Getting started with Amazon S3

PDF (/pdfs/AmazonS3/latest/userguide/s3-userguide.pdf#GetStartedWithS3) | RSS (s3-userguide-rss-updates.rss)

You can get started with Amazon S3 by working with buckets and objects. A *bucket* is a container for objects. An *object* is a file and any metadata that describes that file.

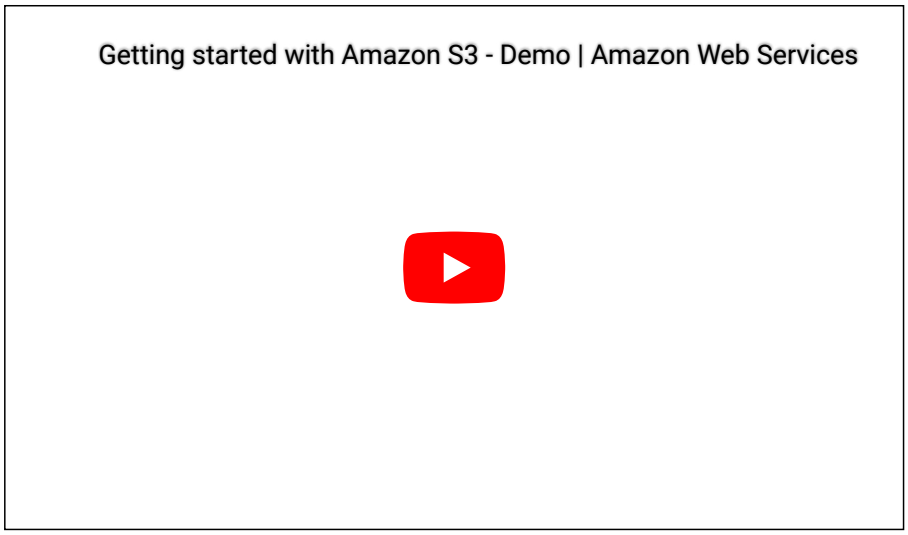
To store an object in Amazon S3, you create a bucket and then upload the object to the bucket. When the object is in the bucket, you can open it, download it, and move it. When you no longer need an object or a bucket, you can clean up your resources.

With Amazon S3, you pay only for what you use. For more information about Amazon S3 features and pricing, see Amazon S3 (https://aws.amazon.com/s3) . If you are a new Amazon S3 customer, you can get started with Amazon S3 for free. For more information, see AWS Free Tier (https://aws.amazon.com/free) .

> **Note**
>
> For more information about using the Amazon S3 Express One Zone storage class with directory buckets, see Directory buckets and S3 Express One Zone (./s3-express-one-zone.html) and Directory buckets overview (./directory-buckets-overview.html) .

Video: Getting started with Amazon S3

The following video shows you how to get started with Amazon S3.



Prerequisites

Before you begin, confirm that you've completed the steps in Setting up Amazon S3 (#setting-up-s3) .

Setting up Amazon S3

When you sign up for AWS, your AWS account is automatically signed up for all services in AWS, including Amazon S3. You are charged only for the services that you use.

With Amazon S3, you pay only for what you use. For more information about Amazon S3 features and pricing, see Amazon S3 (https://aws.amazon.com/s3) . If you are a new Amazon S3 customer, you can get started with Amazon S3 for free. For more information, see AWS Free Tier (https://aws.amazon.com/free) .

To set up Amazon S3, use the steps in the following sections.

When you sign up for AWS and set up Amazon S3, you can optionally change the display language in the AWS Management Console. For more information, see Changing the language of the AWS Management Console (https://docs.aws.amazon.com/awsconsolehelpdocs/latest/gsg/getting-started.html#change-language) in the *AWS Management Console Getting Started Guide*.

Topics

Sign up for an AWS account

If you do not have an AWS account, complete the following steps to create one.

To sign up for an AWS account

1. Open https://portal.aws.amazon.com/billing/signup (https://portal.aws.amazon.com/billing/signup) .
2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

   When you sign up for an AWS account, an *AWS account root user* is created. The root user has access to all AWS services and resources in the account. As a security best practice, assign administrative access to a user, and use only the root user to perform tasks that require root user access (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html#root-user-tasks) .

AWS sends you a confirmation email after the sign-up process is complete. At any time, you can view your current account activity and manage your account by going to https://aws.amazon.com/ (https://aws.amazon.com/) and choosing **My Account**.

Create a user with administrative access

After you sign up for an AWS account, secure your AWS account root user, enable AWS IAM Identity Center, and create an administrative user so that you don't use the root user for everyday tasks.

Secure your AWS account root user

1. Sign in to the AWS Management Console (https://console.aws.amazon.com/) as the account owner by choosing **Root user** and entering your AWS account email address. On the next page, enter your password.

