All

QUESTION 1 INCORRECT

You have created an S3 bucket in us-east-1 region by not changing default "configure options" and "permissions". Which of the following options are incorrect in terms of default settings?(choose 2 options)

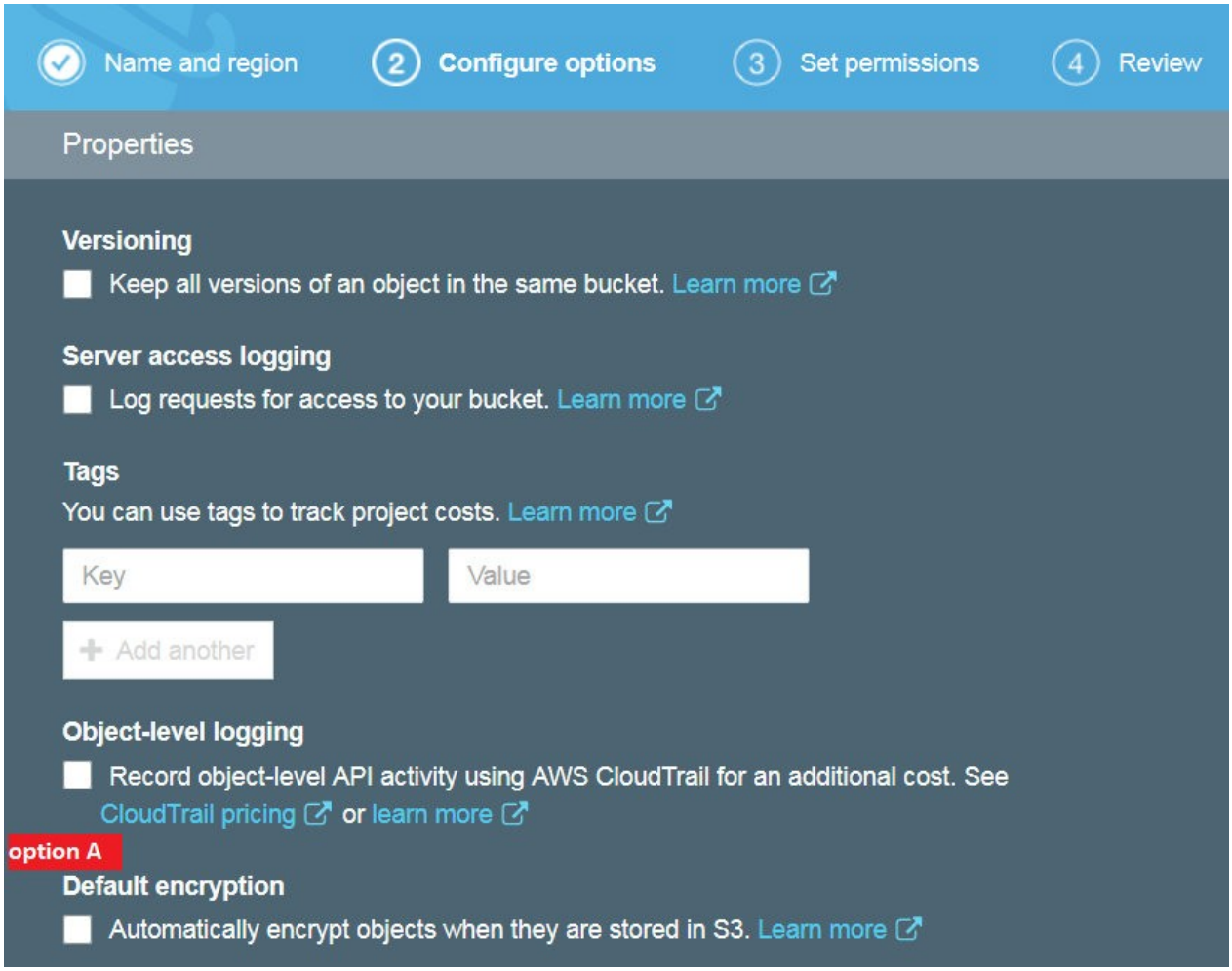
- [ ] A. Encryption is disabled.
- [x] B. Transfer Acceleration is enabled. ✔
- [x] C. No bucket policy exists. ✖
- [ ] D. Versioning is enabled. ✔

Explanation :

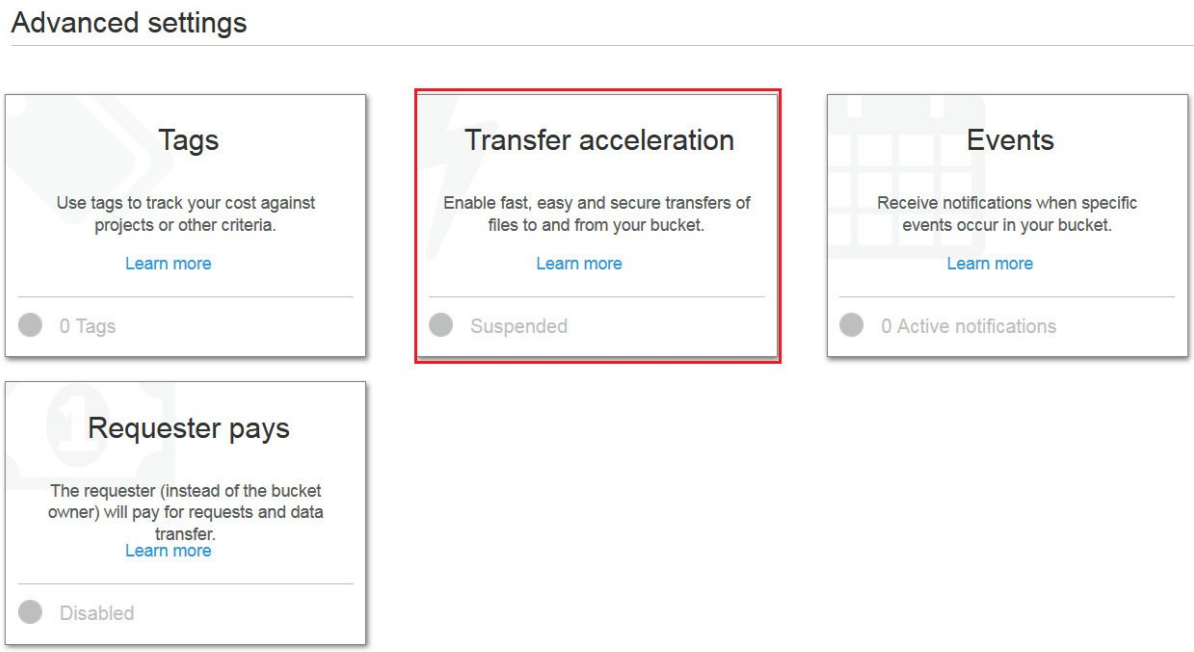
Answer: B, D

When creating an S3 bucket, you can change the default configuration according to your requirements or leave the default options and continue to create the bucket. You can always change the configuration after you created the bucket.

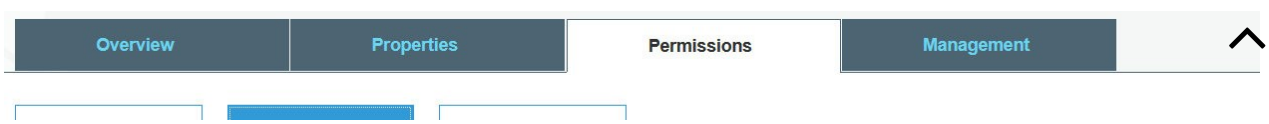
For option A, Default encryption is not enabled.

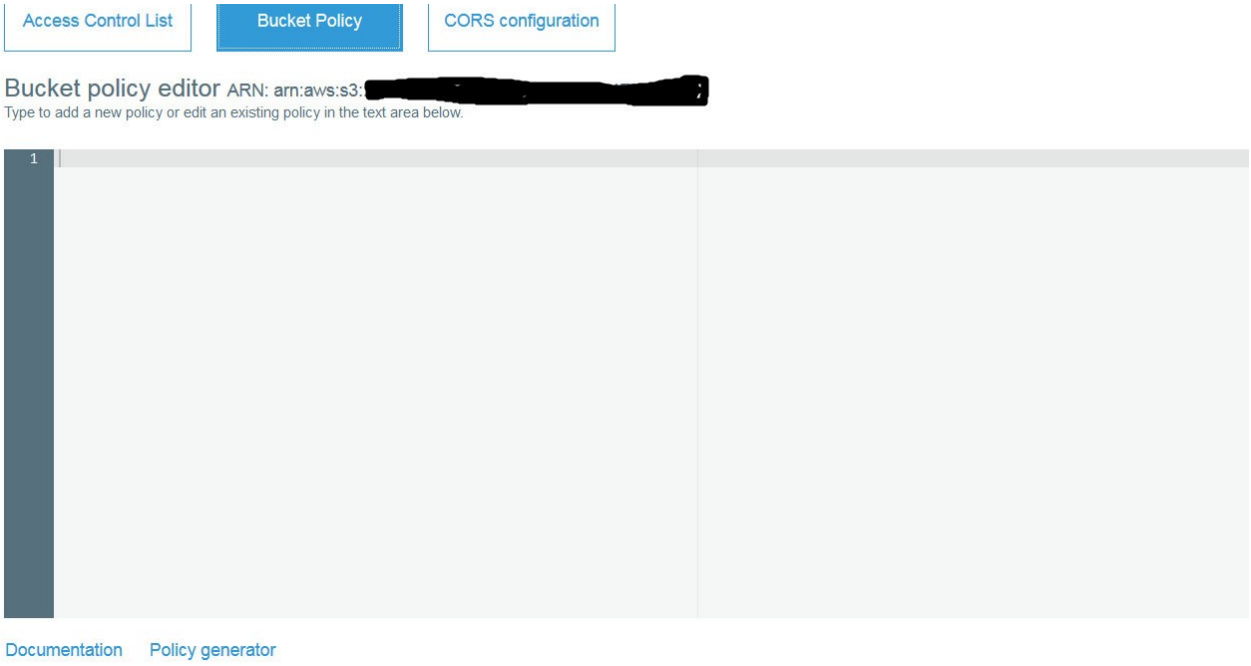


For option B, Transfer Acceleration is suspended by default.

