Amazon Simple Storage Service

Console User Guide

API Version 2006-03-01

Amazon Web Services, LLC

Amazon Simple Storage Service: Console User Guide

Amazon Web Services, LLC

Welcome to Amazon S3

This is the *Amazon Simple Storage Service (Amazon S3) Console User Guide*. It explains the AWS Management Console interface when working with Amazon S3. You can use console to create buckets, store and retrieve your objects, and manage permissions to your resources without having to write any code.

Amazon Simple Storage Service (Amazon S3) is a web service that enables you to store data in the cloud. You can then download the data or use the data with other AWS services, such as Amazon Elastic Cloud Computer (see Amazon Elastic Compute Cloud (Amazon EC2)).

How do I...?

Information	Relevant Sections
General product overview and pricing	Amazon Simple Storage Service (Amazon S3)
General information about Amazon S3	Introduction to Amazon S3 (p. 2)
Conceptual information about Amazon S3	Amazon S3 Concepts (p. 3)
Using the AWS Management Console to interact with Amazon S3	Using the Console (p. 8)
Working with buckets using AWS Management Console	Working with Buckets (p. 10)
Working with objects using AWS Management Console	Working with Objects (p. 29)

Introduction to Amazon S3

Topics

This introduction to Amazon S3 is intended to give you a detailed summary of this web service. After reading this section, you should have a good idea of what it offers and how you can use Amazon S3 for your business.

Overview of Amazon S3

Amazon S3 is storage for the Internet. It is designed to make web-scale computing easier for developers.

The AWS Management Console makes it easy to store and retrieve any amount of data, at any time, from anywhere on the web. It gives any user access to the same highly scalable, reliable, fast, inexpensive data storage infrastructure that Amazon uses to run its own global network of web sites.

Advantages to Amazon S3

Amazon S3 is intentionally built with a minimal feature set that focuses on simplicity and robustness. Following are some of advantages of the Amazon S3 service:

- **Unlimited storage—**There is no limit to the amount of data you can store on Amazon S3
- **Standard interface—**Amazon S3 uses standards based REST and SOAP interfaces designed to work with any Internet-development toolkit
- **Scalable—**Amazon S3 can scale in terms of storage, request rate, and users to support an unlimited number of web-scale applications
- **Reliability—**Store data with up to 99.999999999% durability, with 99.99% availability
- **Inexpensive—**Amazon S3 is built from inexpensive commodity hardware components

Amazon S3 Concepts

Topics

This section describes key concepts and terminology you need to understand to use Amazon S3 effectively. They are presented in the order you will most like encounter them.

Buckets

A bucket is a container for objects stored in Amazon S3. Every object is contained in a bucket. For example, if the object named `photos/puppy.jpg` is stored in the `johnsmith` bucket, then it is addressable using the URL `http://johnsmith.s3.amazonaws.com/photos/puppy.jpg`

Buckets serve several purposes: they organize the Amazon S3 namespace at the highest level, they identify the account responsible for storage and data transfer charges, they play a role in access control, and they serve as the unit of aggregation for usage reporting.

You can configure buckets so that they are created in a specific Region. For more information, see Regions (p. 4).

Objects

Objects are the fundamental entities stored in Amazon S3. When using the console, you can think of them as being files. Objects consist of data and metadata. The data portion is opaque to Amazon S3. The metadata is a set of name-value pairs that describe the object. These include some default metadata such as the date last modified, and standard HTTP metadata such as Content-Type. The developer can also specify custom metadata at the time the object is stored.

An object is uniquely identified within a bucket by a key (name).

Folders

Folders are available in the AWS Management Console, but are not part of the core Amazon S3 API. You use folders to group objects in a bucket.

When you create a folder in the AWS Management Console, Amazon S3 creates a zero-byte object with a forward slash (/) at the end of the object name in your bucket. Amazon S3 interprets the forward slash as a delimiter when performing list operations. For example, if you create a new folder in the AWS Management Console called `logs`, Amazon S3 creates an object called `logs/`. If you upload an object called `history.txt` to the `logs` folder using the AWS Management Console, the full key name for this object is `logs/history.txt`.

For more information about how Amazon S3 treats keys, go to Amazon S3 Developer Guide.

Keys

A key is like a file name; it is the unique identifier for an object within a bucket. Every object in a bucket has exactly one key. Because the combination of a bucket, key, and version ID uniquely identify each object, Amazon S3 can be thought of as a basic data map between "bucket + key + version" and the object itself. Every object in Amazon S3 can be uniquely addressed through the combination of the web service endpoint, bucket name, key, and optionally, a version. For example, in the URL http://doc.s3.amazonaws.com/2006-03-01/AmazonS3.wsdl, "doc" is the name of the bucket and "2006-03-01/AmazonS3.wsdl" is the key.

Regions

You can choose the geographical Region where Amazon S3 will store the buckets you create. You might choose a Region to optimize latency, minimize costs, or address regulatory requirements. Amazon S3 currently supports the following Regions:

- **US Standard—**Uses Amazon S3 servers in the United States
  This is the default Region. The US Standard Region automatically routes requests to facilities in Northern Virginia or the Pacific Northwest using network maps. To use this region, select US - Standard as the region when creating a bucket in the console. The US Standard Region provides eventual consistency for all requests.
- **US West (Oregon) Region—**Uses Amazon S3 servers in Oregon
  To use this Region, choose Oregon as the Region when creating the bucket in the AWS Management Console. In Amazon S3, the US West (Oregon) Region provides read-after-write consistency for PUTS of new objects in your Amazon S3 bucket and eventual consistency for overwrite PUTS and DELETES.
- **US West (Northern California) Region—**Uses Amazon S3 servers in Northern California
  To use this Region, choose US - N. California as the Region when creating the bucket in the AWS Management Console. In Amazon S3, the US Northern California Region provides read-after-write consistency for PUTS of new objects in your Amazon S3 bucket and eventual consistency for overwrite PUTS and DELETES.
- **EU (Ireland) Region—**Uses Amazon S3 servers in Ireland
  To use this Region, choose EU - Ireland as the Region when creating the bucket in the AWS Management Console.. In Amazon S3, the EU (Ireland) Region provides read-after-write consistency for PUTS of new objects in your Amazon S3 bucket and eventual consistency for overwrite PUTS and DELETES.
- **Asia Pacific (Singapore) Region—**Uses Amazon S3 servers in Singapore
  To use this Region, choose Singapore as the Region when creating the bucket in the AWS Management Console. In Amazon S3, the Asia Pacific (Singapore) Region provides read-after-write consistency for PUTS of new objects in your Amazon S3 bucket and eventual consistency for overwrite PUTS and DELETES.
- **Asia Pacific (Sydney) Region—**Uses Amazon S3 servers in Sydney
  To use this Region, choose Sydney as the Region when creating the bucket in the AWS Management Console. In Amazon S3, the Asia Pacific (Sydney) Region provides read-after-write consistency for PUTS of new objects in your Amazon S3 bucket and eventual consistency for overwrite PUTS and DELETES.
- **Asia Pacific (Tokyo) Region—**Uses Amazon S3 servers in Tokyo
  To use this Region, choose Tokyo as the Region when creating the bucket in the AWS Management Console. In Amazon S3, the Asia Pacific (Tokyo) Region provides read-after-write consistency for PUTS of new objects in your Amazon S3 bucket and eventual consistency for overwrite PUTS and DELETES.
- **South America (Sao Paulo) Region—**Uses Amazon S3 servers in Sao Paulo
  To use this Region, choose Sao Paulo as the Region when creating the bucket in the AWS Management Console. In Amazon S3, the South America (Sao Paulo) Region provides read-after-write consistency

for PUTS of new objects in your Amazon S3 bucket and eventual consistency for overwrite PUTS and DELETES.

Objects stored in a Region never leave the Region unless you explicitly transfer them to another Region. For example, objects stored in the EU (Ireland) Region never leave it. The objects stored in an S3 region physically remain in that region. Amazon S3 does not keep copies or move it to any other region. However, you can access the objects from anywhere, as long as you have necessary permissions.

Access Control

Amazon S3 has two ways of controlling access to buckets and objects: access control lists (ACLs) and bucket policies. Access Control Lists (ACLs), you can define the permissions associated with each individual Amazon S3 bucket or object resource. Policies are a collection of statements that define a user's permissions to access Amazon S3 resources. Policies can be attached to users, groups, or Amazon S3 buckets, enabling centralized management of permissions.

Amazon S3 Data Consistency Model

Updates to a single key are atomic. For example, if you PUT to an existing key, a subsequent read might return the old data or the updated data, but it will never write corrupted or partial data.

Amazon S3 achieves high availability by replicating data across multiple servers within Amazon's data centers. After a "success" is returned, your data is safely stored. However, information about the changes might not immediately replicate across Amazon S3 and you might observe the following behaviors:

- A process writes a new object to Amazon S3 and immediately attempts to read it. Until the change is fully propagated, Amazon S3 might report "key does not exist."
- A process writes a new object to Amazon S3 and immediately lists keys within its bucket. Until the change is fully propagated, the object might not appear in the list.
- A process replaces an existing object and immediately attempts to read it. Until the change is fully propagated, Amazon S3 might return the prior data.
- A process deletes an existing object and immediately attempts to read it. Until the deletion is fully propagated, Amazon S3 might return the deleted data.
- A process deletes an existing object and immediately lists keys within its bucket. Until the deletion is fully propagated, Amazon S3 might list the deleted object.

The US Standard Region provides eventual consistency for all requests. All other regions provide read-after-write consistency for PUTS of new objects and eventual consistency for overwrite PUTS and DELETES.

> **Note**
> Amazon S3 does not currently support object locking. If two puts are simultaneously made to the same key, the put with the latest time stamp wins. If this is an issue, you will need to build an object-locking mechanism into your application.
> Updates are key-based; there is no way to make atomic updates across keys. For example, you cannot make the update of one key dependent on the update of another key unless you design this functionality into your application.

The following table describes the characteristics of eventually consistent read and consistent read.

Eventually Consistent Read	Consistent Read
Stale reads possible	No stale reads
Lowest read latency	Potential higher read latency

Eventually Consistent Read	Consistent Read
Highest read throughput	Potential lower read throughput

For more information about the Amazon S3 Data Consistency Model see the Amazon S3 Developer Guide.

Limitations of the AWS Management Console

The AWS Management Console is a powerful tool that makes using Amazon S3 easy. The following features are currently unavailable in the AWS Management Console:

- Requester pays
- BitTorrent
- Versioning

The AWS Management Console will be updated to support all these Amazon S3 features.

Paying for Amazon S3

Pricing for Amazon S3 is designed so that you don't have to plan for the storage requirements of your application. Most storage providers force you to purchase a predetermined amount of storage and network transfer capacity: If you exceed that capacity, your service is shut off or you are charged high overage fees. If you do not exceed that capacity, you pay as though you used it all.

Amazon S3 charges you only for what you actually use, with no hidden fees and no overage charges. This gives developers a variable-cost service that can grow with their business while enjoying the cost advantages of Amazon's infrastructure.

Before storing anything in Amazon S3, you need to register with the service and provide a payment instrument that will be charged at the end of each month. There are no set-up fees to begin using the service. At the end of the month, your payment instrument is automatically charged for that month's usage.

For information about paying for Amazon S3 storage, go to the AWS Resource Center.

Related Amazon Web Service Products

Once we load your data into Amazon S3 you can use it with all AWS products. The following products are the ones you might use most frequently:

- **Amazon CloudFront—**This web service provides an easy way to distribute content to end users with low latency, high data transfer speeds, and no commitments.
  For more information, go to Amazon CloudFront.
- **Amazon ElasticCompute Cloud—**This web service provides virtual compute resources in the cloud. For more information, go to Amazon Elastic Compute Cloud.
- **Amazon Elastic MapReduce—**This web service enables businesses, researchers, data analysts, and developers to easily and cost-effectively process vast amounts of data.

It utilizes a hosted Hadoop framework running on the web-scale infrastructure of Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Simple Storage Service (Amazon S3). For more information, go to Amazon Elastic MapReduce.

- **Amazon Import/Export—**This service enables you to mail a storage device, such as a RAID drive, to Amazon so that we can upload your (terabytes) of data onto Amazon S3. For more information, go to *AWS Import/Export Developer Guide*.

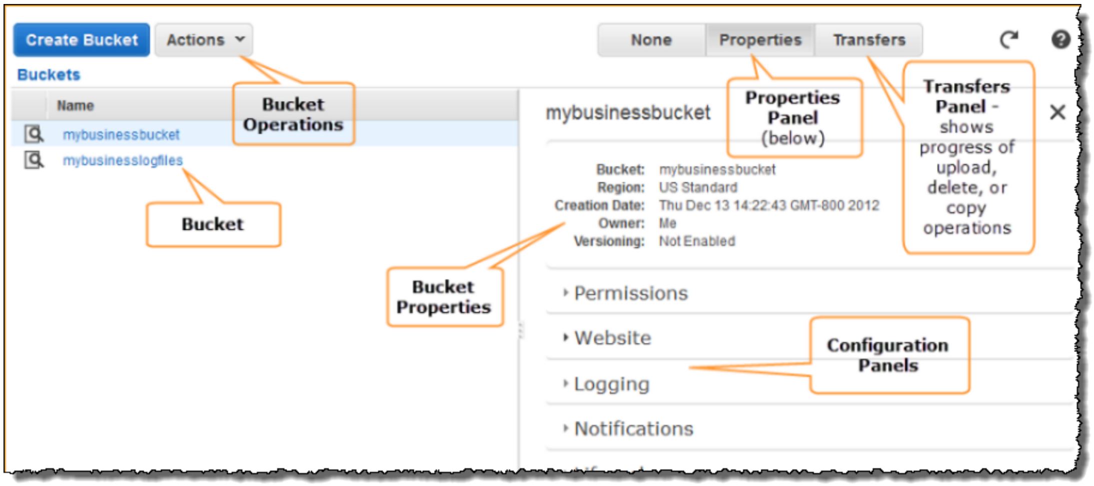
Introduction to the Console

This section provides an overview of the functionality of the AWS Management Console, which is located at https://console.aws.amazon.com/s3/home.

To use the information in this guide, you must have an Amazon S3 account. If you do not, please go to the Amazon S3 Getting Started Guide and follow the instructions for registering for Amazon S3.

The AWS Management Console provides access to multiple AWS products. The Amazon S3 console is shown for illustration.

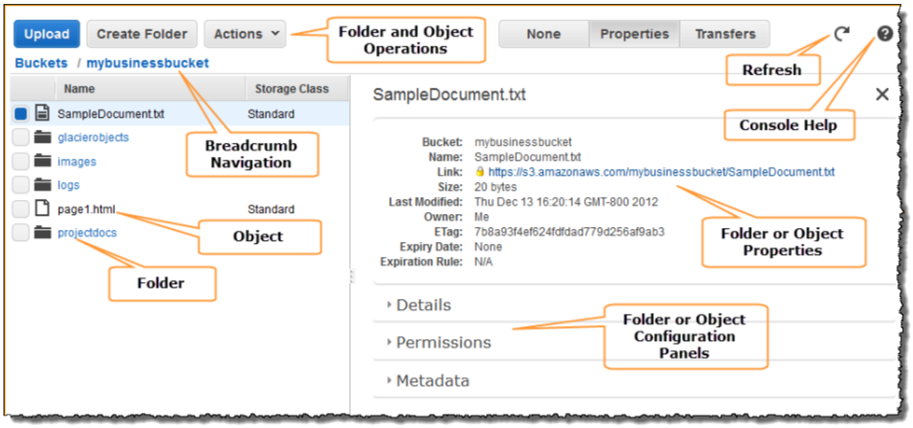
Buckets View



Bucket: mybusinessbucket
Region: US Standard
Creation Date: Thu Dec 13 14:22:43 GMT-800 2012
Owner: Me
Versioning: Not Enabled

The Buckets list shows the buckets you own. The details pane shows bucket properties and the configuration options.

Objects and Folders View



Name	Storage Class
SampleDocument.txt	Standard
glacierobjects	
images	
logs	
page1.html	Standard
projectdocs	

SampleDocument.txt

Bucket: mybusinessbucket
Name: SampleDocument.txt
Link: https://s3.amazonaws.com/mybusinessbucket/SampleDocument.txt
Size: 20 bytes
Last Modified: Thu Dec 13 16:20:14 GMT-800 2012
Owner: Me
ETag: 7b8a93f4ef624fdfdad779d256af9ab3
Expiry Date: None
Expiration Rule: N/A

The Objects and Folders list shows the contents of the Amazon S3 bucket that is indicated. You use folders to create logical groupings of objects. The details pane shows the properties of the object that is selected in the Objects and Folders list.

You can use the console to manage all your Amazon S3 resources. You can also use the console to manage multiple objects at the same time.

Working with a Single Bucket, Object, or Folder

1	Right-click the bucket, object, or folder you want to work with.
2	Select the action you want to perform from the drop-down list.

Tip

You can use the **SHIFT** and **CRTL** keys to select multiple objects and perform the same action on them simultaneously.

Working with Buckets

Topics

Every object you store in Amazon S3 resides in a bucket. You can use buckets to group related objects, in the way you use a directory to group files in a file system. Buckets have properties, such as access permissions, versioning status, and you can specify the region where you want them to reside.

This section explains how to use the Amazon S3 console to create, delete, and manage buckets.

Creating a Bucket

Before you can upload data into Amazon S3, you must create a bucket to store the data in. Buckets have configuration properties, including their geographical region, who has access to the objects in the bucket, and other metadata, such as the storage class of the objects in the bucket.

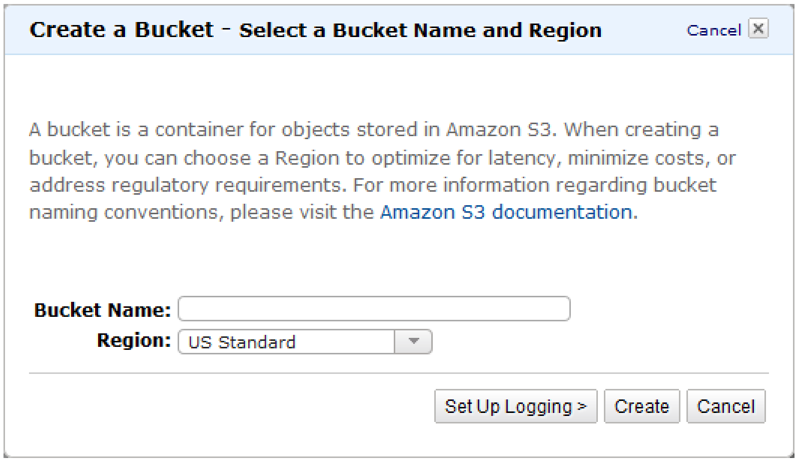
The console enables you to use folders, which you can store objects in. Folders, like objects, must reside in a bucket. For more information about using folders, see Working With Folders (p. 51).

Use the following procedure to create a bucket.

> **Note**
> You are not charged for creating a bucket; you are only charged for storing objects in the bucket and for transferring objects out of the bucket.

To create a bucket

1. Sign into the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3.
2. Click **Create Bucket**.
3. In the Create Bucket dialog box, in the Bucket Name box, type a name for your bucket.



Create a Bucket - Select a Bucket Name and Region

A bucket is a container for objects stored in Amazon S3. When creating a bucket, you can choose a Region to optimize for latency, minimize costs, or address regulatory requirements. For more information regarding bucket naming conventions, please visit the Amazon S3 documentation.

Bucket Name:

Region: US Standard

The name that you choose must be unique across all existing bucket names in Amazon S3. One way to help ensure uniqueness is to prefix your bucket names with the name of your organization.

