



# Amazon-Web-Services

## Exam Questions SAA-C03

AWS Certified Solutions Architect - Associate (SAA-C03)

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

- (Topic 1)

A company hosts a containerized web application on a fleet of on-premises servers that process incoming requests. The number of requests is growing quickly. The on-premises servers cannot handle the increased number of requests. The company wants to move the application to AWS with minimum code changes and minimum development effort.

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

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

**Answer:** A

#### Explanation:

AWS Fargate is a serverless compute engine that lets users run containers without having to manage servers or clusters of Amazon EC2 instances<sup>1</sup>. Users can use AWS Fargate on Amazon Elastic Container Service (Amazon ECS) to run the containerized web application with Service Auto Scaling. Amazon ECS is a fully managed container orchestration service that supports both Docker and Kubernetes<sup>2</sup>. Service Auto Scaling is a feature that allows users to adjust the desired number of tasks in an ECS service based on CloudWatch metrics, such as CPU utilization or request count<sup>3</sup>. Users can use AWS Fargate on Amazon ECS to migrate the application to AWS with minimum code changes and minimum development effort, as they only need to package their application in containers and specify the CPU and memory requirements.

Users can also use an Application Load Balancer to distribute the incoming requests. An Application Load Balancer is a load balancer that operates at the application layer and routes traffic to targets based on the content of the request. Users can register their ECS tasks as targets for an Application Load Balancer and configure listener rules to route requests to different target groups based on path or host headers. Users can use an Application Load Balancer to improve the availability and performance of their web application.

### NEW QUESTION 2

- (Topic 1)

A company uses NFS to store large video files in on-premises network attached storage. Each video file ranges in size from 1MB to 500 GB. The total storage is 70 TB and is no longer growing. The company decides to migrate the video files to Amazon S3. The company must migrate the video files as soon as possible while using the least possible network bandwidth.

Which solution will meet these requirements?

- A. Create an S3 bucket Create an IAM role that has permissions to write to the S3 bucket
- B. Use the AWS CLI to copy all files locally to the S3 bucket.
- C. Create an AWS Snowball Edge job
- D. Receive a Snowball Edge device on premise
- E. Use the Snowball Edge client to transfer data to the device
- F. Return the device so that AWS can import the data into Amazon S3.
- G. Deploy an S3 File Gateway on premise
- H. Create a public service endpoint to connect to the S3 File Gateway Create an S3 bucket Create a new NFS file share on the S3 File Gateway Point the new file share to the S3 bucket
- I. Transfer the data from the existing NFS file share to the S3 File Gateway.
- J. Set up an AWS Direct Connect connection between the on-premises network and AWS
- K. Deploy an S3 File Gateway on premise
- L. Create a public virtual interface (VIF) to connect to the S3 File Gateway
- M. Create an S3 bucket
- N. Create a new NFS file share on the S3 File Gateway
- O. Point the new file share to the S3 bucket
- P. Transfer the data from the existing NFS file share to the S3 File Gateway.

**Answer:** B

#### Explanation:

The basic difference between Snowball and Snowball Edge is the capacity they provide. Snowball provides a total of 50 TB or 80 TB, out of which 42 TB or 72 TB is available, while Amazon Snowball Edge provides 100 TB, out of which 83 TB is available.

### NEW QUESTION 3

- (Topic 1)

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

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

**Answer:** B

#### Explanation:

In Static Websites, Web pages are returned by the server which are prebuilt. They use simple languages such as HTML, CSS, or JavaScript.

There is no processing of content on the server (according to the user) in Static Websites. Web pages are returned by the server with no change therefore, static Websites are fast.

There is no interaction with databases.

Also, they are less costly as the host does not need to support server-side processing with different languages.

=====

In Dynamic Websites, Web pages are returned by the server which are processed during runtime means they are not prebuilt web pages but they are built during runtime according to the user's demand.

These use server-side scripting languages such as PHP, Node.js, ASP.NET and many more supported by the server.

So, they are slower than static websites but updates and interaction with databases are possible.

#### NEW QUESTION 4

- (Topic 1)

A company uses 50 TB of data for reporting. The company wants to move this data from on premises to AWS. A custom application in the company's data center runs a weekly data transformation job. The company plans to pause the application until the data transfer is complete and needs to begin the transfer process as soon as possible.

The data center does not have any available network bandwidth for additional workloads. A solutions architect must transfer the data and must configure the transformation job to continue to run in the AWS Cloud.

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

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

**Answer: D**

#### Explanation:

AWS Snowball Edge is a type of Snowball device with on-board storage and compute power for select AWS capabilities. Snowball Edge can do local processing and edge-computing workloads in addition to transferring data between your local environment and the AWS Cloud<sup>1</sup>. Users can order an AWS Snowball Edge Storage Optimized device that includes Amazon EC2 compute to move 50 TB of data from on premises to AWS. The Storage Optimized device has 80 TB of usable storage and 40 vCPUs of compute power<sup>2</sup>. Users can copy the data to the device using the AWS OpsHub graphical user interface or the Snowball client command line tool<sup>3</sup>. Users can also create and run Amazon EC2 instances on the device using Amazon Machine Images (AMIs) that are compatible with the sbec1 instance type. Users can use the Snowball Edge device to transfer the data and run the transformation job locally without using any network bandwidth.

Users can also create a new EC2 instance on AWS to run the transformation application after the data transfer is complete. Amazon EC2 is a web service that provides secure, resizable compute capacity in the cloud. Users can launch an EC2 instance in the same AWS Region where they send their Snowball Edge device and choose an AMI that matches their application requirements. Users can use the EC2 instance to continue running the transformation job in the AWS Cloud.

#### NEW QUESTION 5

- (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 6

- (Topic 1)

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

Which solution meets these requirements?

- A. Enable Amazon GuardDuty on the account.
- B. Enable Amazon Inspector on the EC2 instances.

- C. Enable AWS Shield and assign Amazon Route 53 to it.
- D. Enable AWS Shield Advanced and assign the ELB to it.

**Answer:** D

**Explanation:**

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

**NEW QUESTION 7**

- (Topic 1)

A company needs the ability to analyze the log files of its proprietary application. The logs are stored in JSON format in an Amazon S3 bucket. Queries will be simple and will run on-demand. A solutions architect needs to perform the analysis with minimal changes to the existing architecture. What should the solutions architect do to meet these requirements with the LEAST amount of operational overhead?

- A. Use Amazon Redshift to load all the content into one place and run the SQL queries as needed.
- B. Use Amazon CloudWatch Logs to store the logs. Run SQL queries as needed from the Amazon CloudWatch console.
- C. Use Amazon Athena directly with Amazon S3 to run the queries as needed.
- D. Use AWS Glue to catalog the logs. Use a transient Apache Spark cluster on Amazon EMR to run the SQL queries as needed.

**Answer:** C

**Explanation:**

Amazon Athena can be used to query JSON in S3.

**NEW QUESTION 8**

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

Amazon CloudFront is a content delivery network (CDN) that caches content at edge locations around the world, providing low latency and high transfer speeds to users accessing the content. Adding a CloudFront distribution in front of the S3 bucket will cache the static website's content at edge locations around the world, decreasing latency for users accessing the website. This solution is also cost-effective as it only charges for the data transfer and requests made by users accessing the content from the CloudFront edge locations. Additionally, this solution provides scalability and reliability benefits as CloudFront can automatically scale to handle increased demand and provide high availability for the website.

**NEW QUESTION 9**

- (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 certificates.
- 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 operations.
- 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 operations.
- 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 operations.
- K. Store the encrypted data on Amazon Elastic Block Store (Amazon EBS) volumes.

