

---

# **Amazon Simple Storage Service**

## **Console User Guide**

**API Version 2006-03-01**



# **Amazon Simple Storage Service: Console User Guide**

Copyright © 2011 Amazon Web Services LLC or its affiliates. All rights reserved.

## Table of Contents

Welcome to Amazon S3 .....	1
Introduction to Amazon S3 .....	2
Introduction to the Console .....	7
Working with Buckets .....	9
Creating a Bucket .....	9
Browsing the Objects in Your Bucket .....	12
Managing Bucket Logging .....	13
Managing Bucket Website Configuration .....	14
Editing Bucket Permissions .....	15
Enabling RRS Lost Object Notifications .....	16
Deleting a Bucket .....	17
Working with Objects .....	19
Uploading Objects into Amazon S3 .....	19
Editing Object Properties .....	24
Editing Object Permissions .....	25
Editing Object Metadata .....	27
Opening an Object .....	29
Downloading an Object .....	29
Copying an Object .....	30
Deleting an Object .....	32
Working with Folders .....	33
Creating a Folder .....	33
Deleting a Folder .....	34
Amazon S3 Resources .....	35
Document History .....	37
Glossary .....	39

---

# 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	<a href="#">Amazon Simple Storage Service (Amazon S3)</a>
General information about Amazon S3	<a href="#">Introduction to Amazon S3 (p. 2)</a>
Conceptual information about Amazon S3	<a href="#">Amazon S3 Concepts (p. 3)</a>
Using the AWS Management Console to interact with Amazon S3	<a href="#">Using the Console (p. 7)</a>
Working with buckets using AWS Management Console	<a href="#">Working with Buckets (p. 9)</a>
Working with objects using AWS Management Console	<a href="#">Working with Objects (p. 19)</a>

# Introduction to Amazon S3

---

## Topics

- [Overview of Amazon S3 \(p. 2\)](#)
- [Advantages to Amazon S3 \(p. 2\)](#)
- [Amazon S3 Concepts \(p. 3\)](#)
- [Limitations of the AWS Management Console \(p. 5\)](#)
- [Paying for Amazon S3 \(p. 6\)](#)
- [Related Amazon Web Service Products \(p. 6\)](#)

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

- [Buckets \(p. 3\)](#)
- [Objects \(p. 3\)](#)
- [Folders \(p. 3\)](#)
- [Keys \(p. 4\)](#)
- [Regions \(p. 4\)](#)
- [Access Control \(p. 4\)](#)
- [Amazon S3 Data Consistency Model \(p. 5\)](#)

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 likely 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 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(Northern California)**—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)**—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.
- **APAC (Singapore)**—Uses Amazon S3 servers in Singapore.  
To use this Region, choose APAC - Singapore as the Region when creating the bucket in the AWS Management Console. In Amazon S3, the APAC (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.

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. The EU (Ireland), US (Northern California), and APAC (Singapore) 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
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:

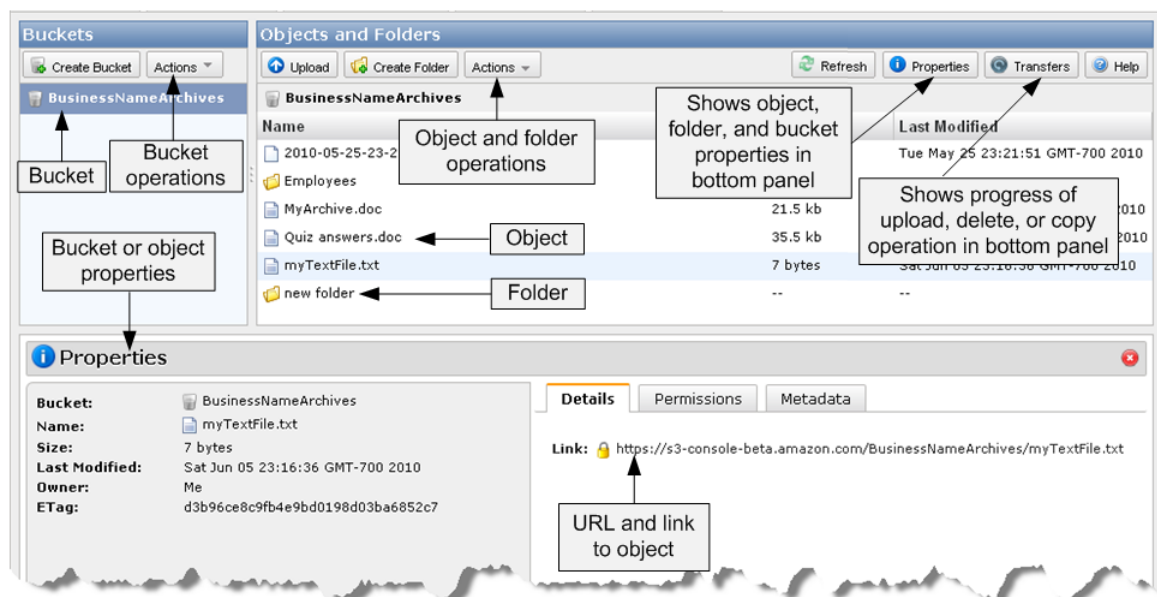
- **Amazon CloudFront**—This web service provides an easy way to distribute content to end users with low latency, high data transfer speeds, and no commitments.  
For more information, go to [Amazon CloudFront](#).
- **Amazon ElasticCompute Cloud**—This web service provides virtual compute resources in the cloud.  
For more information, go to [Amazon ElasticCompute 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>. This guide uses the functions available from the Amazon S3 tab.

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 console appears similar to the following figure when you click the Amazon S3 tab.



The left pane shows the buckets you own. The right pane shows the folders and objects in a selected bucket.

You use folders to create logical groupings of objects. All objects and folders reside in an Amazon S3 bucket.

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

- [Creating a Bucket \(p. 9\)](#)
- [Browsing the Objects in Your Bucket \(p. 12\)](#)
- [Managing Bucket Logging \(p. 13\)](#)
- [Managing Bucket Website Configuration \(p. 14\)](#)
- [Editing Bucket Permissions \(p. 15\)](#)
- [Enabling RRS Lost Object Notifications \(p. 16\)](#)
- [Deleting a Bucket \(p. 17\)](#)

This section describes how to use the console to create, delete, and manage buckets. 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. One difference, however is that buckets have properties, such as access permissions, versioning status, and you can specify the region where you want them to reside.

## 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 \(p. 33\)](#).

Use the following procedure to create a bucket.



