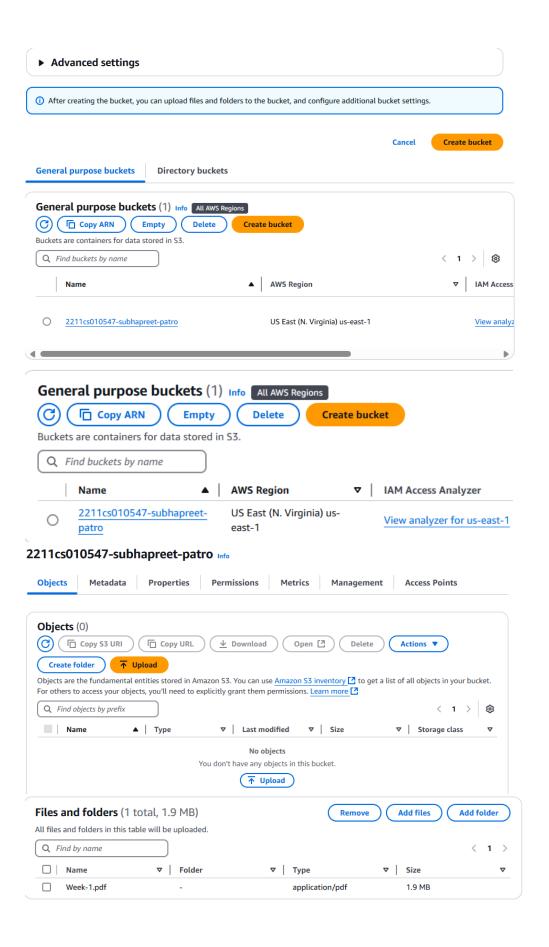
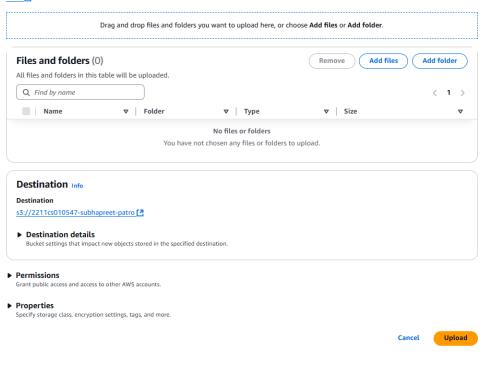


Bucket type Info			
• General purpose Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.	O Directory Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.		
Bucket name Info 2211CS010547-subhapreet-patro Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming ? Copy settings from existing bucket - optional Only the bucket settings in the following configuration are copied. Choose bucket Format: s3://bucket/prefix			
		Object Ownership Info Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.	
		ACLs disabled (recommended) All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.	Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
Object Ownership Bucket owner enforced			
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 53 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 53 resources. ✓ Block public and cross-account access to buckets and objects through any public bucket or access point policies ✓ S3 will lignore public and cross-account access for buckets and objects through any public bucket or access point policies ✓ S3 will lignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects. 			
		Bucket Versioning Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more Bucket Versioning Disable Enable	
		Tags - optional (0) You can use bucket tags to track storage costs and organize buckets. Learn more	
		No tags associated with this bucket. Add tag	
Default encryption Info Server-side encryption is automatically applied to new objects stored in this bucket.			
Encryption type Info Server-side encryption with Amazon S3 managed keys (SSE-S3) Server-side encryption with AWS Key Management Service keys (SSE-KMS) Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS) Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the Amazon S3 pricing page. [2]			
Bucket Key Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more Disable Enable			



Upload Info

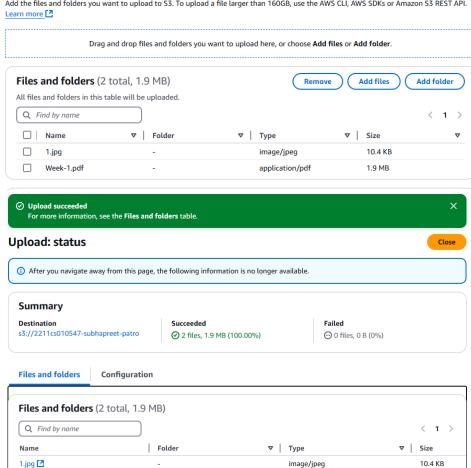
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. Learn more 🛂