**Answer:** D

**NEW QUESTION 10**

- (Topic 1)

A company runs an ecommerce application on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. The Auto Scaling group scales based on CPU utilization metrics. The ecommerce application stores the transaction data in a MySQL 8.0 database that is hosted on a large EC2 instance.

The database's performance degrades quickly as application load increases. The application handles more read requests than write transactions. The company wants a solution that will automatically scale the database to meet the demand of unpredictable read workloads while maintaining high availability.

Which solution will meet these requirements?



- A. Use Amazon Redshift with a single node for leader and compute functionality.
- B. Use Amazon RDS with a Single-AZ deployment Configure Amazon RDS to add reader instances in a different Availability Zone.
- C. Use Amazon Aurora with a Multi-AZ deployment
- D. Configure Aurora Auto Scaling with Aurora Replicas.
- E. Use Amazon ElastiCache for Memcached with EC2 Spot Instances.

**Answer:** C

**Explanation:**

AURORA is 5x performance improvement over MySQL on RDS and handles more read requests than write,; maintaining high availability = Multi-AZ deployment

**NEW QUESTION 10**

- (Topic 1)

A company is hosting a web application on AWS using a single Amazon EC2 instance that stores user-uploaded documents in an Amazon EBS volume. For better scalability and availability, the company duplicated the architecture and created a second EC2 instance and EBS volume in another Availability Zone placing both behind an Application Load Balancer After completing this change, users reported that, each time they refreshed the website, they could see one subset of their documents or the other, but never all of the documents at the same time.

What should a solutions architect propose to ensure users see all of their documents at once?

- A. Copy the data so both EBS volumes contain all the documents.
- B. Configure the Application Load Balancer to direct a user to the server with the documents
- C. Copy the data from both EBS volumes to Amazon EFS Modify the application to save new documents to Amazon EFS
- D. Configure the Application Load Balancer to send the request to both servers Return each document from the correct server.

**Answer:** C

**Explanation:**

<https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html#how-it-works-ec2>

**NEW QUESTION 14**

- (Topic 1)

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

Which solution will meet these requirements?

- A. Create stage variables in API Gateway with Name="Endpoint-URL" and Value="Company Domain Name" to overwrite the default UR
- B. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM).
- C. Create Route 53 DNS records with the company's domain nam
- D. Point the alias record to the Regional API Gateway stage endpoint
- E. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the us-east-1 Region.
- F. Create a Regional API Gateway endpoint
- G. Associate the API Gateway endpoint with the company's domain nam
- H. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the same Regio
- I. Attach the certificate to the API Gateway endpoint
- J. Configure Route 53 to route traffic to the API Gateway endpoint.
- K. Create a Regional API Gateway endpoint
- L. Associate the API Gateway endpoint with the company's domain nam
- M. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the us-east-1 Regio
- N. Attach the certificate to the API Gateway API
- O. Create Route 53 DNS records with the company's domain nam
- P. Point an A record to the company's domain name.

**Answer:** C

**Explanation:**

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

**NEW QUESTION 18**

- (Topic 1)

A company is running an SMB file server in its data center. The file server stores large files that are accessed frequently for the first few days after the files are created. After 7 days the files are rarely accessed.

The total data size is increasing and is close to the company's total storage capacity. A solutions architect must increase the company's available storage space without losing low-latency access to the most recently accessed files. The solutions architect must also provide file lifecycle management to avoid future storage issues.

Which solution will meet these requirements?

- A. Use AWS DataSync to copy data that is older than 7 days from the SMB file server to AWS.
- B. Create an Amazon S3 File Gateway to extend the company's storage spac
- C. Create an S3 Lifecycle policy to transition the data to S3 Glacier Deep Archive after 7 days.
- D. Create an Amazon FSx for Windows File Server file system to extend the company's storage space.
- E. Install a utility on each user's computer to access Amazon S3. Create an S3 Lifecycle policy to transition the data to S3 Glacier Flexible Retrieval after 7 days.

**Answer:** B

**Explanation:**

Amazon S3 File Gateway is a hybrid cloud storage service that enables on-premises applications to seamlessly use Amazon S3 cloud storage. It provides a file interface to Amazon S3 and supports SMB and NFS protocols. It also supports S3 Lifecycle policies that can automatically transition data from S3 Standard to S3 Glacier Deep Archive after a specified period of time. This solution will meet the requirements of increasing the company's available storage space without losing low-latency access to the most recently accessed files and providing file lifecycle management to avoid future storage issues.

Reference:

<https://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html>

**NEW QUESTION 21**

- (Topic 1)

A company is storing sensitive user information in an Amazon S3 bucket. The company wants to provide secure access to this bucket from the application tier running on Amazon EC2 instances inside a VPC.

Which combination of steps should a solutions architect take to accomplish this? (Select TWO.)

- A. Configure a VPC gateway endpoint for Amazon S3 within the VPC
- B. Create a bucket policy to make the objects in the S3 bucket public
- C. Create a bucket policy that limits access to only the application tier running in the VPC
- D. Create an IAM user with an S3 access policy and copy the IAM credentials to the EC2 instance
- E. Create a NAT instance and have the EC2 instances use the NAT instance to access the S3 bucket

**Answer:** AC

**Explanation:**

<https://aws.amazon.com/premiumsupport/knowledge-center/s3-private-connection-no-authentication/>

**NEW QUESTION 22**

- (Topic 1)

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

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

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

**Answer:** B

**Explanation:**

From <https://docs.aws.amazon.com/kms/latest/developerguide/custom-key-store-overview.html>

For most users, the default AWS KMS key store, which is protected by FIPS 140-2 validated cryptographic modules, fulfills their security requirements. There is no need to add an extra layer of maintenance responsibility or a dependency on an additional service. However, you might consider creating a custom key store if your organization has any of the following requirements: Key material cannot be stored in a shared environment. Key material must be subject to a secondary, independent audit path. The HSMs that generate and store key material must be certified at FIPS 140-2 Level 3.

<https://docs.aws.amazon.com/kms/latest/developerguide/custom-key-store-overview.html>

<https://docs.aws.amazon.com/kms/latest/developerguide/multi-region-keys-overview.html>

**NEW QUESTION 25**

- (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 26**

- (Topic 1)

A company has more than 5 TB of file data on Windows file servers that run on-premises. Users and applications interact with the data each day.

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

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

**Answer: D**

**Explanation:**

<https://docs.aws.amazon.com/filegateway/latest/filefsxw/what-is-file-fsxw.html>

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

Reference:

AWS FSx for Windows File Server: <https://aws.amazon.com/fsx/windows/> AWS FSx File Gateway: <https://aws.amazon.com/fsx/file-gateway/>

AWS Site-to-Site VPN: <https://aws.amazon.com/vpn/site-to-site-vpn/>

**NEW QUESTION 31**

- (Topic 1)

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

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

**Answer: D**

**Explanation:**

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-capacity-reservations.html>

Reserve instances: You will have to pay for the whole term (1 year or 3 years) which is not cost effective

**NEW QUESTION 33**

- (Topic 1)

A company has several web servers that need to frequently access a common Amazon RDS MySQL Multi-AZ DB instance. The company wants a secure method for the web servers to connect to the database while meeting a security requirement to rotate user credentials frequently. Which solution meets these requirements?

