# **Creating a bucket**

To upload your data to Amazon S3, you must first create an Amazon S3 bucket in one of the AWS Regions. When you create a bucket, you must choose a bucket name and Region. You can optionally choose other storage management options for the bucket. After you create a bucket, you cannot change the bucket name or Region. For information about naming buckets, see [Bucket naming rules](https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucketnamingrules.html).

**Using the S3 console**

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. Choose Create bucket.  
   The Create bucket wizard opens.
3. In Bucket name, enter a DNS-compliant name for your bucket.  
   The bucket name must:
   1. Be unique across all of Amazon S3.
   2. Be between 3 and 63 characters long.
   3. Not contain uppercase characters.
   4. Start with a lowercase letter or number.
4. After you create the bucket, you cannot change its name. For information about naming buckets, see [Bucket naming rules](https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucketnamingrules.html).  
   **Important**Avoid including sensitive information, such as account number, in the bucket name. The bucket name is visible in the URLs that point to the objects in the bucket.
5. In Region, choose the AWS Region where you want the bucket to reside.  
   Choose a Region close to you to minimize latency and costs and address regulatory requirements. Objects stored in a Region never leave that Region unless you explicitly transfer them to another Region. For a list of Amazon S3 AWS Regions, see [AWS service endpoints](https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region) in the *Amazon Web Services General Reference*.
6. Under Object Ownership, to disable or enable ACLs and control ownership of objects uploaded in your bucket, choose one of the following settings:  
   ACLs disabled
   1. Bucket owner enforced – ACLs are disabled, and the bucket owner automatically owns and has full control over every object in the bucket. ACLs no longer affect permissions to data in the S3 bucket. The bucket uses policies to define access control.  
      To require that all new buckets are created with ACLs disabled by using IAM or AWS Organizations policies, see [Disabling ACLs for all new buckets (bucket owner enforced)](https://docs.aws.amazon.com/AmazonS3/latest/userguide/ensure-object-ownership.html#object-ownership-requiring-bucket-owner-enforced).
7. ACLs enabled
   1. Bucket owner preferred – The bucket owner owns and has full control over new objects that other accounts write to the bucket with the bucket-owner-full-control canned ACL.  
      If you apply the bucket owner preferred setting, to require all Amazon S3 uploads to include the bucket-owner-full-control canned ACL, you can [add a bucket policy](https://docs.aws.amazon.com/AmazonS3/latest/userguide/ensure-object-ownership.html#ensure-object-ownership-bucket-policy) that only allows object uploads that use this ACL.
   2. Object writer – The AWS account that uploads an object owns the object, has full control over it, and can grant other users access to it through ACLs.
8. **Note**To apply the Bucket owner enforced setting or the Bucket owner preferred setting, you must have the following permission: s3:CreateBucket and s3:PutBucketOwnershipControls.
9. In Bucket settings for Block Public Access, choose the Block Public Access settings that you want to apply to the bucket.  
   We recommend that you keep all settings enabled unless you know that you need to turn off one or more of them for your use case, such as to host a public website. Block Public Access settings that you enable for the bucket are also enabled for all access points that you create on the bucket. For more information about blocking public access, see [Blocking public access to your Amazon S3 storage](https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html).
10. (Optional) If you want to enable S3 Object Lock, do the following:
    1. Choose Advanced settings, and read the message that appears.  
       **Important**You can only enable S3 Object Lock for a bucket when you create it. If you enable Object Lock for the bucket, you cannot disable it later. Enabling Object Lock also enables versioning for the bucket. After you enable Object Lock for the bucket, you must configure the Object Lock default retention and legal hold settings to protect new objects from being deleted or overwritten. For more information, see [Configuring S3 Object Lock using the console](https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-console.html).
    2. If you want to enable Object Lock, enter **enable** in the text box and choose Confirm.
11. For more information about the S3 Object Lock feature, see [Using S3 Object Lock](https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html).  
    **Note**To create an Object Lock enabled bucket, you must have the following permissions: s3:CreateBucket, s3:PutBucketVersioning and s3:PutBucketObjectLockConfiguration.
12. Choose Create bucket