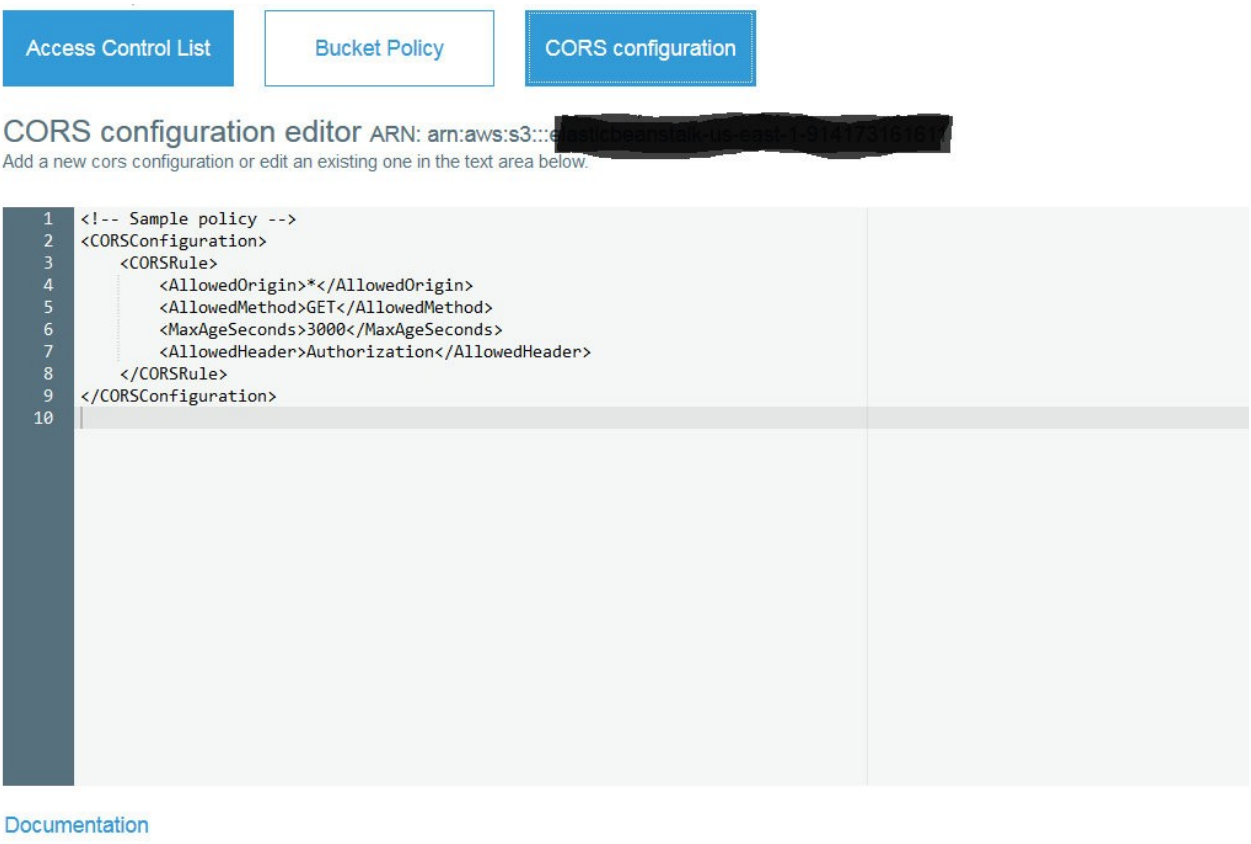


For Option C, bucket policy does not exist by default. We can restrict bucket access through bucket policy.





For option D, By default Versioning is Disabled.



Ask our Experts

QUESTION 2 INCORRECT

Which of the following are S3 bucket properties?(Choose 2 options)

- [ ] A. Server access logging ✔
- [x] B. Object level logging ✔
- [x] C. Storage class ✖
- [ ] D. Metadata

Explanation :

Answer: A, B

Following are S3 bucket properties.

a. **Versioning** – Versioning enables you to keep multiple versions of an object in one bucket. By default, versioning is disabled for a new bucket. For information about enabling versioning, see How Do I Enable or Suspend Versioning for an S3 Bucket?.

b. **Server access logging** – Server access logging provides detailed records for the requests that are made to your bucket. By default, Amazon S3 does not collect server access logs. For information about enabling server access logging, see How Do I Enable Server Access Logging for an S3 Bucket?.

c. **Static website hosting** – You can host a static website on Amazon S3. To enable static website hosting, choose **Static website hosting** and then specify the settings you want to use. For more information, see How Do I Configure an S3 Bucket for Static Website Hosting?.

d. **Object-level logging** – Object-level logging records object-level API activity by using CloudTrail data events. For information about enabling object-level logging, see How Do I Enable Object-Level Logging for an S3 Bucket with AWS CloudTrail Data Events?.

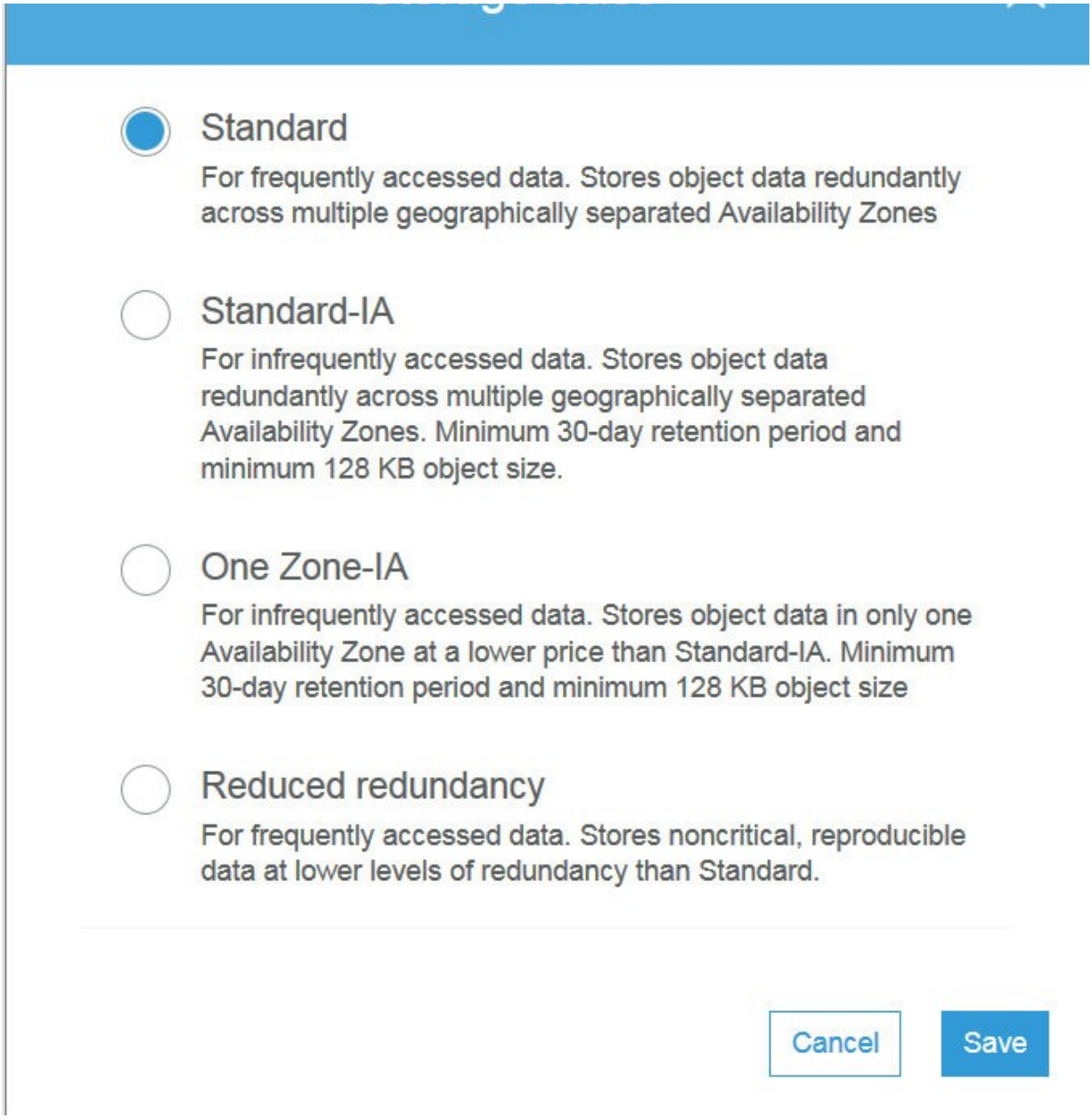
e. **Tags** – With AWS cost allocation, you can use bucket tags to annotate billing for your use of a bucket. A tag is a key-value pair that represents a label that you assign to a bucket. To add tags, choose **Tags**, and then choose **Add tag**. For more information, see Using Cost Allocation Tags for S3 Buckets in the *Amazon Simple Storage Service Developer Guide*.

f. **Transfer acceleration** – Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. For information about enabling transfer acceleration, see How Do I Enable Transfer Acceleration for an S3 Bucket?.

g. **Events** – You can enable certain Amazon S3 bucket events to send a notification message to a destination whenever the events occur. To enable events, choose **Events** and then specify the settings you want to use. For more information, see How Do I Enable and Configure Event Notifications for an S3 Bucket?.

- https://docs.aws.amazon.com/AmazonS3/latest/user-guide/view-bucket-properties.html (https://docs.aws.amazon.com/AmazonS3/latest/user-guide/view-bucket-properties.html)

Option C, Storage class property is at object level, not at bucket level. Following are different storage classes.



For more information on storage classes, refer documentation here.

- https://docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html)

For option D, metadata is at object level property, not bucket level.For detailed information on object metadata, refer documentation here.
https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMetadata.html#object-metadata (https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMetadata.html#object-metadata)

Ask our Experts

QUESTION 3 INCORRECT

You have created an S3 bucket in us-east-1 region with default configuration. You are

located in Asia and deleted an object in the bucket using AWS CLI. However, when you tried to list the objects in the bucket, you still see the object you deleted. You are even able to download the object. What could have caused this behaviour?

- A. Cross region deletes are not supported by AWS ✖
- B. AWS provides eventual consistency for DELETES. ✔
- C. AWS keeps copy of deleted object for 7 days in STANDARD storage.
- D. AWS provides strong consistency for DELETES.

Explanation :

Answer: B

Amazon S3 offers eventual consistency for overwrite PUTS and DELETES in all regions.

