on Amazon EC2. The company wants this application to be highly available with tow operational complexity
Which architecture otters the HGHEST availability?

A. Add a second ActiveMQ server to another Availably Zone Add an additional consumer EC2 instance in another Availability Zone. Replicate the MySQL database to another Availability Zone.
B. Use Amazon MO with active/standby brokers configured across two Availability Zones Add an additional consumer EC2 instance in another Availability Zone. Replicate the MySQL database to another Availability Zone.
C. Use Amazon MO with active/standby blotters configured across two Availability Zones. Add an additional consumer EC2 instance in another Availability Zone. Use Amazon ROS tor MySQL with Multi-AZ enabled.
D. Use Amazon MQ with active/standby brokers configured across two Availability Zones Add an Auto Scaling group for the consumer EC2 instances across two Availability Zones. Use Amazon RDS for MySQL with Multi-AZ enabled.

Correct Answer: D
Section:
Explanation:
Amazon S3 is a highly scalable and durable object storage service that can store and retrieve anyamount of data from anywhere on the web1. Users can configure the application to upload images directly from each user's

browser to Amazon S3 through the use of a presigned URL. A presigned URLis a URL that gives access to an object in an S3 bucket for a limited time and with a specific action,such as uploading an object2. Users can generate a presigned URL programmatically using the AWS SDKs or AWS CLI. By using a presigned URL, users can reduce coupling within the application and improve website performance, as they do not need to send the images to the web server first.AWS Lambda is a serverless compute service that runs code in response to events and automaticallymanages the underlying compute resources3. Users can configure S3 Event Notifications to invoke an AWS Lambda function when an image is uploaded. S3 Event Notifications is a feature that allows users to receive notifications when certain events happen in an S3 bucket, such as object creation or deletion. Users can configure S3 Event Notifications to invoke a Lambda function that resizes the image and stores it back in the same or a different S3 bucket. This way, users can offload the image resizing task from the web server to Lambda.

QUESTION 77
A company hosts a containerized web application on a fleet of on-premises servers that process incoming requests. The number of requests is growing quickly. The on-premises servers cannot handle the increased number of requests. The company wants to move the application to AWS with minimum code changes and minimum development effort. Which solution will meet these requirements with the LEAST operational overhead?

A. Use AWS Fargate on Amazon Elastic Container Service (Amazon ECS) to run the containerized web application with Service Auto Scaling. Use an Application Load Balancer to distribute the incoming requests.
B. Use two Amazon EC2 instances to host the containerized web application. Use an Application Load Balancer to distribute the incoming requests
C. Use AWS Lambda with a new code that uses one of the supported languages. Create multiple Lambda functions to support the load. Use Amazon API Gateway as an entry point to the Lambda functions.
D. Use a high performance computing (HPC) solution such as AWS ParallelClusterto establish an HPC cluster that can process the incoming requests at the appropriate scale.

Correct Answer: A
Section:
Explanation:
AWS Fargate is a serverless compute engine that lets users run containers without having to manage servers or clusters of Amazon EC2 instances1. Users can use AWS Fargate on Amazon Elastic Container Service (Amazon ECS) to run the containerized web application with Service Auto
Scaling. Amazon ECS is a fully managed container orchestration service that supports both Docker and Kubernetes2. Service Auto Scaling is a feature that allows users to adjust the desired number of tasks in an ECS service based on CloudWatch metrics, such as CPU utilization or request count3.Users can use AWS Fargate on Amazon ECS to migrate the application to AWS with minimum code changes and minimum development effort, as they only need to package their application in containers and specify the CPU and memory requirements.Users can also use an Application Load Balancer to distribute the incoming requests. An Application Load Balancer is a load balancer that operates at the application layer and routes traffic to targets based on the content of the request. Users can register their ECS tasks as targets for an Application Load Balancer and configure listener rules to route requests to different target groups based on path or host headers. Users can use an Application Load Balancer to improve the availability and performance of their web application.

QUESTION 78
A company uses 50 TB of data for reporting. The company wants to move this data from on premises to AWS A custom application in the company's data center runs a weekly data transformation job. The company plans to pause the application until the data transfer is complete and needs to begin the transfer process as soon as possible. The data center does not have any available network bandwidth for additional workloads A solutions architect must transfer the data and must configure the transformation job to continue to run in the AWS Cloud Which solution will meet these requirements with the LEAST operational overhead?

A. Use AWS DataSync to move the data Create a custom transformation job by using AWS Glue
B. Order an AWS Snowcone device to move the data Deploy the transformation application to the device
C. Order an AWS Snowball Edge Storage Optimized device. Copy the data to the device. Create a custom transformation job by using AWS Glue
D. Order an AWS D. Snowball Edge Storage Optimized device that includes Amazon EC2 compute Copy the data to the device Create a new EC2 instance on AWS to run the transformation application

Correct Answer: C
Section:
Explanation:

QUESTION 79
A company has created an image analysis application in which users can upload photos and add photo frames to their images. The users upload images and metadata to indicate which photo frames they want to add to their images. The application uses a single Amazon EC2 instance and Amazon DynamoDB to store the metadata.
The application is becoming more popular, and the number of users is increasing. The company expects the number of concurrent users to vary significantly depending on the time of day and day of week. The company must ensure that the application can scale to meet the needs of the growing user base.
Which solution meats these requirements?

A. Use AWS Lambda to process the photos. Store the photos and metadata in DynamoDB.
B. Use Amazon Kinesis Data Firehose to process the photos and to store the photos and metadata.
C. Use AWS Lambda to process the photos. Store the photos in Amazon S3. Retain DynamoDB to store the metadata.
D. Increase the number of EC2 instances to three. Use Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volumes to store the photos and metadata.

Correct Answer: C
Section:
Explanation:
https://www.quora.com/How-can-I-use-DynamoDB-for-storing-metadata-for-Amazon-S3-objectsThis solution meets the requirements of scalability, performance, and availability. AWS Lambda can process the photos in parallel and scale up or down automatically depending on the demand.Amazon S3 can store the photos and metadata reliably and durably, and provide high availability and low latency. DynamoDB can store the metadata efficiently and provide consistent performance. This solution also reduces the cost and complexity of managing EC2 instances and EBS volumes.Option A is incorrect because storing the photos in DynamoDB is not a good practice, as it can increase the storage cost and limit the throughput. Option B is incorrect because Kinesis Data Firehose is not designed for processing photos, but for streaming data to destinations such as S3 or Redshift. Option D is incorrect because increasing the number of EC2 instances and using Provisioned IOPS SSD volumes does not guarantee scalability, as it depends on the load balancer and the application code. It also increases the cost and complexity of managing the infrastructure.Reference:https://aws.amazon.com/certification/certified-solutions-architect-professional/ https://www.examtopics.com/discussions/amazon/view/7193-exam-aws-certified-solutions- architect-professional-topic-1/ https://aws.amazon.com/architecture/

QUESTION 80
A company is running an online transaction processing (OLTP) workload on AWS. This workload uses an unencrypted Amazon RDS DB instance in a Multi-AZ deployment. Daily database snapshots are taken from this instance. What should a solutions architect do to ensure the database and snapshots are always encrypted moving forward?

A. Encrypt a copy of the latest DB snapshot. Replace existing DB instance by restoring the encrypted snapshot
B. Create a new encrypted Amazon Elastic Block Store (Amazon EBS) volume and copy the snapshots to it Enable encryption on the DB instance
C. Copy the snapshots and enable encryption using AWS Key Management Service (AWS KMS) Restore encrypted snapshot to an existing DB instance
D. Copy the snapshots to an Amazon S3 bucket that is encrypted using server-side encryption with AWS Key Management Service (AWS KMS) managed keys (SSE-KMS)

Correct Answer: A
Section:
Explanation:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_RestoreFromSnapshot.html#US ER_RestoreFromSnapshot.CON Under "Encrypt unencrypted resources" - https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ EBSEncryption.html

QUESTION 81
A company wants to build a scalable key management Infrastructure to support developers who need to encrypt data in their applications. What should a solutions architect do to reduce the operational burden?

A. Use multifactor authentication (MFA) to protect the encryption keys.
B. Use AWS Key Management Service (AWS KMS) to protect the encryption keys
C. Use AWS Certificate Manager (ACM) to create, store, and assign the encryption keys
D. Use an IAM policy to limit the scope of users who have access permissions to protect the encryption keys

Correct Answer: B
Section:
Explanation:
https://aws.amazon.com/kms/faqs/#:~:text=If%20you%20are%20a%20developer%20who%20needs %20to%20digitally,a%20broad%20set%20of%20industry%20and%20regional%20compliance%20regi mes.

QUESTION 82
A company has a dynamic web application hosted on two Amazon EC2 instances. The company has its own SSL certificate, which is on each instance to perform SSL termination. There has been an increase in traffic recently,

and the operations team determined that SSL encryption and decryption is causing the compute capacity of the web servers to reach their maximum limit. What should a solutions architect do to increase the application's performance?

A. Create a new SSL certificate using AWS Certificate Manager (ACM) install the ACM certificate on each instance
B. Create an Amazon S3 bucket Migrate the SSL certificate to the S3 bucket Configure the EC2 instances to reference the bucket for SSL termination
C. Create another EC2 instance as a proxy server Migrate the SSL certificate to the new instance and configure it to direct connections to the existing EC2 instances
D. Import the SSL certificate into AWS Certificate Manager (ACM) Create an Application Load Balancer with an HTTPS listener that uses the SSL certificate from ACM

Correct Answer: D
Section:
Explanation:
https://aws.amazon.com/certificate-manager/:
"With AWS Certificate Manager, you can quickly request a certificate, deploy it on ACM-integrated AWS resources, such as Elastic Load Balancers, Amazon CloudFront distributions, and APIs on API Gateway, and let AWS Certificate Manager handle certificate renewals. It also enables you to create private certificates for your internal resources and manage the certificate lifecycle centrally."

QUESTION 83
A company has a highly dynamic batch processing job that uses many Amazon EC2 instances to complete it. The job is stateless in nature, can be started and stopped at any given time with no negative impact, and typically takes upwards of 60 minutes total to complete. The company has asked a solutions architect to design a scalable and cost-effective solution that meets the requirements of the job. What should the solutions architect recommend?

A. Implement EC2 Spot Instances
B. Purchase EC2 Reserved Instances
C. Implement EC2 On-Demand Instances
D. Implement the processing on AWS Lambda

Correct Answer: A
Section:
Explanation:

QUESTION 84
A company runs its two-tier ecommerce website on AWS. The web tier consists of a load balancer that sends traffic to Amazon EC2 instances. The database tier uses an Amazon RDS DB instance. The EC2 instances and the RDS DB instance should not be exposed to the public internet. The EC2 instances require internet access to complete payment processing of orders through a third-party web service. The application must be highly available. Which combination of configuration options will meet these requirements? (Choose two.)

A. Use an Auto Scaling group to launch the EC2 instances in private subnets. Deploy an RDS Multi-AZ DB instance in private subnets.
B. Configure a VPC with two private subnets and two NAT gateways across two Availability Zones.
Deploy an Application Load Balancer in the private subnets.
C. Use an Auto Scaling group to launch the EC2 instances in public subnets across two Availability Zones. Deploy an RDS Multi-AZ DB instance in private subnets.
D. Configure a VPC with one public subnet, one private subnet, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnet.
E. Configure a VPC with two public subnets, two private subnets, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnets.

Correct Answer: A, E
Section:
Explanation:
Before you begin: Decide which two Availability Zones you will use for your EC2 instances. Configure your virtual private cloud (VPC) with at least one public subnet in each of these Availability Zones. These public subnets are used to configure the load balancer. You can launch your EC2 instances in other subnets of these Availability Zones instead.

QUESTION 85
A solutions architect needs to implement a solution to reduce a company's storage costs. All the company's data is in the Amazon S3 Standard storage class. The company must keep all data for at least 25 years. Data from the most recent 2 years must be highly available and immediately retrievable.
Which solution will meet these requirements?

A. Set up an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive immediately.
B. Set up an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 2 years.
C. Use S3 Intelligent-Tiering. Activate the archiving option to ensure that data is archived in S3 Glacier Deep Archive.
D. Set up an S3 Lifecycle policy to transition objects to S3 One Zone-Infrequent Access (S3 One Zone- IA) immediately and to S3 Glacier Deep Archive after 2 years.

Correct Answer: B
Section:

QUESTION 86
A media company is evaluating the possibility ot moving rts systems to the AWS Cloud The company needs at least 10 TB of storage with the maximum possible I/O performance for video processing. 300 TB of very durable storage for storing media content, and 900 TB of storage to meet requirements for archival media that is not in use anymore Which set of services should a solutions architect recommend to meet these requirements?

A. Amazon EBS for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage
B. Amazon EBS for maximum performance, Amazon EFS for durable data storage and Amazon S3 Glacier for archival storage
C. Amazon EC2 instance store for maximum performance. Amazon EFS for durable data storage and Amazon S3 for archival storage
D. Amazon EC2 Instance store for maximum performance. Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage

Correct Answer: A
Section:
Explanation:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html

QUESTION 87
A company wants to run applications in containers in the AWS Cloud. These applications are stateless and can tolerate disruptions within the underlying infrastructure. The company needs a solution that minimizes cost and operational overhead.
What should a solutions architect do to meet these requirements?

A. Use Spot Instances in an Amazon EC2 Auto Scaling group to run the application containers.
B. Use Spot Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group.
C. Use On-Demand Instances in an Amazon EC2 Auto Scaling group to run the application containers.
D. Use On-Demand Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group.

Correct Answer: B
Section:
Explanation:

QUESTION 88
A company is running a multi-tier web application on premises. The web application is containerized and runs on a number of Linux hosts connected to a PostgreSQL database that contains user records. The operational overhead of maintaining the infrastructure and capacity planning is limiting the company's growth. A solutions architect must improve the application's infrastructure. Which combination of actions should the solutions architect take to accomplish this? (Choose two.)

A. Migrate the PostgreSQL database to Amazon Aurora

B. Migrate the web application to be hosted on Amazon EC2 instances.
C. Set up an Amazon CloudFront distribution for the web application content.
D. Set up Amazon ElastiCache between the web application and the PostgreSQL database.
E. Migrate the web application to be hosted on AWS Fargate with Amazon Elastic Container Service (Amazon ECS).

Correct Answer: A, E
Section:

QUESTION 89
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 in 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

Correct Answer: B
Section:
Explanation:
https://docs.aws.amazon.com/autoscaling/application/userguide/application-auto-scaling-targettracking. html

QUESTION 90
A company is developing a file-sharing application that will use an Amazon S3 bucket for storage. The company wants to serve all the files through an Amazon CloudFront distribution. The company does not want the files to be accessible through direct navigation to the S3 URL.
What should a solutions architect do to meet these requirements?

A. Write individual policies for each S3 bucket to grant read permission for only CloudFront access.
B. Create an IAM user. Grant the user read permission to objects in the S3 bucket. Assign the user to CloudFront.
C. Write an S3 bucket policy that assigns the CloudFront distribution ID as the Principal and assigns the target S3 bucket as the Amazon Resource Name (ARN).
D. Create an origin access identity (OAI). Assign the OAI to the CloudFront distribution. Configure the S3 bucket permissions so that only the OAI has read permission.

Correct Answer: D
Section:
Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-access-to-amazon-s3/ https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-contentrestricting- access-to-s3.html#private-content-restricting- access-to-s3-overview

QUESTION 91
A company's website provides users with downloadable historical performance reports. The website needs a solution that will scale to meet the company's website demands globally. The solution should be cost-effective, limit the provisioning of infrastructure resources, and provide the fastest possible response time.
Which combination should a solutions architect recommend to meet these requirements?

A. Amazon CloudFront and Amazon S3
B. AWS Lambda and Amazon DynamoDB
C. Application Load Balancer with Amazon EC2 Auto Scaling

D. Amazon Route 53 with internal Application Load Balancers

Correct Answer: A
Section:
Explanation:
Cloudfront for rapid response and s3 to minimize infrastructure.

QUESTION 92
A company runs an Oracle database on premises. As part of the company's migration to AWS, the company wants to upgrade the database to the most recent available version. The company also wants to set up disaster recovery (DR) for the database. The company needs to minimize the operational overhead for normal operations and DR setup. The company also needs to maintain access to the database's underlying operating system. Which solution will meet these requirements?

A. Migrate the Oracle database to an Amazon EC2 instance. Set up database replication to a different AWS Region.
B. Migrate the Oracle database to Amazon RDS for Oracle. Activate Cross-Region automated backups to replicate the snapshots to another AWS Region.
C. Migrate the Oracle database to Amazon RDS Custom for Oracle. Create a read replica for the database in another AWS Region.
D. Migrate the Oracle database to Amazon RDS for Oracle. Create a standby database in another Availability Zone.

Correct Answer: C
Section:
Explanation:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/rds-custom.html
and
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/working-with-custom-oracle.html

QUESTION 93
A company wants to move its application to a serverless solution. The serverless solution needs to analyze existing and new data by using SL. The company stores the data in an Amazon S3 bucket. The data requires encryption and must be replicated to a different AWS Region.
Which solution will meet these requirements with the LEAST operational overhead?

A. Create a new S3 bucket. Load the data into the new S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with AWS KMS multi-Region kays (SSE-KMS). Use Amazon Athena to query the data.
B. Create a new S3 bucket. Load the data into the new S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with AWS KMS multi-Region keys (SSE-KMS). Use Amazon RDS to query the data.
C. Load the data into the existing S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use Amazon Athena to query the data.
D. Load the data into the existing S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use Amazon RDS to query the data.

Correct Answer: A
Section:

QUESTION 94
A company runs workloads on AWS. The company needs to connect to a service from an external provider. The service is hosted in the provider's VPC. According to the company's security team, the connectivity must be private and must be restricted to the target service. The connection must be initiated only from the company's VPC.
Which solution will mast these requirements?

A. Create a VPC peering connection between the company's VPC and the provider's VPC. Update the route table to connect to the target service.
B. Ask the provider to create a virtual private gateway in its VPC. Use AWS PrivateLink to connect to the target service.
C. Create a NAT gateway in a public subnet of the company's VPC. Update the route table to connect to the target service.

D. Ask the provider to create a VPC endpoint for the target service. Use AWS PrivateLink to connect to the target service.

