Amazon Simple Storage Service

Console User Guide

Amazon Simple Storage Service: Console User Guide

Table of Contents

Welcome to the New Amazon S3 Console User Guide

*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

This is the *Amazon Simple Storage Service Console User Guide* for the new Amazon S3 console.

The Amazon S3 console is one of the interfaces that you can use to work with Amazon S3. The console enables you to perform Amazon S3 tasks without writing any code.

Topics

Creating and Configuring an S3 Bucket

*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

Amazon S3 is cloud storage for the Internet. To upload your data (photos, videos, documents etc.), you first create a bucket in one of the AWS Regions. You can then upload your data objects to the bucket.

Every object you store in Amazon S3 resides in a bucket. You can use buckets to group related objects in the same way that you use a directory to group files in a file system.

Amazon S3 creates buckets in the AWS Region that you specify. You can choose any AWS Region that is geographically close to you to optimize latency, minimize costs, or address regulatory requirements. For example, if you reside in Europe, you might find it advantageous to create buckets in the EU (Ireland) or EU (Frankfurt) regions. For a list of Amazon S3 AWS Regions, see Regions and Endpoints in the *Amazon Web Services General Reference*.

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. For more information about pricing, see Amazon Simple Storage Service (S3) FAQs.

Amazon S3 bucket names are globally unique, regardless of the AWS Region in which you create the bucket. You specify the name at the time you create the bucket. For bucket naming guidelines, see Bucket Restrictions and Limitations in the *Amazon Simple Storage Service Developer Guide*.

The following topics explain how to use the Amazon S3 console to create, delete, and manage buckets.

Topics

How Do I Create an S3 Bucket?

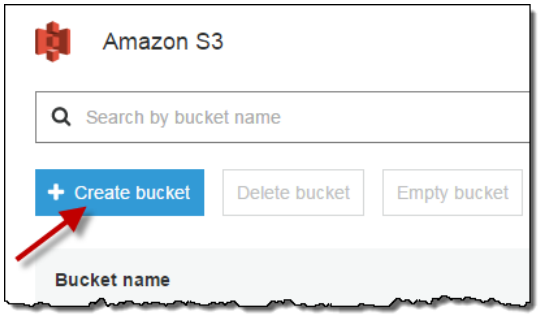
*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

Before you can upload data to Amazon Simple Storage Service, you must create a bucket in one of the AWS Regions to store your data in. After you create a bucket, you can upload an unlimited number of data objects to the bucket.

Buckets have configuration properties, including their geographical region, who has access to the objects in the bucket, and other metadata.

To create an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. Choose **Create bucket**.



3. On the **Name and region** page, type a name for your bucket and choose the AWS Region where you want the bucket to reside. Complete the fields on this page as follows:

   a. For **Bucket name**, type a unique DNS-compliant name for your new bucket. Follow these naming guidelines:

      - The name must be unique across all existing bucket names in Amazon S3.
      - The name must be between 3 and 63 characters long.

- After you create the bucket you cannot change the name, so choose wisely.
- Choose a bucket name that reflects the objects in the bucket because the bucket name is visible in the URL that points to the objects that you're going to put in your bucket.

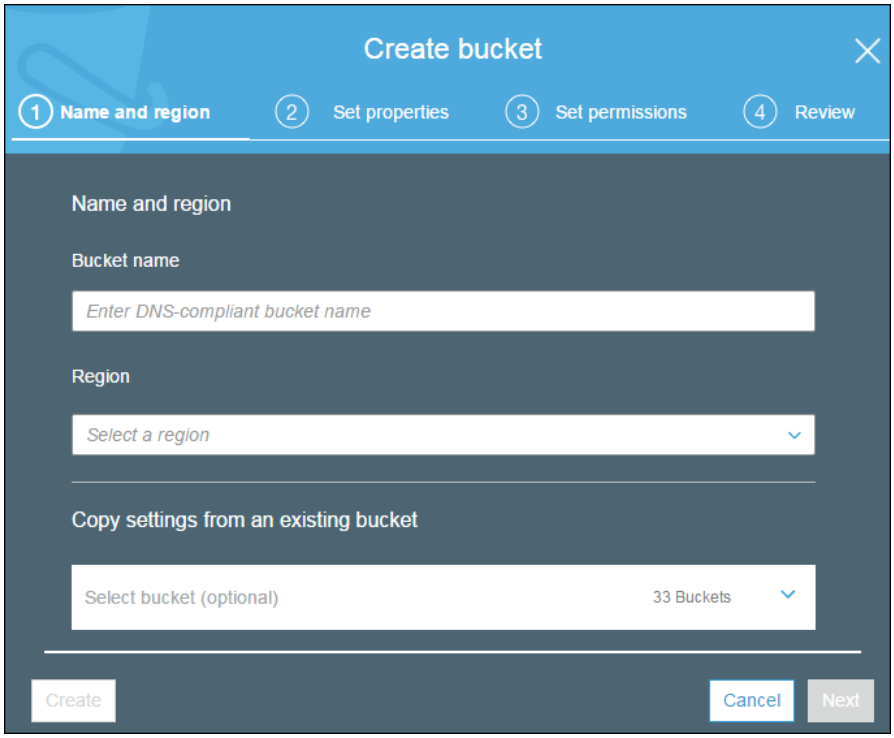
For information about naming buckets, see Rules for Bucket Naming in the *Amazon Simple Storage Service Developer Guide*.

b. For **Region**, choose the AWS Region where you want the bucket to reside. Choose a Region close to you to minimize latency and costs, or to address regulatory requirements. Objects stored in a Region never leave that Region unless you explicitly transfer them to another Region. For a list of Amazon S3 AWS Regions, see Regions and Endpoints in the *Amazon Web Services General Reference*.

c. (Optional) If you have already set up a bucket that has the same settings that you want to use for the new bucket that you want to create, you can set it up quickly by choosing **Copy settings from an existing bucket**, and then choosing the bucket whose settings you want to copy.

d. Do one of the following:

- If you copied settings from another bucket, choose **Create**. You're done, so skip the following steps.
- If not, choose **Next**.



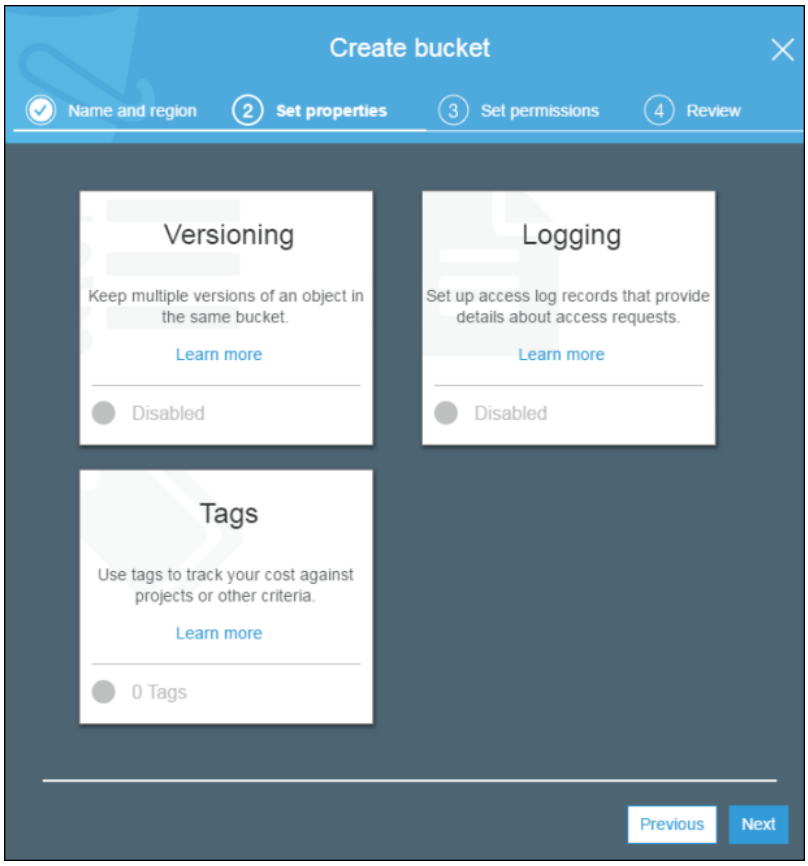
4. On the **Set properties** page, you can configure the following properties for the bucket. Or, you can configure these properties later, after you create the bucket.

a. **Versioning** – Versioning enables you to keep multiple versions of an object in one bucket. Versioning is disabled for a new bucket by default. For information on enabling versioning, see How Do I Enable or Suspend Versioning for an S3 Bucket? (p. 10).