- A process deletes an existing object and immediately lists keys within its bucket. Until the deletion is fully propagated, Amazon S3 might list the deleted object.

https://docs.aws.amazon.com/AmazonS3/latest/dev/Introduction.html#CoreConcepts (https://docs.aws.amazon.com/AmazonS3/latest/dev/Introduction.html#CoreConcepts) and refer to "Amazon S3 Data Consistency Model"

For option A, you can perform DELETE operation from Console, CLI, programmatically from any region as long as you have access to perform.

For option C, AWS S3 deletes any object for which DELETE request is made from an authorized IAM entity.

It does not keep a copy unless you have versioning enabled and you have multiple versions of the deleted object.

The `DELETE` operation removes the null version (if there is one) of an object and inserts a delete marker, which becomes the current version of the object. If there isn't a null version, Amazon S3 does not remove any objects.

https://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectDELETE.html (https://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectDELETE.html)

In this case, bucket is created with default configuration which has versioning disabled. For option D, AWS does not provide strong consistency for DELETES.

Ask our Experts

QUESTION 4 INCORRECT

Your organization is planning to upload large number of files to AWS cloud. These files need to be immediately available for download across different geographical

files need to be immediately available for download across different geographical regions right after the upload is complete. They consulted you to check if S3 is a suitable solution for the use case. What do you suggest?

- A. S3 is not suitable for immediate downloads because new AWS provides eventual consistency for new objects.
- B. S3 is suitable for immediate downloads because AWS provides read-after-write consistency for new objects. ✔
- C. EFS is suitable for immediate downloads because AWS provides eventual consistency for new objects.
- D. S3 is suitable for immediate downloads because AWS provides strong consistency for new objects. ✖

Explanation :

Answer: B

Amazon S3 provides read-after-write consistency for PUTS of new objects in your S3 bucket in all regions with one caveat. The caveat is that if you make a HEAD or GET request to the key name (to find if the object exists) before creating the object, Amazon S3 provides eventual consistency for read-after-write.

- **Read-after-write Consistency:** Amazon S3 now supports read-after-write consistency for new objects added to Amazon S3 in US Standard region. Prior to this announcement, all regions except US Standard supported read-after-write consistency for new objects uploaded to Amazon S3. With this enhancement, Amazon S3 now supports read-after-write consistency in all regions for new objects added to Amazon S3. Read-after-write consistency allows you to retrieve objects immediately after creation in Amazon S3.

Option A is not true. Eventual consistency is for overwrite PUTS and DELETES. Option C is not true. EFS provides read-after-write consistency.

Data Consistency in Amazon EFS

Amazon EFS provides the open-after-close consistency semantics that applications expect from NFS.

In Amazon EFS, write operations will be durably stored across Availability Zones when:

- An application performs a synchronous write operation (for example, using the `open` Linux command with the `O_DIRECT` flag, or the `fsync` Linux command).
- An application closes a file.

Amazon EFS provides stronger consistency guarantees than open-after-close semantics depending on the access pattern. Applications that perform synchronous data access and perform non-appending writes will have read-after-write consistency for data access.

For option D, AWS provides strong consistency for DynamoDB, not for S3.

DynamoDB supports *eventually consistent* and *strongly consistent* reads.

Eventually Consistent Reads

When you read data from a DynamoDB table, the response might not reflect the results of a recently completed write operation. The response might include some stale data. If you repeat your read request after a short time, the response should return the latest data.

Strongly Consistent Reads

When you request a strongly consistent read, DynamoDB returns a response with the most up-to-date data, reflecting the updates from all prior write operations that were successful. A strongly consistent read might not be available if there is a network delay or outage.

Note

DynamoDB uses eventually consistent reads, unless you specify otherwise. Read operations (such as `GetItem`, `Query`, and `Scan`) provide a `ConsistentRead` parameter. If you set this parameter to true, DynamoDB uses strongly consistent reads during the operation.

Ask our Experts

QUESTION 5 INCORRECT

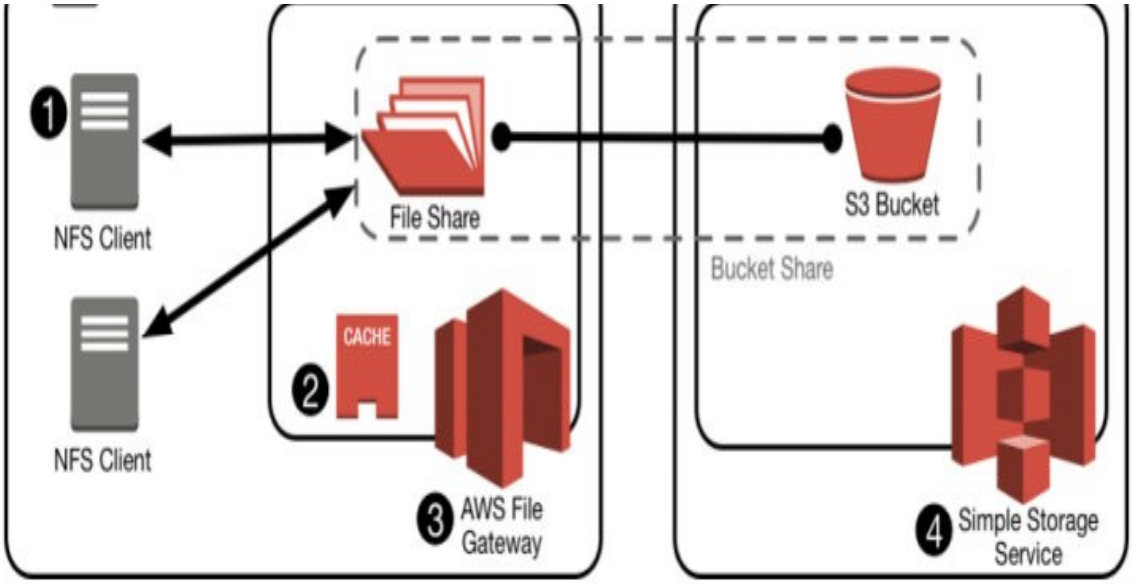
You are a solutions architect. Your organization is building an application on premise. But would like to keep the storage on AWS. Objects/files must only be accessed via the application as there are relational and access related logics built in the application. But, as an exception, Administrators should be able to access the objects/files directly from AWS S3 console/API bypassing the application. What solution would you provide?

- A. Cached Volume Gateway
- B. Stored Volume Gateway
- C. File Gateway ✔
- D. Custom built S3 solution ✖

Explanation :

Answer: C

The File Gateway presents a file interface that enables you to store files as objects in Amazon S3 using the industry-standard NFS and SMB file protocols, and access those files via NFS and SMB from your datacenter or Amazon EC2, or access those files as objects with the S3 API.



- https://d1.awsstatic.com/whitepapers/aws-storage-gateway-file-gateway-for-hybrid-architectures.pdf (https://d1.awsstatic.com/whitepapers/aws-storage-gateway-file-gateway-for-hybrid-architectures.pdf)

For option A, with Cached Volumen Gateway, you store your data in Amazon Simple Storage Service (Amazon S3) and retain a copy of frequently accessed data subsets locally. However, these are stored as snapshots in S3 and cannot be accessed through console/API.

For option B, with stored volumes, you store the entire set of volume data on-premises and store periodic point-in-time backups (snapshots) in AWS. In this model, your on-premises storage is primary, delivering low-latency access to your entire dataset. AWS storage is the backup that you can restore in the event of a disaster in your data center.
For option D, although custom built solution using S3 might work, it is recommended to use AWS provided services where ever possible.

- For more information in AWS storage gateways, refer documentation here. https://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html (https://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html)

Ask our Experts

QUESTION 6 CORRECT

You have created an S3 bucket in us-east-1 region with default configurations. You have uploaded few documents and would like to share it with a group of people in

have uploaded few documents and would like to share it with a group of people in your organization within the specified time duration. What is the recommended approach?

- A. Create one IAM user per person, attach managed policy for each user with GetObject action on your S3 bucket. Users can login to AWS console and download documents.
- B. Create one IAM user per person, add them to an IAM grop, attach managed policy for the group with GetObject action on your S3 bucket. Users can login to AWS console and download documents.
- C. Generate pre-signed URL with an expiry date and share the URL with all persons via email. ✔
- D. By default, S3 bucket has public access enabled. Share the document URLs with all persons via email.

Explanation :

Answer: C

All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre-signed URL, using their own security credentials, to grant time-limited permission to download the objects.

Anyone who receives the pre-signed URL can then access the object. For example, if you have a video in your bucket and both the bucket and the object are private, you can share the video with others by generating a pre-signed URL.

For more information, refer documentation here.

- https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html)

For options A and B, although these solutions work, it's a whole lot of setup for enabling download of documents. Also, AWS recommends using temporary credentials for use cases where users ocasionally need access to AWS resources.
In this case, pre-signed URL is granting temporary access on the S3 objects and access gets expired when the time limit has reached.
Option D is incorrect. All objects in S3 bucket are private by default.

Ask our Experts

QUESTION 7 INCORRECT

Which of the following are valid statements about Amazon S3? (Choose 3 options)

- [x] A. S3 provides read-after-write consistency for any type of PUTS. ✖
- [ ] B. S3 provides strong consistency for PUTs or DELETES.
- [x] C. A successful response to a PUT request for new object only occurs when the object is completely saved. ✔
- [x] D. S3 might return prior data when a process replaces an existing object and immediately attempts to read. ✔

- [x] **E.** S3 provides eventual consistency for overwrite PUTS and DELETES ✔

Explanation :

Answer: C, D, E

Amazon S3 provides read-after-write consistency for PUTS of new objects in your S3 bucket in all regions with one caveat. The caveat is that if you make a HEAD or GET request to the key name (to find if the object exists) before creating the object, Amazon S3 provides eventual consistency for read-after-write.

- **Read-after-write Consistency:** Amazon S3 now supports read-after-write consistency for new objects added to Amazon S3 in US Standard region. Prior to this announcement, all regions except US Standard supported read-after-write consistency for new objects uploaded to Amazon S3. With this enhancement, Amazon S3 now supports read-after-write consistency in all regions for new objects added to Amazon S3. Read-after-write consistency allows you to retrieve objects immediately after creation in Amazon S3.