Correct Answer: D
Section:

QUESTION 95
A company is migrating its on-premises PostgreSQL database to Amazon Aurora PostgreSQL. The onpremises database must remain online and accessible during the migration. The Aurora database must remain synchronized with the on- premises database.
Which combination of actions must a solutions architect take to meet these requirements? (Choose two.)

A. Create an ongoing replication task.
B. Create a database backup of the on-premises database
C. Create an AWS Database Migration Service (AWS DMS) replication server
D. Convert the database schema by using the AWS Schema Conversion Tool (AWS SCT).
E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to monitor the database synchronization

Correct Answer: A, C
Section:

QUESTION 96
A company uses AWS Organizations to create dedicated AWS accounts for each business unit to manage each business unit's account independently upon request. The root email recipient missed a notification that was sent to the root user email address of one account. The company wants to ensure that all future notifications are not missed. Future notifications must be limited to account administrators. Which solution will meet these requirements?

A. Configure the company's email server to forward notification email messages that are sent to the AWS account root user email address to all users in the organization.
B. Configure all AWS account root user email addresses as distribution lists that go to a few administrators who can respond to alerts. Configure AWS account alternate contacts in the AWS Organizations console or programmatically.
C. Configure all AWS account root user email messages to be sent to one administrator who is responsible for monitoring alerts and forwarding those alerts to the appropriate groups.
D. Configure all existing AWS accounts and all newly created accounts to use the same root user email address. Configure AWS account alternate contacts in the AWS Organizations console or programmatically.

Correct Answer: B
Section:
Explanation:

QUESTION 97
A company runs its ecommerce application on AWS. Every new order is published as a message in a RabbitMQ queue that runs on an Amazon EC2 instance in a single Availability Zone. These messages are processed by a different application that runs on a separate EC2 instance. This application stores the details in a PostgreSQL database on another EC2 instance. All the EC2 instances are in the same Availability Zone. The company needs to redesign its architecture to provide the highest availability with the least operational overhead. What should a solutions architect do to meet these requirements?

A. Migrate the queue to a redundant pair (active/standby) of RabbitMQ instances on Amazon MQ.
Create a Multi-AZ Auto Scaling group (or EC2 instances that host the application. Create another Multi-AZ Auto Scaling group for EC2 instances that host the PostgreSQL database.
B. Migrate the queue to a redundant pair (active/standby) of RabbitMQ instances on Amazon MQ.
Create a Multi-AZ Auto Scaling group for EC2 instances that host the application. Migrate the database to run on a Multi-AZ deployment of Amazon RDS for PostgreSQL.
C. Create a Multi-AZ Auto Scaling group for EC2 instances that host the RabbitMQ queue. Create another Multi-AZ Auto Scaling group for EC2 instances that host the application. Migrate the database to run on a Multi-AZ deployment of Amazon RDS fqjPostgreSQL.
D. Create a Multi-AZ Auto Scaling group for EC2 instances that host the RabbitMQ queue. Create another Multi-AZ Auto Scaling group for EC2 instances that host the application. Create a third Multi- AZ Auto Scaling group for EC2 instances that host the PostgreSQL database.

Correct Answer: B

Section:
Explanation:
Migrating to Amazon MQ reduces the overhead on the queue management. C and D are dismissed. Deciding between A and B means deciding to go for an AutoScaling group for EC2 or an RDS for Postgress (both multi- AZ). The RDS option has less operational impact, as provide as a service the tools and software required. Consider for instance, the effort to add an additional node like a read replica, to the DB. https://docs.aws.amazon.com/amazon-mq/latest/developer-guide/active-standby-broker- deployment.html https://aws.amazon.com/rds/postgresql/

QUESTION 98
A reporting team receives files each day in an Amazon S3 bucket. The reporting team manually reviews and copies the files from this initial S3 bucket to an analysis S3 bucket each day at the same time to use with Amazon QuickSight. Additional teams are starting to send more files in larger sizes to the initial S3 bucket.
The reporting team wants to move the files automatically analysis S3 bucket as the files enter the initial S3 bucket. The reporting team also wants to use AWS Lambda functions to run patternmatching code on the copied dat a. In addition, the reporting team wants to send the data files to a pipeline in Amazon SageMaker Pipelines.
What should a solutions architect do to meet these requirements with the LEAST operational overhead?

A. Create a Lambda function to copy the files to the analysis S3 bucket. Create an S3 event notification for the analysis S3 bucket. Configure Lambda and SageMaker Pipelines as destinations of the event notification. Configure s30bjectCreated:Put as the event type.
B. Create a Lambda function to copy the files to the analysis S3 bucket. Configure the analysis S3 bucket to send event notifications to Amazon EventBridge (Amazon CloudWatch Events). Configure an ObjectCreated rule in EventBridge (CloudWatch Events). Configure Lambda and SageMaker Pipelines as targets for the rule.
C. Configure S3 replication between the S3 buckets. Create an S3 event notification for the analysis S3 bucket. Configure Lambda and SageMaker Pipelines as destinations of the event notification. Configure s30bjectCreated:Put as the event type.
D. Configure S3 replication between the S3 buckets. Configure the analysis S3 bucket to send event notifications to Amazon EventBridge (Amazon CloudWatch Events). Configure an ObjectCreated rule in EventBridge (CloudWatch Events). Configure Lambda and SageMaker Pipelines as targets for the rule.

Correct Answer: D
Section:
Explanation:
This solution meets the requirements of moving the files automatically, running Lambda functions on the copied data, and sending the data files to SageMaker Pipelines with the least operational overhead. S3 replication can copy the files from the initial S3 bucket to the analysis S3 bucket as they arrive. The analysis S3 bucket can send event notifications to Amazon EventBridge (Amazon CloudWatch Events) when an object is created. EventBridge can trigger Lambda and SageMaker Pipelines as targets for the ObjectCreated rule. Lambda can run pattern-matching code on the copied data, and SageMaker Pipelines can execute a pipeline with the data files.Option A is incorrect because creating a Lambda function to copy the files to the analysis S3 bucket is not necessary when S3 replication can do that automatically. It also adds operational overhead to manage the Lambda function. Option B is incorrect because creating a Lambda function to copy the files to the analysis S3 bucket is not necessary when S3 replication can do that automatically. It also adds operational overhead to manage the Lambda function. Option C is incorrect because using S3 event notification with multiple destinations can result in throttling or delivery failures if there are too many events.Reference:https://aws.amazon.com/blogs/machine-learning/automate-feature-engineering-pipelines-with- amazon-sagemaker/ https://docs.aws.amazon.com/sagemaker/latest/dg/automating-sagemaker-with-eventbridge.html

QUESTION 99
A solutions architect needs to help a company optimize the cost of running an application on AWS.
The application will use Amazon EC2 instances, AWS Fargate, and AWS Lambda for compute within the architecture. The EC2 instances will run the data ingestion layer of the application. EC2 usage will be sporadic and unpredictable. Workloads that run on EC2 instances can be interrupted at any time. The application front end will run on Fargate, and Lambda will serve the API layer. The front-end utilization and API layer utilization will be predictable over the course of the next year. Which combination of purchasing options will provide the MOST cost-effective solution for hosting this application? (Choose two.)

A. Use Spot Instances for the data ingestion layer
B. Use On-Demand Instances for the data ingestion layer
C. Purchase a 1-year Compute Savings Plan for the front end and API layer.
D. Purchase 1-year All Upfront Reserved instances for the data ingestion layer.
E. Purchase a 1-year EC2 instance Savings Plan for the front end and API layer.

Correct Answer: A, C
Section:

QUESTION 100
A company runs a web-based portal that provides users with global breaking news, local alerts, and weather updates. The portal delivers each user a personalized view by using mixture of static and dynamic content. Content is served over HTTPS through an API server running on an Amazon EC2 instance behind an Application Load Balancer (ALB). The company wants the portal to provide this content to its users across the world as quickly as possible. How should a solutions architect design the application to ensure the LEAST amount of latency for all users?

A. Deploy the application stack in a single AWS Region. Use Amazon CloudFront to serve all static and dynamic content by specifying the ALB as an origin.
B. Deploy the application stack in two AWS Regions. Use an Amazon Route 53 latency routing policy to serve all content from the ALB in the closest Region.
C. Deploy the application stack in a single AWS Region. Use Amazon CloudFront to serve the static content. Serve the dynamic content directly from the ALB.
D. Deploy the application stack in two AWS Regions. Use an Amazon Route 53 geolocation routing policy to serve all content from the ALB in the closest Region.

Correct Answer: A
Section:
Explanation:
https://aws.amazon.com/blogs/networking-and-content-delivery/deliver-your-apps-dynamiccontent- using-amazon-cloudfront-getting-started-template/

QUESTION 101
A gaming company is designing a highly available architecture. The application runs on a modified Linux kernel and supports only UDP-based traffic. The company needs the front-end tier to provide the best possible user experience. That tier must have low latency, route traffic to the nearest edge location, and provide static IP addresses for entry into the application endpoints. What should a solutions architect do to meet these requirements?

A. Configure Amazon Route 53 to forward requests to an Application Load Balancer. Use AWS Lambda for the application in AWS Application Auto Scaling.
B. Configure Amazon CloudFront to forward requests to a Network Load Balancer. Use AWS Lambda for the application in an AWS Application Auto Scaling group.
C. Configure AWS Global Accelerator to forward requests to a Network Load Balancer. Use Amazon EC2 instances for the application in an EC2 Auto Scaling group.
D. Configure Amazon API Gateway to forward requests to an Application Load Balancer. Use Amazon EC2 instances for the application in an EC2 Auto Scaling group.

Correct Answer: C
Section:

QUESTION 102
A company wants to migrate its existing on-premises monolithic application to AWS.
The company wants to keep as much of the front- end code and the backend code as possible.
However, the company wants to break the application into smaller applications. A different team will manage each application. The company needs a highly scalable solution that minimizes operational overhead. Which solution will meet these requirements?

A. Host the application on AWS Lambda Integrate the application with Amazon API Gateway.
B. Host the application with AWS Amplify. Connect the application to an Amazon API Gateway API that is integrated with AWS Lambda.
C. Host the application on Amazon EC2 instances. Set up an Application Load Balancer with EC2 instances in an Auto Scaling group as targets.
D. Host the application on Amazon Elastic Container Service (Amazon ECS) Set up an Application Load Balancer with Amazon ECS as the target.

Correct Answer: D
Section:
Explanation:
https://aws.amazon.com/blogs/compute/microservice-delivery-with-amazon-ecs-and-applicationload- balancers/

QUESTION 103
A company recently started using Amazon Aurora as the data store for its global ecommerce application When large reports are run developers report that the ecommerce application is performing poorly After reviewing metrics in Amazon CloudWatch, a solutions architect finds that the ReadlOPS and CPUUtilization metrics are spiking when monthly reports run. What is the MOST cost-effective solution?

A. Migrate the monthly reporting to Amazon Redshift.

B. Migrate the monthly reporting to an Aurora Replica
C. Migrate the Aurora database to a larger instance class
D. Increase the Provisioned IOPS on the Aurora instance

Correct Answer: B
Section:
Explanation:
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html #Aurora.Replication.Replicas Aurora Replicas have two main purposes. You can issue queries to them to scale the read operations for your application. You typically do so by connecting to the reader endpoint of the cluster. That way, Aurora can spread the load for read-only connections across as many Aurora Replicas as you have in the cluster. Aurora Replicas also help to increase availability. If the writer instance in a cluster becomes unavailable, Aurora automatically promotes one of the reader instances to take its place as the new writer. https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Overview.html

QUESTION 104
A company hosts a website analytics application on a single Amazon EC2 On-Demand Instance. The analytics software is written in PHP and uses a MySQL database. The analytics software, the web server that provides PHP, and the database server are all hosted on the EC2 instance. The application is showing signs of performance degradation during busy times and is presenting 5xx errors. The company needs to make the application scale seamlessly. Which solution will meet these requirements MOST cost-effectively?

A. Migrate the database to an Amazon RDS for MySQL DB instance. Create an AMI of the web application. Use the AMI to launch a second EC2 On-Demand Instance. Use an Application Load Balancer to distribute the load to each EC2 instance.
B. Migrate the database to an Amazon RDS for MySQL DB instance. Create an AMI of the web application. Use the AMI to launch a second EC2 On-Demand Instance. Use Amazon Route 53 weighted routing to distribute the load across the two EC2 instances.
C. Migrate the database to an Amazon Aurora MySQL DB instance. Create an AWS Lambda function to stop the EC2 instance and change the instance type. Create an Amazon CloudWatch alarm to invoke the Lambda function when CPU utilization surpasses 75%.
D. Migrate the database to an Amazon Aurora MySQL DB instance. Create an AMI of the web application. Apply the AMI to a launch template. Create an Auto Scaling group with the launch template Configure the launch template to use a Spot Fleet. Attach an Application Load Balancer to the Auto Scaling group.

Correct Answer: D
Section:

QUESTION 105

A company runs a stateless web application in production on a group of Amazon EC2 On-Demand Instances behind an Application Load Balancer. The application experiences heavy usage during an 8- hour period each business day. Application usage is moderate and steady overnight Application usage is low during weekends.

The company wants to minimize its EC2 costs without affecting the availability of the application.

Which solution will meet these requirements?

A. Use Spot Instances for the entire workload.
B. Use Reserved instances for the baseline level of usage Use Spot Instances for any additional capacity that the application needs.
C. Use On-Demand Instances for the baseline level of usage. Use Spot Instances for any additional capacity that the application needs
D. Use Dedicated Instances for the baseline level of usage. Use On-Demand Instances for any additional capacity that the application needs

Correct Answer: B
Section:

QUESTION 106
A company needs to retain application logs files for a critical application for 10 years. The application team regularly accesses logs from the past month for troubleshooting, but logs older than 1 month are rarely accessed. The application generates more than 10 TB of logs per month.
Which storage option meets these requirements MOST cost-effectively?

A. Store the Iogs in Amazon S3 Use AWS Backup lo move logs more than 1 month old to S3 Glacier Deep Archive
B. Store the logs in Amazon S3 Use S3 Lifecycle policies to move logs more than 1 month old to S3 Glacier Deep Archive
C. Store the logs in Amazon CloudWatch Logs Use AWS Backup to move logs more then 1 month old to S3 Glacier Deep Archive
D. Store the logs in Amazon CloudWatch Logs Use Amazon S3 Lifecycle policies to move logs more than 1 month old to S3 Glacier Deep Archive

Correct Answer: B
Section:
Explanation:
You need S3 to be able to archive the logs after one month. Cannot do that with CloudWatch Logs.

QUESTION 107
A company has a data ingestion workflow that includes the following components:
• An Amazon Simple Notation Service (Amazon SNS) topic that receives notifications about new data deliveries
• An AWS Lambda function that processes and stores the data
The ingestion workflow occasionally fails because of network connectivity issues. When tenure occurs the corresponding data is not ingested unless the company manually reruns the job. What should a solutions architect do to ensure that all notifications are eventually processed?

A. Configure the Lambda function (or deployment across multiple Availability Zones
B. Modify me Lambda functions configuration to increase the CPU and memory allocations tor the (unction
C. Configure the SNS topic's retry strategy to increase both the number of retries and the wait time between retries
D. Configure an Amazon Simple Queue Service (Amazon SQS) queue as the on failure destination Modify the Lambda function to process messages in the queue

Correct Answer: D
Section:
Explanation:
https://docs.aws.amazon.com/sns/latest/dg/sns-dead-letter-queues.html

QUESTION 108
A company has a service that produces event dat a. The company wants to use AWS to process the event data as it is received. The data is written in a specific order that must be maintained throughout processing The company wants to implement a solution that minimizes operational overhead.
How should a solutions architect accomplish this?

A. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue to hold messages Set up an AWS Lambda function to process messages from the queue

B. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process Configure an AWS Lambda function as a subscriber.
C. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to hold messages. Set up an AWS Lambda function to process messages from the queue independently
D. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a subscriber.

Correct Answer: A
Section:
Explanation:
The details are revealed in below url:
https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFOqueues. html FIFO (First-In-First-Out) queues are designed to enhance messaging between applications when the order of operations and events is critical, or where duplicates can't be tolerated. Examples of situations where you might use FIFO queues include the following: To make sure that user-entered commands are run in the right order. To display the correct product price by sending price modifications in the right order. To prevent a student from enrolling in a course before registering for an account.

QUESTION 109
A company is migrating an application from on-premises servers to Amazon EC2 instances. As part of the migration design requirements, a solutions architect must implement infrastructure metric alarms. The company does not need to take action if CPU utilization increases to more than 50% for a short burst of time. However, if the CPU utilization increases to more than 50% and read IOPS on the disk are high at the same time, the company needs to act as soon as possible. The solutions architect also must reduce false alarms.
What should the solutions architect do to meet these requirements?

A. Create Amazon CloudWatch composite alarms where possible.
B. Create Amazon CloudWatch dashboards to visualize the metrics and react to issues quickly.
C. Create Amazon CloudWatch Synthetics canaries to monitor the application and raise an alarm.
D. Create single Amazon CloudWatch metric alarms with multiple metric thresholds where possible.

Correct Answer: A
Section:

QUESTION 110
A company runs an application using Amazon ECS. The application creates esi/ed versions of an original image and then makes Amazon S3 API calls to store the resized images in Amazon S3. How can a solutions architect ensure that the application has permission to access Amazon S3?

A. Update the S3 role in AWS IAM to allow read/write access from Amazon ECS, and then relaunch the container.
B. Create an IAM role with S3 permissions, and then specify that role as the taskRoleAm in the task definition.
C. Create a security group that allows access from Amazon ECS to Amazon S3, and update the launch configuration used by the ECS cluster.
D. Create an IAM user with S3 permissions, and then relaunch the Amazon EC2 instances for the ECS cluster while logged in as this account.

Correct Answer: B
Section:

QUESTION 111
A solutions architect needs to securely store a database user name and password that an application uses to access an Amazon RDS DB instance. The application that accesses the database runs on an Amazon EC2 instance. The solutions architect wants to create a secure parameter in AWS Systems Manager Parameter Store.
What should the solutions architect do to meet this requirement?

A. Create an IAM role that has read access to the Parameter Store parameter. Allow Decrypt access to an AWS Key Management Service (AWS KMS) key that is used to encrypt the parameter. Assign this IAM role to the EC2 instance.
B. Create an IAM policy that allows read access to the Parameter Store parameter. Allow Decrypt access to an AWS Key Management Service (AWS KMS) key that is used to encrypt the parameter. Assign this IAM policy to the EC2 instance.
C. Create an IAM trust relationship between the Parameter Store parameter and the EC2 instance.

