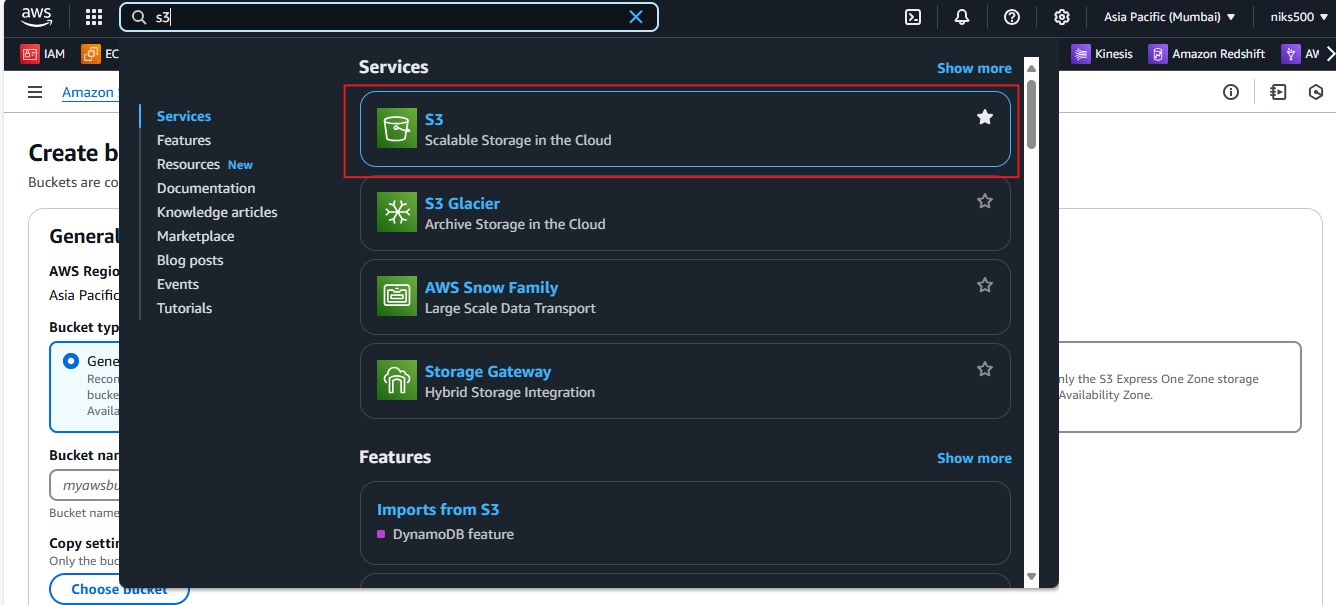
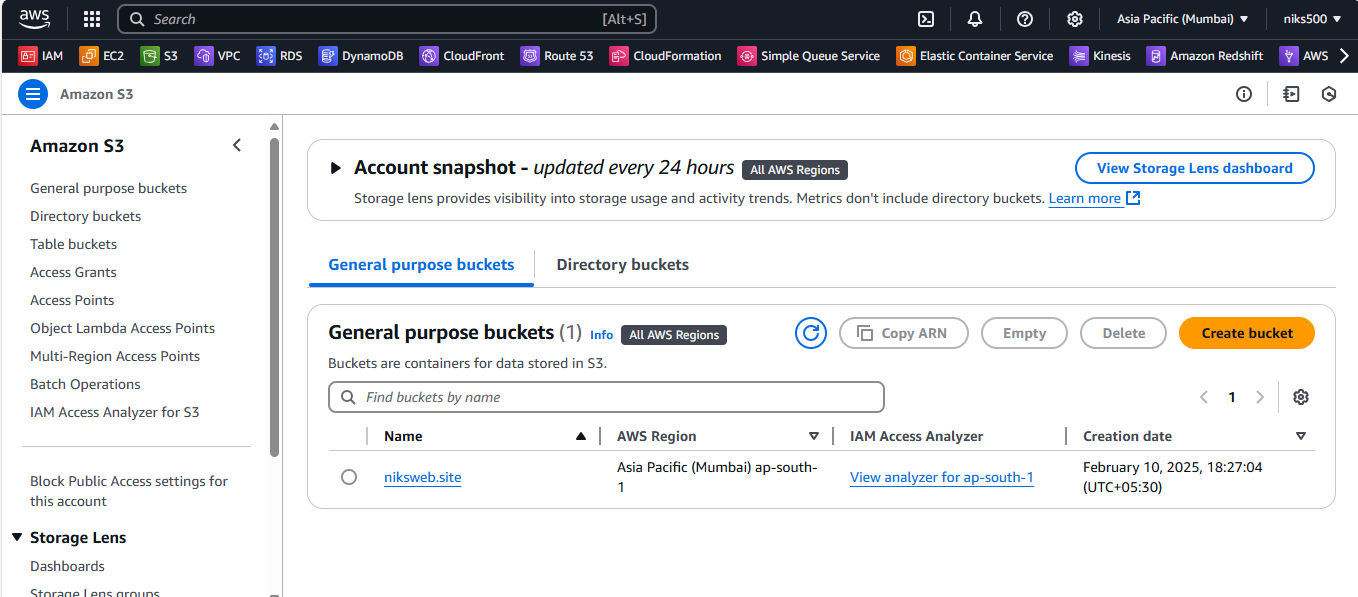
**1. Bucket-Level Access Control (Using Bucket Policy)**