Amazon S3 offers eventual consistency for overwrite PUTS and DELETES in all regions. For more information on S3 consistency model, refer documentation here.

https://docs.aws.amazon.com/AmazonS3/latest/dev/Introduction.html #CoreConcepts (https://docs.aws.amazon.com/AmazonS3/latest/dev/Introduction.html#CoreConcepts)

and refer to "Amazon S3 Data Consistency Model"

Option A is incorrect. Read-after-write consistency is only provided for new object PUTS, not for any type of PUTS.

Option B is incorrect. AWS does not provide strong consistency for S3 objects. Strong consistency model is for DynamoDB reads.

Option C translates to read-after-write consistency model. Hence correct.

Option D translates to eventual consistency model. Hence correct. Option E is correct from above statements.

Ask our Experts

QUESTION 8 INCORRECT

You are designing a web application that stores static assets in an Amazon S3 bucket. You expect this bucket to immediately receive over 400 requests with a mix of GET/PUT/DELETE per second. What should you do to ensure optimal performance?

- [ ] **A.** Amazon S3 will automatically manage performance at this scale. ✖
- [ ] **B.** Add a random prefix to the key names. ✔
- [ ] **C.** Use a predictable naming scheme, such as sequential numbers or date time sequences, in the key names.
- [ ] **D.** Use multi-part upload.

Explanation :

Correct Answer: B

Latest Update: Based on the New S3 announcement (S3 performance)Amazon S3 now provides increased request rate performance. But AWS not yet updated the exam Questions. So as per exam Option B is the correct answer.

- https://aws.amazon.com/about-aws/whats-new/2018/07/amazon-s3-announces-increased-request-rate-performance/ (https://aws.amazon.com/about-aws/whats-new/2018/07/amazon-s3-announces-increased-request-rate-performance/)

Amazon S3 maintains an index of object key names in each AWS Region. Object keys are stored in UTF-8 binary ordering across multiple partitions in the index. The key name determines which partition the key is stored in. Although Amazon S3 automatically scales to high request rates, using a sequential prefix, such as timestamp or an alphabetical sequence, increases the likelihood that Amazon S3 will target a specific partition for a large number of your keys, potentially overwhelming the I/O capacity of
the partition. When your workload is a mix of request types, introduce some randomness to key names by adding a hash string as a prefix to the key name. By introducing randomness to your key names the I/O load will be distributed across multiple index partitions. For example, you can compute an MD5 hash of the character sequence that you plan to assign as the key and add 3 or 4 characters from the hash as a prefix to the key name. The following example shows key names with a 4 character hexadecimal hash added as a prefix.

Without the 4 character hash prefix, S3 may distribute all of this load to 1 or 2 index partitions since the name of each object begins with examplebucket/2013-26-05-15-00-0 and all objects in
the index are stored in alpha-numeric order. The 4 character hash prefix ensures that the load is
spread across multiple index partitions. When your workload is sending mostly GET requests, you can add randomness to key names. In addition, you can integrate Amazon CloudFront with Amazon S3 to distribute content to your users with low latency and a high data transfer rate.

```
examplebucket/232a-2013-26-05-15-00-00/cust1234234/photo1.jpg
examplebucket/7b54-2013-26-05-15-00-00/cust3857422/photo2.jpg
examplebucket/921c-2013-26-05-15-00-00/cust1248473/photo2.jpg
examplebucket/ba65-2013-26-05-15-00-00/cust8474937/photo2.jpg
examplebucket/8761-2013-26-05-15-00-00/cust1248473/photo3.jpg
examplebucket/2e4f-2013-26-05-15-00-01/cust1248473/photo4.jpg
examplebucket/9810-2013-26-05-15-00-01/cust1248473/photo5.jpg
examplebucket/7e34-2013-26-05-15-00-01/cust1248473/photo6.jpg
examplebucket/c34a-2013-26-05-15-00-01/cust1248473/photo7.jpg
...
```

Explanation based on the New announcement:

AWS Doc says that

Amazon S3 now provides increased performance to support at least 3,500 requests per second to add data and 5,500 requests per second to retrieve data, which can save significant processing time for no additional charge. Each S3 prefix can support these request rates, making it simple to increase performance significantly.

For More Information:

- https://aws.amazon.com/about-aws/whats-new/2018/07/amazon-s3-announces-increased-request-rate-performance/ (https://aws.amazon.com/about-aws/whats-new/2018/07/amazon-s3-announces-increased-request-rate-performance/)

Ask our Experts

QUESTION 9 CORRECT

You have an applicaton running on EC2. When the application trying to upload a 7 GB file to S3, operation fails. What could be the reason for failure and what would be the solution?

- A. With a single PUT operation, you can upload objects up to 5 GB in size. Use multi-part upload for larger file uploads. ✔
- B. EC2 is designed to work best with EBS volumes. Use EBS Provisioned IOPs and use an Amazon EBS-optimized instance.
- C. NAT gateway only supports data transfers going out upto 5 GB. Use EBS Provisioned IOPs and use an Amazon EBS-optimized instance.
- D. VPC Endpoints only supports data transfers going out upto 5 GB. Use EBS Provisioned IOPs and use an Amazon EBS-optimized instance.

Explanation :

Answer: A

AWS recommends using multi-part uploads for larger objects.

Uploading Objects

Depending on the size of the data you are uploading, Amazon S3 offers the following options:

- **Upload objects in a single operation—**With a single PUT operation, you can upload objects up to 5 GB in size. For more information, see Uploading Objects in a Single Operation.
- **Upload objects in parts—**Using the multipart upload API, you can upload large objects, up to 5 TB. The multipart upload API is designed to improve the upload experience for larger objects. You can upload objects in parts. These object parts can be uploaded independently, in any order, and in parallel. You can use a multipart upload for objects from 5 MB to 5 TB in size. For more information, see Uploading Objects Using Multipart Upload API.

We recommend that you use multipart uploading in the following ways:

- If you're uploading large objects over a stable high-bandwidth network, use multipart uploading to maximize the use of your available bandwidth by uploading object parts in parallel for multi-threaded performance.
- If you're uploading over a spotty network, use multipart uploading to increase resiliency to network errors by avoiding upload restarts. When using multipart uploading, you need to retry uploading only parts that are interrupted during the upload. You don't need to restart uploading your object from the beginning.

For more information on multi-part uploads, refer documentation here.
https://docs.aws.amazon.com/AmazonS3/latest/dev/mpuoverview.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/mpuoverview.html)

For option B, Amazon EBS is a storage for the drives of your virtual machines. It stores data as blocks of the same size and organizes them through the hierarchy similar to a traditional file system. EBS is not a standalone storage service like Amazon S3 so you can use it only in combination with Amazon EC2.
Objects can be stored on EBS volumes, but not cost-effective and not highly resilient and fault tolarant compared to S3.
Optionc C and D are incorrect. NAT Gateway ad VPC endpoints do not have any data transfer limitations.

Ask our Experts

QUESTION 10 CORRECT

You have an application on EC2 which stores the files in an S3 bucket. EC2 is being launched using a role which has GetObject permissions on the S3 bucket defined in its policy. The users who authenticate to this application will get a pre-signed URL for the files in S3 bucket using EC2 role temporary credentials. However, users reporting they get an error when accessing pre- signed URLs. What could be the reason? (Choose 2 options)

- [x] A. Pre-signed URLs expired. ✔
- [ ] B. Logged in user must be an IAM user to download file through pre-signed URL.
- [x] C. Bucket might have a policy with Deny. EC2 role not whitelisted in the policy statement with Deny. ✔
- [ ] D. Default policy on temporary credentials does not have GetObject privileges on S3 bucket.

Explanation :

Answer: A, C

All objects in S3 are private by default. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre- signed URL, using their own security credentials, to grant time-limited permission to download the objects.

Anyone who receives the pre-signed URL can then access the object. For example, if you have a video in your bucket and both the bucket and the object are private, you can share the video with others by generating a pre-signed URL.

For more information, refer documentation here.
https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html)

For option A, while generating pre-signed URL programatically using SDK/API, we give a duration how long should the URL be valid. When the URL is accessed after the specified duration, you would get an error.

For option B, AWS recommends to use temporary credentials when ever users need time- limited access to AWS resources instead of using IAM users for each request.

For more information on temporary credentials, refer documentation here.
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html)

For option C, if a bucket policy contains Effect as Deny, you must whitelist all the IAM resources which need access on the bucket. Otherwise, IAM resources cannot access S3 bucket even if they have full access.

For detailed information on how to restrict bucket, refer documentation here.
https://aws.amazon.com/blogs/security/how-to-restrict-amazon-s3-bucket-access-to-a-specific- (https://aws.amazon.com/blogs/security/how-to-restrict-amazon-s3-bucket-access-to-a-specific-iam-role/)iam-role/ (https://aws.amazon.com/blogs/security/how-to-restrict-amazon-s3-bucket-access-to-a-specific-)

For option D, policy is an optional parameter when temporary credentials are generated using AssumeRole (which is how EC2 generates temporary credentials using instance-profile). There is no default policy.

Policy

An IAM policy in JSON format.

This parameter is optional. If you pass a policy to this operation, the resulting temporary credentials have the permissions of the assumed role *and* the policy that you pass. This gives you a way to further restrict the permissions for the resulting temporary security credentials. You cannot use the passed policy to grant permissions that are in excess of those allowed by the permissions policy of the role that is being assumed. For more information, see Permissions for AssumeRole, AssumeRoleWithSAML, and AssumeRoleWithWebIdentity in the *IAM User Guide*.

The format for this parameter, as described by its regex pattern, is a string of characters up to 2048 characters in length. The characters can be any ASCII character from the space character to the end of the valid character list (\u0020-\u00FF). It can also include the tab (\u0009), linefeed (\u000A), and carriage return (\u000D) characters.

Note

The policy plaintext must be 2048 bytes or shorter. However, an internal conversion compresses it into a packed binary format with a separate limit. The `PackedPolicySize` response element indicates by percentage how close to the upper size limit the policy is, where 100 percent is the maximum allowed size.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: No

Ask our Experts

QUESTION 11 INCORRECT

Your organization has an S3 bucket which stores confidential information. Access is granted to certain programmatic IAM users and restricted the requests from these IAM

users to be originated from within your organization IP address range. However, your organization suspect there might be requests from other IP addresses to S3 buckets to download certain objects. How would you troubleshoot to find out requester IP address? (choose 2 options)

- [x] A. Enable VPC flow logs in the region where S3 bucket exists. ✖
- [x] B. Enable Server logging ✔
- [ ] C. Enable CloudTrail logging using OPTIONS object ✔
- [ ] D. Enable CloudWatch metrics

Explanation :

Answer: B, C

Server access logging provides detailed records for the requests that are made to a bucket. Server access logs are useful for many applications. For example, access log information can be useful in security and access audits.