Specify Amazon RDS as a principal in the trust policy.

D. Create an IAM trust relationship between the DB instance and the EC2 instance. Specify Systems Manager as a principal in the trust policy.

Correct Answer: A
Section:
Explanation:

QUESTION 112
An entertainment company is using Amazon DynamoDB to store media metadat a. The application is read intensive and experiencing delays. The company does not have staff to handle additional operational overhead and needs to improve the performance efficiency of DynamoDB without reconfiguring the application.
What should a solutions architect recommend to meet this requirement?

A. Use Amazon ElastiCache for Redis.
B. Use Amazon DynamoDB Accelerator (DAX).
C. Replicate data by using DynamoDB global tables.
D. Use Amazon ElastiCache for Memcached with Auto Discovery enabled.

Correct Answer: B
Section:
Explanation:
https://aws.amazon.com/dynamodb/dax/

QUESTION 113
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.

Correct Answer: D
Section:
Explanation:
Service control policies (SCPs) are one type of policy that you can use to manage your organization. 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. See https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html.

QUESTION 114
A company is concerned about the security of its public web application due to recent web attacks.
The application uses an Application Load Balancer (ALB). A solutions architect must reduce the risk of DDoS attacks against the application. What should the solutions architect do to meet this requirement?

A. Add an Amazon Inspector agent to the ALB.
B. Configure Amazon Macie to prevent attacks.
C. Enable AWS Shield Advanced to prevent attacks.
D. Configure Amazon GuardDuty to monitor the ALB.

Correct Answer: C
Section:

QUESTION 115
A company runs a production application on a fleet of Amazon EC2 instances. The application reads the data from an Amazon SQS queue and processes the messages in parallel. The message volume is unpredictable and often has intermittent traffic. This application should continually process messages without any downtime.
Which solution meets these requirements MOST cost-effectively?

A. Use Spot Instances exclusively to handle the maximum capacity required.
B. Use Reserved Instances exclusively to handle the maximum capacity required.
C. Use Reserved Instances for the baseline capacity and use Spot Instances to handle additional capacity.
D. Use Reserved Instances for the baseline capacity and use On-Demand Instances to handle additional capacity.

Correct Answer: D
Section:
Explanation:
We recommend that you use On-Demand Instances for applications with short-term, irregular workloads that cannot be interrupted. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-on-demand-instances.html

QUESTION 116
A solutions architect must design a solution that uses Amazon CloudFront with an Amazon S3 origin to store a static website. The company's security policy requires that all website traffic be inspected by AWS WAR How should the solutions architect comply with these requirements?

A. Configure an S3 bucket policy lo accept requests coming from the AWS WAF Amazon Resource Name (ARN) only.
B. Configure Amazon CloudFront to forward all incoming requests to AWS WAF before requesting content from the S3 origin.
C. Configure a security group that allows Amazon CloudFront IP addresses to access Amazon S3 only.
Associate AWS WAF to CloudFront.
D. Configure Amazon CloudFront and Amazon S3 to use an origin access identity (OAI) to restrict access to the S3 bucket. Enable AWS WAF on the distribution.

Correct Answer: D
Section:
Explanation:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-contentrestricting-access-to-s3.html
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-webawswaf.html

QUESTION 117
A company wants to manage Amazon Machine Images (AMIs). The company currently copies AMIs to the same AWS Region where the AMIs were created. The company needs to design an application that captures AWS API calls and sends alerts whenever the Amazon EC2 Createlmage API operation is called within the company's account. Which solution will meet these requirements with the LEAST operational overhead?

A. Create an AWS Lambda function to query AWS CloudTrail logs and to send an alert when a Createlmage API call is detected.
B. Configure AWS CloudTrail with an Amazon Simple Notification Service {Amazon SNS) notification that occurs when updated logs are sent to Amazon S3. Use Amazon Athena to create a new table and to query on Createlmage when an API call is detected.
C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for the Createlmage API call.
Configure the target as an Amazon Simple Notification Service (Amazon SNS) topic to send an alert when a Createlmage API call is detected.
D. Configure an Amazon Simple Queue Service (Amazon SQS) FIFO queue as a target for AWS CloudTrail logs. Create an AWS Lambda function to send an alert to an Amazon Simple Notification Service (Amazon SNS) topic when a Createlmage API call is detected.

Correct Answer: C
Section:
Explanation:

QUESTION 118
An online retail company has more than 50 million active customers and receives more than 25,000 orders each day. The company collects purchase data for customers and stores this data in Amazon S3. Additional customer data is stored in Amazon RDS.
The company wants to make all the data available to various teams so that the teams can perform analytics. The solution must provide the ability to manage fine-grained permissions for the data and must minimize operational overhead. Which solution will meet these requirements?

A. Migrate the purchase data to write directly to Amazon RDS. Use RDS access controls to limit access.
B. Schedule an AWS Lambda function to periodically copy data from Amazon RDS to Amazon S3.
Create an AWS Glue crawler. Use Amazon Athena to query the data. Use S3 policies to limit access.
C. Create a data lake by using AWS Lake Formation. Create an AWS Glue JDBC connection to Amazon RDS. Register (he S3 bucket in Lake Formation. Use Lake Formation access controls to limit access.
D. Create an Amazon Redshift cluster. Schedule an AWS Lambda function to periodically copy data from Amazon S3 and Amazon RDS to Amazon Redshift. Use Amazon Redshift access controls to limit access.

Correct Answer: D
Section:
Explanation:

QUESTION 119
A company provides an API to its users that automates inquiries for tax computations based on item prices. The company experiences a larger number of inquiries during the holiday season only that cause slower response times. A solutions architect needs to design a solution that is scalable and elastic.
What should the solutions architect do to accomplish this?

A. Provide an API hosted on an Amazon EC2 instance. The EC2 instance performs the required computations when the API request is made.
B. Design a REST API using Amazon API Gateway that accepts the item names. API Gateway passes item names to AWS Lambda for tax computations.
C. Create an Application Load Balancer that has two Amazon EC2 instances behind it. The EC2 instances will compute the tax on the received item names.
D. Design a REST API using Amazon API Gateway that connects with an API hosted on an Amazon EC2 instance. API Gateway accepts and passes the item names to the EC2 instance for tax computations.

Correct Answer: B
Section:
Explanation:
Lambda server-less is scalable and elastic than EC2 api gateway solution

QUESTION 120
A company wants to use high performance computing (HPC) infrastructure on AWS for financial risk modeling. The company's HPC workloads run on Linux. Each HPC workflow runs on hundreds of Amazon EC2 Spot Instances, is shorl- lived, and generates thousands of output files that are ultimately stored in persistent storage for analytics and long-term future use. The company seeks a cloud storage solution that permits the copying of on-premises data to longterm persistent storage to make data available for processing by all EC2 instances. The solution should also be a high performance file system that is integrated with persistent storage to read and write datasets and output files.
Which combination of AWS services meets these requirements?

A. Amazon FSx for Lustre integrated with Amazon S3
B. Amazon FSx for Windows File Server integrated with Amazon S3
C. Amazon S3 Glacier integrated with Amazon Elastic Block Store (Amazon EBS)
D. Amazon S3 bucket with a VPC endpoint integrated with an Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2) volume

Correct Answer: A
Section:
Explanation:

https://aws.amazon.com/fsx/lustre/
Amazon FSx for Lustre is a fully managed service that provides cost-effective, high-performance, scalable storage for compute workloads. Many workloads such as machine learning, high performance computing (HPC), video rendering, and financial simulations depend on compute instances accessing the same set of data through high-performance shared storage.

QUESTION 121
A company is running a publicly accessible serverless application that uses Amazon API Gateway and AWS Lambd a. The application's traffic recently spiked due to fraudulent requests from botnets. Which steps should a solutions architect take to block requests from unauthorized users? (Select TWO.)

A. Create a usage plan with an API key that is shared with genuine users only.
B. Integrate logic within the Lambda function to ignore the requests from fraudulent IP addresses.
C. Implement an AWS WAF rule to target malicious requests and trigger actions to filter them out.
D. Convert the existing public API to a private API. Update the DNS records to redirect users to the new API endpoint.
E. Create an IAM role for each user attempting to access the API. A user will assume the role when making the API call.

Correct Answer: A, C
Section:
Explanation:
https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usageplans.html#:~:text=Don%27t%20rely%20on%20API%20keys%20as%20your%20only%20means%20of%20authentication%20and%20authorization% 20for%20your%20APIs
https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html

QUESTION 122
A solutions architect is designing the architecture of a new application being deployed to the AWS Cloud. The application will run on Amazon EC2 On-Demand Instances and will automatically scale across multiple Availability Zones. The EC2 instances will scale up and down frequently throughout the day. An Application Load Balancer (ALB) will handle the load distribution. The architecture needs to support distributed session data management. The company is willing to make changes to code if needed.
What should the solutions architect do to ensure that the architecture supports distributed session data management?

A. Use Amazon ElastiCache to manage and store session data.
B. Use session affinity (sticky sessions) of the ALB to manage session data.
C. Use Session Manager from AWS Systems Manager to manage the session.
D. Use the GetSessionToken API operation in AWS Security Token Service (AWS STS) to manage the session

Correct Answer: A
Section:
Explanation:
https://aws.amazon.com/vi/caching/session-management/
In order to address scalability and to provide a shared data storage for sessions that can be accessible from any individual web server, you can abstract the HTTP sessions from the web servers themselves. A common solution to for this is to leverage an In-Memory Key/Value store such as Redis and Memcached. ElastiCache offerings for In-Memory key/value stores include ElastiCache for Redis, which can support replication, and ElastiCache for Memcached which does not support replication.

QUESTION 123
A company hosts a marketing website in an on-premises data center. The website consists of static documents and runs on a single server. An administrator updates the website content infrequently and uses an SFTP client to upload new documents.
The company decides to host its website on AWS and to use Amazon CloudFront. The company's solutions architect creates a CloudFront distribution. The solutions architect must design the most cost-effective and resilient architecture for website hosting to serve as the CloudFront origin.
Which solution will meet these requirements?

A. Create a virtual server by using Amazon Lightsail. Configure the web server in the Lightsail instance. Upload website content by using an SFTP client.

B. Create an AWS Auto Scaling group for Amazon EC2 instances. Use an Application Load Balancer.
Upload website content by using an SFTP client.
C. Create a private Amazon S3 bucket. Use an S3 bucket policy to allow access from a CloudFront origin access identity (OAI). Upload website content by using theAWSCLI.
D. Create a public Amazon S3 bucket. Configure AWS Transfer for SFTP. Configure the S3 bucket for website hosting. Upload website content by using the SFTP client.

Correct Answer: C
Section:
Explanation:
https://docs.aws.amazon.com/cli/latest/reference/transfer/describe-server.html

QUESTION 124
A company is developing an ecommerce application that will consist of a load-balanced front end, a container-based application, and a relational database. A solutions architect needs to create a highly available solution that operates with as little manual intervention as possible.
Which solutions meet these requirements? (Select TWO.)

A. Create an Amazon RDS DB instance in Multi-AZ mode.
B. Create an Amazon RDS DB instance and one or more replicas in another Availability Zone.
C. Create an Amazon EC2 in stance-based Docker cluster to handle the dynamic application load.
D. Create an Amazon Elastic Container Service (Amazon ECS) cluster with a Fargate launch type to handle the dynamic application load.
E. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an Amazon EC2 launch type to handle the dynamic application load.

Correct Answer: A, D
Section:
Explanation:
https://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcome.html
1. Relational database: RDS
2. Container-based applications: ECS
"Amazon ECS enables you to launch and stop your container-based applications by using simple API calls. You can also retrieve the state of your cluster from a centralized service and have access to many familiar Amazon EC2 features." 3. Little manual intervention: Fargate
You can run your tasks and services on a serverless infrastructure that is managed by AWS Fargate.
Alternatively, for more control over your infrastructure, you can run your tasks and services on a cluster of Amazon EC2 instances that you manage.

QUESTION 125
A company is designing a cloud communications platform that is driven by APIs. The application is hosted on Amazon EC2 instances behind a Network Load Balancer (NLB). The company uses Amazon API Gateway to provide external users with access to the application through APIs. The company wants to protect the platform against web exploits like SQL injection and also wants to detect and mitigate large, sophisticated DDoS attacks.
Which combination of solutions provides the MOST protection? (Select TWO.)

A. Use AWS WAF to protect the NLB.
B. Use AWS Shield Advanced with the NLB.
C. Use AWS WAF to protect Amazon API Gateway.
D. Use Amazon GuardDuty with AWS Shield Standard.
E. Use AWS Shield Standard with Amazon API Gateway.

Correct Answer: B, C
Section:
Explanation:
AWS Shield Advanced provides expanded DDoS attack protection for your Amazon EC2 instances, Elastic Load Balancing load balancers, CloudFront distributions, Route 53 hosted zones, and AWS Global Accelerator standard accelerators.AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to your protected web application resources. You can protect the following resource

types:Amazon CloudFront distribution Amazon API Gateway REST API Application Load Balancer AWS AppSync GraphQL API Amazon Cognito user pool https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.htm

QUESTION 126
What should a solutions architect do to ensure that all objects uploaded to an Amazon S3 bucket are encrypted?

A. Update the bucket policy to deny if the PutObject does not have an s3 x-amz-acl header set
B. Update the bucket policy to deny if the PutObject does not have an s3:x-amz-aci header set to private.
C. Update the bucket policy to deny if the PutObject does not have an aws SecureTransport header set to true
D. Update the bucket policy to deny if the PutObject does not have an x-amz-server-sideencryption header set.

Correct Answer: D
Section:
Explanation:
https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-toamazons3/#:~:text=Solution%20overview,console%2C%20CLI%2C%20or%20SDK.&text=To%20encrypt%20an%20object%20at,S3%2C%20or% 20SSE%2DKMS.

QUESTION 127
A company uses a legacy application to produce data in CSV format The legacy application stores the output data In Amazon S3 The company is deploying a new commercial off-the-shelf (COTS) application that can perform complex SQL queries to analyze data that is stored Amazon Redshift and Amazon S3 only However the COTS application cannot process the csv files that the legacy application produces The company cannot update the legacy application to produce data in another format The company needs to implement a solution so that the COTS application can use the data that the legacy applicator produces. Which solution will meet these requirements with the LEAST operational overhead?

A. Create a AWS Glue extract, transform, and load (ETL) job that runs on a schedule. Configure the ETL job to process the .csv files and store the processed data in Amazon Redshit.
B. Develop a Python script that runs on Amazon EC2 instances to convert the. csv files to sql files invoke the Python script on cron schedule to store the output files in Amazon S3.
C. Create an AWS Lambda function and an Amazon DynamoDB table. Use an S3 event to invoke the Lambda function. Configure the Lambda function to perform an extract transform, and load (ETL) job to process the .csv files and store the processed data in the DynamoDB table.
D. Use Amazon EventBridge (Amazon CloudWatch Events) to launch an Amazon EMR cluster on a weekly schedule. Configure the EMR cluster to perform an extract, tractform, and load (ETL) job to process the .csv files and store the processed data in an Amazon Redshift table.

Correct Answer: A
Section:
Explanation:
This solution meets the requirements of implementing a solution so that the COTS application can use the data that the legacy application produces with the least operational overhead. AWS Glue is a fully managed service that provides a serverless ETL platform to prepare and load data for analytics. AWS Glue can process data in various formats, including .csv files, and store the processed data in Amazon Redshift, which is a fully managed data warehouse service that supports complex SQL queries. AWS Glue can run ETL jobs on a schedule, which can automate the data processing and loading process. Option B is incorrect because developing a Python script that runs on Amazon EC2 instances to convert the .csv files to sql files can increase the operational overhead and complexity, and it may not provide consistent data processing and loading for the COTS application. Option C is incorrect because creating an AWS Lambda function and an Amazon DynamoDB table to process the .csv files and store the processed data in the DynamoDB table does not meet the requirement of using Amazon Redshift as the data source for the COTS application. Option D is incorrect because using Amazon EventBridge (Amazon CloudWatch Events) to launch an Amazon EMR cluster on a weekly schedule to process the .csv files and store the processed data in an Amazon Redshift table can increase the operational overhead and complexity, and it may not provide timely data processing and loading for the COTS application. https://aws.amazon.com/glue/

QUESTION 128
A medical records company is hosting an application on Amazon EC2 instances. The application processes customer data files that are stored on Amazon S3. The EC2 instances are hosted in public subnets. The EC2 instances access Amazon S3 over the internet, but they do not require any other network access.
A new requirement mandates that the network traffic for file transfers take a private route and not be sent over the internet. Which change to the network architecture should a solutions architect recommend to meet this requirement?

A. Create a NAT gateway. Configure the route table for the public subnets to send traffic to Amazon S3 through the NAT gateway.
B. Configure the security group for the EC2 instances to restrict outbound traffic so that only traffic to the S3 prefix list is permitted.

C. Move the EC2 instances to private subnets. Create a VPC endpoint for Amazon S3, and link the endpoint to the route table for the private subnets
D. Remove the internet gateway from the VPC. Set up an AWS Direct Connect connection, and route traffic to Amazon S3 over the Direct Connect connection.

Correct Answer: C
Section:
Explanation:
To meet the new requirement of transferring files over a private route, the EC2 instances should be moved to private subnets, which do not have direct access to the internet. This ensures that the traffic for file transfers does not go over the internet. To enable the EC2 instances to access Amazon S3, a VPC endpoint for Amazon S3 can be created. VPC endpoints allow resources within a VPC to communicate with resources in other services without the traffic being sent over the internet. By linking the VPC endpoint to the route table for the private subnets, the EC2 instances can access Amazon S3 over a private connection within the VPC.

QUESTION 129
A company uses a popular content management system (CMS) for its corporate website. However, the required patching and maintenance are burdensome. The company is redesigning its website and wants anew solution. The website will be updated four times a year and does not need to have any dynamic content available. The solution must provide high scalability and enhanced security. Which combination of changes will meet these requirements with the LEAST operational overhead?
(Choose two.)

