Amazon

Exam Questions AWS-Solution-Architect-Associate

Amazon AWS Certified Solutions Architect - Associate

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 4)
A solutions architect needs to design the architecture for an application that a vendor provides as a Docker container image The container needs 50 GB of storage available for temporary files The infrastructure must be serverless.
Which solution meets these requirements with the LEAST operational overhead?

A. Create an AWS Lambda function that uses the Docker container image with an Amazon S3 mounted volume that has more than 50 GB of space
B. Create an AWS Lambda function that uses the Docker container image with an Amazon Elastic Block Store (Amazon EBS) volume that has more than 50 GB of space
C. Create an Amazon Elastic Container Service (Amazon ECS) cluster that uses the AWS Fargate launch type Create a task definition for the container image with an Amazon Elastic File System (Amazon EFS) volum
D. Create a service with that task definition.
E. Create an Amazon Elastic Container Service (Amazon ECS) cluster that uses the Amazon EC2 launch type with an Amazon Elastic Block Store (Amazon EBS) volume that has more than 50 GB of space Create a task definition for the container imag
F. Create a service with that task definition.

Answer: C

Explanation:
The AWS Fargate launch type is a serverless way to run containers on Amazon ECS,
without having to manage any underlying infrastructure. You only pay for the resources required to run your containers, and AWS handles the provisioning, scaling, and security of the cluster. Amazon EFS is a fully managed, elastic, and scalable file system that can be mounted to multiple containers, and provides high availability and durability. By using AWS Fargate and Amazon EFS, you can run your Docker container image with 50 GB of storage available for temporary files, with the least operational overhead. This solution meets the requirements of the question.
References:
? AWS Fargate
? Amazon Elastic File System
? Using Amazon EFS file systems with Amazon ECS

NEW QUESTION 2
- (Topic 4)
A company migrated a MySQL database from the company's on-premises data center to an Amazon RDS for MySQL DB instance. The company sized the RDS DB instance to meet the company's average daily workload. Once a month, the database performs slowly when the company runs queries for a report. The company wants to have the ability to run reports and maintain the performance of the daily workloads.
Which solution will meet these requirements?

A. Create a read replica of the databas
B. Direct the queries to the read replica.
C. Create a backup of the databas
D. Restore the backup to another DB instanc
E. Direct the queries to the new database.
F. Export the data to Amazon S3. Use Amazon Athena to query the S3 bucket.
G. Resize the DB instance to accommodate the additional workload.

Answer: C

Explanation:
Amazon Athena is a service that allows you to run SQL queries on data stored in Amazon S3. It is serverless, meaning you do not need to provision or manage any infrastructure. You only pay for the queries you run and the amount of data scanned1.
By using Amazon Athena to query your data in Amazon S3, you can achieve the following benefits:
? You can run queries for your report without affecting the performance of your
Amazon RDS for MySQL DB instance. You can export your data from your DB instance to an S3 bucket and use Athena to query the data in the bucket. This way, you can avoid the overhead and contention of running queries on your DB instance.
? You can reduce the cost and complexity of running queries for your report. You do
not need to create a read replica or a backup of your DB instance, which would incur additional charges and require maintenance. You also do not need to resize your DB instance to accommodate the additional workload, which would increase your operational overhead.
? You can leverage the scalability and flexibility of Amazon S3 and Athena. You can
store large amounts of data in S3 and query them with Athena without worrying about capacity or performance limitations. You can also use different formats, compression methods, and partitioning schemes to optimize your data storage and query performance1.

NEW QUESTION 3
- (Topic 4)
A company is creating an application that runs on containers in a VPC. The application stores and accesses data in an Amazon S3 bucket During the development phase, the application will store and access 1 TB of data in Amazon S3 each day. The company wants to minimize costs and wants to prevent traffic from traversing the internet whenever possible.
Which solution will meet these requirements?

A. Enable S3 Intelligent-Tiering for the S3 bucket.
B. Enable S3 Transfer Acceleration for the S3 bucket.
C. Create a gateway VPC endpoint for Amazon S3. Associate this endpoint with all route tables in the VPC.
D. Create an interface endpoint for Amazon S3 in the VP
E. Associate this endpoint with all route tables in the VPC.

Answer: C

Explanation:
A gateway VPC endpoint for Amazon S3 enables private connections between the VPC and Amazon S3 that do not require an internet gateway or NAT device. This minimizes costs and prevents traffic from traversing the internet. A gateway VPC endpoint uses a prefix list as the route target in a VPC route table to route traffic privately to Amazon S31. Associating the endpoint with all route tables in the VPC ensures that all subnets can access Amazon S3 through the endpoint.

Option A is incorrect because S3 Intelligent-Tiering is a storage class that optimizes storage costs by automatically moving objects between two access tiers based on changing access patterns. It does not affect the network traffic between the VPC and Amazon S32.
Option B is incorrect because S3 Transfer Acceleration is a feature that enables fast, easy, and secure transfers of files over long distances between clients and an S3 bucket. It does not prevent traffic from traversing the internet3.
Option D is incorrect because an interface VPC endpoint for Amazon S3 is powered by AWS PrivateLink, which requires an elastic network interface (ENI) with a private IP address in each subnet. This adds complexity and cost to the solution. Moreover, an interface VPC endpoint does not support cross-Region access to Amazon S3. Reference URL: 1: https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html 2: https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html#sc- dynamic-data-access 3: https://docs.aws.amazon.com/AmazonS3/latest/userguide/transfer-acceleration.html : https://aws.amazon.com/blogs/architecture/choosing-your-vpc-endpoint-strategy-for- amazon-s3/

NEW QUESTION 4
- (Topic 4)
A company wants to use an AWS CloudFormatlon stack for its application in a test environment. The company stores the CloudFormation template in an Amazon S3 bucket that blocks public access. The company wants to grant CloudFormation access to the template in the S3 bucket based on specific user requests to create the test environment The solution must follow security best practices.
Which solution will meet these requirements?

A. Create a gateway VPC endpoint for Amazon S3. Configure the CloudFormation stack to use the S3 object URL
B. Create an Amazon API Gateway REST API that has the S3 bucket as the targe
C. Configure the CloudFormat10n stack to use the API Gateway URL _
D. Create a presigned URL for the template object_ Configure the CloudFormation stack to use the presigned URL.
E. Allow public access to the template object in the S3 bucke
F. Block the public access after the test environment is created

Answer: C

Explanation:
 it allows CloudFormation to access the template in the S3 bucket without granting public access or creating additional resources. A presigned URL is a URL that is signed with the access key of an IAM user or role that has permission to access the object. The presigned URL can be used by anyone who receives it, but it expires after a specified time. By creating a presigned URL for the template object and configuring the CloudFormation stack to use it, the company can grant CloudFormation access to the template based on specific user requests and follow security best practices. References:
? Using Amazon S3 Presigned URLs
? Using Amazon S3 Buckets

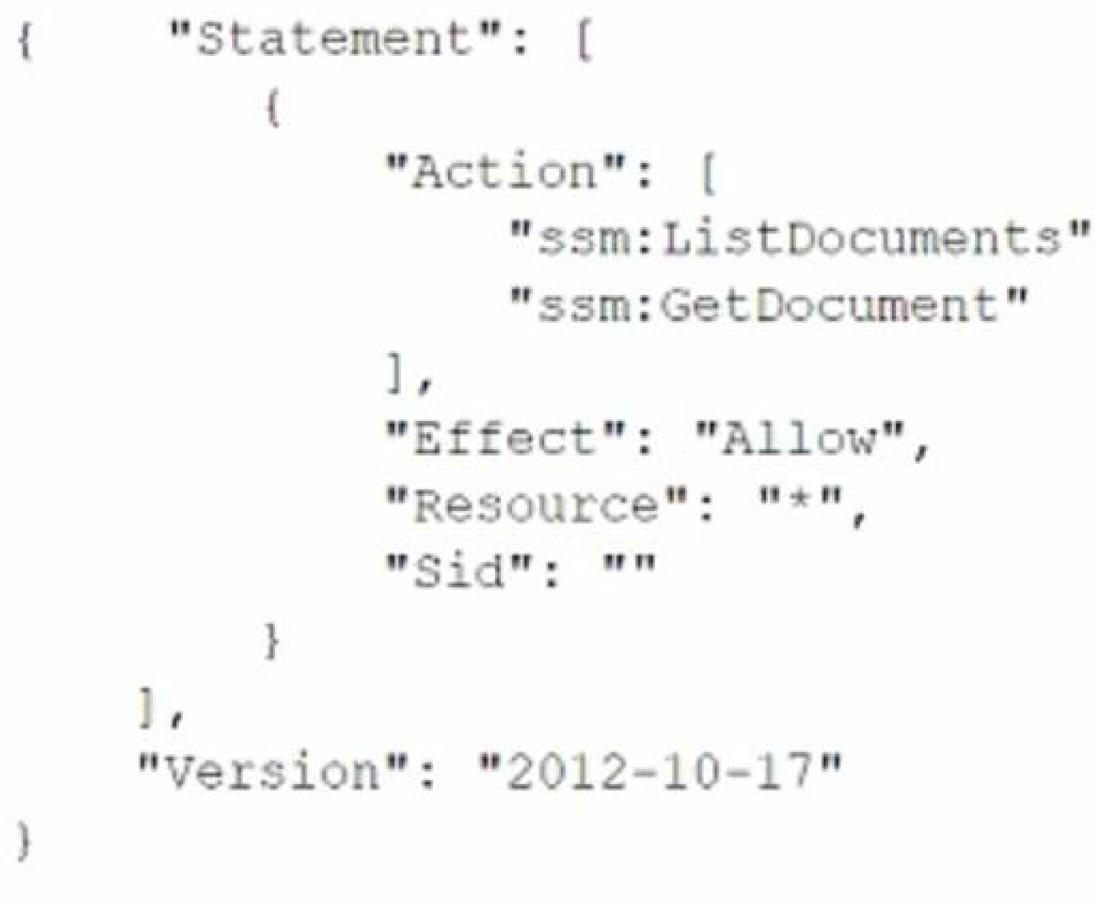
NEW QUESTION 5
- (Topic 4)
A company wants to analyze and generate reports to track the usage of its mobile app. The app is popular and has a global user base The company uses a custom report building program to analyze application usage.
The program generates multiple reports during the last week of each month. The program takes less than 10 minutes to produce each report. The company rarely uses the program to generate reports outside of the last week of each month. The company wants to generate reports in the least amount of time when the reports are requested.
Which solution will meet these requirements MOST cost-effectively?

A. Run the program by using Amazon EC2 On-Demand Instance
B. Create an Amazon EventBridge rule to start the EC2 instances when reports are requeste
C. Run the EC2 instances continuously during the last week of each month.
D. Run the program in AWS Lambd
E. Create an Amazon EventBridge rule to run a Lambda function when reports are requested.
F. Run the program in Amazon Elastic Container Service (Amazon ECS). Schedule Amazon ECS to run the program when reports are requested.
G. Run the program by using Amazon EC2 Spot Instance
H. Create an Amazon EventBridge rule to start the EC2 instances when reports are requeste
I. Run the EC2 instances continuously during the last week of each month.

Answer: B

Explanation:
 This solution meets the requirements most cost-effectively because it leverages the serverless and event-driven capabilities of AWS Lambda and Amazon EventBridge. AWS Lambda allows you to run code without provisioning or managing servers, and you pay only for the compute time you consume. Amazon EventBridge is a serverless event bus service that lets you connect your applications with data from various sources and routes that data to targets such as AWS Lambda. By using Amazon EventBridge, you can create a rule that triggers a Lambda function to run the program when reports are requested, and you can also schedule the rule to run during the last week of each month. This way, you can generate reports in the least amount of time and pay only for the resources you use.
References:
? AWS Lambda
? Amazon EventBridge

NEW QUESTION 6
- (Topic 4)
A solutions architect wants to use the following JSON text as an identity-based policy to grant specific permissions:



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

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

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

Answer: AB

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

NEW QUESTION 7
- (Topic 4)
A company containerized a Windows job that runs on .NET 6 Framework under a Windows container. The company wants to run this job in the AWS Cloud. The job runs every 10 minutes. The job's runtime varies between 1 minute and 3 minutes.
Which solution will meet these requirements MOST cost-effectively?

A. Create an AWS Lambda function based on the container image of the jo
B. Configure Amazon EventBridge to invoke the function every 10 minutes.
C. Use AWS Batch to create a job that uses AWS Fargate resource
D. Configure the job scheduling to run every 10 minutes.
E. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate to run the jo
F. Create a scheduled task based on the container image of the job to run every 10 minutes.
G. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate to run the jo
H. Create a standalone task based on the container image of the jo
I. Use Windows task scheduler to run the job every 10 minutes.

Answer: A

Explanation:
AWS Lambda supports container images as a packaging format for functions. You can use existing container development workflows to package and deploy Lambda functions as container images of up to 10 GB in size. You can also use familiar tools such as Docker CLI to build, test, and push your container images to Amazon Elastic Container Registry (Amazon ECR). You can then create an AWS Lambda function based on the container image of your job and configure Amazon EventBridge to invoke the function every 10 minutes using a cron expression. This solution will be cost-effective as you only pay for the compute time you consume when your function runs. References: https://docs.aws.amazon.com/lambda/latest/dg/images-create.html
https://docs.aws.amazon.com/eventbridge/latest/userguide/run-lambda-schedule.html

NEW QUESTION 8
- (Topic 4)
A company stores raw collected data in an Amazon S3 bucket. The data is used for several types of analytics on behalf of the company's customers. The type of analytics requested to determines the access pattern on the S3 objects.

