
# Discipline

## Transfer Acceleration, Requester Pay Model & Default Encryption

**CS5002**

Activity-6

**Sheikh Muhammed Tadeeb (AU19B1014)**

## ❖ Problem Statement:

List a document for Feature like

1. Transfer Acceleration with screenshots and also the Costing/Pricing for that feature.
2. Requester pay model with screenshots and also the Costing/Pricing for that feature.
3. Default encryption and Select Amazon S3 key (SSE-S3) and Costing/Pricing for it.

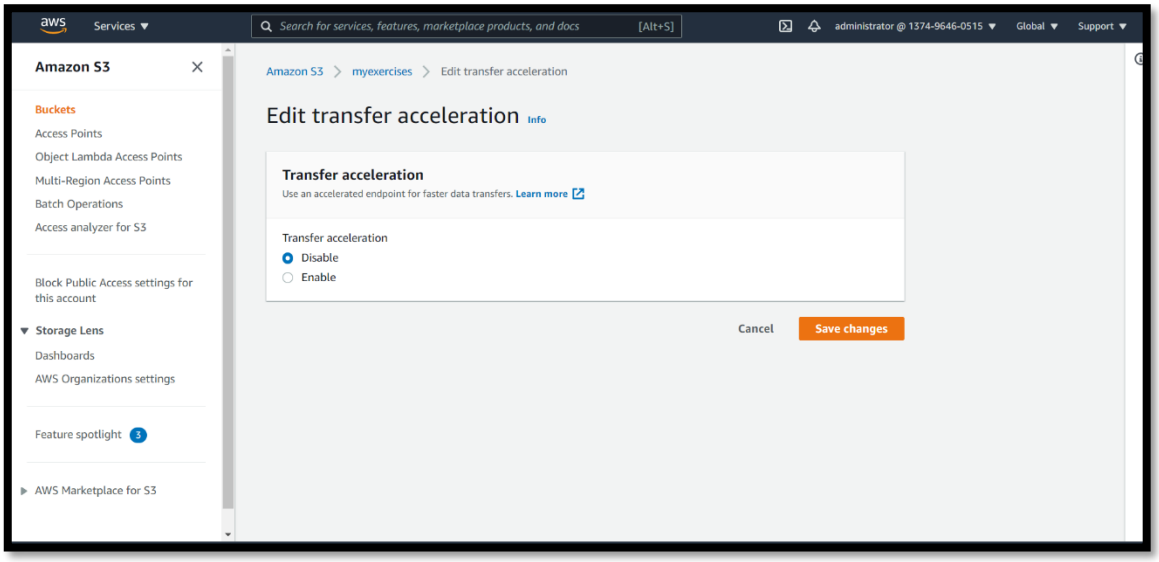
## ❖ Solution1)

- **Brief:**

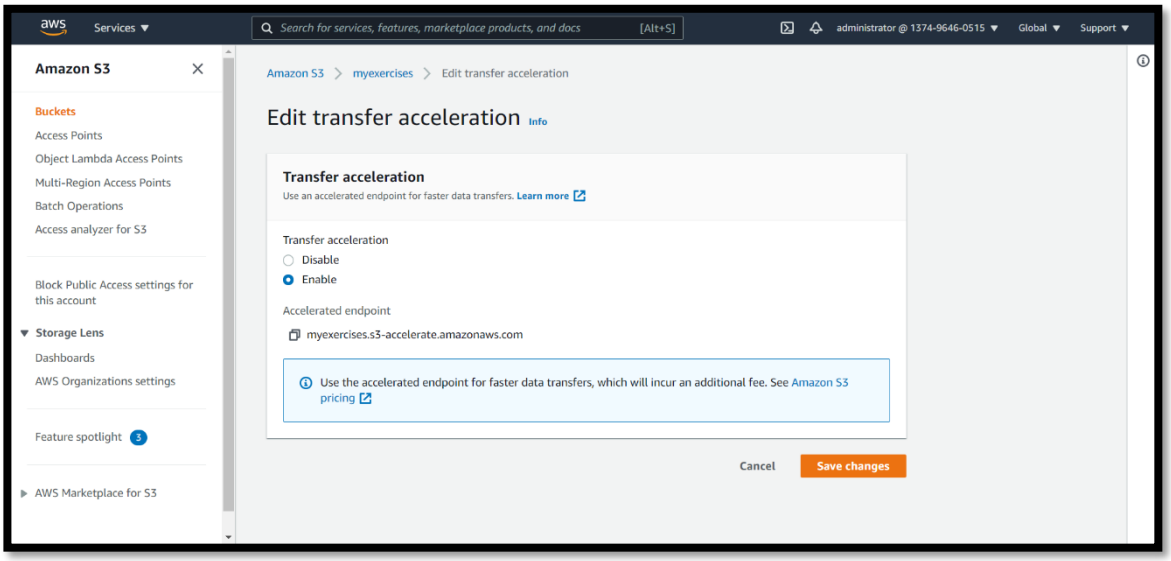
  Amazon S3 Transfer Acceleration is a bucket-level feature that enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. Transfer Acceleration takes advantage of the globally distributed edge locations in Amazon CloudFront. As the data arrives at an edge location, the data is routed to Amazon S3 over an optimized network path.

