**QUESTION 7**

A company has an application that generates a large number of files, each approximately 5 MB in size. The files are stored in Amazon S3.

Company policy requires the files to be stored for 4 years before they can be deleted Immediate accessibility is always required as the files contain critical business data that is not easy to reproduce.

The files are frequently accessed in the first 30 days of the object creation but are rarely accessed after the first 30 days

Which storage solution is MOST cost-effective?

1. Create an S3 bucket lifecycle policy to move Mm from S3 Standard to S3 Glacier 30 days from object creation.

Delete the Tiles 4 years after object creation.

1. Create an S3 bucket lifecycle policy to move tiles from S3 Standard to S3 One Zone-infrequent Access (S3 One Zone-IA) 30 days from object creation.

Delete the fees 4 years after object creation.

1. Create an S3 bucket lifecycle policy to move files from S3 Standard-infrequent Access (S3 Standard-lA) 30 from object creation.

Delete the ties 4 years after object creation.

1. Create an S3 bucket Lifecycle policy to move files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 30 days from object creation.

Move the files to S3 Glacier 4 years after object carton.

**Answer:** C

**QUESTION 26**

A company has a production web application in which users upload documents through

a web interlace or a mobile app.

According to a new regulatory requirement, new documents cannot be modified or deleted after they are stored.

What should a solutions architect do to meet this requirement?

1. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning and S3 Object Lock enabled.
2. Store the uploaded documents in an Amazon S3 bucket.

Configure an S3 Lifecycle policy to archive the documents periodically.

1. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning enabled. Configure an ACL to restrict all access to read-only.

1. Store the uploaded documents on an Amazon Elastic File System (Amazon EFS) volume.

Access the data by mounting the volume in read-only mode.

**Answer:** A

**Explanation:**

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

**QUESTION 29**

A survey company has gathered data for several years from areas in the United States.

The company hosts the data in an Amazon S3 bucket that is 3 TB in size and growing.

The company has started to share the data with a European marketing firm that has S3 buckets.

The company wants to ensure that its data transfer costs remain as low as possible.

Which solution will meet these requirements?

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

**Answer:** A

**QUESTION 30**

A company uses Amazon S3 to store its confidential audit documents.

The S3 bucket uses bucket policies to restrict access to audit team IAM user credentials according to the principle of least privilege.

Company managers are worried about accidental deletion of documents in the S3 bucket and want a more secure solution.

What should a solutions architect do to secure the audit documents?

1. Enable the versioning and MFA Delete features on the S3 bucket.

1. Enable multi-factor authentication (MFA) on the IAM user credentials for each audit team IAM user account.
2. Add an S3 Lifecycle policy to the audit team's IAM user accounts to deny the s3:DeleteObject action during audit dates.
3. Use AWS Key Management Service (AWS KMS) to encrypt the S3 bucket and restrict audit team IAM user accounts from accessing the KMS key.

**Answer:** A

**QUESTION 32**

A company has applications that run on Amazon EC2 instances in a VPC.

One of the applications needs to call the Amazon S3 API to store and read objects.

According to the company's security regulations, no traffic from the applications is allowed to travel across the internet.

Which solution will meet these requirements?

1. Configure an S3 interface endpoint.
2. Configure an S3 gateway endpoint.
3. Create an S3 bucket in a private subnet.
4. Create an S3 bucket in the same Region as the EC2 instance.

**Answer:** A

**Explanation:** <https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interfaceendpoints.html#types-of-vpc-endpoints-for-s3>

**QUESTION 33**

A company is storing sensitive user information in an Amazon S3 bucket.

The company wants to provide secure access to this bucket from the application tier running on Amazon EC2 instances inside a VPC.

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

1. Configure a VPC gateway endpoint for Amazon S3 within the VPC.
2. Create a bucket policy to make the objects to the S3 bucket public.
3. Create a bucket policy that limits access to only the application tier running in the VPC.
4. Create an IAM user with an S3 access policy and copy the IAM credentials to the EC2 instance.
5. Create a NAT instance and have the EC2 instances use the NAT instance to access the S3 bucket.