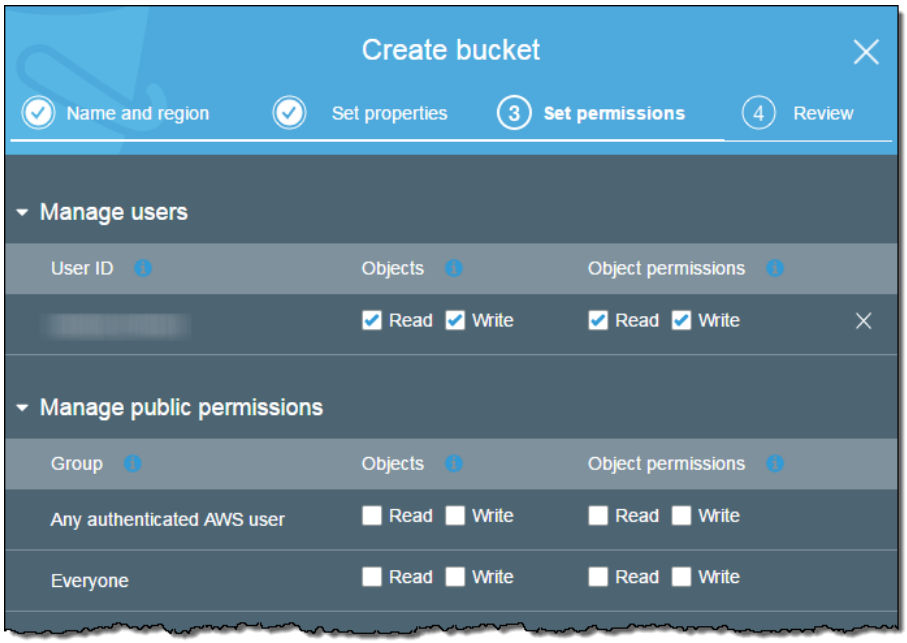
b. **Logging** – Server access logging provides detailed records for the requests made to your bucket. By default, Amazon S3 does not collect server access logs. To enable logging for the bucket, choose **Logging**. To disable logging, choose **Disable logging**. Choose **Save** to save your

settings. For more information, see Server Access Logging in the *Amazon Simple Storage Service Developer Guide*

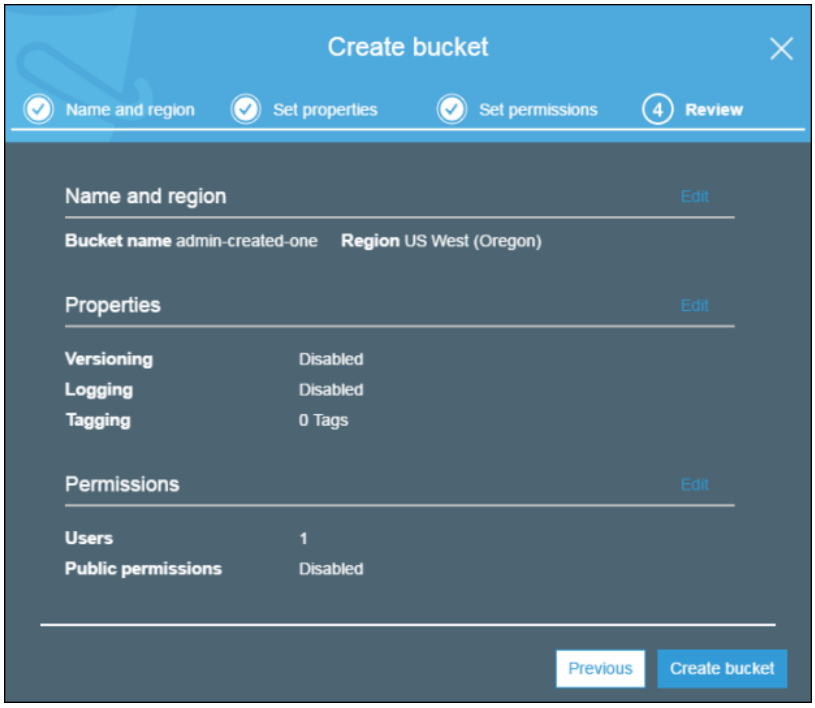
c. **Tags** – With AWS cost allocation, you can use tags to annotate billing for your use of a bucket. A tag is a key-value pair that represents a label that you assign to a bucket. To add tags, choose **Tags**, and then choose **Add tag**.



5. Choose **Next**.
6. On the **Set permissions** page, you manage permissions. You can make changes to permissions after you create the bucket. When you're done configuring permissions on the bucket, choose **Next**.



7. On the **Review** page, verify the settings. If you see something you want to change, choose **Edit**. If your current settings are correct, choose **Create bucket**.



How Do I Delete an S3 Bucket?

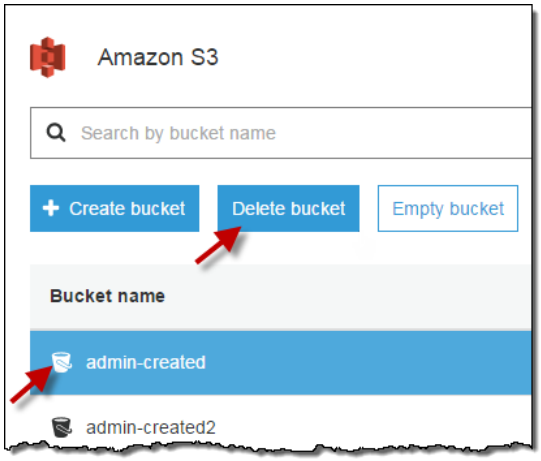
*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

You can delete a bucket and all of the objects contained in the bucket. You can also delete an empty bucket. When you delete a bucket with versioning enabled, all versions of all the objects in the bucket are deleted. For more information, see Managing Objects in a Versioning-Enabled Bucket and Deleting/Emptying a Bucket in the *Amazon Simple Storage Service Developer Guide*.

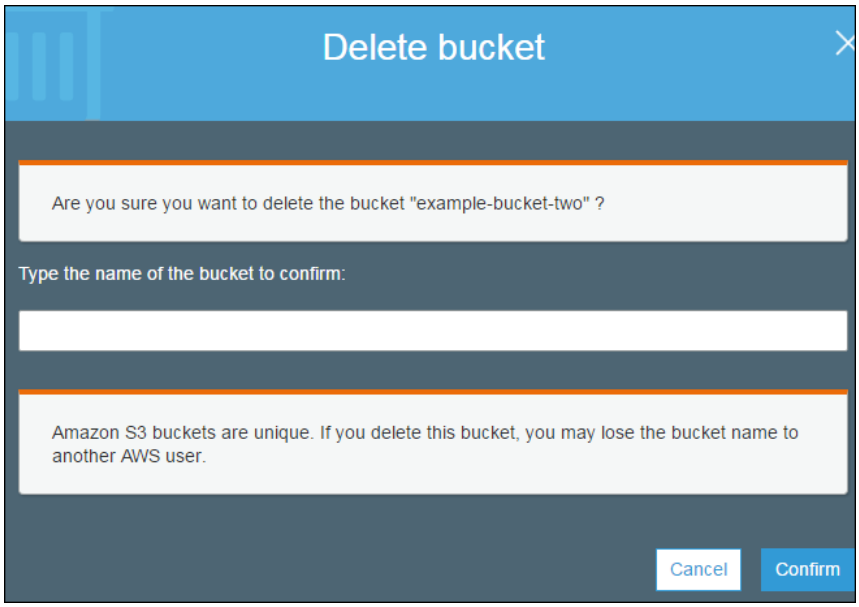
> **Important**
> If you want to continue to use the same bucket name, don't delete the bucket. We recommend that you empty the bucket and keep it. After a bucket is deleted, the name becomes available to reuse, but the name might not be available for you to reuse for various reasons. For example, it might take some time before the name can be reused and some other account could create a bucket with that name before you do.