A. Deploy an AWS WAF web ACL in front of the website to provide HTTPS functionality
B. Create and deploy an AWS Lambda function to manage and serve the website content
C. Create the new website and an Amazon S3 bucket Deploy the website on the S3 bucket with static website hosting enabled
D. Create the new website. Deploy the website by using an Auto Scaling group of Amazon EC2 instances behind an Application Load Balancer.

Correct Answer: A, D
Section:
Explanation:
A -> We can configure CloudFront to require HTTPS from clients (enhanced security) https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-viewers-to- cloudfront.html D -> storing static website on S3 provides scalability and less operational overhead, then configuration of Application LB and EC2 instances (hence E is out)

QUESTION 130
A company stores its application logs in an Amazon CloudWatch Logs log group. A new policy requires the company to store all application logs in Amazon OpenSearch Service (Amazon Elasticsearch Service) in near-real time. Which solution will meet this requirement with the LEAST operational overhead?

A. Configure a CloudWatch Logs subscription to stream the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).
B. Create an AWS Lambda function. Use the log group to invoke the function to write the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).
C. Create an Amazon Kinesis Data Firehose delivery stream Configure the log group as the delivery stream's source. Configure Amazon OpenSearch Service (Amazon Elasticsearch Service) as the delivery stream's destination.
D. Install and configure Amazon Kinesis Agent on each application server to deliver the logs to Amazon Kinesis Data Streams. Configure Kinesis Data Streams to deliver the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service)

Correct Answer: A
Section:
Explanation:

QUESTION 131
A company is building a web-based application running on Amazon EC2 instances in multiple Availability Zones. The web application will provide access to a repository of text documents totaling about 900 TB in size. The company anticipates that the web application will experience periods of high demand. A solutions architect must ensure that the storage component for the text documents can scale to meet the demand of the application at all times. The company is concerned about the overall cost of the solution.
Which storage solution meets these requirements MOST cost-effectively?

A. Amazon Elastic Block Store (Amazon EBS)
B. Amazon Elastic File System (Amazon EFS)
C. Amazon Elasticsearch Service (Amazon ES)
D. Amazon S3

Correct Answer: D
Section:
Explanation:
Amazon S3 is cheapest and can be accessed from anywhere.

QUESTION 132
A global company is using Amazon API Gateway to design REST APIs for its loyalty club users in the us-east-1 Region and the ap-southeast-2 Region. A solutions architect must design a solution to protect these API Gateway managed REST APIs across multiple accounts from SQL injection and cross-site scripting attacks.
Which solution will meet these requirements with the LEAST amount of administrative effort?

A. Set up AWS WAF in both Regions. Associate Regional web ACLs with an API stage.
B. Set up AWS Firewall Manager in both Regions. Centrally configure AWS WAF rules.
C. Set up AWS Shield in bath Regions. Associate Regional web ACLs with an API stage.
D. Set up AWS Shield in one of the Regions. Associate Regional web ACLs with an API stage.

Correct Answer: B
Section:
Explanation:

QUESTION 133
A company has implemented a self-managed DNS solution on three Amazon EC2 instances behind a Network Load Balancer (NLB) in the us-west-2 Region. Most of the company's users are located in the United States and Europe. The company wants to improve the performance and availability of the solution. The company launches and configures three EC2 instances in the eu-west-1 Region and adds the EC2 instances as targets for a new NLB. Which solution can the company use to route traffic to all the EC2 instances?

A. Create an Amazon Route 53 geolocation routing policy to route requests to one of the two NLBs.
Create an Amazon CloudFront distribution. Use the Route 53 record as the distribution's origin.
B. Create a standard accelerator in AWS Global Accelerator. Create endpoint groups in us-west-2 and eu-west-1. Add the two NLBs as endpoints for the endpoint groups.
C. Attach Elastic IP addresses to the six EC2 instances. Create an Amazon Route 53 geolocation routing policy to route requests to one of the six EC2 instances. Create an Amazon CloudFront distribution. Use the Route 53 record as the distribution's origin.
D. Replace the two NLBs with two Application Load Balancers (ALBs). Create an Amazon Route 53 latency routing policy to route requests to one of the two ALBs. Create an Amazon CloudFront distribution. Use the Route 53 record as the distribution's origin.

Correct Answer: B
Section:

QUESTION 134
A solution architect must create a disaster recovery (DR) plan for a high-volume software as a service (SaaS) platform. All data for the platform is stored in an Amazon Aurora MySQL DB cluster.
The DR plan must replcate data to a secondary AWS Region.
Which solution will meet these requirements MOST cost-effectively?
Use MySQL binary log replication to an Aurora cluster

A. Use MySQL binary log replication to an Aurora cluster in the secondary Region Provision one DB instance for the Aurora cluster in the secondary Region.

B. Set up an Aurora global database for the DB cluster. When setup is complete, remove the DB instance from the secondary Region.
C. Use AWS Database Migration Service (AWS QMS) to continuously replicate data to an Aurora cluster in the secondary Region Remove theDB instance from the secondary Region.
D. Set up an Aurora global database for the DB cluster Specify a minimum of one DB instance in the secondary Region

Correct Answer: D
Section:

QUESTION 135
A company has a multi-tier application deployed on several Amazon EC2 instances in an Auto Scaling group. An Amazon RDS for Oracle instance is the application's data layer that uses Oracle-specific PL/SQL functions. Traffic to the application has been steadily increasing. This is causing the EC2 instances to become overloaded and the RDS instance to run out of storage. The Auto Scaling group does not have any scaling metrics and defines the minimum healthy instance count only. The company predicts that traffic will continue to increase at a steady but unpredictable rate before levelling off. What should a solutions architect do to ensure the system can automatically scale for the increased traffic? (Select TWO.)

A. Configure storage Auto Scaling on the RDS for Oracle Instance.
B. Migrate the database to Amazon Aurora to use Auto Scaling storage.
C. Configure an alarm on the RDS for Oracle Instance for low free storage space
D. Configure the Auto Scaling group to use the average CPU as the scaling metric
E. Configure the Auto Scaling group to use the average free memory as the seeing metric

Correct Answer: A, D
Section:
Explanation:
Auto scaling storage RDS will ease storage issues and migrating Oracle Pl/Sql to Aurora is cumbersome. Also Aurora has auto storage scaling by default.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PIOPS.StorageTypes.html#USER_PI OPS.Autoscaling

QUESTION 136
A company has an AWS Lambda function that needs read access to an Amazon S3 bucket that is located in the same AWS account. Which solution will meet these requirement in the MOST secure manner?

A. Apply an S3 bucket pokey that grants road access to the S3 bucket
B. Apply an IAM role to the Lambda function Apply an IAM policy to the role to grant read access to the S3 bucket
C. Embed an access key and a secret key In the Lambda function's coda to grant the required IAM permissions for read access to the S3 bucket
D. Apply an IAM role to the Lambda function. Apply an IAM policy to the role to grant read access to all S3 buckets In the account

Correct Answer: B
Section:

QUESTION 137
A company wants to implement a disaster recovery plan for its primary on-premises file storage volume. The file storage volume is mounted from an Internet Small Computer Systems Interface (iSCSI) device on a local storage server. The file storage volume holds hundreds of terabytes (TB) of data.
The company wants to ensure that end users retain immediate access to all file types from the onpremises systems without experiencing latency. Which solution will meet these requirements with the LEAST amount of change to the company's existing infrastructure?

A. Provision an Amazon S3 File Gateway as a virtual machine (VM) that is hosted on premises. Set the local cache to 10 TB. Modify existing applications to access the files through the NFS protocol. To recover from a disaster, provision an Amazon EC2 instance and mount the S3 bucket that contains the files.
B. Provision an AWS Storage Gateway tape gateway. Use a data backup solution to back up all existing data to a virtual tape library. Configure the data backup solution to run nightly after the initial backup is complete. To recover from a disaster, provision an Amazon EC2 instance and restore the data to an Amazon Elastic Block Store (Amazon EBS) volume from the volumes in the virtual tape library.
C. Provision an AWS Storage Gateway Volume Gateway cached volume. Set the local cache to 10 TB.
Mount the Volume Gateway cached volume to the existing file server by using iSCSI. and copy all files to the storage volume. Configure scheduled snapshots of the storage volume. To recover from a disaster, restore a

snapshot to an Amazon Elastic Block Store (Amazon EBS) volume and attach the EBS volume to an Amazon EC2 instance.

D. Provision an AWS Storage Gateway Volume Gateway stored volume with the same amount of disk space as the existing file storage volume. Mount the Volume Gateway stored volume to the existing file server by using iSCSI, and copy all files to the storage volume. Configure scheduled snapshots of the storage volume. To recover from a disaster, restore a snapshot to an Amazon Elastic Block Store (Amazon EBS) volume and attach the EBS volume to an Amazon EC2 instance.

Correct Answer: D
Section:
Explanation:

QUESTION 138
A company is launching a new application deployed on an Amazon Elastic Container Service (Amazon ECS) cluster and is using the Fargate launch type tor ECS tasks The company is monitoring CPU and memory usage because it is expecting high traffic to the application upon its launch However the company wants to reduce costs when utilization decreases What should a solutions architect recommend?

A. Use Amazon EC2 Auto Scaling to scale at certain periods based on previous traffic patterns
B. Use an AWS Lambda function to scale Amazon ECS based on metric breaches that trigger an Amazon CloudWatch alarm
C. Use Amazon EC2 Auto Scaling with simple scaling policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm
D. Use AWS Application Auto Scaling with target tracking policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm

Correct Answer: D
Section:
Explanation:
https://docs.aws.amazon.com/autoscaling/application/userguide/what-is-application-auto-scaling.html

QUESTION 139
A data analytics company wants to migrate its batch processing system to AWS. The company receives thousands of small data files periodically during the day through FTP. A on-premises batch job processes the data files overnight. However, the batch job takes hours to finish running.
The company wants the AWS solution to process incoming data files are possible with minimal changes to the FTP clients that send the files. The solution must delete the incoming data files the files have been processed successfully. Processing for each file needs to take 3-8 minutes.
Which solution will meet these requirements in the MOST operationally efficient way?

A. Use an Amazon EC2 instance that runs an FTP server to store incoming files as objects in Amazon S3 Glacier Flexible Retrieval. Configure a job queue in AWS Batch. Use Amazon EventBridge rules to invoke the job to process the objects nightly from S3 Glacier Flexible Retrieval. Delete the objects after the job has processed the objects.
B. Use an Amazon EC2 instance that runs an FTP server to store incoming files on an Amazon Elastic Block Store (Amazon EBS) volume. Configure a job queue in AWS Batch. Use Amazon EventBridge rules to invoke the process the files nightly from the EBS volume. Delete the files after the job has processed the files.
C. Use AWS Transfer Family to create an FTP server to store incoming files on an Amazon Elastic Block Store (Amazon EBS) volume. Configure a job queue in AWS Batch. Use an Amazon S3 event notification when each files arrives to invoke the job in AWS Batch. Delete the files after the job has processed the files.
D. Use AWS Transfer Family to create an FTP server to store incoming files in Amazon S3 Standard.
Create an AWS Lambda function to process the files and to delete the files after they are proessed.yse an S3 event notification to invoke the lambda function when the fils arrive

Correct Answer: D
Section:
Explanation:
This option is the most operationally efficient because it uses AWS Transfer Family to create an FTP server that can store incoming files in Amazon S3 Standard12, which is a low-cost and highly available storage service. It also uses AWS Lambda to process the files and delete them after they are processed, which is a serverless and scalable solution that does not require any batch scheduling or infrastructure management. It also uses S3 event notifications to invoke the Lambda function when the files arrive, which enables near real-time processing of the incoming data files3. Option A is less efficient because it uses Amazon S3 Glacier Flexible Retrieval, which is a cold storage class that has higher retrieval costs and longer retrieval times than Amazon S3 Standard. It also uses EventBridge rules to invoke the job nightly, which does not meet the requirement of processing incoming data files as soon as possible. Option B is less efficient because it uses an EBS volume to store incoming files, which is a block storage service that has higher costs and lower durability than Amazon S3. It also uses EventBridge rules to invoke the job nightly, which does not meet the requirement of processing incoming data files as soon as possible. Option C is less efficient because it uses an EBS volume to store incoming files, which is a block storage service that has higher costs and lower durability than Amazon S3. It also uses AWS Batch to process the files, which requires managing compute resources and job queues.

QUESTION 140
A company hosts a three-tier web application that includes a PostgreSQL database The database stores the metadata from documents The company searches the metadata for key terms to retrieve documents that the company reviews in a report each month The documents are stored in Amazon S3 The documents are usually written only once, but they are updated frequency The reporting process takes a few hours with the use of relational queries The reporting process must not affect any document modifications or the addition of new documents.
What are the MOST operationally efficient solutions that meet these requirements? (Select TWO)

A. Set up a new Amazon DocumentDB (with MongoDB compatibility) cluster that includes a read replica Scale the read replica to generate the reports.
B. Set up a new Amazon RDS for PostgreSQL Reserved Instance and an On-Demand read replica Scale the read replica to generate the reports
C. Set up a new Amazon Aurora PostgreSQL DB cluster that includes a Reserved Instance and an Aurora Replica issue queries to the Aurora Replica to generate the reports.
D. Set up a new Amazon RDS for PostgreSQL Multi-AZ Reserved Instance Configure the reporting module to query the secondary RDS node so that the reporting module does not affect the primary node
E. Set up a new Amazon DynamoDB table to store the documents Use a fixed write capacity to support new document entries Automatically scale the read capacity to support the reports

Correct Answer: B, C
Section:

QUESTION 141
At part of budget planning. management wants a report of AWS billed dams listed by user. The data will be used to create department budgets. A solution architect needs to determine the most efficient way to obtain this report Information Which solution meets these requirement?

A. Run a query with Amazon Athena to generate the report.
B. Create a report in Cost Explorer and download the report
C. Access the bill details from the runing dashboard and download Via bill.
D. Modify a cost budget in AWS Budgets to alert with Amazon Simple Email Service (Amazon SES).

Correct Answer: B
Section:

QUESTION 142
A company needs to provide its employee with secure access to confidential and sensitive files. The company wants to ensure that the files can be accessed only by authorized users. The files must be downloaded security to the employees devices.
The files are stored in an on-premises Windows files server. However, due to an increase in remote usage, the file server out of capacity. Which solution will meet these requirement?

A. Migrate the file server to an Amazon EC2 instance in a public subnet. Configure the security group to limit inbound traffic to the employees ,IP addresses.
B. Migrate the files to an Amazon FSx for Windows File Server file system. Integrate the Amazon FSx file system with the on-premises Active Directory Configure AWS Client VPN.
C. Migrate the files to Amazon S3, and create a private VPC endpoint. Create a signed URL to allow download.
D. Migrate the files to Amazon S3, and create a public VPC endpoint Allow employees to sign on with AWS IAM identity Center (AWS Sing-On).

Correct Answer: B
Section:
Explanation:
Windows file server is on-premise and we need something to replicate the data to the cloud, the only option we have is AWS FSx for Windows File Server. Also, since the information is confidential and

QUESTION 143
A company is using AWS to design a web application that will process insurance quotes Users will request quotes from the application Quotes must be separated by quote type, must be responded to within 24 hours, and must not get lost The solution must maximize operational efficiency and must minimize maintenance. Which solution meets these requirements?

A. Create multiple Amazon Kinesis data streams based on the quote type Configure the web application to send messages to the proper data stream Configure each backend group of application servers to use the Kinesis Client Library (KCL) to pool messages from its own data stream
B. Create an AWS Lambda function and an Amazon Simple Notification Service (Amazon SNS) topic for each quote type Subscribe the Lambda function to its associated SNS topic Configure the application to publish requests tot quotes to the appropriate SNS topic
C. Create a single Amazon Simple Notification Service (Amazon SNS) topic Subscribe Amazon Simple Queue Service (Amazon SQS) queues to the SNS topic Configure SNS message filtering to publish messages to the proper SQS queue based on the quote type Configure each backend application server to use its own SQS queue
D. Create multiple Amazon Kinesis Data Firehose delivery streams based on the quote type to deliver data streams to an Amazon Elasucsearch Service (Amazon ES) cluster Configure the application to send messages to the proper delivery stream Configure each backend group of application servers to search for the messages from Amazon ES and process them accordingly

Correct Answer: C
Section:

QUESTION 144
A company hosts a multi-tier web application that uses an Amazon Aurora MySQL DB cluster for storage. The application tier is hosted on Amazon EC2 instances. The company's IT security guidelines mandate that the database credentials be encrypted and rotated every 14 days What should a solutions architect do to meet this requirement with the LEAST operational effort?

A. Create a new AWS Key Management Service (AWS KMS) encryption key Use AWS Secrets Manager to create a new secret that uses the KMS key with the appropriate credentials Associate the secret with the Aurora DB cluster Configure a custom rotation period of 14 days
B. Create two parameters in AWS Systems Manager Parameter Store one for the user name as a string parameter and one that uses the SecureStnng type for the password Select AWS Key Management Service (AWS KMS) encryption for the password parameter, and load these parameters in the application tier Implement an AWS Lambda function that rotates the password every 14 days.
C. Store a file that contains the credentials in an AWS Key Management Service (AWS KMS) encrypted Amazon Elastic File System (Amazon EFS) file system Mount the EFS file system in all EC2 instances of the application tier. Restrict the access to the file on the file system so that the application can read the file and that only super users can modify the file Implement an AWS Lambda function that rotates the key in Aurora every 14 days and writes new credentials into the file
D. Store a file that contains the credentials in an AWS Key Management Service (AWS KMS) encrypted Amazon S3 bucket that the application uses to load the credentials Download the file to the application regularly to ensure that the correct credentials are used Implement an AWS Lambda function that rotates the Aurora credentials every 14 days and uploads these credentials to the file in the S3 bucket

Correct Answer: A
Section:

QUESTION 145
A company is running a critical business application on Amazon EC2 instances behind an Application Load Balancer The EC2 instances run in an Auto Scaling group and access an Amazon RDS DB instance The design did not pass an operational review because the EC2 instances and the DB instance are all located in a single Availability Zone A solutions architect must update the design to use a second Availability Zone Which solution will make the application highly available?