**Answer:** AC

**Explanation:** <https://aws.amazon.com/premiumsupport/knowledge-center/s3-private-connection-noauthentication/>

**QUESTION 38**

A company needs to store data in Amazon S3 and must prevent the data from being changed.

The company wants new objects that are uploaded to Amazon S3 to remain unchangeable for a nonspecific amount of time until the company decides to modify the objects.

Only specific users in the company's AWS account can have the ability to delete the objects.

What should a solutions architect do to meet these requirements?

1. Create an S3 Glacier vault Apply a write-once, read-many (WORM) vault lock policy to the objects.
2. Create an S3 bucket with S3 Object Lock enabled Enable versioning. Set a retention period of 100 years.

Use governance mode as the S3 bucket's default retention mode for new objects.

1. Create an S3 bucket.

Use AWS CloudTrail to track any S3 API events that modify the objects.

Upon notification, restore the modified objects from any backup versions that the company has.

1. Create an S3 bucket with S3 Object Lock enabled.

Enable versioning.

Add a legal hold to the objects.

Add the s3:PutObjectLegalHold permission to the IAM policies of users who need to delete the objects.

**Answer:** D

**QUESTION 39**

A social media company allows users to upload images to its website.

The website runs on Amazon EC2 instances.

During upload requests, the website resizes the images to a standard size and stores the resized images in Amazon S3.

Users are experiencing slow upload requests to the website.

The company needs to reduce coupling within the application and improve website performance. A solutions architect must design the most operationally efficient process for image uploads.

Which combination of actions should the solutions architect take to meet these requirements? (Choose TWO)

1. Configure the application to upload images to S3 Glacier.

1. Configure the web server to upload the original images to Amazon S3.
2. Configure the application to upload images directly from each user's browser to Amazon S3 through the use of a presigned URL.
3. Configure S3 Event Notifications to invoke an AWS Lambda function when an image is uploaded.

Use the function to resize the image.

1. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function on a schedule to resize uploaded images.

**Answer:** BD

**QUESTION 55**

A solutions architect needs to implement a solution to reduce a company's storage costs.

All the company's data is in the Amazon S3 Standard storage class.

The company must keep all data for at least 25 years.

Data from the most recent 2 years must be highly available and immediately retrievable.

Which solution will meet these requirements?

1. Set up an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive immediately.

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

**Answer:** B

**QUESTION 65**

A company needs to retain application logs files for a critical application for 10 years.

The application team regularly accesses logs from the past month for troubleshooting, but logs older than 1 month are rarely accessed.

The application generates more than 10 TB of logs per month.

Which storage option meets these requirements MOST cost-effectively?

1. Store the Iogs in Amazon S3.

Use AWS Backup to move logs more than 1 month old to S3 Glacier Deep Archive.

1. Store the logs in Amazon S3.

Use S3 Lifecycle policies to move logs more than 1 month old to S3 Glacier Deep Archive.

1. Store the logs in Amazon CloudWatch Logs.

Use AWS Backup to move logs more then 1 month old to S3 Glacier Deep Archive.

1. Store the logs in Amazon CloudWatch Logs.

Use Amazon S3 Lifecycle policies to move logs more than 1 month old to S3 Glacier Deep Archive.

**Answer:** B

**Explanation:**

You need S3 to be able to archive the logs after one month. Cannot do that with CloudWatch Logs.

**QUESTION 65**

A company needs to retain application logs files for a critical application for 10 years.

The application team regularly accesses logs from the past month for troubleshooting, but logs older than 1 month are rarely accessed.

The application generates more than 10 TB of logs per month.

Which storage option meets these requirements MOST cost-effectively?

1. Store the Iogs in Amazon S3.

Use AWS Backup to move logs more than 1 month old to S3 Glacier Deep Archive.

1. Store the logs in Amazon S3.

Use S3 Lifecycle policies to move logs more than 1 month old to S3 Glacier Deep Archive.

1. Store the logs in Amazon CloudWatch Logs.

Use AWS Backup to move logs more then 1 month old to S3 Glacier Deep Archive.