- A. Store the database user credentials in AWS Secrets Manager. Grant the necessary IAM permissions to allow the web servers to access AWS Secrets Manager.
- B. Store the database user credentials in AWS Systems Manager OpsCenter. Grant the necessary IAM permissions to allow the web servers to access OpsCenter.
- C. Store the database user credentials in a secure Amazon S3 bucket. Grant the necessary IAM permissions to allow the web servers to retrieve credentials and access the database.
- D. Store the database user credentials in files encrypted with AWS Key Management Service (AWS KMS) on the web server file system.
- E. The web server should be able to decrypt the files and access the database.

**Answer: A**

**Explanation:**

AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.

<https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html>

Secrets Manager enables you to replace hardcoded credentials in your code, including passwords, with an API call to Secrets Manager to retrieve the secret programmatically. This helps ensure the secret can't be compromised by someone examining your code, because the secret no longer exists in the code. Also, you can configure Secrets Manager to automatically rotate the secret for you according to a specified schedule. This enables you to replace long-term secrets with short-term ones, significantly reducing the risk of compromise.

**NEW QUESTION 37**

- (Topic 1)

A company recently migrated to AWS and wants to implement a solution to protect the traffic that flows in and out of the production VPC. The company had an inspection server in its on-premises data center. The inspection server performed specific operations such as traffic flow inspection and traffic filtering. The company wants to have the same functionalities in the AWS Cloud. Which solution will meet these requirements?

- A. Use Amazon GuardDuty for traffic inspection and traffic filtering in the production VPC.
- B. Use Traffic Mirroring to mirror traffic from the production VPC for traffic inspection and filtering.
- C. Use AWS Network Firewall to create the required rules for traffic inspection and traffic filtering for the production VPC.



D. Use AWS Firewall Manager to create the required rules for traffic inspection and traffic filtering for the production VPC.

**Answer:** C

**Explanation:**

AWS Network Firewall supports both inspection and filtering as required

**NEW QUESTION 42**

- (Topic 1)

A survey company has gathered data for several years from areas in the United States. The company hosts the data in an Amazon S3 bucket that is 3 TB in size and growing. The company has started to share the data with a European marketing firm that has S3 buckets. The company wants to ensure that its data transfer costs remain as low as possible.

Which solution will meet these requirements?

- A. Configure the Requester Pays feature on the company's S3 bucket.
- B. Configure S3 Cross-Region Replication from the company's S3 bucket to one of the marketing firm's S3 buckets.
- C. Configure cross-account access for the marketing firm so that the marketing firm has access to the company's S3 bucket.
- D. Configure the company's S3 bucket to use S3 Intelligent-Tiering. Sync the S3 bucket to one of the marketing firm's S3 buckets.

**Answer:** A

**Explanation:**

"Typically, you configure buckets to be Requester Pays buckets when you want to share data but not incur charges associated with others accessing the data. For example, you might use Requester Pays buckets when making available large datasets, such as zip code directories, reference data, geospatial information, or web crawling data." <https://docs.aws.amazon.com/AmazonS3/latest/userguide/RequesterPaysBuckets.html>

**NEW QUESTION 43**

- (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 47**

- (Topic 1)

A company has an AWS Glue extract, transform, and load (ETL) job that runs every day at the same time. The job processes XML data that is in an Amazon S3 bucket.

New data is added to the S3 bucket every day. A solutions architect notices that AWS Glue is processing all the data during each run.

What should the solutions architect do to prevent AWS Glue from reprocessing old data?

- A. Edit the job to use job bookmarks.
- B. Edit the job to delete data after the data is processed.
- C. Edit the job by setting the NumberOfWorkers field to 1.
- D. Use a FindMatches machine learning (ML) transform.

**Answer:** C

**Explanation:**

This is the purpose of bookmarks: "AWS Glue tracks data that has already been processed during a previous run of an ETL job by persisting state information from the job run. This persisted state information is called a job bookmark. Job bookmarks help AWS Glue maintain state information and prevent the reprocessing of old data." <https://docs.aws.amazon.com/glue/latest/dg/monitor-continuations.html>

**NEW QUESTION 51**

- (Topic 1)

A company is designing an application where users upload small files into Amazon S3. After a user uploads a file, the file requires one-time simple processing to transform the data and save the data in JSON format for later analysis.

Each file must be processed as quickly as possible after it is uploaded. Demand will vary. On some days, users will upload a high number of files. On other days, users will upload a few files or no files.

Which solution meets these requirements with the LEAST operational overhead?

- A. Configure Amazon EMR to read text files from Amazon S3. Run processing scripts to transform the data
- B. Store the resulting JSON file in an Amazon Aurora DB cluster.
- C. Configure Amazon S3 to send an event notification to an Amazon Simple Queue Service (Amazon SQS) queue
- D. Use Amazon EC2 instances to read from the queue and process the data
- E. Store the resulting JSON file in Amazon DynamoDB.
- F. Configure Amazon S3 to send an event notification to an Amazon Simple Queue Service (Amazon SQS) queue
- G. Use an AWS Lambda function to read from the queue and process the data
- H. Store the resulting JSON file in Amazon DynamoDB
- I. Most Voted
- J. Configure Amazon EventBridge (Amazon CloudWatch Events) to send an event to Amazon Kinesis Data Streams when a new file is uploaded
- K. Use an AWS Lambda function to consume the event from the stream and process the data
- L. Store the resulting JSON file in Amazon Aurora DB cluster.

**Answer: C**

**Explanation:**

Amazon S3 sends event notifications about S3 buckets (for example, object created, object removed, or object restored) to an SNS topic in the same Region. The SNS topic publishes the event to an SQS queue in the central Region.

The SQS queue is configured as the event source for your Lambda function and buffers the event messages for the Lambda function.

The Lambda function polls the SQS queue for messages and processes the Amazon S3 event notifications according to your application's requirements.

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/subscribe-a-lambda-function-to-event-notifications-from-s3-buckets-in-different-aws-regions.html>

**NEW QUESTION 54**

- (Topic 1)

A company is preparing to store confidential data in Amazon S3. For compliance reasons, the data must be encrypted at rest. Encryption key usage must be logged for auditing purposes. Keys must be rotated every year.

Which solution meets these requirements and is the MOST operationally efficient?

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

**Answer: D**

**Explanation:**

<https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html> When you enable automatic key rotation for a customer managed key, AWS KMS generates new cryptographic material for the KMS key every year. AWS KMS also saves the KMS key's older cryptographic material in perpetuity so it can be used to decrypt data that the KMS key encrypted.

Key rotation in AWS KMS is a cryptographic best practice that is designed to be transparent and easy to use. AWS KMS supports optional automatic key rotation only for customer managed CMKs. Enable and disable key rotation. Automatic key rotation is disabled by default on customer managed CMKs. When you enable (or re-enable) key rotation, AWS KMS automatically rotates the CMK 365 days after the enable date and every 365 days thereafter.

**NEW QUESTION 55**

- (Topic 1)

A solutions architect is designing a VPC with public and private subnets. The VPC and subnets use IPv4 CIDR blocks. There is one public subnet and one private subnet in each of three Availability Zones (AZs) for high availability. An internet gateway is used to provide internet access for the public subnets. The private subnets require access to the internet to allow Amazon EC2 instances to download software updates.

What should the solutions architect do to enable Internet access for the private subnets?

- A. Create three NAT gateways, one for each public subnet in each AZ
- B. Create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ.
- C. Create three NAT instances, one for each private subnet in each AZ
- D. Create a private route table for each AZ that forwards non-VPC traffic to the NAT instance in its AZ.
- E. Create a second internet gateway on one of the private subnets
- F. Update the route table for the private subnets that forward non-VPC traffic to the private internet gateway.
- G. Create an egress-only internet gateway on one of the public subnets
- H. Update the route table for the private subnets that forward non-VPC traffic to the egress-only internet gateway.