  Note: When we use Transfer Acceleration, additional data transfer charges might apply.

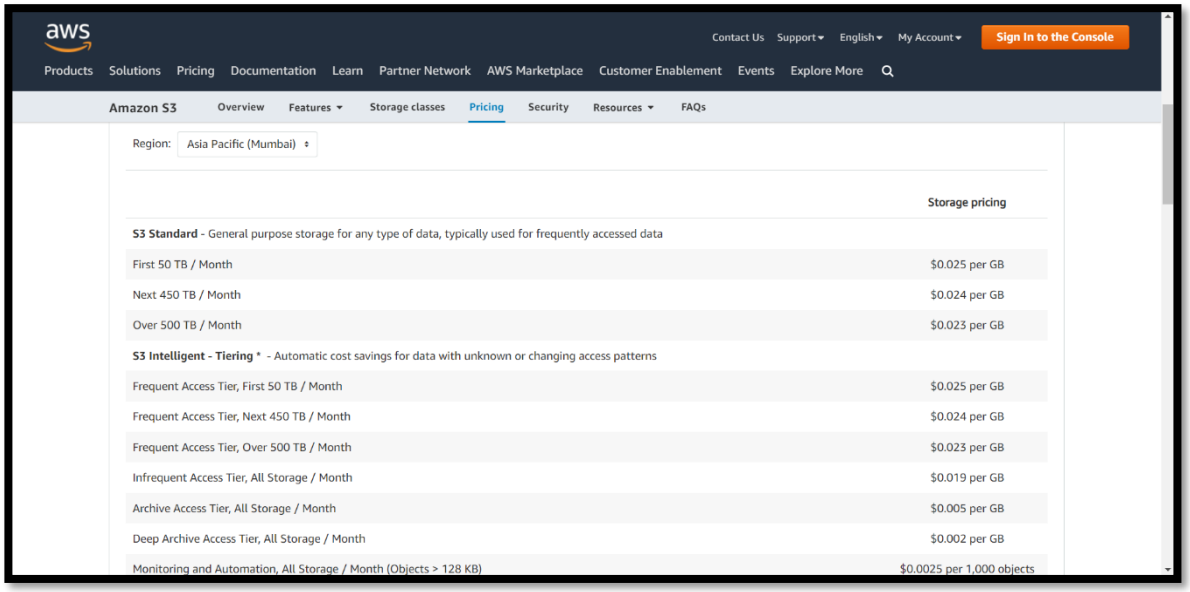
- **Before State:**

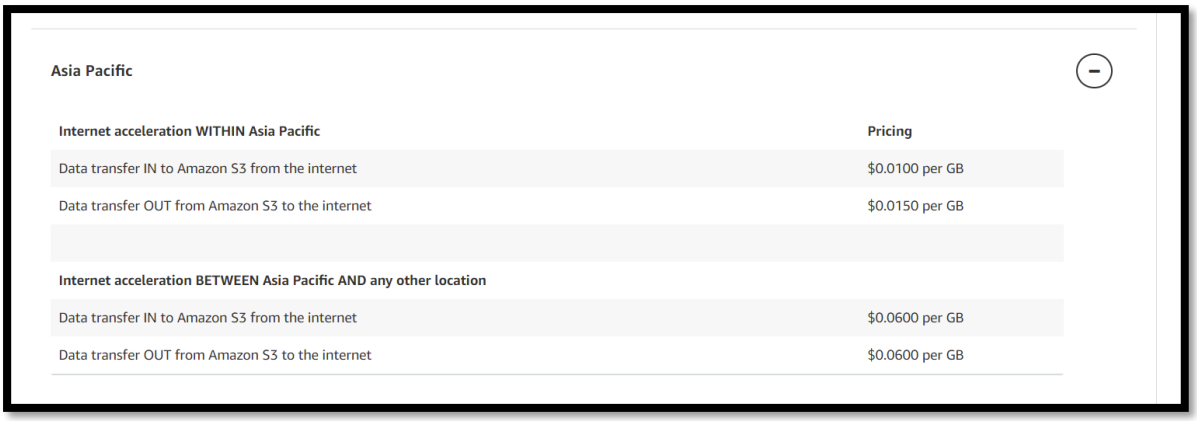


- **After State:**




- **Costing:**



Asia Pacific

| Internet acceleration WITHIN Asia Pacific | Pricing |
|---|---|
| Data transfer IN to Amazon S3 from the internet | $0.0100 per GB |
| Data transfer OUT from Amazon S3 to the internet | $0.0150 per GB |
| | |
| **Internet acceleration BETWEEN Asia Pacific AND any other location** | |
| Data transfer IN to Amazon S3 from the internet | $0.0600 per GB |
| Data transfer OUT from Amazon S3 to the internet | $0.0600 per GB |

Note: [Amazon S3 Simple Storage Service Pricing - Amazon Web Services]

## ❖ Solution2)

- **Brief:**

  In general, bucket owners pay for all Amazon S3 storage and data transfer costs that are associated with their bucket. However, you can configure a bucket to be a Requester Pays bucket. With Requester Pays