1. Store the logs in Amazon CloudWatch Logs.

Use Amazon S3 Lifecycle policies to move logs more than 1 month old to S3 Glacier Deep Archive.

**Answer:** B

**Explanation:**

You need S3 to be able to archive the logs after one month. Cannot do that with CloudWatch Logs.

**QUESTION 71**

A company sells ringtones created from clips of popular songs.

The files containing the ringtones are stored in Amazon S3 Standard and are at least 128 KB in size.

The company has millions of files, but downloads are infrequent for ringtones older than 90 days. The company needs to save money on storage while keeping the most accessed files readily available for its users.

Which action should the company take to meet these requirements MOST cost-effectively?

1. Configure S3 Standard-Infrequent Access (S3 Standard-IA) storage for the initial storage tier of the objects.

1. Move the files to S3 Intelligent-Tiering and configure it to move objects to a less expensive storage tier after 90 days.
2. Configure S3 inventory to manage objects and move them to S3 Standard-Infrequent Access (S3 Standard-1A) after 90 days.
3. Implement an S3 Lifecycle policy that moves the objects from S3 Standard to S3 StandardInfrequent Access (S3 Standard-1A) after 90 days.

**Answer:** D

**QUESTION 72**

A company needs to save the results from a medical trial to an Amazon S3 repository.

The repository must allow a few scientists to add new files and must restrict all other users to readonly access. No users can have the ability to modify or delete any files in the repository.

The company must keep every file in the repository for a minimum of 1 year after its creation date.

Which solution will meet these requirements?

1. Use S3 Object Lock In governance mode with a legal hold of 1 year.
2. Use S3 Object Lock in compliance mode with a retention period of 365 days.
3. Use an IAM role to restrict all users from deleting or changing objects in the S3 bucket Use an S3 bucket policy to only allow the IAM role.
4. Configure the S3 bucket to invoke an AWS Lambda function every tune an object is added. Configure the function to track the hash of the saved object to that modified objects can be marked accordingly.

**Answer:** B

**QUESTION 103**

A company uses AWS Organizations to manage multiple AWS accounts for different departments.

The management account has an Amazon S3 bucket that contains project reports.

The company wants to limit access to this S3 bucket to only users of accounts within the organization in AWS Organizations.

Which solution meets these requirements with the LEAST amount of operational overhead?

1. Add the aws:PrincipalOrgID global condition key with a reference to the organization ID to the S3 bucket policy.

1. Create an organizational unit (OU) for each department.

Add the aws:PrincipalOrgPaths global condition key to the S3 bucket policy.

1. Use AWS CloudTrail to monitor the CreateAccount, InviteAccountToOrganization, LeaveOrganization, and RemoveAccountFromOrganization events. Update the S3 bucket policy accordingly.

1. Tag each user that needs access to the S3 bucket.

Add the aws:PrincipalTag global condition key to the S3 bucket policy.

**Answer:** A

**Explanation:**

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

The aws:PrincipalOrgID global key provides an alternative to listing all the account IDs for all AWS accounts in an organization.

For example, the following Amazon S3 bucket policy allows members of any account in the XXX organization to add an object into the examtopics bucket.

{"Version": "2020-09-10",

"Statement": {

"Sid": "AllowPutObject",

"Effect": "Allow",

"Principal": "\*",

"Action": "s3:PutObject",

"Resource": "arn:aws:s3:::examtopics/\*",

"Condition": {"StringEquals":

{"aws:PrincipalOrgID":["XXX"]}}}}

<https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_condition-keys.html>

**QUESTION 104**

An application runs on an Amazon EC2 instance in a VPC.

The application processes logs that are stored in an Amazon S3 bucket.

The EC2 instance needs to access the S3 bucket without connectivity to the internet.

Which solution will provide private network connectivity to Amazon S3?

1. Create a gateway VPC endpoint to the S3 bucket.

1. Stream the logs to Amazon CloudWatch Logs. Export the logs to the S3 bucket.
2. Create an instance profile on Amazon EC2 to allow S3 access.
3. Create an Amazon API Gateway API with a private link to access the S3 endpoint.