**Answer: A**

**Explanation:**

<https://aws.amazon.com/about-aws/whats-new/2018/03/introducing-amazon-vpc-nat-gateway-in-the-aws-govcloud-us-region/#:~:text=NAT%20Gateway%20is%20a%20highly,instances%20in%20a%20private%20subnet.>

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html>

**NEW QUESTION 58**

- (Topic 1)

A company has an automobile sales website that stores its listings in a database on Amazon RDS. When an automobile is sold, the listing needs to be removed from the website, and the data must be sent to multiple target systems.

Which design should a solutions architect recommend?

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

D. Subscribe to an RDS event notification and send an Amazon Simple Notification Service (Amazon SNS) topic fanned out to multiple Amazon Simple Queue Service (Amazon SQS) queues Use AWS Lambda functions to update the targets

**Answer:** D

**Explanation:**

<https://docs.aws.amazon.com/lambda/latest/dg/services-rds.html> <https://docs.aws.amazon.com/lambda/latest/dg/with-sns.html>

### NEW QUESTION 63

- (Topic 1)

A company uses AWS Organizations to manage multiple AWS accounts for different departments. The management account has an Amazon S3 bucket that contains project reports. The company wants to limit access to this S3 bucket to only users of accounts within the organization in AWS Organizations. Which solution meets these requirements with the LEAST amount of operational overhead?

- A. Add the aws:PrincipalOrgID global condition key with a reference to the organization ID to the S3 bucket policy.
- B. Create an organizational unit (OU) for each department
- C. Add the aws:PrincipalOrgPaths global condition key to the S3 bucket policy.
- D. Use AWS CloudTrail to monitor the CreateAccount, InviteAccountToOrganization, LeaveOrganization, and RemoveAccountFromOrganization event
- E. Update the S3 bucket policy accordingly.
- F. Tag each user that needs access to the S3 bucket
- G. Add the aws:PrincipalTag global condition key to the S3 bucket policy.

**Answer:** A

**Explanation:**

<https://aws.amazon.com/blogs/security/control-access-to-aws-resources-by-using-the-aws-organization-of-iam-principals/>

The aws:PrincipalOrgID global key provides an alternative to listing all the account IDs for all AWS accounts in an organization. For example, the following Amazon S3 bucket policy allows members of any account in the XXX organization to add an object into the examtopics bucket.

```
{
  "Version": "2020-09-10",
  "Statement": [
    {
      "Sid": "AllowPutObject",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::examtopics/*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": ["XXX"]
        }
      }
    }
  ]
}
```

[https://docs.aws.amazon.com/IAM/latest/UserGuide/reference\\_policies\\_condition-keys.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_condition-keys.html)

### NEW QUESTION 65

- (Topic 1)

A company recently launched a variety of new workloads on Amazon EC2 instances in its AWS account. The company needs to create a strategy to access and administer the instances remotely and securely. The company needs to implement a repeatable process that works with native AWS services and follows the AWS Well-Architected Framework.

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

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

**Answer:** B

**Explanation:**

<https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-launch-managed-instance.html>

### NEW QUESTION 70

- (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 74

- (Topic 2)

A company wants to migrate its on-premises data center to AWS. According to the company's compliance requirements, the company can use only the ap-northeast-3 Region. Company administrators are not permitted to connect VPCs to the internet.

Which solutions will meet these requirements? (Choose two.)

- A. Use AWS Control Tower to implement data residency guardrails to deny internet access and deny access to all AWS Regions except ap-northeast-3.
- B. Use rules in AWS WAF to prevent internet access
- C. Deny access to all AWS Regions except ap-northeast-3 in the AWS account settings.
- D. Use AWS Organizations to configure service control policies (SCPs) that prevent VPCs from gaining internet access
- E. Deny access to all AWS Regions except ap-northeast-3.
- F. Create an outbound rule for the network ACL in each VPC to deny all traffic from 0.0.0.0/0. Create an IAM policy for each user to prevent the use of any AWS Region other than ap-northeast-3.
- G. Use AWS Config to activate managed rules to detect and alert for internet gateways and to detect and alert for new resources deployed outside of ap-northeast-3.

**Answer:** AC

#### Explanation:

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scps\\_examples\\_vpc.html#example\\_vpc\\_2](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_vpc.html#example_vpc_2)

#### NEW QUESTION 76

- (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 77

- (Topic 2)

A solutions architect needs to help a company optimize the cost of running an application on AWS. The application will use Amazon EC2 instances, AWS Fargate, and AWS Lambda for compute within the architecture.

The EC2 instances will run the data ingestion layer of the application. EC2 usage will be sporadic and unpredictable. Workloads that run on EC2 instances can be interrupted at any time. The application front end will run on Fargate, and Lambda will serve the API layer. The front-end utilization and API layer utilization will be predictable over the course of the next year.

Which combination of purchasing options will provide the MOST cost-effective solution for hosting this application? (Choose two.)

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

**Answer:** AC

#### Explanation:

EC2 instance Savings Plan saves 72% while Compute Savings Plans saves 66%. But according to link, it says "Compute Savings Plans provide the most flexibility and help to reduce your costs by up to 66%. These plans automatically apply to EC2 instance usage regardless of instance family, size, AZ, region, OS or tenancy, and also apply to Fargate and Lambda usage." EC2 instance Savings Plans are not applied to Fargate or Lambda

#### NEW QUESTION 80

- (Topic 2)

A company wants to use the AWS Cloud to make an existing application highly available and resilient. The current version of the application resides in the company's data center. The application recently experienced data loss after a database server crashed because of an unexpected power outage.

The company needs a solution that avoids any single points of failure. The solution must give the application the ability to scale to meet user demand.

Which solution will meet these requirements?

- A. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones
- B. Use an Amazon RDS DB instance in a Multi-AZ configuration.
- C. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group in a single Availability Zone
- D. Deploy the database on an EC2 instance



- E. Enable EC2 Auto Recovery.
- F. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zone
- G. Use an Amazon RDS DB instance with a read replica in a single Availability Zon
- H. Promote the read replica to replace the primary DB instance if the primary DB instance fails.
- I. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones Deploy the primary and secondary database servers on EC2 instances across multiple Availability Zones Use Amazon Elastic Block Store (Amazon EBS) Multi-Attach to create shared storage between the instances.

**Answer:** A

**Explanation:**

Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. Use an Amazon RDS DB instance in a Multi-AZ configuration. To make an existing application highly available and resilient while avoiding any single points of failure and giving the application the ability to scale to meet user demand, the best solution would be to deploy the application servers using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones and use an Amazon RDS DB instance in a Multi-AZ configuration. By using an Amazon RDS DB instance in a Multi-AZ configuration, the database is automatically replicated across multiple Availability Zones, ensuring that the database is highly available and can withstand the failure of a single Availability Zone. This provides fault tolerance and avoids any single points of failure.

**NEW QUESTION 85**

- (Topic 2)

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

Which solution meets these requirements MOST cost-effectively?

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

**Answer:** C

**Explanation:**

This solution meets the requirements of a disaster recovery solution to back up the data that is generated by an analytics application, stored in JSON format, and must be accessible in milliseconds if it is needed. Amazon S3 Standard is a durable and scalable storage class for frequently accessed data. It can store any amount of data and provide high availability and performance. It can also support millisecond access time for data retrieval.