To delete an S3 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 **Bucket name** list, choose the bucket icon next to the name of bucket that you want to delete and then choose **Delete bucket**.



3. In the **Delete bucket** dialog box, type the name of the bucket that you want to delete for confirmation and then choose **Confirm**.



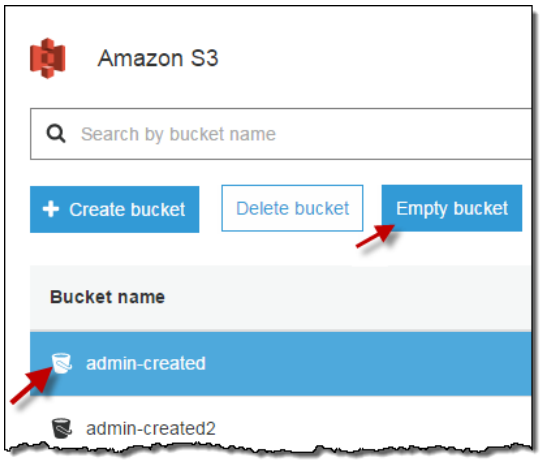
How Do I Empty an S3 Bucket?

*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

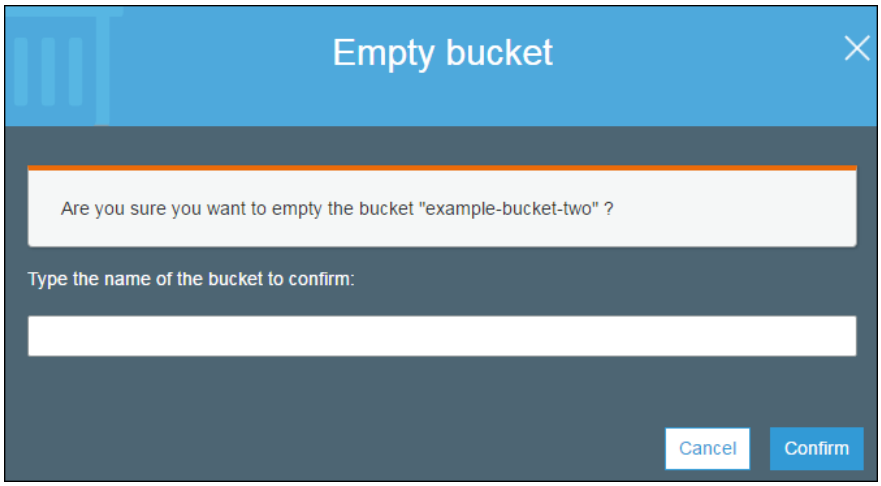
You can empty a bucket, which deletes all of the objects in the bucket without deleting the bucket. When you empty a bucket with versioning enabled, all versions of all the objects in the bucket are deleted. For more information, see Managing Objects in a Versioning-Enabled Bucket and Deleting/Emptying a Bucket in the *Amazon Simple Storage Service Developer Guide*.

To empty an S3 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 **Bucket name** list, choose the bucket icon next to the name of bucket that you want to delete and then choose **Empty bucket**.



3. In the **Empty bucket** dialog box, type the name of the bucket you want to empty for confirmation and then choose **Confirm**.



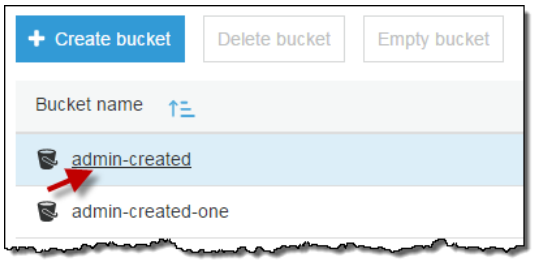
How Do I View the Properties for an S3 Bucket?

*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

This topic explains how to view the properties for an S3 bucket.

To view the properties for an S3 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 **Bucket name** list, choose the name of the bucket that you want to view the properties for.



3. Choose **Properties**.

4. On the **Properties** page, you can configure the following properties for the bucket.

   a. **Versioning** – Versioning enables you to keep multiple versions of an object in one bucket. Versioning is disabled for a new bucket by default. For information on enabling versioning, see How Do I Enable or Suspend Versioning for an S3 Bucket? (p. 10).

   b. **Static website hosting** – You can host a static website on Amazon S3. To enable static website hosting, choose **Static website hosting** and then specify the settings you want to use. For more information, see How Do I Configure an S3 Bucket for Static Website Hosting? (p. 14).

   c. **Logging** – Server access logging provides detailed records for the requests made to your bucket. By default, Amazon S3 does not collect server access logs. For information on enabling server access logging, see How Do I Enable Server Access Logging for an S3 Bucket? (p. 12).

   d. **Tags** – 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. To add tags, choose **Tags** and then choose **Add tag**.

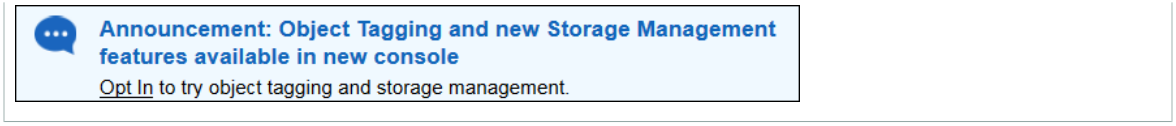
   e. **Cross-region replication** – Enables automatic, asynchronous copying of objects across buckets in different AWS Regions. To enable cross-region replication, choose **Cross-region replication** and then specify the settings you want to use. For more information, see How Do I Enable and Configure Cross-Region Replication for an S3 Bucket? (p. 19).

   f. **Transfer acceleration** – Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. For information on enabling transfer acceleration, see How Do I Enable Transfer Acceleration for an S3 Bucket? (p. 28).

   g. **Events** – You can enable certain Amazon S3 bucket events to send a notification message to a destination whenever the events occur. To enable events, choose **Events** and then specify the settings you want to use. For more information, see How Do I Enable and Configure Event Notifications for an S3 Bucket? (p. 24).

How Do I Enable or Suspend Versioning for an S3 Bucket?

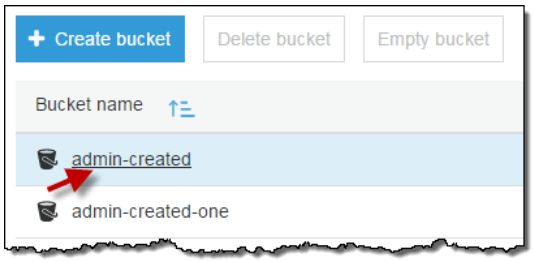
*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*



Versioning enables you to keep multiple versions of an object in one bucket. This section describes how to enable object versioning on a bucket. For more information about versioning support in Amazon S3, see Object Versioning and Using Versioning in the *Amazon Simple Storage Service Developer Guide*.