Upload Info

Week-1.pdf 🛂

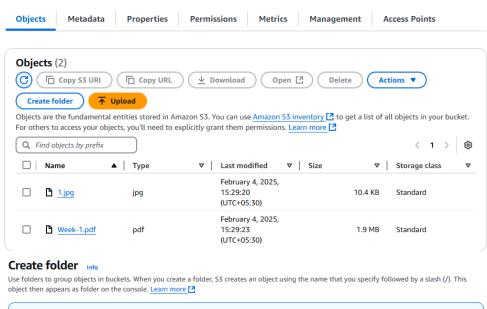
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API.



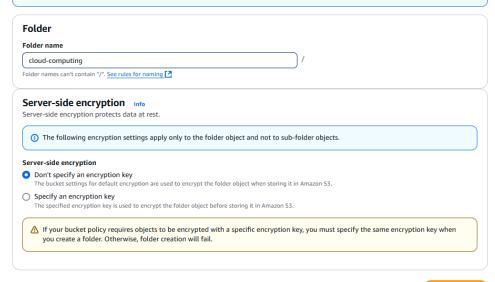
application/pdf

1.9 MB

2211cs010547-subhapreet-patro Info



① Your bucket policy might block folder creation If your bucket policy prevents uploading objects without specific tags, metadata, or access control list (ACL) grantees, you will not be able to create a folder using this configuration. Instead, you can use the <u>upload configuration</u> to upload an empty folder and specify the appropriate settings.