The company cannot predict or control the access pattern. The company wants to reduce its S3 costs.
which solution will meet these requirements?

A. Use S3 replication to transition infrequently accessed objects to S3 Standard-Infrequent Access (S3 Standard-1A)
B. Use S3 Lifecycle rules to transition objects from S3 Standard to Standard-Infrequent Access (S3 Standard-1A).
C. Use S3 Lifecycle rules for transition objects from S3 Standard to S3 Intelligent-Tiering.
D. Use S3 Inventory to identify and transition objects that have not been accessed from S3 Standard to S3 Intelligent-Tiering.

Answer: C

Explanation:
S3 Intelligent-Tiering is a storage class that automatically reduces storage costs by moving data to the most cost-effective access tier based on access frequency. It has two access tiers: frequent access and infrequent access. Data is stored in the frequent access tier by default, and moved to the infrequent access tier after 30 consecutive days of no access. If the data is accessed again, it is moved back to the frequent access tie1r. By using S3 Lifecycle rules to transition objects from S3 Standard to S3 Intelligent-Tiering, the solution can reduce S3 costs for data with unknown or changing access patterns.
* A. Use S3 replication to transition infrequently accessed objects to S3 Standard-Infrequent Access (S3 Standard-IA). This solution will not meet the requirement of reducing S3 costs for data with unknown or changing access patterns, as S3 replication is a feature that copies objects across buckets or Regions for redundancy or compliance purposes. It does not automatically move objects to a different storage class based on access frequency2.
* B. Use S3 Lifecycle rules to transition objects from S3 Standard to Standard-Infrequent Access (S3 Standard-IA). This solution will not meet the requirement of reducing S3 costs for data with unknown or changing access patterns, as S3 Standard-IA is a storage class that offers lower storage costs than S3 Standard, but charges a retrieval fee for accessing the data. It is suitable for long-lived and infrequently accessed data, not for data with changing access patterns1.
* D. Use S3 Inventory to identify and transition objects that have not been accessed from S3 Stand-ard to S3 Intelligent-Tiering. This solution will not meet the requirement of reducing S3 costs for data with unknown or changing access patterns, as S3 Inventory is a feature that provides a report of the objects in a bucket and their metadata on a daily or weekly basis. It does not automatically move objects to a different storage class based on access frequency3.
Reference URL: https://aws.amazon.com/s3/storage-classes/intelligent-tiering/
S3 Intelligent-Tiering is the best solution for reducing S3 costs when the access pattern is unpredictable or changing. S3 Intelligent-Tiering automatically moves objects between two access tiers (frequent and infrequent) based on the access frequency, without any performance impact or retrieval fees. S3 Intelligent-Tiering also has an optional archive tier for objects that are rarely accessed. S3 Lifecycle rules can be used to transition objects from S3 Standard to S3 Intelligent-Tiering.
Reference URLs:
1 https://aws.amazon.com/s3/storage-classes/intelligent-tiering/
2 https://docs.aws.amazon.com/AmazonS3/latest/userguide/using-intelligent-tiering.html
3 https://docs.aws.amazon.com/AmazonS3/latest/userguide/intelligent-tiering- overview.html

NEW QUESTION 9
- (Topic 4)
A company's ecommerce website has unpredictable traffic and uses AWS Lambda functions to directly access a private Amazon RDS for PostgreSQL DB instance. The company wants to maintain predictable database performance and ensure that the Lambda invocations do not overload the database with too many connections.
What should a solutions architect do to meet these requirements?

A. Point the client driver at an RDS custom endpoin
B. Deploy the Lambda functions inside a VPC.
C. Point the client driver at an RDS proxy endpoin
D. Deploy the Lambda functions inside a VPC.
E. Point the client driver at an RDS custom endpoin
F. Deploy the Lambda functions outside a VPC.
G. Point the client driver at an RDS proxy endpoin
H. Deploy the Lambda functions outside a VPC.

Answer: B

Explanation:
To maintain predictable database performance and ensure that the Lambda invocations do not overload the database with too many connections, a solutions architect should point the client driver at an RDS proxy endpoint and deploy the Lambda functions inside a VPC. An RDS proxy is a fully managed database proxy that allows applications to share connections to a database, improving database availability and scalability. By using an RDS proxy, the Lambda functions can reuse existing connections, rather than creating new ones for every invocation, reducing the connection overhead and latency. Deploying the Lambda functions inside a VPC allows them to access the private RDS DB instance securely and efficiently, without exposing it to the public internet. References:
? Using Amazon RDS Proxy with AWS Lambda
? Configuring a Lambda function to access resources in a VPC

NEW QUESTION 10
- (Topic 4)
A social media company runs its application on Amazon EC2 instances behind an Application Load Balancer (ALB). The ALB is the origin for an Amazon CloudFront distribution. The application has more than a billion images stored in an Amazon S3 bucket and processes thousands of images each second. The company wants to resize the images dynamically and serve appropriate formats to clients.
Which solution will meet these requirements with the LEAST operational overhead?

A. Install an external image management library on an EC2 instanc
B. Use the image management library to process the images.
C. Create a CloudFront origin request polic
D. Use the policy to automatically resize images and to serve the appropriate format based on the User-Agent HTTP header in the request.
E. Use a Lambda@Edge function with an external image management librar
F. Associate the Lambda@Edge function with the CloudFront behaviors that serve the images.
G. Create a CloudFront response headers polic
H. Use the policy to automatically resize images and to serve the appropriate format based on the User-Agent HTTP header in the request.

Answer: C

Explanation:
Lambda@Edge is a service that allows you to run Lambda functions at CloudFront edge locations. It can be used to modify requests and responses that flow through CloudFront. CloudFront origin request policy is a policy that controls the values (URL query strings, HTTP headers, and cookies) that are included in

requests that CloudFront sends to the origin. It can be used to collect additional information at the origin or to customize the origin response. CloudFront response headers policy is a policy that specifies the HTTP headers that CloudFront removes or adds in responses that it sends to viewers. It can be used to add security or custom headers to responses.
Based on these definitions, the solution that will meet the requirements with the least operational overhead is:
* C. Use a Lambda@Edge function with an external image management library. Associate the Lambda@Edge function with the CloudFront behaviors that serve the images.
This solution would allow the application to use a Lambda@Edge function to resize the images dynamically and serve appropriate formats to clients based on the User-Agent HTTP header in the request. The Lambda@Edge function would run at the edge locations,
reducing latency and load on the origin. The application code would only need to include an external image management library that can perform image manipulation tasks1.

NEW QUESTION 10
- (Topic 4)
A financial company needs to handle highly sensitive data The company will store the data in an Amazon S3 bucket The company needs to ensure that the data is encrypted in transit and at rest The company must manage the encryption keys outside the AWS Cloud
Which solution will meet these requirements?

A. Encrypt the data in the S3 bucket with server-side encryption (SSE) that uses an AWS Key Management Service (AWS KMS) customer managed key
B. Encrypt the data in the S3 bucket with server-side encryption (SSE) that uses an AWS Key Management Service (AWS KMS) AWS managed key
C. Encrypt the data in the S3 bucket with the default server-side encryption (SSE)
D. Encrypt the data at the company's data center before storing the data in the S3 bucket

Answer: D

Explanation:
This option is the only solution that meets the requirements because it allows the company to encrypt the data with its own encryption keys and tools outside the AWS Cloud. By encrypting the data at the company's data center before storing the data in the S3 bucket, the company can ensure that the data is encrypted in transit and at rest, and that the company has full control over the encryption keys and processes. This option also avoids the need to use any AWS encryption services or features, which may not be compatible with the company's security policies or compliance standards.
* A. Encrypt the data in the S3 bucket with server-side encryption (SSE) that uses an AWS Key Management Service (AWS KMS) customer managed key. This option does not meet the requirements because it does not allow the company to manage the encryption keys outside the AWS Cloud. Although the company can create and use its own customer managed key in AWS KMS, the key is still stored and managed by AWS KMS, which is a service within the AWS Cloud. Moreover, the company still needs to use the AWS encryption features and APIs to encrypt and decrypt the data in the S3 bucket, which may not be compatible with the company's security policies or compliance standards.
* B. Encrypt the data in the S3 bucket with server-side encryption (SSE) that uses an AWS Key Management Service (AWS KMS) AWS managed key. This option does not meet the requirements because it does not allow the company to manage the encryption keys outside the AWS Cloud. In this option, the company uses the default AWS managed key in AWS KMS, which is created and managed by AWS on behalf of the company. The company has no control over the key rotation, deletion, or recovery policies. Moreover, the company still needs to use the AWS encryption features and APIs to encrypt and decrypt the data in the S3 bucket, which may not be compatible with the company's security policies or compliance standards.
* C. Encrypt the data in the S3 bucket with the default server-side encryption (SSE). This option does not meet the requirements because it does not allow the company to manage the encryption keys outside the AWS Cloud. In this option, the company uses the default server-side encryption with Amazon S3 managed keys (SSE-S3), which is applied to every bucket in Amazon S3. The company has no visibility or control over the encryption keys, which are managed by Amazon S3. Moreover, the company still needs to use the AWS encryption features and APIs to encrypt and decrypt the data in the S3 bucket, which may not be compatible with the company's security policies or compliance standards. References:
? 1 Protecting data with encryption - Amazon Simple Storage Service
? 2 Protecting data with server-side encryption - Amazon Simple Storage Service
? 3 Protecting data by using client-side encryption - Amazon Simple Storage Service
? 4 AWS Key Management Service Concepts - AWS Key Management Service

NEW QUESTION 13
- (Topic 4)
An image hosting company uploads its large assets to Amazon S3 Standard buckets The company uses multipart upload in parallel by using S3 APIs and overwrites if the same object is uploaded again. For the first 30 days after upload, the objects will be accessed frequently. The objects will be used less frequently after 30 days, but the access patterns for each object will be inconsistent The company must optimize its S3 storage costs while maintaining high availability and resiliency of stored assets.
Which combination of actions should a solutions architect recommend to meet these requirements? (Select TWO.)

A. Move assets to S3 Intelligent-Tiering after 30 days.
B. Configure an S3 Lifecycle policy to clean up incomplete multipart uploads.
C. Configure an S3 Lifecycle policy to clean up expired object delete markers.
D. Move assets to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days
E. Move assets to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.

Answer: AB

Explanation:
S3 Intelligent-Tiering is a storage class that automatically moves data to the most cost-effective access tier based on access frequency, without performance impact, retrieval fees, or operational overhead1. It is ideal for data with unknown or changing access patterns, such as the company's assets. By moving assets to S3 Intelligent-Tiering after 30 days, the company can optimize its storage costs while maintaining high availability and resilience of stored assets.
S3 Lifecycle is a feature that enables you to manage your objects so that they are stored cost effectively throughout their lifecycle2. You can create lifecycle rules to define actions that Amazon S3 applies to a group of objects. One of the actions is to abort incomplete multipart uploads that can occur when an upload is interrupted. By configuring an S3 Lifecycle policy to clean up incomplete multipart uploads, the company can reduce its storage costs and avoid paying for parts that are not used.
Option C is incorrect because expired object delete markers are automatically deleted by Amazon S3 and do not incur any storage costs3. Therefore, configuring an S3 Lifecycle policy to clean up expired object delete markers will not have any effect on the company's storage costs.
Option D is incorrect because S3 Standard-IA is a storage class for data that is accessed less frequently, but requires rapid access when needed1. It has a lower storage cost than S3 Standard, but it has a higher retrieval cost and a minimum storage duration charge of 30 days. Therefore, moving assets to S3 Standard-IA after 30 days may not optimize the company's storage costs if the assets are still accessed occasionally.
Option E is incorrect because S3 One Zone-IA is a storage class for data that is accessed less frequently, but requires rapid access when needed1. It has a lower storage cost than S3 Standard-IA, but it stores data in only one Availability Zone and has less resilience than other storage classes. It also has a higher retrieval cost and a minimum storage duration charge of 30 days. Therefore, moving assets to S3 One Zone-IA after 30 days may not optimize the company's storage

costs if the assets are still accessed occasionally or require high availability. Reference URL: 1: https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html 2: https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lifecycle-mgmt.html 3: https://docs.aws.amazon.com/AmazonS3/latest/userguide/delete-or-empty- bucket.html#delete-bucket-considerations : https://docs.aws.amazon.com/AmazonS3/latest/userguide/mpuoverview.html : https://aws.amazon.com/certification/certified-solutions-architect-associate/

NEW QUESTION 18

- (Topic 4)
A company is creating an application The company stores data from tests of the application in multiple on-premises locations
The company needs to connect the on-premises locations to VPCs in an AWS Region in the AWS Cloud The number of accounts and VPCs will increase during the next year The network architecture must simplify the administration of new connections and must provide the ability to scale.
Which solution will meet these requirements with the LEAST administrative overhead'?

A. Create a peering connection between the VPCs Create a VPN connection between the VPCs and the on-premises locations.
B. Launch an Amazon EC2 instance On the instance, include VPN software that uses a VPN connection to connect all VPCs and on-premises locations.
C. Create a transit gateway Create VPC attachments for the VPC connections Create VPN attachments for the on-premises connections.
D. Create an AWS Direct Connect connection between the on-premises locations and acentral VP
E. Connect the central VPC to other VPCs by using peering connections.