The bucket name is visible in the URL that points to the objects that you're going to put in your bucket. For that reason, choose a bucket name that reflects the objects in the bucket.

Bucket names must comply with the following requirements.

- Can contain lowercase letters, numbers, periods (.), underscores (_), and dashes (-).
- Must start with a number or letter.
- Must be between 3 and 255 characters long.
- Must not be formatted as an IP address (e.g., 192.168.5.4) .

To conform with DNS requirements, we recommend the following, additional guidelines when creating bucket names. Bucket names:

- Should not contain underscores (_)
- Should be between 3 and 63 characters long
- Should not end with a dash
- Cannot contain two, adjacent periods
- Cannot contain dashes next to periods (e.g., `my-.bucket.com` and `my.-bucket` are invalid)

> **Note**
> If you want to use your S3 bucket as an origin for an Amazon CloudFront distribution, the requirements for naming S3 buckets are more restrictive. For more information, see the `DNSName` element in the "S3Origin Child Elements" table in the DistributionConfig Complex Type section of the *Amazon CloudFront API Reference*.

To take advantage of Amazon S3's CNAME support, you should name your bucket the same as your website's base address (e.g. `www.mysite.com`). For more information about CNAME, go to Virtual Hosting in the Amazon S3 Developer Guide.

> **Note**
> Once you create a bucket, you cannot change the name of it. Make sure the bucket name you choose is appropriate.

4. In the **Region** box, click the region where you want the bucket to reside.

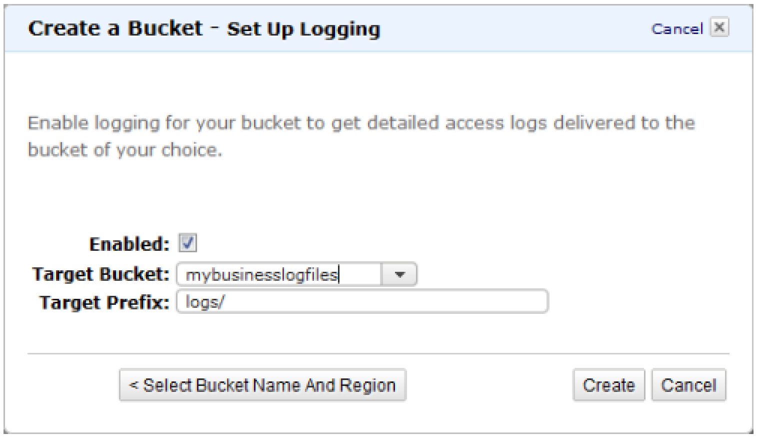
   You should choose a region close to you to optimize latency, minimize costs, or to address regulatory requirements. Objects stored in a region never leave that region unless you explicitly transfer them to another region. For more information about regions, see Regions (p. 4).

   In the next step, you have the opportunity to set up logging. Server access logging provides detailed records for the requests made against your bucket. An access log record contains details about the request, such as the request type, the resources specified in the request worked, and the time and date the request was processed. Server access logs are useful for many applications because they give bucket owners insight into the nature of requests made by clients not under their control. Amazon S3 delivers access logs to your bucket. By default, Amazon S3 does not collect server access logs.
5. Do one of the following.

To...	Do this...
Create a bucket without setting up logging	Click **Create**
Set up server access logging for the bucket you're creating	Click **Set Up Logging**

> **Note**
> There is no extra charge for enabling server access logging on an Amazon S3 bucket. However, any log files the system delivers to you will accrue the usual charges for storage. (You can delete log files at any time.) We do not assess data transfer charges for delivering log files to your bucket, but we do charge the normal data transfer rate for accessing the log files. For more information, go to Amazon S3 Pricing.

6. If you clicked **Set Up Logging** in the **Create a Bucket - Set Up Logging** dialog box, do the following:


Create a Bucket - Set Up Logging
Cancel ☒
< Select Bucket Name And Region
Create
Cancel

Enable logging for your bucket to get detailed access logs delivered to the bucket of your choice.

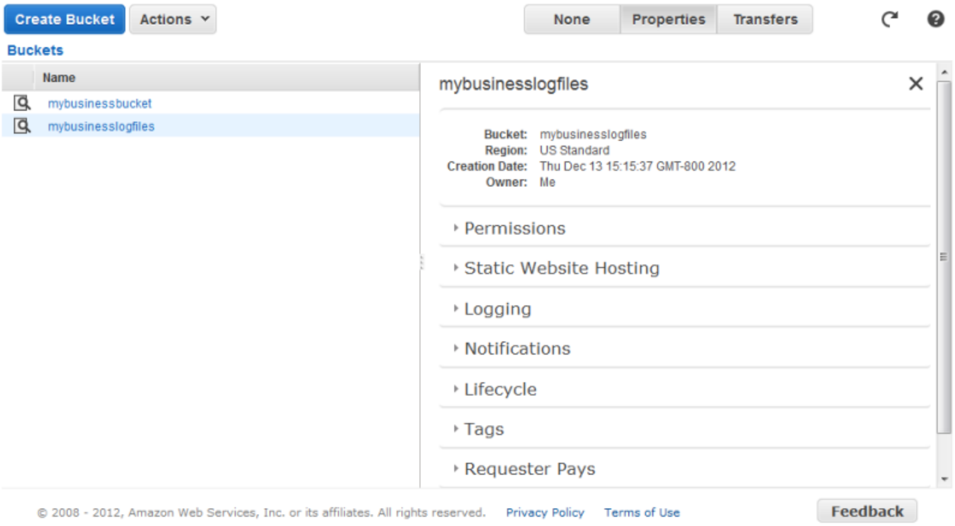
Enabled: ☑
Target Bucket: mybusinesslogfiles
Target Prefix: logs/

   a. Select the **Enabled** check box.
   b. In the **Target Bucket** box, select the bucket where you want the log files stored.
   c. (Optional In **Target Prefix** box, specify a prefix for the name of the log files.

      Amazon S3 adds the prefix to the log file names when storing them in your bucket. For example, if you specify the prefix "logs/," all logs stored in the target bucket are prefixed with `logs/`, so, all the logs will be stored in the `logs` folder.

7. Click **Create**.

   If Amazon S3 successfully creates your bucket, the console displays your empty bucket.



mybusinesslogfiles

Bucket: mybusinesslogfiles
Region: US Standard
Creation Date: Thu Dec 13 15:15:37 GMT-800 2012
Owner: Me

Browsing the Objects in Your Bucket

This section describes how to use the console to browse and display the objects and folders in your bucket.

To list the objects in a bucket

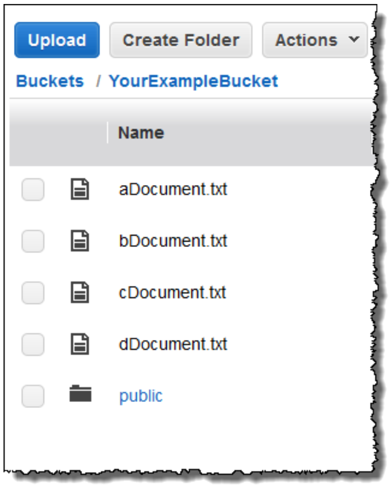
- Click the bucket whose objects you want to display.

  The Objects and Folders list displays the objects and folders in the selected bucket.

  > **Note**
  > If you have a large number of objects in a bucket, you can scroll down to the bottom of the Objects and Folders panel. When the scroll bar reaches the bottom of the list, the AWS Management Console automatically retrieves the next set of keys in your bucket, refreshes the view, and shows them in the console view.

When you click a bucket name, the console lists all the objects in the bucket in alphanumeric order. However, if your bucket contains large number of objects, scrolling down the long list to search for an object can be cumbersome. The jump feature enables you to type a string, and the console skips ahead to the specific object in the object list. If there are no objects whose key name match the specified string, console jumps to the next object in the list, in alphanumeric order.

For example, assume you have a bucket (ExampleBucket) with the following objects.



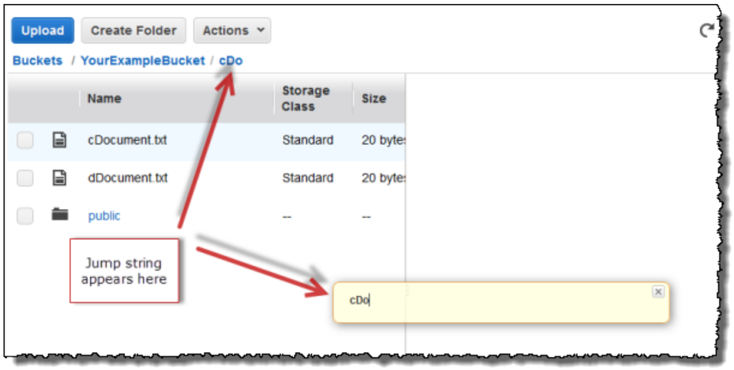
Name
aDocument.txt
bDocument.txt
cDocument.txt
dDocument.txt
public

To jump to an object in your list

1. Click the bucket name to display its objects.
2. Begin typing an object key name.

   As you begin typing characters, for example, a letter **c**, the console performs the following actions:

   - Opens a *jump* dialog box showing the character you typed
   - Skips ahead to the first object whose key name starts with the string you typed
   - Appends the jump string to the existing navigation breadcrumb



Name	Storage Class	Size
cDocument.txt	Standard	20 byte
dDocument.txt	Standard	20 byte
public	--	--

3. While the jump dialog box is visible, do one of the following:

   - **Press Enter –** This closes the jump dialog box. The jump results (such as the **cDo** shown in the preceding example screenshot) remain.
   - **Press ESC –** This cancels the jump operation and the *jump* dialog box closes.

Tip
To return to the top of the list, press the **Backspace** key.

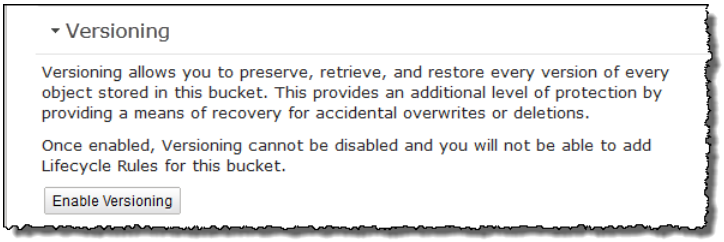
Enabling Bucket Versioning

This section describes how to enable versioning on a bucket. For more information about versioning support in Amazon S3, see Using Versioning in the *Amazon Simple Storage Service Developer Guide*. For more information about managing objects when versioning is enabled, see Managing Objects in a Versioning-Enabled Bucket (p. 48).

Note
You cannot set lifecycle configuration on a versioning-enabled bucket. For information about lifecycle management, go to Object Lifecycle Management in the *AWS Simple Storage Service Developer Guide*.

To enable versioning on a bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Buckets** list, click the details icon on the left of the bucket name and then click **Properties** to display bucket properties.
3. In the **Properties** pane, click **Versioning** and then click **Enable Versioning**.



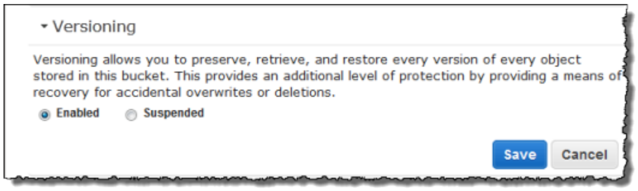
▾ Versioning

Versioning allows you to preserve, retrieve, and restore every version of every object stored in this bucket. This provides an additional level of protection by providing a means of recovery for accidental overwrites or deletions.

Once enabled, Versioning cannot be disabled and you will not be able to add Lifecycle Rules for this bucket.

4. The console displays a confirmation dialog. Click **OK** to enable versioning on the bucket.

   Amazon S3 enables versioning on the bucket. Accordingly, the console UI replaces the **Enable Versioning** button with the **Enabled** and **Suspended** radio buttons showing the versioning state.



▾ Versioning

Versioning allows you to preserve, retrieve, and restore every version of every object stored in this bucket. This provides an additional level of protection by providing a means of recovery for accidental overwrites or deletions.

● Enabled ○ Suspended

   After you enable versioning on a bucket, it can be only be in the enabled or suspended state; you cannot disable versioning on a bucket. If you suspend versioning, Amazon S3 suspends the creation of object versions for all operations, but preserve any existing object versions. For more information, see Working with Versioning-Suspended Buckets in the *Amazon Simple Storage Service Developer Guide*.

Managing Bucket Logging

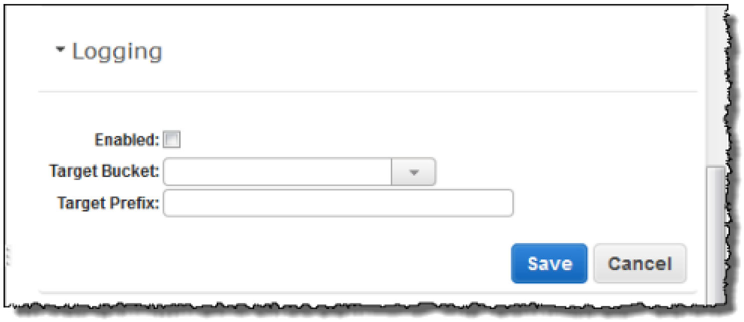
Logging provides a way to get detailed access logs delivered to a bucket you choose. An access log record contains details about the request, such as the request type, the resources specified in the request worked, and the time and date the request was processed. Server access logs are useful for many applications because they give bucket owners insight into the nature of requests made by clients not under their control. By default, Amazon S3 doesn't collect service access logs, but when you enable logging Amazon S3 delivers access logs to your bucket on an hourly basis.

This section describes how to use the console to enable and disable logging for a bucket. You can store logs in the same bucket you enable logging for, or you can store the logs in a different bucket. For more information about bucket logging, go to Accessing Server Logs.

> **Note**
> There is no extra charge for enabling server access logging on an Amazon S3 bucket. However, any log files the system delivers to you will accrue the usual charges for storage. (You can delete the log files at any time.) We do not assess data transfer charges for log file delivery, but we do charge the normal data transfer rate for accessing the log files.

To enable or disable logging on a bucket

1. Sign into the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3.
2. Select the bucket whose logging you want to enable or disable.
3. Click **Logging**.



4. Under **Logging**, elect the **Enabled** check box to enable logging, or clear the **Enabled** check box to disable logging.
5. (Optional) In the **Target Bucket** box, click a bucket to save your log files to, and in the **Target Prefix** box, enter a prefix to add to your log file names.

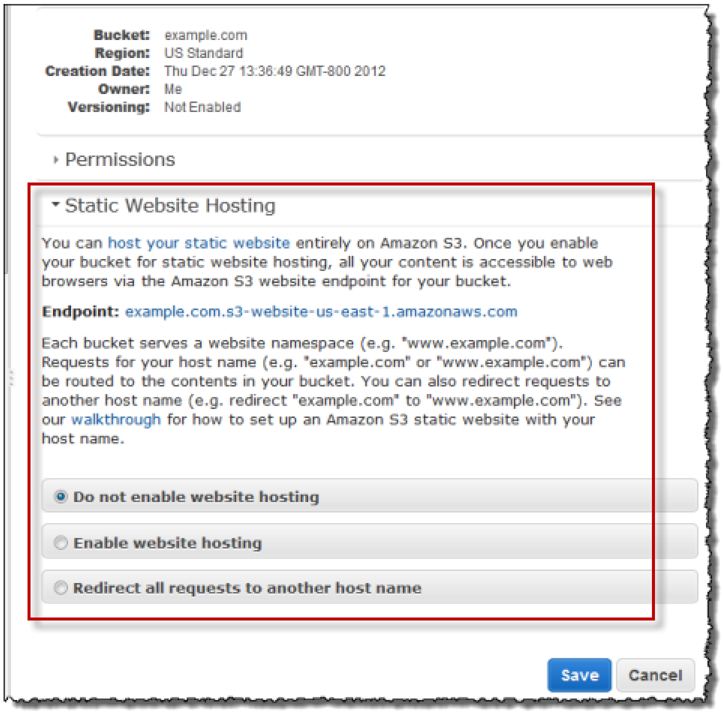
   Amazon S3 adds the prefix to the log file names when it uploads them to your bucket. For example, if you specify a prefix of "logs/," all logs stored in the target bucket are prefixed with `logs/`, so, all the logs will be stored in the `logs` folder.
6. Click **Save**.

Configuring a Bucket for Website Hosting

You can host static websites on Amazon S3. For conceptual information, go to Hosting Websites on Amazon S3 in the *Amazon Simple Storage Service Developer Guide*. This section explains how to use the Amazon S3 console to configure a bucket as a website.

To manage a bucket's website configuration

1. Sign into the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3.
2. In the Buckets pane, click the bucket that you want to configure.
3. In the result pane, click **Static Website Hosting**.



Bucket: example.com
Region: US Standard
Creation Date: Thu Dec 27 13:36:49 GMT-800 2012
Owner: Me
Versioning: Not Enabled

You can host your static website entirely on Amazon S3. Once you enable your bucket for static website hosting, all your content is accessible to web browsers via the Amazon S3 website endpoint for your bucket.

Endpoint: example.com.s3-website-us-east-1.amazonaws.com

Each bucket serves a website namespace (e.g. "www.example.com"). Requests for your host name (e.g. "example.com" or "www.example.com") can be routed to the contents in your bucket. You can also redirect requests to another host name (e.g. redirect "example.com" to "www.example.com"). See our walkthrough for how to set up an Amazon S3 static website with your host name.

● Do not enable website hosting

○ Enable website hosting

○ Redirect all requests to another host name

4. Do one of the following:

   - To configure a bucket for website hosting, click **Enable website hosting**. In the **Index Document** box, type the name of the index document. Optionally, in the **Error Document** box, you can also provide the name of a custom error document and specify custom rules to redirect requests. For more information, go to Configure Bucket for Website Hosting in the *Amazon Simple Storage Service Developer Guide*.
   - To redirect all requests to a different web page, click **Redirect all requests to another host name**. In the **Redirect all requests to**box, type the name of the location where you want requests to be redirected, for example, example.com or http://example.com. If you don't specify the protocol (http, https), the protocol of the original request is used. If you redirect all requests, then any request made to the bucket's website endpoint will be redirected to the specified host name.

5. When the settings are as you want them, click **Save**.

Note

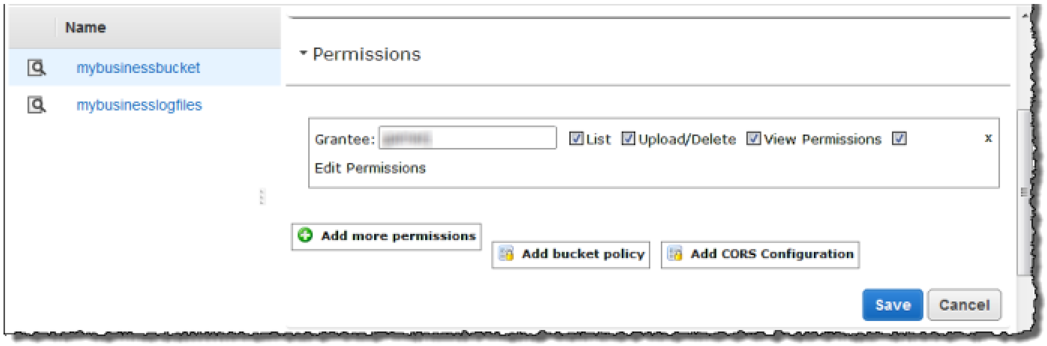
If you click **Do not enable website hosting**, Amazon S3 removes any existing website configuration from the bucket, and the bucket is not accessible from the website endpoint. However, the bucket is still available at the REST endpoint.