Option A is incorrect because Amazon OpenSearch Service (Amazon Elasticsearch Service) is a search and analytics service that can index and query data, but it is not a backup solution for data stored in JSON format. Option B is incorrect because Amazon S3 Glacier is a low-cost storage class for data archiving and long-term backup, but it does not support millisecond access time for data retrieval. Option D is incorrect because Amazon RDS for PostgreSQL is a relational database service that can store and query structured data, but it is not a backup solution for data stored in JSON format.

References:

? <https://aws.amazon.com/s3/storage-classes/>

? [https://aws.amazon.com/s3/faqs/#Durability\\_and\\_data\\_protection](https://aws.amazon.com/s3/faqs/#Durability_and_data_protection)

**NEW QUESTION 89**

- (Topic 2)

A company is concerned about the security of its public web application due to recent web attacks. The application uses an Application Load Balancer (ALB). A solutions architect must reduce the risk of DDoS attacks against the application.

What should the solutions architect do to meet this requirement?

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

**Answer:** C

**Explanation:**

AWS Shield Advanced provides expanded DDoS attack protection for your Amazon EC2 instances, Elastic Load Balancing load balancers, CloudFront distributions, Route 53 hosted zones, and AWS Global Accelerator standard accelerators. <https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html>

**NEW QUESTION 90**

- (Topic 2)

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

Which solution will mast these requirements?

- A. Create a VPC peering connection between the company's VPC and the provider's VP
- B. Update the route table to connect to the target service.
- C. Ask the provider to create a virtual private gateway in its VP
- D. Use AWS PrivateLink to connect to the target service.
- E. Create a NAT gateway in a public subnet of the company's VP
- F. Update the route table to connect to the target service.
- G. Ask the provider to create a VPC endpoint for the target servic
- H. Use AWS PrivateLink to connect to the target service.

**Answer:** D

**Explanation:**

**\*\*AWS PrivateLink** provides private connectivity between VPCs, AWS services, and your on-premises networks, without exposing your traffic to the public internet\*\*. AWS PrivateLink makes it easy to connect services across different accounts and VPCs to significantly simplify your network architecture. Interface **\*\*VPC endpoints\*\***, powered by AWS PrivateLink, connect you to services hosted by AWS Partners and supported solutions available in AWS Marketplace.  
<https://aws.amazon.com/privatelink/>

**NEW QUESTION 93**

- (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 96**

- (Topic 2)

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

How should a solutions architect design the application to ensure the LEAST amount of latency for all users?

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

**Answer:** A

**Explanation:**

<https://aws.amazon.com/blogs/networking-and-content-delivery/deliver-your-apps-dynamic-content-using-amazon-cloudfront-getting-started-template/>

**NEW QUESTION 100**

- (Topic 2)

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

Which solution will meet these requirements?

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

**Answer:** C

**Explanation:**

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/rds-custom.html> and <https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/working-with-custom-oracle.html>

**NEW QUESTION 104**

- (Topic 2)

A company wants to run a gaming application on Amazon EC2 instances that are part of an Auto Scaling group in the AWS Cloud. The application will transmit data by using UDP packets. The company wants to ensure that the application can scale out and in as traffic increases and decreases.

What should a solutions architect do to meet these requirements?

- A. Attach a Network Load Balancer to the Auto Scaling group.
- B. Attach an Application Load Balancer to the Auto Scaling group.
- C. Deploy an Amazon Route 53 record set with a weighted policy to route traffic appropriately.

D. Deploy a NAT instance that is configured with port forwarding to the EC2 instances in the Auto Scaling group.

**Answer:** A

**Explanation:**

This solution meets the requirements of running a gaming application that transmits data by using UDP packets and scaling out and in as traffic increases and decreases. A Network Load Balancer can handle millions of requests per second while maintaining high throughput at ultra low latency, and it supports both TCP and UDP protocols. An Auto Scaling group can automatically adjust the number of EC2 instances based on the demand and the scaling policies.

Option B is incorrect because an Application Load Balancer does not support UDP protocol, only HTTP and HTTPS. Option C is incorrect because Amazon Route 53 is a DNS service that can route traffic based on different policies, but it does not provide load balancing or scaling capabilities. Option D is incorrect because a NAT instance is used to enable instances in a private subnet to connect to the internet or other AWS services, but it does not provide load balancing or scaling capabilities.

References:

? <https://aws.amazon.com/blogs/aws/new-udp-load-balancing-for-network-load-balancer/>

? <https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html>

**NEW QUESTION 107**

- (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 112**

- (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 114**

- (Topic 2)

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

Which solution will meet these requirements MOST cost-effectively?

- A. Migrate the database to an Amazon RDS for MySQL DB instance
- B. Create an AMI of the web application
- C. Use the AMI to launch a second EC2 On-Demand Instance
- D. Use an Application Load Balancer to distribute the load to each EC2 instance.
- E. Migrate the database to an Amazon RDS for MySQL DB instance
- F. Create an AMI of the web application
- G. Use the AMI to launch a second EC2 On-Demand Instance
- H. Use Amazon Route 53 weighted routing to distribute the load across the two EC2 instances.
- I. Migrate the database to an Amazon Aurora MySQL DB instance
- J. Create an AWS Lambda function to stop the EC2 instance and change the instance type
- K. Create an Amazon CloudWatch alarm to invoke the Lambda function when CPU utilization surpasses 75%.
- L. Migrate the database to an Amazon Aurora MySQL DB instance
- M. Create an AMI of the web application
- N. Apply the AMI to a launch template



- O. Create an Auto Scaling group with the launch template Configure the launch template to use a Spot Fleet
- P. Attach an Application Load Balancer to the Auto Scaling group.

**Answer:** D

**Explanation:**

Migrate the database to Amazon Aurora MySQL - this will let the DB scale on it's own; it'll scale automatically without needing adjustment. Create AMI of the web app and using a launch template - this will make the creating of any future instances of the app seamless. They can then be added to the auto scaling group which will save them money as it will scale up and down based on demand. Using a spot fleet to launch instances- This solves the "MOST cost-effective" portion of the question as spot instances come at a huge discount at the cost of being terminated at any time Amazon deems fit. I think this is why there's a bit of disagreement on this. While it's the most cost effective, it would be a terrible choice if amazon were to terminate that spot instance during a busy period.

**NEW QUESTION 116**

- (Topic 2)

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

- A. Set up AWS WAF in both Region
- B. Associate Regional web ACLs with an API stage.
- C. Set up AWS Firewall Manager in both Region
- D. Centrally configure AWS WAF rules.
- E. Set up AWS Shield in both Region
- F. Associate Regional web ACLs with an API stage.
- G. Set up AWS Shield in one of the Region
- H. Associate Regional web ACLs with an API stage.

**Answer:** A

**Explanation:**

Using AWS WAF has several benefits. Additional protection against web attacks using criteria that you specify. You can define criteria using characteristics of web requests such as the following: Presence of SQL code that is likely to be malicious (known as SQL injection). Presence of a script that is likely to be malicious (known as cross-site scripting). AWS Firewall Manager simplifies your administration and maintenance tasks across multiple accounts and resources for a variety of protections. <https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html>

**NEW QUESTION 121**

- (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 125**

- (Topic 2)

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

- A. Migrate the queue to a redundant pair (active/standby) of RabbitMQ instances on Amazon M
- B. Create a Multi-AZ Auto Scaling group (or EC2 instances that host the applicatio
- C. Create another Multi-AZ Auto Scaling group for EC2 instances that host the PostgreSQL database.
- D. Migrate the queue to a redundant pair (active/standby) of RabbitMQ instances on Amazon M
- E. Create a Multi-AZ Auto Scaling group for EC2 instances that host the applicatio
- F. Migrate the database to run on a Multi-AZ deployment of Amazon RDS for PostgreSQL.
- G. Create a Multi-AZ Auto Scaling group for EC2 instances that host the RabbitMQ queu
- H. Create another Multi-AZ Auto Scaling group for EC2 instances that host the application.Migrate the database to run on a Multi-AZ deployment of Amazon RDS for PostgreSQL.
- I. Create a Multi-AZ Auto Scaling group for EC2 instances that host the RabbitMQ queue.Create another Multi-AZ Auto Scaling group for EC2 instances that host the applicatio
- J. Create a third Multi-AZ Auto Scaling group for EC2 instances that host the PostgreSQL database.



