

1. Search S3 and click buckets:

The screenshot shows the AWS S3 service page. On the left, there's a sidebar with navigation links for 'Amazon S3', 'Buckets' (General purpose, Directory, Table, Vector), and 'Access management & security' (Access Points, Access Grants). The main area is titled 'Services' and lists three services: 'S3 Scalable Storage in the Cloud', 'S3 Glacier Archive Storage in the Cloud', and 'AWS Snow Family Large Scale Data Transport'. Each service has a star icon and a 'Show more' link.

2. Click on Create bucket :

The screenshot shows the 'General purpose buckets' list page. It displays one bucket entry: 'General purpose buckets (1) Info'. Below the list, there are buttons for 'Copy ARN', 'Empty', 'Delete', and 'Create bucket'. A search bar at the top says 'Find buckets by name'. The table headers are 'Name' and 'AWS Region'. The 'Creation date' header is also present.

3. Select General purpose , Give a bucket Name:

The screenshot shows the 'Create bucket' configuration page. Under 'General configuration', it shows the 'AWS Region' as 'Asia Pacific (Mumbai) ap-south-1' and the 'Bucket type' as 'General purpose'. The 'Bucket name' field contains 'hasrat-resume'. There are sections for 'Copy settings from existing bucket - optional' and 'Choose bucket'. A note at the bottom says 'Format: s3://bucket/prefix'.

4. Untick Block all public access and Click create bucket:

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

⚠️ Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

I acknowledge that the current settings might result in this bucket and the objects within becoming public.

5. Click on the Bucket Name (hasrat-resume) :

The screenshot shows the AWS S3 console under the 'General purpose buckets' tab. The 'hasrat-resume' bucket is listed with the following details:

Name	AWS Region	Creation date
hasrat-resume	Asia Pacific (Mumbai) ap-south-1	December 17, 2025, 19:58:31 (UTC+05:30)

Actions available for the bucket include: Copy ARN, Empty, Delete, and Create bucket.

6. Click upload and upload the static website files (index.html , style.css) :

The screenshot shows the 'Objects' tab for the 'hasrat-resume' bucket. Two files are listed:

Name	Type	Last modified	Size	Storage class
index.html	html	December 17, 2025, 19:59:03 (UTC+05:30)	2.3 KB	Standard
style.css	css	December 17, 2025, 19:59:03 (UTC+05:30)	1.0 KB	Standard

Actions available for the objects include: Copy S3 URI, Copy URL, Download, Open, Delete, Actions (Edit, Delete, Create folder), and Upload.

7. Inside the Bucket click on Properties Tab:

The screenshot shows the AWS S3 console for a bucket named "hasrat-resume". The top navigation bar has tabs for Objects, Metadata, Properties (which is underlined in blue), Permissions, Metrics, Management, and Access Points. The main content area is currently empty.

8. Scroll down and Click on edit Static web hosting and Select Enable and Save :

The screenshot shows the "Edit static website hosting" configuration page. It includes sections for "Static website hosting" (with a note about using the bucket as a website endpoint), "Hosting type" (set to "Host a static website"), and "Index document" (set to "index.html"). A note at the bottom explains that content must be publicly readable. The "Error document - optional" field is also shown.

9. Now click on Permissions Tab:

The screenshot shows the AWS S3 console for the same bucket, now with the "Permissions" tab selected. The top navigation bar shows Objects, Metadata, Properties, Permissions (underlined in blue), Metrics, Management, and Access Points. The main content area is currently empty.