Answer: C

Explanation:
A transit gateway is a network transit hub that enables you to connect your VPCs and on-premises networks in a centralized and scalable way. You can create VPC attachments to connect your VPCs to the transit gateway, and VPN attachments to connect your on-premises networks to the transit gateway over the internet. The transit gateway acts as a router between the attached networks, and simplifies the administration of new connections by reducing the number of peering or VPN connections required. You can also use transit gateway route tables to control the routing of traffic between the attached networks. By creating a transit gateway and using VPC and VPN attachments, you can meet the requirements of the company with the least administrative overhead.
References:
? AWS Transit Gateway
? Transit gateway attachments
? Transit gateway route tables

NEW QUESTION 23

- (Topic 4)
A company hosts a multi-tier web application on Amazon Linux Amazon EC2 instances behind an Application Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones. The company observes that the Auto Scaling group launches more On-Demand Instances when the application's end users access high volumes of static web content. The company wants to optimize cost.
What should a solutions architect do to redesign the application MOST cost-effectively?

A. Update the Auto Scaling group to use Reserved Instances instead of On-Demand Instances.
B. Update the Auto Scaling group to scale by launching Spot Instances instead of On- Demand Instances.
C. Create an Amazon CloudFront distribution to host the static web contents from an Amazon S3 bucket.
D. Create an AWS Lambda function behind an Amazon API Gateway API to host the static website contents.

Answer: C

Explanation:
This answer is correct because it meets the requirements of optimizing cost and reducing the workload on the database. Amazon CloudFront is a content delivery network (CDN) service that speeds up distribution of your static and dynamic web content, such as .html,.css, .js, and image files, to your users. CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you’re serving with CloudFront, the request is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance. You can create an Amazon CloudFront distribution to host the static web contents from an Amazon S3 bucket, which is an origin that you define for CloudFront. This way, you can offload the requests for static web content from your EC2 instances to CloudFront, which can improve the performance and availability of your website, and reduce the cost of running your EC2 instances.
References:
? https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introducti on.html
? https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteHosting.html

NEW QUESTION 24

- (Topic 4)
A company maintains an Amazon RDS database that maps users to cost centers. The company has accounts in an organization in AWS Organizations. The company needs a solution that will tag all resources that are created in a specific AWS account in the organization. The solution must tag each resource with the cost center ID of the user who created the resource.
Which solution will meet these requirements?

A. Move the specific AWS account to a new organizational unit (OU) in Organizations from the management accoun
B. Create a service control policy (SCP) that requires all existing resources to have the correct cost center tag before the resources are create
C. Apply the SCP to the new OU.
D. Create an AWS Lambda function to tag the resources after the Lambda function looks up the appropriate cost center from the RDS databas
E. Configure an Amazon EventBridge rule that reacts to AWS CloudTrail events to invoke the Lambda function.
F. Create an AWS CloudFormation stack to deploy an AWS Lambda functio
G. Configure the Lambda function to look up the appropriate cost center from the RDS database and to tag resource
H. Create an Amazon EventBridge scheduled rule to invoke the CloudFormation stack.
I. Create an AWS Lambda function to tag the resources with a default valu
J. Configure an Amazon EventBridge rule that reacts to AWS CloudTrail events to invoke the Lambda function when a resource is missing the cost center tag.

Answer: B

Explanation:
AWS Lambda is a serverless compute service that lets you run code without provisioning or managing servers. Lambda can be used to tag resources with the

cost center ID of the user who created the resource, by querying the RDS database that maps users to cost centers. Amazon EventBridge is a serverless event bus service that enables event-driven architectures. EventBridge can be configured to react to AWS CloudTrail events, which are recorded API calls made by or on behalf of the AWS account. EventBridge can invoke the Lambda function when a resource is created in the specific AWS account, passing the user identity and resource information as parameters. This solution will meet the requirements, as it enables automatic tagging of resources based on the user and cost center mapping.
References:
? 1 provides an overview of AWS Lambda and its benefits.
? 2 provides an overview of Amazon EventBridge and its benefits.
? 3 explains the concept and benefits of AWS CloudTrail events.

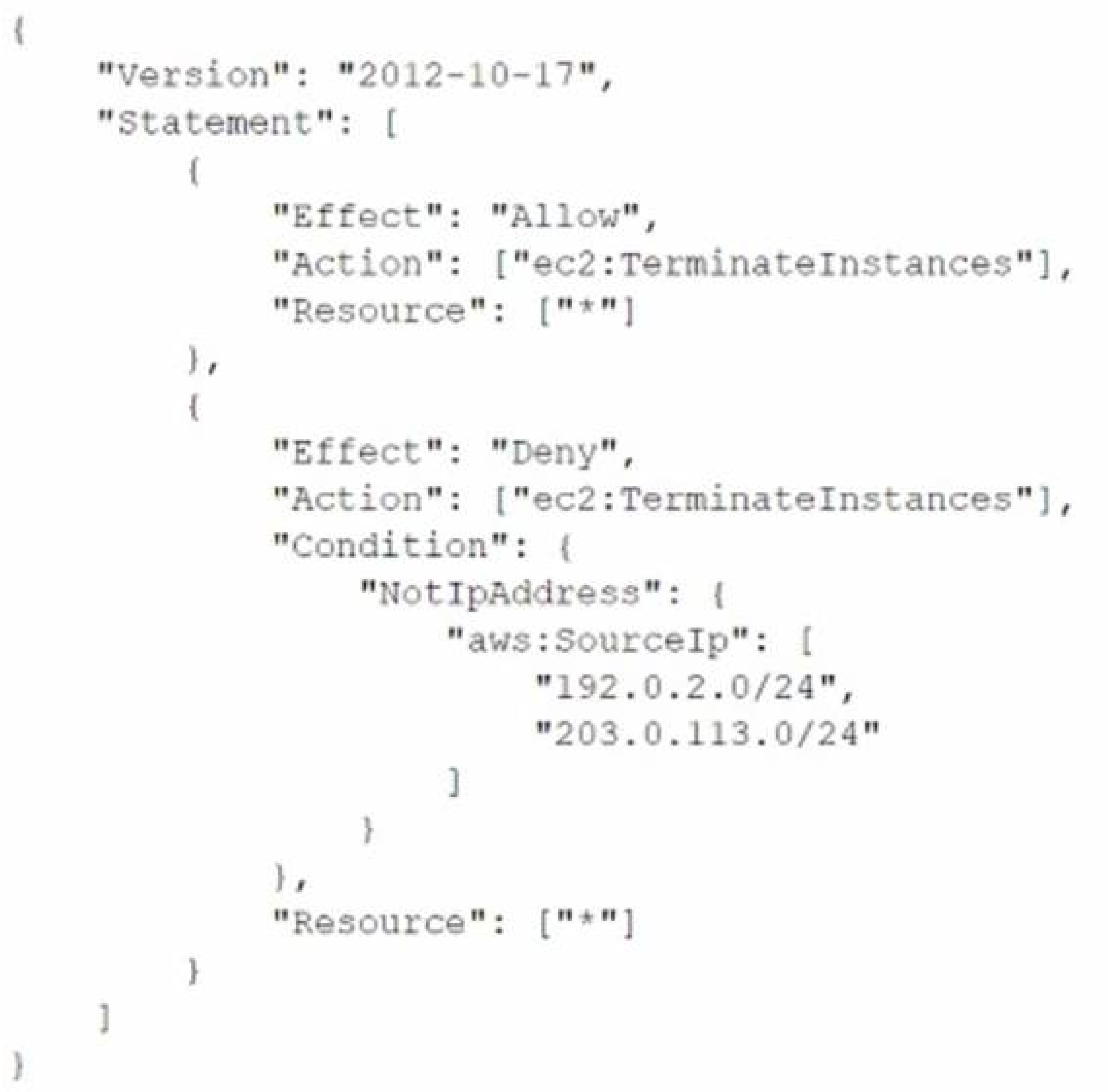
NEW QUESTION 25
- (Topic 4)
An online video game company must maintain ultra-low latency for its game servers. The game servers run on Amazon EC2 instances. The company needs a solution that can
handle millions of UDP internet traffic requests each second.
Which solution will meet these requirements MOST cost-effectively?

A. Configure an Application Load Balancer with the required protocol and ports for the internet traffi
B. Specify the EC2 instances as the targets.
C. Configure a Gateway Load Balancer for the internet traffi
D. Specify the EC2 instances as the targets.
E. Configure a Network Load Balancer with the required protocol and ports for the internet traffi
F. Specify the EC2 instances as the targets.
G. Launch an identical set of game servers on EC2 instances in separate AWS Region
H. Route internet traffic to both sets of EC2 instances.

Answer: C

Explanation:
The most cost-effective solution for the online video game company is to configure a Network Load Balancer with the required protocol and ports for the internet traffic and specify the EC2 instances as the targets. This solution will enable the company to handle millions of UDP requests per second with ultra-low latency and high performance. A Network Load Balancer is a type of Elastic Load Balancing that operates at the connection level (Layer 4) and routes traffic to targets (EC2 instances, microservices, or containers) within Amazon VPC based on IP protocol data. A Network Load Balancer is ideal for load balancing of both TCP and UDP traffic, as it is capable of handling millions of requests per second while maintaining high throughput at ultra-low latency. A Network Load Balancer also preserves the source IP address of the clients to the back-end applications, which can be useful for logging or security purposes1.

NEW QUESTION 28
- (Topic 4)
A company uses Amazon EC2 instances to host its internal systems. As part of a deployment operation, an administrator tries to use the AWS CLI to terminate an EC2 instance. However, the administrator receives a 403 (Access Denied) error message.
The administrator is using an IAM role that has the following IAM policy attached:



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["ec2:TerminateInstances"],
            "Resource": ["*"]
        },
        {
            "Effect": "Deny",
            "Action": ["ec2:TerminateInstances"],
            "Condition": {
                "NotIpAddress": {
                    "aws:SourceIp": [
                        "192.0.2.0/24",
                        "203.0.113.0/24"
                    ]
                }
            },
            "Resource": ["*"]
        }
    ]
}
```

What is the cause of the unsuccessful request?

A. The EC2 instance has a resource-based policy with a Deny statement.
B. The principal has not been specified in the policy statement
C. The "Action" field does not grant the actions that are required to terminate the EC2 instance.

D. The request to terminate the EC2 instance does not originate from the CIDR blocks 192.0.2.0/24 or 203.0 113.0/24

Answer: D

NEW QUESTION 30
- (Topic 4)
A recent analysis of a company's IT expenses highlights the need to reduce backup costs. The company's chief information officer wants to simplify the on-premises backup infrastructure and reduce costs by eliminating the use of physical backup tapes. The company must preserve the existing investment in the on-premises backup applications and workflows.
What should a solutions architect recommend?

A. Set up AWS Storage Gateway to connect with the backup applications using the NFS interface.
B. Set up an Amazon EFS file system that connects with the backup applications using the NFS interface.
C. Set up an Amazon EFS file system that connects with the backup applications using the iSCSI interface.
D. Set up AWS Storage Gateway to connect with the backup applications using the iSCSI- virtual tape library (VTL) interface.

Answer: D

Explanation:
it allows the company to simplify the on-premises backup infrastructure and reduce costs by eliminating the use of physical backup tapes. By setting up AWS Storage Gateway to connect with the backup applications using the iSCSI-virtual tape library (VTL) interface, the company can store backup data on virtual tapes in S3 or Glacier. This preserves the existing investment in the on-premises backup applications and workflows while leveraging AWS storage services.
References:
? AWS Storage Gateway
? Tape Gateway

NEW QUESTION 33
- (Topic 4)
A company is reviewing a recent migration of a three-tier application to a VPC. The security team discovers that the principle of least privilege is not being applied to Amazon EC2 security group ingress and egress rules between the application tiers.
What should a solutions architect do to correct this issue?

A. Create security group rules using the instance ID as the source or destination.
B. Create security group rules using the security group ID as the source or destination.
C. Create security group rules using the VPC CIDR blocks as the source or destination.
D. Create security group rules using the subnet CIDR blocks as the source or destination.

Answer: B

Explanation:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group- rules.html

NEW QUESTION 36
- (Topic 4)
A company wants to migrate an on-premises legacy application to AWS. The application ingests customer order files from an on-premises enterprise resource planning (ERP) system. The application then uploads the files to an SFTP server. The application uses a scheduled job that checks for order files every hour.
The company already has an AWS account that has connectivity to the on-premises network. The new application on AWS must support integration with the existing ERP system. The new application must be secure and resilient and must use the SFTP protocol to process orders from the ERP system immediately.
Which solution will meet these requirements?

A. Create an AWS Transfer Family SFTP internet-facing server in two Availability Zone
B. Use Amazon S3 storag
C. Create an AWS Lambda function to process order file
D. Use S3 Event Notifications to send s3: ObjectCreated: * events to the Lambda function.
E. Create an AWS Transfer Family SFTP internet-facing server in one Availability Zon
F. Use Amazon Elastic File System (Amazon EFS) storag
G. Create an AWS Lambda function to process order file
H. Use a Transfer Family managed workflow to invoke the Lambda function.
I. Create an AWS Transfer Family SFTP internal server in two Availability Zone
J. Use Amazon Elastic File System (Amazon EFS) storag
K. Create an AWS Step Functions state machine to process order file
L. Use Amazon EventBridge Scheduler to invoke the state machine to periodically check Amazon EFS for order files.
M. Create an AWS Transfer Family SFTP internal server in two Availability Zone
N. Use Amazon S3 storag
O. Create an AWS Lambda function to process order file
P. Use a Transfer Family managed workflow to invoke the Lambda function.

Answer: D

Explanation:
This solution meets the requirements because it uses the following components and features:
? AWS Transfer Family SFTP internal server: This allows the application to securely
transfer order files from the on-premises ERP system to AWS using the SFTP protocol over a private connection. The internal server is deployed in two Availability Zones for high availability and fault tolerance.
? Amazon S3 storage: This provides scalable, durable, and cost-effective object
storage for the order files. Amazon S3 also supports encryption at rest and in transit, as well as lifecycle policies and versioning for data protection and compliance.
? AWS Lambda function: This enables the application to process the order files in a
serverless manner, without provisioning or managing servers. The Lambda function can perform any custom logic or transformation on the order files, such as validating, parsing, or enriching the data.

? Transfer Family managed workflow: This simplifies the orchestration of the file
processing tasks by triggering the Lambda function as soon as a file is uploaded to the SFTP server. The managed workflow also provides error handling, retry policies, and logging capabilities.

NEW QUESTION 37
- (Topic 4)
A company is deploying an application that processes large quantities of data in parallel. The company plans to use Amazon EC2 instances for the workload. The network architecture must be configurable to prevent groups of nodes from sharing the same underlying hardware.
Which networking solution meets these requirements?

A. Run the EC2 instances in a spread placement group.
B. Group the EC2 instances in separate accounts.
C. Configure the EC2 instances with dedicated tenancy.
D. Configure the EC2 instances with shared tenancy.

Answer: A

Explanation:
it allows the company to deploy an application that processes large quantities of data in parallel and prevent groups of nodes from sharing the same underlying hardware. By running the EC2 instances in a spread placement group, the company can launch a small number of instances across distinct underlying hardware to reduce correlated failures. A spread placement group ensures that each instance is isolated from each other at the rack level. References:
? Placement Groups
? Spread Placement Groups

NEW QUESTION 42
- (Topic 4)
A company has a mobile chat application with a data store based in Amazon uynamoUb. users would like new messages to be read with as little latency as possible A solutions architect needs to design an optimal solution that requires minimal application changes.
Which method should the solutions architect select?

A. Configure Amazon DynamoDB Accelerator (DAX) for the new messages tabl
B. Update the code to use the DAXendpoint.
C. Add DynamoDB read repticas to handle the increased read loa
D. Update the application to point to the read endpoint for the read replicas.
E. Double the number of read capacity units for the new messages table in DynamoD
F. Continue to use the existing DynamoDB endpoint.
G. Add an Amazon ElastiCache for Redis cache to the application stac
H. Update the application to point to the Redis cache endpoint instead of DynamoDB.

Answer: A

Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/dynamodb-high- latency/
Amazon DynamoDB Accelerator (DAX) is a fully managed in-memory cache for DynamoDB that improves the performance of DynamoDB tables by up to 10 times and
provides microsecond level of response time at any scale. It is compatible with DynamoDB API operations and requires minimal code changes to use1. By configuring DAX for the
new messages table, the solution can reduce the latency for reading new messages with minimal application changes.
* B. Add DynamoDB read repticas to handle the increased read load. Update the application to point to the read endpoint for the read replicas. This solution will not work, as DynamoDB does not support read replicas as a feature. Read replicas are available for Amazon RDS, not for DynamoDB2.
* C. Double the number of read capacity units for the new messages table in DynamoDB. Continue to use the existing DynamoDB endpoint. This solution will not meet the requirement of reading new messages with as little latency as possible, as increasing the
read capacity units will only increase the throughput of DynamoDB, not the performance or latency3.
* D. Add an Amazon ElastiCache for Redis cache to the application stack. Update the application to point to the Redis cache endpoint instead of DynamoDB. This solution will not meet the requirement of minimal application changes, as adding ElastiCache for Redis will require significant code changes to implement caching logic, such as querying cache first, updating cache after writing to DynamoDB, and invalidating cache when needed. Reference URL:
https://aws.amazon.com/dynamodb/dax/

NEW QUESTION 45
- (Topic 4)
A company is building an Amazon Elastic Kubernetes Service (Amazon EKS) cluster for its workloads. All secrets that are stored in Amazon EKS must be encrypted in the Kubernetes etcd key-value store.
Which solution will meet these requirements?

A. Create a new AWS Key Management Service (AWS KMS) key Use AWS Secrets Manager to manage rotate, and store all secrets in Amazon EKS.
B. Create a new AWS Key Management Service (AWS KMS) key Enable Amazon EKS KMS secrets encryption on the Amazon EKS cluster.
C. Create the Amazon EKS cluster with default options Use the Amazon Elastic Block Store (Amazon EBS) Container Storage Interface (CSI) driver as an add-on.
D. Create a new AWS Key Management Service (AWS KMS) key with the ahas/aws/ebs alias Enable default Amazon Elastic Block Store (Amazon EBS) volume encryption for the account.

Answer: B

Explanation:
This option is the most secure and simple way to encrypt the secrets that are stored in Amazon EKS. AWS Key Management Service (AWS KMS) is a service that allows you to create and manage encryption keys that can be used to encrypt your data. Amazon EKS KMS secrets encryption is a feature that enables you to use a KMS key to encrypt the secrets that are stored in the Kubernetes etcd key-value store. This provides an additional layer of protection for your sensitive data, such as passwords, tokens, and keys. You can create a new KMS key or use an existing one, and then enable the Amazon EKS KMS secrets encryption on the Amazon EKS cluster. You can also use IAM policies to control who can access or use the KMS key.
Option A is not correct because using AWS Secrets Manager to manage, rotate, and store all secrets in Amazon EKS is not necessary or efficient. AWS Secrets Manager is a service that helps you securely store, retrieve, and rotate your secrets, such as database credentials, API keys, and passwords. You can use it to

manage secrets that are used by your applications or services outside of Amazon EKS, but it is not designed to encrypt the secrets that are stored in the Kubernetes etcd key-value store. Moreover, using AWS Secrets Manager would incur additional costs and complexity, and it would not leverage the native Kubernetes secrets management capabilities.
Option C is not correct because using the Amazon EBS Container Storage Interface (CSI) driver as an add-on does not encrypt the secrets that are stored in Amazon EKS. The Amazon EBS CSI driver is a plugin that allows you to use Amazon EBS volumes as persistent storage for your Kubernetes pods. It is useful for providing durable and scalable storage for your applications, but it does not affect the encryption of the secrets that are stored in the Kubernetes etcd key-value store. Moreover, using the Amazon EBS CSI driver would require additional configuration and resources, and it would not provide the same level of security as using a KMS key.
Option D is not correct because creating a new AWS KMS key with the alias aws/ebs and enabling default Amazon EBS volume encryption for the account does not encrypt the secrets that are stored in Amazon EKS. The alias aws/ebs is a reserved alias that is used by AWS to create a default KMS key for your account. This key is used to encrypt the Amazon EBS volumes that are created in your account, unless you specify a different KMS key. Enabling default Amazon EBS volume encryption for the account is a setting that ensures that all new Amazon EBS volumes are encrypted by default. However, these features do not affect the encryption of the secrets that are stored in the Kubernetes etcd key-value store. Moreover, using the default KMS key or the default encryption setting would not provide the same level of control and security as using a custom KMS key and enabling the Amazon EKS KMS secrets encryption feature. References:
? Encrypting secrets used in Amazon EKS
? What Is AWS Key Management Service?
? What Is AWS Secrets Manager?
? Amazon EBS CSI driver
? Encryption at rest

NEW QUESTION 49
- (Topic 4)
A company used an Amazon RDS for MySQL DB instance during application testing. Before terminating the DB instance at the end of the test cycle, a solutions architect created two backups. The solutions architect created the first backup by using the mysqldump utility to create a database dump. The solutions architect created the second backup by enabling the final DB snapshot option on RDS termination.
The company is now planning for a new test cycle and wants to create a new DB instance from the most recent backup. The company has chosen a MySQL-compatible edition of Amazon Aurora to host the DB instance.
Which solutions will create the new DB instance? (Select TWO.)

A. Import the RDS snapshot directly into Aurora.
B. Upload the RDS snapshot to Amazon S3. Then import the RDS snapshot into Aurora.
C. Upload the database dump to Amazon S3. Then import the database dump into Aurora.
D. Use AWS Database Migration Service (AWS DMS) to import the RDS snapshot into Aurora.
E. Upload the database dump to Amazon S3. Then use AWS Database Migration Service (AWS DMS) to import the database dump into Aurora.

Answer: AC

Explanation:
These answers are correct because they meet the requirements of creating a new DB instance from the most recent backup and using a MySQL-compatible edition of Amazon Aurora to host the DB instance. You can import the RDS snapshot directly into Aurora if the MySQL DB instance and the Aurora DB cluster are running the same version of MySQL. For example, you can restore a MySQL version 5.6 snapshot directly to Aurora MySQL version 5.6, but you can’t restore a MySQL version 5.6 snapshot directly to Aurora MySQL version 5.7. This method is simple and requires the fewest number of steps. You can upload the database dump to Amazon S3 and then import the database dump into Aurora if the MySQL DB instance and the Aurora DB cluster are running different versions of MySQL. For example, you can import a MySQL version 5.6 database dump into Aurora MySQL version 5.7, but you can’t restore a MySQL version 5.6 snapshot directly to Aurora MySQL version 5.7. This method is more flexible and allows you to migrate across different versions of MySQL.
References:
? https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL
.Migrating.RDSMySQL.Import.html
? https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL
.Migrating.RDSMySQL.Dump.html

NEW QUESTION 52
- (Topic 4)
A company stores multiple Amazon Machine Images (AMIs) in an AWS account to launch its Amazon EC2 instances. The AMIs contain critical data and configurations that are necessary for the company's operations. The company wants to implement a solution that will recover accidentally deleted AMIs quickly and efficiently.
Which solution will meet these requirements with the LEAST operational overhead?

A. Create Amazon Elastic Block Store (Amazon EBS) snapshots of the AMI
B. Store the snapshots in a separate AWS account.
C. Copy all AMIs to another AWS account periodically.
D. Create a retention rule in Recycle Bin.
E. Upload the AMIs to an Amazon S3 bucket that has Cross-Region Replication.

Answer: C

Explanation:
Recycle Bin is a data recovery feature that enables you to restore accidentally deleted Amazon EBS snapshots and EBS-backed AMIs. When using Recycle Bin, if your resources are deleted, they are retained in the Recycle Bin for a time period that you specify before being permanently deleted. You can restore a resource from the Recycle Bin at any time before its retention period expires. This solution has the least operational overhead, as you do not need to create, copy, or upload any additional resources. You can also manage tags and permissions for AMIs in the Recycle Bin. AMIs in the Recycle Bin do not incur any additional charges.