**Answer:** A

**QUESTION 122**

A company stores call transcript files on a monthly basis.

Users access the files randomly within 1 year of the call, but users access the files infrequently after 1 year.

The company wants to optimize its solution by giving users the ability to query and retrieve files that are less than 1-yearold as quickly as possible.

A delay in retrieving older files is acceptable.

Which solution will meet these requirements MOST cost-effectively?

1. Store individual files with tags in Amazon S3 Glacier Instant Retrieval.

Query the tags to retrieve the files from S3 Glacier Instant Retrieval.

1. Store individual files in Amazon S3 Intelligent-Tiering.

Use S3 Lifecycle policies to move the files to S3 Glacier Flexible Retrieval after 1 year.

Query and retrieve the files that are in Amazon S3 by using Amazon Athena.

Query and retrieve the files that are in S3 Glacier by using S3 Glacier Select.

1. Store individual files with tags in Amazon S3 Standard storage.

Store search metadata for each archive in Amazon S3 Standard storage.

Use S3 Lifecycle policies to move the files to S3 Glacier Instant Retrieval after 1 year.

Query and retrieve the files by searching for metadata from Amazon S3.

1. Store individual files in Amazon S3 Standard storage.

Use S3 Lifecycle policies to move the files to S3 Glacier Deep Archive after 1 year.

Store search metadata in Amazon RDS. Query the files from Amazon RDS.

Retrieve the files from S3 Glacier Deep Archive.

**Answer:** C

**QUESTION 122**

A company stores call transcript files on a monthly basis.

Users access the files randomly within 1 year of the call, but users access the files infrequently after 1 year.

The company wants to optimize its solution by giving users the ability to query and retrieve files that are less than 1-yearold as quickly as possible.

A delay in retrieving older files is acceptable.

Which solution will meet these requirements MOST cost-effectively?

1. Store individual files with tags in Amazon S3 Glacier Instant Retrieval.

Query the tags to retrieve the files from S3 Glacier Instant Retrieval.

1. Store individual files in Amazon S3 Intelligent-Tiering.

Use S3 Lifecycle policies to move the files to S3 Glacier Flexible Retrieval after 1 year.

Query and retrieve the files that are in Amazon S3 by using Amazon Athena. Query and retrieve the files that are in S3 Glacier by using S3 Glacier Select.

1. Store individual files with tags in Amazon S3 Standard storage.

Store search metadata for each archive in Amazon S3 Standard storage.

Use S3 Lifecycle policies to move the files to S3 Glacier Instant Retrieval after 1 year. Query and retrieve the files by searching for metadata from Amazon S3.

1. Store individual files in Amazon S3 Standard storage.

Use S3 Lifecycle policies to move the files to S3 Glacier Deep Archive after 1 year.

Store search metadata in Amazon RDS. Query the files from Amazon RDS. Retrieve the files from S3 Glacier Deep Archive.

**Answer:** C

**QUESTION 126**

A company needs to store its accounting records in Amazon S3.

The records must be immediately accessible for 1 year and then must be archived for an additional 9 years.

No one at the company, including administrative users and root users, can be able to delete the records during the entire 10-year period.

The records must be stored with maximum resiliency.

Which solution will meet these requirements?

1. Store the records in S3 Glacier for the entire 10-year period.

Use an access control policy to deny deletion of the records for a period of 10 years.

1. Store the records by using S3 Intelligent-Tiering.

Use an IAM policy to deny deletion of the records.

After 10 years, change the IAM policy to allow deletion.

1. Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 Glacier Deep Archive after 1 year.

Use S3 Object Lock in compliance mode for a period of 10 years.

1. Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 One ZoneInfrequent Access (S3 One Zone-IA) after 1 year. Use S3 Object Lock in governance mode for a period of 10 years.

**Answer:** C

**QUESTION 126**

A company needs to store its accounting records in Amazon S3.

The records must be immediately accessible for 1 year and then must be archived for an additional 9 years.