**Answer:** B

**Explanation:**

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

**NEW QUESTION 127**

- (Topic 2)

A company's application is having performance issues. The application is stateful and needs to complete in-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 they 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 group.
- B. Make the changes by using the AWS Management Console.
- C. Modify the CloudFormation templates to run the EC2 instances in an Auto Scaling group.
- 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 instances.
- 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 instances.
- 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 130**

- (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 132**

- (Topic 2)

A company has a legacy data processing application that runs on Amazon EC2 instances. Data is processed sequentially, but the order of results does not matter. The application uses a monolithic architecture. The only way that the company can scale the application to meet increased demand is to increase the size of the instances.

The company's developers have decided to rewrite the application to use a microservices architecture on Amazon Elastic Container Service (Amazon ECS).

What should a solutions architect recommend for communication between the microservices?

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

**Answer:** A

**Explanation:**

Queue has limited throughput (300 msg/s without batching, 3000 msg/s with batching whereby up to 10 msg per batch operation; Message duplicates not allowed in the queue (exactly-once delivery); Message order is preserved (FIFO); Queue name must end with .fifo

### NEW QUESTION 135

- (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 137

- (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 142

- (Topic 2)

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

Which solution can the company use to route traffic to all the EC2 instances?

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

**Answer:** B

#### Explanation:

For standard accelerators, Global Accelerator uses the AWS global network to route traffic to the optimal regional endpoint based on health, client location, and policies that you configure, which increases the availability of your applications. Endpoints for standard accelerators can be Network Load Balancers, Application Load Balancers, Amazon EC2 instances, or Elastic IP addresses that are located in one AWS Region or multiple Regions.

<https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global-accelerator.html>

### NEW QUESTION 143

- (Topic 2)

A company is migrating an application from on-premises servers to Amazon EC2 instances. As part of the migration design requirements, a solutions architect must implement infrastructure metric alarms. The company does not need to take action if CPU utilization increases to more than 50% for a short burst of time. However, if the CPU

utilization increases to more than 50% and read IOPS on the disk are high at the same time, the company needs to act as soon as possible. The solutions architect also must reduce false alarms.

What should the solutions architect do to meet these requirements?

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

**Answer:** A

**Explanation:**

Composite alarms determine their states by monitoring the states of other alarms. You can **use composite alarms to reduce alarm noise**. For example, you can create a composite alarm where the underlying metric alarms go into ALARM when they meet specific conditions. You then can set up your composite alarm to go into ALARM and send you notifications when the underlying metric alarms go into ALARM by configuring the underlying metric alarms never to take actions. Currently, composite alarms can take the following actions: [https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Create\\_Composite\\_Alarm.html](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Create_Composite_Alarm.html)

**NEW QUESTION 144**

- (Topic 3)

A media company hosts its website on AWS. The website application's architecture includes a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB) and a database that is hosted on Amazon Aurora. The company's cyber security team reports that the application is vulnerable to SQL injection. How should the company resolve this issue?

- A. Use AWS WAF in front of the ALB. Associate the appropriate web ACLs with AWS WAF.
- B. Create an ALB listener rule to reply to SQL injection with a fixed response.
- C. Subscribe to AWS Shield Advanced to block all SQL injection attempts automatically.
- D. Set up Amazon Inspector to block all SQL injection attempts automatically.

**Answer:** A

**Explanation:**

<https://aws.amazon.com/premiumsupport/knowledge-center/waf-block-common-attacks/#:~:text=To%20protect%20your%20applications%20against,%2C%20query%20string%2C%20or%20URI.> -----

----- Protect against SQL injection and cross-site scripting To protect your applications against SQL injection and cross-site scripting (XSS) attacks, use the built-in SQL injection and cross-site scripting engines. Remember that attacks can be performed on different parts of the HTTP request, such as the HTTP header, query string, or URI. Configure the AWS WAF rules to inspect different parts of the HTTP request against the built-in mitigation engines.

**NEW QUESTION 146**

- (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 lag no more than 1 second behind the primary DB instance. The database routinely runs scheduled stored procedures.

As traffic on the website increases, the replicas 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 150**

- (Topic 3)

A gaming company is moving its public scoreboard from a data center to the AWS Cloud. The company uses Amazon EC2 Windows Server instances behind an Application Load Balancer to host its dynamic application. The company needs a highly available storage solution for the application. The application consists of static files and dynamic server-side code.

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

- A. Store the static files on Amazon S3. Use Amazon CloudFront to cache objects at the edge.
- B. Store the static files on Amazon S3. Use Amazon ElastiCache to cache objects at the edge.
- C. Store the server-side code on Amazon Elastic File System (Amazon EFS). Mount the EFS volume on each EC2 instance to share the files.
- D. Store the server-side code on Amazon FSx for Windows File Share.
- E. Mount the FSx for Windows File Share volume on each EC2 instance to share the files.
- F. Store the server-side code on a General Purpose SSD (gp2) Amazon Elastic Block Store (Amazon EBS) volume.
- G. Mount the EBS volume on each EC2 instance to share the files.

**Answer:** AD



**Explanation:**

A because Elasticache, despite being ideal for leaderboards per Amazon, doesn't cache at edge locations. D because FSx has higher performance for low latency needs. <https://www.techtarget.com/searchaws/tip/Amazon-FSx-vs-EFS-Compare-the-AWS-file-services> "FSx is built for high performance and submillisecond latency using solid-state drive storage volumes. This design enables users to select storage capacity and latency independently. Thus, even a subterabyte file system can have 256 Mbps or higher throughput and support volumes up to 64 TB."

Amazon S3 is an object storage service that can store static files such as images, videos, documents, etc. Amazon EFS is a file storage service that can store files in a hierarchical structure and supports NFS protocol. Amazon FSx for Windows File Server is a file storage service that can store files in a hierarchical structure and supports SMB protocol. Amazon EBS is a block storage service that can store data in fixed-size blocks and attach to EC2 instances.

Based on these definitions, the combination of steps that should be taken to meet the requirements are:

\* A. Store the static files on Amazon S3. Use Amazon CloudFront to cache objects at the edge. D. Store the server-side code on Amazon FSx for Windows File Server. Mount the FSx for Windows File Server volume on each EC2 instance to share the files.

**NEW QUESTION 155**

- (Topic 3)

A company deploys an application on five Amazon EC2 instances. An Application Load Balancer (ALB) distributes traffic to the instances by using a target group. The average CPU usage on each of the instances is below 10% most of the time. With occasional surges to 65%.

A solution architect needs to implement a solution to automate the scalability of the application. The solution must optimize the cost of the architecture and must ensure that the application has enough CPU resources when surges occur.

Which solution will meet these requirements?

