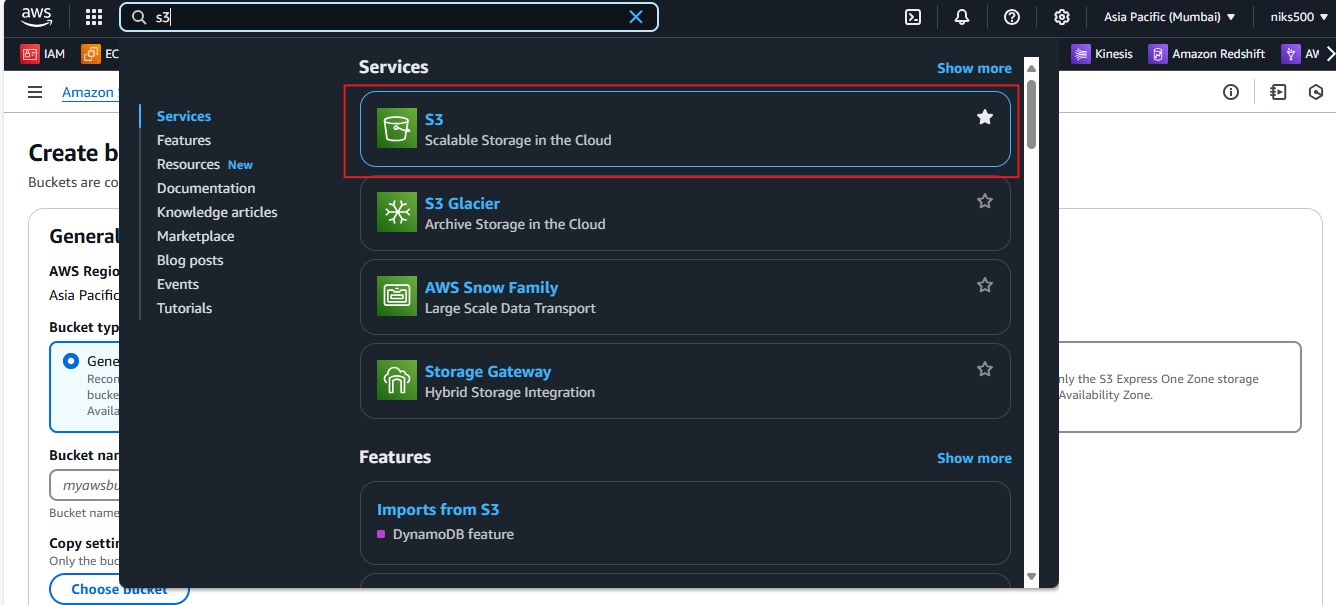
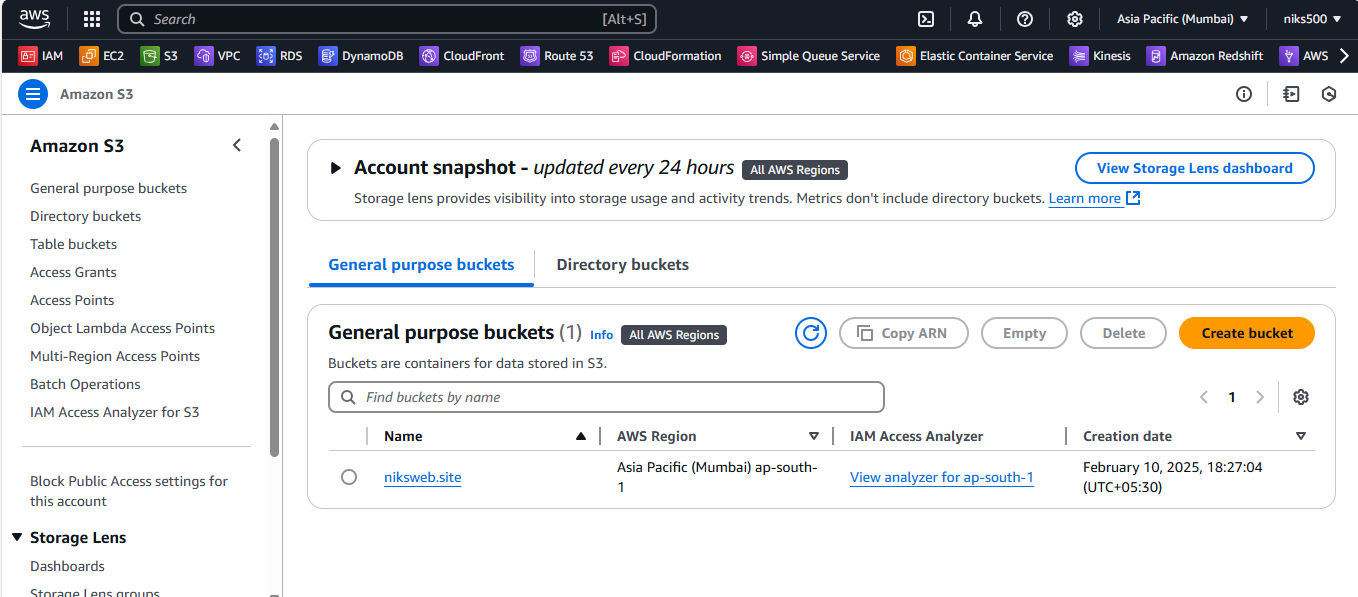
**Implementing a Bucket Policy via AWS Management Console**