For details on how to enable logging for S3, refer documentation here.

https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html#server-access-logging-overview (https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html#server-access-logging-overview)

For information about the format of the log file, refer documentation here.

https://docs.aws.amazon.com/AmazonS3/latest/dev/LogFormat.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/LogFormat.html)

For option A, S3 is a managed service and not part of VPC. So enabling VPC flow logs does not report traffic sent to S3 bucket.

Option B is correct.

Option C is correct. Using the information collected by CloudTrail, you can determine what request was made to Amazon S3, the source IP address from which the request was made, who made the request, when it was made, and so on. This information helps you to track changes made to your AWS resources and to troubleshoot operational issues.

Amazon S3 Object-Level Actions Tracked by CloudTrail Logging

You can also get CloudTrail logs for object-level Amazon S3 actions. To do this, specify the Amazon S3 object for your trail. When an object-level action occurs in your account, CloudTrail evaluates your trail settings. If the event matches the object that you specified in a trail, the event is logged. For more information, see Data Events in the *AWS CloudTrail User Guide*. The following table lists the object-level actions that CloudTrail can log:

For detailed information about how S3 requests are tracked using CloudTrail, refer documentation here.

https://docs.aws.amazon.com/AmazonS3/latest/dev/cloudtrail-logging.html#cloudtrail-logging- s3-info (https://docs.aws.amazon.com/AmazonS3/latest/dev/cloudtrail-logging.html#cloudtrail-logging-%20s3-info)
For option D, although CloudWatch has metrics for S3 requests, this does not provide detailed information about each request. It generates metrics for number of request sent for each type.
For more information about S3 CloudWatch request metrics, refer documentation here.

https://docs.aws.amazon.com/AmazonS3/latest/dev/cloudwatch-monitoring.html#s3-request-cloudwatch-metrics (https://docs.aws.amazon.com/AmazonS3/latest/dev/cloudwatch-monitoring.html#s3-request-cloudwatch-metrics)

Ask our Experts

QUESTION 12 INCORRECT

Your organization is planning to build a web and mobile applications which can upload few

100,000 images everyday into S3. This application expects sudden increase in volume, however they are lean on budget and looking for a cost-effective solution. As an architect, you were approached if S3 suits their requirement. What information you must gather from your organization to make a decision?(choose 2 options)

- [x] A. Gather information on high availability of data and frequency of requests to choose storage class of objects in S3. ✔
- [x] B. Gather information on total size to properly design prefix namespace. ✖
- [ ] C. Gather information on total size to provision storage on S3 bucket.
- [ ] D. Gather information on number of requests during peak time. ✔

Explanation :

Answer: A, D

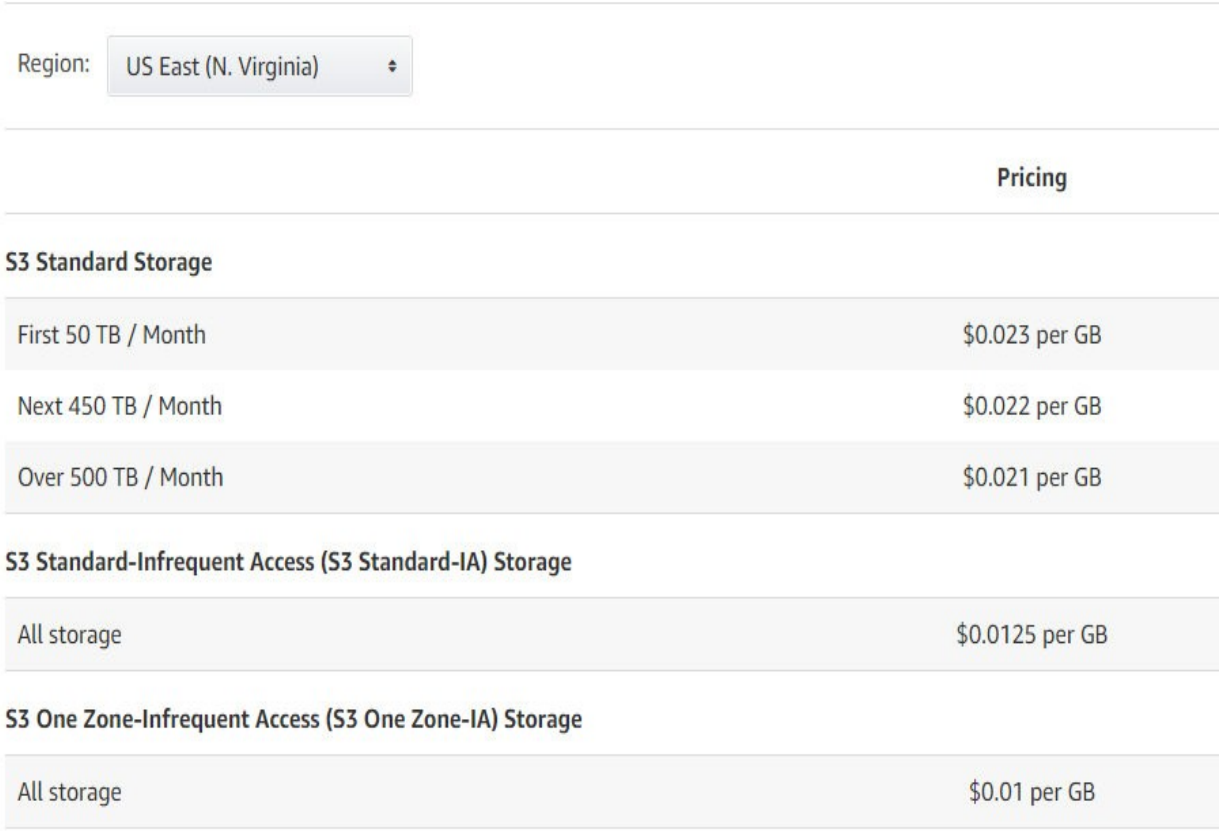
For option A, S3 offers different storage classes. Based on the storage type, availability % would change along with cost.

If the images need to be highly available and frequently accessed, choose STANDARD. If the images need not be highly available but frequently accessed, choose REDUCED_REDUNDANCY class.

If the images need to be highly available but not frequently accessed, choose STANDARD_IA class.

If the images need not be highly available and not frequently accessed, choose ONEZONE_IA Following are the prices for each storage class.

Storage Pricing (varies by region)



For more information on S3 storage classes, refer documentation here.

- https://docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html)

For option B, prefix naming is required for optimal performance if we expect higher number of objects, not large sized objects. Option D is correct. Following is the explanation.
Amazon S3 maintains an index of object key names in each AWS Region. Object keys are stored in UTF-8 binary ordering across multiple partitions in the index. The key name determines which partition the key is stored in. Although Amazon S3 automatically scales to high request rates, using a sequential prefix, such as timestamp or an alphabetical sequence, increases the likelihood that Amazon S3 will target a specific partition for a large number of your keys, potentially overwhelming the I/O capacity of the partition.
When your workload is a mix of request types, introduce some randomness to key names by adding a hash string as a prefix to the key name. By introducing randomness to your key names the I/O load will be distributed across multiple index partitions. For example, you can compute an MD5 hash of the character sequence that you plan to assign as the key and add 3 or 4 characters from the hash as a prefix to the key name. The following example shows key names with a 4 character hexadecimal hash added as a prefix.

```
examplebucket/232a-2013-26-05-15-00-00/cust1234234/photo1.jpg
examplebucket/7b54-2013-26-05-15-00-00/cust3857422/photo2.jpg
```

```
examplebucket/921c-2013-26-05-15-00-00/cust1248473/photo2.jpg
examplebucket/ba65-2013-26-05-15-00-00/cust8474937/photo2.jpg
examplebucket/8761-2013-26-05-15-00-00/cust1248473/photo3.jpg
examplebucket/2e4f-2013-26-05-15-00-01/cust1248473/photo4.jpg
examplebucket/9810-2013-26-05-15-00-01/cust1248473/photo5.jpg
examplebucket/7e34-2013-26-05-15-00-01/cust1248473/photo6.jpg
examplebucket/c34a-2013-26-05-15-00-01/cust1248473/photo7.jpg
...
```

Without the 4 character hash prefix, S3 may distribute all of this load to 1 or 2 index partitions since the name of each object begins with examplebucket/2013-26-05-15-00-0 and all objects in the index are stored in alpha-numeric order. The 4 character hash prefix ensures that the load is spread across multiple index partitions.

When your workload is sending mostly GET requests, you can add randomness to key names. In addition, you can integrate Amazon CloudFront with Amazon S3 to distribute content to your users with low latency and a high data transfer rate.
For option C, AWS S3 storage is virtually unlimited. No need to provision any storage upfront.

Ask our Experts

QUESTION 13 INCORRECT

Which of the following are system metadata for objects in S3?(choose 3 options)

- [x] A. x-amz-server-side-encryption ✔
- [x] B. x-amz-meta-object-id ✖
- [x] C. x-amz-version-id ✔
- [ ] D. Content-Length ✔
- [ ] E. x-amz-meta-location

Explanation :

Answer: A, C, D

AWS S3 bucket objects contain two kinds of metadata, system metadata and user-defined metadata.

System metadata:

Metadata such as object creation date is system controlled where only Amazon S3 can modify the value.

Other system metadata, such as the storage class configured for the object and whether the object has server-side encryption enabled, are examples of system metadata whose values you control. If your bucket is configured as a website, sometimes you might want to redirect a page request to another page or an external URL. In this case, a

webpage is

an object in your bucket. Amazon S3 stores the page redirect value as system metadata whose value you control.
When you create objects, you can configure values of these system metadata items or update the values when you need to
User-defined metadata:
When uploading an object, you can also assign metadata to the object. You provide this optional information as a name-value (key-value) pair when you send a PUT or POST request to create the object. When you upload objects using the REST API, the optional user-defined metadata names must begin with **"x-amz-meta-"** to distinguish them from other HTTP headers
For more information on object metadata, refer documentation here.
https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMetadata.html#object-metadata
(https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMetadata.html#object-metadata)
So, options B and E starts with x-amz-meta and are user-defined metadata.