   For help signing in by using root user, see Signing in as the root user (https://docs.aws.amazon.com/signin/latest/userguide/console-sign-in-tutorials.html#introduction-to-root-user-sign-in-tutorial) in the *AWS Sign-In User Guide*.
2. Turn on multi-factor authentication (MFA) for your root user.

   For instructions, see Enable a virtual MFA device for your AWS account root user (console) (https://docs.aws.amazon.com/IAM/latest/UserGuide/enable-virt-mfa-for-root.html) in the *IAM User Guide*.

Create a user with administrative access

1. Enable IAM Identity Center.

   For instructions, see Enabling AWS IAM Identity Center (https://docs.aws.amazon.com/singlesignon/latest/userguide/get-set-up-for-idc.html) in the *AWS IAM Identity Center User Guide*.
2. In IAM Identity Center, grant administrative access to a user.

For a tutorial about using the IAM Identity Center directory as your identity source, see Configure user access with the default IAM Identity Center directory (https://docs.aws.amazon.com/singlesignon/latest/userguide/quick-start-default-idc.html) in the *AWS IAM Identity Center User Guide*.

Sign in as the user with administrative access

- To sign in with your IAM Identity Center user, use the sign-in URL that was sent to your email address when you created the IAM Identity Center user.

  For help signing in using an IAM Identity Center user, see Signing in to the AWS access portal (https://docs.aws.amazon.com/signin/latest/userguide/iam-id-center-sign-in-tutorial.html) in the *AWS Sign-In User Guide*.

Assign access to additional users

1. In IAM Identity Center, create a permission set that follows the best practice of applying least-privilege permissions.

   For instructions, see Create a permission set (https://docs.aws.amazon.com/singlesignon/latest/userguide/get-started-create-a-permission-set.html) in the *AWS IAM Identity Center User Guide*.
2. Assign users to a group, and then assign single sign-on access to the group.

   For instructions, see Add groups (https://docs.aws.amazon.com/singlesignon/latest/userguide/addgroups.html) in the *AWS IAM Identity Center User Guide*.

Step 1: Create your first S3 bucket

After you sign up for AWS, you're ready to create a bucket in Amazon S3 using the AWS Management Console. Every object in Amazon S3 is stored in a *bucket*. Before you can store data in Amazon S3, you must create a bucket.

> **Note**
>
> For more information about using the Amazon S3 Express One Zone storage class with directory buckets, see Directory buckets and S3 Express One Zone (./s3-express-one-zone.html) and Directory buckets overview (./directory-buckets-overview.html) .

> **Note**
>
> You are not charged for creating a bucket. You are charged only for storing objects in the bucket and for transferring objects in and out of the bucket. The charges that you incur through following the examples in this guide are minimal (less than $1). For more information about storage charges, see Amazon S3 pricing (https://aws.amazon.com/s3/pricing/) .

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/ (https://console.aws.amazon.com/s3/) .
2. In the navigation bar on the top of the page, choose the name of the currently displayed AWS Region. Next, choose the Region in which you want to create a bucket.

   > **Note**
   >
   > To minimize latency and costs and address regulatory requirements, choose a Region close to you. 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*.

3. In the left navigation pane, choose **Buckets**.
4. Choose **Create bucket**.

   The **Create bucket** page opens.
5. Under **General configuration**, view the AWS Region where your bucket will be created.
6. Under **Bucket type**, choose **General purpose**.
7. For **Bucket name**, enter a name for your bucket.

   The bucket name must:

   - Be unique within a partition. A partition is a grouping of Regions. AWS currently has three partitions: `aws` (Standard Regions), `aws-cn` (China Regions), and `aws-us-gov` (AWS GovCloud (US) Regions).
   - Be between 3 and 63 characters long.
   - Consist only of lowercase letters, numbers, dots (.), and hyphens (-). For best compatibility, we recommend that you avoid using dots (.) in bucket names, except for buckets that are used only for static website hosting.
   - Begin and end with a letter or number.

   After you create the bucket, you cannot change its name. The AWS account that creates the bucket owns it. For more information about naming buckets, see Bucket naming rules (./bucketnamingrules.html) .

   > **Important**
   >
   > Avoid including sensitive information, such as account numbers, in the bucket name. The bucket name is visible in the URLs that point to the objects in the bucket.

8. AWS Management Console allows you to copy an existing bucket's settings to your new bucket. If you do not want to copy the settings of an existing bucket, skip to the next step.