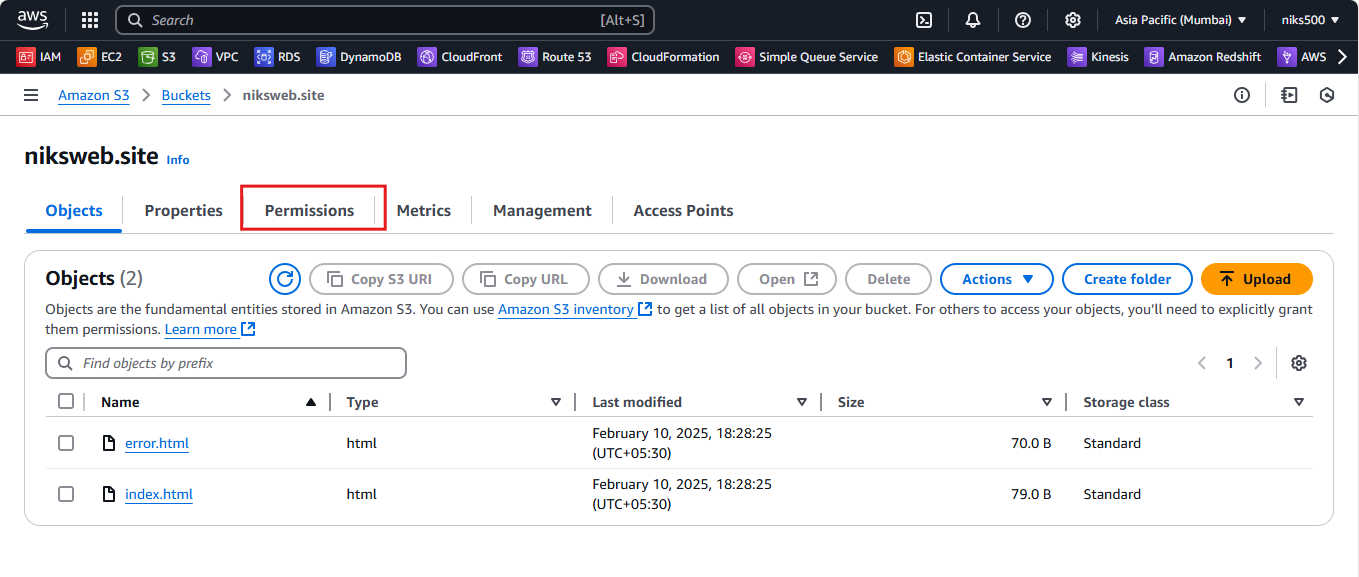
1. **Sign in to the AWS Management Console:**
   * Go to the [AWS Management Console](https://aws.amazon.com/console/).
   * Sign in with your AWS credentials.
2. **Navigate to S3:**
   * In the AWS Console, search for **S3** in the search bar and select **S3** from the list.