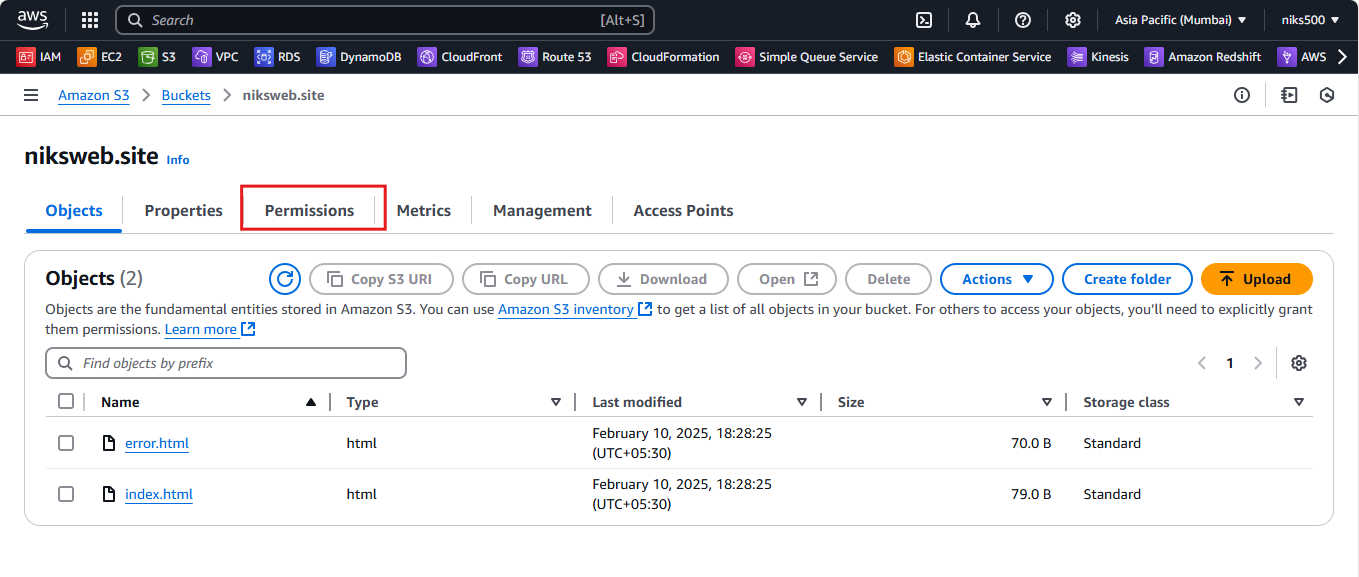
1. **Sign in to AWS Console:**
   * Go to the [AWS Management Console](https://aws.amazon.com/console/) and sign in.
2. **Navigate to S3:**
   * In the AWS Console, search for **S3** in the search bar and select **S3**.