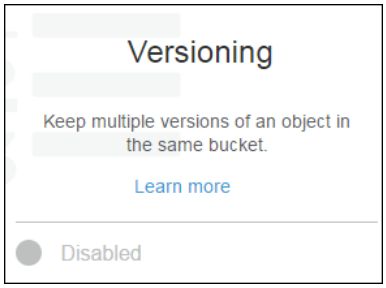
To enable or disable versioning on an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that you want to enable versioning for.

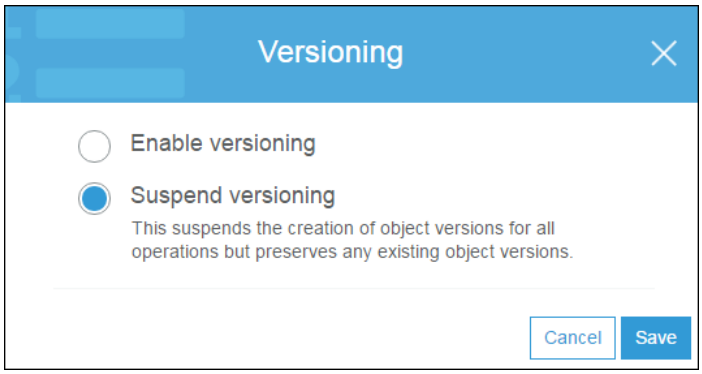


3. Choose **Properties**.

4. Choose **Versioning**.



5. Choose **Enable versioning** or **Suspend versioning**, and then choose **Save**.



How Do I Enable Server Access Logging for an S3 Bucket?

*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

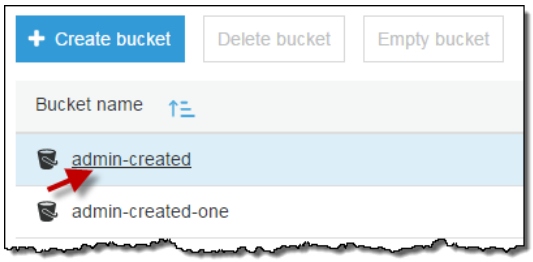
Server access logging provides detailed records for the requests made to a bucket. Server access logs are useful for many applications because they give bucket owners insight into the nature of requests made by clients not under their control. By default, Amazon Simple Storage Service (Amazon S3) doesn't collect server access logs. This topic describes how to enable logging for a bucket. For more information, see Server Access Logging in the *Amazon Simple Storage Service Developer Guide*.

When you enable logging, Amazon S3 delivers access logs to a target bucket that you choose. An access log record contains details about the requests made to a bucket. This can include the request type, the resources specified in the request, and the time and date the request was processed. For more information, see Server Access Log Format in the *Amazon Simple Storage Service Developer Guide*.

> **Important**
> There is no extra charge for enabling server access logging on an Amazon S3 bucket. However, any log files that 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.

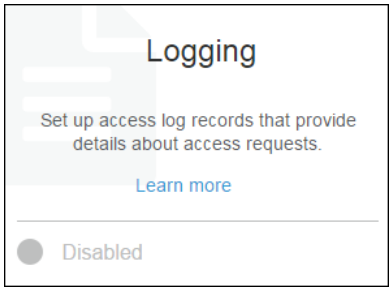
To enable server access logging for an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that you want to enable server access logging for.

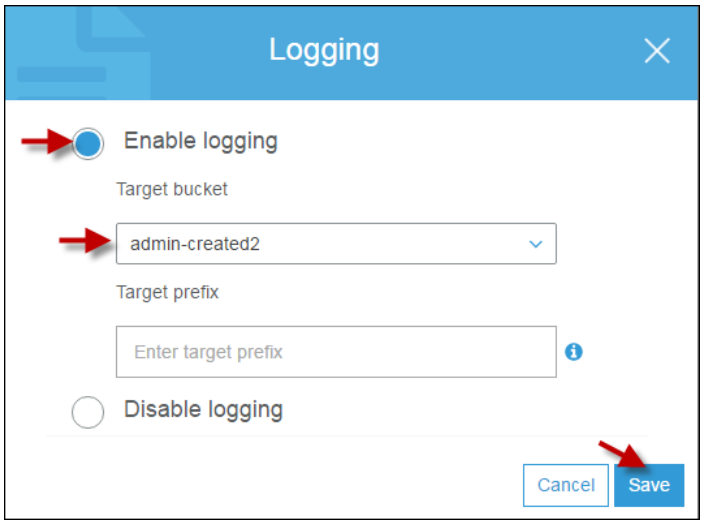


3. Choose **Properties**.

4. Choose **Logging**.



5. Choose **Enable Logging**. For **Target**, choose the name of the bucket that you want to receive the log record objects.



6. (Optional) For **Target prefix**, type a key name prefix for log objects, so that all of the log objects begin with the same string.
7. Choose **Save**.

More Info

- How Do I View the Properties for an S3 Bucket? (p. 9)

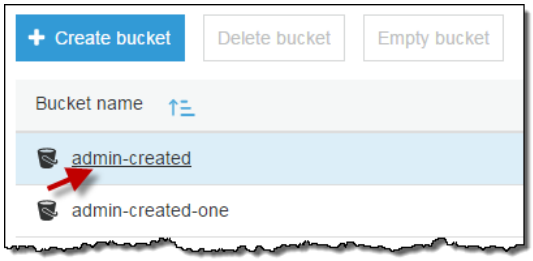
How Do I Configure an S3 Bucket for Static Website Hosting?

*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

You can host a static website on Amazon S3. On a static website, individual web pages include static content and they might also contain client-side scripts. By contrast, a dynamic website relies on server-side processing, including server-side scripts such as PHP, JSP, or ASP.NET. Amazon S3 does not support server-side scripting. For more information, see Hosting a Static Website on Amazon S3 in the *Amazon Simple Storage Service Developer Guide*.

To configure an S3 bucket for static website hosting

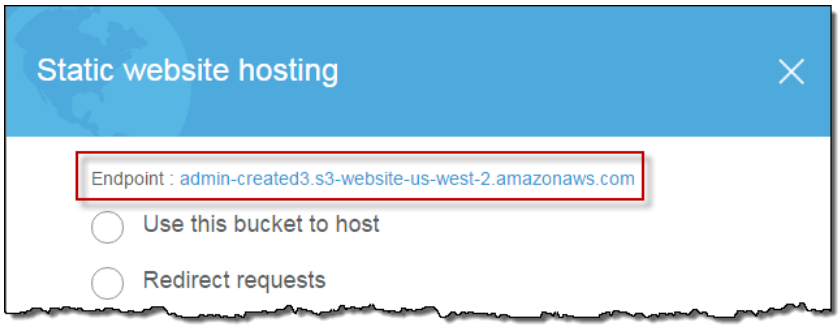
1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that you want to enable static website hosting for.



3. Choose **Properties**.

4. Choose **Static website hosting**.

After you enable your bucket for static website hosting, web browsers can access all of your content through the Amazon S3 website endpoint for your bucket.

