**Create Bucket in S3:**

**Step 1: Sign in to AWS Management Console**

* Navigate to the [AWS Management Console](https://aws.amazon.com/console/) and sign in with your AWS account credentials.

**Step 2: Open the Amazon S3 Console**

* Once logged in, use the search bar at the top of the console to search for "S3". Click on the S3 option that appears in the dropdown menu to open the S3 Management Console.

**Step 3: Create a New Bucket**

* Inside the S3 Management Console, click the "Create bucket" button. This will open the "Create bucket" dialog.

**Step 4: Specify Bucket Details**

* **Bucket Name:** Enter a unique name for your bucket. The name must be globally unique across all existing bucket names in Amazon S3 (not just your account). It must comply with DNS naming conventions.
* **AWS Region:** Select the AWS Region where you want the bucket to reside. Choose a region close to you or your customers to minimize latency and costs, or to address regulatory requirements.

**Step 5: Configure Options (Optional)**

* On the same creation page, you can configure additional options such as:
  + **Versioning:** To keep multiple versions of an object in the same bucket.
  + **Server Access Logging:** To log requests made to your bucket.
  + **Tags:** To set metadata tags for easier management.
  + **Object-level logging:** To record object-level actions.
  + **Default encryption:** To automatically encrypt objects when stored.
  + **Public Access settings:** To manage public access to your bucket. AWS recommends blocking all public access unless necessary.
  + **Object Lock:** To prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely.

**Step 6: Set Permissions**

* By default, buckets are created with Block all public access enabled. You can customize the access permissions as needed, but it's essential to understand the implications of making a bucket publicly accessible.

**Upload File to S3 Bucket:**

**Step 1: Select Your Bucket**

* In the S3 Management Console, you'll see a list of your buckets. Click on the name of the bucket where you want to upload your file.

**Step 2: Upload File**

* Inside your bucket, click the “Upload” button.
* You will be presented with the upload page. Here, you can either drag and drop files into the designated area or click the “Add files” button to browse and select files from your computer.

**Step 3: Set File and Folder**

* If you want to organize your files, you can specify a folder by typing the folder name followed by a slash before the file name in the "Key" field (e.g., "myFolder/myFile.txt"). If the folder does not exist, S3 will create it for you as part of the upload process.
* After adding your files, you can click the “Next” button to proceed.

**Step 4: Set Permissions**

* On the Set permissions page, you can choose who can access the files you're uploading. By default, the files inherit the permissions of the bucket. You can also set custom permissions here.
* AWS recommends using bucket policies or IAM roles for access control, but you can also set individual file permissions if needed.
* After setting the permissions, click “Next”.

**Create acsses key:**

**Step 1: Open the IAM Console**

* Once logged in, use the search bar at the top of the console to search for "IAM". Click on the IAM option that appears in the dropdown menu to open the IAM Dashboard.

**Step 2: Navigate to Users**

* In the IAM dashboard, look for the "Users" option in the navigation pane on the left side of the console and click on it. This will show you a list of IAM users in your account.

**Step 3: Select the User**

* Find and click on the name of the user for whom you want to create an access key. If the user does not exist yet, you will need to create a new user by clicking the “Add user” button and following the prompts to complete the user creation process.

**Step 4: Access the Security Credentials Tab**

* Once you are on the user's details page, click on the "Security credentials" tab. This tab contains information about the user's credentials, including access keys, SSH keys for AWS CodeCommit, and more.

**Step 5: Create Access Key**

* In the "Access keys" section, click the “Create access key” button. A new access key will be generated for the user.
* You will see a popup window with the Access Key ID and Secret Access Key. This is the only time you will be able to view or download the Secret Access Key, so make sure to save it securely. You can click “Download .csv file” to save the credentials to your computer.