

## Exam Questions SAA-C03

AWS Certified Solutions Architect - Associate (SAA-C03)

<https://www.2passeasy.com/dumps/SAA-C03/>



### NEW QUESTION 1

- (Topic 1)

A company hosts its web applications in the AWS Cloud. The company configures Elastic Load Balancers to use certificate that are imported into AWS Certificate Manager (ACM). The company's security team must be notified 30 days before the expiration of each certificate.

What should a solutions architect recommend to meet the requirement?

- A. Add a rule in ACM to publish a custom message to an Amazon Simple Notification Service (Amazon SNS) topic every day beginning 30 days before any certificate will expire.
- B. Create an AWS Config rule that checks for certificates that will expire within 30 days
- C. Configure Amazon EventBridge (Amazon CloudWatch Events) to invoke a custom alert by way of Amazon Simple Notification Service (Amazon SNS) when AWS Config reports a noncompliant resource
- D. Use AWS Trusted Advisor to check for certificates that will expire within 30 days
- E. Create an Amazon CloudWatch alarm that is based on Trusted Advisor metrics for check status changes. Configure the alarm to send a custom alert by way of Amazon Simple Notification Service (Amazon SNS)
- F. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to detect any certificates that will expire within 30 days
- G. Configure the rule to invoke an AWS Lambda function
- H. Configure the Lambda function to send a custom alert by way of Amazon Simple Notification Service (Amazon SNS).

**Answer: B**

#### Explanation:

<https://aws.amazon.com/premiumsupport/knowledge-center/acm-certificate-expiration/>

### NEW QUESTION 2

- (Topic 1)

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
- B. Use Amazon Inspector to scan the objects in the bucket
- C. If objects contain PII
- D. trigger an S3 Lifecycle policy to remove the objects that contain PII.
- E. Use an Amazon S3 bucket as a secure transfer point
- F. Use Amazon Macie to scan the objects in the bucket
- G. If objects contain PII
- H. Use Amazon Simple Notification Service (Amazon SNS) to trigger a notification to the administrators to remove the objects that contain PII.
- I. Implement custom scanning algorithms in an AWS Lambda function
- J. Trigger the function when objects are loaded into the bucket
- K. If objects contain PII
- L. use Amazon Simple Notification Service (Amazon SNS) to trigger a notification to the administrators to remove the objects that contain PII.
- M. Implement custom scanning algorithms in an AWS Lambda function
- N. Trigger the function when objects are loaded into the bucket
- O. If objects contain PII
- P. use Amazon Simple Email Service (Amazon SES) to trigger a notification to the administrators and trigger an S3 Lifecycle policy to remove the objects that contain PII.

**Answer: B**

#### Explanation:

To meet the requirements of detecting and alerting the administrators when PII is shared and automating remediation with the least development effort, the best approach would be to use Amazon S3 bucket as a secure transfer point and scan the objects in the bucket with Amazon Macie. Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect sensitive data stored in Amazon S3. It can be used to classify sensitive data, monitor access to sensitive data, and automate remediation actions.

In this scenario, after uploading the files to the Amazon S3 bucket, the objects can be scanned for PII by Amazon Macie, and if it detects any PII, it can trigger an Amazon Simple Notification Service (SNS) notification to alert the administrators to remove the objects containing PII. This approach requires the least development effort, as Amazon Macie already has pre-built data classification rules that can detect PII in various formats. Hence, option B is the correct answer.

References:

? Amazon Macie User Guide: <https://docs.aws.amazon.com/macie/latest/userguide/what-is-macie.html>

? AWS Well-Architected Framework - Security Pillar: <https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html>

### NEW QUESTION 3

- (Topic 1)

A company is implementing a new business application. The application runs on two Amazon EC2 instances and uses an Amazon S3 bucket for document storage. A solutions architect needs to ensure that the EC2 instances can access the S3 bucket.

What should the solutions architect do to meet this requirement?

- A. Create an IAM role that grants access to the S3 bucket
- B. Attach the role to the EC2 instances.
- C. Create an IAM policy that grants access to the S3 bucket
- D. Attach the policy to the EC2 instances.
- E. Create an IAM group that grants access to the S3 bucket
- F. Attach the group to the EC2 instances.
- G. Create an IAM user that grants access to the S3 bucket
- H. Attach the user account to the EC2 instances.

**Answer:** A

**Explanation:**

<https://aws.amazon.com/premiumsupport/knowledge-center/ec2-instance-access-s3-bucket/>

#### NEW QUESTION 4

- (Topic 1)

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

**Answer:** B

**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.

#### NEW QUESTION 5

- (Topic 1)

A company runs an on-premises application that is powered by a MySQL database. The company is migrating the application to AWS to increase the application's elasticity and availability.

The current architecture shows heavy read activity on the database during times of normal operation. Every 4 hours, the company's development team pulls a full export of the production database to populate a database in the staging environment. During this period, users experience unacceptable application latency. The development team is unable to use the staging environment until the procedure completes.

A solutions architect must recommend replacement architecture that alleviates the application latency issue. The replacement architecture also must give the development team the ability to continue using the staging environment without delay.

Which solution meets these requirements?

- A. Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production.
- B. Populate the staging database by implementing a backup and restore process that uses the mysqldump utility.
- C. Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production. Use database cloning to create the staging database on-demand.
- D. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas for production. Use the standby instance for the staging database.
- E. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas for production.
- F. Populate the staging database by implementing a backup and restore process that uses the mysqldump utility.

**Answer:** B

**Explanation:**

<https://aws.amazon.com/blogs/aws/amazon-aurora-fast-database-cloning/>

#### NEW QUESTION 6

- (Topic 1)

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

**Answer:** D

**Explanation:**

<https://aws.amazon.com/global-accelerator/faqs/>

HTTP /HTTPS - ALB ; TCP and UDP - NLB; Lowest latency routing and more throughput. Also supports failover, uses Anycast IP addressing - Global Accelerator Caching at Edge Locations – CloudFront

AWS Global Accelerator automatically checks the health of your applications and routes user traffic only to healthy application endpoints. If the health status changes or you make configuration updates, AWS Global Accelerator reacts instantaneously to route your users to the next available endpoint.

### NEW QUESTION 7

- (Topic 1)

A company's containerized application runs on an Amazon EC2 instance. The application needs to download security certificates before it can communicate with other business applications. The company wants a highly secure solution to encrypt and decrypt the certificates in near real time. The solution also needs to store data in highly available storage after the data is encrypted.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Create AWS Secrets Manager secrets for encrypted certificate
- B. Manually update the certificates as needed
- C. Control access to the data by using fine-grained IAM access.
- D. Create an AWS Lambda function that uses the Python cryptography library to receive and perform encryption operation
- E. Store the function in an Amazon S3 bucket.
- F. Create an AWS Key Management Service (AWS KMS) customer managed key
- G. Allow the EC2 role to use the KMS key for encryption operation
- H. Store the encrypted data on Amazon S3.
- I. Create an AWS Key Management Service (AWS KMS) customer managed key
- J. Allow the EC2 role to use the KMS key for encryption operation
- K. Store the encrypted data on Amazon Elastic Block Store (Amazon EBS) volumes.

**Answer:** D

### NEW QUESTION 8

- (Topic 1)

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 meets these requirements?

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

**Answer:** C

#### Explanation:

<https://www.quora.com/How-can-I-use-DynamoDB-for-storing-metadata-for-Amazon-S3-objects>

This 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.

References:

? <https://aws.amazon.com/certification/certified-solutions-architect-professional/>

? <https://www.examtips.com/discussions/amazon/view/7193-exam-aws-certified-solutions-architect-professional-topic-1/>

? <https://aws.amazon.com/architecture/>

### NEW QUESTION 9

- (Topic 1)

A company hosts a data lake on AWS. The data lake consists of data in Amazon S3 and Amazon RDS for PostgreSQL. The company needs a reporting solution that provides data visualization and includes all the data sources within the data lake. Only the company's management team should have full access to all the visualizations. The rest of the company should have only limited access.

Which solution will meet these requirements?

- A. Create an analysis in Amazon QuickSight
- B. Connect all the data sources and create new dataset
- C. Publish dashboards to visualize the data
- D. Share the dashboards with the appropriate IAM roles.
- E. Create an analysis in Amazon QuickSight
- F. Connect all the data sources and create new dataset
- G. Publish dashboards to visualize the data
- H. Share the dashboards with the appropriate users and groups.
- I. Create an AWS Glue table and crawler for the data in Amazon S3. Create an AWS Glue extract, transform, and load (ETL) job to produce report
- J. Publish the reports to Amazon S3. Use S3 bucket policies to limit access to the reports.
- K. Create an AWS Glue table and crawler for the data in Amazon S3. Use Amazon Athena Federated Query to access data within Amazon RDS for PostgreSQL
- L. Generate reports by using Amazon Athena
- M. Publish the reports to Amazon S3. Use S3 bucket policies to limit access to the reports.