Editing Bucket Permissions

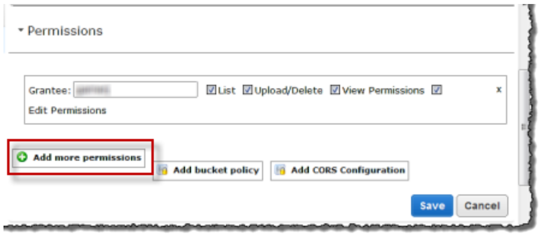
Bucket permissions specify who is allowed access to the objects in a bucket and what permissions you have granted them. For example, one person might have only read permission while another might have read and write permissions.

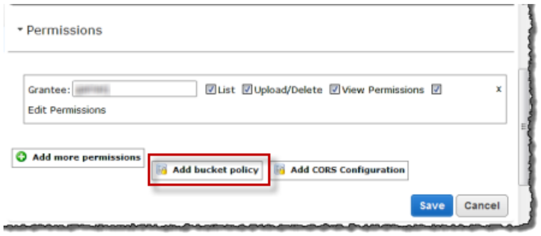
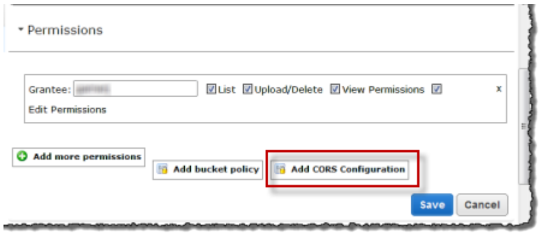
To edit bucket permissions

1. Sign into the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3.
2. In the Buckets list, click the bucket whose properties you want to view.



3. Click **Permissions**, and then do any of the following:

To...	Do this...
Change an existing permission	Beside the grantee whose permissions you want to change, select the check box for a permission to grant it, or clear the box to deny it.
Add permissions for a person or group	a. Click **Add more permissions**. b. In **Grantee** box of the new line that appears, add the name of the person or group for which you want to set permissions. The name can be the email address associated with an AWS account, a canonical ID, or a group name. You can add as many as 100 grantees. c. Select the check boxes next to the permissions you want to grant. 
Remove a person or group from the permission list	Click the "x" on the line of the grantee you want to remove.

To...	Do this...
Add a bucket policy	a. Click **Add bucket policy**. The **Bucket Policy Editor** appears. b. Paste your bucket policy into the box provided. For help in generating a policy, you can use the AWS Policy Generator. For examples of Amazon S3 bucket policies, see Example Cases for Amazon S3 Bucket Policies in the Amazon Simple Storage Service *Developer Guide*. c. Click **Save**.  Permissions Grantee: ☑List ☑Upload/Delete ☑View Permissions ☑ x Edit Permissions Add more permissions Add bucket policy Add CORS Configuration Save Cancel
Add a Cross-Origin Resource Sharing (CORS) configuration	a. Click **Add CORS Configuration**. In the **CORS Configuration Editor**, paste your CORS configuration into the field provided, and then click **Save**. For information about CORS configuration, see Enabling Cross-Origin Resource Sharing in the *Amazon Simple Storage Service Developer Guide*.  Permissions Grantee: ☑List ☑Upload/Delete ☑View Permissions ☑ x Edit Permissions Add more permissions Add bucket policy Add CORS Configuration Save Cancel

There are built-in groups that you can choose from the **Grantee** drop-down list box:

- **Authenticated Users –** This group consists of any user that has an Amazon AWS Account.
- **Everyone –** This group grants anonymous access to your bucket.

You can grant access to an account by using the e-mail address that the user entered when signing up for an AWS account. You can grant an account any of the following permissions:

- **List –** Allows the grantee to view a list of the objects in the bucket.
- **Upload/Delete –** Allows the grantee to access the object when they logged in.
- **View Permissions –** Allows the grantee to view the permissions associated with the object.
- **Edit Permissions –** Allows the grantee to edit the permissions associated with the object.

Caution
We highly recommend against granting the Everyone group **Upload/Delete** permission. Doing so will allow anyone to store objects in your bucket, for which you will be billed, and allows others to delete objects that you may want to keep.

4. Click **Save**.

Enabling RRS Lost Object Notifications

You can enable event notifications, which are sent to an Amazon Simple Notification Service (SNS) topic. Currently Amazon S3 sends a notification only when Amazon S3 detects that a Reduced Redundancy Storage (RRS) object has been lost.

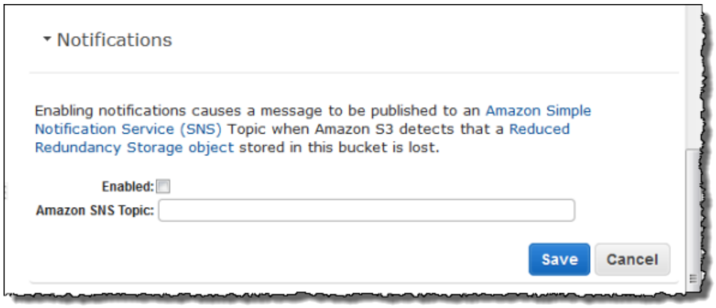
This section explains how to use the Amazon S3 console to enable notifications. For information on using the Amazon S3 API to enable bucket notifications, see Setting Up Notification of Bucket Events.

Enabling bucket notifications requires an existing Amazon SNS topic where notifications can be published. For information on creating an Amazon SNS topic, go to Create a Topic in the Amazon Simple Notification Service *Getting Started Guide*.

A message is published to this Amazon SNS topic and the topic subscribers are notified. To create an Amazon SNS topic using the API, see the Amazon SNS Reference Guide, Create Topic.

To enable or disable bucket notifications

1. Sign into the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3.
2. In the Buckets pane, click the bucket whose properties you want to view.
3. Click **Notifications**.



▾ Notifications

Enabling notifications causes a message to be published to an Amazon Simple Notification Service (SNS) Topic when Amazon S3 detects that a Reduced Redundancy Storage object stored in this bucket is lost.

Enabled: □
Amazon SNS Topic:

4. Select the **Enabled** check box to enable notifications, or clear the **Enabled** check box to disable notifications.
5. In **Amazon SNS Topic** box, type the name of the Amazon SNS topic that will receive notifications from Amazon S3. To learn more about the Amazon SNS topic format, go to http://aws.amazon.com/sns/faqs/#10.
6. Click **Save**. Amazon S3 will send a test message to all subscribers.

Deleting a Bucket

You can only delete an empty bucket. If there are objects in the bucket, you must delete them before you delete the bucket. For information about deleting objects, see Deleting an Object (p. 44) .

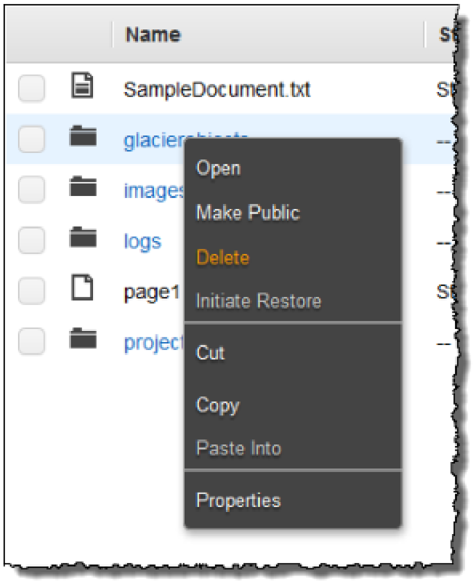
This section explains how to use the console to delete an Amazon S3 bucket.

Note

When you delete a bucket, there may be a delay (of up to one hour) before the bucket name is available for reuse in a new region or by a new bucket owner. If you re-create the bucket in the same region or with the same bucket owner, there is no delay.

To delete a bucket

1. Sign into the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3.
2. Right-click the bucket that you want to delete and then click **Delete**.



3. When a confirmation message appears, click **OK**.

Managing Lifecycle Configuration

This section explains how to manage lifecycle configuration rules for a bucket: adding, viewing, deleting, and disabling rules. Each rule identifies objects and actions that you want Amazon S3 to perform when the objects reach a specific date or a time interval since their creation. For more information about lifecycle configuration, go to Object Lifecycle Management in the *Amazon S3 Developer Guide*.

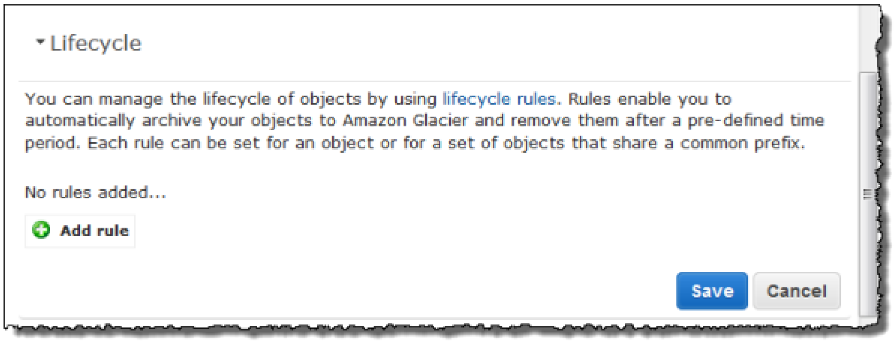
Caution

You can use lifecycle configuration rules to archive or delete objects after a specified period of time or on a specified date. A transition action archives an object, and an expiration action deletes the object. Archived objects are not directly accessible unless you restore a temporary copy. Additionally, you cannot use a lifecycle configuration rule to change the storage class of the archived object from Glacier to Standard or RRS. For more information about archiving objects or scheduling object deletion, see Before You Decide to Archive Objects and Before You Decide to Expire Objects in the *Amazon S3 Developer Guide*.

To add a lifecycle configuration rule

1. Sign into the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3.

2. In the Buckets list, click the bucket whose lifecycle configuration you want to configure, and then click **Lifecycle**.

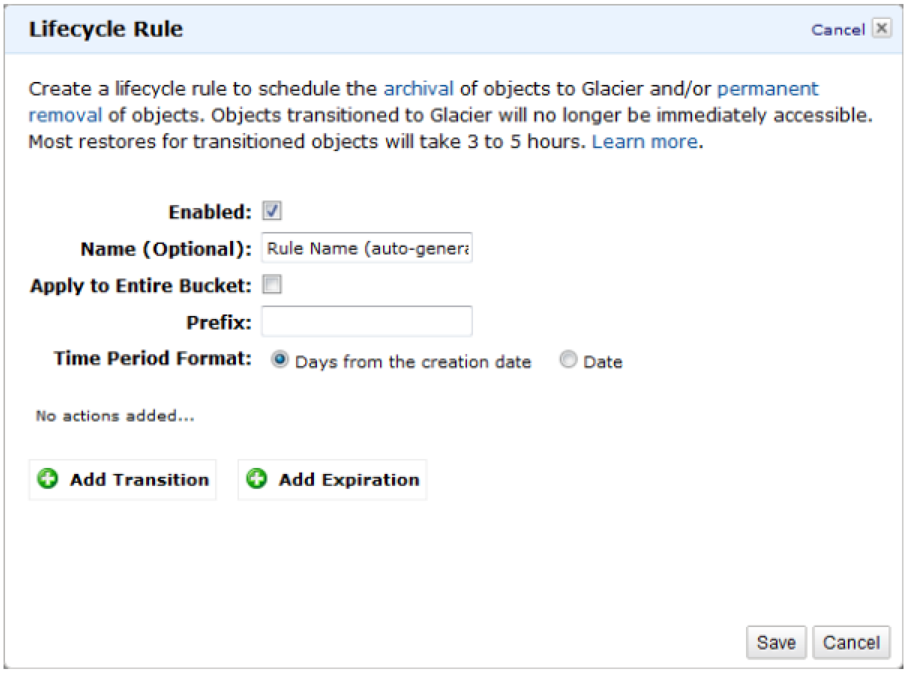


▾ Lifecycle

You can manage the lifecycle of objects by using lifecycle rules. Rules enable you to automatically archive your objects to Amazon Glacier and remove them after a pre-defined time period. Each rule can be set for an object or for a set of objects that share a common prefix.

No rules added...

3. Click **Add rule**.



Lifecycle Rule

Create a lifecycle rule to schedule the archival of objects to Glacier and/or permanent removal of objects. Objects transitioned to Glacier will no longer be immediately accessible. Most restores for transitioned objects will take 3 to 5 hours. Learn more.

Enabled: ☑
Name (Optional): Rule Name (auto-genera
Apply to Entire Bucket: □
Prefix:
Time Period Format: ● Days from the creation date ○ Date

No actions added...

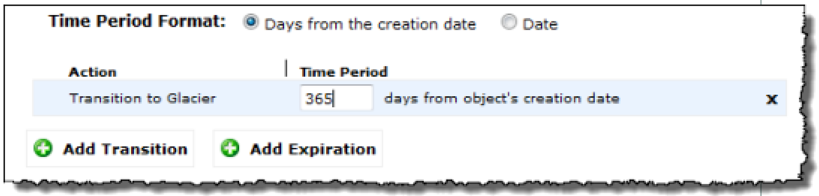
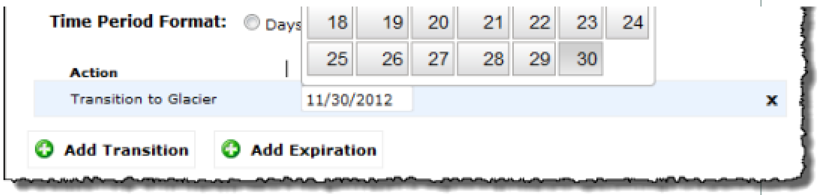
4. In the **Lifecycle Rule** dialog box, specify the following attributes:

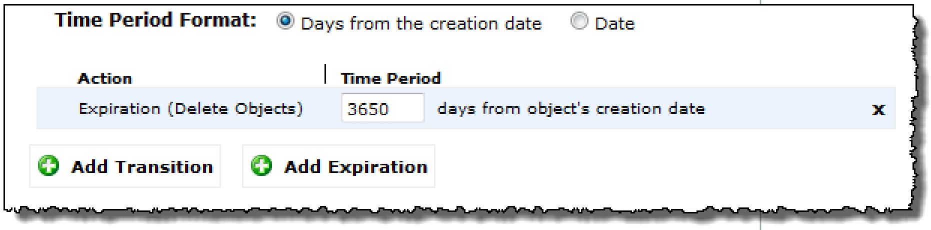
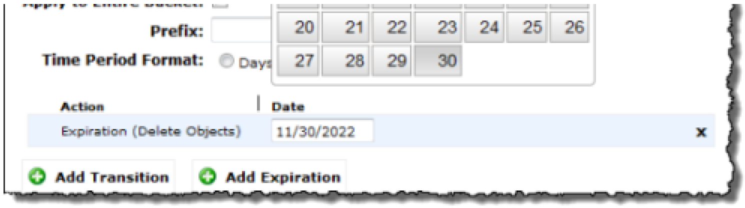
   - **Enabled –** If selected, indicates that the rule is enabled. If cleared, Amazon S3 will not apply the rule to associated objects.
   - **Name –** (Optional) Identifies the rule. The name must be unique within the bucket. By default, Amazon S3 will generate a unique identifier for the rule.
   - **Apply to Entire Bucket –** If selected, the rule applies to all objects in the bucket, and the **Prefix** attribute is ignored.
   - **Prefix –** Specifies the subset of objects to which the rule applies. For example, "logs/" would apply to all objects in the "logs" folder. For information about how to specify a prefix value, and the upper and lower bounds of expiration time, go to Object Expiration in the *Amazon S3 Developer Guide*.
   - **Time Period Format –** Specifies whether the rule will be applied a specified number of days from the date the object was created or on a specified date.

   - Add a transition and/or expiration action.

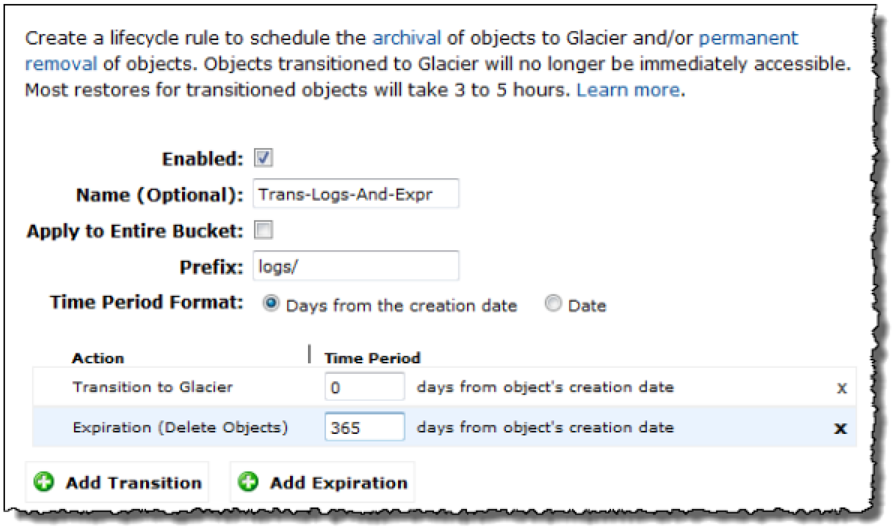
Note

A rule can have one transition action and/or one expiration action. You cannot create a rule with more than one of either action.

To...	Do this...
Add a transition rule	Click **Add Transition** and then do one of the following: a. If you specified **Days from creation date** as the **Time Period Format** for the rule, under **Time Period** type the number of days after the object's creation date when it will be archived .  Time Period Format: ● Days from the creation date ○ Date Action | Time Period Transition to Glacier 365 days from object's creation date x b. If you specified **Date** as the time period format for the rule, under **Time Period**, type the **Date** that the object will be archived using the format "mm/dd/yyyy", or click the date on the calendar that appears.  Time Period Format: ○ Days Action Transition to Glacier 11/30/2012 x 18 19 20 21 22 23 24 25 26 27 28 29 30 Add Transition Add Expiration

To...	Do this...
Add an expiration rule	Click **Add Expiration** and then do one of the following: a. If you specified **Days from creation date** as the time period format for the rule, under **Time Period** type the number of days after the object's creation date when it will be archived.  Time Period Format: ● Days from the creation date ○ Date Action | Time Period Expiration (Delete Objects) | 3650 days from object's creation date x b. If you specified **Date** as the time period format for the rule, type the **Date** that the object will be archived using the format "mm/dd/yyyy", or click the date on the calendar that appears..  Prefix: Time Period Format: ○ Days Action | Date Expiration (Delete Objects) | 11/30/2022 x 20 21 22 23 24 25 26 27 28 29 30 Add Transition Add Expiration

The following example shows a rule that immediately transitions objects with the prefix "logs/" to the Glacier storage class and then expires the objects after 365 days.



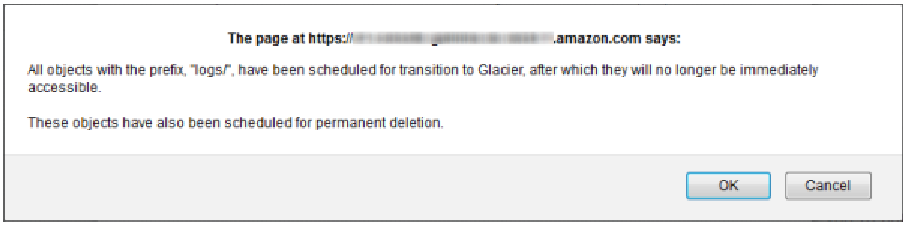
Create a lifecycle rule to schedule the archival of objects to Glacier and/or permanent removal of objects. Objects transitioned to Glacier will no longer be immediately accessible. Most restores for transitioned objects will take 3 to 5 hours. Learn more.