References:
? Recover AMIs from the Recycle Bin
? Recover an accidentally deleted Linux AMI

NEW QUESTION 56
- (Topic 4)
A company runs an infrastructure monitoring service. The company is building a new feature that will enable the service to monitor data in customer AWS accounts. The new feature will call AWS APIs in customer accounts to describe Amazon EC2 instances and read Amazon CloudWatch metrics.
What should the company do to obtain access to customer accounts in the MOST secure way?

A. Ensure that the customers create an 1AM role in their account with read-only EC2 and CloudWatch permissions and a trust policy to the company's account.
B. Create a serverless API that implements a token vending machine to provide temporary AWS credentials for a role with read-only EC2 and CloudWatch permissions.
C. Ensure that the customers create an 1AM user in their account with read-only EC2 and CloudWatch permission
D. Encrypt and store customer access and secret keys in a secrets management system.
E. Ensure that the customers create an Amazon Cognito user in their account to use an 1AM role with read-only EC2 and CloudWatch permission
F. Encrypt and store the Amazon Cognito user and password in a secrets management system.

Answer: A

Explanation:
By having customers create an IAM role with the necessary permissions in their own accounts, the company can use AWS Identity and Access Management (IAM) to establish cross-account access. The trust policy allows the company's AWS account to assume the customer's IAM role temporarily, granting access to the specified resources (EC2 instances and CloudWatch metrics) within the customer's account. This approach follows the principle of least privilege, as the company only requests the necessary permissions and does not require long-term access keys or user credentials from the customers.

NEW QUESTION 60
- (Topic 4)
A company has deployed a multiplayer game for mobile devices. The game requires live
location tracking of players based on latitude and longitude. The data store for the game must support rapid updates and retrieval of locations.
The game uses an Amazon RDS for PostgreSQL DB instance with read replicas to store the location data. During peak usage periods, the database is unable to maintain the performance that is needed for reading and writing updates. The game's user base is increasing rapidly.
What should a solutions architect do to improve the performance of the data tier?

A. Take a snapshot of the existing DB instanc
B. Restore the snapshot with Multi-AZ enabled.
C. Migrate from Amazon RDS to Amazon OpenSearch Service with OpenSearch Dashboards.
D. Deploy Amazon DynamoDB Accelerator (DAX) in front of the existing DB instanc
E. Modify the game to use DAX.
F. Deploy an Amazon ElastiCache for Redis cluster in front of the existing DB instanc
G. Modify the game to use Redis.

Answer: D

Explanation:
The solution that will improve the performance of the data tier is to deploy an Amazon ElastiCache for Redis cluster in front of the existing DB instance and modify the game to use Redis. This solution will enable the game to store and retrieve the location data of the players in a fast and scalable way, as Redis is an in-memory data store that supports geospatial data types and commands. By using ElastiCache for Redis, the game can reduce the load on the RDS for PostgreSQL DB instance, which is not optimized for high-frequency updates and queries of location data. ElastiCache for Redis also supports replication, sharding, and auto scaling to handle the increasing user base of the game. The other solutions are not as effective as the first one because they either do not improve the performance, do not support geospatial data, or do not leverage caching. Taking a snapshot of the existing DB instance and restoring it with Multi-AZ enabled will not improve the performance of the data tier, as it only provides high availability and durability, but not scalability or low latency. Migrating from Amazon RDS to Amazon OpenSearch Service with OpenSearch Dashboards will not improve the performance of the data tier, as OpenSearch Service is mainly designed for full-text search and analytics, not for real-time location tracking. OpenSearch Service also does not support geospatial data types and commands natively, unlike Redis. Deploying Amazon DynamoDB Accelerator (DAX) in front of the existing DB instance and modifying the game to use DAX will not improve the performance of the data tier, as DAX is only compatible with DynamoDB, not with RDS for PostgreSQL. DAX also does not support geospatial data types and commands.
References:
? Amazon ElastiCache for Redis
? Geospatial Data Support - Amazon ElastiCache for Redis
? Amazon RDS for PostgreSQL
? Amazon OpenSearch Service
? Amazon DynamoDB Accelerator (DAX)

NEW QUESTION 63
- (Topic 4)
A solutions architect is designing a REST API in Amazon API Gateway for a cash payback service The application requires 1 GB of memory and 2 GB of storage for its computation resources. The application will require that the data is in a relational format.
Which additional combination of AWS services will meet these requirements with the LEAST administrative effort? {Select TWO.)

A. Amazon EC2
B. AWS Lambda
C. Amazon RDS
D. Amazon DynamoDB
E. Amazon Elastic Kubernetes Services (Amazon EKS)

Answer: BC

Explanation:
AWS Lambda is a service that lets users run code without provisioning or managing servers. It automatically scales and manages the underlying compute resources for the code. It supports multiple languages, such as Java, Python, Node.js, and G1o. By using AWS Lambda for the REST API, the solution can meet the requirements of 1 GB of memory and minimal administrative effort.
Amazon RDS is a service that makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups. It supports multiple database engines, such as MySQL, PostgreSQL, Oracle, and SQL Server2. By using Amazon RDS for the data store, the solution can meet the requirements of 2 GB of storage and a relational format.
* A. Amazon EC2. This solution will not meet the requirement of minimal administrative effort, as Amazon EC2 is a service that provides virtual servers in the cloud that users have to configure and manage themselves. It requires users to choose an instance type, an operating system, a security group, and other options3.
* D. Amazon DynamoDB. This solution will not meet the requirement of a relational format, as Amazon DynamoDB is a service that provides a key-value and document database that delivers single-digit millisecond performance at any scale. It is a non-relational or NoSQL database that does not support joins or transactions.
* E. Amazon Elastic Kubernetes Services (Amazon EKS). This solution will not meet the requirement of minimal administrative effort, as Amazon EKS is a service

that provides a fully managed Kubernetes service that users have to configure and manage themselves. It requires users to create clusters, nodes groups, pods, services, and other Kubernetes resources.
Reference URL: https://aws.amazon.com/lambda/

NEW QUESTION 65
- (Topic 4)
A retail company has several businesses. The IT team for each business manages its own AWS account. Each team account is part of an organization in AWS Organizations. Each team monitors its product inventory levels in an Amazon DynamoDB table in the team's own AWS account.
The company is deploying a central inventory reporting application into a shared AWS account. The application must be able to read items from all the teams' DynamoDB tables.
Which authentication option will meet these requirements MOST securely?

A. Integrate DynamoDB with AWS Secrets Manager in the inventory application accoun
B. Configure the application to use the correct secret from Secrets Manager to authenticate and read the DynamoDB tabl
C. Schedule secret rotation for every 30 days.
D. In every business account, create an 1AM user that has programmatic acces
E. Configure the application to use the correct 1AM user access key ID and secret access key to authenticate and read the DynamoDB tabl
F. Manually rotate 1AM access keys every 30 days.
G. In every business account, create an 1AM role named BU_ROLE with a policy that gives the role access to the DynamoDB table and a trust policy to trust a specific role in the inventory application accoun
H. In the inventory account, create a role named APP_ROLE that allows access to the STS AssumeRole API operatio
I. Configure the application to use APP_ROLE and assume the cross-account role BU_ROLE to read the DynamoDB table.
J. Integrate DynamoDB with AWS Certificate Manager (ACM). Generate identity certificates to authenticate DynamoD
K. Configure the application to use the correct certificate to authenticate and read the DynamoDB table.

Answer: C

Explanation:
This solution meets the requirements most securely because it uses IAM roles and the STS AssumeRole API operation to authenticate and authorize the inventory application to access the DynamoDB tables in different accounts. IAM roles are more secure than IAM users or certificates because they do not require long-term credentials or passwords. Instead, IAM roles provide temporary security credentials that are automatically rotated and can be configured with a limited duration. The STS AssumeRole API operation enables you to request temporary credentials for a role that you are allowed to assume. By using this operation, you can delegate access to resources that are in different AWS accounts that you own or that are owned by third parties. The trust policy of the role defines which entities can assume the role, and the permissions policy of the role defines which actions can be performed on the resources. By using this solution, you can avoid hard- coding credentials or certificates in the inventory application, and you can also avoid storing them in Secrets Manager or ACM. You can also leverage the built-in security features of IAM and STS, such as MFA, access logging, and policy conditions.
References:
? IAM Roles
? STS AssumeRole
? Tutorial: Delegate Access Across AWS Accounts Using IAM Roles

NEW QUESTION 68
- (Topic 4)
A company runs a three-tier application in two AWS Regions. The web tier, the application tier, and the database tier run on Amazon EC2 instances. The company uses Amazon RDS for Microsoft SQL Server Enterprise for the database tier The database tier is experiencing high load when weekly and monthly reports are run. The company wants to reduce the load on the database tier.
Which solution will meet these requirements with the LEAST administrative effort?

A. Create read replica
B. Configure the reports to use the new read replicas.
C. Convert the RDS database to Amazon DynamoDB_ Configure the reports to use DynamoDB
D. Modify the existing RDS DB instances by selecting a larger instance size.
E. Modify the existing ROS DB instances and put the instances into an Auto Scaling group.

Answer: A

Explanation:
it allows the company to create read replicas of its RDS database and reduce the load on the database tier. By creating read replicas, the company can offload read traffic from the primary database instance to one or more replicas. By configuring the reports to use the new read replicas, the company can improve performance and availability of its database tier. References:
? Working with Read Replicas
? Read Replicas for Amazon RDS for SQL Server

NEW QUESTION 70
- (Topic 4)
A company needs to integrate with a third-party data feed. The data feed sends a webhook to notify an external service when new data is ready for consumption A developer wrote an AWS Lambfe function to retrieve data when the company receives a webhook callback The developer must make the Lambda function available for the third party to call.
Which solution will meet these requirements with the MOST operational efficiency?

A. Create a function URL for the Lambda functio
B. Provide the Lambda function URL to the third party for the webhook.
C. Deploy an Application Load Balancer (ALB) in front of the Lambda functio
D. Provide the ALB URL to the third party for the webhook
E. Create an Amazon Simple Notification Service (Amazon SNS) topi
F. Attach the topic to the Lambda functio
G. Provide the public hostname of the SNS topic to the third party for the webhook.
H. Create an Amazon Simple Queue Service (Amazon SQS) queu
I. Attach the queue to the Lambda functio
J. Provide the public hostname of the SQS queue to the third party forthe webhook.

Answer: A

Explanation:
A function URL is a unique identifier for a Lambda function that can be used to invoke the function over HTTPS. It is composed of the API endpoint of the AWS Region where the function is deployed, and the name or ARN of the function1. By creating a function URL for the Lambda function, the solution can make the Lambda function available for the third party to call with the most operational efficiency.
* B. Deploy an Application Load Balancer (ALB) in front of the Lambda function. Provide the ALB URL to the third party for the webhook. This solution will not meet the requirement of the most operational efficiency, as it involves creating and managing an additional resource (ALB) that is not necessary for invoking a Lambda function over HTTPS2.
* C. Create an Amazon Simple Notification Service (Amazon SNS) topic. Attach the topic to the Lambda function. Provide the public hostname of the SNS topic to the third party for the webhook. This solution will not work, as Amazon SNS topics do not have public hostnames that can be used as webhooks. SNS topics are used to publish messages to subscribers, not to receive messages from external sources3.
* D. Create an Amazon Simple Queue Service (Amazon SQS) queue. Attach the queue to the Lamb-da function. Provide the public hostname of the SQS queue to the third party for the webhook. This solution will not work, as Amazon SQS queues do not have public hostnames that can be used as webhooks. SQS queues are used to send, store, and receive messages between AWS services, not to receive messages from external sources. Reference URL:
https://docs.aws.amazon.com/lambda/latest/dg/lambda-api-permissions- ref.html

NEW QUESTION 73
- (Topic 4)
A company runs a container application by using Amazon Elastic Kubernetes Service (Amazon EKS). The application includes microservices that manage customers and place orders. The company needs to route incoming requests to the appropriate microservices.
Which solution will meet this requirement MOST cost-effectively?

A. Use the AWS Load Balancer Controller to provision a Network Load Balancer.
B. Use the AWS Load Balancer Controller to provision an Application Load Balancer.
C. Use an AWS Lambda function to connect the requests to Amazon EKS.
D. Use Amazon API Gateway to connect the requests to Amazon EKS.

Answer: B

Explanation:
An Application Load Balancer is a type of Elastic Load Balancer that operates at the application layer (layer 7) of the OSI model. It can distribute incoming traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions. It can also route requests based on the content of the request, such as the host name, path, or query parameters1.
The AWS Load Balancer Controller is a controller that helps you manage Elastic Load Balancers for your Kubernetes cluster. It can provision Application Load Balancers or Network Load Balancers when you create Kubernetes Ingress or Service resources2.
By using the AWS Load Balancer Controller to provision an Application Load Balancer for your Amazon EKS cluster, you can achieve the following benefits:
? You can route incoming requests to the appropriate microservices based on the
rules you define in your Ingress resource. For example, you can route requests with different host names or paths to different microservices that handle customers and orders2.
? You can improve the performance and availability of your container applications by
distributing the load across multiple targets and enabling health checks and automatic scaling1.
? You can reduce the cost and complexity of managing your load balancers by using
a single controller that integrates with Amazon EKS and Kubernetes. You do not need to manually create or configure load balancers or update them when your cluster changes2.

NEW QUESTION 78
- (Topic 4)
A company wants to use an event-driven programming model with AWS Lambda. The company wants to reduce startup latency for Lambda functions that run on Java 11. The company does not have strict latency requirements for the applications. The company wants to reduce cold starts and outlier latencies when a function scales up.
Which solution will meet these requirements MOST cost-effectively?

A. Configure Lambda provisioned concurrency.
B. Increase the timeout of the Lambda functions.
C. Increase the memory of the Lambda functions.
D. Configure Lambda SnapStart.

Answer: D

Explanation:
To reduce startup latency for Lambda functions that run on Java 11, Lambda SnapStart is a suitable solution. Lambda SnapStart is a feature that enables faster cold starts and lower outlier latencies for Java 11 functions. Lambda SnapStart uses a pre- initialized Java Virtual Machine (JVM) to run the functions, which reduces the initialization time and memory footprint. Lambda SnapStart does not incur any additional charges. References:
? Lambda SnapStart for Java 11 Functions
? Lambda SnapStart FAQs

NEW QUESTION 79
- (Topic 4)
A company has a three-tier application for image sharing. The application uses an Amazon EC2 instance for the front-end layer, another EC2 instance for the application layer, and a third EC2 instance for a MySQL database. A solutions architect must design a scalable and highly available solution that requires the least amount of change to the application.
Which solution meets these requirements?

A. Use Amazon S3 to host the front-end laye
B. Use AWS Lambda functions for the application laye
C. Move the database to an Amazon DynamoDB tabl
D. Use Amazon S3 to store and serve users’ images.
E. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end layer and the application laye
F. Move the database to an Amazon RDS DB instance with multiple read replicas to serve users’ images.

G. Use Amazon S3 to host the front-end laye
H. Use a fleet of EC2 instances in an Auto Scaling group for the application laye
I. Move the database to a memory optimized instance type to store and serve users' images.
J. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end layer and the application laye
K. Move the database to an Amazon RDS Multi-AZ DB instanc
L. Use Amazon S3 to store and serve users' images.

Answer: D

Explanation:
for "Highly available": Multi-AZ & for "least amount of changes to the application": Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring

NEW QUESTION 80
- (Topic 4)
A company runs multiple workloads in its on-premises data center. The company's data center cannot scale fast enough to meet the company's expanding business needs. The company wants to collect usage and configuration data about the on-premises servers and workloads to plan a migration to AWS.
Which solution will meet these requirements?

A. Set the home AWS Region in AWS Migration Hu
B. Use AWS Systems Manager to collect data about the on-premises servers.
C. Set the home AWS Region in AWS Migration Hu
D. Use AWS Application Discovery Service to collect data about the on-premises servers.
E. Use the AWS Schema Conversion Tool (AWS SCT) to create the relevant template
F. Use AWS Trusted Advisor to collect data about the on-premises servers.
G. Use the AWS Schema Conversion Tool (AWS SCT) to create the relevant templates.Use AWS Database Migration Service (AWS DMS) to collect data about the on-premises servers.

Answer: B

Explanation:
The most suitable solution for the company's requirements is to set the home AWS Region in AWS Migration Hub and use AWS Application Discovery Service to collect data about the on-premises servers. This solution will enable the company to gather usage and configuration data of its on-premises servers and workloads, and plan a migration to AWS.
AWS Migration Hub is a service that simplifies and accelerates migration tracking by aggregating migration status information into a single console. Users can view the discovered servers, group them into applications, and track the migration status of each application from the Migration Hub console in their home Region. The home Region is the AWS Region where users store their migration data, regardless of which Regions they migrate into1.
AWS Application Discovery Service is a service that helps users plan their migration to AWS by collecting usage and configuration data about their on-premises servers and databases. Application Discovery Service is integrated with AWS Migration Hub and supports two methods of performing discovery: agentless discovery and agent-based discovery. Agentless discovery can be performed by deploying the Application Discovery Service Agentless Collector through VMware vCenter, which collects static configuration data and utilization data for virtual machines (VMs) and databases. Agent-based discovery can be performed by deploying the AWS Application Discovery Agent on each of the VMs and physical servers, which collects static configuration data, detailed time-series system-performance information, inbound and outbound network connections, and processes that are running2.
The other options are not correct because they do not meet the requirements or are not relevant for the use case. Using the AWS Schema Conversion Tool (AWS SCT) to create the relevant templates and using AWS Trusted Advisor to collect data about the on- premises servers is not correct because this solution is not suitable for collecting usage and configuration data of on-premises servers and workloads. AWS SCT is a tool that helps users convert database schemas and code objects from one database engine to another, such as from Oracle to PostgreSQL3. AWS Trusted Advisor is a service that provides best practice recommendations for cost optimization, performance, security, fault tolerance, and service limits4. Using the AWS Schema Conversion Tool (AWS SCT) to create the relevant templates and using AWS Database Migration Service (AWS DMS) to collect data about the on-premises servers is not correct because this solution is not suitable for collecting usage and configuration data of on-premises servers and workloads. As mentioned above, AWS SCT is a tool that helps users convert database schemas and code objects from one database engine to another. AWS DMS is a service that helps users migrate relational databases, non-relational databases, and other types of data stores to
AWS with minimal downtime5. References:
? Home Region - AWS Migration Hub
? What is AWS Application Discovery Service? - AWS Application Discovery Service
? AWS Schema Conversion Tool - Amazon Web Services
? What Is Trusted Advisor? - Trusted Advisor
? What Is AWS Database Migration Service? - AWS Database Migration Service

NEW QUESTION 83
- (Topic 4)
A company uses Amazon S3 as its data lake. The company has a new partner that must use SFTP to upload data files A solutions architect needs to implement a highly available SFTP solution that minimizes operational overhead.
Which solution will meet these requirements?

A. Use AWS Transfer Family to configure an SFTP-enabled server with a publicly accessible endpoint Choose the S3 data lake as the destination
B. Use Amazon S3 File Gateway as an SFTP server Expose the S3 File Gateway endpoint URL to the new partner Share the S3 File Gateway endpoint with the newpartner
C. Launch an Amazon EC2 instance in a private subnet in a VP
D. Instruct the new partner to upload files to the EC2 instance by using a VP
E. Run a cron job script on the EC2 instance to upload files to the S3 data lake
F. Launch Amazon EC2 instances in a private subnet in a VP
G. Place a Network Load Balancer (NLB) in front of the EC2 instance
H. Create an SFTP listener port for the NLBShare the NLB hostname with the new partner Run a cron job script on the EC2 instances to upload files to the S3 data lake.

Answer: A

Explanation:
This option is the most cost-effective and simple way to enable SFTP access to the S3 data lake. AWS Transfer Family is a fully managed service that supports secure file transfers over SFTP, FTPS, and FTP protocols. You can create an SFTP-enabled server with a public endpoint and associate it with your S3 bucket.

You can also use AWS Identity and Access Management (IAM) roles and policies to control access to your S3 data lake. The service scales automatically to handle any volume of file transfers and provides high availability and durability. You do not need to provision, manage, or patch any servers or load balancers.
Option B is not correct because Amazon S3 File Gateway is not an SFTP server. It is a hybrid cloud storage service that provides a local file system interface to S3. You can use it to store and retrieve files as objects in S3 using standard file protocols such as NFS and SMB. However, it does not support SFTP protocol, and it requires deploying a file gateway appliance on-premises or on EC2.
Option C is not cost-effective or scalable because it requires launching and managing an EC2 instance in a private subnet and setting up a VPN connection for the new partner. This would incur additional costs for the EC2 instance, the VPN connection, and the data transfer. It would also introduce complexity and security risks to the solution. Moreover, it would require running a cron job script on the EC2 instance to upload files to the S3 data lake, which is not efficient or reliable.
Option D is not cost-effective or scalable because it requires launching and managing multiple EC2 instances in a private subnet and placing a NLB in front of them. This would incur additional costs for the EC2 instances, the NLB, and the data transfer. It would also introduce complexity and security risks to the solution. Moreover, it would require running a cron job script on the EC2 instances to upload files to the S3 data lake, which is not efficient or reliable. References:
? What Is AWS Transfer Family?
? What Is Amazon S3 File Gateway?
? What Is Amazon EC2?
? [What Is Amazon Virtual Private Cloud?]
? [What Is a Network Load Balancer?]

NEW QUESTION 86
- (Topic 4)
A company has resources across multiple AWS Regions and accounts. A newly hired solutions architect discovers a previous employee did not provide details about the resources invent^. The solutions architect needs to build and map the relationship details of the various workloads across all accounts.
Which solution will meet these requirements in the MOST operationally efficient way?

A. Use AWS Systems Manager Inventory to generate a map view from the detailed view report.
B. Use AWS Step Functions to collect workload details Build architecture diagrams of theworkloads manually.
C. Use Workload Discovery on AWS to generate architecture diagrams of the workloads.
D. Use AWS X-Ray to view the workload details Build architecture diagrams with relationships

Answer: C

Explanation:
Workload Discovery on AWS (formerly called AWS Perspective) is a tool that visualizes AWS Cloud workloads. It maintains an inventory of the AWS resources across your accounts and Regions, mapping relationships between them, and displaying them in a web UI. It also allows you to query AWS Cost and Usage Reports, search for resources, save and export architecture diagrams, and more1. By using Workload Discovery on AWS, the solution can build and map the relationship details of the various workloads across all accounts with the least operational effort.
* A. Use AWS Systems Manager Inventory to generate a map view from the detailed view report. This solution will not meet the requirement of building and mapping the relationship details of the various workloads across all accounts, as AWS Systems Manager Inventory is a feature that collects metadata from your managed instances and stores it in a central Amazon S3 bucket. It does not provide a map view or architecture diagrams of the workloads2.
* B. Use AWS Step Functions to collect workload details Build architecture diagrams of the work-loads manually. This solution will not meet the requirement of the least operational effort, as it involves creating and managing state machines to orchestrate the workload details collection, and building architecture diagrams manually.
* D. Use AWS X-Ray to view the workload details Build architecture diagrams with relationships. This solution will not meet the requirement of the least operational effort, as it involves instrumenting your applications with X-Ray SDKs to collect workload details, and building architecture diagrams manually.
Reference URL: https://aws.amazon.com/solutions/implementations/workload-discovery- on-aws/

NEW QUESTION 87
- (Topic 4)
A company's reporting system delivers hundreds of .csv files to an Amazon S3 bucket each day. The company must convert these files to Apache Parquet format and must store the files in a transformed data bucket.
Which solution will meet these requirements with the LEAST development effort?

A. Create an Amazon EMR cluster with Apache Spark installe
B. Write a Spark application to transform the dat
C. Use EMR File System (EMRFS) to write files to the transformed data bucket.
D. Create an AWS Glue crawler to discover the dat
E. Create an AWS Glue extract, transform, and load (ETL) job to transform the dat
F. Specify the transformed data bucket in the output step.
G. Use AWS Batch to create a job definition with Bash syntax to transform the data and output the data to the transformed data bucke
H. Use the job definition to submit a jo
I. Specify an array job as the job type.
J. Create an AWS Lambda function to transform the data and output the data to the transformed data bucke
K. Configure an event notification for the S3 bucke
L. Specify the Lambda function as the destination for the event notification.

Answer: B

Explanation:
https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/three- aws-glue-etl-job-types-for-converting-data-to-apache-parquet.html

NEW QUESTION 89
- (Topic 4)
A company wants to manage Amazon Machine Images (AMIs). The company currently copies AMIs to the same AWS Region where the AMIs were created. The company needs to design an application that captures AWS API calls and sends alerts whenever the Amazon EC2 CreateImage API operation is called within the company's account.
Which solution will meet these requirements with the LEAST operational overhead?

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

D. Configure the target as an Amazon Simple Notification Service (Amazon SNS) topic to send an alert when a CreateImage API call is detected.
E. Configure an Amazon Simple Queue Service (Amazon SQS) FIFO queue as a target for AWS CloudTrail log
F. Create an AWS Lambda function to send an alert to an Amazon Simple Notification Service (Amazon SNS) topic when a CreateImage API call is detected.

Answer: C

Explanation:
https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/monitor-ami-events.html#:~:text=For%20example%2C%20you%20can%20create%20an%20EventBridge%20rule%20that%20detects%20when%20the%20AMI%20creation%20process%20has%20completed%20and%20then%20invokes%20an%20Amazon%20SNS%20topic%20to% 20send%20an%20email%20notification%20to%20you.

NEW QUESTION 92
- (Topic 4)
A company previously migrated its data warehouse solution to AWS. The company also has an AWS Direct Connect connection. Corporate office users query the data warehouse using a visualization tool. The average size of a query returned by the data warehouse is 50 MB and each webpage sent by the visualization tool is approximately 500 KB. Result sets returned by the data warehouse are not cached.
Which solution provides the LOWEST data transfer egress cost for the company?

A. Host the visualization tool on premises and query the data warehouse directly over the internet.
B. Host the visualization tool in the same AWS Region as the data warehous
C. Access it over the internet.
D. Host the visualization tool on premises and query the data warehouse directly over a Direct Connect connection at a location in the same AWS Region.
E. Host the visualization tool in the same AWS Region as the data warehouse and access it over a Direct Connect connection at a location in the same Region.

Answer: D

Explanation:
https://aws.amazon.com/directconnect/pricing/ https://aws.amazon.com/blogs/aws/aws-data-transfer-prices-reduced/

NEW QUESTION 97
- (Topic 4)
A company runs a container application on a Kubernetes cluster in the company's data center The application uses Advanced Message Queuing Protocol (AMQP) to communicate with a message queue The data center cannot scale fast enough to meet the company's expanding business needs The company wants to migrate the workloads to AWS
Which solution will meet these requirements with the LEAST operational overhead? \

A. Migrate the container application to Amazon Elastic Container Service (Amazon ECS) Use Amazon Simple Queue Service (Amazon SQS) to retrieve the messages.
B. Migrate the container application to Amazon Elastic Kubernetes Service (Amazon EKS) Use Amazon MQ to retrieve the messages.
C. Use highly available Amazon EC2 instances to run the application Use Amazon MQ to retrieve the messages.
D. Use AWS Lambda functions to run the application Use Amazon Simple Queue Service (Amazon SQS) to retrieve the messages.

Answer: B

Explanation:
This option is the best solution because it allows the company to migrate the container application to AWS with minimal changes and leverage a managed service to run the Kubernetes cluster and the message queue. By using Amazon EKS, the company can run the container application on a fully managed Kubernetes control plane that is compatible with the existing Kubernetes tools and plugins. Amazon EKS handles the provisioning, scaling, patching, and security of the Kubernetes cluster, reducing the operational overhead and complexity. By using Amazon MQ, the company can use a fully managed message broker service that supports AMQP and other popular messaging protocols. Amazon MQ handles the administration, maintenance, and scaling of the message broker, ensuring high availability, durability, and security of the messages.