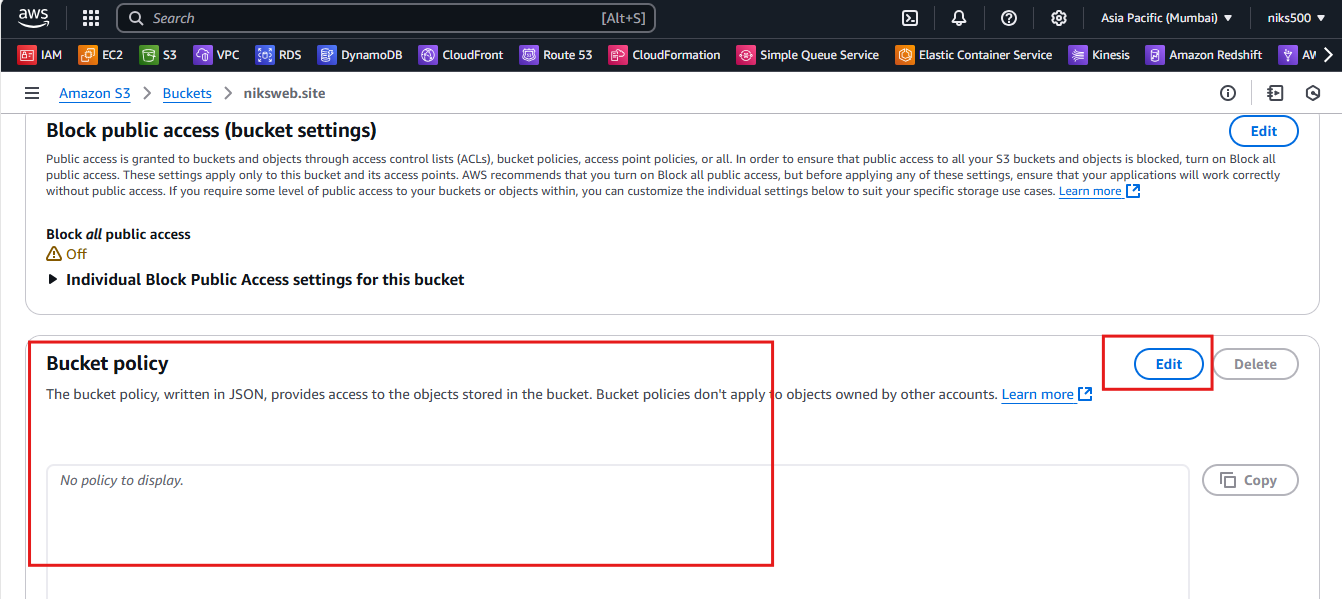
1. **Select Your Bucket:**
   * In the S3 dashboard, select the bucket for which you want to configure access control.



1. **Go to Permissions Tab:**
   * In the left sidebar, click on the **Permissions** tab.



1. **Bucket Policy:**
   * Under the **Bucket Policy** section, click **Edit** to add or modify a policy.



* + You can add a JSON policy to allow or deny access based on conditions, like the IP address, user identity, or other factors.