### Note

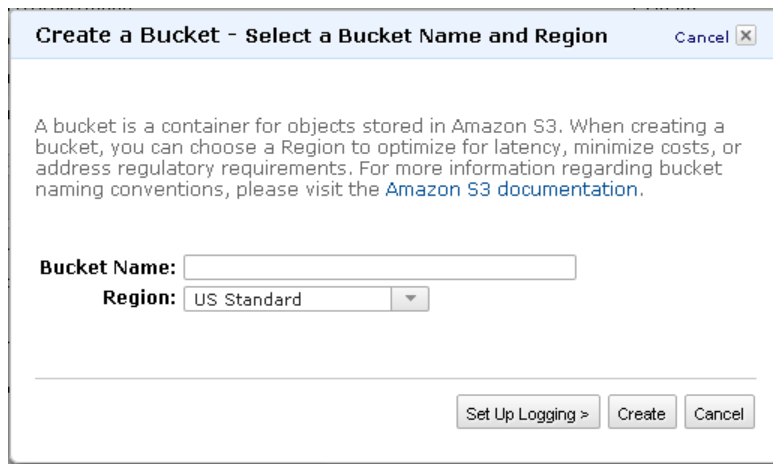
You are not charged for creating a bucket; you are only charged for storing objects in the bucket and for transferring objects in and out of the bucket.

### To create a bucket

1. Go to the [AWS Management Console](#) web page.

2. In the drop-down list box, select **Amazon S3** and click **Sign in to the AWS Console**.
3. On the Amazon S3 tab, click **Create Bucket**.

The **Create a Bucket** dialog box appears.



4. Enter a bucket name in the **Bucket Name** field.

The bucket name you choose must be unique across all existing bucket names in Amazon S3. One way to do that is to prefix your bucket names with your company's name.

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. Bucket names:

- 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.

5. In the **Region** drop-down list box, select a region.

By default, Amazon S3 creates buckets in the US-Standard region. 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.

6. Do one of the following.

To...	Do this...
Create a bucket without setting up logging	Click <b>Create</b>
Set up server access logging for the bucket you're creating	Click <b>Set Up Logging&gt;</b>



### Note

There is no extra charge for enabling the 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](#).

7. If you clicked **Set Up Logging**, the **Create a Bucket - Set Up Logging** dialog box appears so that you can set up logging:

**Create a Bucket - Set Up Logging** Cancel

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

**Enabled:** ☒

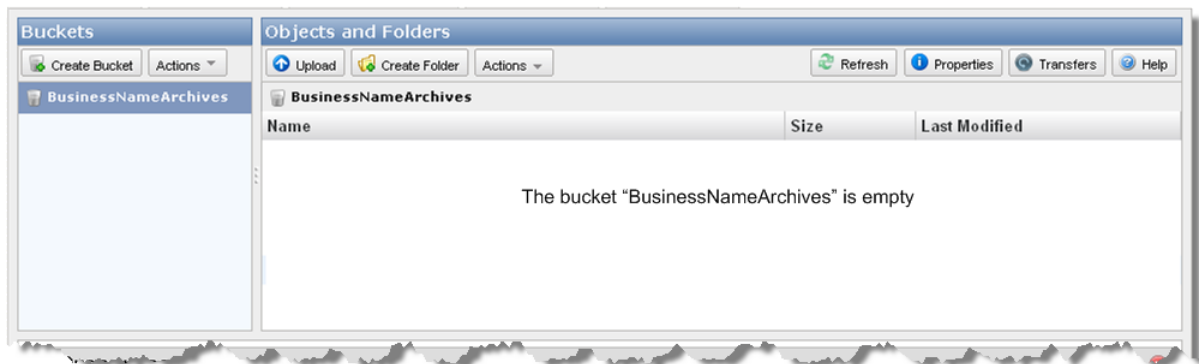
**Target Bucket:** BusinessNameArchives

**Target Prefix:** logs/

< Select Bucket Name And Region Create Cancel

- a. Select the **Enabled** check box.  
This choice enables logging.

- b. In **Target Bucket**, select the bucket where you want the log files stored.
  - c. In **Target Prefix**, you have the option of specifying 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.
8. Click **Create**.
- If Amazon S3 successfully creates your bucket, the console displays your empty bucket.



## 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 & Folders** panel lists the objects and folders in the selected bucket.

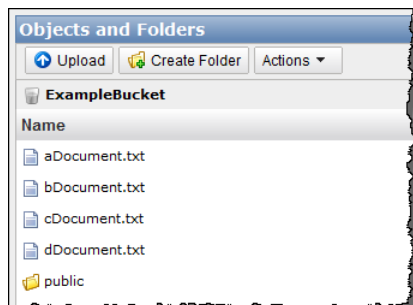


#### Note

If you have a large number of objects in a bucket, you can scroll down to the bottom of the **Objects and Folders** panel, and 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.

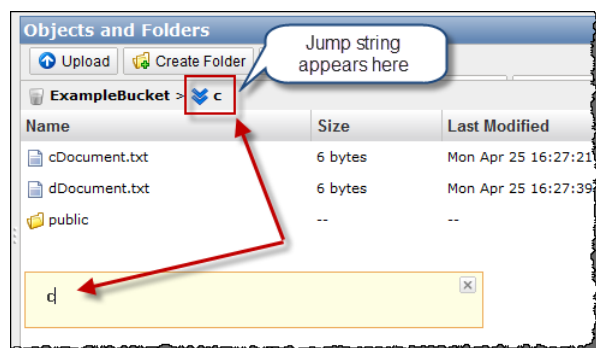
For example, assume you have a bucket (ExampleBucket) with the following objects.



### To jump to an object in your list

1. Click the bucket name to display 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 breadcrumb

The resulting console is shown in the following illustration:



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 **c** shown in the preceding example screenshot) remain.
  - **Press ESC**—This cancels the *jump* operation and the *jump* dialog box closes.



#### Tip

You can always return to the top of the list by pressing **Backspace** key.

## Managing Bucket Logging

This section describes how to use the console to enable and disable logging for a bucket. 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.

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. In the AWS Management Console, select the bucket whose logging you want to enable or disable.
2. Click the **Properties** button.  
The **Properties** dialog box opens.

The screenshot shows the 'Logging' tab of the 'Properties' dialog box. It contains an 'Enabled' checkbox, a 'Target Bucket' dropdown menu, and a 'Target Prefix' text input field. At the bottom right, there are 'Save' and 'Cancel' buttons.

3. Click the **Logging** tab.
4. Select the **Enabled** check box to enable logging, or clear the **Enabled** check box to disable logging.
5. Optionally, in **Target Bucket** choose a bucket to save your log files to, and in **Target Prefix** enter a prefix to prepend to your log file names.  
Amazon S3 adds the prefix to the log file names when storing them in 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**.