**Answer:** B

#### Explanation:

Amazon QuickSight is a data visualization service that allows you to create interactive dashboards and reports from various data sources, including Amazon S3 and Amazon RDS for PostgreSQL. You can connect all the data sources and create new datasets in QuickSight, and then publish dashboards to visualize the



data. You can also share the dashboards with the appropriate users and groups, and control their access levels using IAM roles and permissions.  
Reference: <https://docs.aws.amazon.com/quicksight/latest/user/working-with-data-sources.html>

#### NEW QUESTION 10

- (Topic 1)

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

- A. Create an AWS Storage Gateway volume gateway.
- B. Create a file share that uses the required client protocol. Connect the application server to the file share.
- C. Create an AWS Storage Gateway tape gateway. Configure it to use Amazon S3. Connect the application server to the tape gateway.
- D. Create an Amazon EC2 Windows instance. Install and configure a Windows file share role on the instance.
- E. Connect the application server to the file share.
- F. Create an Amazon FSx for Windows File Server file system. Attach the file system to the origin server.
- G. Connect the application server to the file system.

**Answer:** D

#### Explanation:

<https://aws.amazon.com/fsx/lustre/>

Amazon FSx has native support for Windows file system features and for the industry-standard Server Message Block (SMB) protocol to access file storage over a network. <https://docs.aws.amazon.com/fsx/latest/WindowsGuide/what-is.html>

#### NEW QUESTION 10

- (Topic 1)

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.
- B. Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source.
- C. Use AWS Lambda functions to transform the data.
- D. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.
- E. Deploy an Amazon EC2 instance to host an API that sends data to AWS Glue.
- F. Stop source/destination checking on the EC2 instance.
- G. Use AWS Glue to transform the data and to send the data to Amazon S3.
- H. Configure an Amazon API Gateway API to send data to an Amazon Kinesis data stream.
- I. Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source.
- J. Use AWS Lambda functions to transform the data.
- K. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.
- L. Configure an Amazon API Gateway API to send data to AWS Glue.
- M. Use AWS Lambda functions to transform the data.
- N. Use AWS Glue to send the data to Amazon S3.

**Answer:** C

#### NEW QUESTION 14

- (Topic 1)

A company has an Amazon S3 bucket that contains critical data. 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.

**Answer:** AB

#### 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>

#### NEW QUESTION 17

- (Topic 1)

A company's dynamic website is hosted using on-premises servers in the United States. The company is launching its product in Europe, and it wants to optimize site loading times for new European users. The site's backend must remain in the United States. The product is being launched in a few days, and an immediate solution is needed.  
What should the solutions architect recommend?

- A. Launch an Amazon EC2 instance in us-east-1 and migrate the site to it.
- B. Move the website to Amazon S3. Use cross-Region replication between Regions.
- C. Use Amazon CloudFront with a custom origin pointing to the on-premises servers.

D. Use an Amazon Route 53 geo-proximity routing policy pointing to on-premises servers.

**Answer:** C

**Explanation:**

<https://aws.amazon.com/pt/blogs/aws/amazon-cloudfront-support-for-custom-origins/>

You can now create a CloudFront distribution using a custom origin. Each distribution will can point to an S3 or to a custom origin. This could be another storage service, or it could be something more interesting and more dynamic, such as an EC2 instance or even an Elastic Load Balancer

#### NEW QUESTION 19

- (Topic 1)

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
- C. Tag those resources manually.
- D. Write API calls to check all resources for proper tag allocation
- E. Periodically run the code on an EC2 instance.
- F. Write API calls to check all resources for proper tag allocation
- G. Schedule an AWS Lambda function through Amazon CloudWatch to periodically run the code.

**Answer:** A

**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](https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_use-managed-rules.html))

#### NEW QUESTION 21

- (Topic 1)

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
- B. 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.
- C. Store the database credentials in a configuration file in an encrypted Amazon S3 bucket
- D. 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
- E. Use S3 Versioning to ensure the ability to fall back to previous values.
- F. Store the database credentials as a secret in AWS Secrets Manager
- G. Turn on automatic rotation for the secret
- H. Attach the required permission to the EC2 role to grant access to the secret.
- I. Store the database credentials as encrypted parameters in AWS Systems Manager Parameter Store
- J. Turn on automatic rotation for the encrypted parameter
- K. Attach the required permission to the EC2 role to grant access to the encrypted parameters.

**Answer:** C

**Explanation:**

[https://docs.aws.amazon.com/secretsmanager/latest/userguide/create\\_database\\_secret.html](https://docs.aws.amazon.com/secretsmanager/latest/userguide/create_database_secret.html)

#### NEW QUESTION 23

- (Topic 1)

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
- E. Use the function to resize the image
- F. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function on a schedule to resize uploaded images.

**Answer:** CD

**Explanation:**

Amazon S3 is a highly scalable and durable object storage service that can store and retrieve any amount of data from anywhere on the web<sup>1</sup>. 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 URL is 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 object<sup>2</sup>. 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 automatically manages the underlying compute resources<sup>3</sup>. 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.

#### NEW QUESTION 28

- (Topic 1)

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 on-premises 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-time 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

**Answer:** B

#### 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/>

#### NEW QUESTION 32

- (Topic 1)

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

**Answer:** D

#### Explanation:

<https://aws.amazon.com/solutions/implementations/aws-streaming-data-solution-for-amazon-kinesis/>

#### NEW QUESTION 33

- (Topic 1)

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

**Answer:** C

#### 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 addresses 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](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html#VPCSecurityGroups)

#### NEW QUESTION 36

- (Topic 1)

An application development team is designing a microservice that will convert large images to smaller, compressed images. When a user uploads an image through the web interface, the microservice should store the image in an Amazon S3 bucket, process and compress the image with an AWS Lambda function, and store the image in its compressed form in a different S3 bucket.

A solutions architect needs to design a solution that uses durable, stateless components to process the images automatically.

Which combination of actions will meet these requirements? (Choose two.)

- A. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure the S3 bucket to send a notification to the SQS queue when an image is uploaded to the S3 bucket.
- B. Configure the Lambda function to use the Amazon Simple Queue Service (Amazon SQS) queue as the invocation source. When the SQS message is



successfully processed, delete the message in the queue

- C. Configure the Lambda function to monitor the S3 bucket for new uploads When an uploaded image is detected write the file name to a text file in memory and use the text file to keep track of the images that were processed
- D. Launch an Amazon EC2 instance to monitor an Amazon Simple Queue Service(Amazon SQS) queue When items are added to the queue log the file name in a text file on the EC2 instance and invoke the Lambda function
- E. Configure an Amazon EventBridge (Amazon CloudWatch Events) event to monitor the S3 bucket When an image is uploaded
- F. send an alert to an Amazon Simple Notification Service (Amazon SNS) topic with the application owner's email address for further processing

**Answer:** AB

**Explanation:**

? Creating an Amazon Simple Queue Service (SQS) queue and configuring the S3 bucket to send a notification to the SQS queue when an image is uploaded to the S3 bucket will ensure that the Lambda function is triggered in a stateless and durable manner.

? Configuring the Lambda function to use the SQS queue as the invocation source, and deleting the message in the queue after it is successfully processed will ensure that the Lambda function processes the image in a stateless and durable manner.

Amazon SQS is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating-message oriented middleware, and empowers developers to focus on differentiating work. When new images are uploaded to the S3 bucket, SQS will trigger the Lambda function to process the image and compress it. Once the image is processed, the SQS message is deleted, ensuring that the Lambda function is stateless and durable.

**NEW QUESTION 38**

- (Topic 1)

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
- B. 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.
- C. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console
- D. 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.
- E. Use AWS Directory Service
- F. Create a two-way trust relationship with the company's self- managed Microsoft Active Directory.
- G. Deploy an identity provider (IdP) on premise
- H. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console.

**Answer:** A

**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

**NEW QUESTION 40**

- (Topic 1)

An application allows users at a company's headquarters to access product data. The product data is stored in an Amazon RDS MySQL DB instance. The operations team has isolated an application performance slowdown and wants to separate read traffic from write traffic. A solutions architect needs to optimize the application's performance quickly.