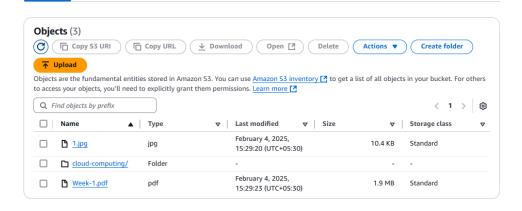
Cancel

Create folder

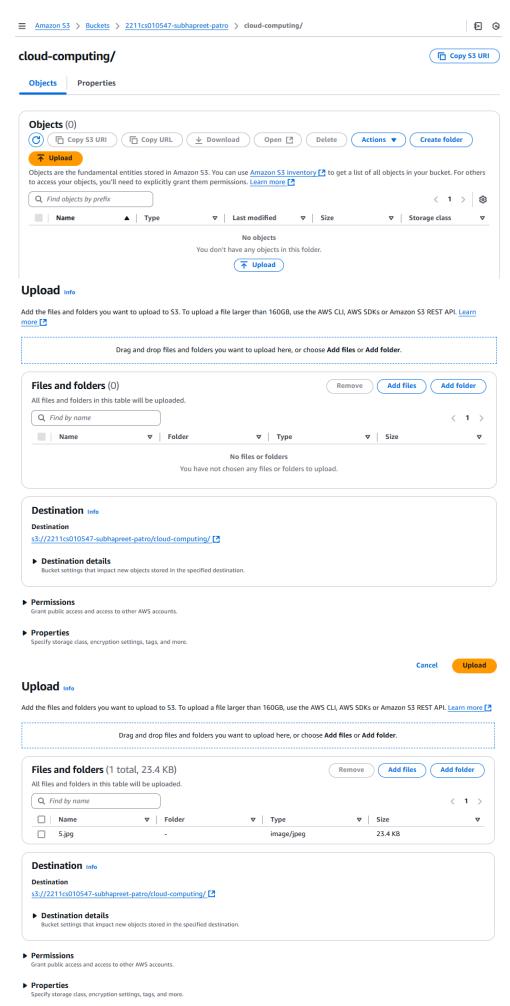
2211cs010547-subhapreet-patro Info

Properties

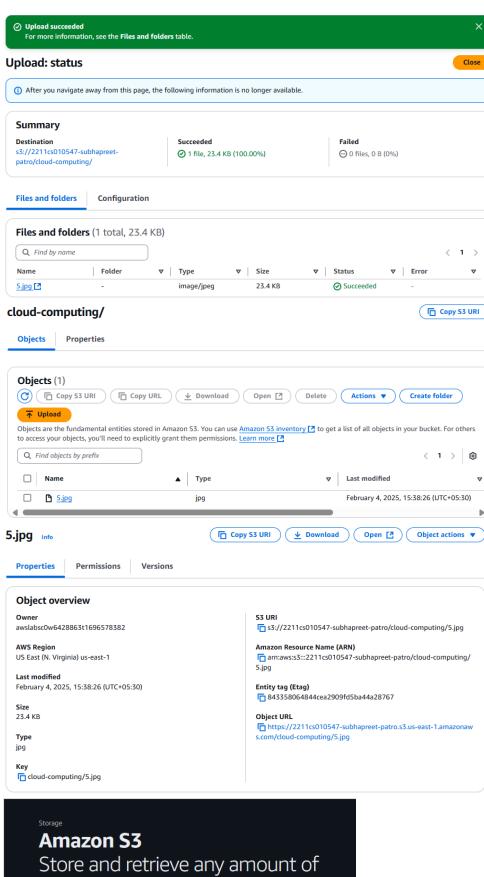
Objects Metadata



Permissions Metrics Management Access Points



Cancel Upload





Create bucket Info Buckets are containers for data stored in S3. General configuration **AWS Region** US East (N. Virginia) us-east-1 Bucket type Info General purpose Directory commended for low-latency use cases. These buckets use only the S3 press One Zone storage class, which provides faster processing of data thin a single Availability Zone. buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones Bucket name Info 2211cs010547-subhapreet-patro-1 Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming Copy settings from existing bucket - optional he bucket settings in the following configuration are copied. Choose bucket Format: s3://bucket/prefix Object Ownership Info Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects. ACLs disabled (recommended) ACLs enabled Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs. All objects in this bucket are owned by this and its objects is specified using only polic d by this account. Access to this bucket

ACLs disabled (recommended) All objects in this bucket are owned by this account. Access to this bucket and its objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies. Me recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing. Object Ownership Bucket owner preferred If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer. Object writer The object writer remains the object owner. If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. Learn more

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) 53 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 53 resources using ACLs. Block public access to buckets and objects granted through new public bucket or access point policies 53 will lignore all ACLs that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to 53 resources. Block public and cross-account access to buckets and objects through new public bucket or access point policies 53 will lignore public and cross-account access to buckets and objects through new public bucket or access point policies 54 will lignore public and cross-account access to buckets and objects through new public bucket or access point policies

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning

Disable

Enable

Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type Info

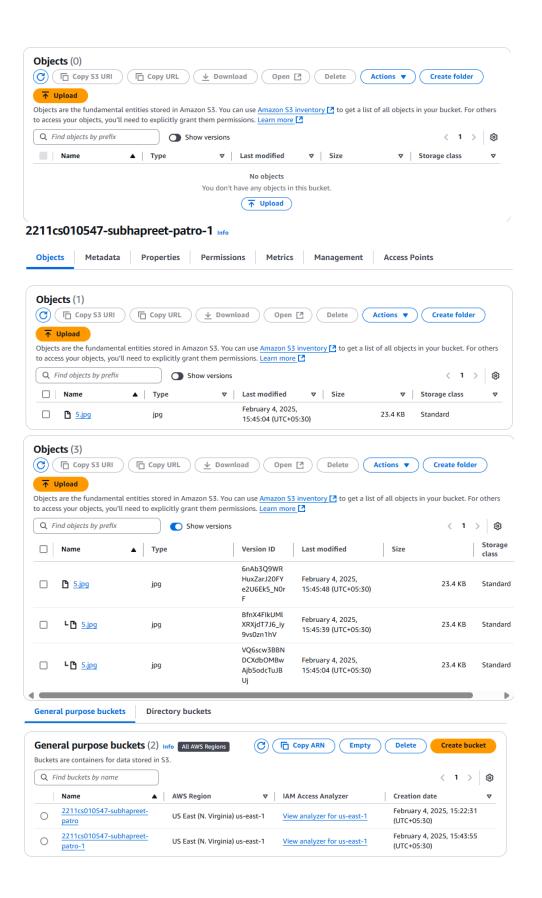
- Server-side encryption with Amazon S3 managed keys (SSE-S3)
- O Server-side encryption with AWS Key Management Service keys (SSE-KMS)
- Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
 Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the Amazon S3 pricing page. [2]