## Managing Bucket Website Configuration

This section describes how to use the console to manage website configuration of your bucket. For more information on Amazon S3 website feature, go to [Hosting Websites on Amazon S3](#) in the *Amazon Simple Storage Service Developer Guide*.

#### To manage a bucket's website configuration

1. On the AWS Management Console's Amazon S3 tab, select the bucket whose properties you want to view.
2. Click the **Properties** button on the **Buckets and Folders** panel.  
A new panel opens at the bottom of the page.

Permissions Website Logging Notifications

You can [host your static websites](#) entirely out of Amazon S3. Once your bucket has been configured as a website, you can access all your content via the Amazon S3 website endpoint for your bucket.

Enabled: ☒

Index Document:

Error Document:

Endpoint:

Save Cancel

3. Make sure the **Website** tab is visible as shown in the previous step.
4. Select the **Enabled** check box to enable website on the bucket.
5. Provide an index document name in the **Index Document Suffix** field.  
You must provide an index document name when adding website configuration to the bucket.
6. Provide an error document name in the **Error Document Key** field.  
The error document is optional for adding website configuration to the bucket.
7. Click **Save**.



#### Note

If you clear the Enabled check box, Amazon S3 removes any existing website configuration from the bucket, and the bucket is not accessible via the website endpoints.

## Editing Bucket Permissions

This section describes how to use the console to edit a bucket's permissions for other users (called grantees). Bucket permissions specify who can access the objects in a bucket and what permissions they have. For example, one grantee might only have read permissions while another might have read and write permissions.

### To edit a bucket's permissions

1. On the AWS Management Console's Amazon S3 tab, select the bucket whose properties you want to view.
2. Click the **Properties** button on the **Buckets and Folders** panel.  
A new panel opens at the bottom of the page.

Permissions Website Logging Notifications

Grantee:

☒ List ☒ Upload/Delete ☒ View Permissions ☒ Edit Permissions X

Add more permissions Remove selected permissions Add bucket policy

Save Cancel

3. On the **Permissions** tab do one of the following:

To...	Do this...
Change an existing permission	Select or clear the check boxes next to the permissions you want to grant (selected) or remove (cleared).
To add permissions for a person or group	<ol style="list-style-type: none"><li>Click <b>Add more permissions</b>. A new line appears in the list.</li><li>In <b>Grantee</b>, add the name of the person or group you want to set permissions for. To add grantees, you can enter the e-mail addresses that they used when getting an AWS account, canonical ID, or group name. (You can add up to 100 grantees.)</li><li>Select the check boxes next to the permissions you want to grant.</li></ol>
To remove a person or group from the permission list	Select the "X" on the line of the grantee you want to remove.

There are built-in group accounts 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 object

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

- **List**—Enables the account to list the objects in the bucket
- **Upload/Delete**—Enables the account to access the object when they logged in
- **View Permissions**—Can view the permissions associated with the object
- **Edit Permissions**—Can edit the permissions associated with the object



### Caution

We highly recommend that you do not grant the Everyone group **Upload/Delete** access to your buckets because you will have no control over the objects others can store and their associated charges.

4. Click **Save**.

## Enabling RRS Lost Object Notifications

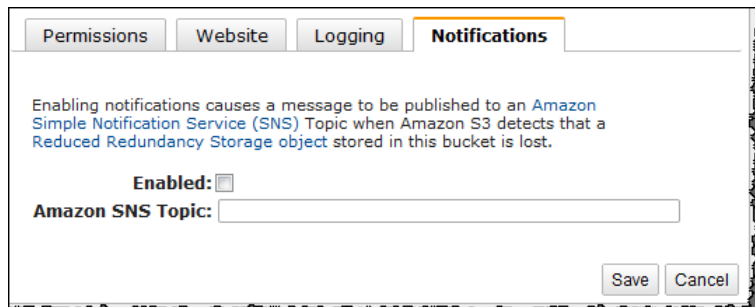
You can configure bucket properties to enable event notifications that are sent to an Amazon Simple Notification Server (SNS) topic. The SNS topic subscribers receive the notifications. Currently Amazon S3 only sends a notification in the event that Amazon S3 detects that a Reduced Redundancy Storage (RRS) object has been lost.

This section describes how to use the console to enable notifications. You can also use the API to enable bucket notifications. For more information, see [Setting Up Notification of Bucket Events](#).

Enabling bucket notifications requires an existing Amazon SNS topic where notifications can be published, in case of an event. 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 bucket notifications

1. On the AWS Management Console's **Amazon S3** tab, select the bucket whose properties you want to view.
2. Click the **Properties** button on the **Buckets and Folders** panel.  
A new panel opens at the bottom of the page. Click the **Notifications** tab.



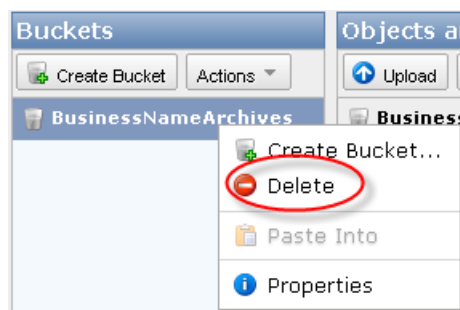
3. Select the **Enabled** check box to enable notifications, or clear the **Enabled** check box to disable notifications.
4. In **Amazon SNS Topic** textbox specify the Amazon SNS Topic name. The name must follow a specific format. To learn more about the Amazon SNS topic format, go to <http://aws.amazon.com/sns/faqs/#10>
5. Click **Save**. All subscribers to the Amazon SNS topic will receive a test notification to verify that messages can be published.

## Deleting a Bucket

This section describes how to use the console to delete one of your buckets. You can only delete an empty bucket. If there are objects in the bucket, you must delete them before deleting the bucket. For more information about deleting objects, see [Deleting an Object \(p. 32\)](#).

### To delete a bucket

1. On the AWS Management Console, select the Amazon S3 tab, and then right-click the bucket you want to delete.  
A drop-down list opens showing the actions you can take on the selected bucket.



2. Click **Delete**.

3. Click **OK** when prompted to confirm the deletion.

# Working with Objects

---

## Topics

- [Uploading Objects into Amazon S3 \(p. 19\)](#)
- [Editing Object Properties \(p. 24\)](#)
- [Opening an Object \(p. 29\)](#)
- [Downloading an Object \(p. 29\)](#)
- [Copying an Object \(p. 30\)](#)
- [Deleting an Object \(p. 32\)](#)

This section describes how to use the console to create, manage, and delete objects. 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. The maximum size of an object is 5 TB. You can have an unlimited number of objects in a bucket.