What should the solutions architect recommend?

- A. Change the existing database to a Multi-AZ deployment
- B. Serve the read requests from the primary Availability Zone.
- C. Change the existing database to a Multi-AZ deployment
- D. Serve the read requests from the secondary Availability Zone.
- E. Create read replicas for the database
- F. Configure the read replicas with half of the compute and storage resources as the source database.
- G. Create read replicas for the database
- H. Configure the read replicas with the same compute and storage resources as the source database.

**Answer:** D

**Explanation:**

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_MySQL.Replication.ReadReplicas.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_MySQL.Replication.ReadReplicas.html)

**NEW QUESTION 41**

- (Topic 1)

A company has a production web application in which users upload documents through a web interface or a mobile app. According to a new regulatory requirement, new documents cannot be modified or deleted after they are stored.

What should a solutions architect do to meet this requirement?

- A. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning and S3 Object Lock enabled
- B. Store the uploaded documents in an Amazon S3 bucket
- C. Configure an S3 Lifecycle policy to archive the documents periodically.
- D. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning enabled Configure an ACL to restrict all access to read-only.
- E. Store the uploaded documents on an Amazon Elastic File System (Amazon EFS) volume
- F. Access the data by mounting the volume in read-only mode.



**Answer:** A

**Explanation:**

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html>

**NEW QUESTION 42**

- (Topic 1)

A company wants to reduce the cost of its existing three-tier web architecture. The web, application, and database servers are running on Amazon EC2 instances for the development, test, and production environments. The EC2 instances average 30% CPU utilization during peak hours and 10% CPU utilization during non-peak hours.

The production EC2 instances run 24 hours a day. The development and test EC2 instances run for at least 8 hours each day. The company plans to implement automation to stop the development and test EC2 instances when they are not in use.

Which EC2 instance purchasing solution will meet the company's requirements MOST cost-effectively?

- A. Use Spot Instances for the production EC2 instance
- B. Use Reserved Instances for the development and test EC2 instances.
- C. Use Reserved Instances for the production EC2 instance
- D. Use On-Demand Instances for the development and test EC2 instances.
- E. Use Spot blocks for the production EC2 instance
- F. Use Reserved Instances for the development and test EC2 instances.
- G. Use On-Demand Instances for the production EC2 instance
- H. Use Spot blocks for the development and test EC2 instances.

**Answer:** B

**NEW QUESTION 45**

- (Topic 2)

A company produces batch data that comes from different databases. The company also produces live stream data from network sensors and application APIs.

The company needs to consolidate all the data into one place for business analytics. The company needs to process the incoming data and then stage the data in different Amazon S3 buckets. Teams will later run one-time queries and import the data into a business intelligence tool to show key performance indicators (KPIs).

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose two.)

- A. Use Amazon Athena for one-time queries Use Amazon QuickSight to create dashboards for KPIs
- B. Use Amazon Kinesis Data Analytics for one-time queries Use Amazon QuickSight to create dashboards for KPIs
- C. Create custom AWS Lambda functions to move the individual records from the databases to an Amazon Redshift cluster
- D. Use an AWS Glue extract, transform, and load (ETL) job to convert the data into JSON format Load the data into multiple Amazon OpenSearch Service (Amazon Elasticsearch Service) clusters
- E. Use blueprints in AWS Lake Formation to identify the data that can be ingested into a data lake Use AWS Glue to crawl the source extract the data and load the data into Amazon S3 in Apache Parquet format

**Answer:** AE

**Explanation:**

Amazon Athena is the best choice for running one-time queries on streaming data. Although Amazon Kinesis Data Analytics provides an easy and familiar standard SQL language to analyze streaming data in real-time, it is designed for continuous queries rather than one-time queries[1]. On the other hand, Amazon Athena is a serverless interactive query service that allows querying data in Amazon S3 using SQL. It is optimized for ad-hoc querying and is ideal for running one-time queries on streaming data[2]. AWS Lake Formation uses as a central place to have all your data for analytics purposes (E). Athena integrates perfectly with S3 and can make queries (A).

**NEW QUESTION 46**

- (Topic 2)

A company is migrating its on-premises PostgreSQL database to Amazon Aurora PostgreSQL. The on-premises 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

**Answer:** AC

**Explanation:**

AWS Database Migration Service supports homogeneous migrations such as Oracle to Oracle, as well as heterogeneous migrations between different database platforms, such as Oracle or Microsoft SQL Server to Amazon Aurora. With AWS Database Migration Service, you can also continuously replicate data with low latency from any supported source to any supported target. For example, you can replicate from multiple sources to Amazon Simple Storage Service (Amazon S3) to build a highly available and scalable data lake solution. You can also consolidate databases into a petabyte-scale data warehouse by streaming data to Amazon Redshift. Learn more about the supported source and target databases. <https://aws.amazon.com/dms/>

**NEW QUESTION 51**

- (Topic 2)

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.

**Answer:** D

**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](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html).

**NEW QUESTION 53**

- (Topic 2)

A company has an ecommerce checkout workflow that writes an order to a database and calls a service to process the payment. Users are experiencing timeouts during the checkout process. When users resubmit the checkout form, multiple unique orders are created for the same desired transaction. How should a solutions architect refactor this workflow to prevent the creation of multiple orders?

- A. Configure the web application to send an order message to Amazon Kinesis Data Firehose
- B. Set the payment service to retrieve the message from Kinesis Data Firehose and process the order.
- C. Create a rule in AWS CloudTrail to invoke an AWS Lambda function based on the logged application path request Use Lambda to query the database, call the payment service, and pass in the order information.
- D. Store the order in the database
- E. Send a message that includes the order number to Amazon Simple Notification Service (Amazon SNS). Set the payment service to poll Amazon SNS
- F. retrieve the message, and process the order.
- G. Store the order in the database
- H. Send a message that includes the order number to an Amazon Simple Queue Service (Amazon SQS) FIFO queue
- I. Set the payment service to retrieve the message and process the order
- J. Delete the message from the queue.

**Answer:** D

**Explanation:**

This approach ensures that the order creation and payment processing steps are separate and atomic. By sending the order information to an SQS FIFO queue, the payment service can process the order one at a time and in the order they were received. If the payment service is unable to process an order, it can be retried later, preventing the creation of multiple orders. The deletion of the message from the queue after it is processed will prevent the same message from being processed multiple times.

**NEW QUESTION 56**

- (Topic 2)

A new employee has joined a company as a deployment engineer. The deployment engineer will be using AWS CloudFormation templates to create multiple AWS resources. A solutions architect wants the deployment engineer to perform job activities while following the principle of least privilege. Which steps should the solutions architect do in conjunction to reach this goal? (Select two.)

- A. Have the deployment engineer use AWS account root user credentials for performing AWS CloudFormation stack operations.
- B. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the PowerUsers IAM policy attached.
- C. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the Administrate/Access IAM policy attached.
- D. Create a new IAM User for the deployment engineer and add the IAM user to a group that has an IAM policy that allows AWS CloudFormation actions only.
- E. Create an IAM role for the deployment engineer to explicitly define the permissions specific to the AWS CloudFormation stack and launch stacks using the IAM role.

**Answer:** DE

**Explanation:**

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html) [https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_users.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html)

**NEW QUESTION 58**

- (Topic 2)

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
- C. Route the traffic from the Lambda function through the VPN.
- D. Update the route tables in the VPC to allow the Lambda function to access the on-premises data center through Direct Connect.
- E. Create an Elastic IP address
- F. Configure the Lambda function to send traffic through the Elastic IP address without an elastic network interface.

**Answer:** A

**Explanation:**

<https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html#vpc-managing-eni>

**NEW QUESTION 62**

- (Topic 2)

A company has an event-driven application that invokes AWS Lambda functions up to 800 times each minute with varying runtimes. The Lambda functions access

data that is stored in an Amazon Aurora MySQL OB cluster. The company is noticing connection timeouts as user activity increases. The database shows no signs of being overloaded. CPU, memory, and disk access metrics are all low. Which solution will resolve this issue with the LEAST operational overhead?

- A. Adjust the size of the Aurora MySQL nodes to handle more connection
- B. Configure retry logic in the Lambda functions for attempts to connect to the database
- C. Set up Amazon ElastiCache for Redis to cache commonly read items from the database
- D. Configure the Lambda functions to connect to ElastiCache for reads.
- E. Add an Aurora Replica as a reader node
- F. Configure the Lambda functions to connect to the reader endpoint of the OB cluster rather than to the writer endpoint.
- G. Use Amazon ROS Proxy to create a proxy
- H. Set the DB cluster as the target database. Configure the Lambda functions to connect to the proxy rather than to the DB cluster.