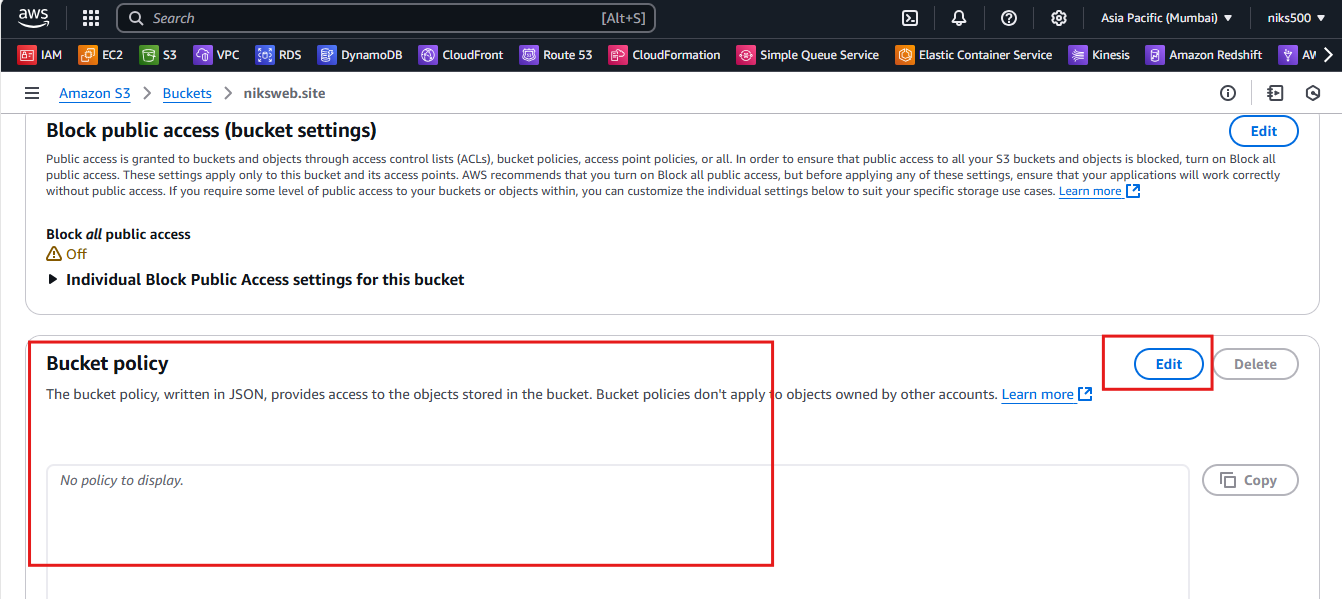
1. **Select Your Bucket:**
   * In the S3 dashboard, click on the name of the bucket to which you want to apply the policy.



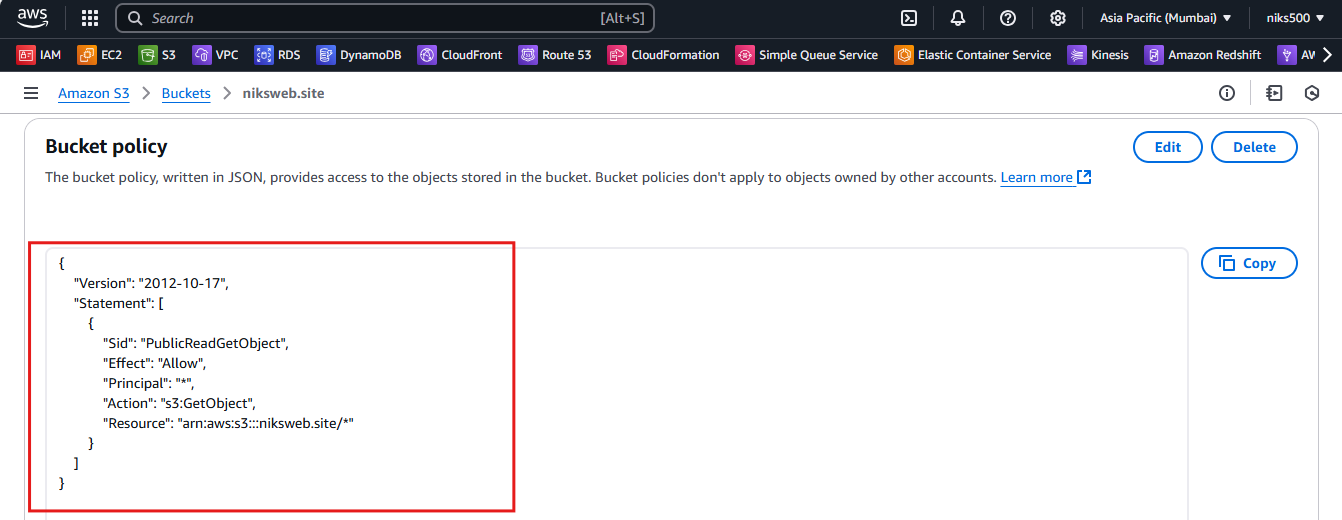
1. **Go to the Permissions Tab:**
   * In the left sidebar of your bucket's dashboard, select the **Permissions** tab.



1. **Add a Bucket Policy:**
   * Scroll down to the **Bucket Policy** section and click on the **Edit** button.