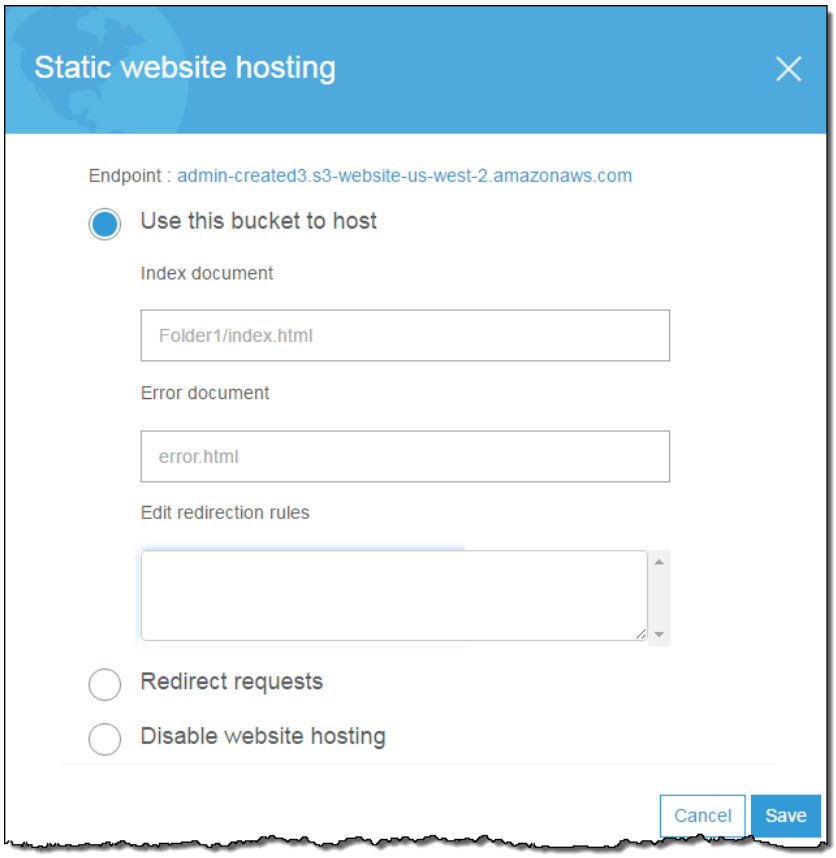


5. Choose **Use this bucket to host**.

   a. For **Index Document**, type the name of the index document, which is typically named index.html. When you configure a bucket for website hosting, you must specify an index document. Amazon S3 returns this index document when requests are made to the root domain or any of the subfolders. For more information, see Configure a Bucket for Website Hosting in the *Amazon Simple Storage Service Developer Guide*.

   b. (Optional) For **Error Document**, type the name of a custom error document. If an error occurs, Amazon S3 returns an HTML error document. For 4XX class errors, you can optionally provide your own custom error document, in which you can provide additional guidance to your users. For more information, see Custom Error Document Support in the *Amazon Simple Storage Service Developer Guide*.

   c. (Optional) For **Edit redirection rules**, describe the rules using XML in the text area if you want to specify advanced redirection rules. For example, you can conditionally route requests according to specific object key names or prefixes in the request. For more information, see Configure a Bucket for Website Hosting in the *Amazon Simple Storage Service Developer Guide*.