   > **Note**
   >
   > This option:
   >
   > - Is not available in the AWS CLI and is only available in console
   > - Is not available for directory buckets
   > - Does not copy the bucket policy from the existing bucket to the new bucket

   To copy an existing bucket's settings, under **Copy settings from existing bucket**, select **Choose bucket**. The **Choose bucket** window opens. Find the bucket with the settings that you would like to copy, and select **Choose bucket**. The **Choose bucket** window closes, and the **Create bucket** window re-opens.

   Under **Copy settings from existing bucket**, you will now see the name of the bucket you selected. You will also see a **Restore defaults** option that you can use to remove the copied bucket settings. Review the remaining bucket settings, on the **Create bucket** page. You will see that they now match the settings of the bucket that you selected. You can skip to the final step.
9. 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

   - **Bucket owner enforced (default)** – ACLs are disabled, and the bucket owner automatically owns and has full control over every object in the bucket. ACLs no longer affect access permissions to data in the S3 bucket. The bucket uses policies exclusively to define access control.

     By default, ACLs are disabled. A majority of modern use cases in Amazon S3 no longer require the use of ACLs. We recommend that you keep ACLs disabled, except in unusual circumstances where you must control access for each object individually. For more information, see Controlling ownership of objects and disabling ACLs for your bucket (./about-object-ownership.html) .

   ACLs enabled

- **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 (./ensure-object-ownership.html#ensure-object-ownership-bucket-policy) that allows only object uploads that use this ACL.
- **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.

> **Note**
>
> The default setting is **Bucket owner enforced**. To apply the default setting and keep ACLs disabled, only the `s3:CreateBucket` permission is needed. To enable ACLs, you must have the `s3:PutBucketOwnershipControls` permission.

10. Under **Block Public Access settings for this bucket**, choose the Block Public Access settings that you want to apply to the bucket.

    By default, all four Block Public Access settings are enabled. We recommend that you keep all settings enabled, unless you know that you need to turn off one or more of them for your specific use case. For more information about blocking public access, see Blocking public access to your Amazon S3 storage (./access-control-block-public-access.html) .

> **Note**
>
> To enable all Block Public Access settings, only the `s3:CreateBucket` permission is required. To turn off any Block Public Access settings, you must have the `s3:PutBucketPublicAccessBlock` permission.

11. (Optional) Under **Bucket Versioning**, you can choose if you wish to keep variants of objects in your bucket. For more information about versioning, see Retaining multiple versions of objects with S3 Versioning (./Versioning.html) .

    To disable or enable versioning on your bucket, choose either **Disable** or **Enable**.
12. (Optional) Under **Tags**, you can choose to add tags to your bucket. Tags are key-value pairs used to categorize storage.

    To add a bucket tag, enter a **Key** and optionally a **Value** and choose **Add Tag**.
13. Under **Default encryption**, choose **Edit**.
14. To configure default encryption, under **Encryption type**, choose one of the following:
    - **Amazon S3 managed key (SSE-S3)**
    - **AWS Key Management Service key (SSE-KMS)**

> **Important**
>
> If you use the SSE-KMS option for your default encryption configuration, you are subject to the requests per second (RPS) quota of AWS KMS. For more information about AWS KMS quotas and how to request a quota increase, see Quotas (https://docs.aws.amazon.com/kms/latest/developerguide/limits.html) in the *AWS Key Management Service Developer Guide*.

    Buckets and new objects are encrypted with server-side encryption with an **Amazon S3 managed key** as the base level of encryption configuration. For more information about default encryption, see Setting default server-side encryption behavior for Amazon S3 buckets (./bucket-encryption.html) .

    For more information about using Amazon S3 server-side encryption to encrypt your data, see Using server-side encryption with Amazon S3 managed keys (SSE-S3) (./UsingServerSideEncryption.html) .
15. If you chose **AWS Key Management Service key (SSE-KMS)**, do the following:
    a. Under **AWS KMS key**, specify your KMS key in one of the following ways:

- To choose from a list of available KMS keys, choose **Choose from your AWS KMS keys**, and choose your **KMS key** from the list of available keys.

  Both the AWS managed key (`aws/s3`) and your customer managed keys appear in this list. For more information about customer managed keys, see Customer keys and AWS keys (https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#key-mgmt) in the *AWS Key Management Service Developer Guide*.
- To enter the KMS key ARN, choose **Enter AWS KMS key ARN**, and enter your KMS key ARN in the field that appears.
- To create a new customer managed key in the AWS KMS console, choose **Create a KMS key**.

  For more information about creating an AWS KMS key, see Creating keys (https://docs.aws.amazon.com/kms/latest/developerguide/create-keys.html) in the *AWS Key Management Service Developer Guide*.