- A. Create an Amazon CloudWatch alarm that enters the ALARM state when the CPUUtilization metric is less than 20%. Create an AWS Lambda function that the CloudWatch alarm invokes to terminate one of the EC2 instances in the ALB target group.
- B. Create an EC2 Auto Scaling group.
- C. Select the existing ALB as the load balancer and the existing target group as the target group.
- D. Set a target tracking scaling policy that is based on the ASGAverageCPUUtilization metric.
- E. Set the minimum instances to 2, the desired capacity to 3, the maximum instances to 6, and the target value to 50%. Add the EC2 instances to the Auto Scaling group.
- F. Create an EC2 Auto Scaling group.
- G. Select the existing ALB as the load balancer and the existing target group.
- H. Set the minimum instances to 2, the desired capacity to 3, and the maximum instances to 6. Add the EC2 instances to the Scaling group.
- I. Create two Amazon CloudWatch alarms.
- J. Configure the first CloudWatch alarm to enter the ALARM state when the average CPUUtilization metric is below 20%. Configure the second CloudWatch alarm to enter the ALARM state when the average CPUUtilization metric is above 50%. Configure the alarms to publish to an Amazon Simple Notification Service (Amazon SNS) topic to send an email message.
- K. After receiving the message, log in to decrease or increase the number of EC2 instances that are running.

**Answer:** B

**Explanation:**

- An Auto Scaling group will automatically scale the EC2 instances to match changes in demand. This optimizes cost by only running as many instances as needed.
- A target tracking scaling policy monitors the ASGAverageCPUUtilization metric and scales to keep the average CPU around the 50% target value. This ensures there are enough resources during CPU surges.
- The ALB and target group are reused, so the application architecture does not change. The Auto Scaling group is associated to the existing load balancer setup.
- A minimum of 2 and maximum of 6 instances provides the ability to scale between 3 and 6 instances as needed based on demand.
- Costs are optimized by starting with only 3 instances (the desired capacity) and scaling up as needed. When CPU usage drops, instances are terminated to match the desired capacity.

**NEW QUESTION 159**

- (Topic 3)

A company wants to migrate a Windows-based application from on premises to the AWS Cloud. The application has three tiers, a business tier, and a database tier with Microsoft SQL Server. The company wants to use specific features of SQL Server such as native backups and Data Quality Services. The company also needs to share files for process between the tiers.

How should a solution architect design the architecture to meet these requirements?

- A. Host all three on Amazon instance.
- B. Use Amazon FSx File Gateway for file sharing between tiers.
- C. Host all three on Amazon EC2 instance.
- D. Use Amazon FSx for Windows file sharing between the tiers.
- E. Host the application tier and the business tier on Amazon EC2 instance.
- F. Host the database tier on Amazon RD.
- G. Use Amazon Elastic File System (Amazon EFS) for file sharing between the tiers.
- H. Host the application tier and the business tier on Amazon EC2 instance.
- I. Host the database tier on Amazon RD.
- J. Use a Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volume for file sharing between the tiers.

**Answer:** B

**Explanation:**

This solution will allow the company to host all three tiers on Amazon EC2 instances while using Amazon FSx for Windows File Server to provide Windows-based file sharing between the tiers. This will allow the company to use specific features of SQL Server, such as native backups and Data Quality Services, while sharing files for processing between the tiers.

**NEW QUESTION 164**

- (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 167**

- (Topic 3)

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

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

**Answer:** C

**Explanation:**

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.AuroraMySQL.html>

**NEW QUESTION 169**

- (Topic 3)

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

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

**Answer:** D

**Explanation:**

To grant the necessary permissions to an AWS Lambda function to upload files to Amazon S3, a solutions architect should create an IAM execution role with the required permissions and attach the IAM role to the Lambda function. This approach follows the principle of least privilege and ensures that the Lambda function can only access the resources it needs to perform its specific task.

**NEW QUESTION 174**

- (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 seeing 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 178**

- (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 183**

- (Topic 3)

A solution architect needs to assign a new microservice for a company's application. Clients must be able to call an HTTPS endpoint to reach the microservice. The microservice also must use AWS identity and Access Management (IAM) for authentication calls. The solution architect will write the logic for this microservice by using a single AWS Lambda function that is written in Go 1.x.

Which solution will deploy the function in the MOST operationally efficient way?

- A. Create an Amazon API Gateway REST API
- B. Configure the method to use the Lambda function
- C. Enable IAM authentication on the API.
- D. Create a Lambda function URL for the function
- E. Specify AWS\_IAM as the authentication type.
- F. Create an Amazon CloudFront distribution
- G. Deploy the function to Lambda@Edge
- H. Integrate IAM authentication logic into the Lambda@Edge function.
- I. Create an Amazon CloudFront distribution
- J. Deploy the function to CloudFront Function
- K. Specify AWS\_IAM as the authentication type.

**Answer:** A

**Explanation:**

A. Create an Amazon API Gateway REST API. Configure the method to use the Lambda function. Enable IAM authentication on the API. This option is the most operationally efficient as it allows you to use API Gateway to handle the HTTPS endpoint and also allows you to use IAM to authenticate the calls to the microservice. API Gateway also provides many additional features such as caching, throttling, and monitoring, which can be useful for a microservice.

**NEW QUESTION 186**

- (Topic 3)

A company hosts its application on AWS. The company uses Amazon Cognito to manage users. When users log in to the application, the application fetches required data from Amazon DynamoDB by using a REST API that is hosted in Amazon API Gateway. The company wants an AWS managed solution that will control access to the REST API to reduce development efforts.

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

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

**Answer:** D

**Explanation:**

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-integrate-with-cognito.html>

To control access to the REST API and reduce development efforts, the company can use an Amazon Cognito user pool authorizer in API Gateway. This will allow Amazon Cognito to validate each request and ensure that only authenticated users can access the API. This solution has the LEAST operational overhead, as it does not require the company to develop and maintain any additional infrastructure or code.

**NEW QUESTION 187**

- (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 188

- (Topic 3)

A company is hosting a three-tier ecommerce application in the AWS Cloud. The company hosts the website on Amazon S3 and integrates the website with an API that handles sales requests. The company hosts the API on three Amazon EC2 instances behind an Application Load Balancer (ALB). The API consists of static and dynamic front-end content along with backend workers that process sales requests asynchronously.

The company is expecting a significant and sudden increase in the number of sales requests during events for the launch of new products

What should a solutions architect recommend to ensure that all the requests are processed successfully?

- A. Add an Amazon CloudFront distribution for the dynamic content
- B. Increase the number of EC2 instances to handle the increase in traffic.
- C. Add an Amazon CloudFront distribution for the static content
- D. Place the EC2 instances in an Auto Scaling group to launch new instances based on network traffic.
- E. Add an Amazon CloudFront distribution for the dynamic content
- F. Add an Amazon ElastiCache instance in front of the ALB to reduce traffic for the API to handle.
- G. Add an Amazon CloudFront distribution for the static content
- H. Add an Amazon Simple Queue Service (Amazon SQS) queue to receive requests from the website for later processing by the EC2 instances.