6. Choose **Save**.
7. Add a bucket policy to the website bucket to grant everyone access to the objects in the bucket. When you configure a bucket as a website, you must make the objects that you want to serve publicly readable. To do so, you write a bucket policy that grants everyone `s3:GetObject` permission. The following example bucket policy grants everyone access to the objects in the `example-bucket` bucket.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::example-bucket/*"
            ]
        }
    ]
}
```

For information about adding a bucket policy, see How Do I Add an S3 Bucket Policy? (p. 91). For more information, see Permissions Required for Website in the *Amazon Simple Storage Service Developer Guide*.

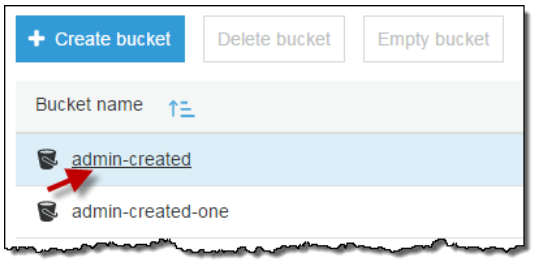
Note
If you choose **Disable website hosting**, Amazon S3 removes any existing website configuration from the bucket, and the bucket is not accessible from the website endpoint. However, the bucket is still available at the REST endpoint. For a list of Amazon S3 endpoints, see Amazon S3 Regions and Endpoints in the *Amazon Web Services General Reference*.

How Do I Redirect Requests to an S3 Bucket Hosted Website to Another Host?

You can redirect all requests to your S3 bucket hosted static website to another host.

To redirect all requests to an S3 bucket's website endpoint to another host

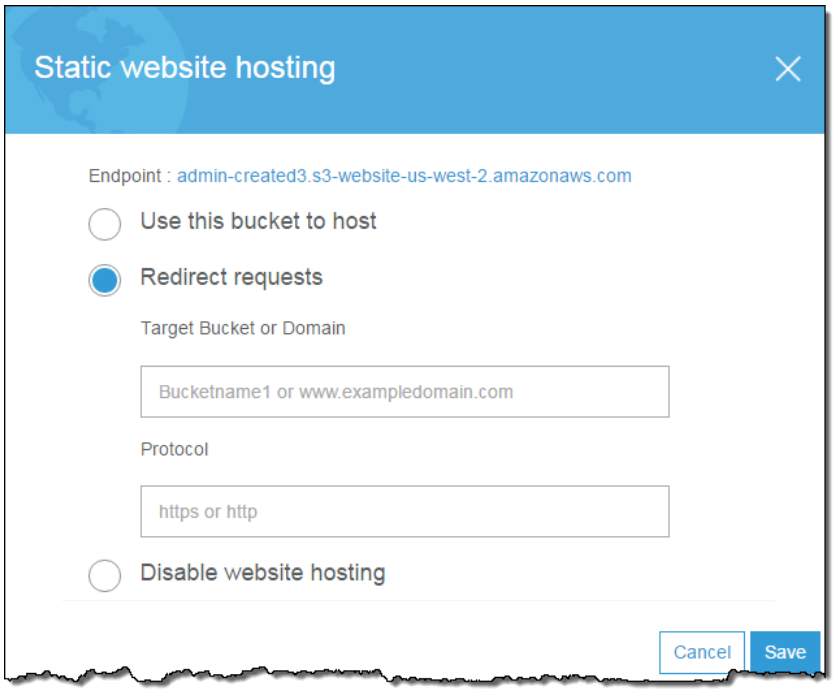
1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that you want to redirect all requests from.



3. Choose **Properties**.

4. Choose **Static website hosting**.

5. Choose **Redirect requests**.



a. For **Target bucket or domain**, type the name of the bucket or the domain name where you want requests to be redirected. To redirect requests to another bucket, type the name of the target bucket. For example, if you are redirecting to a root domain address, you would type **www.example.com**. For more information, see Configure a Bucket for Website Hosting in the *Amazon Simple Storage Service Developer Guide*.

b. For **Protocol**, type the protocol (http, https) for the redirected requests. If no protocol is specified, the protocol of the original request is used. If you redirect all requests, any request made to the bucket's website endpoint will be redirected to the specified host name.

6. Choose **Save**.

Advanced Settings for S3 Bucket Properties

*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

This section describes how to configure advanced S3 bucket property settings for cross-region replication, event notification, and transfer acceleration.

Topics

- How Do I Enable and Configure Event Notifications for an S3 Bucket? (p. 24)
- How Do I Enable Transfer Acceleration for an S3 Bucket? (p. 28)

How Do I Enable and Configure Cross-Region Replication for an S3 Bucket?

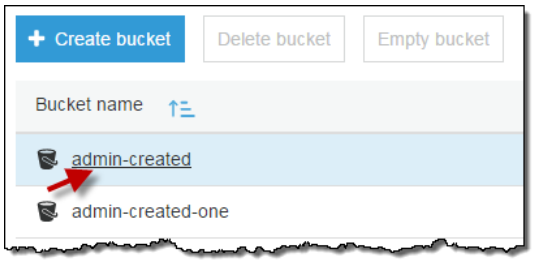
*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

Cross-region replication is the automatic, asynchronous copying of objects across buckets in different AWS Regions. When you enable cross-region replication, Amazon S3 replicates newly created objects, object updates, and object deletions from a source bucket to a destination bucket in a different region. Cross-region replication has specific requirements that define what can and cannot be replicated across regions based on how the object is created and how it is encrypted. For more information, see Cross-Region Replication in the *Amazon Simple Storage Service Developer Guide*.

Cross-region replication requires that versioning must be enabled on both your source bucket and your destination bucket that is in a different region. For more information, see How Do I Enable or Suspend Versioning for an S3 Bucket? (p. 10).

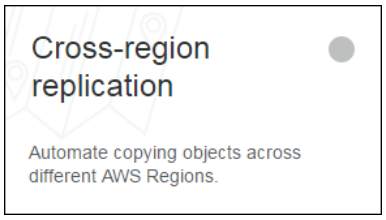
To enable cross-region replication of an S3 bucket to another bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that you want to enable cross-region replication for.



3. Choose **Properties**.

4. Under **Advanced settings**, choose **Cross-region replication**.

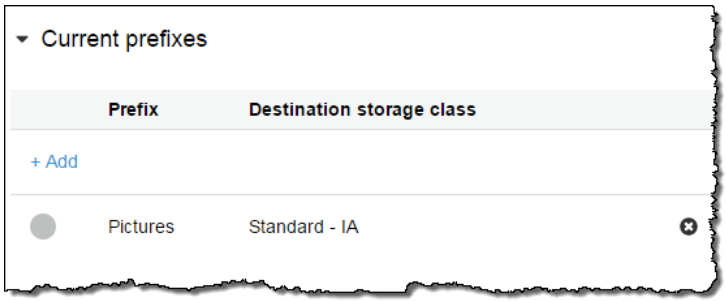


5. Choose **Enable cross-region replication**, and then configure your settings as follows:

   a. For **Destination**, choose the region of the destination bucket and then choose the destination bucket. If you do not see your desired destination bucket in the list, confirm that the bucket exists in the region you selected and that you have enabled versioning on that bucket.

   b. For **Source**, choose **Whole bucket** to replicate the whole bucket or choose **Prefix in this bucket** to replicate all objects with the same prefix (for example, all objects in a specific folder).

      - If you choose **Prefix in this bucket**, choose the arrow next to **Current prefixes**, choose **+Add**, type a prefix to use, and then choose a destination storage class. You can add more than one prefix.

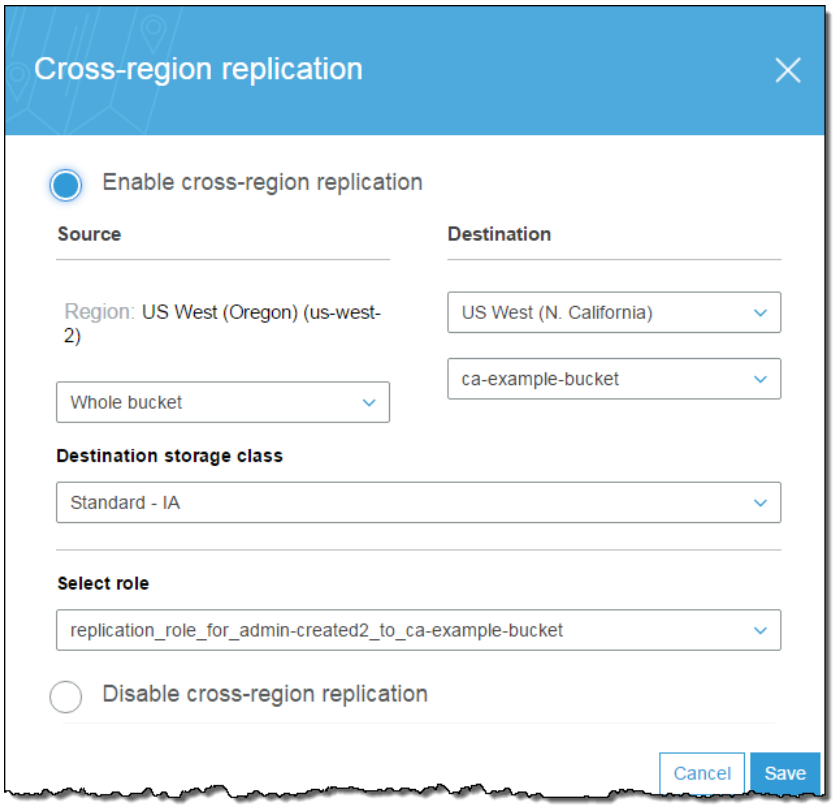


   c. For **Destination storage class**, choose the storage class you want to use for the replicated objects.

   d. To perform cross-region replication of objects on your behalf, you need to set up an AWS Identity and Access Management (IAM) role that Amazon S3 can use. For **Select role**, do one of the following:

      - If you want Amazon S3 to create a new IAM role for you, choose **Create new role** and then choose **Save**. Amazon S3 will generate a policy for the IAM role that matches the source and destination buckets you choose. The generated role is named based on the bucket names using the following naming convention: **replication_role_for_*source-bucket*_to_*destination-bucket***

      - If you want to use an existing IAM role, choose an IAM role that allows Amazon S3 to replicate objects from the source bucket to the destination bucket on your behalf and then choose **Save.**



You have now enabled cross-region replication of one bucket to another. The time it takes for Amazon S3 to replicate an object depends on the object size. It can take up to several hours to replicate a large-sized object.

> **Note**
> Metadata for an object remains identical between original objects and replica objects. Lifecycle rules abide by the creation time of the original object, and not by when the replicated object becomes available in the destination bucket. However, lifecycle actions on objects pending replication do not resolve until the replication has completed.

How Do I Disable Cross-Region Replication for an S3 Bucket?

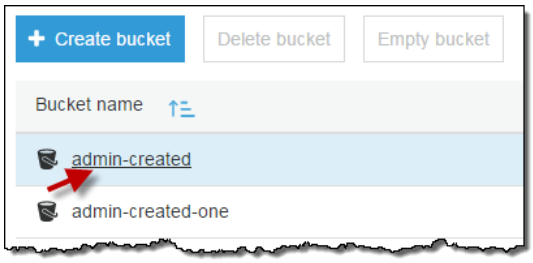
*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

Cross-region replication is the automatic, asynchronous copying of objects across buckets in different AWS Regions. For more information, see Cross-Region Replication in the Amazon Simple Storage Service Developer Guide.

Cross-region replication requires that versioning must be enabled on both your source bucket and your destination bucket that is in a different region. For more information, see How Do I Enable or Suspend Versioning for an S3 Bucket? (p. 10).

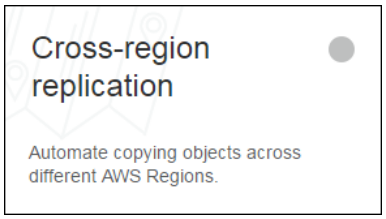
To disable cross-region replication of an S3 bucket to another bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that you want to enable versioning for.

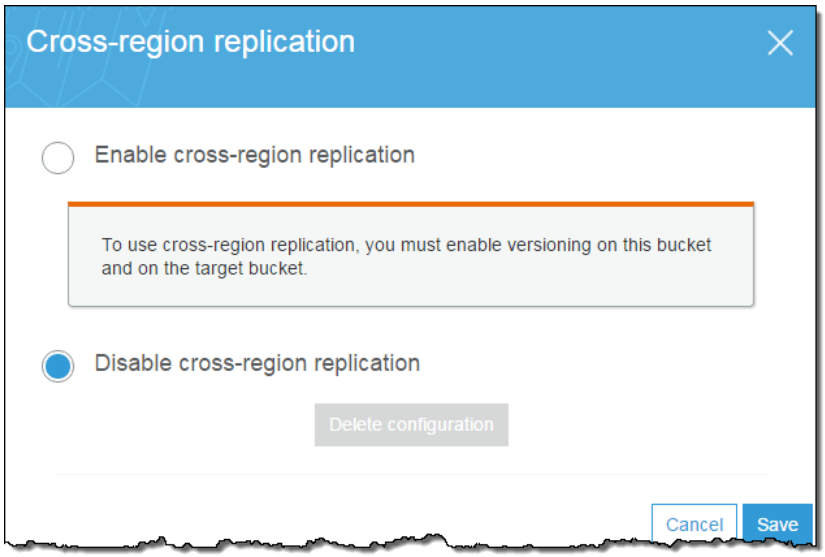


3. Choose **Properties**.

4. Under **Advanced settings**, choose **Cross-region replication**.



5. Choose **Disable cross-region replication**.



6. Choose **Save**.

How Do I Set Up a Destination to Receive Event Notifications?

*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

Before you can enable event notifications for your bucket you must set up one of the following destination types:

An Amazon SNS topic

Amazon Simple Notification Service (Amazon SNS) is a web service that coordinates and manages the delivery or sending of messages to subscribing endpoints or clients. You can use the Amazon SNS console to create an Amazon SNS topic that your notifications can be sent to. The Amazon SNS topic must be in the same region as your Amazon S3 bucket. For information about creating an Amazon SNS topic, see Getting Started in the *Amazon Simple Notification Service Developer Guide*.

Before you can use the Amazon SNS topic that you create as an event notification destination, you need the following:

- The Amazon Resource Name (ARN) for the Amazon SNS topic
- A valid Amazon SNS topic subscription (the topic subscribers are notified when a message is published to your Amazon SNS topic)
- A permissions policy that you set up in the Amazon SNS console (as shown in the following example)