Example Bucket Policy (Allow public read access to objects):



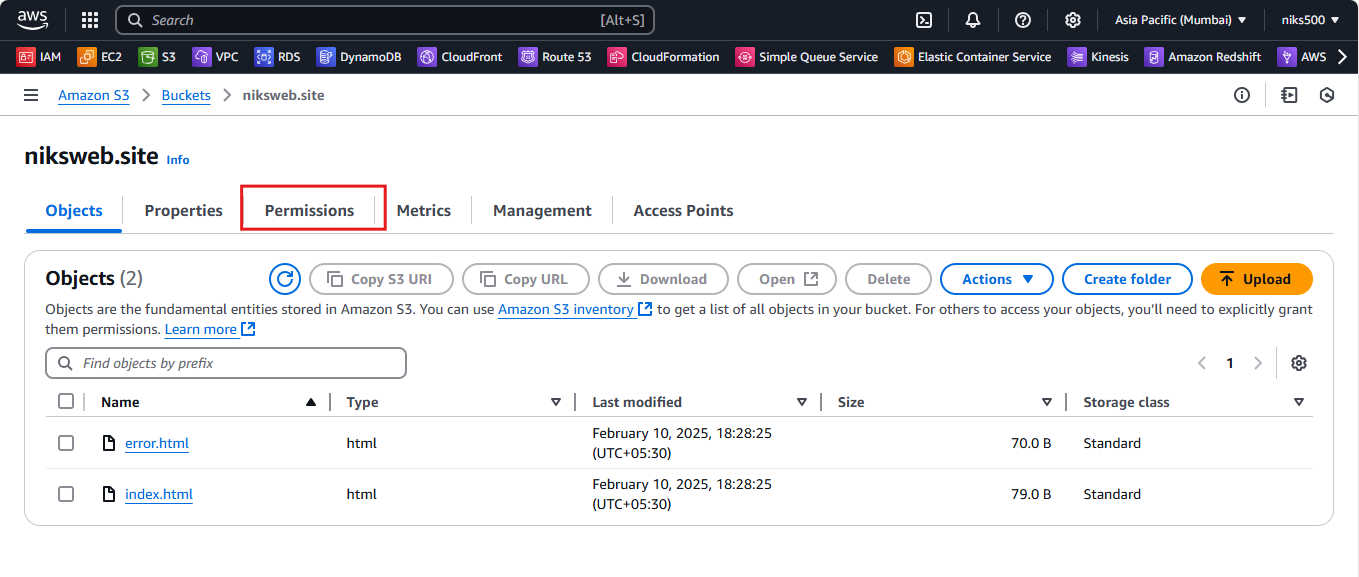
This policy allows public read access to all objects in the bucket ***niksweb.site***. Replace with your bucket name.