Ask our Experts

QUESTION 14 CORRECT

Your organization needs to meet audit compliance and hence need to log all the requests sent to a set of 10 buckets which contains confidential information. These also will be periodically used to find out if any requests are being made from outside the organization's IP address range. Your AWS application team had enabled S3 server access logging for all the buckets into a common logging bucket named s3-server-logging. But after few hours they noticed no logs were being written into logging bucket. What could be the reason?

- A. Bucket user-defined deny policy is not allowing Log Delivery group to write into S3 logging bucket. ✔
- B. Bucket public access is not enabled.
- C. Write access is disabled for Log Delivery group.
- D. Bucket name for server access logging should be "s3-server-access-logging" inorder to write the request logs.

Explanation :

Answer: A
Server access logging provides detailed records for the requests that are made to a bucket. Server access logs are useful for many applications. For example, access log information can be useful in security and access audits.

For details on logging for S3, refer documentation here.
https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html#server-access-logging-overview
(https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html#server-access-logging-overview)

For option A, S3 buckets would often be restricted using bucket policy with Effect as Deny except whitelisted IAM resources who would require access.
For detailed information on how to restrict bucket, refer documentation here.
https://aws.amazon.com/blogs/security/how-to-restrict-amazon-s3-bucket-access-to-a-specific-iam-role/ (https://aws.amazon.com/blogs/security/how-to-restrict-amazon-s3-bucket-access-to-a-specific-iam-role/)
For providing access to log delivery group, you need to explicitly add following statement to your bucket policy.

```
{

"Version": "2012-10-17",

"Statement": [

{


Delivery service",

"Sid": "Permit access log delivery by AWS ID for Log


"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::858827067514:root"

},

"Action": "s3:PutObject",

"Resource": "arn:aws:s3:::examplebucket/logs/*"

}

]

}
```

Also make sure the arn “arn:aws:iam::858827067514:root” is whitelisted in the Deny statement of your bucket policy.

For option B, public access is not required to be enabled for writing logs into S3 bucket. Only access required is PutObject for Log Delivery group.
For option C, although by default, Log Delivery group permission is disabled, permission will be granted when the bucket is selected as target for logging.

When you enable logging on a bucket, the console both enables logging on the source bucket and adds a grant in the

target bucket's access control list (ACL) granting write permission to the Log Delivery group.

https://docs.aws.amazon.com/AmazonS3/latest/dev/enable-logging-console.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/enable-logging-console.html)
Option D is a false statement.

Ask our Experts

QUESTION 15 CORRECT

You are building a web application which will allow authenticated users to upload videos to AWS S3 bucket. However, while testing the application, you found that the upload requests to S3 are being blocked. What should you do to make the upload work?

- A. Enable public access to allow uploads from web applications.
- B. Add configuration in S3 bucket CORS to allow PUT requests from web application URL. ✔
- C. Add Content-Length and Content-MD5 headers while sending upload requests to S3
- D. Web application URL must be added to bucket policy to allow PutObject requests.

Explanation :

Answer: B

Cross-origin resource sharing (CORS) defines a way for client web applications that are loaded in one domain to interact with resources in a different domain. With CORS support, you can build rich client-side web applications with Amazon S3 and selectively allow cross-origin access to

your Amazon S3 resources.

For more information on CORS, refer documentation here.
https://docs.aws.amazon.com/AmazonS3/latest/dev/cors.html#example-scenarios-cors (https://docs.aws.amazon.com/AmazonS3/latest/dev/cors.html#example-scenarios-cors)

For option A, enabling public access will not enable web application to send requests to S3 bucket. Further more, AWS does not recommend enabling public access on an S3 bucket unless you are hosting static assets which can be accessed by all.

For more information on securing S3 buckets, refer documentation here.
. https://aws.amazon.com/premiumsupport/knowledge-center/secure-s3-resources/ (http://.https:/aws.amazon.com/premiumsupport/knowledge-center/secure-s3-resources/)

For option C, Content-Length and Content-MD5 are system metadata for object. They are set during creating/uploading an object. However, these paramaters do not enable web application to send requests to S3 bucket.

For option D, AWS S3 bucket policy does not grant permissions based on the web application

URLs.

However, you can setup a condition in the policy to restrict access only if the request is being sent from a certain URL using "aws:Referer" context-key.

https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html#example- bucket-policies-use-case-4 (https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html#example-bucket-policies-use-case-4)

Ask our Experts

QUESTION 16 CORRECT

You have uploaded a file to AWS S3 bucket with content 'foo'. You have overwritten the file with content 'bar'. When you made a GetObject request immediately after overwrite, what output can you expect?

- A. foo
- B. bar
- C. either foo or bar or no results ✔
- D. An error stating "Object updating. Please try after some time."

Explanation :

Answer: C

Amazon S3 offers eventual consistency for overwrite PUTS and DELETES in all regions.

A process replaces an existing object and immediately attempts to read it. Until the change is fully propagated, Amazon S3 might return the prior data.

Ask our Experts

QUESTION 17 CORRECT

You created a bucket named "myfirstwhizbucket" in US West region. What are valid URLs for accessing the bucket?(choose 3 options)

- [x] A. https://myfirstwhizbucket.s3-us-west-1.amazonaws.com ✔
- [ ] B. https://s3.myfirstwhizbucket.us-west-1.amazonaws.com
- [x] C. https://s3-us-west-1.amazonaws.com/myfirstwhizbucket ✔
- [x] D. https://s3.us-west-1.amazonaws.com/myfirstwhizbucket ✔

E. https://s3.amazonaws.com/myfirstwhizbucket

Explanation :

Answer: A, C, D

Accessing a Bucket

You can access your bucket using the Amazon S3 console. Using the console UI, you can perform almost all bucket operations without having to write any code.

If you access a bucket programmatically, note that Amazon S3 supports RESTful architecture in which your buckets and objects are resources, each with a resource URI that uniquely identifies the resource.

Amazon S3 supports both virtual-hosted–style and path-style URLs to access a bucket.

- In a virtual-hosted–style URL, the bucket name is part of the domain name in the URL. For example:
  - `http://bucket.s3.amazonaws.com`
  - `http://bucket.s3-aws-region.amazonaws.com.`

  In a virtual-hosted–style URL, you can use either of these endpoints. If you make a request to the `http://bucket.s3.amazonaws.com` endpoint, the DNS has sufficient information to route your request directly to the Region where your bucket resides.
  For more information, see Virtual Hosting of Buckets.

- In a path-style URL, the bucket name is not part of the domain (unless you use a Region-specific endpoint). For example:
  - US East (N. Virginia) Region endpoint, `http://s3.amazonaws.com/bucket`
  - Region-specific endpoint, `http://s3-aws-region.amazonaws.com/bucket`

  In a path-style URL, the endpoint you use must match the Region in which the bucket resides. For example, if your bucket is in the South America (São Paulo) Region, you must use the `http://s3-sa-east-1.amazonaws.com/bucket` endpoint. If your bucket is in the US East (N. Virginia) Region, you must use the `http://s3.amazonaws.com/bucket` endpoint.

For option A, it matches the virtual-hosted-style URL and it is correct.

For option B, it does not match any of the above mentioned URL patterns. It is incorrect. For option C, it matches the path-style URL and it is correct.
For option D, it does not match any of the above mentioned URL patterns. But It's working. You can access the bucket by using this URL. So, Option D also correct answer.

For option E, it matches path-style URL, but since the bucket is in us-west-1 region, it must contain the region in the endpoint. So it is incorrect.

Ask our Experts

QUESTION 18 INCORRECT

What are the minimum and maximum file sizes that can be stored in S3 respectively?

A. 1 KB and 5 gigabytes

B. 1 KB and 5 terabytes ✖

C. 1 Byte and 5 gigabytes

D. 0 Bytes and 5 terabytes ✔

Explanation :

Answer: D

Q: How much data can I store in Amazon S3?

The total volume of data and number of objects you can store are unlimited. Individual Amazon S3 objects can range in size from a minimum of 0 bytes to a maximum of 5 terabytes. The largest object that can be uploaded in a single PUT is 5 gigabytes. For objects larger than 100 megabytes, customers should consider using the Multipart Upload capability.

Ask our Experts

QUESTION 19 INCORRECT

Your organization writes lot of application logs on regular basis to AWS s3 bucket and are the only copies available, not stored anywhere else. These files range between 10MB-500MB in size and are not accessed regularly. They are required once in a while to troubleshoot application issues. Application team need last 60 days log files to be immediately available when required. Logs older than 60 days need not be accessible immediately, but need to keep a copy for reference. What approach you will recommend to keep the billing cost to minimum?

A. Set object storage class to STANDARD-IA. Use Lifecycle Management to move data from STANDARD-IA to Glacier after 60 days. ✔

B. Set object storage class to STANDARD. Use Lifecycle Management to move data from STANDARD to STANDARD-IA after 60 days.