* A. Migrate the container application to Amazon Elastic Container Service (Amazon ECS) Use Amazon Simple Queue Service (Amazon SQS) to retrieve the messages. This option is not optimal because it requires the company to change the container orchestration platform from Kubernetes to ECS, which can introduce additional complexity and risk. Moreover, it requires the company to change the messaging protocol from AMQP to SQS, which can also affect the application logic and performance. Amazon ECS and Amazon SQS are both fully managed services that simplify the deployment and management of containers and messages, but they may not be compatible with the existing application architecture and requirements.
* C. Use highly available Amazon EC2 instances to run the application Use Amazon MQ to retrieve the messages. This option is not ideal because it requires the company to manage the EC2 instances that host the container application. The company would need to provision, configure, scale, patch, and monitor the EC2 instances, which can increase the operational overhead and infrastructure costs. Moreover, the company would need to install and maintain the Kubernetes software on the EC2 instances, which can also add complexity and risk. Amazon MQ is a fully managed message broker service that supports AMQP and other popular messaging protocols, but it cannot compensate for the lack of a managed Kubernetes service.
* D. Use AWS Lambda functions to run the application Use Amazon Simple Queue Service (Amazon SQS) to retrieve the messages. This option is not feasible because AWS Lambda does not support running container applications directly. Lambda functions are executed in a sandboxed environment that is isolated from other functions and resources. To run container applications on Lambda, the company would need to use a custom runtime or a wrapper library that emulates the container API, which can introduce additional complexity and overhead. Moreover, Lambda functions have limitations in terms of available CPU, memory, and runtime, which may not suit the application needs. Amazon SQS is a fully managed message queue service that supports asynchronous communication, but it does not support AMQP or other messaging protocols.
References:
? 1 Amazon Elastic Kubernetes Service - Amazon Web Services
? 2 Amazon MQ - Amazon Web Services
? 3 Amazon Elastic Container Service - Amazon Web Services
? 4 AWS Lambda FAQs - Amazon Web Services

NEW QUESTION 101
- (Topic 4)
A company wants to create an application to store employee data in a hierarchical structured relationship. The company needs a minimum-latency response to high-traffic queries for the employee data and must protect any sensitive data. The company also needs to receive monthly email messages if any financial information is present in the employee data.
Which combination of steps should a solutions architect take to meet these requirements? (Select TWO.)

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

Answer: BE

Explanation:
Generally, for building a hierarchical relationship model, a graph database such as Amazon Neptune is a better choice. In some cases, however, DynamoDB is a better choice for hierarchical data modeling because of its flexibility, security, performance, and scale. https://docs.aws.amazon.com/prescriptive-guidance/latest/dynamodb- hierarchical-data-model/introduction.html

NEW QUESTION 103
- (Topic 4)
An ecommerce company stores terabytes of customer data in the AWS Cloud. The data contains personally identifiable information (Pll). The company wants to use the data in three applications. Only one of the applications needs to process the Pll. The Pll must be removed before the other two applications process the data.
Which solution will meet these requirements with the LEAST operational overhead?

A. Store the data in an Amazon DynamoDB tabl
B. Create a proxy application layer to intercept and process the data that each application requests.
C. Store the data in an Amazon S3 bucke
D. Process and transform the data by using S3 Object Lambda before returning the data to the requesting application.
E. Process the data and store the transformed data in three separate Amazon S3 buckets so that each application has its own custom datase
F. Point each application to its respectiveS3 bucket.
G. Process the data and store the transformed data in three separate Amazon DynamoDB tables so that each application has its own custom datase
H. Point each application to its respective DynamoDB table.

Answer: B

Explanation:
https://aws.amazon.com/blogs/aws/introducing-amazon-s3-object-lambda- use-your-code-to-process-data-as-it-is-being-retrieved-from-s3/
S3 Object Lambda is a new feature of Amazon S3 that enables customers to add their own code to process data retrieved from S3 before returning it to the application. By using S3 Object Lambda, the data can be processed and transformed in real-time, without the need to store multiple copies of the data in separate S3 buckets or DynamoDB tables.
In this case, the Pll can be removed from the data by the code added to S3 Object Lambda before returning the data to the two applications that do not need to process Pll. The one application that requires Pll can be pointed to the original S3 bucket where the Pll is still stored.
Using S3 Object Lambda is the simplest and most cost-effective solution, as it eliminates the need to maintain multiple copies of the same data in different buckets or tables, which can result in additional storage costs and operational overhead.

NEW QUESTION 105
- (Topic 4)
A company has data collection sensors at different locations. The data collection sensors stream a high volume of data to the company. The company wants to design a platform on AWS to ingest and process high-volume streaming data. The solution must be scalable and support data collection in near real time. The company must store the data in Amazon S3 for future reporting.
Which solution will meet these requirements with the LEAST operational overhead?

A. Use Amazon Kinesis Data Firehose to deliver streaming data to Amazon S3.
B. Use AWS Glue to deliver streaming data to Amazon S3.
C. Use AWS Lambda to deliver streaming data and store the data to Amazon S3.
D. Use AWS Database Migration Service (AWS DMS) to deliver streaming data to Amazon S3.

Answer: A

Explanation:
To ingest and process high-volume streaming data with the least operational overhead, Amazon Kinesis Data Firehose is a suitable solution. Amazon Kinesis Data Firehose can capture, transform, and deliver streaming data to Amazon S3 or other destinations. Amazon Kinesis Data Firehose can scale automatically to match the throughput of the data and handle any amount of data. Amazon Kinesis Data Firehose is also a fully managed service that does not require any servers to provision or manage. References:
? What Is Amazon Kinesis Data Firehose?
? Amazon Kinesis Data Firehose Pricing

NEW QUESTION 106
- (Topic 4)
A company needs to store data from its healthcare application. The application's data frequently changes. A new regulation requires audit z access at all levels of the stored data.
The company hosts the application on an on-premises infrastructure that is running out of storage capacity. A solutions architect must securely migrate the existing data to AWS while satisfying the new regulation.
Which solution will meet these requirements?

A. Use AWS DataSync to move the existing data to Amazon S3. Use AWS CloudTrail to log data events.
B. Use AWS Snowcone to move the existing data to Amazon $3. Use AWS CloudTrail to log management events.
C. Use Amazon S3 Transfer Acceleration to move the existing data to Amazon S3. Use AWS CloudTrail to log data events.
D. Use AWS Storage Gateway to move the existing data to Amazon S3. Use AWS CloudTrail to log management events.

Answer: A

Explanation:
This answer is correct because it meets the requirements of securely migrating the existing data to AWS and satisfying the new regulation. AWS DataSync is a service that makes it easy to move large amounts of data online between on-premises storage and Amazon S3. DataSync automatically encrypts data in transit and verifies data integrity during transfer. AWS CloudTrail is a service that records AWS API calls for your account and delivers log files to Amazon S3. CloudTrail can log data events, which show the resource operations performed on or within a resource in your AWS account, such as S3 object-level API activity. By using CloudTrail to log data events, you can audit access at all levels of the stored data.
References:
? https://docs.aws.amazon.com/datasync/latest/userguide/what-is-datasync.html
? https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-data-events- with-cloudtrail.html

NEW QUESTION 111
- (Topic 4)
A global marketing company has applications that run in the ap-southeast-2 Region and the eu-west-1 Region. Applications that run in a VPC in eu-west-1 need to communicate securely with databases that run in a VPC in ap-southeast-2.
Which network design will meet these requirements?

A. Create a VPC peering connection between the eu-west-1 VPC and the ap-southeast-2 VP
B. Create an inbound rule in the eu-west-1 application security group that allows traffic from the database server IP addresses in the ap-southeast-2 security group.
C. Configure a VPC peering connection between the ap-southeast-2 VPC and the eu-west- 1 VP
D. Update the subnet route table
E. Create an inbound rule in the ap-southeast-2 database security group that references the security group ID of the application servers in eu-west-1.
F. Configure a VPC peering connection between the ap-southeast-2 VPC and the eu-west- 1 VP
G. Update the subnet route tables Create an inbound rule in the ap-southeast-2 database security group that allows traffic from the eu-west-1 application server IP addresses.
H. Create a transit gateway with a peering attachment between the eu-west-1 VPC and the ap-southeast-2 VP
I. After the transit gateways are properly peered and routing is configured, create an inbound rule in the database security group that references the security group ID of the application servers in eu-west-1.

Answer: C

Explanation:
"You cannot reference the security group of a peer VPC that's in a different Region. Instead, use the CIDR block of the peer VPC."
https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-security-groups.html

NEW QUESTION 115
- (Topic 4)
A company is running a microservices application on Amazon EC2 instances. The company wants to migrate the application to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster for scalability. The company must configure the Amazon EKS control plane with endpoint private access set to true and endpoint public access set to false to maintain security compliance The company must also put the data plane in private subnets. However, the company has received error notifications because the node cannot join the cluster.
Which solution will allow the node to join the cluster?

A. Grant the required permission in AWS Identity and Access Management (1AM) to the AmazonEKSNodeRole 1AM role.
B. Create interface VPC endpoints to allow nodes to access the control plane.
C. Recreate nodes in the public subnet Restrict security groups for EC2 nodes
D. Allow outbound traffic in the security group of the nodes.

Answer: B

Explanation:
Kubernetes API requests within your cluster's VPC (such as node to control plane communication) use the private VPC endpoint.
https://docs.aws.amazon.com/eks/latest/userguide/cluster-endpoint.html

NEW QUESTION 117
- (Topic 4)
A company stores critical data in Amazon DynamoDB tables in the company's AWS account. An IT administrator accidentally deleted a DynamoDB table. The deletion caused a significant loss of data and disrupted the company's operations. The company wants to prevent this type of disruption in the future.
Which solution will meet this requirement with the LEAST operational overhead?

A. Configure a trail in AWS CloudTrai
B. Create an Amazon EventBridge rule for delete action
C. Create an AWS Lambda function to automatically restore deleted DynamoDBtables.
D. Create a backup and restore plan for the DynamoDB table
E. Recover the DynamoDB tables manually.
F. Configure deletion protection on the DynamoDB tables.
G. Enable point-in-time recovery on the DynamoDB tables.

Answer: C

Explanation:
Deletion protection is a feature of DynamoDB that prevents accidental deletion of tables. When deletion protection is enabled, you cannot delete a table unless you explicitly disable it first. This adds an extra layer of security and reduces the risk of data loss and operational disruption. Deletion protection is easy to enable and disable using the AWS Management Console, the AWS CLI, or the DynamoDB API. This solution has the least operational overhead, as you do not need to create, manage, or invoke any additional resources or services. References:
? Using deletion protection to protect your table
? Preventing Accidental Table Deletion in DynamoDB
? Amazon DynamoDB now supports table deletion protection

NEW QUESTION 119
- (Topic 4)
A company has multiple Windows file servers on premises. The company wants to migrate and consolidate its files into an Amazon FSx for Windows File Server file system. File permissions must be preserved to ensure that access rights do not change.
Which solutions will meet these requirements? (Select TWO.)

A. Deploy AWS DataSync agents on premise
B. Schedule DataSync tasks to transfer the data to the FSx for Windows File Server file system.
C. Copy the shares on each file server into Amazon S3 buckets by using the AWS CLI Schedule AWS DataSync tasks to transfer the data to the FSx for Windows File Server file system.
D. Remove the drives from each file server Ship the drives to AWS for import into Amazon S3. Schedule AWS DataSync tasks to transfer the data to the FSx for Windows File Server file system
E. Order an AWS Snowcone devic
F. Connect the device to the on-premises networ
G. Launch AWS DataSync agents on the devic
H. Schedule DataSync tasks to transfer the data to the FSx for Windows File Server file system,
I. Order an AWS Snowball Edge Storage Optimized devic
J. Connect the device to the on- premises networ
K. Copy data to the device by using the AWS CL
L. Ship the device back to AWS for import into Amazon S3. Schedule AWS DataSync tasks to transfer the data to the FSx for Windows File Server file system.

Answer: AD

Explanation:
A This option involves deploying DataSync agents on your on-premises file servers and using DataSync to transfer the data directly to the FSx for Windows File Server. DataSync ensures that file permissions are preserved during the migration process. D This option involves using an AWS Snowcone device, a portable data transfer device. You would connect the Snowcone device to your on-premises network, launch DataSync agents on the device, and schedule DataSync tasks to transfer the data to FSx for Windows File Server. DataSync handles the migration process while preserving file permissions.

NEW QUESTION 124
- (Topic 4)
The customers of a finance company request appointments with financial advisors by sending text messages. A web application that runs on Amazon EC2 instances accepts the appointment requests. The text messages are published to an Amazon Simple Queue Service (Amazon SQS) queue through the web application. Another application that runs on EC2 instances then sends meeting invitations and meeting confirmation email messages to the customers. After successful scheduling, this application stores the meeting information in an Amazon DynamoDB database.
As the company expands, customers report that their meeting invitations are taking longer to arrive.
What should a solutions architect recommend to resolve this issue?

A. Add a DynamoDB Accelerator (DAX) cluster in front of the DynamoDB database.
B. Add an Amazon API Gateway API in front of the web application that accepts the appointment requests.
C. Add an Amazon CloudFront distributio
D. Set the origin as the web application that accepts the appointment requests.
E. Add an Auto Scaling group for the application that sends meeting invitation
F. Configure the Auto Scaling group to scale based on the depth of the SQS queue.

Answer: D

Explanation:
To resolve the issue of longer delivery times for meeting invitations, the solutions architect can recommend adding an Auto Scaling group for the application that sends meeting invitations and configuring the Auto Scaling group to scale based on the depth of the SQS queue. This will allow the application to scale up as the number of appointment requests increases, improving the performance and delivery times of the meeting invitations.

NEW QUESTION 128
- (Topic 4)
A company has an online gaming application that has TCP and UDP multiplayer gaming capabilities. The company uses Amazon Route 53 to point the application traffic to multiple Network Load Balancers (NLBs) in different AWS Regions. The company needs to improve application performance and decrease latency for the online game in preparation for user growth.