> ⚠ **Important**
>
> You can use only KMS keys that are available in the same AWS Region as the bucket. The Amazon S3 console lists only the first 100 KMS keys in the same Region as the bucket. To use a KMS key that is not listed, you must enter your KMS key ARN. If you want to use a KMS key that is owned by a different account, you must first have permission to use the key and then you must enter the KMS key ARN. For more information on cross account permissions for KMS keys, see Creating KMS keys that other accounts can use (https://docs.aws.amazon.com/kms/latest/developerguide/key-policy-modifying-external-accounts.html#cross-account-console) in the *AWS Key Management Service Developer Guide*. For more information on SSE-KMS, see Specifying server-side encryption with AWS KMS (SSE-KMS) (./specifying-kms-encryption.html) .
>
> When you use an AWS KMS key for server-side encryption in Amazon S3, you must choose a symmetric encryption KMS key. Amazon S3 supports only symmetric encryption KMS keys and not asymmetric KMS keys. For more information, see Identifying symmetric and asymmetric KMS keys (https://docs.aws.amazon.com/kms/latest/developerguide/find-symm-asymm.html) in the *AWS Key Management Service Developer Guide*.

For more information about creating an AWS KMS key, see Creating keys (https://docs.aws.amazon.com/kms/latest/developerguide/create-keys.html) in the *AWS Key Management Service Developer Guide*. For more information about using AWS KMS with Amazon S3, see Using server-side encryption with AWS KMS keys (SSE-KMS) (./UsingKMSEncryption.html) .

b. When you configure your bucket to use default encryption with SSE-KMS, you can also enable S3 Bucket Keys. S3 Bucket Keys lower the cost of encryption by decreasing request traffic from Amazon S3 to AWS KMS. For more information, see Reducing the cost of SSE-KMS with Amazon S3 Bucket Keys (./bucket-key.html) .

   To use S3 Bucket Keys, under **Bucket Key**, choose **Enable**.

16. (Optional) If you want to enable S3 Object Lock, do the following:

    a. Choose **Advanced settings**.

> ⚠ **Important**
>
> Enabling Object Lock also enables versioning for the bucket. After enabling you must configure the Object Lock default retention and legal hold settings to protect new objects from being deleted or overwritten.

    b. If you want to enable Object Lock, choose **Enable**, read the warning that appears, and acknowledge it.

For more information, see Locking objects with Object Lock (./object-lock.html) .

> ⓘ **Note**

To create an Object Lock enabled bucket, you must have the following permissions: `s3:CreateBucket`, `s3:PutBucketVersioning` and `s3:PutBucketObjectLockConfiguration`.

17. Choose **Create bucket**.

You've created a bucket in Amazon S3.

Next step

To add an object to your bucket, see Step 2: Upload an object to your bucket (#uploading-an-object-bucket) .

Step 2: Upload an object to your bucket

After creating a bucket in Amazon S3, you're ready to upload an object to the bucket. An object can be any kind of file: a text file, a photo, a video, and so on.

> **Note**
>
> For more information about using the Amazon S3 Express One Zone storage class with directory buckets, see Directory buckets and S3 Express One Zone (./s3-express-one-zone.html) and Directory buckets overview (./directory-buckets-overview.html) .

To upload an object to a bucket

1. Open the Amazon S3 console at https://console.aws.amazon.com/s3/ (https://console.aws.amazon.com/s3/) .
2. In the **Buckets** list, choose the name of the bucket that you want to upload your object to.
3. On the **Objects** tab for your bucket, choose **Upload**.
4. Under **Files and folders**, choose **Add files**.
5. Choose a file to upload, and then choose **Open.**
6. Choose **Upload**.

You've successfully uploaded an object to your bucket.

Next step

To view your object, see Step 3: Download an object (#accessing-an-object) .

Step 3: Download an object

After you upload an object to a bucket, you can view information about your object and download the object to your local computer.

> **Note**
>
> For more information about using the Amazon S3 Express One Zone storage class with directory buckets, see Directory buckets and S3 Express One Zone (./s3-express-one-zone.html) and Directory buckets overview (./directory-buckets-overview.html) .

Using the S3 console

This section explains how to use the Amazon S3 console to download an object from an S3 bucket.

> **Note**

- You can download only one object at a time.
- If you use the Amazon S3 console to download an object whose key name ends with a period (.), the period is removed from the key name of the downloaded object. To retain the period at the end of the name of the downloaded object, you must use the AWS Command Line Interface (AWS CLI), AWS SDKs, or Amazon S3 REST API.

To download an object from an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/ (https://console.aws.amazon.com/s3/) .
2. In the **Buckets** list, choose the name of the bucket that you want to download an object from.
3. You can download an object from an S3 bucket in any of the following ways:
   - Select the check box next to the object, and choose **Download**. If you want to download the object to a specific folder, on the **Actions** menu, choose **Download as**.
   - If you want to download a specific version of the object, turn on **Show versions** (located next to the search box). Select the check box next to the version of the object that you want, and choose **Download**. If you want to download the object to a specific folder, on the **Actions** menu, choose **Download as**.