## Uploading Objects into Amazon S3

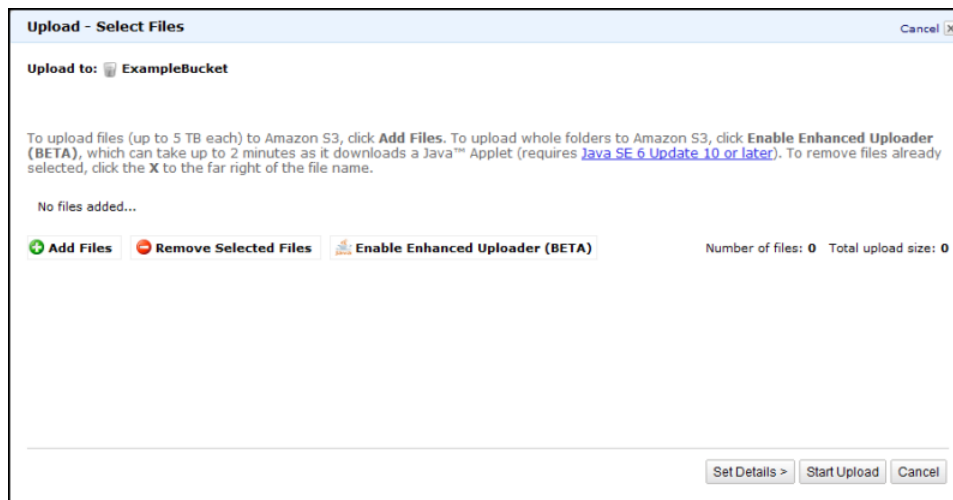
This section describes how to use the AWS Management Console to upload one or more files or entire folders into Amazon S3. Amazon S3 stores all files in the specified bucket.

If you choose to upload a folder, Amazon S3 uploads all the files and subfolders from the specified folder to your bucket, and 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`, then Amazon S3 uploads the files and assigns the corresponding object key names `images/sample1.jpg`, and `images/sample2.jpg`. Note that the key names include the folder name prefix.

If you choose to upload one or more files without a folder, Amazon S3 uploads the files and assigns the file names as the key values for the objects created.

### To upload files and folders into Amazon S3

1. On the Amazon S3 tab in the [AWS Management Console](#), click the bucket you want to upload one or more files or folders into, and then click **Upload** in the **Objects and Folders** panel.  
The **Upload - Select Files** wizard opens as shown in the following sample wizard in Firefox:



- If you want to upload a folder you must click **Enable Enhanced Uploader** for the Java applet. After you download the Java applet, the **Enable Enhanced Uploader** link disappears from the wizard. You only need to do this once per console session and you can transfer entire folders.

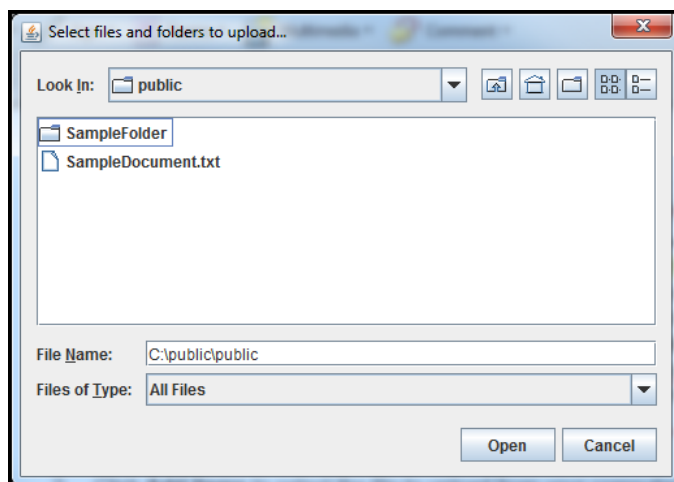


#### Note

If you are behind any corporate firewall you will need to install your corporate supported proxy client for the Java applet to work.

- Click **Add Files** on the **Upload Files and Folders** wizard to select the files and folders to upload from your computer.  
A file selection dialog box opens:
  - If you enabled the advanced uploader in step 2, you see a Java file selection dialog box.
  - If you didn't, you see an operating-system specific dialog box.

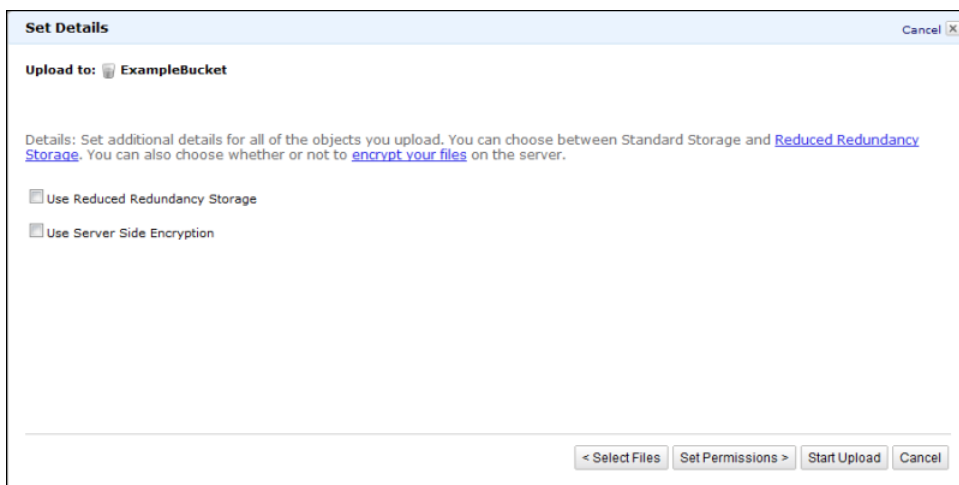
The following image shows a sample Java file selection dialog box.



- Select the files and folders you want to upload and click **Open**.  
The **Upload - Select Files and Folders** wizard shows the files and folders that you have selected to upload.
- Choose one of the following options:

To...	Do this...
Upload objects now	Click <b>Start Upload</b> . Your upload begins immediately and you're done. Skip the rest of the procedure.
Set details on the objects	Click <b>Set Details</b> . The <b>Set Details</b> window opens. Continue to the next step.
Set permissions on the objects	Click <b>Set Details</b> . The <b>Set Details</b> window opens. Continue to step 7.
Set metadata for your objects	Click <b>Set Details</b> . The <b>Set Details</b> window opens. Click <b>Set Permissions</b> and continue to step 8.

6. Set additional details for all of the objects that you upload. You can choose to reduce the level of data redundancy for non-critical files. You can also choose whether or not to encrypt your files on the server.



- a. If you want to use Reduced Redundancy Storage for the object, select the **Use Reduced Redundancy Storage** check box.
  - b. If you want to encrypt the object server-side, select the **Use Server Side Encryption** check box.
7. If you want to set permissions, click **Set Permissions**.