**Answer: D**

**Explanation:**

1. database shows no signs of being overloaded. CPU, memory, and disk access metrics are all low ==> A and C out. We cannot only add nodes instance or add read replica, because database workload is totally fine, very low. 2. "least operational overhead" ==> B out, because B needs to configure lambda. 3. ROS proxy: Shares infrequently used connections; High availability with failover; Drives increased efficiency ==> proxy can leverage failover to redirect traffic from timeout RDS instance to healthy RDS instance. So D is right.

**NEW QUESTION 66**

- (Topic 2)

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.

**Answer: B**

**Explanation:**

ElastiCache enhances the performance of web applications by quickly retrieving information from fully-managed in-memory data stores. It utilizes Memcached and Redis, and manages to considerably reduce the time your applications would, otherwise, take to read data from disk-based databases. Amazon CloudFront supports dynamic content from HTTP and WebSocket protocols, which are based on the Transmission Control Protocol (TCP) protocol. Common use cases include dynamic API calls, web pages and web applications, as well as an application's static files such as audio and images. It also supports on-demand media streaming over HTTP. AWS Global Accelerator supports both User Datagram Protocol (UDP) and TCP-based protocols. It is commonly used for non-HTTP use cases, such as gaming, IoT and voice over IP. It is also good for HTTP use cases that need static IP addresses or fast regional failover.

**NEW QUESTION 68**

- (Topic 2)

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
- C. Use the log group to invoke the function to write the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).
- D. Create an Amazon Kinesis Data Firehose delivery stream
- E. Configure the log group as the delivery stream's source
- F. Configure Amazon OpenSearch Service (Amazon Elasticsearch Service) as the delivery stream's destination.
- G. Install and configure Amazon Kinesis Agent on each application server to deliver the logs to Amazon Kinesis Data Stream
- H. Configure Kinesis Data Streams to deliver the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service)

**Answer: B**

**Explanation:**

<https://computingforgeeks.com/stream-logs-in-aws-from-cloudwatch-to-elasticsearch/>

**NEW QUESTION 70**

- (Topic 2)

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 WAF.

How should the solutions architect comply with these requirements?

- A. Configure an S3 bucket policy to 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.
- D. Associate AWS WAF to CloudFront.
- E. Configure Amazon CloudFront and Amazon S3 to use an origin access identity (OAI) to restrict access to the S3 bucket.
- F. Enable AWS WAF on the distribution.

**Answer: D**



**Explanation:**

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html>  
<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-aws-waf.html>

**NEW QUESTION 75**

- (Topic 2)

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 alert
- C. Configure AWS account alternate contacts in the AWS Organizations console or programmatically.
- D. 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.
- E. Configure all existing AWS accounts and all newly created accounts to use the same root user email address
- F. Configure AWS account alternate contacts in the AWS Organizations console or programmatically.

**Answer: B**

**Explanation:**

Use a group email address for the management account's root user [https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_best-practices\\_mgmt-acct.html#best-practices\\_mgmt-acct\\_email-address](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_best-practices_mgmt-acct.html#best-practices_mgmt-acct_email-address)

**NEW QUESTION 78**

- (Topic 2)

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

**Answer: C**

**Explanation:**

<https://aws.amazon.com/blogs/compute/building-loosely-coupled-scalable-c-applications-with-amazon-sqs-and-amazon-sns/>  
<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letter-queues.html>

**NEW QUESTION 83**

- (Topic 2)

A gaming company has a web application that displays scores. The application runs on Amazon EC2 instances behind an Application Load Balancer. The application stores data in an Amazon RDS for MySQL database. Users are starting to experience long delays and interruptions that are caused by database read performance. The company wants to improve the user experience while minimizing changes to the application's architecture. What should a solutions architect do to meet these requirements?

- A. Use Amazon ElastiCache in front of the database.
- B. Use RDS Proxy between the application and the database.
- C. Migrate the application from EC2 instances to AWS Lambda.
- D. Migrate the database from Amazon RDS for MySQL to Amazon DynamoDB.

**Answer: A**

**Explanation:**

ElastiCache can help speed up the read performance of the database by caching frequently accessed data, reducing latency and allowing the application to access the data more quickly. This solution requires minimal modifications to the current architecture, as ElastiCache can be used in conjunction with the existing Amazon RDS for MySQL database.

**NEW QUESTION 88**

- (Topic 2)

A company has a service that produces event data. 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.



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

**Answer:** A

**Explanation:**

The details are revealed in below url: [https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO- queues.html](https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.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.

**NEW QUESTION 89**

- (Topic 2)

A business's backup data totals 700 terabytes (TB) and is kept in network attached storage (NAS) at its data center. This backup data must be available in the event of occasional regulatory inquiries and preserved for a period of seven years. The organization has chosen to relocate its backup data from its on-premises data center to Amazon Web Services (AWS). Within one month, the migration must be completed. The company's public internet connection provides 500 Mbps of dedicated capacity for data transport.

What should a solutions architect do to ensure that data is migrated and stored at the LOWEST possible cost?

- A. Order AWS Snowball devices to transfer the dat
- B. Use a lifecycle policy to transition the files to Amazon S3 Glacier Deep Archive.
- C. Deploy a VPN connection between the data center and Amazon VP
- D. Use the AWS CLI to copy the data from on premises to Amazon S3 Glacier.
- E. Provision a 500 Mbps AWS Direct Connect connection and transfer the data to Amazon S3. Use a lifecycle policy to transition the files to Amazon S3 Glacier Deep Archive.
- F. Use AWS DataSync to transfer the data and deploy a DataSync agent on premise
- G. Use the DataSync task to copy files from the on-premises NAS storage to Amazon S3 Glacier.

**Answer:** A

**Explanation:**

<https://www.omnicalculator.com/other/data-transfer>

**NEW QUESTION 94**

- (Topic 2)

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

**Answer:** D

**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."

**NEW QUESTION 99**

- (Topic 2)

A company's application Is having performance issues The application staleful and needs to complete m-memory tasks on Amazon EC2 instances. The company used AWS CloudFormation to deploy infrastructure and used the M5 EC2 Instance family As traffic increased, the application performance degraded Users are reporting delays when the users attempt to access the application.

Which solution will resolve these issues in the MOST operationally efficient way?

- A. Replace the EC2 Instances with T3 EC2 instances that run in an Auto Scaling grou
- B. Made the changes by using the AWS Management Console.
- C. Modify the CloudFormation templates to run the EC2 instances in an Auto Scaling grou
- D. Increase the desired capacity and the maximum capacity of the Auto Scaling group manually when an increase is necessary
- E. Modify the CloudFormation template
- F. Replace the EC2 instances with R5 EC2 instance
- G. Use Amazon CloudWatch built-in EC2 memory metrics to track the application performance for future capacity planning.
- H. Modify the CloudFormation template
- I. Replace the EC2 instances with R5 EC2 instance
- J. Deploy the Amazon CloudWatch agent on the EC2 instances to generate custom application latency metrics for future capacity planning.

**Answer:** D

**Explanation:**

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudwatch-memory-metrics-ec2/>

#### NEW QUESTION 104

- (Topic 2)

A company runs a global web application on Amazon EC2 instances behind an Application Load Balancer. The application stores data in Amazon Aurora. The company needs to create a disaster recovery solution and can tolerate up to 30 minutes of downtime and potential data loss. The solution does not need to handle the load when the primary infrastructure is healthy.

What should a solutions architect do to meet these requirements?

- A. Deploy the application with the required infrastructure elements in place. Use Amazon Route 53 to configure active-passive failover. Create an Aurora Replica in a second AWS Region.
- B. Host a scaled-down deployment of the application in a second AWS Region. Use Amazon Route 53 to configure active-active failover. Create an Aurora Replica in the second Region.
- C. Replicate the primary infrastructure in a second AWS Region. Use Amazon Route 53 to configure active-active failover. Create an Aurora database that is restored from the latest snapshot.
- D. Back up data with AWS Backup. Use the backup to create the required infrastructure in a second AWS Region. Use Amazon Route 53 to configure active-passive failover. Create an Aurora second primary instance in the second Region.

**Answer:** A

#### Explanation:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html>

#### NEW QUESTION 105

- (Topic 2)

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

**Answer:** A

#### Explanation:

(<https://aws.amazon.com/blogs/security/how-to-restrict-amazon-s3-bucket-access-to-a-specific-iam-role/>)

#### NEW QUESTION 110

- (Topic 2)

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

**Answer:** A

#### Explanation:

Cloudfront for rapid response and s3 to minimize infrastructure.