Enabled: ☑
Name (Optional): Trans-Logs-And-Expr
Apply to Entire Bucket: □
Prefix: logs/
Time Period Format: ● Days from the creation date ○ Date

Action	Time Period	
Transition to Glacier	0 days from object's creation date	x
Expiration (Delete Objects)	365 days from object's creation date	x

5. When all of the settings are as you want them, click **Save**.

   When a confirmation dialog appears, click **OK**.

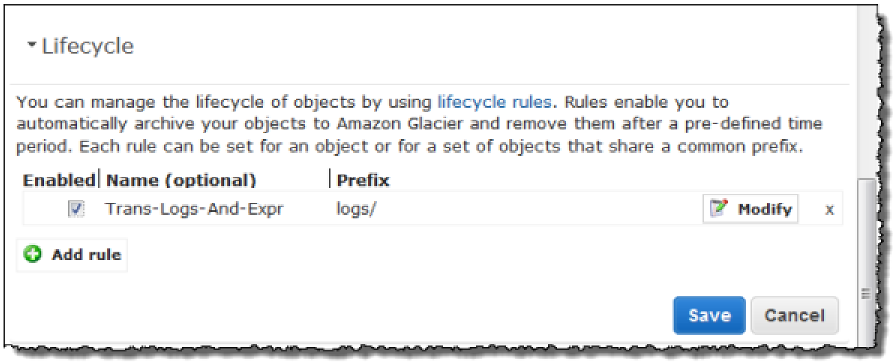


The page at https://[redacted].amazon.com says:

All objects with the prefix, "logs/", have been scheduled for transition to Glacier, after which they will no longer be immediately accessible.

These objects have also been scheduled for permanent deletion.

If the rule does not contain any errors, it is displayed in the **Lifecycle** pane.



▾ Lifecycle

You can manage the lifecycle of objects by using lifecycle rules. Rules enable you to automatically archive your objects to Amazon Glacier and remove them after a pre-defined time period. Each rule can be set for an object or for a set of objects that share a common prefix.

Enabled	Name (optional)	Prefix		
☑	Trans-Logs-And-Expr	logs/	Modify	x

Note

If there is an issue with a rule, an error message is displayed with information about the issue. For example, if the bucket is versioning-enabled or an expiration date is not specified when you create a rule, an error message is displayed. Similarly, if you have multiple rules, Amazon S3 determines if the rule being added will conflict with an existing rule. In that case, the rule cannot be saved.

In some cases, Amazon S3 will display an informational message. For example, if you do not specify a prefix, then an informational message indicates that for a blank prefix, the expiration policy applies to all objects in the bucket. In that case, the rule can be saved.

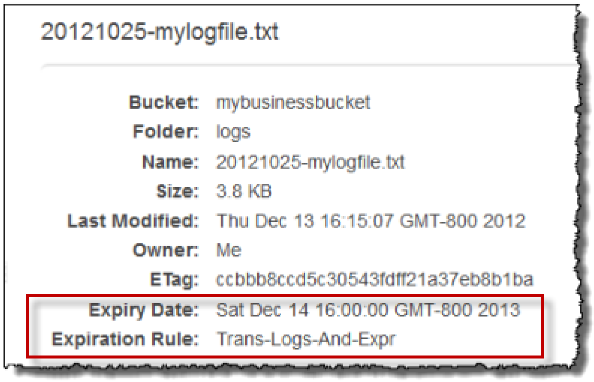
Rules that apply to an object are displayed with the object properties.

To view an object's expiration rule

- In the Object and Folders list, click the object whose properties you want to view.

  Among the object properties, the **Expiry Date** and **Lifecycle Rule** indicate which object expiration rule applies to the object. If no object expiration rule applies to the object, the **Expiry Date** field displays **None**, and the **Lifecycle Rule** field displays **N/A**. .

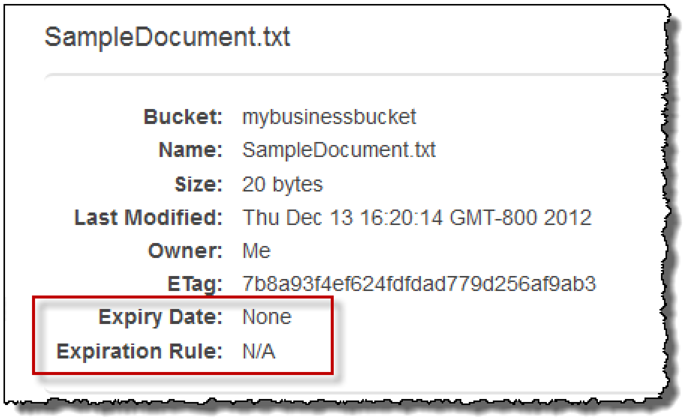
  The following example shows the properties for an object in which an expiration rule named "Trans-Logs-And-Expr" applies to the object.



20121025-mylogfile.txt

Bucket: mybusinessbucket
Folder: logs
Name: 20121025-mylogfile.txt
Size: 3.8 KB
Last Modified: Thu Dec 13 16:15:07 GMT-800 2012
Owner: Me
ETag: ccbbb8ccd5c30543fdff21a37eb8b1ba
Expiry Date: Sat Dec 14 16:00:00 GMT-800 2013
Expiration Rule: Trans-Logs-And-Expr

The following examples shows the properties for an object in which no expiration rule applies to the object.

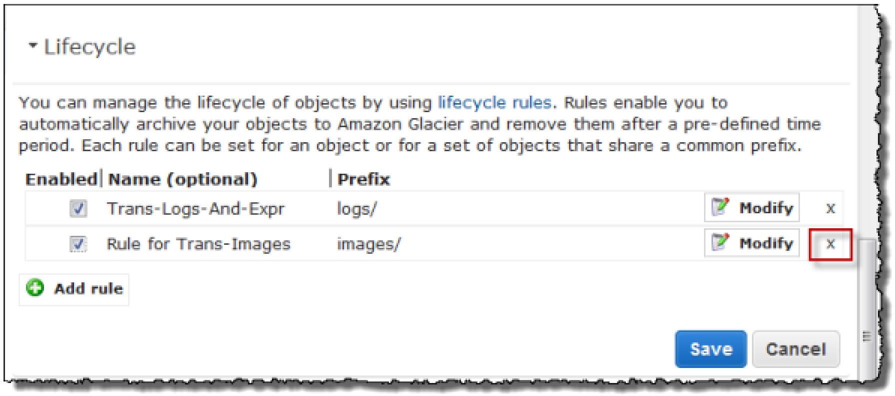


SampleDocument.txt

Bucket: mybusinessbucket
Name: SampleDocument.txt
Size: 20 bytes
Last Modified: Thu Dec 13 16:20:14 GMT-800 2012
Owner: Me
ETag: 7b8a93f4ef624fdfdad779d256af9ab3
Expiry Date: None
Expiration Rule: N/A

To delete a lifecycle configuration rule

1. In the Buckets list, click the name of the bucket that contains the rule, and then click **Lifecycle**.
2. 1. Click the **x** at the end of the row that describes the rule that you want to delete..



▾ Lifecycle

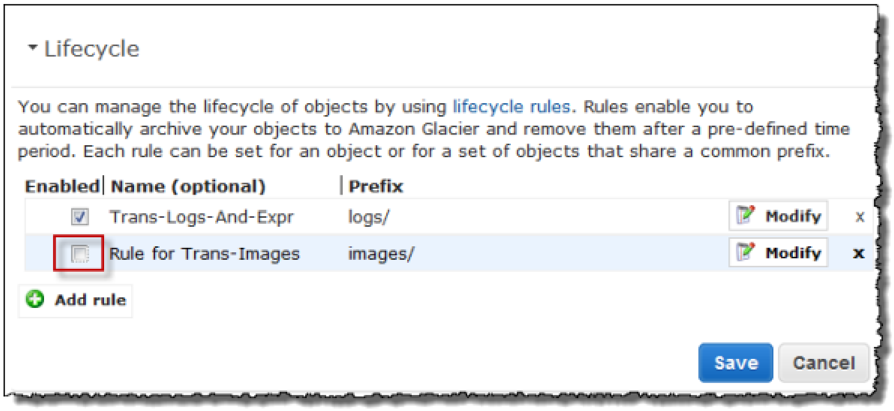
You can manage the lifecycle of objects by using lifecycle rules. Rules enable you to automatically archive your objects to Amazon Glacier and remove them after a pre-defined time period. Each rule can be set for an object or for a set of objects that share a common prefix.

Enabled	Name (optional)	Prefix		
☑	Trans-Logs-And-Expr	logs/	Modify	x
☑	Rule for Trans-Images	images/	Modify	x

3. Click **Save**.

To disable a lifecycle configuration rule

1. In the Buckets list, click the name of the bucket that contains the rule, and then click **Lifecycle**.
2. Clear the **Enabled** check box for the rule.



Lifecycle

You can manage the lifecycle of objects by using lifecycle rules. Rules enable you to automatically archive your objects to Amazon Glacier and remove them after a pre-defined time period. Each rule can be set for an object or for a set of objects that share a common prefix.

Enabled	Name (optional)	Prefix
☑	Trans-Logs-And-Expr	logs/
□	Rule for Trans-Images	images/

3. Click **Save**.

   The rule is not deleted; you can enable it again later if you want.

Managing Cost Allocation Tagging

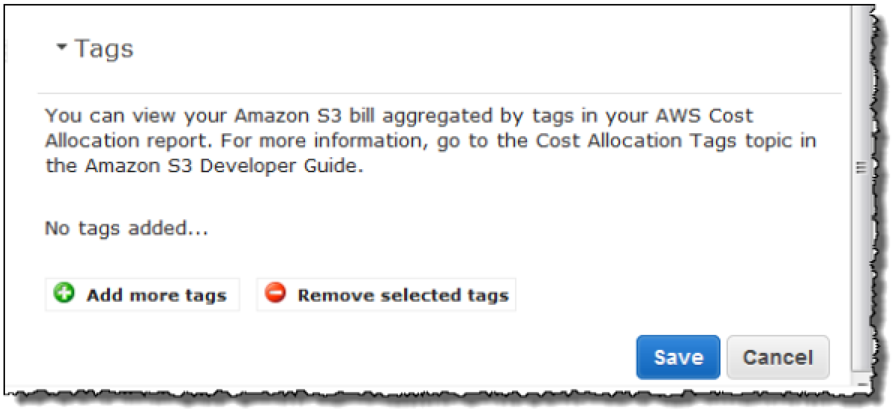
With AWS cost allocation, you can use tags to annotate billing for your use of a bucket. A tag is a key-value pair that represents a label that you assign to a bucket. In your AWS bill, costs are organized by tags that you define.

As a billing resource, a bucket can have as many as 10 tags. In the following example, we'll create a tag that associates the bucket with a particular project. For information about cost allocation tagging, go to Cost Allocation in the *Amazon S3 Developer Guide*.

This section explains how to add and remove cost allocation tags for a bucket.

To add a cost allocation tag

1. Sign into the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3.
2. In the Buckets list, click the bucket name, and then click **Tags**.

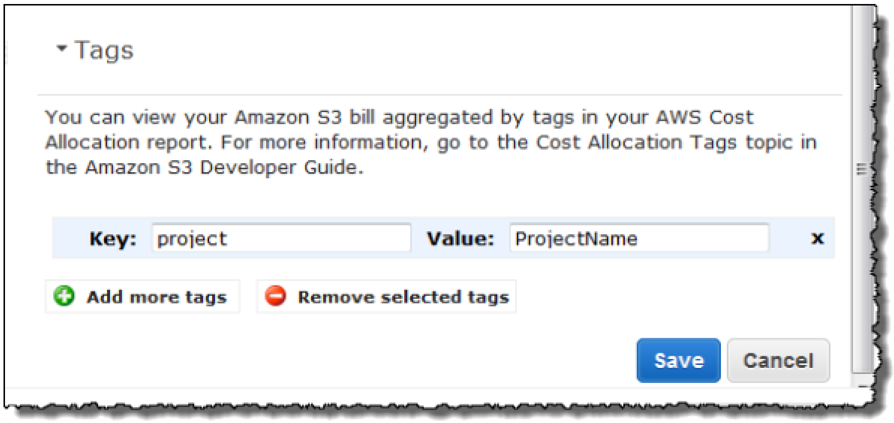


Tags

You can view your Amazon S3 bill aggregated by tags in your AWS Cost Allocation report. For more information, go to the Cost Allocation Tags topic in the Amazon S3 Developer Guide.

No tags added...

3. Click **Add more tags**.
4. In the **Key** and **Value** boxes, type a key name and a value.



You can view your Amazon S3 bill aggregated by tags in your AWS Cost Allocation report. For more information, go to the Cost Allocation Tags topic in the Amazon S3 Developer Guide.

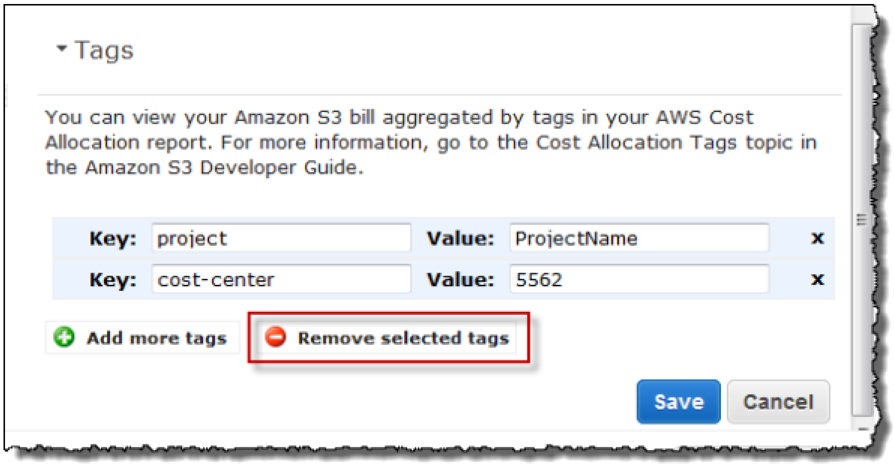
Key: project Value: ProjectName x

5. Click **Save**.

   If there is an issue with a tag, an error message is displayed with information about the issue. For example, if the key-value pair is already in use or a key is missing its associated value, an error message is displayed, and the tag will not be saved.

To delete a cost allocation tag

1. In the Buckets list, click the bucket name, and then click **Tags**.
2. Select one or more tags to delete and click **Remove selected tags**. To select multiple tags, select one tag, and then either press the Shift key and drag to select multiple tags or hold down the Ctrl key while you click additional tags. The following example shows two tags selected.



You can view your Amazon S3 bill aggregated by tags in your AWS Cost Allocation report. For more information, go to the Cost Allocation Tags topic in the Amazon S3 Developer Guide.

Key: project Value: ProjectName x

Key: cost-center Value: 5562 x

   You can also click the **x** to the right of a tag's Value field to delete just that tag.
3. Click **Save**.

Working with Objects

Topics

Objects are the data that you store in Amazon S3. Every object resides within a bucket. Before you can upload an object into Amazon S3, you must have write permissions to a bucket.

Objects can be any file type: images_backup, data, movies, etc. An object can be as large as 5 TB. You can have an unlimited number of objects in a bucket.

This section explains how to use the console to create, manage, and delete objects.

Uploading Objects into Amazon S3

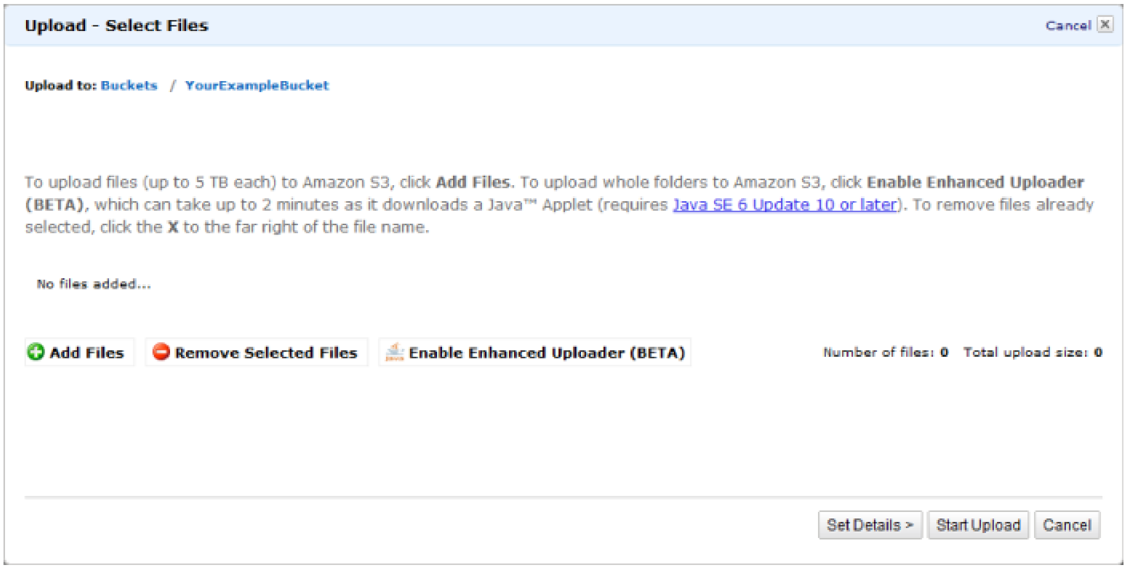
When you upload a folder, Amazon S3 uploads all the files and subfolders from the specified folder to your bucket. It then assigns a key value that is a combination of the uploaded file name and the folder name. For example, if you upload a folder `/images` containing two files, `sample1.jpg` and `sample2.jpg`, Amazon S3 uploads the files and then assigns the corresponding object key names `images/sample1.jpg`, and `images/sample2.jpg`. Note that the key names include the folder name as a prefix.

If you upload one or more files that are not in a folder, Amazon S3 uploads the files and assigns the file names as the key values for the objects created.

This section explains how to use the AWS Management Console to upload one or more files or entire folders into Amazon S3. Amazon S3 stores all files in the specified bucket.

To upload files and folders into Amazon S3

1. Sign into the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3.
2. In the buckets list, click the name of bucket where you want to upload an object and then click **Upload**.



Upload - Select Files

Upload to: Buckets / YourExampleBucket

To upload files (up to 5 TB each) to Amazon S3, click **Add Files**. To upload whole folders to Amazon S3, click **Enable Enhanced Uploader (BETA)**, which can take up to 2 minutes as it downloads a Java™ Applet (requires Java SE 6 Update 10 or later). To remove files already selected, click the **X** to the far right of the file name.

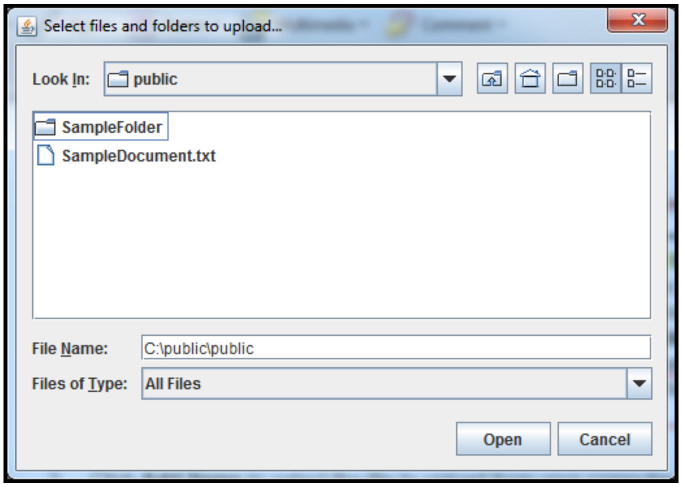
No files added...