You've successfully downloaded your object.

Next step

To copy and paste your object within Amazon S3, see Step 4: Copy your object to a folder (#copying-an-object) .

Step 4: Copy your object to a folder

You've already added an object to a bucket and downloaded the object. Now, you create a folder and copy the object and paste it into the folder.

> **Note**
>
> For more information about using the Amazon S3 Express One Zone storage class with directory buckets, see Directory buckets and S3 Express One Zone (./s3-express-one-zone.html) and Directory buckets overview (./directory-buckets-overview.html) .

To copy an object to a folder

1. In the **Buckets** list, choose your bucket name.
2. Choose **Create folder** and configure a new folder:
   a. Enter a folder name (for example, `favorite-pics`).
   b. For the folder encryption setting, choose **Disable**.
   c. Choose **Save**.
3. Navigate to the Amazon S3 bucket or folder that contains the objects that you want to copy.
4. Select the check box to the left of the names of the objects that you want to copy.
5. Choose **Actions** and choose **Copy** from the list of options that appears.
   Alternatively, choose **Copy** from the options in the upper right.
6. Choose the destination folder:
   a. Choose **Browse S3**.
   b. Choose the option button to the left of the folder name.
      To navigate into a folder and choose a subfolder as your destination, choose the folder name.
   c. Choose **Choose destination**.

The path to your destination folder appears in the **Destination** box. In **Destination**, you can alternately enter your destination path, for example, s3:// *bucket-name* / *folder-name* /.

7. In the bottom right, choose **Copy**.

   Amazon S3 copies your objects to the destination folder.

Next step

To delete an object and a bucket in Amazon S3, see Step 5: Delete your objects and bucket (#deleting-object-bucket) .

Step 5: Delete your objects and bucket

When you no longer need an object or a bucket, we recommend that you delete them to prevent further charges. If you completed this getting started walkthrough as a learning exercise, and you don't plan to use your bucket or objects, we recommend that you delete your bucket and objects so that charges no longer accrue.

Before you delete your bucket, empty the bucket or delete the objects in the bucket. After you delete your objects and bucket, they are no longer available.

If you want to continue to use the same bucket name, we recommend that you delete the objects or empty the bucket, but don't delete the bucket. After you delete a bucket, the name becomes available to reuse. However, another AWS account might create a bucket with the same name before you have a chance to reuse it.

> **Note**
>
> For more information about using the Amazon S3 Express One Zone storage class with directory buckets, see Directory buckets and S3 Express One Zone (./s3-express-one-zone.html) and Directory buckets overview (./directory-buckets-overview.html) .

Topics

- Deleting an object (#clean-up-delete-objects)
- Emptying your bucket (#clean-up-empty-bucket)
- Deleting your bucket (#clean-up-delete-bucket)

Deleting an object

If you want to choose which objects you delete without emptying all the objects from your bucket, you can delete an object.

1. In the **Buckets** list, choose the name of the bucket that you want to delete an object from.
2. Select the object that you want to delete.
3. Choose **Delete** from the options in the upper right.
4. On the **Delete objects** page, type `delete` to confirm deletion of your objects.
5. Choose **Delete objects**.

Emptying your bucket

If you plan to delete your bucket, you must first empty your bucket, which deletes all the objects in the bucket.

To empty a bucket

1. In the **Buckets** list, select the bucket that you want to empty, and then choose **Empty**.

2. To confirm that you want to empty the bucket and delete all the objects in it, in **Empty bucket**, type `permanently delete`.

   > **Important**
   >
   > Emptying the bucket cannot be undone. Objects added to the bucket while the empty bucket action is in progress will be deleted.

3. To empty the bucket and delete all the objects in it, and choose **Empty**.

   An **Empty bucket: Status** page opens that you can use to review a summary of failed and successful object deletions.

4. To return to your bucket list, choose **Exit**.

Deleting your bucket

After you empty your bucket or delete all the objects from your bucket, you can delete your bucket.

1. To delete a bucket, in the **Buckets** list, select the bucket.
2. Choose **Delete**.
3. To confirm deletion, in **Delete bucket**, type the name of the bucket.

   > **Important**
   >
   > Deleting a bucket cannot be undone. Bucket names are unique. If you delete your bucket, another AWS user can use the name. If you want to continue to use the same bucket name, don't delete your bucket. Instead, empty and keep the bucket.

4. To delete your bucket, choose **Delete bucket**.

Next steps

In the preceding examples, you learned how to perform some basic Amazon S3 tasks.