10. Select Bucket policy and Update the Policy.

(Public access is enabled, and Static website hosting is ON
Without a bucket policy, users will get “403 Access Denied”
So this policy allows public read access.) :

The screenshot shows the 'Edit bucket policy' page. At the top, there's a 'Bucket policy' section with a 'Policy examples' link. Below it, the 'Bucket ARN' is listed as `arn:aws:s3:::hasrat-resume`. The main area is titled 'Policy' and contains the following JSON code:

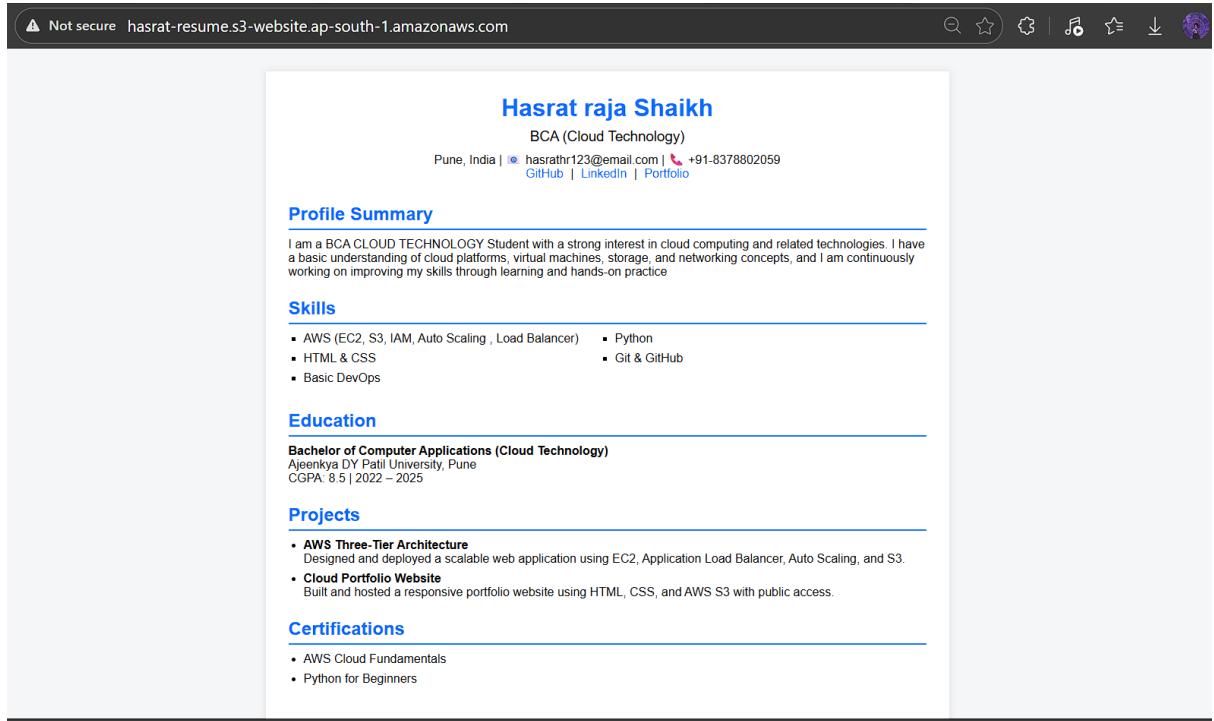
```
1 ▾ {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Sid": "PublicRead",  
6             "Effect": "Allow",  
7             "Principal": "*",  
8             "Action": "s3:GetObject",  
9             "Resource": "arn:aws:s3:::hasrat-resume/*"  
10        }  
11    ]  
12 }
```

To the right of the policy editor, there's a sidebar with 'Edit statement' and 'Select a statement' sections. A note says 'Select an existing statement in the policy or add a new statement.' At the bottom of the sidebar is a blue button labeled '+ Add new statement'.

11. Now copy the Bucket website Endpoint From the Properties Tab :

The screenshot shows the 'Static website hosting' properties tab. At the top, there's an 'Edit' button. Below it, a note says 'We recommend using AWS Amplify Hosting for static website hosting' with links to 'Create Amplify app' and 'View your existing Amplify apps'. The 'S3 static website hosting' section is set to 'Enabled'. Under 'Hosting type', it says 'Bucket hosting'. The 'Bucket website endpoint' section shows the URL `http://hasrat-resume.s3-website.ap-south-1.amazonaws.com`.

12. Paste the Endpoint in the Browser URL tab:



We can see the Static website on S3 is running.