1. **Write the Bucket Policy:**
   * In the **Bucket Policy Editor**, enter the JSON policy that you want to apply to the bucket.



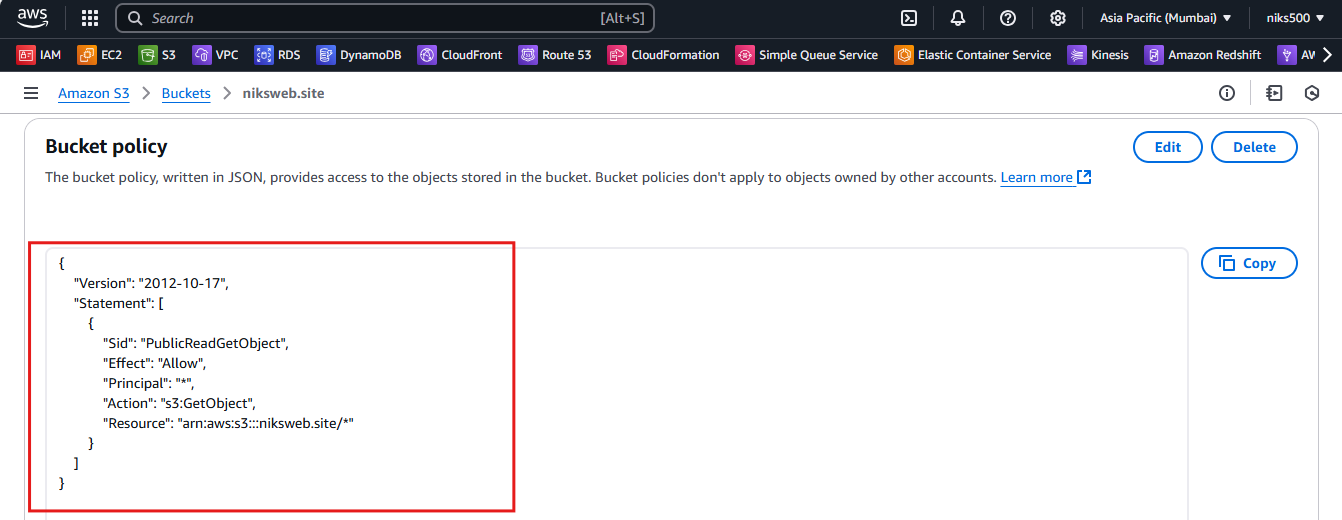
1. **Save Changes:**
   * After you’ve written the policy, click **Save changes** to apply the bucket policy.

===========================================================================

**Example Bucket Policies:**

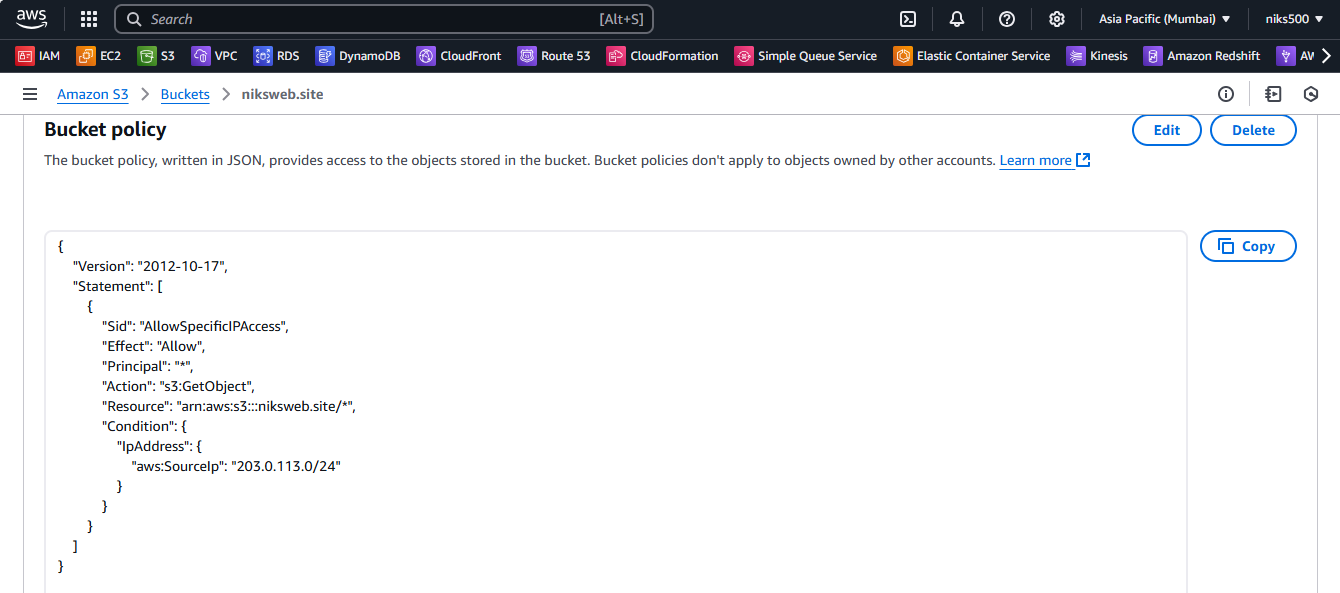
**1. Allow Public Read Access to All Objects in the Bucket**