Number of files: 0 Total upload size: 0

3. (Optional) In the **Upload - Select Files** wizard, if you want to upload an entire folder, click **Enable Enhanced Uploader** to install the necessary Java applet. You only need to do this step once per console session.

   Note
   If you are behind a firewall, you will need to install your organization's supported proxy client for the Java applet to work.

4. Click **Add Files**.



Select files and folders to upload...

Look In: public

SampleFolder
SampleDocument.txt

File Name: C:\public\public

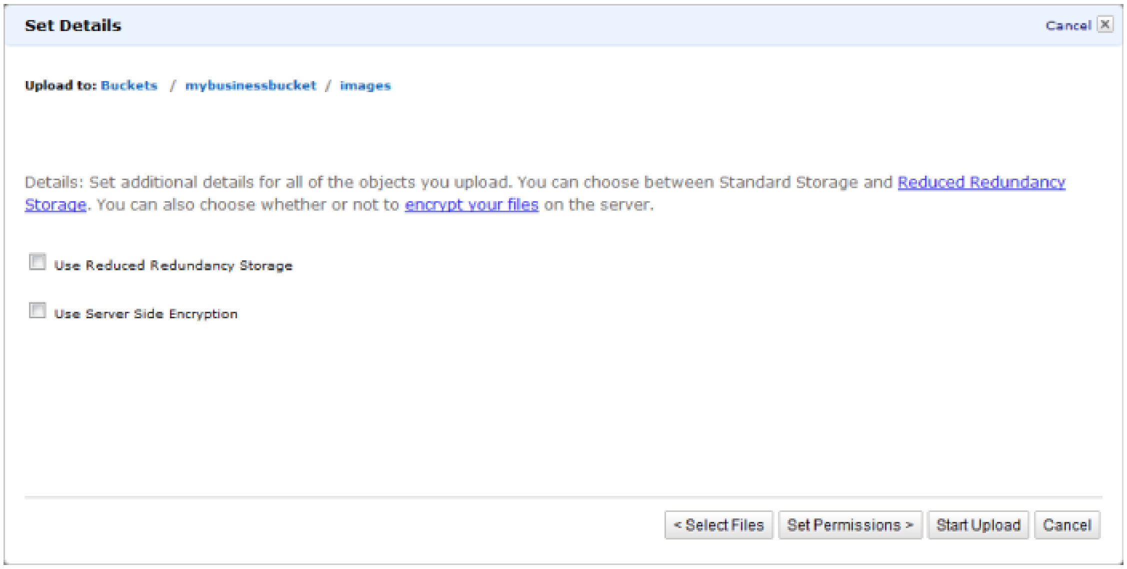
Files of Type: All Files

5. In the dialog box that appears, click the file or files that you want to upload, and then click **Open**.

   - If you enabled the advanced uploader in step 2, you see a Java dialog box titled **Select files and folders to upload**, as shown.
   - If not, you see the **File Upload** dialog box associated with your operating system.

6. Choose one of the following options:

To...	Do this...
Upload objects immediately	Click **Start Upload**. You can skip the rest of this procedure.
Use Reduced Redundancy Storage or Server-Side Encryption	Click **Set Details**, and then select the appropriate check box or boxes.
Set permissions on the objects	Click **Set Details**, click **Set Permissions**, and then continue.
Set metadata for your objects	Click **Set Details**, click **Set Permissions** and then continue.



Set Details

Upload to: Buckets / mybusinessbucket / images

Details: Set additional details for all of the objects you upload. You can choose between Standard Storage and Reduced Redundancy Storage. You can also choose whether or not to encrypt your files on the server.

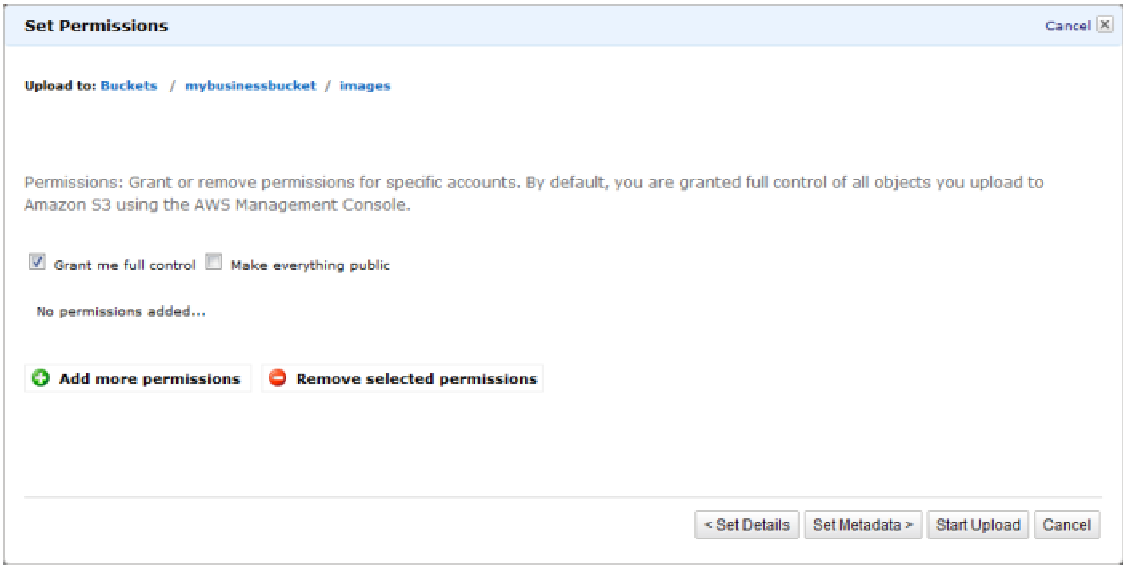
□ Use Reduced Redundancy Storage

□ Use Server Side Encryption

7. In the **Set Permissions** dialog box, do the following:

- Select (the default) or clear the **Grant me full control** check box.
- To grant read access to anonymous requests, select the **Make everything public** check box on the **Upload - Set Permissions** panel. By default, the check box is cleared, so no access is granted.

Note
By default, the owner of the upload has full control over all uploaded objects.



Set Permissions

Upload to: Buckets / mybusinessbucket / images

Permissions: Grant or remove permissions for specific accounts. By default, you are granted full control of all objects you upload to Amazon S3 using the AWS Management Console.

☑ Grant me full control □ Make everything public

No permissions added...

8. To grant access to other users and groups for the objects you are uploading, click **Add more permissions**.

   In the grantee row that appears:

   - For each permission you grant, an entry is made in the object's Access Control List (ACL). For more information, go to Using ACLs in the *Amazon Simple Storage Service Developer Guide*.
   - If you click **Add more permissions**, a new **Grantee** row appears. Each **Grantee** row maps to a grant in the Access Control List (For more information, go to Using ACLs) associated with the object. You can grant permission to a user or one of the predefined Amazon S3 groups.

9. There are two built-in groups that you can choose from the **Grantee** drop-down list box:

   - **Authenticated Users—**This group consists of any user that has an Amazon AWS Account. When you grant the Authenticated User group permission, any valid signed request can perform the appropriate action. The request can be signed by either an AWS Account or IAM User.
   - **Everyone—**This group grants anonymous access to your object

   You can grant permission to an AWS account by entering the accounts canonical user ID or email address in the **Grantee** field. The email address must be the same one they used when signing up for an AWS account. You can grant a grantee any of the following permissions:

   - **Open/Download—**Enables the account to access the object when they are logged in
   - **View Permissions—**Can view the permissions associated with the object
   - **Edit Permissions—**Can edit the permissions associated with the object

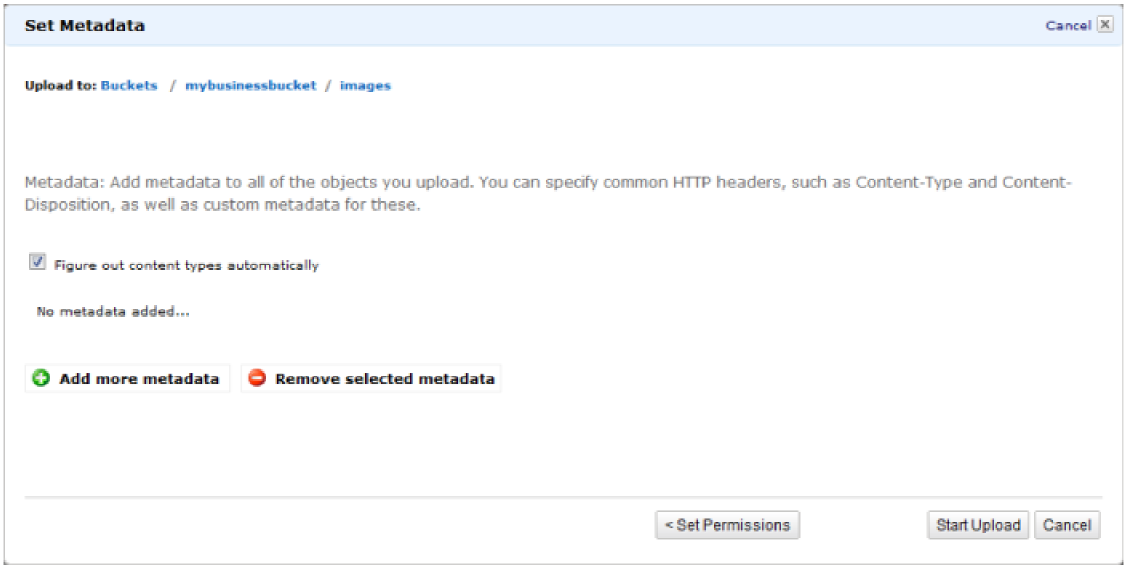
10. To set metadata, click **Set Metadata**.

    In the **Upload - Set Metadata** do the following:

    a. If you want the Amazon S3 to infer the content type of the uploaded objects, select the **Figure out content types automatically** check box (default).

    b. To add custom metadata, click **Add more metadata** and enter the key/value pairs that you want.

Amazon S3 object metadata is represented by a key/value pair. User metadata is stored with the object and returned when you download the object. Amazon S3 does not process custom metadata. Custom metadata can be as large as 2 KB, and both the keys and their values must conform to US-ASCII standards. Any metadata starting with prefix `x-amz-meta-` is treated as user-defined metadata. When you add user-defined metadata, select `x-amz-meta-` from the **Key** box and then append the metadata name to it.



Set Metadata

Upload to: Buckets / mybusinessbucket / images

Metadata: Add metadata to all of the objects you upload. You can specify common HTTP headers, such as Content-Type and Content-Disposition, as well as custom metadata for these.

☑ Figure out content types automatically

No metadata added...

11. Click **Start Upload**.

    You can watch the progress of the upload from within the **Transfers** panel.

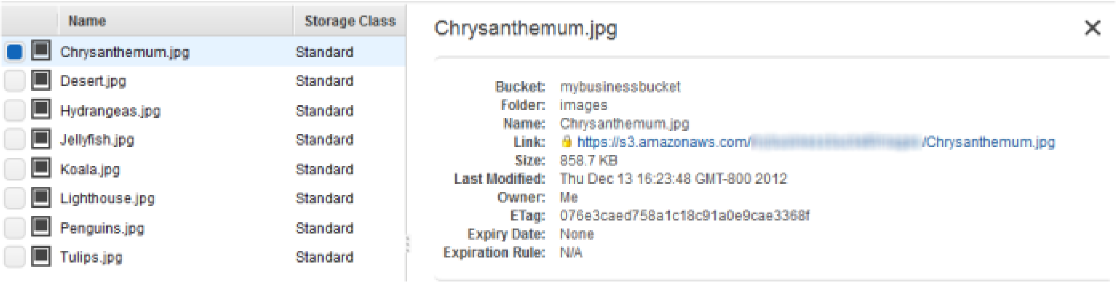
    > **Tip**
    > To hide the **Transfer** panel, click the **None** button. To open it again, click the **Transfers** button.

    When objects upload successfully to Amazon S3, they appear in the Objects and Folders list.

To view file content and properties

- Do either or both of the following:

  - To view the file content, in the Objects and Folders list, double-click the object name.
  - To view object properties, in the Objects and Folders list, click the object.



Name	Storage Class
Chrysanthemum.jpg	Standard
Desert.jpg	Standard
Hydrangeas.jpg	Standard
Jellyfish.jpg	Standard
Koala.jpg	Standard
Lighthouse.jpg	Standard
Penguins.jpg	Standard
Tulips.jpg	Standard

Chrysanthemum.jpg

Bucket:	mybusinessbucket
Folder:	images
Name:	Chrysanthemum.jpg
Link:	https://s3.amazonaws.com/[redacted]/Chrysanthemum.jpg
Size:	858.7 KB
Last Modified:	Thu Dec 13 16:23:48 GMT-800 2012
Owner:	Me
ETag:	076e3caed758a1c18c91a0e9cae3368f
Expiry Date:	None
Expiration Rule:	N/A

Editing Object Properties

Topics

The properties of an object include the object details, permissions, and metadata that you set when you uploaded the object. You can edit these properties at any time.

This section explains the properties of an object that you can change and includes the object's details, permissions, and metadata.

To access the properties of an object

1. In the Objects and Folders list, click the object.
2. Do any or all of the following:

   a. To edit the object details, click **Details**, and then edit the details as explained in Editing Object Details

   b. To edit object permissions, click **Permissions**, and then edit the permissions as explained in Editing Object Permissions.

   c. To edit object metadata, click **Metadata**, and then edit the permissions as explained in Editing Object Metadata.

   When you select a single object in a bucket you can change all of its properties. When you select multiple objects, you can change only the object details.

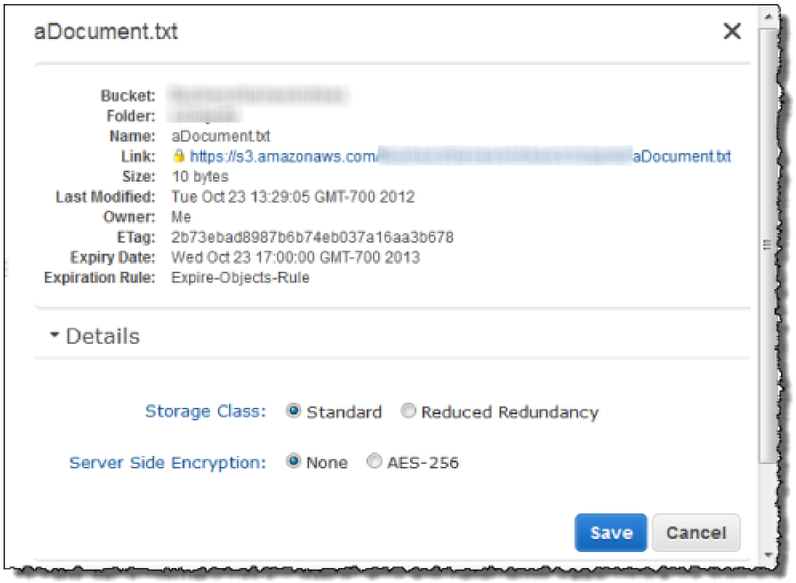
Editing Object Details

This section explains how to use the console to edit the details of one or more selected objects. The property details of an object that you see and can change depends on the storage class of the object:

- **Standard and Reduced Redundancy Storage (RSS) Class**— When an object is in the Standard or RSS storage class, the properties of an object you can see and change include the object's storage redundancy and the state of server-side encryption. In general, you use Amazon S3 RRS to reduce costs by storing non-critical, reproducible data at lower levels of redundancy than Amazon S3's standard storage. For more information, see Using Reduced Redundancy Storage. You can use server-side encryption to encrypt objects at rest. For more information, see Using Encryption.
- **Glacier Storage Class**—When an object is in the Glacier storage class, the properties of the object are view-only if the object has not been restored. When the object is restored, you can modify the date until which the object is restored. In general, you assign objects to the Glacier storage class for archival purposes and you don't need real-time access to them. For more information, see Object Archival (Glacier Storage Class).

Standard and Reduced Redundancy Storage Class

When you select an object stored in the Standard or Reduced Redundancy Storage (RSS) class and click **Details**, the details become visible. You can change the **Storage Class** property or **Server Side Encryption** property of the object and click **Save** to save change to the properties. The following example shows the details for an object.



aDocument.txt

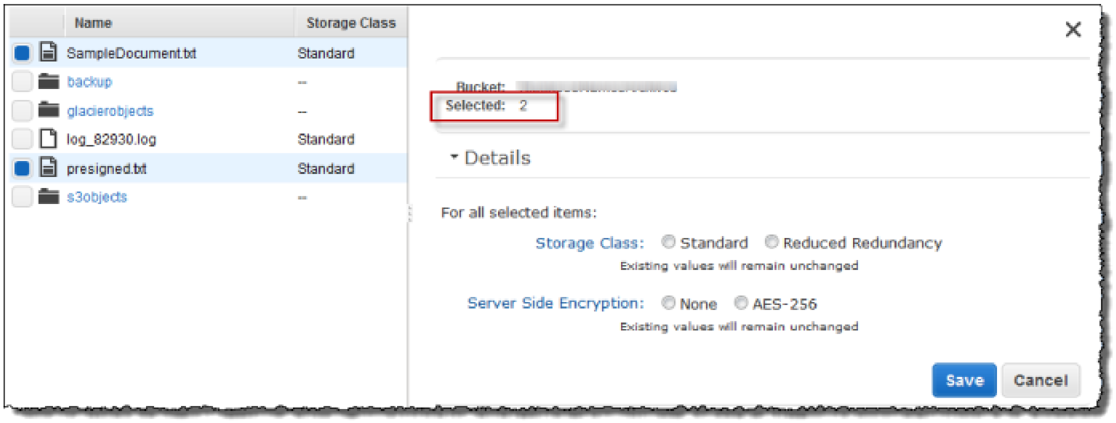
Bucket:	[redacted]
Folder:	[redacted]
Name:	aDocument.txt
Link:	https://s3.amazonaws.com/[redacted]aDocument.txt
Size:	10 bytes
Last Modified:	Tue Oct 23 13:29:05 GMT-700 2012
Owner:	Me
ETag:	2b73ebad8987b6b74eb037a16aa3b678
Expiry Date:	Wed Oct 23 17:00:00 GMT-700 2013
Expiration Rule:	Expire-Objects-Rule

▾ Details

Storage Class: ● Standard ○ Reduced Redundancy

Server Side Encryption: ● None ○ AES-256

When you select two or more objects in a bucket and click **Details**, no selections for **Storage** or **Server Side Encryption** are shown, regardless of the settings of these properties for the files that are part of the selection. In this multiple object select case, the **Details** panel enables you to change one of the two properties for all of the selected objects. For example, if you select **AES-256** for **Server Side Encryption** and click **Save**, then all of the selected objects will be encrypted. The following example shows the details for two selected items.