A. Provision a subnet in each Availability Zone Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones Configure the DB instance with connections to each network
B. Provision two subnets that extend across both Availability Zones Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones Configure the DB instance with connections to each network
C. Provision a subnet in each Availability Zone Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones Configure the DB instance for Multi-AZ deployment
D. Provision a subnet that extends across both Availability Zones Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones Configure the DB instance for Multi-AZ deployment

Correct Answer: C
Section:

QUESTION 146
An application that is hosted on Amazon EC2 instances needs to access an Amazon S3 bucket Traffic must not traverse the internet How should a solutions architect configure access to meet these requirements?

A. Create a private hosted zone by using Amazon Route 53
B. Set up a gateway VPC endpoint for Amazon S3 in the VPC
C. Configure the EC2 instances to use a NAT gateway to access the S3 bucket

D. Establish an AWS Site-to-Site VPN connection between the VPC and the S3 bucket

Correct Answer: B
Section:

QUESTION 147
A company has deployed a web application on AWS. The company hosts the backend database on Amazon RDS for MySQL with a primary DB instance and five read replicas to support scallng needs. The read replicas must lag no more than 1 second behind the primary DB instance. The database routinely runs scheduled stored procedures. As traffic on the website increases, the replicas experince addtional lag during periods of peak load. A solutions architect must reduce the replication lag as much as possible. The solutin architect must minimize changes to the application code and must minimize ongoing operational overhead. Which solution will meet these requirements?

A. Migrate the database to Amazon Aurora MySQL. Replace the read replicas with Aurora Replicas, and configure Aurora Auto Scaling. Replace the store procedures with Aurora MySQL native functions.
B. Deploy an Amazon ElasticCache for Redis cluster in front of the database. Modify the application to check the cache before the applicatin queries the database. Replace the stored procedures with AWS Lambda functions.
C. Migrate the database to a MySQL database that runs on Amazon EC2 instances. Choose large, compute optimized EC2 instances for all replica nodes. Maintain the stored procedures on the EC2 instances.
D. Migrate the database to Amazon DynamicDB provision a large number of read capacity units(RCUs) to support the required throught, and configure on-demand capacity scaling. Replace the store procedures with DynamoDB streams

Correct Answer: A
Section:

QUESTION 148
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

Correct Answer: C
Section:
Explanation:
This option will scale up capacity faster in the morning to improve performance, but will still allow capacity to scale down during off hours. It achieves this as follows: * A target tracking action scales based on a CPU utilization target. By triggering at a lower CPU threshold in the morning, the Auto Scaling group will start scaling up sooner as traffic ramps up, launching instances before utilization gets too high and impacts performance. * Decreasing the cooldown period allows Auto Scaling to scale more aggressively, launching more instances faster until the target is reached. This speeds up the ramp-up of capacity. * However, unlike a scheduled action to set a fixed minimum/maximum capacity, with target tracking the group can still scale down during off hours based on demand. This helps minimize costs.

QUESTION 149
A company is hosting a web application from an Amazon S3 bucket. The application uses Amazon Cognito as an identity provider lo authenticate users and return a JSON Web Token (JWT) that provides access to protected resources that am restored in another S3 bucket.
Upon deployment of the application, users report errors and are unable to access the protected content. A solutions architect must resolve this issue by providing proper permissions so that users can access the protected content. Which solution meets these requirements?

A. Update the Amazon Cognito identity pool to assume the proper IAM role for access to the protected consent.
B. Update the S3 ACL to allow the application to access the protected content
C. Redeploy the application to Amazon 33 to prevent eventually consistent reads m the S3 bucket from affecting the ability of users to access the protected content.
D. Update the Amazon Cognito pool to use custom attribute mappings within tie Identity pool and grant users the proper permissions to access the protected content

Correct Answer: A
Section:
Explanation:

QUESTION 150
A company needs to migrate a legacy application from an on-premises data center to the AWS Cloud because of hardware capacity constraints. The application runs 24 hours a day. & days a week,. The application database storage continues to grow over time.
What should a solution architect do to meet these requirements MOST cost-affectivity?

A. Migrate the application layer to Amazon FC2 Spot Instances Migrate the data storage layer to Amazon S3.
B. Migrate the application layer to Amazon EC2 Reserved Instances Migrate the data storage layer to Amazon RDS On-Demand Instances.
C. Migrate the application layer to Amazon EC2 Reserved instances Migrate the data storage layer to Amazon Aurora Reserved Instances.
D. Migrate the application layer to Amazon EC2 On Demand Amazon Migrate the data storage layer to Amazon RDS Reserved instances.

Correct Answer: C
Section:

QUESTION 151
A company is using a fleet of Amazon EC2 instances to ingest data from on-premises data sources.
The data is in JSON format and Ingestion rates can be as high as 1 MB/s. When an EC2 instance is rebooted, the data in-flight is lost. The company's data science team wants to query Ingested data In near-real time. Which solution provides near-real -time data querying that is scalable with minimal data loss?

A. Publish data to Amazon Kinesis Data Streams Use Kinesis data Analytics to query the data.
B. Publish data to Amazon Kinesis Data Firehose with Amazon Redshift as the destination Use Amazon Redshift to query the data
C. Store ingested data m an EC2 Instance store Publish data to Amazon Kinesis Data Firehose with Amazon S3 as the destination. Use Amazon Athena to query the data.
D. Store ingested data m an Amazon Elastic Block Store (Amazon EBS) volume Publish data to Amazon ElastiCache tor Red Subscribe to the Redis channel to query the data

Correct Answer: A
Section:
Explanation:

QUESTION 152
A company recently migrated its entire IT environment to the AWS Cloud. The company discovers that users are provisioning oversized Amazon EC2 instances and modifying security group rules without using the appropriate change control process A solutions architect must devise a strategy to track and audit these inventory and configuration changes. Which actions should the solutions architect take to meet these requirements? (Select TWO)

A. Enable AWS CloudTrail and use it for auditing
B. Use data lifecycie policies for the Amazon EC2 instances
C. Enable AWS Trusted Advisor and reference the security dashboard
D. Enable AWS Config and create rules for auditing and compliance purposes
E. Restore previous resource configurations with an AWS CloudFormation template

Correct Answer: A, D
Section:
Explanation:
A) Enable AWS CloudTrail and use it for auditing. AWS CloudTrail provides a record of API calls and can be used to audit changes made to EC2 instances and security groups. By analyzing CloudTrail logs, the solutions architect can track who provisioned oversized instances or modified security groups without proper approval. D) Enable AWS Config and create rules for auditing and compliance purposes. AWS Config can record the configuration changes made to resources like EC2 instances and security groups. The solutions architect can create AWS Config rules to monitor for non-compliant changes, like launching certain instance types or opening security group ports without permission. AWS Config would alert on any

violations of these rules.

QUESTION 153
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 calcualtion bath runs. This causes the CPU utilization of the EC2 instaces to immediately peak to 100%, which disrupts the application. What should a solution architect recommend to ensure the application is able to handle the workload and avoid downtime?

A. Configure an Amazon CloudFront distribution in from 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 ElasticCache to remove some of the workload from tha EC2 instances.

Correct Answer: C
Section:
Explanation:
Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule is the best option because it allows for the proactive scaling of the EC2 instances before the monthly batch run begins. This will ensure that the application is able to handle the increased workload without experiencing downtime. The scheduled scaling policy can be configured to increase the number of instances in the Auto Scaling group a few hours before the batch run and then decrease the number of instances after the batch run is complete. This will ensure that the resources are available when needed and not wasted when not needed. The most appropriate solution to handle the increased workload during the monthly batch run and avoid downtime would be to configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule. https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-scheduled-scaling.html
s

QUESTION 154
A company stores its data objects in Amazon S3 Standard storage. A solutions architect has found that 75% of the data is rarely accessed after 30 days. The company needs all the data to remain immediately accessible with the same high availability and resiliency, but the company wants to minimize storage costs.
Which storage solution will meet these requirements?

A. Move the data objects to S3 Glacier Deep Archive after 30 days.
B. Move the data objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
C. Move the data objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.
D. Move the data objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) immediately.

Correct Answer: B
Section:

QUESTION 155
A solutions architect must secure a VPC network that hosts Amazon EC2 instances The EC2 ^stances contain highly sensitive data and tun n a private subnet According to company policy the EC2 instances mat run m the VPC can access only approved third-party software repositories on the internet for software product updates that use the third party's URL Other internet traffic must be blocked. Which solution meets these requirements?

A. Update the route table for the private subnet to route the outbound traffic to an AWS Network Firewall. Configure domain list rule groups
B. Set up an AWS WAF web ACL. Create a custom set of rules that filter traffic requests based on source and destination IP address range sets.
C. Implement strict inbound security group roles Configure an outbound rule that allows traffic only to the authorized software repositories on the internet by specifying the URLs
D. Configure an Application Load Balancer (ALB) in front of the EC2 instances. Direct an outbound traffic to the ALB Use a URL-based rule listener in the ALB's target group for outbound access to the internet

Correct Answer: A
Section:
Explanation:
Send the outbound connection from EC2 to Network Firewall. In Network Firewall, createstateful outbound rules to allow certain domains for software patch download and deny allother domains. https://docs.aws.amazon.com/network-firewall/latest/developerguide/suricata-examples.html#suricata-example-domain-filtering

QUESTION 156
A company has hundreds of Amazon EC2 Linux-based instances in the AWS Cloud. Systems administrators have used shared SSH keys to manage the instances After a recent audit, the company's security team is mandating the removal of all shared keys. A solutions architect must design a solution that provides secure access to the EC2 instances. Which solution will meet this requirement with the LEAST amount of administrative overhead?

A. Use AWS Systems Manager Session Manager to connect to the EC2 instances.
B. Use AWS Security Token Service (AWS STS) to generate one-time SSH keys on demand.
C. Allow shared SSH access to a set of bastion instances. Configure all other instances to allow only SSH access from the bastion instances
D. Use an Amazon Cognito custom authorizer to authenticate users. Invoke an AWS Lambda function to generate a temporary SSH key.

Correct Answer: A
Section:
Explanation:
Session Manager is a fully managed AWS Systems Manager capability. With Session Manager, you can manage your Amazon Elastic Compute Cloud (Amazon EC2) instances, edge devices, on-premises servers, and virtual machines (VMs). You can use either an interactive one-click browser-based shell or the AWS Command Line Interface (AWS CLI). Session Manager provides secure and auditable node management without the need to open inbound ports, maintain bastion hosts, or manage SSH keys. Session Manager also allows you to comply with corporate policies that require controlled access to managed nodes, strict security practices, and fully auditable logs with node access details, while providing end users with simple one-click cross-platform access to your managed nodes. https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html

QUESTION 157
A company is building a data analysis platform on AWS by using AWS Lake Formation. The platform will ingest data from different sources such as Amazon S3 and Amazon RDS. The company needs a secure solution to prevent access to portions of the data that contain sensitive information.

A. Create an IAM role that includes permissions to access Lake Formation tables.
B. Create data filters to implement row-level security and cell-level security.
C. Create an AWS Lambda function that removes sensitive information before Lake Formation ingests re data.
D. Create an AWS Lambda function that perodically Queries and removes sensitive information from Lake Formation tables.

Correct Answer: B
Section:
Explanation:

QUESTION 158
A company wants to create an application to store employee data in a hierarchical structured relationship. The company needs a minimum-latency response to high-traffic queries for the employee data and must protect any sensitive dat a. The company also need to receive monthly email messages if any financial information is present in the employee data. Which combination of steps should a solutin architect take to meet these requirement? (Select TWO.)

A. Use Amazon Redshift to store the employee data in hierarchies. Unload the data to Amazon S3 every month.
B. Use Amazon DynamoDB to store the employee data in hierarchies Export the data to Amazon S3 every month.
C. Configure Amazon Macie for the AWS account Integrate Macie with Amazon EventBridge to send monthly events to AWS Lambda.
D. Use Amazon Athena to analyze the employee data in Amazon S3 integrate Athena with Amazon QuickSight to publish analysis dashboards and share the dashboards with users.
E. Configure Amazon Macie for the AWS account. integrate Macie with Amazon EventBridge to send monthly notifications through an Amazon Simple Notification Service (Amazon SNS) subscription.

Correct Answer: B, E
Section:
Explanation:

QUESTION 159

A solutions architect is designing a multi-tier application for a company. The application's users upload images from a mobile device. The application generates a thumbnail of each image and returns a message to the user to confirm that the image was uploaded successfully.
The thumbnail generation can take up to 60 seconds, but the company wants to provide a faster response time to its users to notify them that the original image was received. The solutions architect must design the application to asynchronously dispatch requests to the different application tiers.
What should the solutions architect do to meet these requirements?

A. Write a custom AWS Lambda function to generate the thumbnail and alert the user. Use the image upload process as an event source to invoke the Lambda function.
B. Create an AWS Step Functions workflow Configure Step Functions to handle the orchestration between the application tiers and alert the user when thumbnail generation is complete
C. Create an Amazon Simple Queue Service (Amazon SQS) message queue. As images are uploaded, place a message on the SQS queue for thumbnail generation. Alert the user through an application message that the image was received
D. Create Amazon Simple Notification Service (Amazon SNS) notification topics and subscriptions Use one subscription with the application to generate the thumbnail after the image upload is complete. Use a second subscription to message the user's mobile app by way of a push notification after thumbnail generation is complete.

Correct Answer: C
Section:
Explanation:
This option is the most efficient because it uses Amazon SQS, which is a fully managed message queuing service that lets you send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available1. It also uses an SQS message queue to asynchronously dispatch requests to the different application tiers, which decouples the image upload process from the thumbnail generation process and enables scalability and reliability. It also alerts the user through an application message that the image was received, which provides a faster response time to the user than waiting for the thumbnail generation to complete. Option A is less efficient because it uses a custom AWS Lambda function to generate the thumbnail and alert the user, which is a way to run code without provisioning or managing servers. However, this does not use an asynchronous dispatch mechanism to separate the image upload process from the thumbnail generation process. It also uses the image upload process as an event source to invoke the Lambda function, which could cause concurrency issues if there are many images uploaded at once. Option B is less efficient because it uses AWS Step Functions, which is a fully managed service that provides a graphical console to arrange and visualize the components of your application as a series of steps2. However, this does not use an asynchronous dispatch mechanism to separate the image upload process from the thumbnail generation process. It also uses Step Functions to handle the orchestration between the application tiers and alert the user when thumbnail generation is complete, which could introduce additional complexity and latency. Option D is less efficient because it uses Amazon SNS, which is a fully managed messaging service that enables you to send messages or notifications directly to users with SMS text messages or email3. However, this does not use an asynchronous dispatch mechanism to separate the image upload process from the thumbnail generation process. It also uses SNS notification topics and subscriptions to generate the thumbnail after the image upload is complete and message the user's mobile app by way of a push notification after thumbnail generation is complete, which could introduce additional complexity and latency.

QUESTION 160
A company uses a 100 GB Amazon RDS for Microsoft SQL Server Single-AZ DB instance in the us-east- 1 Region to store customer transactions. The company needs high availability and automate recovery for the DB instance. The companu must also run reports on the RDS database several times a year. The report process causes transactions to take longer than usual to post to the customer‘ accounts. Which combination of steps will meet these requirements? (Select TWO.)

A. Modify the DB instance from a Single-AZ DB instance to a Multi-AZ deployment.
B. Take a snapshot of the current DB instance. Restore the snapshot to a new RDS deployment in another Availability Zone.
C. Create a read replica of the DB instance in a different Availability Zone. Point All requests for reports to the read replica.
D. Migrate the database to RDS Custom.
E. Use RDS Proxy to limit reporting requests to the maintenance window.

Correct Answer: A, C
Section:
Explanation:
https://medium.com/awesome-cloud/aws-difference-between-multi-az-and-read-replicas-in- amazon-rds-60fe848ef53a

QUESTION 161
A solution architect needs to assign a new microsoft for a company’s application. Clients must be able to call an HTTPS endpoint to reach the micoservice. The microservice also must use AWS identity and Access Management (IAM) to authentication calls. The soltions architect will write the logic for this microservice by using a single AWS Lambda function that is written in Go 1.x. Which solution will deploy the function in the in the MOST operationally efficient way?

A. Create an Amazon API Gateway REST API. Configure the method to use the Lambda function. Enable IAM authentication on the API.
B. Create a Lambda function URL for the function. Specify AWS_IAM as the authentication type.
C. Create an Amazon CloudFront distribution. Deploy the function to Lambda@Edge. Integrate IAM authentication logic into the Lambda@Edge function.
D. Create an Amazon CloudFront distribuion. Deploy the function to CloudFront Functions. Specify AWS_IAM as the authentication type.

Correct Answer: A
Section:

QUESTION 162
A company is using Amazon CloudFront with lis website. The company has enabled logging on the CloudFront distribution, and togs are saved in one of the company's Amazon S3 buckets The company needs to perform advanced analyses on the logs and build visualizations What should a solutions architect do to meet these requirements'?

A. Use standard SQL queries in Amazon Athena to analyze the CloudFront togs in the S3 bucket Vrsualize the results with AWS Glue
B. Use standard SQL queries in Amazon Athena to analyze the CloudFront togs in the S3 bucket Visualize the results with Amazon QuickSight
C. Use standard SQL queries in Amazon DynamoDB to analyze the CloudFront logs m the S3 bucket Visualize the results with AWS Glue
D. Use standard SQL queries in Amazon DynamoOB to analyze the CtoudFront logs m the S3 bucket Visualize the results with Amazon QuickSight

Correct Answer: B
Section:
Explanation:
https://docs.aws.amazon.com/quicksight/latest/user/welcome.html Using Athena to query the CloudFront logs in the S3 bucket and QuickSight to visualize the results is the best solution because it is cost-effective, scalable, and requires no infrastructure setup. It also provides a robust solution that enables the company to perform advanced analysis and build interactive visualizations without the need for a dedicated team of developers.

QUESTION 163
A company provides an online service for posting video content and transcoding it for use by any mobile platform. The application architecture uses Amazon Elastic File System (Amazon EFS) Standard to collect and store the videos so that multiple Amazon EC2 Linux instances can access the video content for processing As the popularity of the service has grown over time, the storage costs have become too expensive. Which storage solution is MOST cost-effective?

A. Use AWS Storage Gateway for files to store and process the video content
B. Use AWS Storage Gateway for volumes to store and process the video content
C. Use Amazon EFS for storing the video content Once processing is complete transfer the files to Amazon Elastic Block Store (Amazon EBS)
D. Use Amazon S3 for storing the video content Move the files temporarily over to an Amazon Elastic Block Store (Amazon EBS) volume attached to the server for processing

Correct Answer: D
Section:

QUESTION 164
A company runs a fleet of web servers using an Amazon RDS for PostgreSQL DB instance After a routine compliance check, the company sets a standard that requires a recovery pant objective (RPO) of less than 1 second for all its production databases.
Which solution meets these requirement?