No one at the company, including administrative users and root users, can be able to delete the records during the entire 10-year period.

The records must be stored with maximum resiliency.

Which solution will meet these requirements?

1. Store the records in S3 Glacier for the entire 10-year period.

Use an access control policy to deny deletion of the records for a period of 10 years.

1. Store the records by using S3 Intelligent-Tiering.

Use an IAM policy to deny deletion of the records.

After 10 years, change the IAM policy to allow deletion.

1. Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 Glacier Deep Archive after 1 year.

Use S3 Object Lock in compliance mode for a period of 10 years.

1. Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 One ZoneInfrequent Access (S3 One Zone-IA) after 1 year.

Use S3 Object Lock in governance mode for a period of 10 years.

**Answer:** C

**QUESTION 147**

A solutions architect is using Amazon S3 to design the storage architecture of a new digital media application.

The media files must be resilient to the loss of an Availability Zone Some files are accessed frequently while other files are rarely accessed in an unpredictable pattern.

The solutions architect must minimize the costs of storing and retrieving the media files.

Which storage option meets these requirements?

1. S3 Standard.
2. S3 Intelligent-Tiering.
3. S3 Standard-Infrequent Access {S3 Standard-IA).
4. S3 One Zone-Infrequent Access (S3 One Zone-IA).

**Answer:** B

**Explanation:**

S3 Intelligent-Tiering -Perfect use case when you don't know the frequency of access or irregular patterns of usage.

Amazon S3 offers a range of storage classes designed for different use cases.

These include S3 Standard for general-purpose storage of frequently accessed data; S3 Intelligent-Tiering for data with unknown or changing access patterns; S3 Standard-Infrequent Access (S3 Standard-IA) and S3 One Zone-Infrequent Access (S3 One Zone-IA) for long-lived, but less frequently accessed data; and Amazon S3 Glacier (S3 Glacier) and Amazon S3 Glacier Deep Archive (S3 Glacier Deep Archive) for long-term archive and digital preservation. If you have data residency requirements that can't be met by an existing AWS Region, you can use the S3 Outposts storage class to store your S3 data on-premises. Amazon S3 also offers capabilities to manage your data throughout its lifecycle. Once an S3 Lifecycle policy is set, your data will automatically transfer to a different storage class without any changes to your application.

**QUESTION 143**

An application development team is designing a microservice that will convert large images to smaller, compressed images.

When a user uploads an image through the web interface, the microservice should store the image in an Amazon S3 bucket, process and compress the image with an AWS Lambda function, and store the image in its compressed form in a different S3 bucket.

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

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

1. Create an Amazon Simple Queue Service (Amazon SQS) queue.

Configure the S3 bucket to send a notification to the SQS queue when an image is uploaded to the S3 bucket.

1. Configure the Lambda function to use the Amazon Simple Queue Service (Amazon SQS) queue as the invocation source.

When the SQS message is successfully processed, delete the message in the queue.

1. Configure the Lambda function to monitor the S3 bucket for new uploads.

When an uploaded image is detected write the file name to a text file in memory and use the text file to keep track of the images that were processed.

1. Launch an Amazon EC2 instance to monitor an Amazon Simple Queue Service (Amazon SQS) queue.

When items are added to the queue log the file name in a text file on the EC2 instance and invoke the Lambda function.

1. Configure an Amazon EventBridge (Amazon CloudWatch Events) event to monitor the S3 bucket.

When an image is uploaded send an alert to an Amazon Simple Notification Service (Amazon SNS) topic with the application owner's email address for further processing

**Answer:** AB

**QUESTION 171**

A company is storing backup files by using Amazon S3 Standard storage.

The files are accessed frequently for 1 month.

However, the files are not accessed after 1 month.

The company must keep the files indefinitely.

Which storage solution will meet these requirements MOST cost-effectively?

1. Configure S3 Intelligent-Tiering to automatically migrate objects.

1. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 Glacier Deep Archive after 1 month.
2. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 StandardInfrequent Access (S3 Standard-IA) after 1 month.
3. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 One ZoneInfrequent Access (S3 One Zone-IA) after 1 month.