buckets, the requester instead of the bucket owner pays the cost of the request and the data download from the bucket. The bucket owner always pays the cost of storing data.

  Typically, you configure buckets to be Requester Pays buckets when you want to share data but not incur charges associated with others accessing the data. For example, you might use Requester Pays buckets when making available large datasets, such as zip code directories, reference data, geospatial information, or web crawling data.

  You must authenticate all requests involving Requester Pays buckets. The request authentication enables Amazon S3 to identify and charge the requester for their use of the Requester Pays bucket.

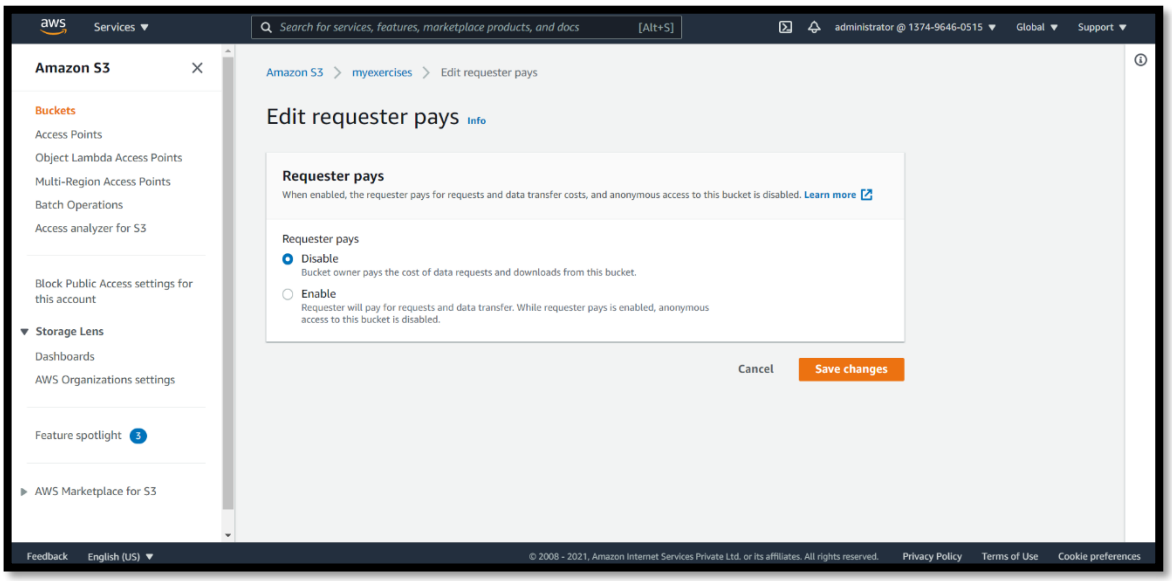
  When the requester assumes an AWS Identity and Access Management (IAM) role before making their request, the account to which the role belongs is charged for the request. For more information about IAM roles, see IAM roles in the IAM User Guide.