The following topics explain the learning paths that you can use to gain a deeper understanding of Amazon S3 so that you can implement it in your applications.

> **Note**
>
> For more information about using the Amazon S3 Express One Zone storage class with directory buckets, see Directory buckets and S3 Express One Zone (./s3-express-one-zone.html) and Directory buckets overview (./directory-buckets-overview.html) .

Topics

Understand common use cases

You can use Amazon S3 to support your specific use case. The AWS Solutions Library (https://aws.amazon.com/solutions/) and AWS Blog (https://aws.amazon.com/blogs/) provide use-case specific

information and tutorials. The following are some common use cases for Amazon S3:

- **Backup and storage** – Use Amazon S3 storage management features to manage costs, meet regulatory requirements, reduce latency, and save multiple distinct copies of your data for compliance requirements.
- **Application hosting** – Deploy, install, and manage web applications that are reliable, highly scalable, and low-cost. For example, you can configure your Amazon S3 bucket to host a static website. For more information, see Hosting a static website using Amazon S3 (./WebsiteHosting.html) .
- **Media hosting** – Build a highly available infrastructure that hosts video, photo, or music uploads and downloads.
- **Software delivery** – Host your software applications for customers to download.

Control access to your buckets and objects

Amazon S3 provides a variety of security features and tools. For an overview, see Access control in Amazon S3 (./access-management.html) .

By default, S3 buckets and the objects in them are private. You have access only to the S3 resources that you create. You can use the following features to grant granular resource permissions that support your specific use case or to audit the permissions of your Amazon S3 resources.

- S3 Block Public Access (https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html) – Block public access to S3 buckets and objects. By default, Block Public Access settings are turned on at the bucket level.
- AWS Identity and Access Management (IAM) identities (https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-iam.html) – Use IAM or AWS IAM Identity Center to create IAM identities in your AWS account to manage access to your Amazon S3 resources. For example, you can use IAM with Amazon S3 to control the type of access that a user or group of users has to an Amazon S3 bucket that your AWS account owns. For more information about IAM identities and best practices, see IAM identities (users, user groups, and roles) (https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html) in the *IAM User Guide*.
- Bucket policies (https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucket-policies.html) – Use IAM-based policy language to configure resource-based permissions for your S3 buckets and the objects in them.
- Access control lists (ACLs) (https://docs.aws.amazon.com/AmazonS3/latest/userguide/acls.html) – Grant read and write permissions for individual buckets and objects to authorized users. As a general rule, we recommend using S3 resource-based policies (bucket policies and access point policies) or IAM user policies for access control instead of ACLs. Policies are a simplified and more flexible access-control option. With bucket policies and access point policies, you can define rules that apply broadly across all requests to your Amazon S3 resources. For more information about the specific cases when you'd use ACLs instead of resource-based policies or IAM user policies, see Identity and Access Management for Amazon S3 (./security-iam.html) .
- S3 Object Ownership (https://docs.aws.amazon.com/AmazonS3/latest/userguide/about-object-ownership.html) – Take ownership of every object in your bucket, simplifying access management for data stored in Amazon S3. S3 Object Ownership is an Amazon S3 bucket-level setting that you can use to disable or enable ACLs. By default, ACLs are disabled. With ACLs disabled, the bucket owner owns all the objects in the bucket and manages access to data exclusively by using access-management policies.
- IAM Access Analyzer for S3 (https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-analyzer.html) – Evaluate and monitor your S3 bucket access policies, ensuring that the policies provide only the intended access to your S3 resources.

Protect and monitor your storage

- Protecting your storage (./data-protection.html) – After you create buckets and upload objects in Amazon S3, you can protect your object storage. For example, you can use S3 Versioning, S3 Replication, and Multi-Region Access Point failover controls for disaster recovery, AWS Backup to back up your data, and

S3 Object Lock to set retention periods, prevent deletions and overwrites, and meet compliance requirements.

- Monitoring your storage (./monitoring-overview.html) – Monitoring is an important part of maintaining the reliability, availability, and performance of Amazon S3 and your AWS solutions. You can monitor storage activity and costs. Also, we recommend that you collect monitoring data from all the parts of your AWS solution so that you can more easily debug a multipoint failure if one occurs.

  You can also use analytics and insights in Amazon S3 to understand, analyze, and optimize your storage usage. For example, use Amazon S3 Storage Lens (./storage_lens.html) to understand, analyze, and optimize your storage. S3 Storage Lens provides 29+ usage and activity metrics and interactive dashboards to aggregate data for your entire organization, specific accounts, Regions, buckets, or prefixes. Use Storage Class Analysis (./analytics-storage-class.html) to analyze storage access patterns to decide when it's time to move your data to a more cost-effective storage class. To manage your costs, you can use S3 Lifecycle (./object-lifecycle-mgmt.html) .