Which solution will meet these requirements?

A. Add an Amazon CloudFront distribution in front of the NLB
B. Increase the Cache- Control: max-age parameter.
C. Replace the NLBs with Application Load Balancers (ALBs). Configure Route 53 to use latency-based routing.
D. Add AWS Global Accelerator in front of the NLB
E. Configure a Global Accelerator endpoint to use the correct listener ports.
F. ‘Add an Amazon API Gateway endpoint behind the NLB
G. Enable API cachin
H. Override method caching for the different stages.

Answer: C

Explanation:
This answer is correct because it improves the application performance and
decreases latency for the online game by using AWS Global Accelerator. AWS Global Accelerator is a networking service that helps you improve the availability, performance, and security of your public applications. Global Accelerator provides two global static public IPs that act as a fixed entry point to your application endpoints, such as NLBs, in different AWS Regions. 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. Global Accelerator also terminates TCP and UDP traffic at the edge locations, which reduces the number of hops and improves the network performance. By adding AWS Global Accelerator in front of the NLBs, you can achieve up to 60% improvement in latency for your online game.
References:
? https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global- accelerator.html

? https://aws.amazon.com/global-accelerator/

NEW QUESTION 133
- (Topic 4)
A company runs multiple Amazon EC2 Linux instances in a VPC across two Availability Zones. The instances host applications that use a hierarchical directory structure. The applications need to read and write rapidly and concurrently to shared storage.
What should a solutions architect do to meet these requirements?

A. Create an Amazon S3 bucke
B. Allow access from all the EC2 instances in the VPC.
C. Create an Amazon Elastic File System (Amazon EFS) file syste
D. Mount the EFS file system from each EC2 instance.
E. Create a file system on a Provisioned IOPS SSD (102) Amazon Elastic Block Store (Amazon EBS) volum
F. Attach the EBS volume to all the EC2 instances.
G. Create file systems on Amazon Elastic Block Store (Amazon EBS) volumes that are attached to each EC2 instanc
H. Synchromze the EBS volumes across the different EC2 instances.

Answer: B

Explanation:
 it allows the EC2 instances to read and write rapidly and concurrently to shared storage across two Availability Zones. Amazon EFS provides a scalable, elastic, and highly available file system that can be mounted from multiple EC2 instances. Amazon EFS supports high levels of throughput and IOPS, and consistent low latencies. Amazon EFS also supports NFSv4 lock upgrading and downgrading, which enables high levels of concurrency. References:
? Amazon EFS Features
? Using Amazon EFS with Amazon EC2

NEW QUESTION 136
- (Topic 4)
A company has two VPCs that are located in the us-west-2 Region within the same AWS account. The company needs to allow network traffic between these VPCs. Approximately 500 GB of data transfer will occur between the VPCs each month.
What is the MOST cost-effective solution to connect these VPCs?

A. Implement AWS Transit Gateway to connect the VPC
B. Update the route tables of each VPC to use the transit gateway for inter-VPC communication.
C. Implement an AWS Site-to-Site VPN tunnel between the VPC
D. Update the route tables of each VPC to use the VPN tunnel for inter-VPC communication.
E. Set up a VPC peering connection between the VPC
F. Update the route tables of each VPC to use the VPC peering connection for inter-VPC communication.
G. Set up a 1 GB AWS Direct Connect connection between the VPC
H. Update the route tables of each VPC to use the Direct Connect connection for inter-VPC communication.

Answer: C

Explanation:
 To connect two VPCs in the same Region within the same AWS account, VPC peering is the most cost-effective solution. VPC peering allows direct network traffic between the VPCs without requiring a gateway, VPN connection, or AWS Transit Gateway. VPC peering also does not incur any additional charges for data transfer between the VPCs.
References:
? What Is VPC Peering?
? VPC Peering Pricing

NEW QUESTION 137
- (Topic 4)
A manufacturing company has machine sensors that upload .csv files to an Amazon S3 bucket. These .csv files must be converted into images and must be made available as soon as possible for the automatic generation of graphical reports.
The images become irrelevant after 1 month, but the .csv files must be kept to train machine learning (ML) models twice a year. The ML trainings and audits are planned weeks in advance.
Which combination of steps will meet these requirements MOST cost-effectively? (Select TWO.)

A. Launch an Amazon EC2 Spot Instance that downloads the .csv files every hour, generates the image files, and uploads the images to the S3 bucket.
B. Design an AWS Lambda function that converts the .csv files into images and stores the images in the S3 bucke
C. Invoke the Lambda function when a .csv file is uploaded.
D. Create S3 Lifecycle rules for .csv files and image files in the S3 bucke
E. Transition the.csv files from S3 Standard to S3 Glacier 1 day after they are uploade
F. Expire the image files after 30 days.
G. Create S3 Lifecycle rules for .csv files and image files in the S3 bucke
H. Transition the.csv files from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) 1 day after they are uploade
I. Expire the image files after 30 days.
J. Create S3 Lifecycle rules for .csv files and image files in the S3 bucke
K. Transition the.csv files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 1 day after they are uploade
L. Keep the image files in Reduced Redundancy Storage (RRS).

Answer: BC

Explanation:
 These answers are correct because they meet the requirements of
converting the .csv files into images, making them available as soon as possible, and minimizing the storage costs. AWS Lambda is a service that lets you run code without provisioning or managing servers. You can use AWS Lambda to design a function that converts the .csv files into images and stores the images in the S3 bucket. You can invoke the Lambda function when a .csv file is uploaded to the S3 bucket by using an S3 event notification. This way, you can ensure that the images are generated and made available as soon as possible for the graphical reports. S3 Lifecycle is a feature that enables you to manage your objects so

that they are stored cost effectively throughout their lifecycle. You can create S3 Lifecycle rules for .csv files and image files in the S3 bucket to transition them to different storage classes or expire them based on your business needs. You can transition the .csv files from S3 Standard to S3 Glacier 1 day after they are uploaded, since they are only needed twice a year for ML trainings and audits that are planned weeks in advance. S3 Glacier is a storage class for data archiving that offers secure, durable, and extremely low-cost storage with retrieval times ranging from minutes to hours. You can expire the image files after 30 days, since they become irrelevant after 1 month. References:
? https://docs.aws.amazon.com/lambda/latest/dg/welcome.html
? https://docs.aws.amazon.com/AmazonS3/latest/userguide/NotificationHowTo.html
? https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lifecycle- mgmt.html
? https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class- intro.html#sc-glacier

NEW QUESTION 142
- (Topic 4)
A company wants to rearchitect a large-scale web application to a serverless microservices architecture. The application uses Amazon EC2 instances and is written in Python.
The company selected one component of the web application to test as a microservice. The component supports hundreds of requests each second. The company wants to create and test the microservice on an AWS solution that supports Python. The solution must also scale automatically and require minimal infrastructure and minimal operational support.
Which solution will meet these requirements?

A. Use a Spot Fleet with auto scaling of EC2 instances that run the most recent Amazon Linux operating system.
B. Use an AWS Elastic Beanstalk web server environment that has high availability configured.
C. Use Amazon Elastic Kubernetes Service (Amazon EKS). Launch Auto Scaling groups of self-managed EC2 instances.
D. Use an AWS Lambda function that runs custom developed code.

Answer: D

Explanation:
AWS Lambda is a serverless compute service that lets you run code without provisioning or managing servers. You can use Lambda to create and test microservices that are written in Python or other supported languages. Lambda scales automatically to handle the number of requests per second. You only pay for the compute time you consume. Lambda also integrates with other AWS services, such as Amazon API Gateway, Amazon S3, Amazon DynamoDB, and Amazon SQS, to enable event-driven architectures. Lambda has minimal infrastructure and operational overhead, as you do not need to manage servers, operating systems, patches, or scaling policies.
The other options are not serverless solutions and require more infrastructure and operational support. They also do not scale automatically to handle the number of requests per second. A Spot Fleet is a collection of EC2 instances that run on spare capacity at low prices. However, Spot Instances can be interrupted by AWS at any time, which can affect the availability and performance of your microservice. AWS Elastic Beanstalk is a service that automates the deployment and management of web applications on EC2 instances. However, you still need to provision, configure, and monitor the underlying EC2 instances and load balancers. Amazon EKS is a service that runs Kubernetes on AWS. However, you still need to create, configure, and manage the EC2 instances that form the Kubernetes cluster and nodes. You also need to install and update the Kubernetes software and tools. References:
? What is AWS Lambda?
? Building Lambda functions with Python
? Create a layer for a Lambda Python function
? AWS Lambda – Function in Python
? How do I call my AWS Lambda function from a local python script?

NEW QUESTION 144
- (Topic 4)
A company runs a real-time data ingestion solution on AWS. The solution consists of the most recent version of Amazon Managed Streaming for Apache Kafka (Amazon MSK). The solution is deployed in a VPC in private subnets across three Availability Zones.
A solutions architect needs to redesign the data ingestion solution to be publicly available over the internet. The data in transit must also be encrypted.
Which solution will meet these requirements with the MOST operational efficiency?

A. Configure public subnets in the existing VP
B. Deploy an MSK cluster in the public subnet
C. Update the MSK cluster security settings to enable mutual TLS authentication.
D. Create a new VPC that has public subnet
E. Deploy an MSK cluster in the public subnet
F. Update the MSK cluster security settings to enable mutual TLS authentication.
G. Deploy an Application Load Balancer (ALB) that uses private subnet
H. Configure an ALB security group inbound rule to allow inbound traffic from the VPC CIDR block for HTTPS protocol.
I. Deploy a Network Load Balancer (NLB) that uses private subnet
J. Configure an NLB listener for HTTPS communication over the internet.

Answer: A

Explanation:
The solution that meets the requirements with the most operational efficiency is to configure public subnets in the existing VPC and deploy an MSK cluster in the public subnets. This solution allows the data ingestion solution to be publicly available over the internet without creating a new VPC or deploying a load balancer. The solution also ensures that the data in transit is encrypted by enabling mutual TLS authentication, which requires both the client and the server to present certificates for verification. This solution leverages the public access feature of Amazon MSK, which is available for clusters running Apache Kafka 2.6.0 or later versions1.
The other solutions are not as efficient as the first one because they either create unnecessary resources or do not encrypt the data in transit. Creating a new VPC with public subnets would incur additional costs and complexity for managing network resources and routing. Deploying an ALB or an NLB would also add more costs and latency for the data ingestion solution. Moreover, an ALB or an NLB would not encrypt the data in transit by itself, unless they are configured with HTTPS listeners and certificates, which would require additional steps and maintenance. Therefore, these solutions are not optimal for the given requirements.
References:
? Public access - Amazon Managed Streaming for Apache Kafka

NEW QUESTION 147
- (Topic 4)
A company is running its production and nonproduction environment workloads in multiple AWS accounts. The accounts are in an organization in AWS

Organizations. The company needs to design a solution that will prevent the modification of cost usage tags.
Which solution will meet these requirements?

A. Create a custom AWS Config rule to prevent tag modification except by authorized principals.
B. Create a custom trail in AWS CloudTrail to prevent tag modification
C. Create a service control policy (SCP) to prevent tag modification except by authonzed principals.
D. Create custom Amazon CloudWatch logs to prevent tag modification.

Answer: C

Explanation:
This solution meets the requirements because it uses SCPs to restrict the actions that can be performed on cost usage tags in the organization. SCPs are a type of organization policy that you can use to manage permissions in your organization. SCPs specify the maximum permissions for an organization, organizational unit (OU), or account. You can use SCPs to enforce consistent tag policies across your organization and prevent unauthorized or accidental changes to your tags. You can also create exceptions for authorized principals, such as administrators or auditors, who need to modify tags for legitimate purposes.
References:
? Service control policies (SCPs) - AWS Organizations
? Tag policies - AWS Organizations

NEW QUESTION 150
- (Topic 4)
A company needs to provide customers with secure access to its data. The company processes customer data and stores the results in an Amazon S3 bucket. All the data is subject to strong regulations and security requirements. The data must be encrypted at rest. Each customer must be able to access only their data from their AWS account. Company employees must not be able to access the data.
Which solution will meet these requirements?

A. Provision an AWS Certificate Manager (ACM) certificate for each custome
B. Encrypt the data client-sid
C. In the private certificate policy, deny access to the certificate for all principals except an 1AM role that the customer provides.
D. Provision a separate AWS Key Management Service (AWS KMS) key for each custome
E. Encrypt the data server-sid
F. In the S3 bucket policy, deny decryption of data for all principals except an 1AM role that the customer provides.
G. Provision a separate AWS Key Management Service (AWS KMS) key for each custome
H. Encrypt the data server-sid
I. In each KMS key policy, deny decryption of data for all principals except an 1AM role that the customer provides.
J. Provision an AWS Certificate Manager (ACM) certificate for each custome
K. Encrypt the data client-sid
L. In the public certificate policy, deny access to the certificate for all principals except an 1AM role that the customer provides.

Answer: C

Explanation:
The correct solution is to provision a separate AWS KMS key for each customer and encrypt the data server-side. This way, the company can use the S3 encryption feature to protect the data at rest and delegate the control of the encryption keys to the customers. The customers can then use their own IAM roles to access and decrypt their data. The company employees will not be able to access the data because they are not authorized by the KMS key policies. The other options are incorrect because:
? Option A and D are using ACM certificates to encrypt the data client-side. This is
not a recommended practice for S3 encryption because it adds complexity and overhead to the encryption process. Moreover, the company will have to manage the certificates and their policies for each customer, which is not scalable and secure.
? Option B is using a separate KMS key for each customer, but it is using the S3
bucket policy to control the decryption access. This is not a secure solution because the bucket policy applies to the entire bucket, not to individual objects. Therefore, the customers will be able to access and decrypt each other’s data if they have the permission to list the bucket contents. The bucket policy also overrides the KMS key policy, which means the company employees can access the data if they have the permission to use the KMS key.
References:
? S3 encryption
? KMS key policies
? ACM certificates

NEW QUESTION 154
......

Relate Links

Contact us