This example policy allows **public read access** to all objects in a bucket. This might be suitable for hosting publicly accessible files like images, videos, or website content.



* **Principal**: \* means the action is allowed for all users (public).
* **Action**: s3:GetObject allows reading (GET) objects from the bucket.
* **Resource**: arn:aws:s3:::my-bucket-name/\* refers to all objects inside the bucket my-bucket-name.

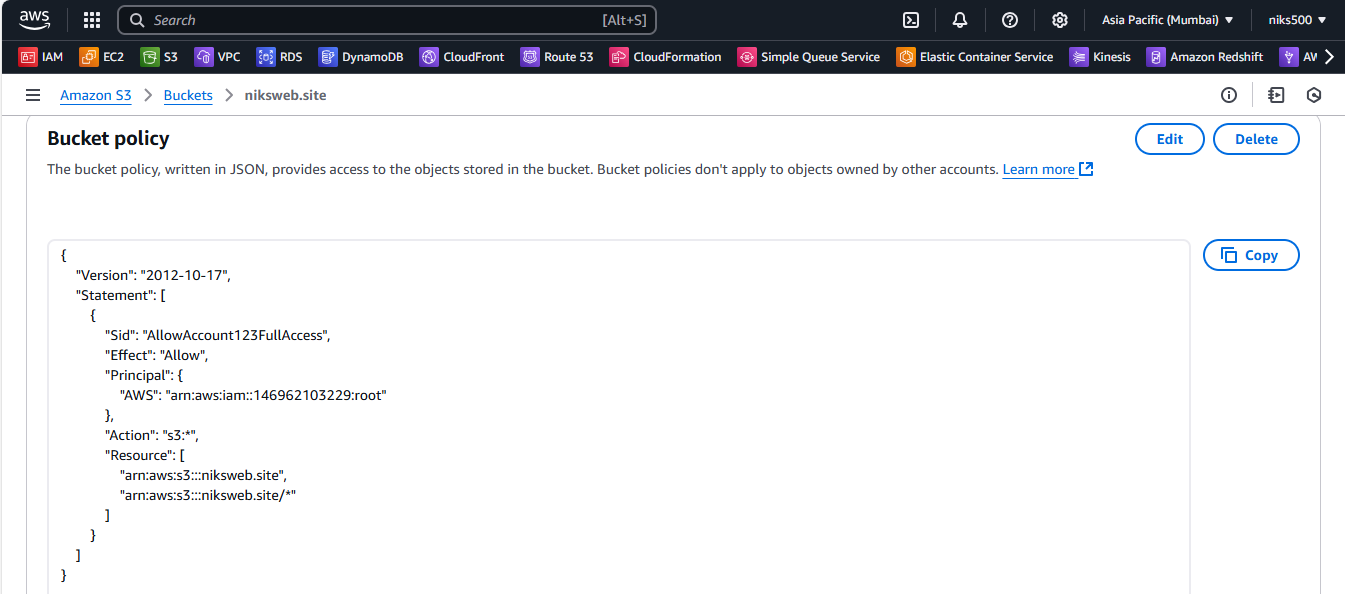
**2. Allow Only Specific IP Addresses to Access the Bucket**

This policy allows **read access** to objects in the bucket but only from specific IP addresses (e.g., 203.0.113.0/24).

* **Condition**: Limits access based on IP address (aws:SourceIp).
* **Action**: Allows only s3:GetObject (read access).

**3. Allow Access from Another AWS Account**

This policy allows another AWS account (123456789012) to have **full access** (read and write) to the objects in your bucket.



* **Principal**: Specifies the AWS account arn:aws:iam::123456789012:root as the trusted entity.
* **Action**: Allows all S3 actions (s3:\*), including both read and write actions.
* **Resource**: The bucket and all its objects (arn:aws:s3:::my-bucket-name/\*).