Develop with Amazon S3

Amazon S3 is a REST service. You can send requests to Amazon S3 using the REST API or the AWS SDK libraries, which wrap the underlying Amazon S3 REST API, simplifying your programming tasks. You can also use the AWS Command Line Interface (AWS CLI) to make Amazon S3 API calls. For more information, see Making requests (https://docs.aws.amazon.com/AmazonS3/latest/API/MakingRequests.html) in the *Amazon S3 API Reference*.

The Amazon S3 REST API is an HTTP interface to Amazon S3. With the REST API, you use standard HTTP requests to create, fetch, and delete buckets and objects. To use the REST API, you can use any toolkit that supports HTTP. You can even use a browser to fetch objects, as long as they are anonymously readable. For more information, see Developing with Amazon S3 (https://docs.aws.amazon.com/AmazonS3/latest/API/developing-s3.html) in the *Amazon S3 API Reference*.

To help you build applications using the language of your choice, we provide the following resources.

AWS CLI

You can access the features of Amazon S3 using the AWS CLI. To download and configure the AWS CLI, see Developing with Amazon S3 using the AWS CLI (https://docs.aws.amazon.com/AmazonS3/latest/API/setup-aws-cli.html) in the *Amazon S3 API Reference*.

The AWS CLI provides two tiers of commands for accessing Amazon S3: High-level (s3 (https://docs.aws.amazon.com/cli/latest/userguide/cli-services-s3-commands.html)) commands and API-level (s3api (https://docs.aws.amazon.com/cli/latest/userguide/cli-services-s3-apicommands.html) and `s3control` commands. The high-level S3 commands simplify performing common tasks, such as creating, manipulating, and deleting objects and buckets. The s3api and s3control commands expose direct access to all Amazon S3 API operations, which you can use to carry out advanced operations that might not be possible with the high-level commands alone.

For a list of Amazon S3 AWS CLI commands, see s3 (https://awscli.amazonaws.com/v2/documentation/api/latest/reference/s3/index.html) , s3api (https://awscli.amazonaws.com/v2/documentation/api/latest/reference/s3api/index.html) , and s3control (https://awscli.amazonaws.com/v2/documentation/api/latest/reference/s3control/index.html) .

AWS SDKs and Explorers

You can use the AWS SDKs when developing applications with Amazon S3. The AWS SDKs simplify your programming tasks by wrapping the underlying REST API. The AWS Mobile SDKs and the Amplify JavaScript library are also available for building connected mobile and web applications using AWS.

In addition to the AWS SDKs, AWS Explorers are available for Visual Studio and Eclipse for Java IDE. In this case, the SDKs and the explorers are bundled together as AWS Toolkits.

For more information, see Developing with Amazon S3 using the AWS SDKs (https://docs.aws.amazon.com/AmazonS3/latest/API/sdk-general-information-section.html) in the *Amazon S3 API*

Reference.

Sample Code and Libraries

The AWS Developer Center (https://aws.amazon.com/code/Amazon-S3) and AWS Code Sample Catalog (https://docs.aws.amazon.com/code-samples/latest/catalog/welcome.html) have sample code and libraries written especially for Amazon S3. You can use these code samples to understand how to implement the Amazon S3 API. You can also view the *Amazon Simple Storage Service API Reference* (https://docs.aws.amazon.com/AmazonS3/latest/API/Welcome.html) to understand the Amazon S3 API operations in detail.

Learn from tutorials

You can get started with step-by-step tutorials to learn more about Amazon S3. These tutorials are intended for a lab-type environment, and they use fictitious company names, user names, and so on. Their purpose is to provide general guidance. They are not intended for direct use in a production environment without careful review and adaptation to meet the unique needs of your organization's environment.

Getting started

- Tutorial: Storing and retrieving a file with Amazon S3 (https://aws.amazon.com/getting-started/hands-on/backup-files-to-amazon-s3/?ref=docs_gateway/amazons3/tutorials.html)
- Tutorial: Getting started using S3 Intelligent-Tiering (https://aws.amazon.com/getting-started/hands-on/getting-started-using-amazon-s3-intelligent-tiering/?ref=docs_gateway/amazons3/tutorials.html)
- Tutorial: Getting started using the Amazon S3 Glacier storage classes (https://aws.amazon.com/getting-started/hands-on/getting-started-using-amazon-s3-glacier-storage-classes/?ref=docs_gateway/amazons3/tutorials.html)