#### NEW QUESTION 113

- (Topic 2)

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).

**Answer:** AE

#### Explanation:

Amazon Aurora is a fully managed, scalable, and highly available relational database service that is compatible with PostgreSQL. Migrating the database to Amazon Aurora would reduce the operational overhead of maintaining the database infrastructure and allow the company to focus on building and scaling the application. AWS Fargate is a fully managed container orchestration service that enables users to run containers without the need to manage the underlying EC2

instances. By using AWS Fargate with Amazon Elastic Container Service (Amazon ECS), the solutions architect can improve the scalability and efficiency of the web application and reduce the operational overhead of maintaining the underlying infrastructure.

#### NEW QUESTION 117

- (Topic 3)

A company is migrating an old application to AWS. The application runs a batch job every hour and is CPU intensive. The batch job takes 15 minutes on average with an on-premises server. The server has 64 virtual CPU (vCPU) and 512 GiB of memory. Which solution will run the batch job within 15 minutes with the LEAST operational overhead?

- A. Use AWS Lambda with functional scaling
- B. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate
- C. Use Amazon Lightsail with AWS Auto Scaling
- D. Use AWS Batch on Amazon EC2

**Answer:** D

#### Explanation:

Use AWS Batch on Amazon EC2. AWS Batch is a fully managed batch processing service that can be used to easily run batch jobs on Amazon EC2 instances. It can scale the number of instances to match the workload, allowing the batch job to be completed in the desired time frame with minimal operational overhead. Using AWS Lambda with Amazon API Gateway - AWS Lambda <https://docs.aws.amazon.com/lambda/latest/dg/services-apigateway.html>  
AWS Lambda FAQs <https://aws.amazon.com/lambda/faqs/>

#### NEW QUESTION 121

- (Topic 3)

A company will deploy 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 scaling needs. The read replicas must log 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 experience additional lag during periods of peak load. A solutions architect must reduce the replication lag as much as possible. The solutions architect must minimize changes to the application code and must minimize ongoing overhead.

Which solution will meet these requirements?

Migrate the database to Amazon Aurora MySQL. Replace the read replicas with Aurora Replicas, and configure Aurora Auto Scaling. Replace the stored procedures with Aurora MySQL native functions.

Deploy an Amazon ElastiCache for Redis cluster in front of the database. Modify the application to check the cache before the application queries the database. Replace the stored procedures with AWS Lambda functions.

- A. Migrate the database to a MySQL database that runs on Amazon EC2 instance
- B. Choose large, compute optimized for all replica nodes
- C. Maintain the stored procedures on the EC2 instances.
- D. Deploy an Amazon ElastiCache for Redis cluster in front of the database
- E. Modify the application to check the cache before the application queries the database
- F. Replace the stored procedures with AWS Lambda functions.
- G. Migrate the database to a MySQL database that runs on Amazon EC2 instance
- H. Choose large, compute optimized EC2 instances for all replica nodes. Maintain the stored procedures on the EC2 instances.
- I. Migrate the database to Amazon DynamoDB, Provision number of read capacity units (RCUs) to support the required throughput, and configure on-demand capacity scaling
- J. Replace the stored procedures with DynamoDB streams.

**Answer:** A

#### Explanation:

Option A is the most appropriate solution for reducing replication lag without significant changes to the application code and minimizing ongoing operational overhead. Migrating the database to Amazon Aurora MySQL allows for improved replication performance and higher scalability compared to Amazon RDS for MySQL. Aurora Replicas provide faster replication, reducing the replication lag, and Aurora Auto Scaling ensures that there are enough Aurora Replicas to handle the incoming traffic. Additionally, Aurora MySQL native functions can replace the stored procedures, reducing the load on the database and improving performance.

#### NEW QUESTION 125

- (Topic 3)

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
- D. Configure all other instances to allow only SSH access from the bastion instances
- E. Use an Amazon Cognito custom authorizer to authenticate user
- F. Invoke an AWS Lambda function to generate a temporary SSH key.

**Answer:** A

#### 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>



#### NEW QUESTION 126

- (Topic 3)

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

**Answer:** D

#### Explanation:

• Amazon S3 for large-scale, durable, and inexpensive storage of the video content. S3 storage costs are significantly lower than EFS. • Amazon EBS only temporarily during processing. By mounting an EBS volume only when a video needs to be processed, and unmounting it after, the time the content spends on the higher-cost EBS storage is minimized. • The EBS volume can be sized to match the workload needs for active processing, keeping costs lower. The volume does not need to store the entire video library long-term.

#### NEW QUESTION 131

- (Topic 3)

A company is using Amazon Route 53 latency-based routing to route requests to its UDP-based application for users around the world. The application is hosted on redundant servers in the company's on-premises data centers in the United States, Asia, and Europe. The company's compliance requirements state that the application must be hosted on premises. The company wants to improve the performance and availability of the application.

What should a solutions architect do to meet these requirements?

- A. A. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator, and register the NLBs as its endpoint.
- B. Provide access to the application by using a CNAME that points to the accelerator DNS.
- C. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoint.
- D. Create an accelerator by using AWS Global Accelerator and register the ALBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.
- E. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three NLBs.
- F. and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.
- G. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three ALBs and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.

**Answer:** A

#### Explanation:

[https://aws.amazon.com/step-functions/#:~:text=AWS%20Step%20Functions%20is%20a,machine%20learning%20\(ML\)%20pipelines](https://aws.amazon.com/step-functions/#:~:text=AWS%20Step%20Functions%20is%20a,machine%20learning%20(ML)%20pipelines).

"A common use case for AWS Step Functions is a task that requires human intervention (for example, an approval process). Step Functions makes it easy to coordinate the components of distributed applications as a series of steps in a visual workflow called a state machine. You can quickly build and run state machines to execute the steps of your application in a reliable and scalable fashion. (<https://aws.amazon.com/pt/blogs/compute/implementing-serverless-manual-approval-steps-in-aws-step-functions-and-amazon-api-gateway/>)"

#### NEW QUESTION 135

- (Topic 3)

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 scaling metric.

**Answer:** AD

#### 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\\_PIOPS.Autoscaling](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PIOPS.StorageTypes.html#USER_PIOPS.Autoscaling)

#### NEW QUESTION 140

- (Topic 3)

A company has an application that runs on several Amazon EC2 instances. Each EC2 instance has multiple Amazon Elastic Block Store (Amazon EBS) data volumes attached to it. The application's EC2 instance configuration and data need to be backed up nightly. The application also needs to be recoverable in a different AWS Region.

Which solution will meet these requirements in the MOST operationally efficient way?

- A. Write an AWS Lambda function that schedules nightly snapshots of the application's EBS volumes and copies the snapshots to a different Region.



- B. Create a backup plan by using AWS Backup to perform nightly backup
- C. Copy the backups to another Region Add the application's EC2 instances as resources
- D. Create a backup plan by using AWS Backup to perform nightly backups Copy the backups to another Region Add the application's EBS volumes as resources
- E. Write an AWS Lambda function that schedules nightly snapshots of the application's EBS volumes and copies the snapshots to a different Availability Zone

**Answer:** B

**Explanation:**

The most operationally efficient solution to meet these requirements would be to create a backup plan by using AWS Backup to perform nightly backups and copying the backups to another Region. Adding the application's EBS volumes as resources will ensure that the application's EC2 instance configuration and data are backed up, and copying the backups to another Region will ensure that the application is recoverable in a different AWS Region.

**NEW QUESTION 144**

- (Topic 3)

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 CloudFront 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 all 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 all 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

**Answer:** A

**Explanation:**

Key phrase in the Question is must scale read and write capacity. Aurora is only for Read. Amazon DynamoDB has two read/write capacity modes for processing reads and writes on your tables: On-demand Provisioned (default, free-tier eligible)

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.html>

**NEW QUESTION 145**

- (Topic 3)

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 in 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 in 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

**Answer:** B

**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.

**NEW QUESTION 146**

- (Topic 3)

A company sells datasets to customers who do research in artificial intelligence and machine learning (AI/ML) The datasets are large, formatted files that are stored in an Amazon S3 bucket in the us-east-1 Region The company hosts a web application that the customers use to purchase access to a given dataset The web application is deployed on multiple Amazon EC2 instances behind an Application Load Balancer After a purchase is made customers receive an S3 signed URL that allows access to the files.