A. Enable a Multi-AZ deployment for the DB Instance
B. Enable auto scaling for the OB instance m one Availability Zone.
C. Configure the 06 instance in one Availability Zone and create multiple read replicas in a separate Availability Zone
D. Configure the 06 instance m one Availability Zone, and configure AWS Database Migration Service (AWS DMS) change data capture (CDC) tasks

Correct Answer: A
Section:

QUESTION 165
A company's facility has badge readers at every entrance throughout the building. When badges are scanned, the readers send a message over HTTPS to indicate who attempted to access that particular entrance. A solutions architect must design a system to process these messages from the sensors. The solution must be highly available, and the results must be made available for the company's security team to analyze. Which system architecture should the solutions architect recommend?

A. Launch an Amazon EC2 instance to serve as the HTTPS endpoint and to process the messagesConfigure the EC2 instance to save the results to an Amazon S3 bucket.
B. Create an HTTPS endpoint in Amazon API Gateway. Configure the API Gateway endpoint to invokean AWS Lambda function to process the messages and save the results to an Amazon DynamoDBtable.
C. Use Amazon Route 53 to direct incoming sensor messages to an AWS Lambda function. Configure the Lambda function to process the messages and save the results to an Amazon DynamoDB table.
D. Create a gateway VPC endpoint for Amazon S3. Configure a Site-to-Site VPN connection from the facility network to the VPC so that sensor data can be written directly to an S3 bucket by way of the VPC endpoint.

Correct Answer: B
Section:

QUESTION 166
A company is designing a shared storage solution for a gaming application that is hosted in the AWS Cloud The company needs the ability to use SMB clients to access data solution must be fully managed. Which AWS solution meets these requirements?

A. Create an AWS DataSync task that shares the data as a mountable file system Mount the file system to the application server
B. Create an Amazon EC2 Windows instance Install and configure a Windows file share role on the instance Connect the application server to the file share
C. Create an Amazon FSx for Windows File Server file system Attach the file system to the origin server Connect the application server to the file system
D. Create an Amazon S3 bucket Assign an IAM role to the application to grant access to the S3 bucket Mount the S3 bucket to the application server

Correct Answer: C
Section:
Explanation:
Amazon FSx for Windows File Server (Amazon FSx) is a fully managed, highly available, and scalable file storage solution built on Windows Server that uses the Server Message Block (SMB) protocol. It allows for Microsoft Active Directory integration, data deduplication, and fully managed backups,among other critical enterprise features. https://aws.amazon.com/blogs/storage/accessing-smb-file- shares-remotely-with-amazon-fsx-for-windows-file-server

QUESTION 167
A company is migrating a Linux-based web server group to AWS. The web servers must access files in a shared file store for some content. The company must not make any changes to the application. What should a solutions architect do to meet these requirements?

A. Create an Amazon S3 Standard bucket with access to the web servers.
B. Configure an Amazon CloudFront distribution with an Amazon S3 bucket as the origin.
C. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system on all web servers.
D. Configure a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume to all web servers.

Correct Answer: C
Section:

QUESTION 168
A company wants to run an in-memory database for a latency-sensitive application that runs on Amazon EC2 instances. The application processes more than 100,000 transactions each minute and requires high network throughput. A solutions architect needs to provide a cost-effective network design that minimizes data transfer charges. Which solution meets these requirements?

A. Launch all EC2 instances in the same Availability Zone within the same AWS Region. Specify a placement group with cluster strategy when launching EC2 instances.
B. Launch all EC2 instances in different Availability Zones within the same AWS Region. Specify a placement group with partition strategy when launching EC2 instances.
C. Deploy an Auto Scaling group to launch EC2 instances in different Availability Zones based on a network utilization target.
D. Deploy an Auto Scaling group with a step scaling policy to launch EC2 instances in different Availability Zones.

Correct Answer: A
Section:

QUESTION 169
A company has a custom application with embedded credentials that retrieves information from an Amazon RDS MySQL DB instance. Management says the application must be made more secure with the least amount of programming effort.
What should a solutions architect do to meet these requirements?

A. Use AWS Key Management Service (AWS KMS) customer master keys (CMKs) to create keys.
Configure the application to load the database credentials from AWS KMS. Enable automatic key rotation.
B. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Create an AWS Lambda function that rotates the credentials in Secret Manager.
C. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager.
D. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Systems Manager Parameter Store. Configure the application to load the database credentials from Parameter Store. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Parameter Store.

Correct Answer: C
Section:
Explanation:

QUESTION 170
A company is planning to store data on Amazon RDS DB instances. The company must encrypt the data at rest. What should a solutions architect do to meet this requirement?

A. Create an encryption key and store the key in AWS Secrets Manager Use the key to encrypt the DB instances
B. Generate a certificate in AWS Certificate Manager (ACM). Enable SSL/TLS on the DB instances by using the certificate
C. Create a customer master key (CMK) in AWS Key Management Service (AWS KMS) Enable encryption for the DB instances
D. Generate a certificate in AWS Identity and Access Management {IAM) Enable SSUTLS on the DB instances by using the certificate

Correct Answer: A
Section:
Explanation:
To encrypt data at rest in Amazon RDS, you can use the encryption feature of Amazon RDS, which uses AWS Key Management Service (AWS KMS). With this feature, Amazon RDS encrypts each database instance with a unique key. This key is stored securely by AWS KMS. You can manage your own keys or use the default AWS-managed keys. When you enable encryption for a DB instance, Amazon RDS encrypts the underlying storage, including the automated backups, read replicas, and snapshots.

QUESTION 171
A payment processing company records all voice communication with its customers and stores the audio files in an Amazon S3 bucket. The company needs to capture the text from the audio files. The company must remove from the text any personally identifiable information (Pll) that belongs to customers.
What should a solutions architect do to meet these requirements?

A. Process the audio files by using Amazon Kinesis Video Streams. Use an AWS Lambda function to scan for known Pll patterns.

B. When an audio file is uploaded to the S3 bucket, invoke an AWS Lambda function to start an Amazon Textract task to analyze the call recordings.
C. Configure an Amazon Transcribe transcription job with Pll redaction turned on. When an audio file is uploaded to the S3 bucket, invoke an AWS Lambda function to start the transcription job. Store the output in a separate S3 bucket.
D. Create an Amazon Connect contact flow that ingests the audio files with transcription turned on. Embed an AWS Lambda function to scan for known Pll patterns. Use Amazon EventBridge (Amazon CloudWatch Events) to start the contact flow when an audio file is uploaded to the S3 bucket.

Correct Answer: C
Section:

QUESTION 172
An ecommerce company is running a multi-tier application on AWS. The front-end and backend tiers run on Amazon EC2, and the database runs on Amazon RDS for MYSQL. The backend tier communities with the RDS instance. There are frequent calls to return identical database from the database that are causing performance slowdowns. Which action should be taken to improve the performance of the backend?

A. Implement Amazon SNS to store the database calls.
B. Implement Amazon ElasticCache to cache the large database.
C. Implement an RDS for MySQL read replica to cache database calls.
D. Implement Amazon Kinesis Data Firehose to stream the calls to the database.

Correct Answer: B
Section:

QUESTION 173
A hospital is designing a new application that gathers symptoms from patients. The hospital has decided to use Amazon Simple Queue Service (Amazon SOS) and Amazon Simple Notification Service (Amazon SNS) in the architecture. A solutions architect is reviewing the infrastructure design Data must be encrypted at test and in transit. Only authorized personnel of the hospital should be able to access the data. Which combination of steps should the solutions architect take to meet these requirements? (Select TWO.)

A. Turn on server-side encryption on the SQS components Update tie default key policy to restrict key usage to a set of authorized principals.
B. Turn on server-side encryption on the SNS components by using an AWS Key Management Service (AWS KMS) customer managed key Apply a key policy to restrict key usage to a set of authorized principals.
C. Turn on encryption on the SNS components Update the default key policy to restrict key usage to a set of authorized principals. Set a condition in the topic pokey to allow only encrypted connections over TLS.
D. Turn on server-side encryption on the SOS components by using an AWS Key Management Service (AWS KMS) customer managed key Apply a key pokey to restrict key usage to a set of authorized principals. Set a condition in the queue pokey to allow only encrypted connections over TLS.
E. Turn on server-side encryption on the SOS components by using an AWS Key Management Service (AWS KMS) customer managed key. Apply an IAM pokey to restrict key usage to a set of authorized principals. Set a condition in the queue pokey to allow only encrypted connections over TLS

Correct Answer: B, D
Section:

QUESTION 174
A solutions architect is creating a new VPC design There are two public subnets for the load balancer, two private subnets for web servers and two private subnets for MySQL The web servers use only HTTPS The solutions architect has already created a security group tor the load balancer allowingport 443 from 0 0 0 0/0 Company policy requires that each resource has the teas! access required tostill be able to perform its tasksWhich additional configuration strategy should the solutions architect use to meet theserequirements?

A. Create a security group for the web servers and allow port 443 from 0.0.0.0/0 Create a security group for the MySQL servers and allow port 3306 from the web servers security group
B. Create a network ACL for the web servers and allow port 443 from 0.0.0.0/0 Create a network ACL (or the MySQL servers and allow port 3306 from the web servers security group
C. Create a security group for the web servers and allow port 443 from the load balancer Create a security group for the MySQL servers and allow port 3306 from the web servers security group
D. Create a network ACL 'or the web servers and allow port 443 from the load balancer Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group

Correct Answer: C
Section:

QUESTION 175
A company wants to use Amazon S3 for the secondary copy of its on-premises dataset. The company would rarely need to access this copy. The storage solution's cost should be minimal. Which storage solution meets these requirements?

A. S3 Standard
B. S3 Intelligent-Tiering
C. S3 Standard-Infrequent Access (S3 Standard-IA)
D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Correct Answer: D
Section:
Explanation:

QUESTION 176
A solutions architect is designing a two-tiered architecture that includes a public subnet and a database subnet. The web servers in the public subnet must be open to the internet on port 443. The Amazon RDS for MySQL D6 instance in the database subnet must be accessible only to the web servers on port 3306.
Which combination of steps should the solutions architect take to meet these requirements? (Select TWO.)

A. Create a network ACL for the public subnet Add a rule to deny outbound traffic to 0 0 0 0/0 on port 3306
B. Create a security group for the DB instance Add a rule to allow traffic from the public subnet CIDR block on port 3306
C. Create a security group for the web servers in the public subnet Add a rule to allow traffic from 0 0 0 O'O on port 443
D. Create a security group for the DB instance Add a rule to allow traffic from the web servers' security group on port 3306
E. Create a security group for the DB instance Add a rule to deny all traffic except traffic from the web servers' security group on port 3306

Correct Answer: B, C
Section:
Explanation:
Security groups are virtual firewalls that protect AWS instances and can be applied to EC2, ELB and RDS1. Security groups have rules for inbound and outbound traffic and are stateful, meaning that responses to allowed inbound traffic are allowed to flow out of the instance2. Network ACLs are different from security groups in several ways. They cover entire subnets, not individual instances, and are stateless, meaning that they require rules for both inbound and outbound traffic2. Network ACLs also support deny rules, while security groups only support allow rules2. To meet the requirements of the scenario, the solutions architect should create two security groups: one for the DB instance and one for the web servers in the public subnet. The security group for the DB instance should allow traffic from the public subnet CIDR block on port 3306, which is the default port for MySQL3. This way, only the web servers in the public subnet can access the DB instance on that port. The security group for the web servers should allow traffic from 0 0 0 O'O on port 443, which is the default port for HTTPS4. This way, the web servers can accept secure connections from the internet on that port.

QUESTION 177
A company has an Amazon S3 data lake that is governed by AWS Lake Formation The company wants to create a visualization in Amazon QuickSight by joining the data in the data lake with operational data that is stored in an Amazon Aurora MySQL database The company wants to enforce columnlevel authorization so that the company's marketing team can access only a subset of columns in the database Which solution will meet these requirements with the LEAST operational overhead?

A. Use Amazon EMR to ingest the data directly from the database to the QuickSight SPICE engine Include only the required columns
B. Use AWS Glue Studio to ingest the data from the database to the S3 data lake Attach an IAM policy to the QuickSight users to enforce column-level access control. Use Amazon S3 as the data source in QuickSight
C. Use AWS Glue Elastic Views to create a materialized view for the database in Amazon S3 Create an S3 bucket policy to enforce column-level access control for the QuickSight users Use Amazon S3 as the data source in QuickSight.
D. Use a Lake Formation blueprint to ingest the data from the database to the S3 data lake Use Lake Formation to enforce column-level access control for the QuickSight users Use Amazon Athena as the data source in

QuickSight

Correct Answer: D
Section:

QUESTION 178
A company has an application that collects data from loT sensors on automobiles. The data is streamed and stored in Amazon S3 through Amazon Kinesis Date Firehose The data produces trillions of S3 objects each year. Each morning, the company uses the data from the previous 30 days to retrain a suite of machine learning (ML) models. Four times each year, the company uses the data from the previous 12 months to perform analysis and train other ML models The data must be available with minimal delay for up to 1 year. After 1 year, the data must be retained for archival purposes.
Which storage solution meets these requirements MOST cost-effectively?

A. Use the S3 Intelligent-Tiering storage class. Create an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 1 year
B. Use the S3 Intelligent-Tiering storage class. Configure S3 Intelligent-Tiering to automatically move objects to S3 Glacier Deep Archive after 1 year.
C. Use the S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Create an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 1 year.
D. Use the S3 Standard storage class. Create an S3 Lifecycle policy to transition objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days, and then to S3 Glacier Deep Archive after 1 year.

Correct Answer: D
Section:

QUESTION 179
A company recently deployed a new auditing system to centralize information about operating system versions patching and installed software for Amazon EC2 instances. A solutions architect must ensure all instances provisioned through EC2 Auto Scaling groups successfully send reports to the auditing system as soon as they are launched and terminated Which solution achieves these goals MOST efficiently?

A. Use a scheduled AWS Lambda function and run a script remotely on all EC2 instances to send data to the audit system.
B. Use EC2 Auto Scaling lifecycle hooks to run a custom script to send data to the audit system when instances are launched and terminated
C. Use an EC2 Auto Scaling launch configuration to run a custom script through user data to send data to the audit system when instances are launched and terminated
D. Run a custom script on the instance operating system to send data to the audit system Configure the script to be invoked by the EC2 Auto Scaling group when the instance starts and is terminated

Correct Answer: B
Section:

QUESTION 180
A company has launched an Amazon RDS for MySQL D6 instance Most of the connections to the database come from serverless applications. Application traffic to the database changes significantly at random intervals At limes of high demand, users report that their applications experience database connection rejection errors.
Which solution will resolve this issue with the LEAST operational overhead?

A. Create a proxy in RDS Proxy Configure the users' applications to use the DB instance through RDS Proxy
B. Deploy Amazon ElastCache for Memcached between the users' application and the DB instance
C. Migrate the DB instance to a different instance class that has higher I/O capacity. Configure the users' applications to use the new DB instance.
D. Configure Multi-AZ for the DB instance Configure the users' application to switch between the DB instances.

Correct Answer: A
Section:

QUESTION 181
A solutions architect is designing the architecture for a software demonstration environment The environment will run on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB) The system will experience significant increases in traffic during working hours but Is not required to operate on weekends. Which combination of actions should the solutions architect take to ensure that the system can scale to meet demand? (Select TWO)

A. Use AWS Auto Scaling to adjust the ALB capacity based on request rate
B. Use AWS Auto Scaling to scale the capacity of the VPC internet gateway
C. Launch the EC2 instances in multiple AWS Regions to distribute the load across Regions
D. Use a target tracking scaling policy to scale the Auto Scaling group based on instance CPU utilization
E. Use scheduled scaling to change the Auto Scaling group minimum, maximum, and desired capacity to zero for weekends Revert to the default values at the start of the week

Correct Answer: D, E
Section:

QUESTION 182
A company has deployed a server less application that invokes an AWS Lambda function when new documents are uploaded to an Amazon S3 bucket The application uses the Lambda function to process the documents After a recent marketing campaign the company noticed that the application did not process many of The documents What should a solutions architect do to improve the architecture of this application?

A. Set the Lambda function's runtime timeout value to 15 minutes
B. Configure an S3 bucket replication policy Stage the documents m the S3 bucket for later processing
C. Deploy an additional Lambda function Load balance the processing of the documents across the two Lambda functions
D. Create an Amazon Simple Queue Service (Amazon SOS) queue Send the requests to the queue Configure the queue as an event source for Lambda.

Correct Answer: D
Section:
Explanation:
To improve the architecture of this application, the best solution would be to use Amazon Simple Queue Service (Amazon SQS) to buffer the requests and decouple the S3 bucket from the Lambda function. This will ensure that the documents are not lost and can be processed at a later time if the Lambda function is not available. This will ensure that the documents are not lost and can be processed at a later time if the Lambda function is not available. By using Amazon SQS, the architecture is decoupled and the Lambda function can process the documents in a scalable and fault-tolerant manner

QUESTION 183
A developer has an application that uses an AWS Lambda function to upload files to Amazon S3 and needs the required permissions to perform the task The developer already has an IAM user with valid IAM credentials required for Amazon S3 What should a solutions architect do to grant the permissions?

A. Add required IAM permissions in the resource policy of the Lambda function
B. Create a signed request using the existing IAM credentials n the Lambda function
C. Create a new IAM user and use the existing IAM credentials in the Lambda function.
D. Create an IAM execution role with the required permissions and attach the IAM rote to the Lambda function

Correct Answer: D
Section:
Explanation:
To grant the necessary permissions to an AWS Lambda function to upload files to Amazon S3, a solutions architect should create an IAM execution role with the required permissions and attach the IAM role to

QUESTION 184
A company has a large dataset for its online advertising business stored in an Amazon RDS for MySQL DB instance in a single Availability Zone. The company wants business reporting queries to run without impacting the write operations to the production DB instance.
Which solution meets these requirements?