**Answer:** B

**QUESTION 171**

A company is storing backup files by using Amazon S3 Standard storage.

The files are accessed frequently for 1 month.

However, the files are not accessed after 1 month.

The company must keep the files indefinitely.

Which storage solution will meet these requirements MOST cost-effectively?

1. Configure S3 Intelligent-Tiering to automatically migrate objects.

1. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 Glacier Deep Archive after 1 month.
2. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 StandardInfrequent Access (S3 Standard-IA) after 1 month.
3. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 One ZoneInfrequent Access (S3 One Zone-IA) after 1 month.

**Answer:** B

**QUESTION 198**

A company wants to move its application to a serverless solution.

The serverless solution needs to analyze existing and new data by using SL.

The company stores the data in an Amazon S3 bucket.

The data requires encryption and must be replicated to a different AWS Region.

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

1. Create a new S3 bucket. Load the data into the new S3 bucket.

Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region.

Use server-side encryption with AWS KMS multi-Region kays (SSE-KMS).

Use Amazon Athena to query the data.

1. Create a new S3 bucket. Load the data into the new S3 bucket.

Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region.

Use server-side encryption with AWS KMS multi-Region keys (SSE-KMS).

Use Amazon RDS to query the data.

1. Load the data into the existing S3 bucket.

Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region.

Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3).

Use Amazon Athena to query the data.

1. Load the data into the existing S3 bucket.

Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region.

Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3).

Use Amazon RDS to query the data.

**Answer:** A

**QUESTION 209**

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

The company must protect the data from accidental deletion.

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

1. Enable versioning on the S3 bucket.

1. Enable MFA Delete on the S3 bucket.
2. Create a bucket policy on the S3 bucket.
3. Enable default encryption on the S3 bucket.
4. Create a lifecycle policy for the objects in the S3 bucket.

**Answer:** AB

**QUESTION 213**

Organizers for a global event want to put daily reports online as static HTML pages.

The pages are expected to generate millions of views from users around the world.

The files are stored In an Amazon S3 bucket.

A solutions architect has been asked to design an efficient and effective solution.

Which action should the solutions architect take to accomplish this?

1. Generate presigned URLs for the files.

1. Use cross-Region replication to all Regions.
2. Use the geoproximtty feature of Amazon Route 53.
3. Use Amazon CloudFront with the S3 bucket as its origin.

**Answer:** D

**QUESTION 214**

A company runs an application using Amazon ECS.

The application creates resized versions of an original image and then makes Amazon S3 API calls to store the resized images in Amazon S3.

How can a solutions architect ensure that the application has permission to access Amazon S3?

1. Update the S3 role in AWS IAM to allow read/write access from Amazon ECS, and then relaunch the container.

1. Create an IAM role with S3 permissions, and then specify that role as the taskRoleAm in the task definition.
2. Create a security group that allows access from Amazon ECS to Amazon S3, and update the launch configuration used by the ECS cluster.
3. Create an IAM user with S3 permissions, and then relaunch the Amazon EC2 instances for the ECS cluster while logged in as this account.

**Answer:** B

**QUESTION 235**

A company is planning to move its data to an Amazon S3 bucket.

The data must be encrypted when it is stored in the S3 bucket.

Additionally, the encryption key must be automatically rotated every year.

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

1. Move the data to the S3 bucket.

Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use the built-in key rotation behavior of SSE-S3 encryption keys.

1. Create an AWS Key Management Service (AWS KMS) customer managed key.

Enable automatic key rotation.

Set the S3 bucket's default encryption behavior to use the customer managed KMS key.

Move the data to the S3 bucket.

1. Create an AWS Key Management Service (AWS KMS) customer managed key.

Set the S3 bucket's default encryption behavior to use the customer managed KMS key.

Move the data to the S3 bucket.

Manually rotate the KMS key every year.

1. Encrypt the data with customer key material before moving the data to the S3 bucket.

Create an AWS Key Management Service (AWS KMS) key without key material.

Import the customer key material into the KMS key.

Enable automatic key rotation.

**Answer:** B