The **Set Permissions** window opens so you can add permissions for the uploaded objects. If you want to grant access to other users and groups (the maximum is 100 grants) for the objects you are uploading, click **Add more permissions**:



#### Note

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



- a. If you want to grant read access to anonymous requests, select the **Make everything public** check box on the **Upload - Set Permissions** panel.
- b. If you want to grant access to other users and groups (the maximum is 100 grants) for the objects you are uploading, click **Add more permissions**.

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.

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

8. If you want to set metadata, click **Set Metadata**.

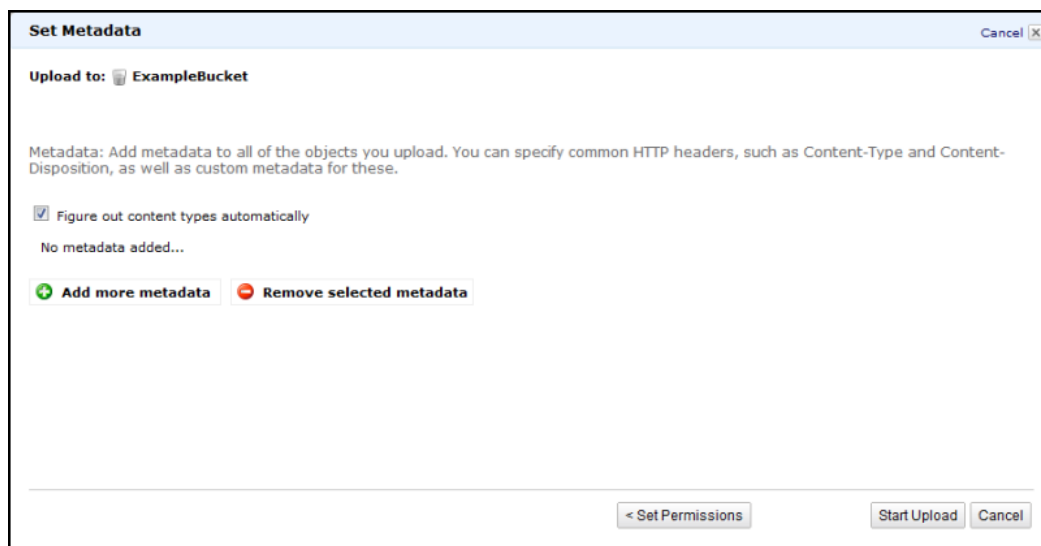
The **Upload - Set Metadata** wizard opens so you can add metadata:

- a. Decide if you want the AWS Management Console to infer the content type of the uploaded objects. By default, **Figure out content types automatically** is checked. This allows the AWS Management Console to infer the content type for all of the objects that you upload based on the file extension associated with the object.
- b. If you don't want the AWS Management Console to infer this, clear the **Figure out content types automatically** check box.

By default, the **Upload Files and Folders - Set Metadata** wizard infers the content type of each uploaded object based on the file extension associated with the object.

- c. Click **Add more metadata** and enter key/value pairs to add metadata.

Amazon S3 object metadata is represented by a key/value pair. There are two types of metadata: system and user. Amazon S3 sometimes processes system metadata (e.g. content-type or content-length), but it never processes user metadata. 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. Any metadata starting with prefix `x-amz-meta-` is considered user-defined metadata. When adding user-defined metadata, select `x-amz-meta-` from the **Key** drop-down list and append the metadata name to it.



9. Click **Start Upload**.  
You can watch the progress of the upload using the **Transfer** panel. The **Transfer** panel appears on the bottom of the screen as soon as you begin the upload.



#### Tip

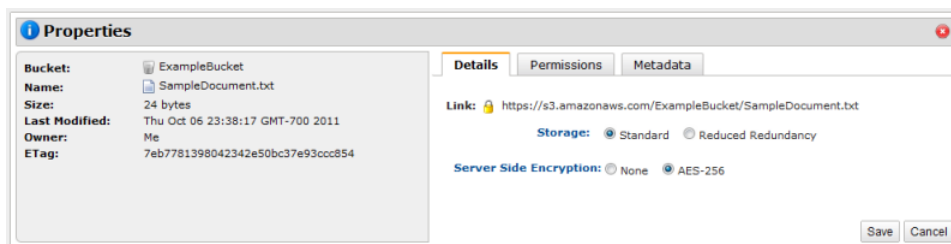
If you want to toggle between hiding and viewing the **Transfer** panel, click the **Transfers** button in the top right of the **Objects and Folders** panel.

When objects upload successfully to Amazon S3, they appear in the object listing.

You have now added an object to your bucket.

#### To view file content and properties

1. Double-click the object name to view file content.
2. Select the object and click **Properties** to view object properties.  
The **Properties** panel opens where you can see the object's properties, as well as a link to the object in Amazon S3. If you click this link, your browser makes anonymous request for this object. Unless you make the object publicly accessible by granting everyone permission on the object (anonymous access), this request will fail.

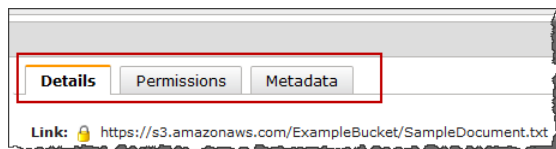


## Editing Object Properties

### Topics

- [Editing Object Details](#) (p. 24)
- [Editing Object Permissions](#) (p. 25)
- [Editing Object Metadata](#) (p. 27)

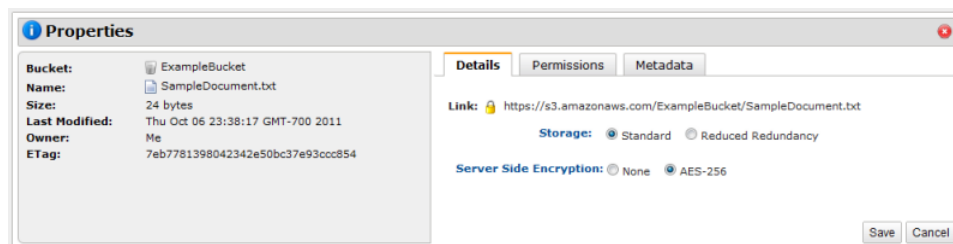
This section describes the properties of an object that you can change and includes the object's details, permissions, and metadata. To access the properties of an object, select the object and either click the **Properties** option in the **Objects and Folders** panel, or select the object and right-click and select **Properties**. When you select a single object, in a bucket you can change all of its properties. When you select multiple objects, you can only change the details of an object. The following example shows the properties panel of a selected object, with the **Details** properties selected.