A. Deploy RDS read replicas to process the business reporting queries.

B. Scale out the DB instance horizontally by placing it behind an Elastic Load Balancer
C. Scale up the DB instance to a larger instance type to handle write operations and queries
D. Deploy the OB distance in multiple Availability Zones to process the business reporting queries

Correct Answer: A
Section:
Explanation:

QUESTION 185
A meteorological startup company has a custom web application to sell weather data to its users online. The company uses Amazon DynamoDB to store is data and wants to bu4d a new service that sends an alert to the managers of four Internal teams every time a new weather event is recorded.
The company does not want true new service to affect the performance of the current application What should a solutions architect do to meet these requirement with the LEAST amount of operational overhead?

A. Use DynamoDB transactions to write new event data to the table Configure the transactions to notify internal teams.
B. Have the current application publish a message to four Amazon Simple Notification Service (Amazon SNS) topics. Have each team subscribe to one topic.
C. Enable Amazon DynamoDB Streams on the table. Use triggers to write to a mingle Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe.
D. Add a custom attribute to each record to flag new items. Write a cron job that scans the table every minute for items that are new and notifies an Amazon Simple Queue Service (Amazon SOS) queue to which the teams can subscribe.

Correct Answer: C
Section:

QUESTION 186
A company is developing a real-time multiplayer game that uses UDP for communications between the client and servers In an Auto Scaling group Spikes in demand are anticipated during the day, so the game server platform must adapt accordingly Developers want to store gamer scores and other non-relational data in a database solution that will scale without intervention Which solution should a solutions architect recommend?

A. Use Amazon Route 53 for traffic distribution and Amazon Aurora Serverless for data storage
B. Use a Network Load Balancer for traffic distribution and Amazon DynamoDB on-demand for data storage
C. Use a Network Load Balancer for traffic distribution and Amazon Aurora Global Database for data storage
D. Use an Application Load Balancer for traffic distribution and Amazon DynamoDB global tables for data storage

Correct Answer: B
Section:

QUESTION 187
A company needs to create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster to host a digital media streaming application. The EKS cluster will use a managed node group that is backed by Amazon Elastic Block Store (Amazon EBS) volumes for storage. The company must encrypt all data at rest by using a customer managed key that is stored in AWS Key Management Service (AWS KMS) Which combination of actions will meet this requirement with the LEAST operational overhead?
(Select TWO.)

A. Use a Kubernetes plugin that uses the customer managed key to perform data encryption.
B. After creation of the EKS cluster, locate the EBS volumes. Enable encryption by using the customer managed key.
C. Enable EBS encryption by default in the AWS Region where the EKS cluster will be created. Select the customer managed key as the default key.
D. Create the EKS cluster Create an IAM role that has cuwlicy that grants permission to the customer managed key. Associate the role with the EKS cluster.
E. Store the customer managed key as a Kubernetes secret in the EKS cluster. Use the customer managed key to encrypt the EBS volumes.

Correct Answer: A, D
Section:
Explanation:
EBS encryption by default is a feature that enables encryption for all new EBS volumes and snapshots created in a Region1. EBS encryption by default uses a service managed key or a customer managed key that is stored in AWS KMS1. EBS encryption by default is suitable for scenarios where data at rest must be encrypted by using a customer managed key, such as the digital media streaming application in the scenario1.
To meet the requirements of the scenario, the solutions architect should enable EBS encryption by default in the AWS Region where the EKS cluster will be created. The solutions architect should select the customer managed key as the default key for encryption1. This way, all new EBS volumes and snapshots created in that Region will be encrypted by using the customer managed key. EKS encryption provider support is a feature that enables envelope encryption of Kubernetes secrets in EKS with a customer managed key that is stored in AWS KMS2. Envelope encryption means that data is encrypted by data encryption keys (DEKs) using AES-GCM; DEKs are encrypted by key encryption keys (KEKs) according to configuration in AWS KMS3. EKS encryption provider support is suitable for scenarios where secrets must be encrypted by using a customer managed key, such as the digital media streaming application in the scenario2. To meet the requirements of the scenario, the solutions architect should create the EKS cluster and create an IAM role that has a policy that grants permission to the customer managed key. The solutions architect should associate the role with the EKS cluster2. This way, the EKS cluster can use envelope encryption of Kubernetes secrets with the customer managed key.

QUESTION 188
A company has an AWS account used for software engineering. The AWS account has access to the company's on-premises data center through a pair of AWS Direct Connect connections. All non-VPC traffic routes to the virtual private gateway.
A development team recently created an AWS Lambda function through the console. The development team needs to allow the function to access a database that runs in a private subnet in the company's data center. Which solution will meet these requirements?

A. Configure the Lambda function to run in the VPC with the appropriate security group.
B. Set up a VPN connection from AWS to the data center. Route the traffic from the Lambda function through the VPN.
C. Update the route tables in the VPC to allow the Lambda function to access the on-premises data center through Direct Connect.
D. Create an Elastic IP address. Configure the Lambda function to send traffic through the Elastic IP address without an elastic network interface.

Correct Answer: A
Section:
Explanation:
https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html#vpc-managing-eni

QUESTION 189
A company has a legacy data processing application that runs on Amazon EC2 instances. Data is processed sequentially, but the order of results does not matter. The application uses a monolithic architecture. The only way that the company can scale the application to meet increased demand is to increase the size of the instances.
The company's developers have decided to rewrite the application to use a microservices architecture on Amazon Elastic Container Service (Amazon ECS). What should a solutions architect recommend for communication between the microservices?

A. Create an Amazon Simple Queue Service (Amazon SQS) queue. Add code to the data producers, and send data to the queue. Add code to the data consumers to process data from the queue.
B. Create an Amazon Simple Notification Service (Amazon SNS) topic. Add code to the data producers, and publish notifications to the topic. Add code to the data consumers to subscribe to the topic.
C. Create an AWS Lambda function to pass messages. Add code to the data producers to call the Lambda function with a data object. Add code to the data consumers to receive a data object that is passed from the Lambda function.
D. Create an Amazon DynamoDB table. Enable DynamoDB Streams. Add code to the data producers to insert data into the table. Add code to the data consumers to use the DynamoDB Streams API to detect new table entries and retrieve the data.

Correct Answer: A
Section:
Explanation:
Queue has Limited throughput (300 msg/s without batching, 3000 msg/s with batching whereby upto 10 msg per batch operation; Msg duplicates not allowed in the queue (exactly-once delivery); Msg order is preserved (FIFO); Queue name must end with .fifo

QUESTION 190
A hospital wants to create digital copies for its large collection of historical written records. The hospital will continue to add hundreds of new documents each day. The hospital's data team will scan the documents and will

upload the documents to the AWS Cloud.
A solutions architect must implement a solution to analyze the documents, extract the medical information, and store the documents so that an application can run SQL queries on the dat a. The solution must maximize scalability and operational efficiency.
Which combination of steps should the solutions architect take to meet these requirements? (Select TWO.)

A. Write the document information to an Amazon EC2 instance that runs a MySQL database.
B. Write the document information to an Amazon S3 bucket. Use Amazon Athena to query the data.
C. Create an Auto Scaling group of Amazon EC2 instances to run a custom application that processes the scanned files and extracts the medical information.
D. Create an AWS Lambda function that runs when new documents are uploaded. Use Amazon Rekognition to convert the documents to raw text. Use Amazon Transcribe Medical to detect and extract relevant medical information from the text.
E. Create an AWS Lambda function that runs when new documents are uploaded. Use Amazon Textract to convert the documents to raw text. Use Amazon Comprehend Medical to detect and extract relevant medical information from the text.

Correct Answer: B, E
Section:
Explanation:
This solution meets the requirements of creating digital copies for a large collection of historical written records, analyzing the documents, extracting the medical information, and storing the documents so that an application can run SQL queries on the data. Writing the document information to an Amazon S3 bucket can provide scalable and durable storage for the scanned files.Using Amazon Athena to query the data can provide serverless and interactive SQL analysis on data stored in S3. Creating an AWS Lambda function that runs when new documents are uploaded can provide event-driven and serverless processing of the scanned files. Using Amazon Textract to convert the documents to raw text can provide accurate optical character recognition (OCR) and extraction of structured data such as tables and forms from documents using artificial intelligence (AI). Using Amazon Comprehend Medical to detect and extract relevant medical information from the text can provide natural language processing (NLP) service that uses machine learning that has been pre-trained to understand and extract health data from medical text.Option A is incorrect because writing the document information to an Amazon EC2 instance that runs a MySQL database can increase the infrastructure overhead and complexity, and it may not be able to handle large volumes of data. Option C is incorrect because creating an Auto Scaling group of Amazon EC2 instances to run a custom application that processes the scanned files and extracts the medical information can increase the infrastructure overhead and complexity, and it may not be able to leverage existing AI and NLP services such as Textract and Comprehend Medical. Option D is incorrect because using Amazon Rekognition to convert the documents to raw text can provide image and video analysis, but it does not support OCR or extraction of structured data from documents. Using Amazon Transcribe Medical to detect and extract relevant medical information from the text can provide speech-to-text transcription service for medical conversations, but it does not support text analysis or extraction of health data from medical text.
Reference: https://aws.amazon.com/s3/ https://aws.amazon.com/athena/ https://aws.amazon.com/lambda/ https://aws.amazon.com/textract/ https://aws.amazon.com/comprehend/medical/

QUESTION 191
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-lime and on-demand streaming?

A. Amazon CloudFront
B. AWS Global Accelerator
C. Amazon Route 53
D. Amazon S3 Transfer Acceleration

Correct Answer: A
Section:
Explanation:
You can use CloudFront to deliver video on demand (VOD) or live streaming video using any HTTPorigin. One way you can set up video workflows in the cloud is by using CloudFront together withAWS Media Services.
https:// docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/ondemand-streaming-video.html

QUESTION 192
A company wants to migrate its MySQL database from on premises to AWS. The company recently experienced a database outage that significantly impacted the business. To ensure this does not happen again, the company wants a reliable database solution on AWS that minimizes data loss and stores every transaction on at least two nodes. Which solution meets these requirements?

A. Create an Amazon RDS DB instance with synchronous replication to three nodes in three Availability Zones.

B. Create an Amazon RDS MySQL DB instance with Multi-AZ functionality enabled to synchronously replicate the data.
C. Create an Amazon RDS MySQL DB instance and then create a read replica in a separate AWS Region that synchronously replicates the data.
D. Create an Amazon EC2 instance with a MySQL engine installed that triggers an AWS Lambda function to synchronously replicate the data to an Amazon RDS MySQL DB instance.

Correct Answer: B
Section:
Explanation:
Q: What does Amazon RDS manage on my behalf?
Amazon RDS manages the work involved in setting up a relational database: from provisioning the infrastructure capacity you request to installing the database software. Once your database is up and running, Amazon RDS automates common administrative tasks such as performing backups and patching the software that powers your database. With optional Multi-AZ deployments, Amazon RDS also manages synchronous data replication across Availability Zones with automatic failover.
https://aws.amazon.com/rds/faqs/

QUESTION 193

An ecommerce company hosts its analytics application in the AWS Cloud. The application generates about 300 MB of data each month. The data is stored in JSON format. The company is evaluating a disaster recovery solution to back up the dat a. The data must be accessible in milliseconds if it is needed, and the data must be kept for 30 days. Which solution meets these requirements MOST cost-effectively?

A. Amazon OpenSearch Service (Amazon Elasticsearch Service)
B. Amazon S3 Glacier
C. Amazon S3 Standard
D. Amazon RDS for PostgreSQL

Correct Answer: C
Section:

QUESTION 194
A company has a Windows-based application that must be migrated to AWS. The application requires the use of a shared Windows file system attached to multiple Amazon EC2 Windows instances that are deployed across multiple Availability Zones.
What should a solutions architect do to meet this requirement?

A. Configure AWS Storage Gateway in volume gateway mode. Mount the volume to each Windows instance.
B. Configure Amazon FSx for Windows File Server. Mount the Amazon FSx file system to each Windows instance.
C. Configure a file system by using Amazon Elastic File System (Amazon EFS). Mount the EFS file system to each Windows instance.
D. Configure an Amazon Elastic Block Store (Amazon EBS) volume with the required size. Attach each EC2 instance to the volume. Mount the file system within the volume to each Windows instance.

Correct Answer: B
Section:

QUESTION 195
A solutions architect is creating a new Amazon CloudFront distribution for an application. Some of the information submitted by users is sensitive. The application uses HTTPS but needs another layer of security. The sensitive information should be protected throughout the entire application stack, and access to the information should be restricted to certain applications. Which action should the solutions architect take?

A. Configure a CloudFront signed URL.
B. Configure a CloudFront signed cookie.
C. Configure a CloudFront field-level encryption profile.
D. Configure CloudFront and set the Origin Protocol Policy setting to HTTPS Only for the ViewerProtocol Policy.

Correct Answer: C
Section:
Explanation:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-levelencryption.html"
With Amazon CloudFront, you can enforce secure end-to-end connections to origin servers by using
HTTPS. Field-level encryption adds an additional layer of security that lets you protect specific data throughout system processing so that only certain applications can see it."

QUESTION 196
A company has a web application with sporadic usage patterns There is heavy usage at the beginning of each month moderate usage at the start of each week and unpredictable usage during the week The application consists of a web server and a MySQL database server running inside the data center The company would like to move the application to the AWS Cloud and needs to select a costeffective database platform that will not require database modifications Which solution will meet these requirements?

A. Amazon DynamoDB
B. Amazon RDS for MySQL
C. MySQL-compatible Amazon Aurora Serverless

D. MySQL deployed on Amazon EC2 in an Auto Scaling group

Correct Answer: C
Section:
Explanation:
Amazon RDS for MySQL is a fully-managed relational database service that makes it easy to set up, operate, and scale MySQL deployments in the cloud. Amazon Aurora Serverless is an on-demand, auto- scaling configuration for Amazon Aurora (MySQL-compatible edition), where the database will automatically start up, shut down, and scale capacity up or down based on your application's needs. It is a simple, cost-effective option for infrequent, intermittent, or unpredictable workloads

QUESTION 197
A company owns an asynchronous API that is used to ingest user requests and, based on the request type, dispatch requests to the appropriate microservice for processing. The company is using Amazon API Gateway to deploy the API front end, and an AWS Lambda function that invokes Amazon DynamoDB to store user requests before dispatching them to the processing microservices. The company provisioned as much DynamoDB throughput as its budget allows, but the company is still experiencing availability issues and is losing user requests. What should a solutions architect do to address this issue without impacting existing users?

A. Add throttling on the API Gateway with server-side throttling limits.
B. Use DynamoDB Accelerator (DAX) and Lambda to buffer writes to DynamoDB.
C. Create a secondary index in DynamoDB for the table with the user requests.
D. Use the Amazon Simple Queue Service (Amazon SQS) queue and Lambda to buffer writes to DynamoDB.

Correct Answer: D
Section:
Explanation:
By using an SQS queue and Lambda, the solutions architect can decouple the API front end from the processing microservices and improve the overall scalability and availability of the system. The SQS queue acts as a buffer, allowing the API front end to continue accepting user requests even if the processing microservices are experiencing high workloads or are temporarily unavailable. The Lambda function can then retrieve requests from the SQS queue and write them to DynamoDB, ensuring that all user requests are stored and processed. This approach allows the company to scale the processing microservices independently from the API front end, ensuring that the API remains available to users even during periods of high demand.

QUESTION 198
A company needs to move data from an Amazon EC2 instance to an Amazon S3 bucket. The company must ensure that no API calls and no data are routed through public internet routes. Only the EC2 instance can have access to upload data to the S3 bucket.
Which solution will meet these requirements?

A. Create an interface VPC endpoint for Amazon S3 in the subnet where the EC2 instance is located.
Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.
B. Create a gateway VPC endpoint for Amazon S3 in the Availability Zone where the EC2 instance is located. Attach appropriate security groups to the endpoint. Attach a resource policy lo the S3 bucket to only allow the EC2 instance's IAM role for access.
C. Run the nslookup tool from inside the EC2 instance to obtain the private IP address of the S3 bucket's service API endpoint. Create a route in the VPC route table to provide the EC2 instance with access to the S3 bucket. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.
D. Use the AWS provided, publicly available ip-ranges.json tile to obtain the private IP address of the S3 bucket's service API endpoint. Create a route in the VPC route table to provide the EC2 instance with access to the S3 bucket. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.

Correct Answer: B
Section:
Explanation:

QUESTION 199
A gaming company hosts a browser-based application on AWS. The users of the application consume a large number of videos and images that are stored in Amazon S3. This content is the same for all users. The application has increased in popularity, and millions of users worldwide are accessing these media files. The company wants to provide the files to the users while reducing the load on the origin. Which solution meets these requirements

MOST cost-effectively?

A. Deploy an AWS Global Accelerator accelerator in front of the web servers.
B. Deploy an Amazon CloudFront web distribution in front of the S3 bucket.
C. Deploy an Amazon ElastiCache for Redis instance in front of the web servers.
D. Deploy an Amazon ElastiCache for Memcached instance in front of the web servers.

Correct Answer: B
Section:

QUESTION 200
A company has two applications: a sender application that sends messages with payloads to be processed and a processing application intended to receive the messages with payloads. The company wants to implement an AWS service to handle messages between the two applications.
The sender application can send about 1.000 messages each hour. The messages may take up to 2 days to be processed. If the messages fail to process, they must be retained so that they do not impact the processing of any remaining messages.
Which solution meets these requirements and is the MOST operationally efficient?

A. Set up an Amazon EC2 instance running a Redis database. Configure both applications to use the instance. Store, process, and delete the messages, respectively.
B. Use an Amazon Kinesis data stream to receive the messages from the sender application.
Integrate the processing application with the Kinesis Client Library (KCL).
C. Integrate the sender and processor applications with an Amazon Simple Queue Service (Amazon SQS) queue. Configure a dead-letter queue to collect the messages that failed to process.
D. Subscribe the processing application to an Amazon Simple Notification Service (Amazon SNS) topic to receive notifications to process. Integrate the sender application to write to the SNS topic.

Correct Answer: C
Section:
Explanation:
https://aws.amazon.com/blogs/compute/building-loosely-coupled-scalable-c-applications-withamazon-sqs-and-amazon-sns/ https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-deadletter-queues.html

QUESTION 201
A company is planning to move its data to an Amazon S3 bucket. The data must be encrypted when it is stored in the S3 bucket. Additionally, the encryption key must be automatically rotated every year. Which solution will meet these requirements with the LEAST operational overhead?