	Name	Storage Class
☑	SampleDocument.txt	Standard
□	backup	--
□	glacierobjects	--
□	log_82930.log	Standard
☑	presigned.txt	Standard
□	s3objects	--

Bucket: [redacted]
Selected: 2

▾ Details

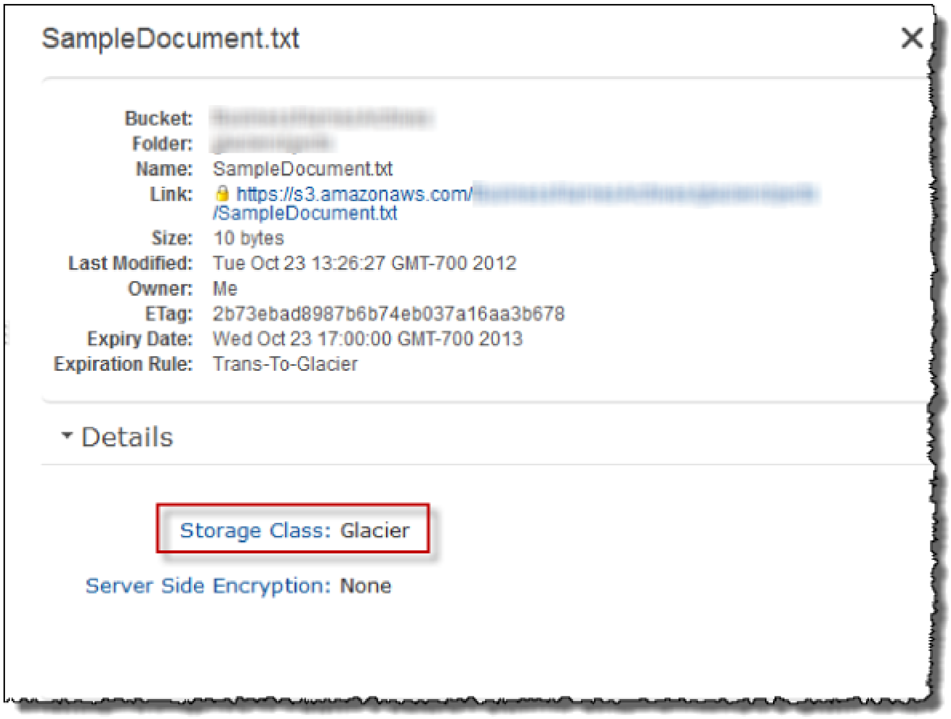
For all selected items:

Storage Class: ○ Standard ○ Reduced Redundancy
Existing values will remain unchanged

Server Side Encryption: ○ None ○ AES-256
Existing values will remain unchanged

Glacier Storage Class

When you select an object stored in the Glacier Storage class and click **Details**, the details appear. If the object has not been restored, the properties of the object are view-only. The following example shows the details properties for an object stored in the Glacier storage class that has not been restored.



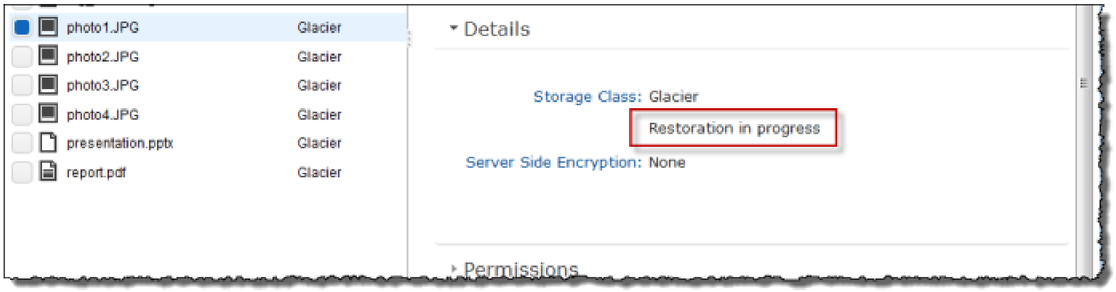
SampleDocument.txt

Bucket:	[redacted]
Folder:	[redacted]
Name:	SampleDocument.txt
Link:	https://s3.amazonaws.com/[redacted]/SampleDocument.txt
Size:	10 bytes
Last Modified:	Tue Oct 23 13:26:27 GMT-700 2012
Owner:	Me
ETag:	2b73ebad8987b6b74eb037a16aa3b678
Expiry Date:	Wed Oct 23 17:00:00 GMT-700 2013
Expiration Rule:	Trans-To-Glacier

Storage Class: Glacier

Server Side Encryption: None

If the object is in the process of being restored, the **Details** tab indicates this. The following example shows the properties for an object stored in the Glacier storage class that is in the process of being restored. For more information about restoring, see Restoring an Object (p. 44).



■	photo1.JPG	Glacier
□	photo2.JPG	Glacier
□	photo3.JPG	Glacier
□	photo4.JPG	Glacier
□	presentation.pptx	Glacier
□	report.pdf	Glacier

Storage Class: Glacier

Restoration in progress

Server Side Encryption: None

If the object is restored, the date until which the object is restored is displayed in the **Details**. The following example shows properties of a restored object. You can use the **Modify** button to change the length of time until which the object is restored.

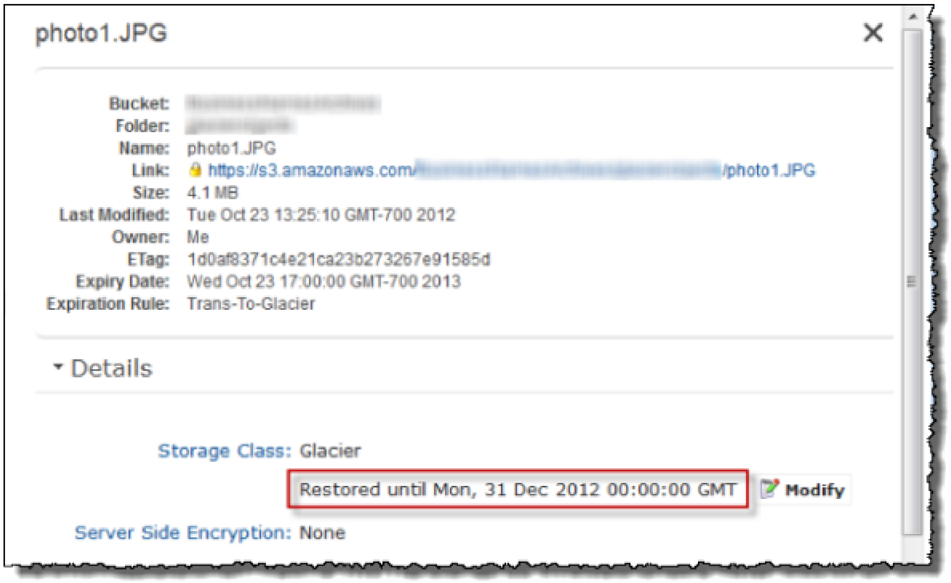


photo1.JPG

Bucket:	[redacted]
Folder:	[redacted]
Name:	photo1.JPG
Link:	https://s3.amazonaws.com/[redacted]/photo1.JPG
Size:	4.1 MB
Last Modified:	Tue Oct 23 13:25:10 GMT-700 2012
Owner:	Me
ETag:	1d0af8371c4e21ca23b273267e91585d
Expiry Date:	Wed Oct 23 17:00:00 GMT-700 2013
Expiration Rule:	Trans-To-Glacier

▾ Details

Storage Class: Glacier

Restored until Mon, 31 Dec 2012 00:00:00 GMT

Server Side Encryption: None

When you select two or more Glacier Storage Class class objects in a bucket and view the **Properties** of the selected objects, the **Properties** pane shows only the bucket name and the number of objects selected.

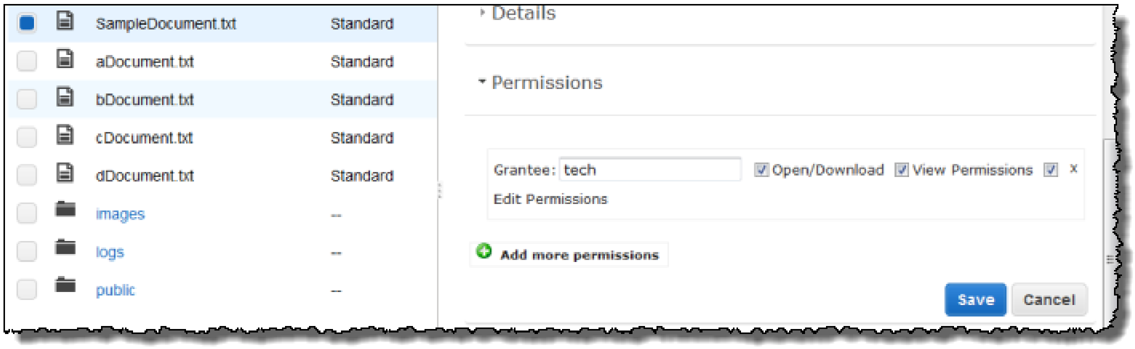
Editing Object Permissions

This section explains how to use the console to edit user permissions for an object. In general, you use permissions to provide other accounts access to an object. By default, the owner has full permissions. You may want to give others read-only permission. To do so, you set permissions by user type or per individual user.

Bucket and object permissions are completely independent; an object does not inherit the permissions from its bucket. For example, if you create a bucket and grant write access to another user, you will not be able to access that user's objects unless the user explicitly grants you access. This also applies if you grant anonymous write access to a bucket. Only the user `anonymous` can access objects the user created unless permission is explicitly granted to the bucket owner.

To change the permissions for an object

1. Sign into the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3.
2. Click on the object whose permissions you want to change, and then click **Permissions**.



■	SampleDocument.txt	Standard
□	aDocument.txt	Standard
□	bDocument.txt	Standard
□	cDocument.txt	Standard
□	dDocument.txt	Standard
□	images	--
□	logs	--
□	public	--

▸ Details

▾ Permissions

Grantee: tech ☑ Open/Download ☑ View Permissions ☑ Edit Permissions

3. Do one of the following:

To...	Do this...
Change a current permission	Select or clear the check boxes next to the permissions that you want to grant (select) or remove (clear).
To add permissions for a person or group	a. Click **Add more permissions**. b. In **Grantee**, add the group or e-mail address AWS account of the person whose permissions you want to set. c. Select or clear the check boxes, as appropriate, next to the permissions you want to grant or deny.
To remove a person or group from the permission list	Click the "x" on the line of the grantee that you want to remove.

There are two built-in groups that you can choose from the **Grantee** drop-down list box:

- **Authenticated Users—**This group consists of any user that has an Amazon AWS Account. When you grant the Authenticated User group permission, any valid signed request can perform the appropriate action. The request can be signed by either an AWS Account or IAM User.
- **Everyone—**This group grants anonymous access to your object

You can grant permission to an AWS account by entering the accounts canonical user ID or email address in the **Grantee** field. The email address must be the same one they used when signing up for an AWS account. You can grant a grantee any of the following permissions:

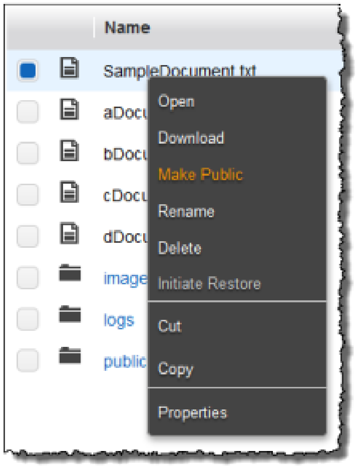
- **Open/Download—**Enables the account to access the object when they are logged in
- **View Permissions—**Can view the permissions associated with the object
- **Edit Permissions—**Can edit the permissions associated with the object

4. Click **Save**.

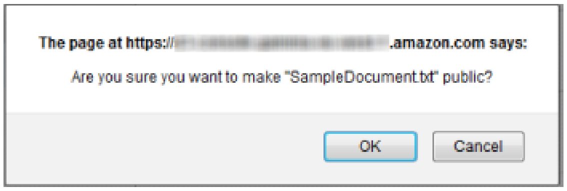
The console provides a shortcut for making objects accessible to everyone, meaning that everyone can both view and download the object.

To make an object accessible by everyone

1. Right-click the object that you want to make accessible.



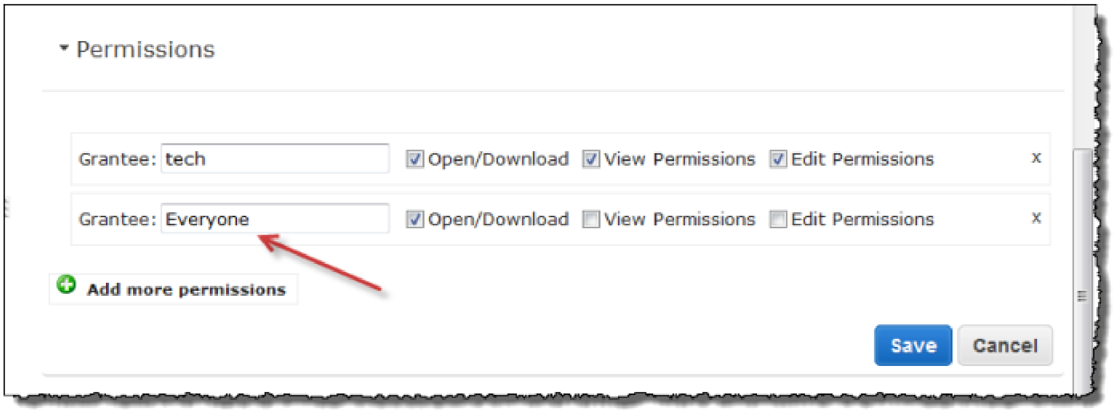
2. The console prompts you to confirm this change. Click OK. When the change is complete, click the Close button in the **Transfers** panel.



The page at https://[redacted].amazon.com says:

Are you sure you want to make "SampleDocument.txt" public?

3. Click **Permissions**. The newly added grantee appears in the display.



Permissions

Grantee: tech ☑ Open/Download ☑ View Permissions ☑ Edit Permissions x

Grantee: Everyone ☑ Open/Download □ View Permissions □ Edit Permissions x

Editing Object Metadata

Each object in Amazon S3 has a set of key/value pairs that represents its metadata. There are two types of metadata:

- **System metadata—**Sometimes processed by Amazon S3, e.g. `Content-Type`, and `Content-Length`
- **User metadata—**Never processed by Amazon S3.

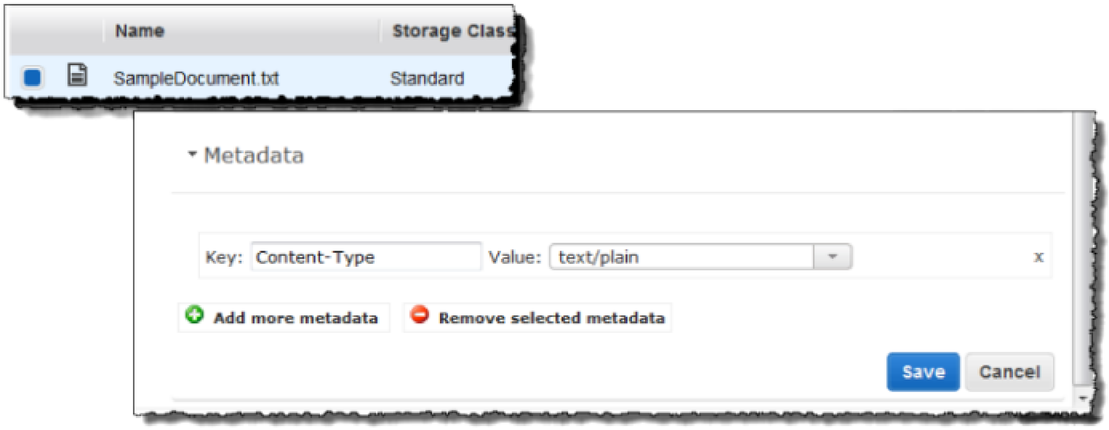
  User metadata is stored with the object and returned with it.

The maximum size for user metadata is 2 KB, and both the keys and their values must conform to US-ASCII standards.

This section explains how to use the console to add and remove the metadata associated with an object.

To edit the metadata of an object

1. Sign into the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3.
2. Click the object whose metadata you want to edit, and then click **Metadata**.



Name	Storage Class
SampleDocument.txt	Standard

Metadata

Key: Content-Type Value: text/plain

3. Do one of the following:

To...	Do This...
Add metadata	a. Click **Add more metadata**. b. In the **Key** box click one of the available keys, or type a new one. c. In the corresponding **Value** box, click an entry in the list, if available, or type a value.
Delete metadata	a. Click the key/value pair that you want to remove. b. Click **Remove selected metadata** or click the "x" on the line of the key/value pair that you want to remove.

4. Click Save.

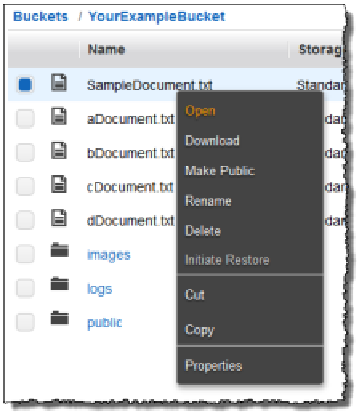
Opening an Object

You can open an object to view it in a browser. This section explains how to use the console to open an object.

To open an object

1. Sign into the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3.
2. Right-click the object that you want to open, and then click **Open**.

> **Tip**
> You can use the **`SHIFT`** and **`CTRL`** keys to select multiple objects and perform the same action on all of them simultaneously.



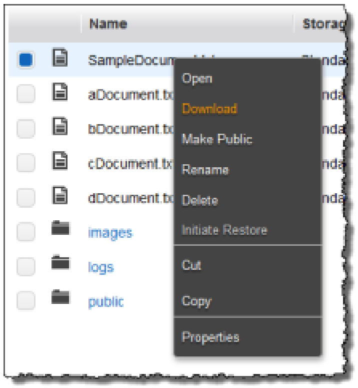
Downloading an Object

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

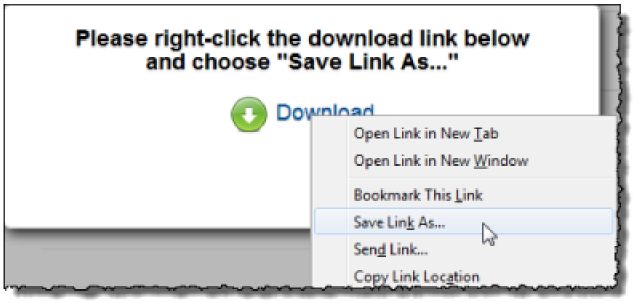
> **Note**
> Data transfer fees apply when you download objects.

To download an object

1. Sign into the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3.
2. Right-click the object you want to download, and then click **Download**.

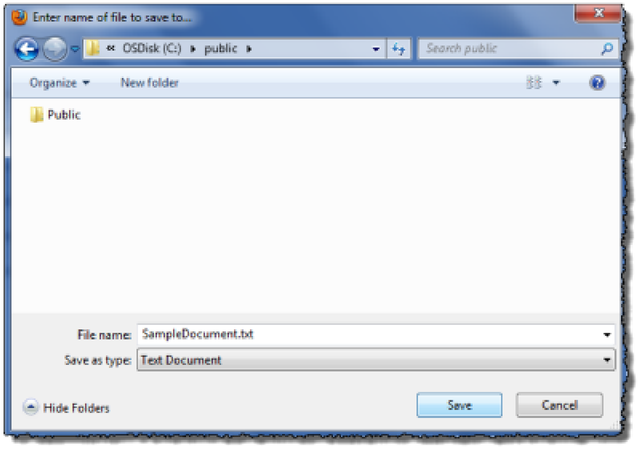


3. Right-click the word **Download**, and then click **Save Link As...**



Please right-click the download link below and choose "Save Link As..."

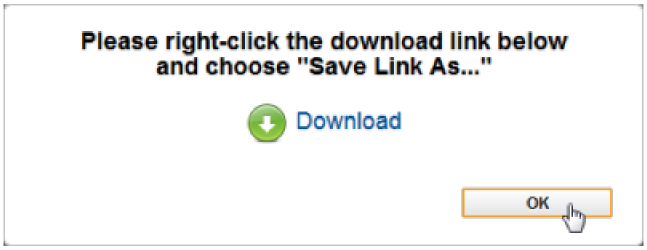
4. Navigate to the folder on your system where you want to download the object and then click **Save**.



File name: SampleDocument.txt

Save as type: Text Document

When the dowload is complete, click **OK** to return to the console.