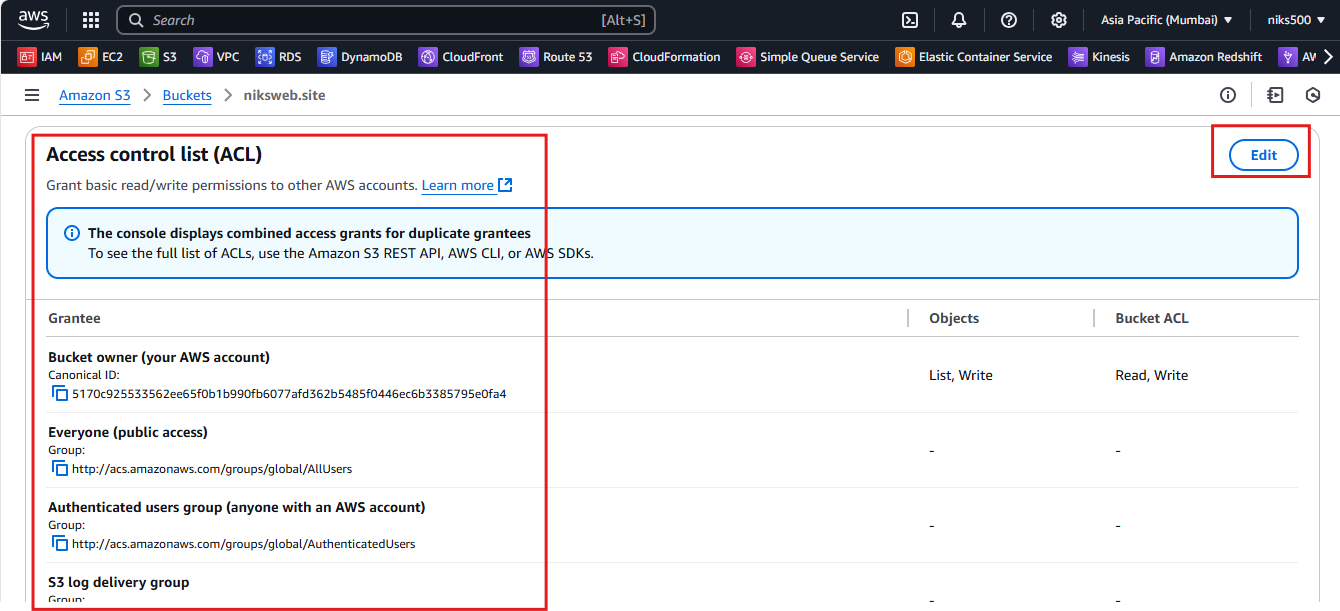
1. **Save Changes:**

* After editing the policy, click **Save changes**.

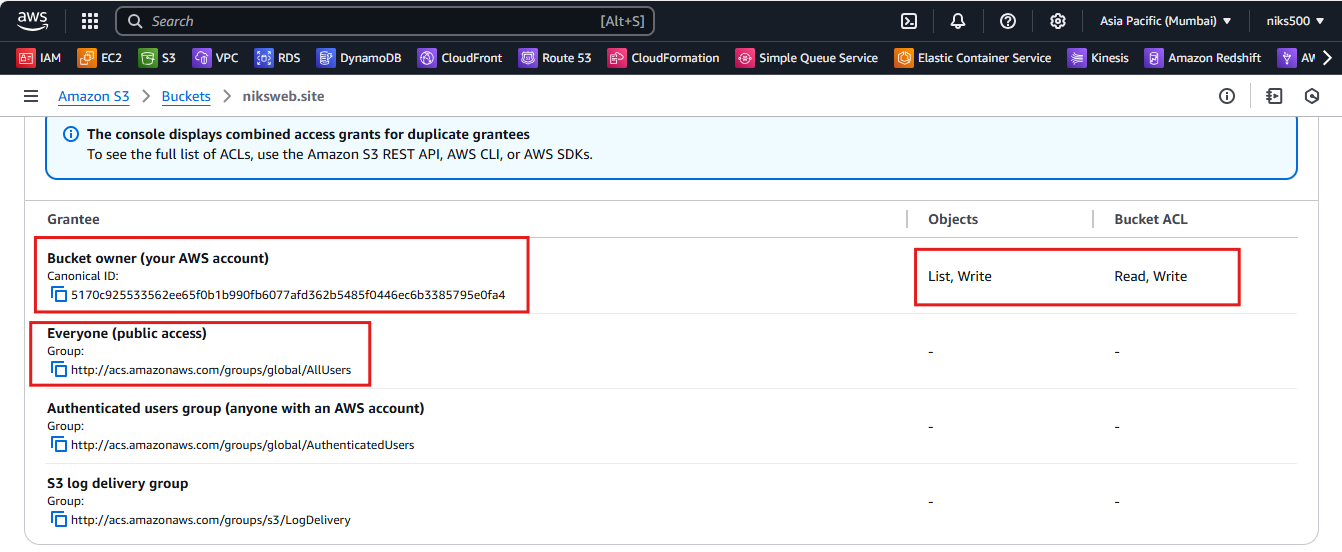
**2. Object-Level Access Control (Using Access Control List - ACL)**

1. **Navigate to Permissions:**
   * After selecting your bucket in the **S3 Console**, click on the **Permissions** tab and scroll down to the **Access Control List** (ACL) section.





1. **Grant Permissions:**
   * **Grant permissions to specific AWS accounts**: You can provide access to specific IAM users or roles by adding their **canonical user IDs**.
   * **Grant public access**: If you need to make objects publicly readable, you can use the **Public Access** settings, but be cautious about exposing sensitive data.



1. **Set Access for Each Group:**
   * Select the **Access Control List (ACL)** options and assign read or write permissions to the relevant user or group.