A. Move the data to the S3 bucket. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use the built-in key rotation behavior of SSE-S3 encryption keys.
B. Create an AWS Key Management Service {AWS KMS) customer managed key. Enable automatic key rotation. Set the S3 bucket's default encryption behavior to use the customer managed KMS key. Move the data to the S3 bucket.
C. Create an AWS Key Management Service (AWS KMS) customer managed key. Set the S3 bucket's default encryption behavior to use the customer managed KMS key. Move the data to the S3 bucket. Manually rotate the KMS key every year.
D. Encrypt the data with customer key material before moving the data to the S3 bucket. Create an AWS Key Management Service (AWS KMS) key without key material. Import the customer key material into the KMS key. Enable automatic key rotation.

Correct Answer: B
Section:
Explanation:
SSE-S3 - is free and uses AWS owned CMKs (CMK = Customer Master Key). The encryption key is owned and managed by AWS, and is shared among many accounts. Its rotation is automatic with time that varies as shown in the table here. The time is not explicitly defined. SSE-KMS - has two flavors: AWS managed CMK. This is free CMK generated only for your account. You can only view it policies and audit usage, but not manage it. Rotation is automatic - once per 1095 days (3 years), Customer managed CMK. This uses your own key that you create and can manage. Rotation is not enabled by default. But if you enable it, it will be automatically rotated every 1 year. This variant can also use an imported key material by you. If you create such key with an imported material, there is no automated rotation. Only manual rotation. SSE-C - customer provided key. The encryption key is fully managed by you outside of AWS. AWS will not rotate it.
This solution meets the requirements of moving data to an Amazon S3 bucket, encrypting the data when it is stored in the S3 bucket, and automatically rotating the encryption key every year with the least operational overhead. AWS Key

Management Service (AWS KMS) is a service that enables you to create and manage encryption keys for your data. A customer managed key is a symmetric encryption key that you create and manage in AWS KMS. You can enable automatic key rotation for a customer managed key, which means that AWS KMS generates new cryptographic material for the key every year. You can set the S3 bucket's default encryption behavior to use the customer managed KMS key, which means that any object that is uploaded to the bucket without specifying an encryption method will be encrypted with that key. Option A is incorrect because using server-side encryption with Amazon S3 managed encryption keys (SSE-S3) does not allow you to control or manage the encryption keys. SSE-S3 uses a unique key for each object, and encrypts that key with a master key that is regularly rotated by S3. However, you cannot enable or disable key rotation for SSE-S3 keys, or specify the rotation interval. Option C is incorrect because manually rotating the KMS key every year can increase the operational overhead and complexity, and it may not meet the requirement of rotating the key every year if you forget or delay the rotation process. Option D is incorrect because encrypting the data with customer key material before moving the data to the S3 bucket can increase the operational overhead and complexity, and it may not provide consistent encryption for all objects in the bucket. Creating a KMS key without key material and importing the customer key material into the KMS key can enable you to use your own source of random bits to generate your KMS keys, but it does not support automatic key rotation. https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucket-encryption.html

QUESTION 202
An application runs on Amazon EC2 instances in private subnets. The application needs to access an Amazon DynamoDB table. What is the MOST secure way to access the table while ensuring that the traffic does not leave the AWS network?

A. Use a VPC endpoint for DynamoDB.
B. Use a NAT gateway in a public subnet.
C. Use a NAT instance in a private subnet.
D. Use the internet gateway attached to the VPC.

Correct Answer: A
Section:
Explanation:
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpointsdynamodb.html
A VPC endpoint for DynamoDB enables Amazon EC2 instances in your VPC to use their private IP addresses to access DynamoDB with no exposure to the public internet. Your EC2 instances do not require public IP addresses, and you don't need an internet gateway, a NAT device, or a virtual private gateway in your VPC. You use endpoint policies to control access to DynamoDB. Traffic between your VPC and the AWS service does not leave the Amazon network.

QUESTION 203
A company uses a payment processing system that requires messages for a particular payment ID to be received in the same order that they were sent Otherwise, the payments might be processed incorrectly. Which actions should a solutions architect take to meet this requirement? (Select TWO.)

A. Write the messages to an Amazon DynamoDB table with the payment ID as the partition key
B. Write the messages to an Amazon Kinesis data stream with the payment ID as the partition key.
C. Write the messages to an Amazon ElastiCache for Memcached cluster with the payment ID as the key
D. Write the messages to an Amazon Simple Queue Service (Amazon SQS) queue Set the message attribute to use the payment ID
E. Write the messages to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the message group to use the payment ID.

Correct Answer: B, E
Section:
Explanation:

QUESTION 204
An IAM user made several configuration changes to AWS resources m their company's account during a production deployment last week. A solutions architect learned that a couple of security group rules are not configured as desired. The solutions architect wants to confirm which IAM user was responsible for making changes.
Which service should the solutions architect use to find the desired information?

A. Amazon GuardDuty
B. Amazon Inspector

C. AWS CloudTrail
D. AWS Config

Correct Answer: C
Section:

QUESTION 205
A company has a three-tier environment on AWS that ingests sensor data from its users' devices The traffic flows through a Network Load Balancer (NIB) then to Amazon EC2 instances for the web tier and finally to EC2 instances for the application tier that makes database calls What should a solutions architect do to improve the security of data in transit to the web tier?

A. Configure a TLS listener and add the server certificate on the NLB
B. Configure AWS Shield Advanced and enable AWS WAF on the NLB
C. Change the load balancer to an Application Load Balancer and attach AWS WAF to it
D. Encrypt the Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instances using AWS Key Management Service (AWS KMS)

Correct Answer: A
Section:

QUESTION 206
A research company runs experiments that are powered by a simulation application and a visualization application. The simulation application runs on Linux and outputs intermediate data to an NFS share every 5 minutes. The visualization application is a Windows desktop application that displays the simulation output and requires an SMB file system.
The company maintains two synchronized file systems. This strategy is causing data duplication and inefficient resource usage. The company needs to migrate the applications to AWS without making code changes to either application.
Which solution will meet these requirements?

A. Migrate both applications to AWS Lambda. Create an Amazon S3 bucket to exchange data between the applications.
B. Migrate both applications to Amazon Elastic Container Service (Amazon ECS). Configure Amazon FSx File Gateway for storage.
C. Migrate the simulation application to Linux Amazon EC2 instances. Migrate the visualization application to Windows EC2 instances. Configure Amazon Simple Queue Service (Amazon SQS) to exchange data between the applications.
D. Migrate the simulation application to Linux Amazon EC2 instances. Migrate the visualization application to Windows EC2 instances. Configure Amazon FSx for NetApp ONTAP for storage.

Correct Answer: D
Section:
Explanation:
This solution will meet the requirements because Amazon FSx for NetApp ONTAP is a fully managed service that provides highly reliable, scalable, and feature-rich file storage built on NetApp's popular ONTAP file system. FSx for ONTAP supports both NFS and SMB protocols, which means it can be accessed by both Linux and Windows applications without code changes. FSx for ONTAP also eliminates data duplication and inefficient resource usage by automatically tiering infrequently accessed data to a lower-cost storage tier and providing storage efficiency features such as deduplication and compression. FSx for ONTAP also integrates with other AWS services such as Amazon S3, AWS Backup, and AWS CloudFormation.By migrating the applications to Amazon EC2 instances, the company can leverage the scalability, security, and performance of AWS compute resources.

QUESTION 207
A company is deploying an application in three AWS Regions using an Application Load Balancer Amazon Route 53 will be used to distribute traffic between these Regions. Which Route 53 configuration should a solutions architect use to provide the MOST high-performing experience?

A. Create an A record with a latency policy.
B. Create an A record with a geolocation policy.
C. Create a CNAME record with a failover policy.
D. Create a CNAME record with a geoproximity policy.

Correct Answer: A
Section:
Explanation:
To provide the most high-performing experience for the users of the application, a solutions architect should use a latency routing policy for the Route 53 A record.This policy allows Route 53 to route traffic to the AWS Region that provides the lowest possible latency for the users1.A latency routing policy can also improve the availability of the application, as Route 53 can automatically route traffic to another Region if the primary Region becomes unavailable2.
1: https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-latency
2: https://aws.amazon.com/route53/faqs/#Latency_Based_Routing

QUESTION 208
A company has an application that delivers on-demand training videos to students around the world. The application also allows authorized content developers to upload videos. The data is stored in an Amazon S3 bucket in the us-east-2 Region.
The company has created an S3 bucket in the eu-west-2 Region and an S3 bucket in the ap-southeast-1 Region. The company wants to replicate the data to the new S3 buckets. The company needs to minimize latency for developers who upload videos and students who stream videos near eu-west-2 and ap-southeast-1.
Which combination of steps will meet these requirements with the FEWEST changes to the application? (Select TWO.)

A. Configure one-way replication from the us-east-2 S3 bucket to the eu-west-2 S3 bucket. Configure one-way replication from the us-east-2 S3 bucket to the ap-southeast-1 S3 bucket.
B. Configure one-way replication from the us-east-2 S3 bucket to the eu-west-2 S3 bucket. Configure one-way replication from the eu-west-2 S3 bucket to the ap-southeast-1 S3 bucket.
C. Configure two-way (bidirectional) replication among the S3 buckets that are in all three Regions.
D. Create an S3 Multi-Region Access Point. Modify the application to use the Amazon Resource Name (ARN) of the Multi-Region Access Point for video streaming. Do not modify the application for video uploads.
E. Create an S3 Multi-Region Access Point Modify the application to use the Amazon Resource Name (ARN) of the Multi-Region Access Point for video streaming and uploads.

Correct Answer: A, E
Section:
Explanation:
These two steps will meet the requirements with the fewest changes to the application because they will enable the company to replicate the data to the new S3 buckets and minimize latency for both video streaming and uploads. One-way replication from the us-east-2 S3 bucket to the other two S3 buckets will ensure that the data is synchronized across all three regions. The company can use S3 Cross-Region Replication (CRR) to automatically copy objects across buckets in different AWS Regions. CRR can help the company achieve lower latency and compliance requirements by keeping copies of their data in different regions. Creating an S3 Multi-Region Access Point and modifying the application to use its ARN will allow the company to access the data through a single global endpoint. An S3 Multi-Region Access Point is a globally unique name that can be used to access objects stored in S3 buckets across multiple regions. It automatically routes requests to the closest S3 bucket with the lowest latency. By using an S3 Multi-Region Access Point, the company can simplify the application architecture and improve the performance and reliability of the application.
Replicating objects
Multi-Region Access Points in Amazon S3

QUESTION 209
An analytics company uses Amazon VPC to run its multi-tier services. The company wants to use RESTful APIs to offer a web analytics service to millions of users. Users must be verified by using an authentication service to access the APIs.
Which solution will meet these requirements with the MOST operational efficiency?

A. Configure an Amazon Cognito user pool for user authentication. Implement Amazon API Gateway REST APIs with a Cognito authorizer.
B. Configure an Amazon Cognito identity pool for user authentication. Implement Amazon API Gateway HTTP APIs with a Cognito authorizer.
C. Configure an AWS Lambda function to handle user authentication. Implement Amazon API Gateway REST APIs with a Lambda authorizer.
D. Configure an IAM user to handle user authentication. Implement Amazon API Gateway HTTP APIs with an IAM authorizer.

Correct Answer: A
Section:
Explanation:
This solution will meet the requirements with the most operational efficiency because:

Amazon Cognito user pools provide a secure and scalable user directory that can store and manage user profiles, and handle user sign-up, sign-in, and access control. User pools can also integrate with social identity providers and enterprise identity providers via SAML or OIDC. User pools can issue JSON Web Tokens (JWTs) that can be used to authenticate users and authorize API requests.
Amazon API Gateway REST APIs enable you to create and deploy APIs that expose your backend services to your clients. REST APIs support multiple authorization mechanisms, including Cognito user pools, IAM, Lambda, and custom authorizers. A Cognito authorizer is a type of Lambda authorizer that uses a Cognito user pool as the identity source. When a client makes a request to a REST API method that is configured with a Cognito authorizer, API Gateway verifies the JWTs that are issued by the user pool and grants access based on the token's claims and the authorizer's configuration.
By using Cognito user pools and API Gateway REST APIs with a Cognito authorizer, you can achieve a high level of security, scalability, and performance for your web analytics service. You can also leverage the built-in features of Cognito and API Gateway, such as user management, token validation, caching, throttling, and monitoring, without having to implement them yourself. This reduces the operational overhead and complexity of your solution.
Amazon Cognito User Pools
Amazon API Gateway REST APIs
Use API Gateway Lambda authorizers

QUESTION 210
A company is designing a tightly coupled high performance computing (HPC) environment in the AWS Cloud The company needs to include features that will optimize the HPC environment for networking and storage.
Which combination of solutions will meet these requirements? (Select TWO)

A. Create an accelerator in AWS Global Accelerator. Configure custom routing for the accelerator.
B. Create an Amazon FSx for Lustre file system. Configure the file system with scratch storage.
C. Create an Amazon CloudFront distribution. Configure the viewer protocol policy to be HTTP and HTTPS.
D. Launch Amazon EC2 instances. Attach an Elastic Fabric Adapter (EFA) to the instances.
E. Create an AWS Elastic Beanstalk deployment to manage the environment.

Correct Answer: B, D
Section:
Explanation:
These two solutions will optimize the HPC environment for networking and storage. Amazon FSx for Lustre is a fully managed service that provides cost-effective, high-performance, scalable storage for compute workloads. It is built on the world's most popular high-performance file system, Lustre, which is designed for applications that require fast storage, such as HPC and machine learning. By configuring the file system with scratch storage, you can achieve sub-millisecond latencies, up to hundreds of GBs/s of throughput, and millions of IOPS. Scratch file systems are ideal for temporary storage and shorter-term processing of data. Data is not replicated and does not persist if a file server fails. For more information, seeAmazon FSx for Lustre.
Elastic Fabric Adapter (EFA) is a network interface for Amazon EC2 instances that enables customers to run applications requiring high levels of inter-node communications at scale on AWS. Its custom-built operating system (OS) bypass hardware interface enhances the performance of inter-instance communications, which is critical to scaling HPC and machine learning applications. EFA provides a low-latency, low-jitter channel for inter-instance communications, enabling your tightly-coupled HPC or distributed machine learning applications to scale to thousands of cores. EFA uses libfabric interface and libfabric APIs for communications, which are supported by most HPC programming models. For more information, seeElastic Fabric Adapter.
The other solutions are not suitable for optimizing the HPC environment for networking and storage. AWS Global Accelerator is a networking service that helps you improve the availability, performance, and security of your public applications by using the AWS global network. It provides two global static public IPs, deterministic routing, fast failover, and TCP termination at the edge for your application endpoints. However, it does not support OS-bypass capabilities or high-performance file systems that are required for HPC and machine learning applications. For more information, seeAWS Global Accelerator.
Amazon CloudFront is a content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment. CloudFront is integrated with AWS services such as Amazon S3, Amazon EC2, AWS Elemental Media Services, AWS Shield, AWS WAF, and AWS Lambda@Edge. However, CloudFront is not designed for HPC and machine learning applications that require high levels of inter-node communications and fast storage. For more information, see [Amazon CloudFront].
AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS. You can simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. However, Elastic Beanstalk is not optimized for HPC and machine learning applications that require OS-bypass capabilities and high-performance file systems. For more information, see [AWS Elastic Beanstalk].

QUESTION 211
A solutions architect wants to use the following JSON text as an identity-based policy to grant specific permissions:

```
{    "Statement": [
        {
            "Action": [
                "ssm:ListDocuments",
                "ssm:GetDocument"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Sid": ""
        }
    ],
    "Version": "2012-10-17"
}
```

Which IAM principals can the solutions architect attach this policy to? (Select TWO.)

A. Role
B. Group
C. Organization
D. Amazon Elastic Container Service (Amazon ECS) resource
E. Amazon EC2 resource

Correct Answer: A, B
Section:
Explanation:
This JSON text is an identity-based policy that grants specific permissions. The IAM principals that the solutions architect can attach this policy to are Role and Group. This is because the policy is written in JSON and is an identity-based policy, which can be attached to IAM principals such as users, groups, and roles.Identity-based policies are permissions policies that you attach to IAM identities (users, groups, or roles) and explicitly state what that identity is allowed (or denied) to do1.Identity-based policies are different from resource-based policies, which define the permissions around the specific resource1.Resource-based policies are attached to a resource, such as an Amazon S3 bucket or an Amazon EC2 instance1.Resource-based policies can also specify a principal, which is the entity that is allowed or denied access to the resource1.Organization is not an IAM principal, but a feature of AWS Organizations that allows you to manage multiple AWS accounts centrally2.Amazon ECS resource and Amazon EC2 resource are not IAM principals, but AWS resources that can have resource-based policies attached to them34.
Identity-based policies and resource-based policies
AWS Organizations
Amazon ECS task role
Amazon EC2 instance profile

QUESTION 212
A company has a three-tier environment on AWS that ingests sensor data from its users' devices The traffic flows through a Network Load Balancer (NIB) then to Amazon EC2 instances for the web tier and finally to EC2 instances for the application tier that makes database calls
What should a solutions architect do to improve the security of data in transit to the web tier?

A. Configure a TLS listener and add the server certificate on the NLB
B. Configure AWS Shield Advanced and enable AWS WAF on the NLB
C. Change the load balancer to an Application Load Balancer and attach AWS WAF to it

D. Encrypt the Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instances using AWS Key Management Service (AWS KMS)

Correct Answer: A
Section:
Explanation:
A: How do you protect your data in transit?
Best Practices:
Implement secure key and certificate management: Store encryption keys and certificates securely and rotate them at appropriate time intervals while applying strict access control; for example, by using a certificate management service, such as AWS Certificate Manager (ACM).
Enforce encryption in transit: Enforce your defined encryption requirements based on appropriate standards and recommendations to help you meet your organizational, legal, and compliance requirements.
Automate detection of unintended data access: Use tools such as GuardDuty to automatically detect attempts to move data outside of defined boundaries based on data classification level, for example, to detect a trojan that is copying data to an unknown or untrusted network using the DNS protocol.
Authenticate network communications: Verify the identity of communications by using protocols that support authentication, such as Transport Layer Security (TLS) or IPsec.
https://wa.aws.amazon.com/wat.question.SEC_9.en.html