  After you configure a bucket to be a Requester Pays bucket, requesters must include x-amz-request-payer in their requests either in the header, for POST, GET and HEAD

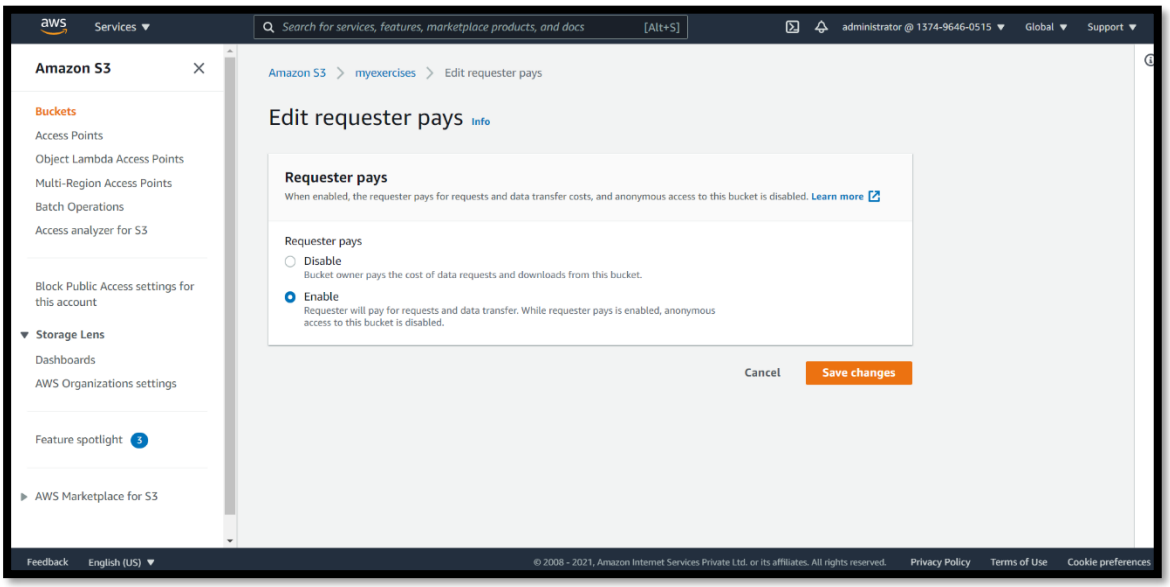
requests, or as a parameter in a REST request to show that they understand that they will be charged for the request and the data download.

Note: If we enable Requester Pays on a bucket, anonymous access to that bucket is not allowed.

- **Before State:**




- **After State:**



- **Costing:**

  The charge for successful Requester Pays requests is straightforward: The requester pays for the data transfer and the request, and the bucket owner pays for the data storage. However, the bucket owner is charged for the request under the following conditions:

  - The requester doesn't include the parameter x-amz-request-payer in the header (GET, HEAD, or POST) or as a parameter (REST) in the request (HTTP code 403).
  - Request authentication fails (HTTP code 403).
  - The request is anonymous (HTTP code 403).
  - The request is a SOAP request.

## ❖ Solution3)

- **Brief:**

  With Amazon S3 default encryption, we can set the default encryption behaviour for an S3 bucket so that all new objects are encrypted when they are stored in the bucket. The objects are encrypted using server-side encryption with either Amazon S3-managed keys (SSE-S3) or AWS KMS keys stored in AWS Key Management Service (AWS KMS) (SSE-KMS).

  When we configure our bucket to use default encryption with SSE-KMS, we can also enable S3 Bucket Keys to decrease request traffic from Amazon S3 to AWS Key Management Service (AWS KMS) and reduce the cost of encryption.

  After we enable default encryption for a bucket, the following encryption behavior applies:

  1. There is no change to the encryption of the objects that existed in the bucket before default encryption was enabled.

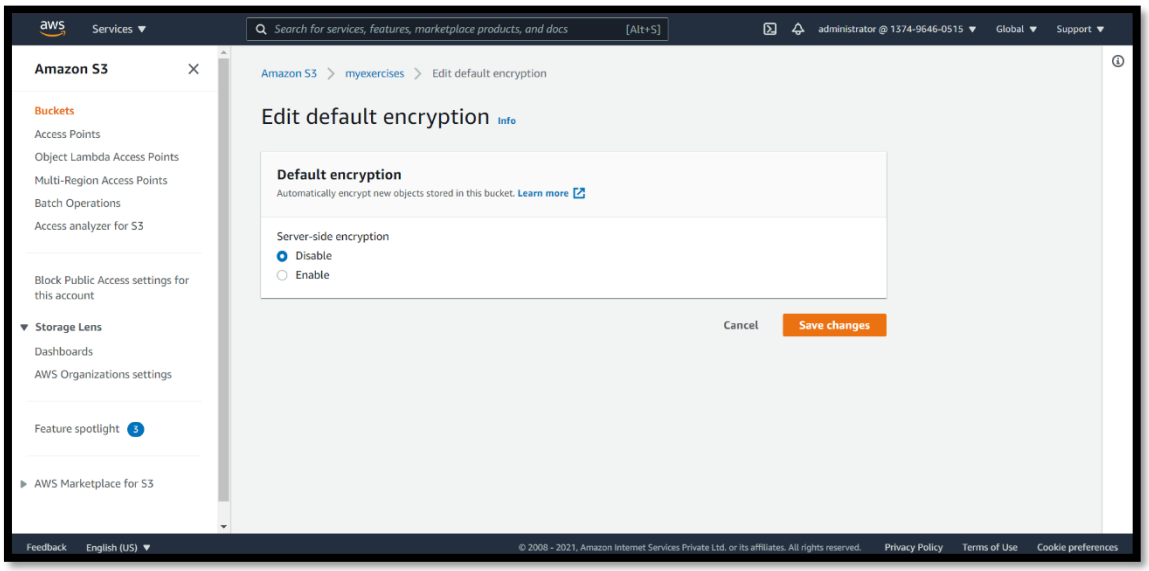
  When we upload objects after enabling default encryption:

1. If our PUT request headers don't include encryption information, Amazon S3 uses the bucket's default encryption settings to encrypt the objects.

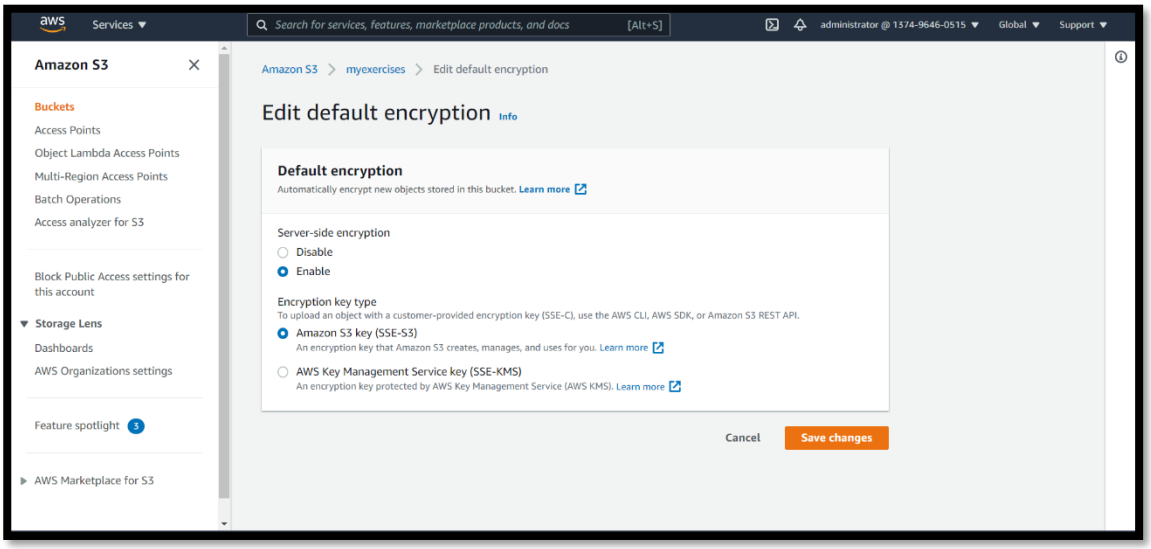
2. If our PUT request headers include encryption information, Amazon S3 uses the encryption information from the PUT request to encrypt objects before storing them in Amazon S3.

Note: Amazon S3 buckets with default bucket encryption using SSE-KMS cannot be used as destination buckets for Logging requests using server access logging. Only SSE-S3 default encryption is supported for server access log destination buckets.

- **Before State:**




- **After State:**



- **Costing:**

  Each AWS KMS key that you create in KMS costs $1/month. The $1/month charge is the same for symmetric keys, asymmetric keys, each multi-Region key (each primary and each replica multi-region key), keys with imported key material, and keys in custom key stores.

  If you enable automatic key rotation, each newly generated backing key costs an additional $1/month. This covers the cost to AWS KMS of retaining all versions of the key material so they can be used to decrypt older ciphertexts.

  You are not charged for the following:

  - Creation and storage of AWS managed or AWS owned KMS keys. These keys are automatically created on your behalf when you first attempt to encrypt a resource in an AWS service that integrates with AWS KMS. You can neither manage the lifecycle or access permissions on AWS managed keys.
  - There is no charge for customer managed KMS keys that are scheduled for deletion. If you cancel the deletion during the waiting period, the customer managed KMS key will incur charges as though it was never scheduled for deletion.
  - There is no monthly charge for data keys or data key pairs that KMS generates beyond the charge for the API call.