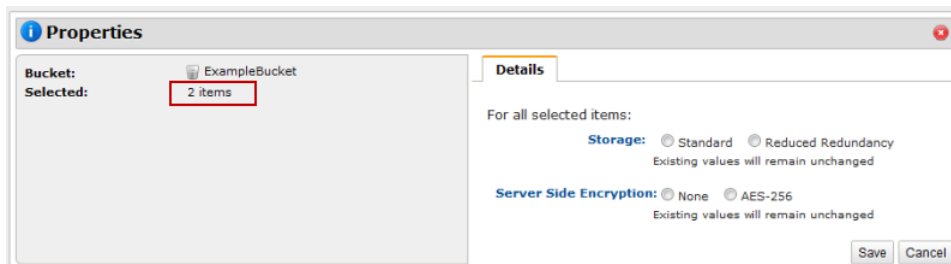
## Editing Object Details

This section describes how to use the console to edit the details of one or more selected objects. The details properties of an object include the object's storage redundancy and the state of server-side encryption. In general, you use Amazon S3 Reduced Redundancy Storage (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](#).

When you select an object in a bucket and click the **Properties** option, the **Details** property panel for the object appears. In the properties panel, you can change the **Storage** (storage redundancy) property or **Server Side Encryption** property of the object and click **Save** to save change to the properties. The following example shows the details properties for an object.



When you select two or more objects in a bucket and click the **Properties** option, the **Details** property panel displayed shows no selections for **Storage** or **Server Side Encryption**, 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 stored encrypted. The following example shows the properties panel for two selected items.



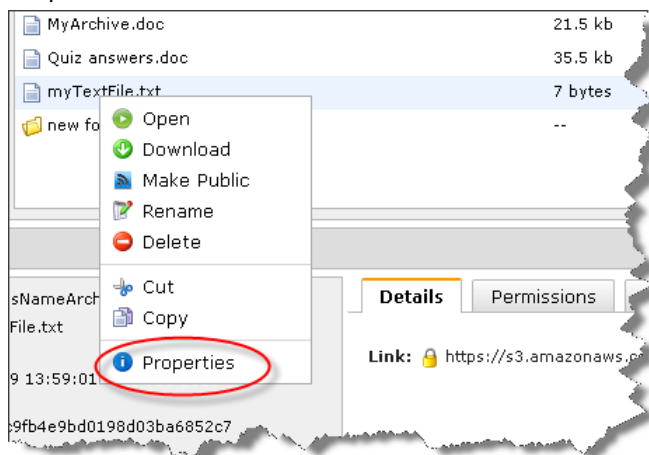
## Editing Object Permissions

This section describes 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 might like to give others read-only permission. 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. On the Amazon S3 tab of the AWS Management Console, right-click the object you want to change the permissions for.



2. Click the **Properties** option.  
The **Property** panel appears on the bottom of the screen.
3. Click the **Permissions** tab.  
The permissions for the grantee appears.

4. 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	<p>a. Click <b>Add more permissions</b>.</p> <p>A new line appears in the list.</p> <p>b. In <b>Grantee</b>, add the e-mail address of the person or group that you want to set permissions for. Use the same e-mail address the person or group used to set up an AWS account.</p> <p>c. Select or clear the check boxes next to the permissions you want to grant (select).</p>
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 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:

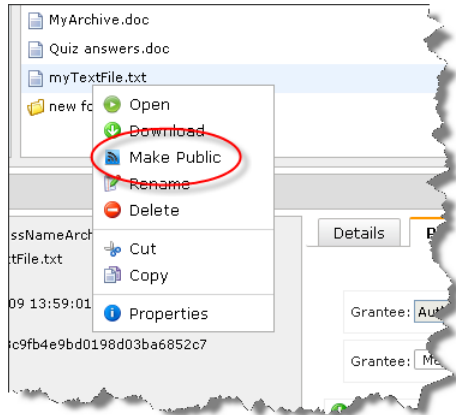
- **Open/Download**—Enables the account to access the object when they are logged in
- **View Permissions**—Can view the permissions associated with the object
- **Edit Permissions**—Can edit the permissions associated with the object

5. Click **Save**.

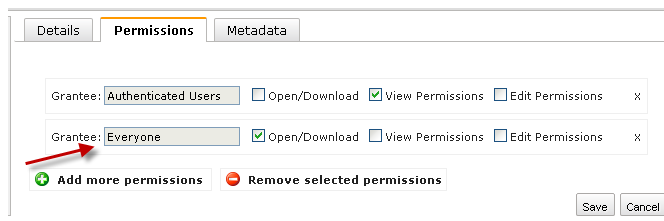
The console provides a shortcut for making objects accessible to everyone, meaning that everyone can both view and download the object.

### To make an object accessible by everyone

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



2. In the drop-down list, click **Make Public**.  
The **Properties** panel displays and shows a new grantee, **Everyone**, that has **Open/Download** permissions.



## Editing Object Metadata

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

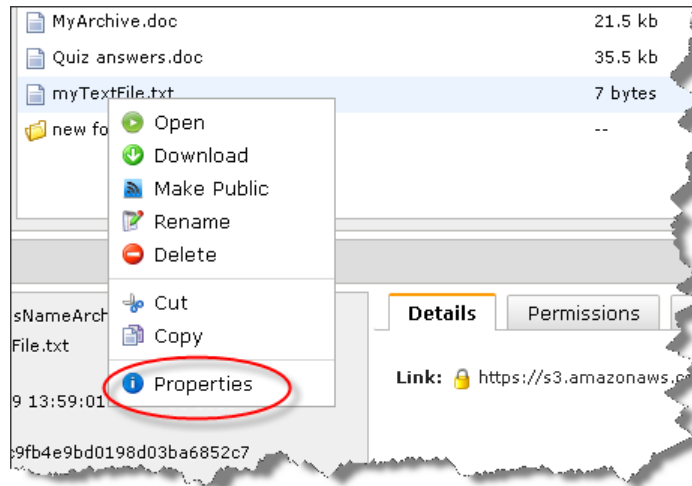
Each object in Amazon S3 has a set of key/value pairs that represents its metadata. There are two types of metadata:

- **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.

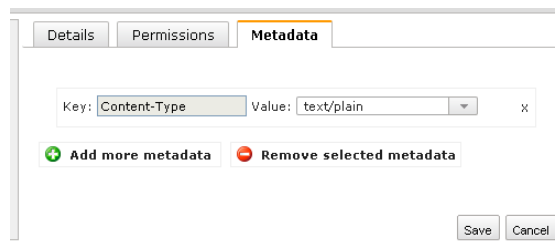
### To edit the metadata of an object

1. On the Amazon S3 tab in the AWS Management Console, right-click the object whose metadata you want to edit.



2. Click the **Properties** option.

The **Property** panel appears on the bottom of the screen.