Please right-click the download link below and choose "Save Link As..."

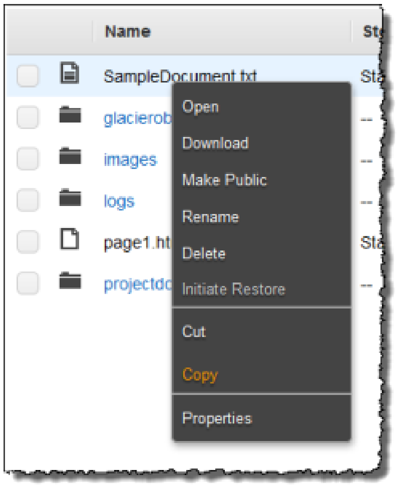
Copying an Object

You can also copy or move an object from one place to another by copying or cutting it from one place and pasting it in the new location.

This section explains how to use the Amazon S3 console to copy an object.

To copy an object

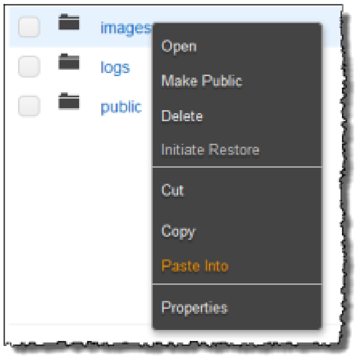
1. Sign into the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3.
2. Right-click the object that you want to copy, and then click **Copy**.



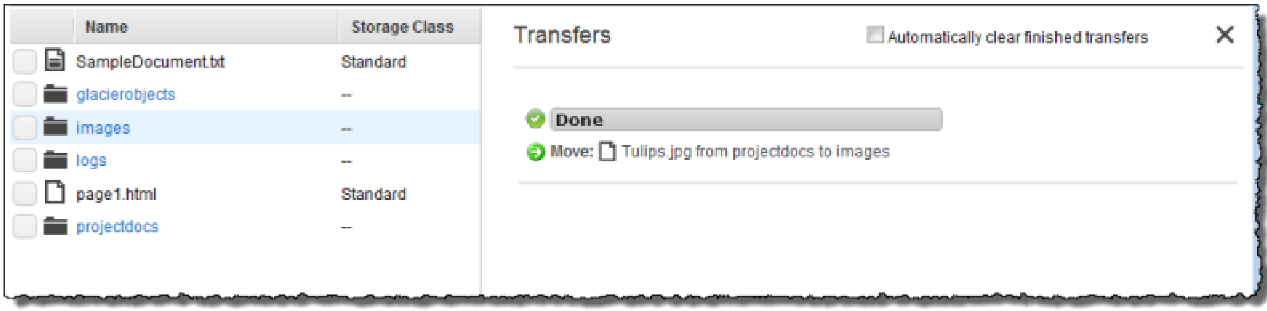
Note

If you click **Cut** instead of **Copy**, you will move your file from its current location to another.

3. Navigate to the bucket and folder where you want to copy the object, right-click the target location, and then click **Paste Into**.



You can monitor the progress of the copy on the **Transfers** panel. To hide or show the **Transfers** panel, click the **Transfers** button on the console.



Name	Storage Class
SampleDocument.txt	Standard
glacierobjects	--
images	--
logs	--
page1.html	Standard
projectdocs	--

Transfers

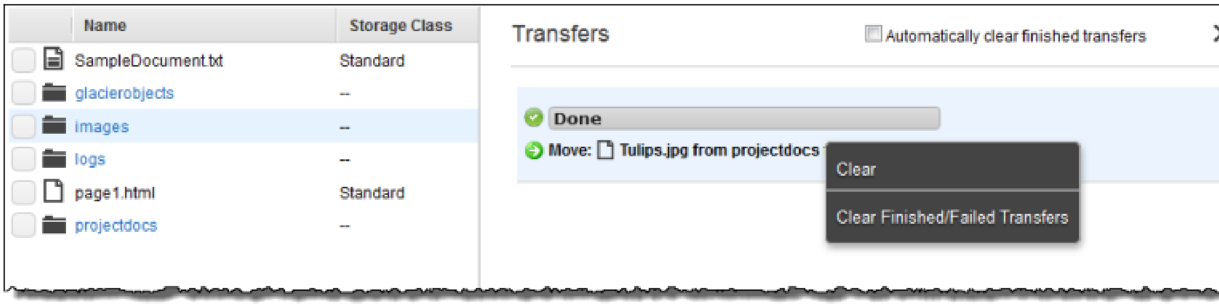
□ Automatically clear finished transfers

Done

Move: Tulips.jpg from projectdocs to images

Note

To clear individual line items in the **Transfers** panel, right-click the items and then click**Clear**. To remove all finished or failed transfers, click **Clear Finished/Failed Transfers**.



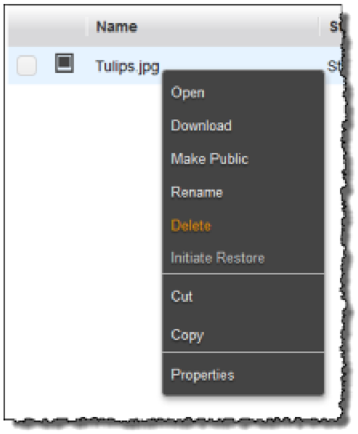
Deleting an Object

Because all objects in your Amazon S3 bucket incur storage costs, you should delete objects that you no longer need. If you are collecting log files, for example, it's a good idea to delete them when they're no longer valuable.

This section explains how to use the Amazon S3 console to delete an object.

To delete an object

1. Sign into the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3.
2. In the Objects and Folders list, right-click the object that you want to delete, and then click **Delete**.



3. When a confirmation message appears, click **OK**.

Restoring an Object

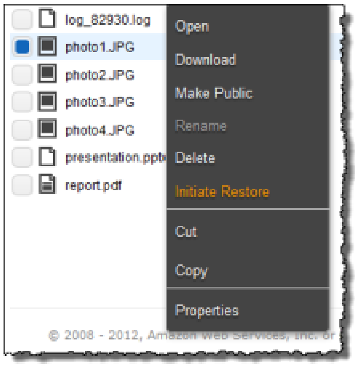
Objects in the Glacier storage class are not immediately accessible: you must first restore a temporary copy of the object to its bucket before it is available. For information about when to use the Glacier storage class for objects, go to Object Lifecycle Management in the *Amazon S3 Developer Guide*. Restored objects are stored only for the number of days that you specify. You can modify the number of days an object is retained after it is restored. If you want a permanent copy of the object, create a copy of it within your Amazon S3 bucket.

This section explains how to use the Amazon S3 console to restore an object that is associated with the storage class Glacier, and procedures for both restoring and modifying the number of days.

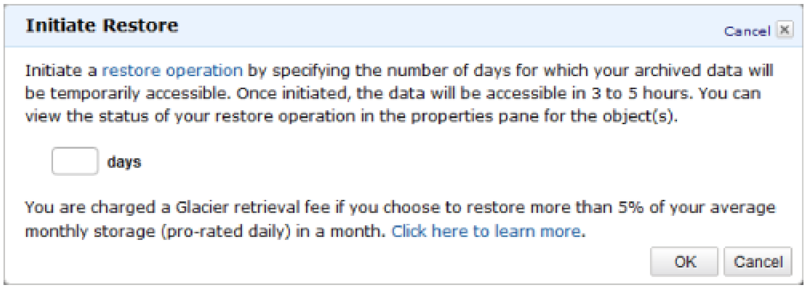
> **Note**
>
> Amazon S3 calculates the restored date of an object by adding the number of days that you specify to the current time when you are restoring the object and then rounding the resulting time to the next day at midnight UTC. This calculation applies to the initial restoration of the object and to any time you modify the restored object's number of days. For example, if an object was restored on 10/15/2012 10:30 a.m. UTC and the number of days was specified as 3, then the object is restored until 10/19/2012 00:00 UTC. If, on 10/16/2012 11:00 a.m. UTC you change the number of days to 1, then the object is restored until 10/18/2012 00:00 UTC.

To restore an object

1. Sign into the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3.
2. Right-click an object in storage class Glacier that you want to restore, and then click Initiate Restore.



3. In the **Initiate Restore** dialog box, type the number of days until the restored object is deleted.


Initiate Restore

Initiate a restore operation by specifying the number of days for which your archived data will be temporarily accessible. Once initiated, the data will be accessible in 3 to 5 hours. You can view the status of your restore operation in the properties pane for the object(s).

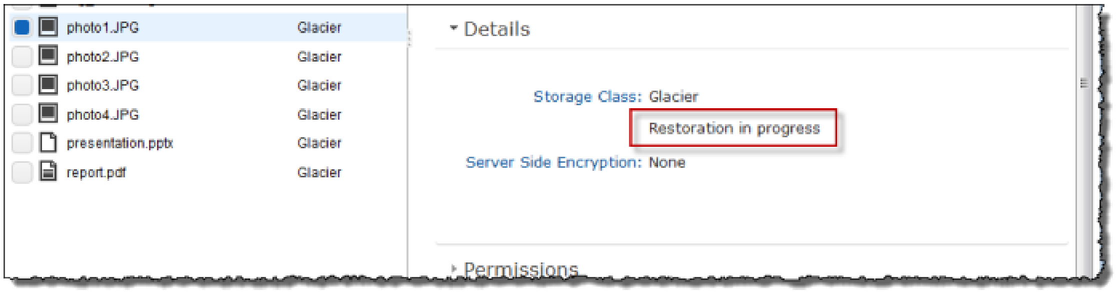
□ days

You are charged a Glacier retrieval fee if you choose to restore more than 5% of your average monthly storage (pro-rated daily) in a month. Click here to learn more.

4. In the confirmation notice that appears, click **OK**.

   Use the object **Details** pane to determine the status of the restoration. For more information, see Editing Object Details (p. 34).

   The following example indicates that an object is in the process of being restored.



● photo1.JPG	Glacier
□ photo2.JPG	Glacier
□ photo3.JPG	Glacier
□ photo4.JPG	Glacier
□ presentation.pptx	Glacier
□ report.pdf	Glacier

▾ Details

Storage Class: Glacier

Restoration in progress

Server Side Encryption: None

▸ Permissions

When the object is restored, the **Details** pane shows the date when the copy of object will be deleted.

The following example shows that an object is restored.

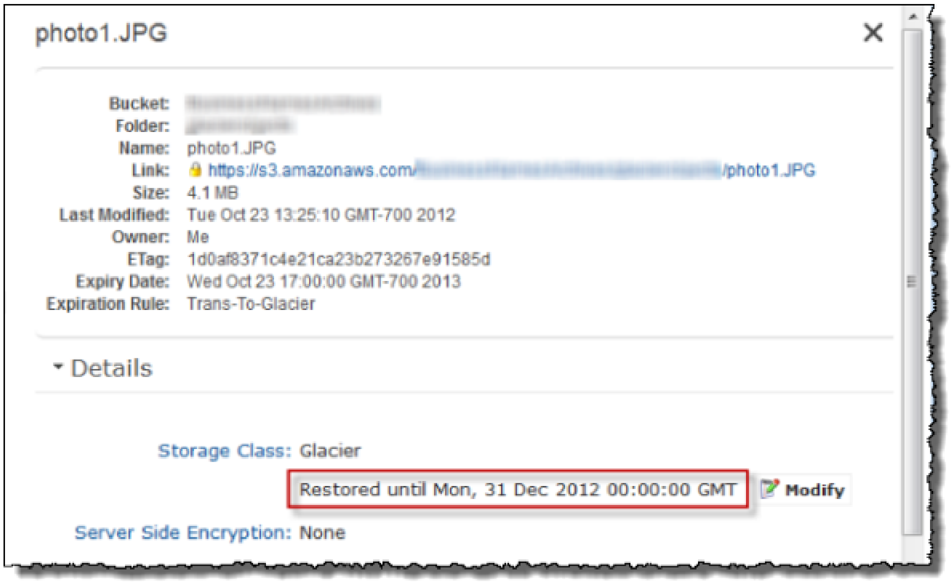


photo1.JPG

Bucket: [redacted]
Folder: [redacted]
Name: photo1.JPG
Link: https://s3.amazonaws.com/[redacted]/photo1.JPG
Size: 4.1 MB
Last Modified: Tue Oct 23 13:25:10 GMT-700 2012
Owner: Me
ETag: 1d0af8371c4e21ca23b273267e91585d
Expiry Date: Wed Oct 23 17:00:00 GMT-700 2013
Expiration Rule: Trans-To-Glacier

▾ Details

Storage Class: Glacier

Restored until Mon, 31 Dec 2012 00:00:00 GMT

Server Side Encryption: None

To extend the length of time of a restored object

1. Sign into the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3.
2. Click the restored object whose lifetime you want to extend, and then click **Details**.

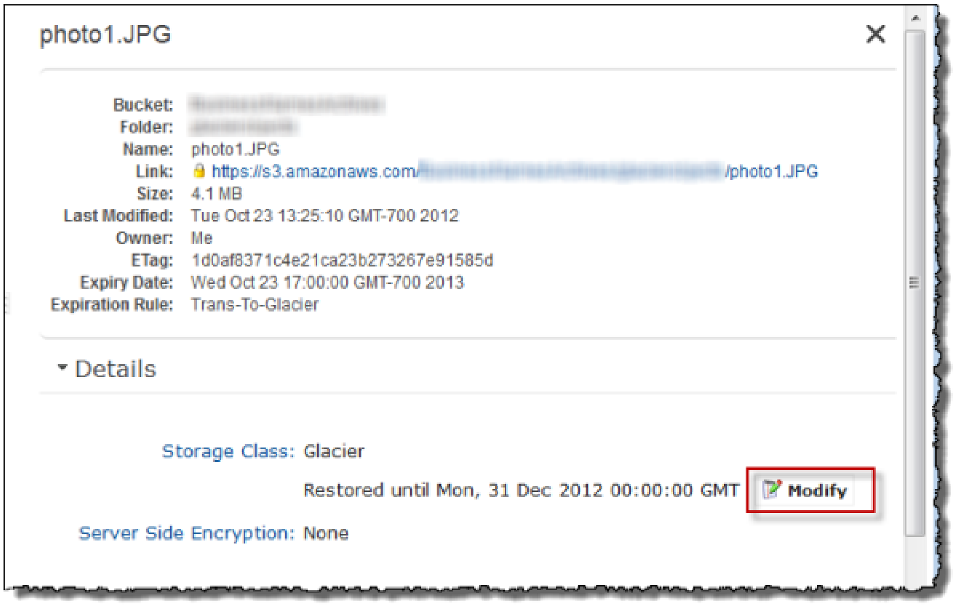


photo1.JPG

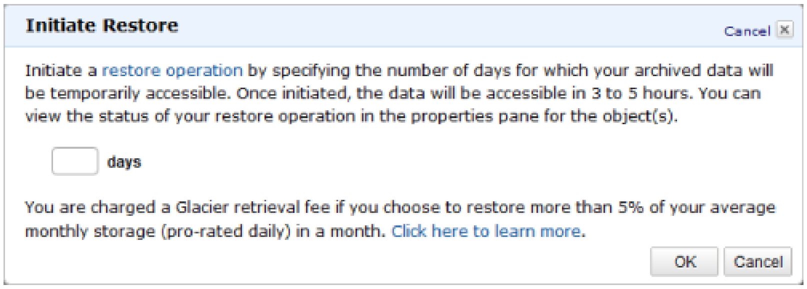
Bucket: [redacted]
Folder: [redacted]
Name: photo1.JPG
Link: https://s3.amazonaws.com/[redacted]/photo1.JPG
Size: 4.1 MB
Last Modified: Tue Oct 23 13:25:10 GMT-700 2012
Owner: Me
ETag: 1d0af8371c4e21ca23b273267e91585d
Expiry Date: Wed Oct 23 17:00:00 GMT-700 2013
Expiration Rule: Trans-To-Glacier

▾ Details

Storage Class: Glacier
Restored until Mon, 31 Dec 2012 00:00:00 GMT

Server Side Encryption: None

3. Click **Modify**.
4. In the **Initiate Restore** dialog box, in the **days** box, type the number of days until the restored object is deleted .



Initiate Restore

Initiate a restore operation by specifying the number of days for which your archived data will be temporarily accessible. Once initiated, the data will be accessible in 3 to 5 hours. You can view the status of your restore operation in the properties pane for the object(s).

days

You are charged a Glacier retrieval fee if you choose to restore more than 5% of your average monthly storage (pro-rated daily) in a month. Click here to learn more.

5. In the confirmation message that appears, click **OK**. The **Restored until** date is changed.

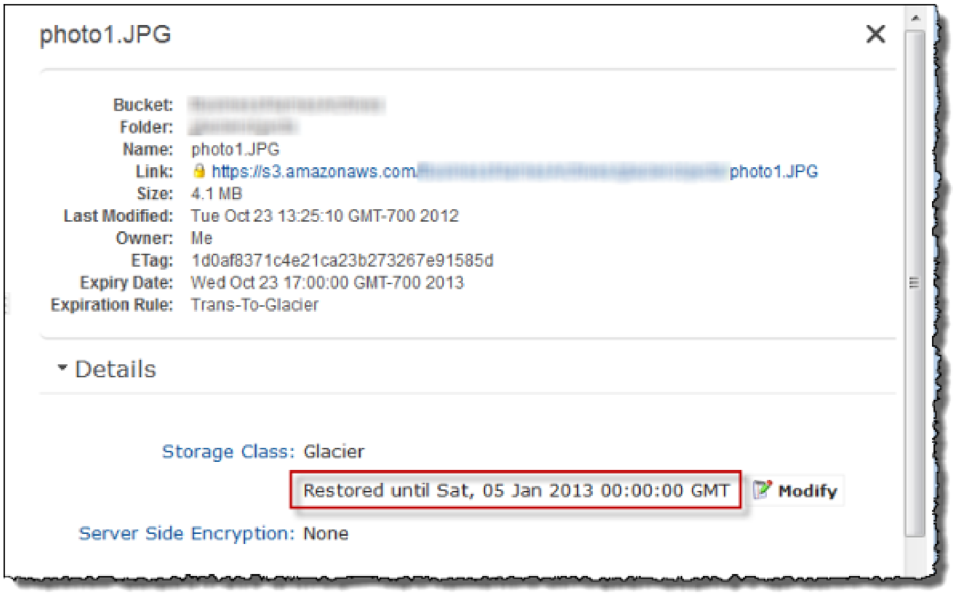


photo1.JPG

Bucket: [redacted]
Folder: [redacted]
Name: photo1.JPG
Link: https://s3.amazonaws.com/[redacted]photo1.JPG
Size: 4.1 MB
Last Modified: Tue Oct 23 13:25:10 GMT-700 2012
Owner: Me
ETag: 1d0af8371c4e21ca23b273267e91585d
Expiry Date: Wed Oct 23 17:00:00 GMT-700 2013
Expiration Rule: Trans-To-Glacier

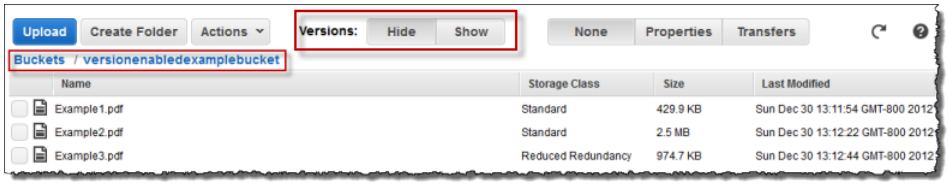
▾ Details

Storage Class: Glacier
Restored until Sat, 05 Jan 2013 00:00:00 GMT
Server Side Encryption: None

Managing Objects in a Versioning-Enabled Bucket

A versioning-enabled bucket can have multiple versions of objects in the bucket. Amazon S3 assigns each object a unique version ID. For more information about versioning support in Amazon S3, see Using Versioning in the *Amazon S3 Simple Storage Service Developer Guide*.