The customers are distributed across North America and Europe The company wants to reduce the cost that is associated with data transfers and wants to maintain or improve performance.

What should a solutions architect do to meet these requirements?

- A. Configure S3 Transfer Acceleration on the existing S3 bucket Direct customer requests to the S3 Transfer Acceleration endpoint Continue to use S3 signed URLs for access control
- B. Deploy an Amazon CloudFront distribution with the existing S3 bucket as the origin Direct customer requests to the CloudFront URL Switch to CloudFront signed URLs for access control
- C. Set up a second S3 bucket in the eu-central-1 Region with S3 Cross-Region Replication between the buckets Direct customer requests to the closest Region Continue to use S3 signed URLs for access control
- D. Modify the web application to enable streaming of the datasets to end user
- E. Configure the web application to read the data from the existing S3 bucket Implement access control directly in the application

**Answer:** B

**Explanation:**

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html>

#### NEW QUESTION 149

- (Topic 3)

A company runs a public three-Tier web application in a VPC. The application runs on Amazon EC2 instances across multiple Availability Zones. The EC2 instances that run in private subnets need to communicate with a license server over the internet. The company needs a managed solution that minimizes operational maintenance.

Which solution meets these requirements?

- A. Provision a NAT instance in a public subnet. Modify each private subnet's route table with a default route that points to the NAT instance.
- B. Provision a NAT instance in a private subnet. Modify each private subnet's route table with a default route that points to the NAT instance.
- C. Provision a NAT gateway in a public subnet. Modify each private subnet's route table with a default route that points to the NAT gateway.
- D. Provision a NAT gateway in a private subnet. Modify each private subnet's route table with a default route that points to the NAT gateway.

**Answer: C**

#### Explanation:

A NAT gateway is a type of network address translation (NAT) device that enables instances in a private subnet to connect to the internet or other AWS services, but prevents the internet from initiating connections with those instances<sup>1</sup>. A NAT gateway is a managed service that requires minimal operational maintenance and can handle up to 45 Gbps of bursty traffic<sup>1</sup>. A NAT gateway is suitable for scenarios where EC2 instances in private subnets need to communicate with a license server over the internet, such as the three-tier web application in the scenario<sup>1</sup>.

To meet the requirements of the scenario, the solutions architect should provision a NAT gateway in a public subnet. The solutions architect should also modify each private subnet's route table with a default route that points to the NAT gateway<sup>1</sup>. This way, the EC2 instances that run in private subnets can access the license server over the internet through the NAT gateway.

#### NEW QUESTION 154

- (Topic 3)

An IAM user made several configuration changes to AWS resources in 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

**Answer: C**

#### Explanation:

The best option is to use AWS CloudTrail to find the desired information. AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of AWS account activities. CloudTrail can be used to log all changes made to resources in an AWS account, including changes made by IAM users, EC2 instances, AWS management console, and other AWS services. By using CloudTrail, the solutions architect can identify the IAM user who made the configuration changes to the security group rules.

#### NEW QUESTION 155

- (Topic 3)

A company has a three-tier application on AWS that ingests sensor data from its users' devices. The traffic flows through a Network Load Balancer (NLB) then to Amazon EC2 instances for the web tier and finally to EC2 instances for the application tier. The application tier makes calls to a database.

What should a solutions architect do to improve the security of the data in transit?

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

**Answer: A**

#### Explanation:

The best option to improve the security of the data in transit is to configure a TLS listener and deploy the server certificate on the NLB. This will ensure that the data is encrypted and secure as it travels through the network. Additionally, you could also configure AWS Shield Advanced and enable AWS WAF on the NLB to further protect the network from malicious attacks. Alternatively, you could also change the load balancer to an Application Load Balancer (ALB) and enable AWS WAF on the ALB. Finally, you could also encrypt the Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instances by using AWS Key Management Service (AWS KMS).

You must specify an SSL certificate for a TLS listener. The load balancer uses the certificate to terminate the connection and decrypt requests from clients before routing them to targets. <https://docs.aws.amazon.com/elasticloadbalancing/latest/network/create-listener.html>

#### NEW QUESTION 160

- (Topic 3)

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 data. The company also needs to receive monthly email messages if any financial information is present in the employee data.

Which combination of steps should a solutions architect take to meet these requirements? (Select TWO.)

- A. Use Amazon Redshift to store the employee data in a hierarchy.
- B. Upload the data to Amazon S3 every month.
- C. Use Amazon DynamoDB to store the employee data in a hierarchy. Export the data to Amazon S3 every month.
- D. Configure Amazon Macie for the AWS account. Integrate Macie with Amazon EventBridge to send monthly events to AWS Lambda.
- E. 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.
- F. Configure Amazon Macie for the AWS account.

G. integrate Macie with Amazon EventBridge to send monthly notifications through an Amazon Simple Notification Service (Amazon SNS) subscription.

**Answer:** BE

**Explanation:**

<https://docs.aws.amazon.com/prescriptive-guidance/latest/dynamodb-hierarchical-data-model/introduction.html>

#### NEW QUESTION 161

- (Topic 3)

A company has a web server running on an Amazon EC2 instance in a public subnet with an Elastic IP address. The default security group is assigned to the EC2 instance. The default network ACL has been modified to block all traffic. A solutions architect needs to make the web server accessible from everywhere on port 443.

Which combination of steps will accomplish this task? (Choose two.)

- A. Create a security group with a rule to allow TCP port 443 from source 0.0.0.0/0.
- B. Create a security group with a rule to allow TCP port 443 to destination 0.0.0.0/0.
- C. Update the network ACL to allow TCP port 443 from source 0.0.0.0/0.
- D. Update the network ACL to allow inbound/outbound TCP port 443 from source 0.0.0.0/0 and to destination 0.0.0.0/0.
- E. Update the network ACL to allow inbound TCP port 443 from source 0.0.0.0/0 and outbound TCP port 32768-65535 to destination 0.0.0.0/0.

**Answer:** AC

**Explanation:**

The combination of steps that will accomplish the task of making the web server accessible from everywhere on port 443 is to create a security group with a rule to allow TCP port 443 from source 0.0.0.0/0 (A) and to update the network ACL to allow inbound TCP port 443 from source 0.0.0.0/0 (C). This will ensure that traffic to port 443 is allowed both at the security group level and at the network ACL level, which will make the web server accessible from everywhere on port 443.

#### NEW QUESTION 164

- (Topic 3)

A research laboratory needs to process approximately 8 TB of data. The laboratory requires sub-millisecond latencies and a minimum throughput of 6 GBps for the storage subsystem. Hundreds of Amazon EC2 instances that run Amazon Linux will distribute and process the data.

Which solution will meet the performance requirements?

- A. Create an Amazon FSx for NetApp ONTAP file system. Set each volume's tiering policy to ALL. Import the raw data into the file system. Mount the file system on the EC2 instances.
- B. Create an Amazon S3 bucket to store the raw data. Create an Amazon FSx for Lustre file system that uses persistent SSD storage. Select the option to import data from and export data to Amazon S3. Mount the file system on the EC2 instances.
- C. Create an Amazon S3 bucket to store the raw data. Create an Amazon FSx for Lustre file system that uses persistent HDD storage. Select the option to import data from and export data to Amazon S3. Mount the file system on the EC2 instances.
- D. Create an Amazon FSx for NetApp ONTAP file system. Set each volume's tiering policy to NON.
- E. Import the raw data into the file system. Mount the file system on the EC2 instances.

**Answer:** B

**Explanation:**

Create an Amazon S3 bucket to store the raw data. Create an Amazon FSx for Lustre file system that uses persistent SSD storage. Select the option to import data from and export data to Amazon S3. Mount the file system on the EC2 instances. Amazon FSx for Lustre uses SSD storage for sub-millisecond latencies and up to 6 GBps throughput, and can import data from and export data to Amazon S3. Additionally, the option to select persistent SSD storage will ensure that the data is stored on the disk and not lost if the file system is stopped.

#### NEW QUESTION 165

- (Topic 3)

A company wants to configure its Amazon CloudFront distribution to use SSL/TLS certificates. The company does not want to use the default domain name for the distribution. Instead, the company wants to use a different domain name for the distribution.

Which solution will deploy the certificate without incurring any additional costs?

- A. Request an Amazon issued private certificate from AWS Certificate Manager (ACM) in the us-east-1 Region.
- B. Request an Amazon issued private certificate from AWS Certificate Manager (ACM) in the us-west-1 Region.
- C. Request an Amazon issued public certificate from AWS Certificate Manager (ACM) in the us-east-1 Region.
- D. Request an Amazon issued public certificate from AWS Certificate Manager (ACM) in the us-west-1 Region.