Optimizing storage costs

- Tutorial: Getting started using S3 Intelligent-Tiering (https://aws.amazon.com/getting-started/hands-on/getting-started-using-amazon-s3-intelligent-tiering/?ref=docs_gateway/amazons3/tutorials.html)
- Tutorial: Getting started using the Amazon S3 Glacier storage classes (https://aws.amazon.com/getting-started/hands-on/getting-started-using-amazon-s3-glacier-storage-classes/?ref=docs_gateway/amazons3/tutorials.html)
- Tutorial: Optimizing costs and gaining visibility into usage with S3 Storage Lens (https://aws.amazon.com/getting-started/hands-on/amazon-s3-storage-lens/?ref=docs_gateway/amazons3/tutorials.html)

Managing storage

- Tutorial: Getting started with Amazon S3 Multi-Region Access Points (https://aws.amazon.com/getting-started/hands-on/getting-started-with-amazon-s3-multi-region-access-points/?ref=docs_gateway/amazons3/tutorials.html)
- Tutorial: Replicating existing objects in your Amazon S3 buckets with S3 Batch Replication (https://aws.amazon.com/getting-started/hands-on/replicate-existing-objects-with-amazon-s3-batch-replication/?ref=docs_gateway/amazons3/tutorials.html)

Hosting videos and websites

- Tutorial: Hosting on-demand streaming video with Amazon S3, Amazon CloudFront, and Amazon Route 53 (./tutorial-s3-cloudfront-route53-video-streaming.html)
- Tutorial: Configuring a static website on Amazon S3 (./HostingWebsiteOnS3Setup.html)
- Tutorial: Configuring a static website using a custom domain registered with Route 53 (./website-hosting-custom-domain-walkthrough.html)

Processing data

- Tutorial: Transforming data for your application with S3 Object Lambda (./tutorial-s3-object-lambda-uppercase.html)
- Tutorial: Detecting and redacting PII data with S3 Object Lambda and Amazon Comprehend (./tutorial-s3-object-lambda-redact-pii.html)
- Tutorial: Using S3 Object Lambda to dynamically watermark images as they are retrieved (https://aws.amazon.com/getting-started/hands-on/amazon-s3-object-lambda-to-dynamically-watermark-images/?ref=docs_gateway/amazons3/tutorials.html)
- Tutorial: Batch-transcoding videos with S3 Batch Operations (./tutorial-s3-batchops-lambda-mediaconvert-video.html)

Protecting data

- Tutorial: Checking the integrity of data in Amazon S3 with additional checksums (https://aws.amazon.com/getting-started/hands-on/amazon-s3-with-additional-checksums/?ref=docs_gateway/amazons3/tutorials.html)
- Tutorial: Replicating data within and between AWS Regions using S3 Replication (https://aws.amazon.com/getting-started/hands-on/replicate-data-using-amazon-s3-replication/?ref=docs_gateway/amazons3/tutorials.html)
- Tutorial: Protecting data on Amazon S3 against accidental deletion or application bugs using S3 Versioning, S3 Object Lock, and S3 Replication (https://aws.amazon.com/getting-started/hands-on/protect-data-on-amazon-s3/?ref=docs_gateway/amazons3/tutorials.html)
- Tutorial: Replicating existing objects in your Amazon S3 buckets with S3 Batch Replication (https://aws.amazon.com/getting-started/hands-on/replicate-existing-objects-with-amazon-s3-batch-replication/?ref=docs_gateway/amazons3/tutorials.html)

Explore training and support

You can learn from AWS experts to advance your skills and get expert assistance achieving your objectives.

- **Training** – Training resources provide a hands-on approach to learning Amazon S3. For more information, see AWS training and certification (https://www.aws.training) and AWS online tech talks (https://aws.amazon.com/events/online-tech-talks) .
- **Discussion Forums** – On the forum, you can review posts to understand what you can and can't do with Amazon S3. You can also post your questions. For more information, see Discussion Forums (https://forums.aws.amazon.com/index.jspa) .
- **Technical Support** – If you have further questions, you can contact Technical Support (https://aws.amazon.com/contact-us) .

Discover highly rated pages *Abstracts generated by AI*

AmazonS3 › userguide
What is Amazon S3?
(https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html)
Amazon S3 offers scalable object storage, management features, access control, data processing, monitoring, analytics.

October 1, 2024

AmazonS3 › userguide
Bucket naming rules
(https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucketnamingrules.html)
Amazon S3 bucket naming conventions cover general purpose, directory buckets, uniqueness, character, length, suffix restrictions

September 28, 2024

AmazonS3 › userguide

Hosting a static website using Amazon S3
(https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteHosting.html)

Host static sites on S3, use CloudFront for HTTPS, and Route 53 for custom domains. Step-by-step walkthroughs available.

January 25, 2024