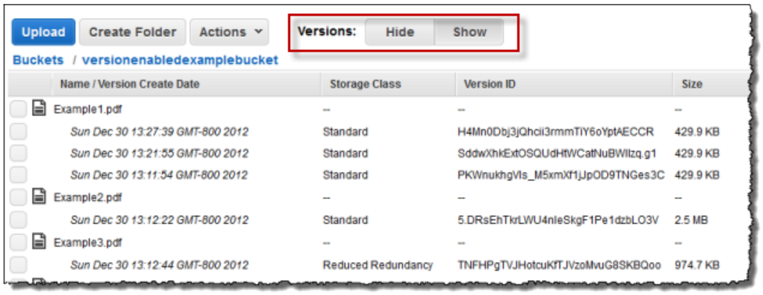
When a bucket is versioning-enabled, you can show or hide all the object versions. The following example shows the list of objects in the `versionenabledexamplebucket` bucket. Version information is hidden, so these objects represent the latest version.



Buckets / versionenabledexamplebucket

Name	Storage Class	Size	Last Modified
Example1.pdf	Standard	429.9 KB	Sun Dec 30 13:11:54 GMT-800 2012
Example2.pdf	Standard	2.5 MB	Sun Dec 30 13:12:22 GMT-800 2012
Example3.pdf	Reduced Redundancy	974.7 KB	Sun Dec 30 13:12:44 GMT-800 2012

If you click **Show**, the console lists all the versions, as shown in the following example:



Buckets / versionenabledexamplebucket

Name / Version Create Date	Storage Class	Version ID	Size
Example1.pdf	--	--	--
Sun Dec 30 13:27:39 GMT-800 2012	Standard	H4Mn0Dbj3jQhcii3rmmTiY6oYptAECCR	429.9 KB
Sun Dec 30 13:21:55 GMT-800 2012	Standard	SddwXhkExtOSQUdHtWCatNuBWIlzq.g1	429.9 KB
Sun Dec 30 13:11:54 GMT-800 2012	Standard	PKWnukhgVls_M5xmXf1jJpOD9TNGes3C	429.9 KB
Example2.pdf	--	--	--
Sun Dec 30 13:12:22 GMT-800 2012	Standard	5.DRsEhTkrLWU4nleSkgF1Pe1dzbLO3V	2.5 MB
Example3.pdf	--	--	--
Sun Dec 30 13:12:44 GMT-800 2012	Reduced Redundancy	TNFHPgTVJHotcuKfTJVzoMvuG8SKBQoo	974.7 KB

For each object version, the console shows a unique version ID, the date and time the object version was created, and other properties.

Uploading an Object

If you upload an object with a key name that already exists in the bucket, Amazon S3 creates another version of the object instead of replacing the existing object. For more information about uploading an object, see Uploading Objects into Amazon S3 (p. 29).

Updating Object Properties

If you update any object properties after the initial object upload-such as changing the storage details or any other metadata changes-then Amazon S3 creates a new object version in the bucket. Also if you rename the object, Amazon S3 creates a new object version.

For example, if you update an object's storage class or change how the object is stored at rest by updating its server-side encryption property, Amazon S3 creates an object version for each property update you save.

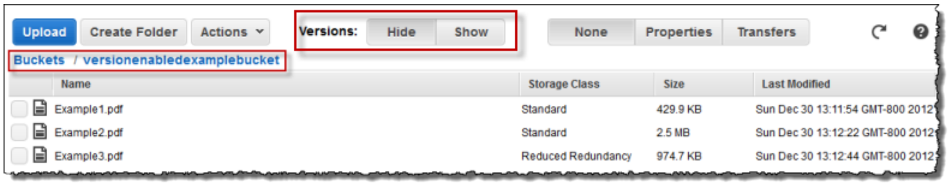
When versions are hidden you can update all the object properties but when versions are shown you can update only the permissions for the specific object version.

For more information about updating object properties, see Editing Object Properties (p. 34).

Deleting Objects from a Versioning-Enabled Bucket

In a versioning-enabled bucket, you can either delete an object from the object list (version information hidden) or delete a specific version of the object.

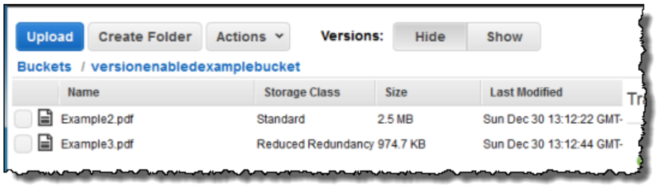
With version information hidden, the console shows the object list as shown in the following example:



Buckets / versionenabledexamplebucket

Name	Storage Class	Size	Last Modified
Example1.pdf	Standard	429.9 KB	Sun Dec 30 13:11:54 GMT-800 2012
Example2.pdf	Standard	2.5 MB	Sun Dec 30 13:12:22 GMT-800 2012
Example3.pdf	Reduced Redundancy	974.7 KB	Sun Dec 30 13:12:44 GMT-800 2012

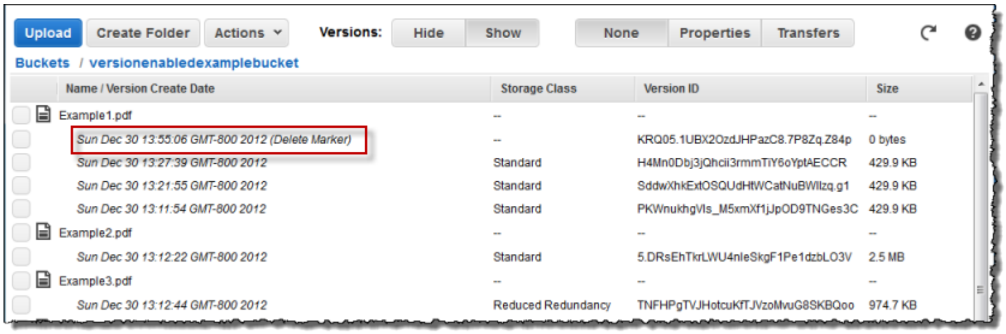
If you select and delete the Example1.pdf object, Amazon S3 adds a delete marker for the object and the object no longer appears in the object list:



Buckets / versionenabledexamplebucket

Name	Storage Class	Size	Last Modified
Example2.pdf	Standard	2.5 MB	Sun Dec 30 13:12:22 GMT-
Example3.pdf	Reduced Redundancy	974.7 KB	Sun Dec 30 13:12:44 GMT-

However, if you click **Show** to list object versions, the Example1.pdf object appears in the list with all versions and a delete marker at the top.



Name / Version Create Date	Storage Class	Version ID	Size
Example1.pdf	--	--	--
Sun Dec 30 13:55:06 GMT-800 2012 (Delete Marker)	--	KRQ05.1UBX2OzdJHPazC8.7P8Zq.Z84p	0 bytes
Sun Dec 30 13:27:39 GMT-800 2012	Standard	H4Mn0Dbj3jQhcii3rmmTiY6oYptAECCR	429.9 KB
Sun Dec 30 13:21:55 GMT-800 2012	Standard	SddwXhkExtOSQUdHtWCatNuBWIlzq.g1	429.9 KB
Sun Dec 30 13:11:54 GMT-800 2012	Standard	PKWnukhgVls_M5xmXf1jJpOD9TNGes3C	429.9 KB
Example2.pdf	--	--	--
Sun Dec 30 13:12:22 GMT-800 2012	Standard	5.DRsEhTkrLWU4nleSkgF1Pe1dzbLO3V	2.5 MB
Example3.pdf	--	--	--
Sun Dec 30 13:12:44 GMT-800 2012	Reduced Redundancy	TNFHPgTVJHotcuKfTJVzoMvuG8SKBQoo	974.7 KB

To delete an object permanently, you must delete all the versions of the object, including the delete maker (if present). If you delete only a specific object version, Amazon S3 permanently deletes only that specific version. If you delete the delete marker, the object reappears in the object list. For more information, see Deleting an Object (p. 44).

Working with Folders

Topics

You can use the Amazon S3 Console to create folders, which you can use to group your objects. An Amazon S3 folder, just like a folder in a computer file system, is a means of grouping objects.

The folder name becomes part of the URL of the object in it. For example, if you upload an object called `history.txt` to the `logs` folder using the AWS Management Console, the full key name for this object is `logs/history.txt`.

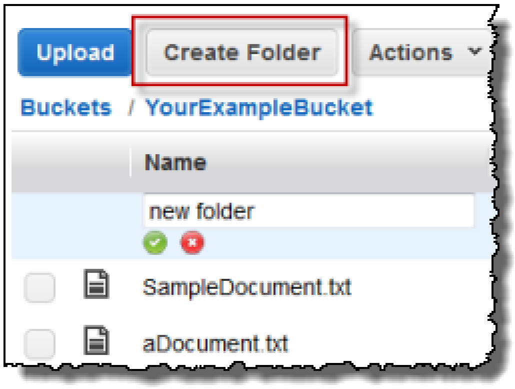
As in a computer file system, you can have folders within folders. You can upload and copy objects directly into a folder.

Creating a Folder

This section describes how to use the console to create a folder.

To create a folder

1. In the Buckets list click the bucket in which you want to create a folder, and then click **Create Folder**.



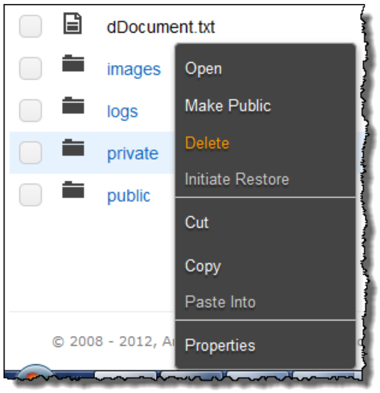
2. Under Name, in the box that appears, type a name for the folder, and then click the check mark.

Deleting a Folder

This section describes how to use the console to delete a folder.

> **Caution**
> When you delete a folder, any objects or folders contained in the folder will be automatically deleted . If you want to retain those objects, you must move them elsewhere before you delete the folder. For information about moving objects, see Copying an Object.

1. In the Objects and Folders list, right-click the folder that you want to delete, and then click **Delete**.



2. When a confirmation message appears, click **OK**.

Amazon S3 Resources

Following is a table that lists related resources that you'll find useful as you work with this service.

Resource	Description
Amazon S3 Getting Started Guide	The Getting Started Guide provides a quick tutorial of the service using the AWS Management Console to accomplish basic Amazon S3 tasks.
Amazon S3 API Reference	The API Reference describes Amazon S3 operations in detail.
Amazon S3 Developer Guide	The developer guide describes how to use Amazon S3 operations.
Amazon S3 Technical FAQ	The FAQ covers the top 20 questions developers have asked about this product.
Amazon S3 Release Notes	The Release Notes give a high-level overview of the current release. They specifically note any new features, corrections, and known issues.
AWS Developer Resource Center	A central starting point to find documentation, code samples, release notes, and other information to help you build innovative applications with AWS.
AWS Management Console	The console allows you to perform Amazon S3 functions using a simple and intuitive web user interface.
Discussion Forums	A community-based forum for developers to discuss technical questions related to Amazon Web Services.
AWS Support Center	The home page for AWS Technical Support, including access to our Developer Forums, Technical FAQs, Service Status page, and Premium Support.
AWS Calculator	Use the AWS calculator to estimate your monthly charges for using AWS services.
AWS Premium Support	The primary web page for information about AWS Premium Support, a one-on-one, fast-response support channel to help you build and run applications on AWS Infrastructure Services.

Resource	Description
Amazon S3 product information	The primary web page for information about Amazon S3.
Contact Us	A central contact point for inquiries concerning AWS billing, account, events, abuse etc.
Conditions of Use	Detailed information about the copyright and trademark usage at Amazon.com and other topics.

Document History

This document history is associated with the 2006-03-01 release of Amazon S3. This guide was last updated on December 31, 2012.

The following table describes the important changes since the last release of the *Amazon Simple Storage Service Console User Guide*.

Change	Description	Date
Console support for enabling bucket versioning	The Amazon S3 console now supports bucket versioning and managing objects in a versioning-enabled bucket. For more information see, Enabling Bucket Versioning (p. 15), and Managing Objects in a Versioning-Enabled Bucket (p. 48).	In this release.
Support for static website hosting at the root domain	Amazon S3 now supports hosting static websites at the root domain. Visitors to your website can access your site from their browser without specifying "www" in the web address (e.g., "example.com"). Many customers already host static websites on Amazon S3 that are accessible via a "www" subdomain (e.g., "www.example.com"). Previously, to support root domain access, you needed to run your own web server to proxy root domain requests from browsers to your website on Amazon S3. Running a web server to proxy requests introduces additional costs, operational burden, and another potential point of failure. Now, you can take advantage of the high availability and durability of Amazon S3 for both "www" and root domain addresses. For an example walkthrough, go to go to Example: Setting Up a Static Website Using a Custom Domain. For conceputal information, go to Hosting Static Websites on Amazon S3 in the *Amazon Simple Storage Service Developer Guide*.	27 December 2012
Console revision	Amazon S3 console has been updated. The documentation topics that refer to the console have been revised accordingly.	14 December 2012

Change	Description	Date
Support for Archiving Data to Amazon Glacier	Amazon S3 now support a storage option that enables you to utilize Amazon Glacier's low-cost storage service for data archival. To archive objects, you define archival rules identifying objects and timeline when you want Amazon S3 to archive these objects to Amazon Glacier. You can easily set the rules on a bucket using the Amazon S3 console or programmatically using the Amazon S3 API or AWS SDKs. In addition to setting object expiration, you can now use lifecycle management to archive data in Amazon S3. For more information, see Managing Lifecycle Configuration (p. 21). For conceptual information, go to Object Lifecycle Management in the *Amazon Simple Storage Service Developer Guide*.	13 November 2012
Cross-Origin Resource Sharing (CORS) support	Amazon S3 now supports Cross-Origin Resource Sharing (CORS). CORS defines a way in which client web applications that are loaded in one domain can interact with or access resources in a different domain. With CORS support in Amazon S3, you can build rich client-side web applications on top of Amazon S3 and selectively allow cross-domain access to your Amazon S3 resources. For more information, see Enabling Cross-Origin Resource Sharing in the *Amazon S3 Developer Guide*.	31 August 2012
AWS Cost Allocation Tagging support	You can use AWS Cost Allocation to control how storage resources are organized on your bill. You do this by defining one or more tags for a bucket. For more information, go to Cost Allocation Tagging in the *Amazon S3 Developer Guide*.	21 August 2012
Object Expiration support	You can use Object Expiration to schedule automatic removal of data after a configured time period. You set object expiration by adding lifecycle configuration to a bucket. For more information, go to Object Expiration.	27 December 2011
New Region supported	Amazon S3 now supports the South America (Sao Paulo) Region. For more information, see Regions (p. 4).	14 December 2011
New Region supported	Amazon S3 now supports the US West (Oregon) Region. For more information, see Regions (p. 4).	08 November 2011
Documentation Update	This release includes enhancements to the object properties related sections. Information about what the **Details** properties tab show when you select one or more objects. For more information, see Editing Object Properties (p. 34).	17 October 2011
Support for server-side encryption in Amazon S3	This release includes support for server-side encryption in the Amazon S3 console. You can now specify that data stored in Amazon S3 is encrypted at rest. When you upload objects to Amazon S3 using the console, you can choose server-side encryption for your data. For more information, see Uploading Objects into Amazon S3 (p. 29). For more information about server-side encryption for data stored in Amazon S3, see Using Server-Side Encryption in the Amazon S3 *Developer Guide*.	5 October 2011

Change	Description	Date
AWS Management Console enhancements	This release includes the following AWS Management Console enhancements: • **Folder upload—**You can now use AWS Management Console to upload folders into Amazon S3. Amazon S3 uploads all the files, and subfolders from the specified folder to your bucket. For more information, see Uploading Objects into Amazon S3 (p. 29) • **Jump feature—**Instead of scrolling through a long list to find an object or folder, you can now simply start typing the first few characters of an object or folder name into the browser when looking at a listing. The console will jump to objects that match or follow what you type. For more information, see Browsing the Objects in Your Bucket (p. 13)	6 June 2011
Support for hosting static websites in Amazon S3	Amazon S3 introduces enhanced support for hosting static websites. This includes support for index documents and custom error documents. When using these features, requests to the root of your bucket or a subfolder (e.g., `http://mywebsite.com/subfolder`) returns your index document instead of the list of objects in your bucket. If an error is encountered, Amazon S3 returns your custom error message instead of an Amazon S3 error message. For information on managing website configuration using the AWS Management Console, see Configuring a Bucket for Website Hosting (p. 16).For more information about Amazon S3's website configuration feature, go to Hosting Websites on Amazon S3 in the *Amazon Simple Storage Service Developer Guide*.	17 February 2011
Large object support	Now, you can use AWS Management Console to upload large objects, up to 5 TB each, to an Amazon S3 bucket.	9 December 2010
Bucket notifications in the console	Now, you can configure bucket properties to enable notifications. These notifications are posted to Amazon Simple Notification Service (SNS) topic in the event a Reduced Redundancy Storage (RRS) object is lost from the bucket.	8 September 2010
Bucket policies in the console	Now, you can add and edit Amazon S3 bucket policies using the AWS Management Console. You can access bucket policies in the AWS Management Console by viewing the properties of the specific bucket. Using bucket policies, you can define security rules that apply to all objects or a subset of objects within a bucket. This makes updating and managing permissions easier.	13 August 2010
New Guide	This is the first release of the *Amazon S3 Console User Guide*. It describes how to use Amazon S3 in the AWS Management Console.	9 June 2010

Glossary

account

AWS account associated with a particular user.

authentication

The process of proving your identity to the system.

bucket

A container for objects stored in Amazon S3. Every object is contained within a bucket. For example, if the object named `photos/puppy.jpg` is stored in the `johnsmith` bucket, then it is addressable using the URL `http://johnsmith.s3.amazonaws.com/photos/puppy.jpg`

canonical ID

A string (ID) and a display name that uniquely represents a user. To locate the CanonicalUser ID for a user, the user must perform the ListAllMyBuckets operation in his or her Amazon S3 account and copy the ID from the Owner XML object.

canonicalization

The process of converting data into a standard format that will be recognized by a service such as Amazon S3.

consistency model

The method through which Amazon S3 achieves high availability, which involves replicating data across multiple servers within Amazon's data centers. After a "success" is returned, your data is safely stored. However, information about the changes might not immediately replicate across Amazon S3.

grantee

An account that can be granted permissions. Grantees can be individuals or groups.

key

The unique identifier for an object within a bucket. Every object in a bucket has exactly one key. Since a bucket and key together uniquely identify each object, Amazon S3 can be thought of as a basic data map between "bucket + key" and the object itself. Every object in Amazon S3 can be uniquely addressed through the combination of the web service endpoint, bucket name, and key, as in http://doc.s3.amazonaws.com/2006-03-01/AmazonS3.wsdl, where "doc" is the name of the bucket, and "2006-03-01/AmazonS3.wsdl" is the key.

metadata

The metadata is a set of name-value pairs that describe the object. These include default metadata such as the date last modified and standard HTTP metadata such as Content-Type. The developer can also specify custom metadata at the time the Object is stored.

object

The fundamental entities stored in Amazon S3. Objects consist of object data and metadata. The data portion is opaque to Amazon S3.

Versioning

Every object in Amazon S3 has a key and a version ID. Objects with the same key but different version IDs can be stored in the same bucket. Versioning is enabled at the bucket layer using `PUT Bucket versioning`.