**Answer:** C

**Explanation:**

This option is the most efficient because it requests an Amazon issued public certificate from AWS Certificate Manager (ACM), which is a service that lets you easily provision, manage, and deploy public and private SSL/TLS certificates for use with AWS services and your internal connected resources<sup>1</sup>. It also requests the certificate in the us-east-1 Region, which is required for using an ACM certificate with CloudFront<sup>2</sup>. It also meets the requirement of deploying the certificate without incurring any additional costs, as ACM does not charge for certificates that are used with supported AWS services<sup>3</sup>. This solution meets the requirement of configuring its CloudFront distribution to use SSL/TLS certificates and using a different domain name for the distribution. Option A is less efficient because it requests an Amazon issued private certificate from ACM, which is a type of certificate that can be used only within your organization or virtual private cloud (VPC). However, this does not meet the requirement of configuring its CloudFront distribution to use SSL/TLS certificates, as CloudFront requires a public certificate. It also requests the certificate in the us-east-1 Region, which is correct. Option B is less efficient because it requests an Amazon issued private certificate from ACM, which is incorrect for the same reason as option A. It also requests the certificate in the us-west-1 Region, which is incorrect as CloudFront requires a certificate in the us-east-1 Region. Option D is less efficient because it requests an Amazon issued public certificate from ACM, which is correct. However, it requests the certificate in the us-west-1 Region, which is incorrect as CloudFront requires a certificate in the us-east-1 Region.

#### NEW QUESTION 169

- (Topic 3)

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

**Answer:** B

**Explanation:**

Lambda server-less is scalable and elastic than EC2 api gateway solution

**NEW QUESTION 170**

- (Topic 3)

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.
- E. Use NFS permission sets on the images to prevent accidental deletion.

**Answer:** B

**Explanation:**

This answer is correct because it provides a resilient and durable replacement for the on-premises file share that is compatible with a serverless web application. Amazon S3 is a fully managed object storage service that can store any amount of data and serve it over the internet. It supports the following features:

? **Resilience:** Amazon S3 stores data across multiple Availability Zones within a Region, and offers 99.999999999% (11 9's) of durability. It also supports cross-region replication, which enables automatic and asynchronous copying of objects across buckets in different AWS Regions.

? **Durability:** Amazon S3 encrypts data at rest using server-side encryption with either Amazon S3-managed keys (SSE-S3), AWS KMS keys (SSE-KMS), or customer-provided keys (SSE-C). It also supports encryption in transit using SSL/TLS. Amazon S3 also provides data protection features such as versioning, which keeps multiple versions of an object in the same bucket, and MFA Delete, which requires additional authentication for deleting an object version or changing the versioning state of a bucket.

? **Performance:** Amazon S3 delivers high performance and scalability for serving static and dynamic web content. It also supports features such as S3 Transfer Acceleration, which speeds up data transfers by routing requests to AWS edge locations, and S3 Select, which enables retrieving only a subset of data from an object by using simple SQL expressions.

The S3 Standard-Infrequent Access (S3 Standard-IA) storage class is suitable for storing images that are rarely accessed, but must be immediately available when needed. It offers the same high durability, throughput, and low latency as S3 Standard, but with a lower storage cost per GB and a higher per-request cost.

References:

? Amazon Simple Storage Service

? Storage classes - Amazon Simple Storage Service

**NEW QUESTION 175**

- (Topic 3)

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 frequently. 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.

**Answer:** BC

**Explanation:**

These options are operationally efficient because they use Amazon RDS read replicas to offload the reporting workload from the primary DB instance and avoid affecting any document modifications or the addition of new documents. They also use Reserved Instances for the primary DB instance to reduce costs and On-Demand or Aurora Replicas for the read replicas to scale as needed. 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 D is less efficient because it uses AWS Lambda to process the files, which has a maximum execution time of 15 minutes per invocation, which might not be enough for processing each file that needs 3-8 minutes. It also uses S3 event notifications to invoke the Lambda function when the files arrive, which could cause concurrency issues if there are thousands of small data files arriving periodically. Option E is less efficient because it uses Amazon DynamoDB, which is a NoSQL database service that does not support relational queries, which are needed for generating the reports. It also uses fixed write capacity, which could cause throttling or underutilization depending on the incoming data files.



#### NEW QUESTION 179

- (Topic 3)

A company collects data from a large number of participants who use wearable devices. The company stores the data in an Amazon DynamoDB table and uses applications to analyze the data. The data workload is constant and predictable. The company wants to stay at or below its forecasted budget for DynamoDB. Which solution will meet these requirements MOST cost-effectively?

- A. Use provisioned mode and DynamoDB Standard-Infrequent Access (DynamoDB Standard-IA). Reserve capacity for the forecasted workload.
- B. Use provisioned mode. Specify the read capacity units (RCUs) and write capacity units (WCUs).
- C. Use on-demand mode.
- D. Set the read capacity units (RCUs) and write capacity units (WCUs) high enough to accommodate changes in the workload.
- E. Use on-demand mode.
- F. Specify the read capacity units (RCUs) and write capacity units (WCUs) with reserved capacity.

**Answer: B**

#### Explanation:

This option is the most efficient because it uses provisioned mode, which is a read/write capacity mode for processing reads and writes on your tables that lets you specify how much read and write throughput you expect your application to perform<sup>1</sup>. It also specifies the read capacity units (RCUs) and write capacity units (WCUs), which are the amount of data your application needs to read or write per second. It also meets the requirement of staying at or below its forecasted budget for DynamoDB, as provisioned mode has lower costs than on-demand mode for predictable workloads. This solution meets the requirement of collecting data from a large number of participants who use wearable devices with a constant and predictable data workload. Option A is less efficient because it uses provisioned mode and DynamoDB Standard-Infrequent Access (DynamoDB Standard-IA), which is a storage class for infrequently accessed items that require milliseconds latency<sup>2</sup>. However, this does not meet the requirement of collecting data from a large number of participants who use wearable devices with a constant and predictable data workload, as DynamoDB Standard-IA is more suitable for items that are accessed less frequently than once every 30 days. Option C is less efficient because it uses on-demand mode, which is a read/write capacity mode that lets you pay only for what you use by automatically adjusting your table's capacity in response to changing demand<sup>3</sup>. However, this does not meet the requirement of staying at or below its forecasted budget for DynamoDB, as on-demand mode has higher costs than provisioned mode for predictable workloads. Option D is less efficient because it uses on-demand mode and specifies the RCUs and WCUs with reserved capacity, which is a way to reserve read and write capacity for your tables in exchange for discounted hourly rates. However, this does not meet the requirement of staying at or below its forecasted budget for DynamoDB, as on-demand mode has higher costs than provisioned mode for predictable workloads. Also, specifying RCUs and WCUs with reserved capacity is not possible with on-demand mode, as it only applies to provisioned mode.

#### NEW QUESTION 183

- (Topic 3)

An ecommerce company is building a distributed application that involves several serverless functions and AWS services to complete order-processing tasks. These tasks require manual approvals as part of the workflow. A solutions architect needs to design an architecture for the order-processing application. The solution must be able to combine multiple AWS Lambda functions into responsive serverless applications. The solution also must orchestrate data and services that run on Amazon EC2 instances, containers, or on-premises servers. Which solution will meet these requirements with the LEAST operational overhead?

- A. Use AWS Step Functions to build the application.
- B. Integrate all the application components in an AWS Glue job.
- C. Use Amazon Simple Queue Service (Amazon SQS) to build the application.
- D. Use AWS Lambda functions and Amazon EventBridge (Amazon CloudWatch Events) events to build the application.

**Answer: A**

#### Explanation:

AWS Step Functions is a fully managed service that makes it easy to build applications by coordinating the components of distributed applications and microservices using visual workflows. With Step Functions, you can combine multiple AWS Lambda functions into responsive serverless applications and orchestrate data and services that run on Amazon EC2 instances, containers, or on-premises servers. Step Functions also allows for manual approvals as part of the workflow. This solution meets all the requirements with the least operational overhead.

[https://aws.amazon.com/step-functions/#:~:text=AWS%20Step%20Functions%20is%20a,machine%20learning%20\(ML\)%20pipelines.](https://aws.amazon.com/step-functions/#:~:text=AWS%20Step%20Functions%20is%20a,machine%20learning%20(ML)%20pipelines.)