**Answer: B**

#### Explanation:

This option is the most efficient because it uses Amazon CloudFront, which is a web service that speeds up distribution of your static and dynamic web content, such as .html,

.css, .js, and image files, to your users<sup>1</sup>. It also uses a CloudFront distribution for the static content, which reduces the load on the EC2 instances and improves the performance and availability of the website. It also uses an Auto Scaling group to launch new instances based on network traffic, which automatically adjusts the compute capacity of your EC2 instances based on load or a schedule<sup>2</sup>. This solution meets the requirement of ensuring that all the requests are processed successfully during events for the launch of new products. Option A is less efficient because it uses a CloudFront distribution for the dynamic content, which is not necessary as the dynamic content is already handled by the API on the EC2 instances. It also increases the number of EC2 instances to handle the increase in traffic, which could incur higher costs and complexity than using an Auto Scaling group. Option C is less efficient because it uses an Amazon ElastiCache instance in front of the ALB to reduce traffic for the API to handle, which is a way to provide a fully managed in-memory data store service that provides sub-millisecond latency for caching and data processing<sup>3</sup>. However, this could introduce additional complexity and latency, and does not scale automatically based on network traffic. Option D is less efficient because it uses an Amazon Simple Queue Service (Amazon SQS) queue to receive requests from the website for later processing by the EC2 instances, which is a way to send, store, and receive messages between software components at any volume. However, this does not provide a faster response time to the users as they have to wait for their requests to be processed by the EC2 instances.

#### NEW QUESTION 192

- (Topic 3)

A solutions architect observes that a nightly batch processing job is automatically scaled up for 1 hour before the desired Amazon EC2 capacity is reached. The peak capacity is the 'same every night and the batch jobs always start at 1 AM. The solutions architect needs to find a cost-effective solution that will allow for the desired EC2 capacity to be reached quickly and allow the Auto Scaling group to scale down after the batch jobs are complete.

What should the solutions architect do to meet these requirements?

- A. Increase the minimum capacity for the Auto Scaling group.
- B. Increase the maximum capacity for the Auto Scaling group.
- C. Configure scheduled scaling to scale up to the desired compute level.
- D. Change the scaling policy to add more EC2 instances during each scaling operation.

**Answer: C**

#### Explanation:

By configuring scheduled scaling, the solutions architect can set the Auto Scaling group to automatically scale up to the desired compute level at a specific time (IAM) when the batch job starts and then automatically scale down after the job is complete. This will allow the desired EC2 capacity to be reached quickly and also help in reducing the cost.

#### NEW QUESTION 194

- (Topic 3)

A company has a regional subscription-based streaming service that runs in a single AWS Region. The architecture consists of web servers and application servers on Amazon EC2 instances. The EC2 instances are in Auto Scaling groups behind Elastic Load Balancers. The architecture includes an Amazon Aurora database cluster that extends across multiple Availability Zones.

The company wants to expand globally and to ensure that its application has minimal downtime.

- A. Extend the Auto Scaling groups for the web tier and the application tier to deploy instances in Availability Zones in a second Region
- B. Use an Aurora global database to deploy the database in the primary Region and the second Region
- C. Use Amazon Route 53 health checks with a failover routing policy to the second Region.
- D. Deploy the web tier and the application tier to a second Region
- E. Add an Aurora PostgreSQL cross-Region Aurora Replica in the second Region
- F. Use Amazon Route 53 health checks with a failovers routing policy to the second Region, Promote the secondary to primary as needed.
- G. Deploy the web tier and the application tier to a second Region
- H. Create an Aurora PostgreSQL database in the second Region
- I. Use AWS Database Migration Service (AWS DMS) to replicate the primary database to the second Region
- J. Use Amazon Route 53 health checks with a failover routing policy to the second Region.
- K. Deploy the web tier and the application tier to a second Region
- L. Use an Amazon Aurora global database to deploy the database in the primary Region and the second Region
- M. Use Amazon Route 53 health checks with a failover routing policy to the second Region
- N. Promote the secondary to primary as needed.

**Answer: D**

#### Explanation:

This option is the most efficient because it deploys the web tier and the application tier to a second Region, which provides high availability and redundancy for the application. It also uses an Amazon Aurora global database, which is a feature that allows a single Aurora database to span multiple AWS Regions<sup>1</sup>. It also deploys the database in the primary Region and the second Region, which provides low latency global reads and fast recovery from a Regional outage. It also



uses Amazon Route 53 health checks with a failover routing policy to the second Region, which provides data protection by routing traffic to healthy endpoints in different Regions<sup>2</sup>. It also promotes the secondary to primary as needed, which provides data consistency by allowing write operations in one of the Regions at a time<sup>3</sup>. This solution meets the requirement of expanding globally and ensuring that its application has minimal downtime. Option A is less efficient because it extends the Auto Scaling groups for the web tier and the application tier to deploy instances in Availability Zones in a second Region, which could incur higher costs and complexity than deploying them separately. It also uses an Aurora global database to deploy the database in the primary Region and the second Region, which is correct. However, it does not use Amazon Route 53 health checks with a failover routing policy to the second Region, which could result in traffic being routed to unhealthy endpoints. Option B is less efficient because it deploys the web tier and the application tier to a second Region, which is correct. It also adds an Aurora PostgreSQL cross-Region Aurora Replica in the second Region, which provides read scalability across Regions. However, it does not use an Aurora global database, which provides faster replication and recovery than cross-Region replicas. It also uses Amazon Route 53 health checks with a failover routing policy to the second Region, which is correct. However, it does not promote the secondary to primary as needed, which could result in data inconsistency or loss. Option C is less efficient because it deploys the web tier and the application tier to a second Region, which is correct. It also creates an Aurora PostgreSQL database in the second Region, which provides data redundancy across Regions. However, it does not use an Aurora global database or cross-Region replicas, which provide faster replication and recovery than creating separate databases. It also uses AWS Database Migration Service (AWS DMS) to replicate the primary database to the second Region, which provides data migration between different sources and targets. However, it does not use an Aurora global database or cross-Region replicas, which provide faster replication and recovery than using AWS DMS. It also uses Amazon Route 53 health checks with a failover routing policy to the second Region, which is correct.

#### NEW QUESTION 196

- (Topic 3)

A company is deploying a new application on Amazon EC2 instances. The application writes data to Amazon Elastic Block Store (Amazon EBS) volumes. The company needs to ensure that all data that is written to the EBS volumes is encrypted at rest.

Which solution will meet this requirement?

- A. Create an IAM role that specifies EBS encryption
- B. Attach the role to the EC2 instances.
- C. Create the EBS volumes as encrypted volumes Attach the EBS volumes to the EC2 instances.
- D. Create an EC2 instance tag that has a key of Encrypt and a value of Tru
- E. Tag all instances that require encryption at the ESS level.
- F. Create an AWS Key Management Service (AWS KMS) key policy that enforces EBS encryption in the account Ensure that the key policy is active.

**Answer:** B

#### Explanation:

The solution that will meet the requirement of ensuring that all data that is written to the EBS volumes is encrypted at rest is B. Create the EBS volumes as encrypted volumes and attach the encrypted EBS volumes to the EC2 instances. When you create an EBS volume, you can specify whether to encrypt the volume. If you choose to encrypt the volume, all data written to the volume is automatically encrypted at rest using AWS-managed keys. You can also use customer-managed keys (CMKs) stored in AWS KMS to encrypt and protect your EBS volumes. You can create encrypted EBS volumes and attach them to EC2 instances to ensure that all data written to the volumes is encrypted at rest.

#### NEW QUESTION 200

- (Topic 3)

A company is running a publicly accessible serverless application that uses Amazon API Gateway and AWS Lambda. The application's traffic recently spiked due to fraudulent requests from botnets.

Which steps should a solutions architect take to block requests from unauthorized users? (Select TWO.)

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

**Answer:** AC

#### Explanation:

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

#### NEW QUESTION 202

- (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 203

- (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 205

- (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 210

.....

## Relate Links

**100% Pass Your SAA-C03 Exam with ExamBible Prep Materials**

<https://www.exambible.com/SAA-C03-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>