3. Click the **Metadata** tab in the **Properties** panel.
4. Do one of the following:

To...	Do This...
Add metadata	<ol style="list-style-type: none"> <li>a. Click <b>Add more metadata</b>.</li> <li>b. Click the <b>Key</b> drop-down list box and select or enter a key. Instead of, or in addition to, selecting an entry in the drop-down list, you can enter a key. For example, you can enter x-amz-storage-class in the text box.</li> <li>c. Enter a value in the corresponding <b>Value</b> text box. You can choose from the drop-down list or enter a value, for example, REDUCED_REDUNDANCY.</li> </ol>
Delete metadata	<ol style="list-style-type: none"> <li>a. Click the key/value pair that you want to remove.</li> <li>b. Click <b>Remove selected metadata</b> or click the "X" on the line of the key/value pair that you want to remove.</li> </ol>

5. Click **Save**.

## Opening an Object

This section describes how to use the console to open an object. Opening an object enables you to view it in a browser.

### To open an object

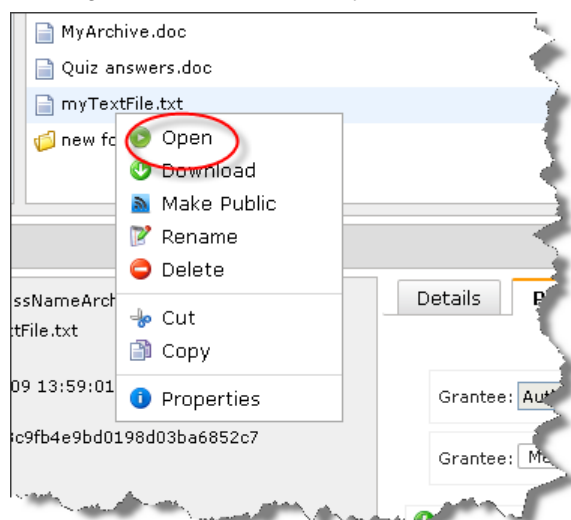
1. On the Amazon S3 tab in the [AWS Management Console](#), right-click the object you want to open.



#### Tip

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

A dialog box shows the actions you can take on the selected object.



2. Click **Open**.  
The object opens in your browser.

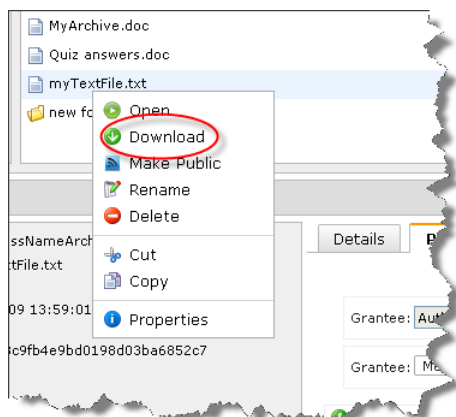
## Downloading an Object

This section describes how to use the console to download an object from Amazon S3 to your computer. Data transfer fees apply when you download objects.

### To download an object

1. On the Amazon S3 tab, in the [AWS Management Console](#), right-click the object you want to download.  
A dialog box displays.

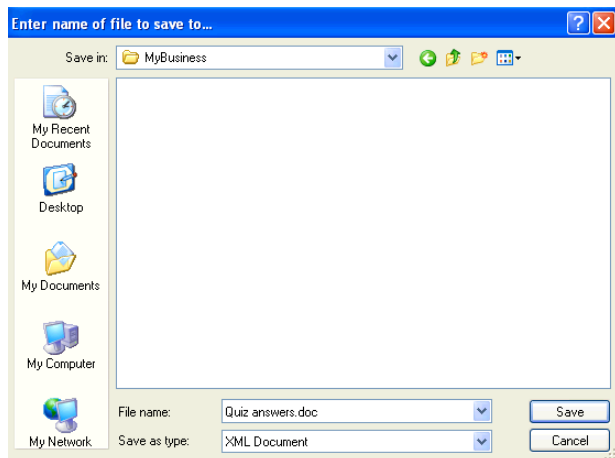




2. In the dialog box, click **Download**.  
The download wizard appears.



3. Right-click the word **download** and click **Save Link As...**  
A dialog box appears.



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

## Copying an Object

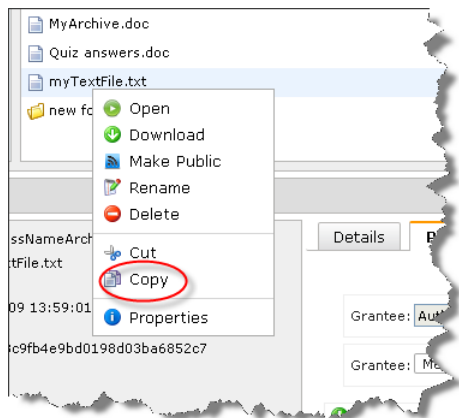
This section describes how to use the console to copy an object. You can also move an object from one place to another by copying (or cutting) it from one place and pasting it into another.

### To copy an object

1. On the Amazon S3 tab, in the AWS Management Console, right-click the object you want to copy.

A dialog box shows the actions you can take on the selected object(s).

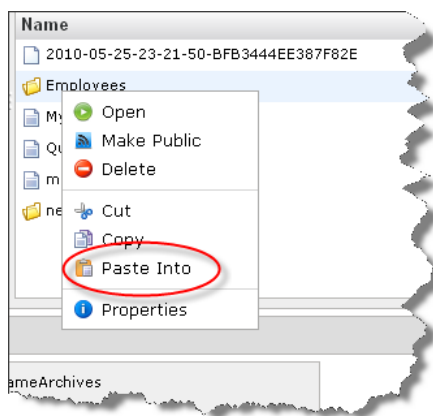
2. Click **Copy**.



#### Note

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

3. Navigate to the bucket (and folder) you want to copy the object to and right-click the target location.
4. Click **Paste Into**.



#### Note

The **Paste Into** option only appears when there is something on the clipboard to paste.

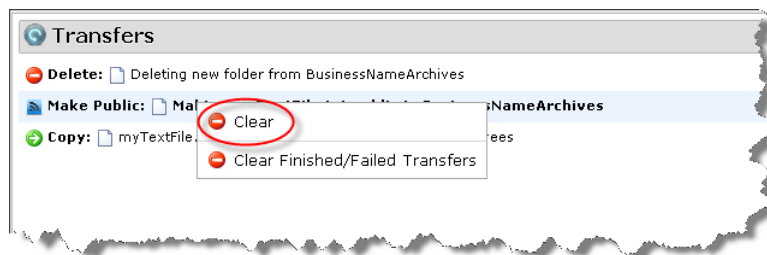
You can monitor the progress of the copy using the **Transfer** panel. To hide or show the **Transfer** panel, click the **Transfers** button at the top right of the console page





### Note

You can clear individual line items in the **Transfers** panel by right-clicking them and selecting **Clear**. To remove all finished or failed transfers, select **Clear Finished/Failed Transfers**.