#### NEW QUESTION 187

- (Topic 3)

A company is developing a new mobile app. The company must implement proper traffic filtering to protect its Application Load Balancer (ALB) against common application-level attacks, such as cross-site scripting or SQL injection. The company has minimal infrastructure and operational staff. The company needs to reduce its share of the responsibility in managing, updating, and securing servers for its AWS environment. What should a solutions architect recommend to meet these requirements?

- A. Configure AWS WAF rules and associate them with the ALB.
- B. Deploy the application using Amazon S3 with public hosting enabled.
- C. Deploy AWS Shield Advanced and add the ALB as a protected resource.
- D. Create a new ALB that directs traffic to an Amazon EC2 instance running a third-party firewall, which then passes the traffic to the current ALB.

**Answer: A**

#### Explanation:

A solutions architect should recommend option A, which is to configure AWS WAF rules and associate them with the ALB. This will allow the company to apply traffic filtering at the application layer, which is necessary for protecting the ALB against common application-level attacks such as cross-site scripting or SQL injection. AWS WAF is a managed service that makes it easy to protect web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. The company can easily manage and update the rules to ensure the security of its application.

#### NEW QUESTION 188

- (Topic 3)

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

**Answer:** B

**Explanation:**

This option is the most efficient because it uses a gateway VPC endpoint for Amazon S3, which provides reliable connectivity to Amazon S3 without requiring an internet gateway or a NAT device for the VPC<sup>1</sup>. A gateway VPC endpoint routes traffic from the VPC to Amazon S3 using a prefix list for the service and does not leave the AWS network<sup>2</sup>. This meets the requirement of not traversing the internet. Option A is less efficient because it uses a private hosted zone by using Amazon Route 53, which is a DNS service that allows you to create custom domain names for your resources within your VPC<sup>3</sup>. However, this does not provide connectivity to Amazon S3 without an internet gateway or a NAT device. Option C is less efficient because it uses a NAT gateway to access the S3 bucket, which is a highly available, managed Network Address Translation (NAT) service that enables instances in a private subnet to connect to the internet or other AWS services, but prevents the internet from initiating a connection with those instances<sup>4</sup>. However, this does not meet the requirement of not traversing the internet. Option D is less efficient because it uses an AWS Site-to-Site VPN connection between the VPC and the S3 bucket, which is a secure and encrypted network connection between your on-premises network and your VPC. However, this does not meet the requirement of not traversing the internet.

**NEW QUESTION 189**

- (Topic 3)

A financial company hosts a web application on AWS. The application uses an Amazon API Gateway Regional API endpoint to give users the ability to retrieve current stock prices. The company's security team has noticed an increase in the number of API requests. The security team is concerned that HTTP flood attacks might take the application offline.

A solutions architect must design a solution to protect the application from this type of attack.

Which solution meets these requirements with the LEAST operational overhead?

- A. Create an Amazon CloudFront distribution in front of the API Gateway Regional API endpoint with a maximum TTL of 24 hours
- B. Create a Regional AWS WAF web ACL with a rate-based rule
- C. Associate the web ACL with the API Gateway stage.
- D. Use Amazon CloudWatch metrics to monitor the Count metric and alert the security team when the predefined rate is reached
- E. Create an Amazon CloudFront distribution with Lambda@Edge in front of the API Gateway Regional API endpoint Create an AWS Lambda function to block requests from IP addresses that exceed the predefined rate.

**Answer:** B

**Explanation:**

<https://docs.aws.amazon.com/waf/latest/developerguide/web-acl.html>

A rate-based rule in AWS WAF allows the security team to configure thresholds that trigger rate-based rules, which enable AWS WAF to track the rate of requests for a specified time period and then block them automatically when the threshold is exceeded. This provides the ability to prevent HTTP flood attacks with minimal operational overhead.

**NEW QUESTION 194**

- (Topic 3)

A company runs a web application that is backed by Amazon RDS. A new database administrator caused data loss by accidentally editing information in a database table To help recover from this type of incident, the company wants the ability to restore the database to its state from 5 minutes before any change within the last 30 days.

Which feature should the solutions architect include in the design to meet this requirement?

- A. Read replicas
- B. Manual snapshots
- C. Automated backups
- D. Multi-AZ deployments

**Answer:** C

**Explanation:**

<https://aws.amazon.com/rds/features/backup/>

Automated backups, will meet the requirement. Amazon RDS allows you to automatically create backups of your DB instance. Automated backups enable point-in-time recovery (PITR) for your DB instance down to a specific second within the retention period, which can be up to 35 days. By setting the retention period to 30 days, the company can restore the database to its state from up to 5 minutes before any change within the last 30 days.

**NEW QUESTION 198**

- (Topic 3)

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 MySQL 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 DynamoDB 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

**Answer:** AD

**Explanation:**

<https://aws.amazon.com/caching/session-management/>

### NEW QUESTION 203

- (Topic 3)

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 periodically Queries and removes sensitive information from Lake Formation tables.

**Answer: B**

#### Explanation:

This option is the most efficient because it uses data filters, which are specifications that restrict access to certain data in query results and engines integrated with Lake Formation<sup>1</sup>. Data filters can be used to implement row-level security and cell-level security, which are techniques to prevent access to portions of the data that contain sensitive information<sup>2</sup>. Data filters can be applied when granting Lake Formation permissions on a Data Catalog table, and can use PartiQL expressions to filter data based on conditions<sup>3</sup>. This solution meets the requirement of providing a secure solution to prevent access to portions of the data that contain sensitive information. Option A is less efficient because it uses an IAM role that includes permissions to access Lake Formation tables, which is a way to grant access to data in Lake Formation using IAM policies<sup>4</sup>. However, this does not provide a way to prevent access to portions of the data that contain sensitive information. Option C is less efficient because it uses an AWS Lambda function that removes sensitive information before Lake Formation ingests the data, which is a way to perform data cleansing or transformation using serverless functions. However, this could involve significant changes to the application code and logic, and could also result in data loss or inconsistency. Option D is less efficient because it uses an AWS Lambda function that periodically queries and removes sensitive information from Lake Formation tables, which is a way to perform data cleansing or transformation using serverless functions. However, this could involve significant changes to the application code and logic, and could also result in data loss or inconsistency.

### NEW QUESTION 207

- (Topic 3)

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

**Answer: C**

#### Explanation:

<https://aws.amazon.com/efs/features/infrequent-access/>

### NEW QUESTION 209

- (Topic 3)

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)

**Answer: D**

#### Explanation:

S3 One Zone-IA is a storage class that is designed for data that is accessed less frequently, but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ and costs 20% less than S3 Standard-IA. This storage class meets the requirements of the company because it provides a low-cost solution for the secondary copy of its on-premises dataset that would rarely need to be accessed. The other storage classes are either more expensive or not suitable for infrequently accessed data.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html>

### NEW QUESTION 214

- (Topic 3)

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-side- encryption header set.

**Answer: D**

#### Explanation:

<https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/#:~:text=Solution%20overview,console%2C%20CLI%2C%20or%20SDK.&text=To%20e ncrypt%20an%20object%20at,S3%2C%20or%20SSE%2DKMS>.

#### NEW QUESTION 215

- (Topic 3)

A company runs a containerized application on a Kubernetes cluster in an on-premises data center. The company is using a MongoDB database for data storage. The company wants to migrate some of these environments to AWS, but no code changes or deployment method changes are possible at this time. The company needs a solution that minimizes operational overhead.

Which solution meets these requirements?

- A. Use Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 worker nodes for compute and MongoDB on EC2 for data storage.
- B. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate for compute and Amazon DynamoDB for data storage.
- C. Use Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 worker nodes for compute and Amazon DynamoDB for data storage.
- D. Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate for compute and Amazon DocumentDB (with MongoDB compatibility) for data storage.

**Answer:** D

**Explanation:**

Amazon DocumentDB (with MongoDB compatibility) is a fast, reliable, and fully managed database service. Amazon DocumentDB makes it easy to set up, operate, and scale MongoDB-compatible databases in the cloud. With Amazon DocumentDB, you can run the same application code and use the same drivers and tools that you use with MongoDB. <https://docs.aws.amazon.com/documentdb/latest/developerguide/what-is.html>

#### NEW QUESTION 217

.....



## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SAA-C03 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SAA-C03 Product From:

<https://www.2passeasy.com/dumps/SAA-C03/>

## Money Back Guarantee

### **SAA-C03 Practice Exam Features:**

- \* SAA-C03 Questions and Answers Updated Frequently
- \* SAA-C03 Practice Questions Verified by Expert Senior Certified Staff
- \* SAA-C03 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* SAA-C03 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year