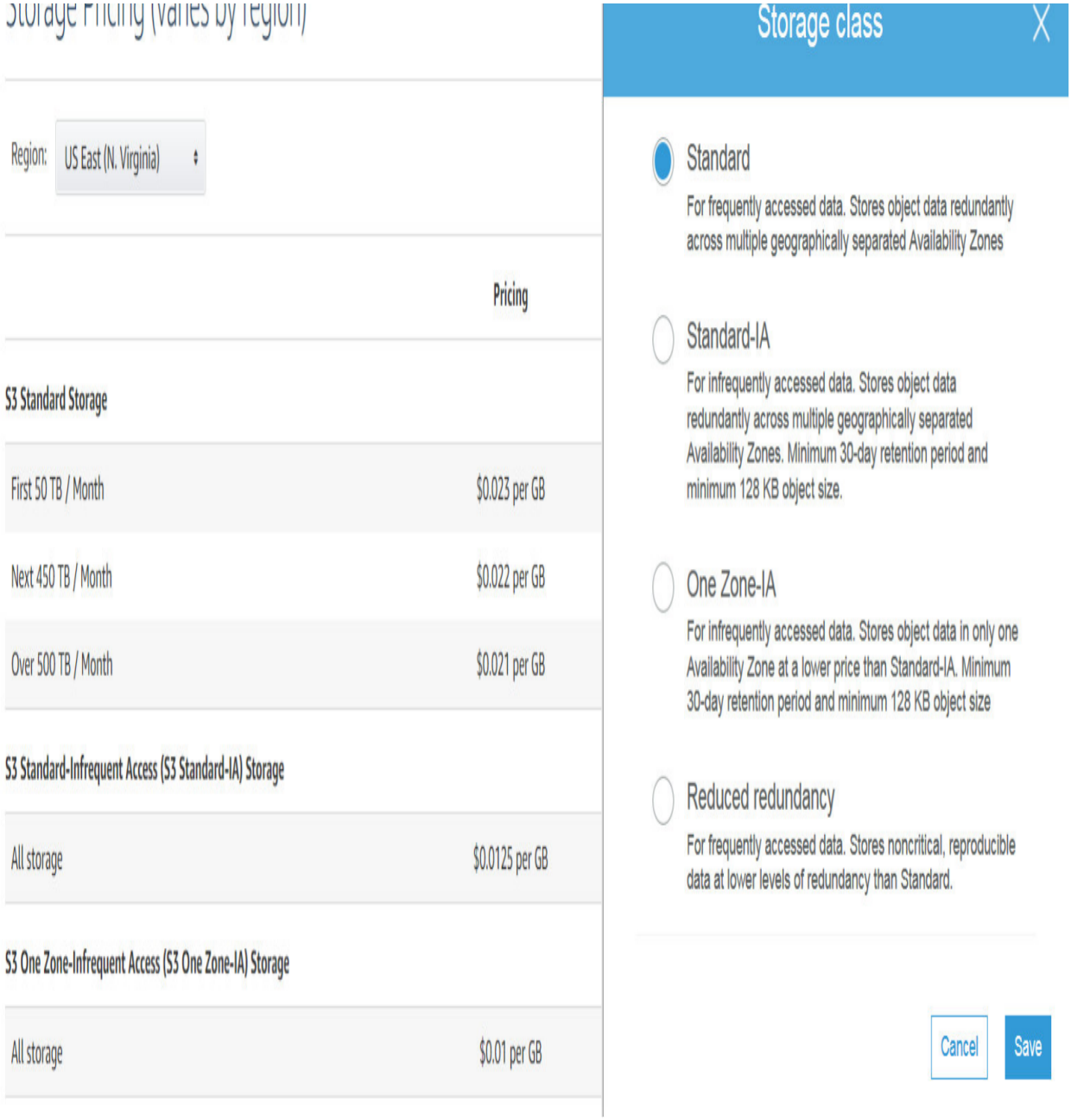
C. Set storage class to STANDARD. Use Lifecycle Management to move data from STANDARD to STANDARD-IA after 30 days and move data from STANDARD-IA to Glacier after 30 days. ✖

D. Set object storage class to OENZONE-IA. Use Lifecycle Management to move data from ONEZONE-IA to Glacier after 60 days.

Explanation :

Answer: A

Following are the storage classes for S3 objects and its pricing models.



STANDARD-IA offers cheaper storage than STANDARD class. However, AWS charges $0.01 per GB of data retrieved from the Infrequent Access storage class apart from the standard download pricing.

Options B, C, D state the initial storage to be STANDARD and ONEZONE-IA.

For the given use case, due to following factors, STANDARD-IA is more suitable than than STANDARD or ONEZONE-IA as initial storage.

Data is not accessed regularly. STANDARD is not suitable
Data is kept for atleast 60 days and minimum file size is 1 MB. Meets STANDARD-IA requisites.
Data is the primary copy, not stored anywhere else. ONEZONE-IA is not suitable.
Data needs to be available immediately when required. Available with all classes except Glacier.

After 60 days, the data can be transitioned to Glacier using Lifecycle management rules since it need not be accessible immediately.

Therefore, from above options, A is correct.
In the question, they mentioned that "Your organization writes lot of application logs on regular basis to AWS s3

bucket and are the only copies available, not stored anywhere else." means the organization is not having another copy of the data at any other location. The data is just stored in S3 only.

So if we use OneZone-IA storage class, it will not maintain a replica of your data in multiple availability zones.

AWS says"**S3 One Zone-Infrequent Access (S3 One Zone-IA; Z-IA) is a new storage class designed for customers who want a lower-cost option for infrequently accessed data, but do not require the multiple Availability Zone data resilience model** of the S3 Standard and S3 Standard-Infrequent Access (S3 Standard-IA; S-IA) storage classes."

Based on the requirement, S3-IA is the suitable Option.

Ask our Experts

QUESTION 20 CORRECT

With S3 Versioning enabled on the bucket, how billing will be applied for the following scenario.

Total days bucket in use: 25 days.

File uploaded on 1st Day of the use – 1 GB.

File uploaded within the same bucket on 15th Day of the use – 5 GB.

- A. Charges 6 GB for 25 days.
- B. Charges 1 GB for 25 days and 5 GB for 11 days. ✔
- C. Charges 1 GB for 14 days and 5 GB for 11 days.
- D. Charges 5 GB for 25 days.

Explanation :

Answer: B

When versioning is enabled on S3 bucket and a new version is added to an existing object, remember that older version still remains and AWS charges same price for old verions and new versions.

Q: How am I charged for using Versioning?

Normal Amazon S3 rates apply for every version of an object stored or requested. For example, let's look at the following scenario to illustrate storage costs when utilizing Versioning (let's assume the current month is 31 days long):

1) Day 1 of the month: You perform a PUT of 4 GB (4,294,967,296 bytes) on your bucket.
2) Day 16 of the month: You perform a PUT of 5 GB (5,368,709,120 bytes) within the same bucket using the same key as the original PUT on Day 1.

When analyzing the storage costs of the above operations, please note that the 4 GB object from Day 1 is not deleted from the bucket when the 5 GB object is written on Day 15. Instead, the 4 GB object is preserved as an older version and the 5 GB object becomes the most recently written version of the object within your bucket. At the end of the month:

Total Byte-Hour usage
[4,294,967,296 bytes x 31 days x (24 hours / day)] + [5,368,709,120 bytes x 16 days x (24 hours / day)] = 5,257,039,970,304 Byte-Hours.

Conversion to Total GB-Months
5,257,039,970,304 Byte-Hours x (1 GB / 1,073,741,824 bytes) x (1 month / 744 hours) = 6.581 GB-Month

In the given use case, 1 GB uploaded on day 1 remains in S3 for all 25 days. 5 GB uploaded on day 15 will be in S3 for only 11 days.

Ask our Experts

QUESTION 21 INCORRECT

You have a version enabled S3 bucket. You have accidentally deleted an object which contains 3 versions. You would want to restore the deleted object. What can be done?

- A. Select the deleted object and choose restore option in More menu.
- B. Delete the delete-marker on the object. ✔
- C. Versioning in S3 only supports keeping multiple copies. It does not support restoring deleted objects.
- D. In version enabled bucket, Delete request only deletes latest version. You can still older verions of the object using version Id in the GET request. ✖

Explanation :

Answer: B

When you delete an object in a versioning-enabled bucket, all versions remain in the bucket and Amazon S3 creates a delete marker for the object. To undelete the object, you must delete this delete marker.

To undelete an object, you must delete the delete marker. Select the check box next to the delete marker of the object to recover, and then choose delete from the More menu.

For more information on how to undelete objects in version enabled S3 bucket, refer documentation here.

- https://docs.aws.amazon.com/AmazonS3/latest/user-guide/undelete-objects.html (https://docs.aws.amazon.com/AmazonS3/latest/user-guide/undelete-objects.html)

Ask our Experts

QUESTION 22 INCORRECT

You have an application which writes application logs to version enabled S3 bucket. Each object has multiple versions attached to it. After 60 days, application deletes the objects in S3 through DELETE API on the object. However, in next month's bill, you see charges for S3 usage on the bucket. What could have caused this?

A. DELETE API call on the object only deletes latest version. ✖

B. DELETE API call on the object does not delete the actual object, but places delete marker on the object. ✔

C. DELETE API call moves the object and its versions to S3 recycle bin from where object can be restored till 30 days.

D. DELETE API for all versions of the object in version enabled bucket cannot be done through API. It can be only done by bucket owner through console.

Explanation :

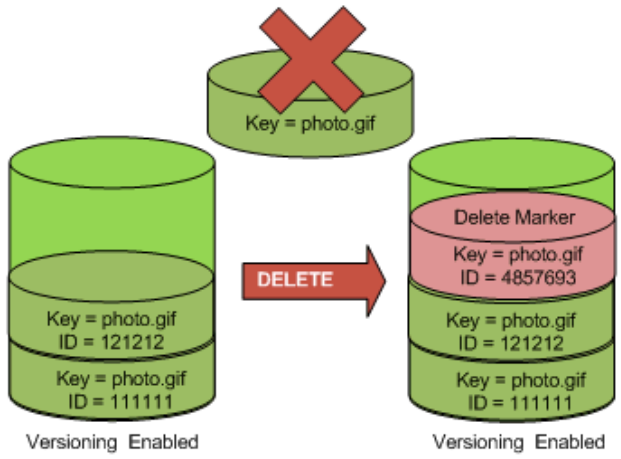
Answer: B

When versioning is enabled, a simple DELETE cannot permanently delete an object.

Instead, Amazon S3 inserts a delete marker in the bucket, and that marker becomes the current version of the object with a new ID. When you try to GET an object whose current version is a

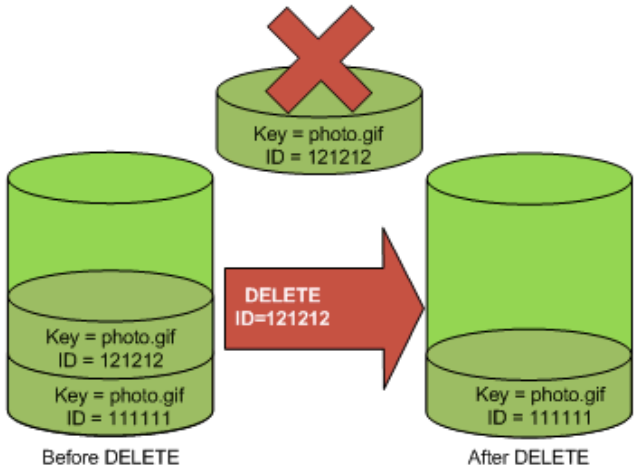
delete marker, Amazon S3 behaves as though the object has been deleted (even though it has not been erased) and returns a 404 error.

The following figure shows that a simple DELETE does not actually remove the specified object. Instead, Amazon S3 inserts a delete marker.