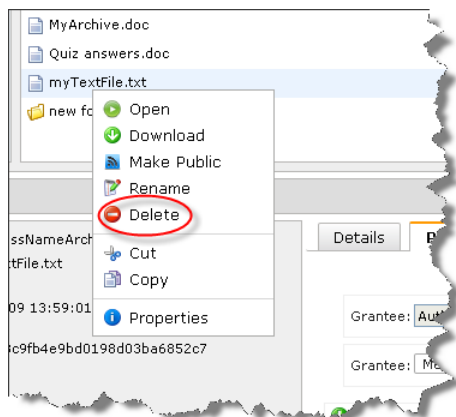


## Deleting an Object

This section describes how to use the console to delete an object. You typically delete objects you no longer need because all objects incur storage costs; deleting unneeded objects reduces your costs. If you are collecting log files, for example, it's a good idea to delete them when they're no longer valuable.

### To delete an object

1. On the Amazon S3 tab, in the AWS Management Console, right-click the object you want to delete. A dialog box shows the actions you can take on the selected object(s).



2. Click **Delete**.
3. Click **OK** when prompted to confirm the deletion.

# Working with Folders

---

## Topics

- [Creating a Folder \(p. 33\)](#)
- [Deleting a Folder \(p. 34\)](#)

The AWS Management Console allows you to create folders, which you can use to group your objects. Just like in a file system, a folder 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`.

You can have folders within folders. (You cannot have buckets within buckets.) You can upload and copy objects directly into a folder.

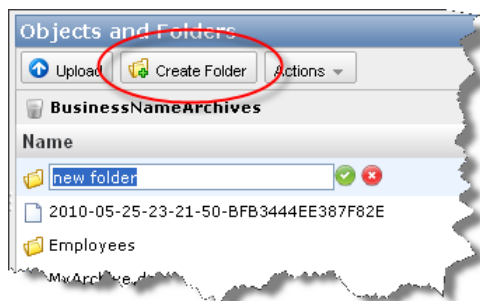
## Creating a Folder

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

### To create a folder

1. Click on the bucket you want to create a folder in.
2. Click **Create Folder**.

The folder appears in the console.



3. In the text entry box, name the folder.

## Deleting a Folder

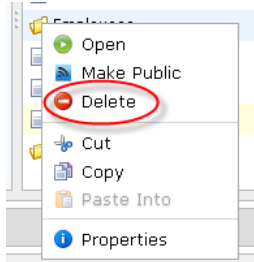
This section describes how to use the console to delete a folder.



### Caution

Unlike a bucket, you can delete a folder without first deleting its contents. Any objects or folders contained in the folder will be deleted automatically when you delete the folder.

1. Right-click the folder you want to delete.  
A dialog box opens.



2. Click **Delete**.
3. Click **OK** when prompted to confirm the deletion.

# Amazon S3 Resources

---

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

Resource	Description
<a href="#">Amazon S3 Getting Started Guide</a>	The Getting Started Guide provides a quick tutorial of the service using the AWS Management Console to accomplish basic Amazon S3 tasks.
<a href="#">Amazon S3 API Reference</a>	The API Reference describes Amazon S3 operations in detail.
<a href="#">Amazon S3 Developer Guide</a>	The developer guide describes how to use Amazon S3 operations.
<a href="#">Amazon S3 Technical FAQ</a>	The FAQ covers the top 20 questions developers have asked about this product.
<a href="#">Amazon S3 Release Notes</a>	The Release Notes give a high-level overview of the current release. They specifically note any new features, corrections, and known issues.
<a href="#">AWS Developer Resource Center</a>	A central starting point to find documentation, code samples, release notes, and other information to help you build innovative applications with AWS.
<a href="#">AWS Management Console</a>	The console allows you to perform Amazon S3 functions using a simple and intuitive web user interface.
<a href="#">Discussion Forums</a>	A community-based forum for developers to discuss technical questions related to Amazon Web Services.
<a href="#">AWS Support Center</a>	The home page for AWS Technical Support, including access to our Developer Forums, Technical FAQs, Service Status page, and Premium Support.
<a href="#">AWS Calculator</a>	Use the AWS calculator to estimate your monthly charges for using AWS services.
<a href="#">AWS Premium Support</a>	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
<a href="#">Amazon S3 product information</a>	The primary web page for information about Amazon S3.
<a href="#">Contact Us</a>	A central contact point for inquiries concerning AWS billing, account, events, abuse etc.
<a href="#">Conditions of Use</a>	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 17 October 2011.

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

Change	Description	Date
Documentation Update	This release includes enhancements to the object properties related sections. Information about what the <b>Details</b> properties tab show when you select one or more objects. For more information, see <a href="#">Editing Object Properties (p. 24)</a> .	In this release.
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 <a href="#">Uploading Objects into Amazon S3 (p. 19)</a> . For more information about server-side encryption for data stored in Amazon S3, see <a href="#">Using Server-Side Encryption</a> in the <i>Amazon S3 Developer Guide</i> .	5 October 2011
AWS Management Console enhancements	<p>This release includes the following AWS Management Console enhancements:</p> <ul style="list-style-type: none"><li>• <b>Folder upload</b>—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 <a href="#">Uploading Objects into Amazon S3 (p. 19)</a></li><li>• <b>Jump feature</b>—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 <a href="#">Browsing the Objects in Your Bucket (p. 12)</a></li></ul>	6 June 2011



Change	Description	Date
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., <a href="http://mywebsite.com/subfolder">http://mywebsite.com/subfolder</a> ) 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 <a href="#">Managing Bucket Website Configuration (p. 14)</a> . For more information about Amazon S3's website configuration feature, go to <a href="#">Hosting Websites on Amazon S3</a> in the <i>Amazon Simple Storage Service Developer Guide</i> .	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 <i>Amazon S3 Console User Guide</i> . 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 <code>photos/puppy.jpg</code> is stored in the <code>johnsmith</code> bucket, then it is addressable using the URL <code>http://johnsmith.s3.amazonaws.com/photos/puppy.jpg</code>
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 <code>ListAllMyBuckets</code> 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 <code>http://doc.s3.amazonaws.com/2006-03-01/AmazonS3.wsdl</code> , 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 <code>PUT Bucket versioning</code> .