Bucket Key

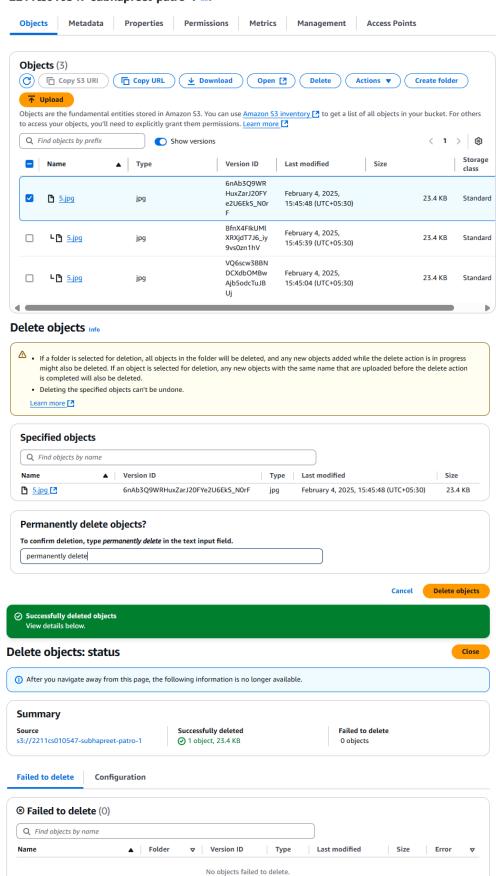
n S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more 🛂

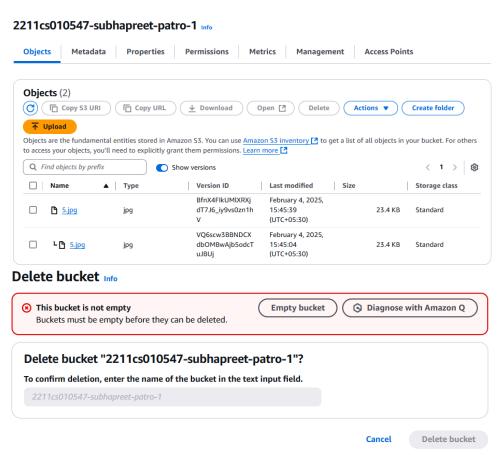
O Disable

Enable



2211cs010547-subhapreet-patro-1 Info





Empty bucket Info



- Emptying the bucket deletes all objects in the bucket and cannot be undone.
 - Objects added to the bucket while the empty bucket action is in progress might be deleted.
 - To prevent new objects from being added to this bucket while the empty bucket action is in progress, you might need to update your bucket policy to stop objects from being added to the bucket.

Learn more [2

1 If your bucket contains a large number of objects, creating a lifecycle rule to delete all objects in the bucket might be a more efficient way of emptying your bucket. Learn more 🔼

Go to lifecycle rule configuration

Permanently delete all objects in bucket "2211cs010547-subhapreet-patro-1"?

To confirm deletion, type permanently delete in the text input field.

permanently delete

Cancel

Empty

Delete bucket Info



- Deleting a bucket cannot be undone.
 - Bucket names are unique. If you delete a bucket, another AWS user can use the name.
 - If this bucket is used with a Multi-Region Access Point in an external account, initiate failover before deleting the
 - · If this bucket is used with an access point in an external account, the requests made through those access points will fail after you delete this bucket.

Learn more 🛂

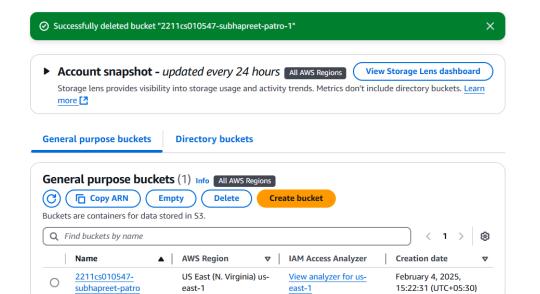
Delete bucket "2211cs010547-subhapreet-patro-1"?

To confirm deletion, enter the name of the bucket in the text input field.

2211cs010547-subhapreet-patro-1

Cancel

Delete bucket



east-1

subhapreet-patro

east-1