To permanently delete versioned objects, you must use DELETE Object versionId.

The following figure shows that deleting a specified object version permanently removes that object.



For information on how to delete versioned objects through API, refer documentation here.

- https://docs.aws.amazon.com/AmazonS3/latest/dev/DeletingObjectVersions.html#delete-obj-version-enabled-bucket-rest

(https://docs.aws.amazon.com/AmazonS3/latest/dev/DeletingObjectVersions.html#delete-obj-version-enabled-bucket-rest)

Option A is not true. DELETE call on an object does not delete latest version unless DELETE call is made with

Option A is not true. DELETE call on object does not delete latest version unless DELETE call is made with latest version id.
Option C is not true. AWS S3 does not have recycle bin.
Option D is not true. DELETE call on versioned object can be made through API by providing version id of the object's version to be deleted.

Ask our Experts

QUESTION 23 CORRECT

You are uploading multiple files ranging 10 GB – 20 GB in size to AWS S3 bucket by using multi- part upload from an application on EC2. Once the upload is complete, you would like to notify a group of people who do not have AWS IAM accounts. How can you achieve this?(choose 2 options)

- [x] **A.** Use S3 event notification and configure Lambda function which sends email using AWS SES non-sandbox. ✔
- [x] **B.** Use S3 event notification and configure SNS which sends email to subsribed email addresses. ✔
- [ ] **C.** Write a custom script on your application side to poll S3 bucket for new files and send email through SES non-sandbox.
- [ ] **D.** Write a custom script on your application side to poll S3 bucket for new files and send email through SES sandbox.

Explanation :

Answer: A, B

The Amazon S3 notification feature enables you to receive notifications when certain events happen in your bucket. To enable notifications, you must first add a notification configuration identifying the events you want Amazon S3 to publish, and the destinations where you want Amazon S3 to send the event notifications.

Currently, Amazon S3 can publish the following events:

- A new object created event—Amazon S3 supports multiple APIs to create objects. You can request notification when only a specific API is used (e.g., `s3:ObjectCreated:Put`) or you can use a wildcard (e.g., `s3:ObjectCreated:*`) to request notification when an object is created regardless of the API used.
- An object removal event—Amazon S3 supports deletes of versioned and unversioned objects. For information about object versioning, see Object Versioning and Using Versioning.
  You can request notification when an object is deleted or a versioned object is permanently deleted by using the `s3:ObjectRemoved:Delete` event type. Or you can request notification when a delete marker is created for a versioned object by using `s3:ObjectRemoved:DeleteMarkerCreated`. You can also use a wildcard `s3:ObjectRemoved:*` to request notification anytime an object is deleted. For information about deleting versioned objects, see Deleting Object Versions.
- A Reduced Redundancy Storage (RRS) object lost event—Amazon S3 sends a notification message when it detects that an object of the RRS storage class has been lost.

Amazon S3 supports the following destinations where it can publish events:

- Amazon Simple Notification Service (Amazon SNS) topic

Amazon SNS is a flexible, fully managed push messaging service. Using this service, you can push messages to mobile devices or distributed services. With SNS you can publish a message once, and deliver it one or more times. An SNS topic is an access point that recipients can dynamically subscribe to in order to receive event notifications. For more information about SNS, see the Amazon SNS product detail page.

- Amazon Simple Queue Service (Amazon SQS) queue
  Amazon SQS is a scalable and fully managed message queuing service. You can use SQS to transmit any volume of data without requiring other services to be always available. In your notification configuration you can request that Amazon S3 publish events to an SQS queue. For more information about SQS, see Amazon SQS product detail page.
- AWS Lambda
  AWS Lambda is a compute service that makes it easy for you to build applications that respond quickly to new information. AWS Lambda runs your code in response to events such as image uploads, in-app activity, website clicks, or outputs from connected devices. You can use AWS Lambda to extend other AWS services with custom logic, or create your own back-end that operates at AWS scale, performance, and security. With AWS Lambda, you can easily create discrete, event-driven applications that execute only when needed and scale automatically from a few requests per day to thousands per second.
  AWS Lambda can run custom code in response to Amazon S3 bucket events. You upload your custom code to AWS Lambda and create what is called a Lambda function. When Amazon S3 detects an event of a specific type (for example, an object created event), it can publish the event to AWS Lambda and invoke your function in Lambda. In response, AWS Lambda executes your function. For more information, see AWS Lambda product detail page.

- https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html)

AWS Simple Email Service (SES) is a cost-effective email service built on the reliable and scalable infrastructure that Amazon.com developed to serve its own customer base. With Amazon SES, you can send transactional email, marketing messages, or any other type of high-quality content.

To help prevent fraud and abuse, and to help protect your reputation as a sender, we apply certain restrictions to new Amazon SES accounts.

We place all new accounts in the Amazon SES sandbox. While your account is in the sandbox, you can use all of the features of Amazon SES. However, when your account is in the sandbox, we apply the following restrictions to your account:

You can only send mail to verified email addresses and domains, or to the Amazon SES

mailbox simulator.

You can only send mail from verified email addresses and domains.

Note

This restriction applies even when your account is not in the sandbox.

You can send a maximum of 200 messages per 24-hour period.

You can send a maximum of 1 message per second.

You can request to move out of sandbox mode when you are ready for production mode.

For more information on how to move out of sandbox mode, refer documentation here.

- https://docs.aws.amazon.com/ses/latest/DeveloperGuide/request-production-access.html (https://docs.aws.amazon.com/ses/latest/DeveloperGuide/request-production-access.html)

Option A triggers Lambda function which uses non-sandbox SES to send email to people who does not have AWS IAM account nor verified in AWS SES.
Option B triggers SNS.

Following document describes how to add SNS event notification to a bucket.

- https://docs.aws.amazon.com/AmazonS3/latest/dev/ways-to-add-notification-config-to-bucket.html

(https://docs.aws.amazon.com/AmazonS3/latest/dev/ways-to-add-notification-config-to-bucket.html)

Options C and D, although sounds feasible options, it requires compute resources to continously monitor S3 for new files.
We should use AWS provided features where ever are applicable. Custom solutions can be built when AWS provided features do not meet the requirement.

Ask our Experts

QUESTION 24 CORRECT

Your organization had built a video sharing website on EC2 within US for which S3 bucket in us- east-1 is used to store the video files. The website has been receiving very good feedback and your organization decided to expand the website all over the world. However, customers in Europe and Asia started to complain that website access, upload and download of videos files are slow. How can you resolve the issue? (choose 2 options)

- [x] **A.** Use CloudFront for improving the performance on website by caching static files. ✔
- [ ] **B.** Use VPC Endpoints in Europe and Asia regions to improve S3 uploads and downloads.
- [x] **C.** Enable Transfer Acceleration feature on S3 bucket which uses AWS edge locations to improve upload and download speeds. ✔
- [ ] **D.** Change your application design to provision higher-memory configuration EC2 instances and process S3 requests through EC2.

Explanation :

Answer: A, C

Option A is correct. AWS CloudFront can be used to improve the performance of your website where network latency is an issue.

- https://docs.aws.amazon.com/AmazonS3/latest/dev/website-hosting-cloudfront- walkthrough.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/website-hosting-cloudfront- walkthrough.html)

(https://docs.aws.amazon.com/AmazonS3/latest/dev/website-hosting-cloudfront- walkthrough.html)

Option B is not correct. VPC endpoints do not support cross-region requests. More over, VPC

endpoints are for accessing AWS resources within VPC.

Option C is correct. Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. Transfer Acceleration takes

advantage of Amazon CloudFront's globally distributed edge locations. As the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path.
For more information on transfer acceleration, refer documentation here.

https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html#transfer-acceleration-why-use (https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html#transfer-acceleration-why-use)
Option D is not a good design. It increases cost on EC2 usage and does not solve the problem with slower upload and download speeds to S3.

Ask our Experts

QUESTION 25 CORRECT

Cross region replication requires versioning to be enabled on?

- A. Only on Destination bucket.
- B. Versioning is useful to avoid accidental deletes and not a requirement for replicating across regions.
- C. Only on Source bucket.
- D. Both Source and Destination buckets. ✔

Explanation :

Answer: D
Cross-region replication is a bucket-level configuration that enables automatic, asynchronous copying of objects across buckets in different AWS Regions. We refer to these buckets as source bucket and destination bucket. These buckets can be owned by different AWS accounts.

Requirements

Requirements for cross-region replication:

- The source and destination buckets must have versioning enabled. For more information about versioning, see Using Versioning.
- The source and destination buckets must be in different AWS Regions. For a list of AWS Regions where you can create a bucket, see Regions and Endpoints in the *AWS General Reference*.
- Amazon S3 must have permissions to replicate objects from that source bucket to the destination bucket on your behalf.

  You can grant these permissions by creating an IAM role. For more information about IAM roles, see Create an IAM Role.

  Important

  To pass the IAM role that you create that grants Amazon S3 replication permissions, you must have the `iam:PassRole` permission. For more information, see Granting a User Permissions to Pass a Role to an AWS Service in the *IAM User Guide*.
- If the source bucket owner also owns the object, the bucket owner has full permissions to replicate the object. If not, the object owner must grant the bucket owner the `READ` and `READ_ACP` permissions via the object ACL. For more information about Amazon S3 actions, see Specifying Permissions in a Policy. For more information about resources and ownership, see Amazon S3 Resources.

For more information on AWS S3 cross-region replication, refer documentation here.

- https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html)

Ask our Experts

Finish Review (https://www.whizlabs.com/learn/course/aws-csaa-practice-tests/quiz/14790)

Certification

- Cloud Certification (https://www.whizlabs.com/cloud-certification-training-courses/)
- Java Certification (https://www.whizlabs.com/oracle-java-certifications/)
- PM Certification (https://www.whizlabs.com/project-management-certifications/)
- Big Data Certification (https://www.whizlabs.com/big-data-certifications/)

Company

- Support (https://help.whizlabs.com/hc/en-us)
- Discussions (http://ask.whizlabs.com/)
- Blog (https://www.whizlabs.com/blog/)

Mobile App

Coming Soon

Follow us

Android Coming Soon

iOS Coming Soon

(https://www.facebook.com/whizlabs.software/)

(https://in.linkedin.com/company/whizlabs-software)

(https://twitter.com/whizlabs?lang=en)

(https://plus.google.com/+WhizlabsSoftware)