```
{
  "Version":"2012-10-17",
  "Id": "__example_policy_ID",
  "Statement":[
    {
      "Sid": "example-statement-ID",
      "Effect":"Allow",
      "Principal": "*",
      "Action": "SNS:Publish",
      "Resource":"arn:aws:sns:region:account-number:topic-name",
      "Condition": {
        "ArnEquals": {
        "aws:SourceArn": "arn:aws:s3:::bucket-name"
         }
       }
     }
   ]
}
```

An Amazon SQS queue

You can use the Amazon SQS console to create an Amazon SQS queue that your notifications can be sent to. The Amazon SQS queue must be in the same region as your Amazon S3 bucket. For information about creating an Amazon SQS queue, see Getting Started with Amazon SQS in the *Amazon Simple Queue Service Developer Guide*.

Before you can use the Amazon SQS queue as an event notification destination, you need the following:

- The Amazon Resource Name (ARN) for the Amazon SQS topic
- A permissions policy that you set up in the Amazon SQS console (as shown in the following example)

```
{
  "Version":"2012-10-17",
  "Id": "__example_policy_ID",
  "Statement":[
    {
      "Sid": "example-statement-ID",
      "Effect":"Allow",
      "Principal": "*",
      "Action": "SQS:*",
      "Resource":"arn:aws:sqs:region:account-number:queue-name",
      "Condition": {
        "ArnEquals": {
        "aws:SourceArn": "arn:aws:s3:::bucket-name"
         }
       }
     }
   ]
}
```

A Lambda function

You can use the AWS Lambda console to create a Lambda function. The Lambda function must be in the same region as your S3 bucket. For information about creating a Lambda function, see the AWS Lambda Developer Guide.

Before you can use the Lambda function as an event notification destination, you must have the name or the ARN of a Lambda function to set up the Lambda function as a event notification destination.

For information about using Lambda with Amazon S3, see Using AWS Lambda: with Amazon S3 in the *AWS Lambda Developer Guide*.

How Do I Enable and Configure Event Notifications for an S3 Bucket?

*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

You can enable certain Amazon S3 bucket events to send a notification message to a destination whenever the events occur. This section explains how to use the Amazon S3 console to enable event notifications. For more information about using event notifications , see Configuring Notifications for Amazon S3 Events in the *Amazon Simple Storage Service Developer Guide*.

Amazon S3 can send notifications for the following events:

- **An object created event** – You choose **ObjectCreated (All)** when configuring your events in the console to enable notifications for anytime an object is created in your bucket. Or, you can select one or

more of the specific object-creation actions to trigger event notifications. These actions are **Put**, **Post**, **Copy**, and **CompleteMultiPartUpload**.

- **An object delete event** – You select **ObjectDelete (All)** when configuring your events in the console to enable notification for anytime an object is deleted. Or, you can select **Delete** to trigger event notifications when an unversioned object is deleted or a versioned object is permanently deleted. You select **Delete Marker Created** to trigger event notifications when a delete marker is created for a versioned object.
- **A Reduced Redundancy Storage (RRS) object lost event** – You select **RRSObjectLost** to be notified when Amazon S3 detects that an object of the RRS storage class has been lost.

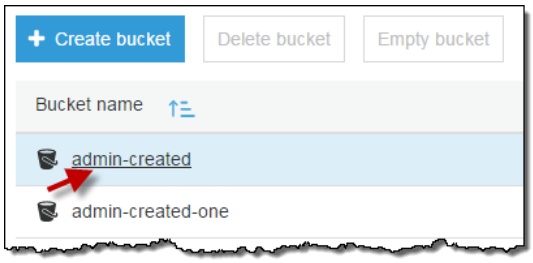
Event notification messages can be sent to the following types of destinations:

- **An Amazon Simple Notification Service (Amazon SNS) topic** – A web service that coordinates and manages the delivery or sending of messages to subscribing endpoints or clients.
- **An Amazon Simple Queue Service (Amazon SQS) queue** – Offers reliable and scalable hosted queues for storing messages as they travel between computer.
- **A Lambda function** – AWS Lambda is a compute service where you can upload your code and the service can run the code on your behalf using the AWS infrastructure. You package up and upload your custom code to AWS Lambda when you create a Lambda function

Before you can enable event notifications for your bucket you must set up one of these destination types. For more information, see How Do I Set Up a Destination to Receive Event Notifications? (p. 23).

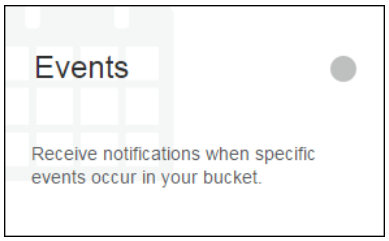
To enable and configure event notifications for an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that you want to enable events for.

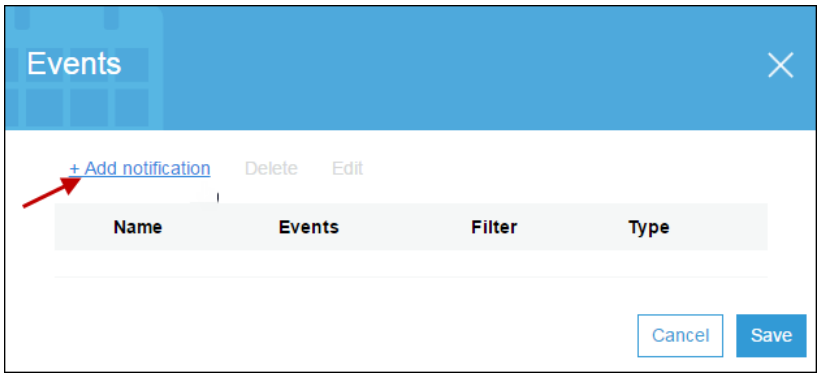


3. Choose **Properties**.

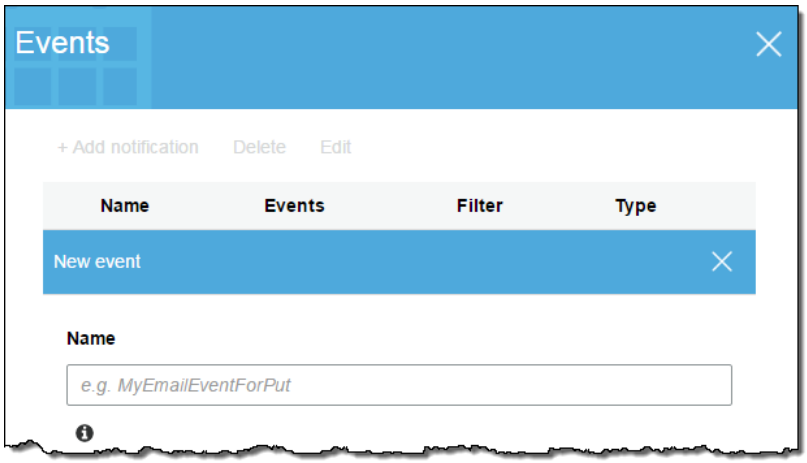
4. Under Advanced settings, choose **Events**.



5. Choose **Add notification**.



6. In **Name**, type a descriptive name for your event configuration. If you do not enter a name, a GUID is autogenerated and used for the name.



7. Under **Events**, select one or more of the type of event occurrences that you want to receive notifications for. When the event occurs a notification is sent to a destination that you choose. For example, you could do any of the following:

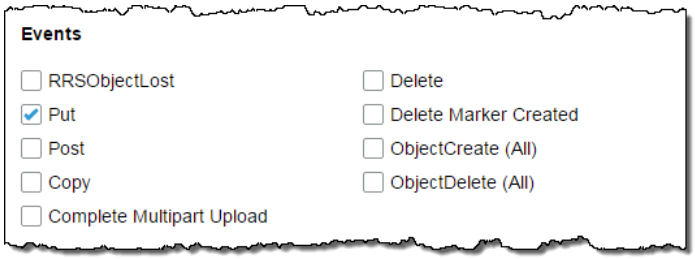
   - Select **ObjectCreate (All)** to enable event notifications for anytime an object is created in the bucket.
   - Select **Put** and **Complete MultipartUpload** to trigger event notifications anytime a new object is put into a bucket and anytime a multipart upload completes.
   - Select **ObjectDelete (All)** to enable event notifications for anytime an object is deleted in the bucket.
   - Select **Delete** or **Delete Marker Created** to trigger notifications for specific types of object deletes.

   For information about deleting versioned objects, see Deleting Object Versions. For information about object versioning, see Object Versioning and Using Versioning.

   Note

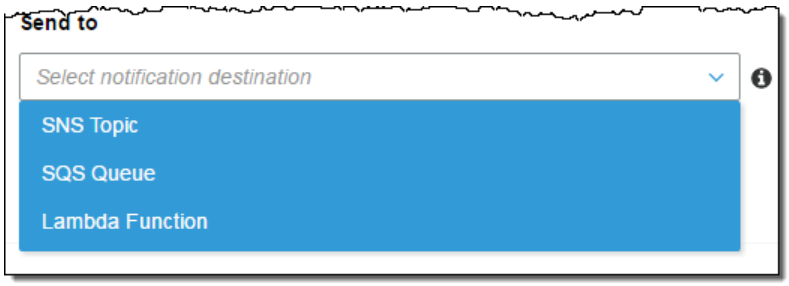
   When you delete the last object from a folder Amazon S3 can generate an object creation event. The Amazon S3 console displays a folder under the following circumstances: 1) when a zero byte object has a trailing slash (/) in its name (in this case there is an actual Amazon S3 object of 0 bytes that represents a folder), and 2) if the object has a slash (/) within its name (in this case there isn't an actual object representing the folder). When there are multiple objects with the same prefix with a trailing slash (/) as part of their names, those objects are shown as being part of a folder. The name of the folder is formed from the characters preceding the trailing slash (/). When you delete all the objects listed under that folder, there is no actual object available to represent the empty folder. Under such circumstance the

Amazon S3 console creates a zero byte object to represent that folder. If you enabled event notification for creation of objects, the zero byte object creation action that is taken by the console will trigger an object creation event.



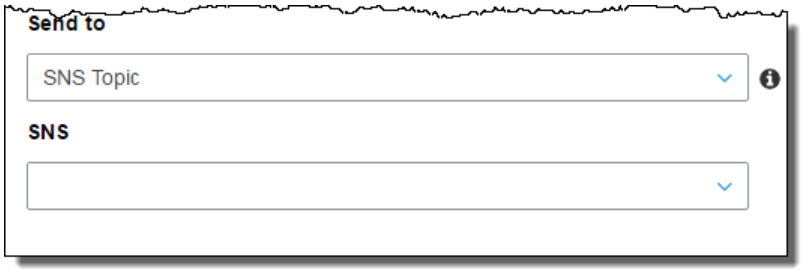
8. Type an object name **Prefix** and/or a **Suffix** to filter the event notifications by the prefix and/or suffix. For example, you can set up a filter so that you are sent a notification only when files are added to an image folder (for example, objects with the name prefix `images/`). For more information, see Configuring Notifications with Object Key Name Filtering.

9. Select the type of destination to have the event notifications sent to.

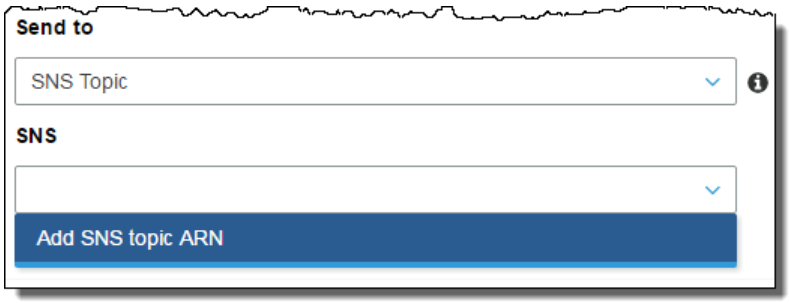


   a. If you select the **SNS Topic** destination type.

      i. In the **SNS topic** box, type the name or select from the menu, the Amazon SNS topic that will receive notifications from Amazon S3. For information about the Amazon SNS topic format, see SNS FAQ.



ii. (Optional) You can also select **Add SNS topic ARN** from the menu and type the **ARN** of the SNS topic in **SNS topic ARN**.



b. If you select the **SQS queue** destination type, do the following:

   i. In **SQS queue**, type or choose a name from the menu of the Amazon SQS queue that you want to receive notifications from Amazon S3. For information about Amazon SQS, see What is Amazon Simple Queue Service? in the *Amazon Simple Queue Service Developer Guide*.

   ii. (Optional) You can also select **Add SQS topic ARN** from the menu and type the ARN of the SQS queue in **SQS queue ARN**.

c. If you select the **Lambda Function** destination type, do the following:

   i. In **Lambda Function**, type or choose the name of the Lambda function that you want to receive notifications from Amazon S3.

   ii. If you don't have any Lambda functions in the region that contains your bucket, you'll be prompted to enter a Lambda function ARN. In **Lambda Function ARN**, type the ARN of the Lambda function that you want to receive notifications from Amazon S3.

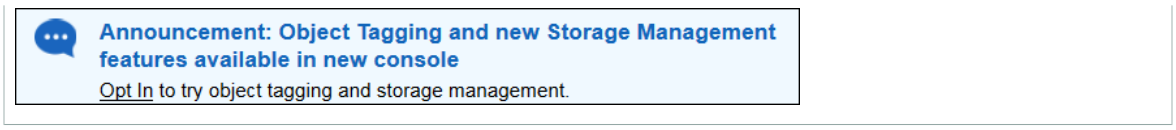
   iii. (Optional) You can also choose **Add Lambda function ARN** from the menu and type the ARN of the Lambda function in **Lambda function ARN**.

   For information about using Lambda with Amazon S3, see Using AWS Lambda: with Amazon S3 in the *AWS Lambda Developer Guide*.

10. Choose **Save**. Amazon S3 will send a test message to the event notification destination.

How Do I Enable Transfer Acceleration for an S3 Bucket?

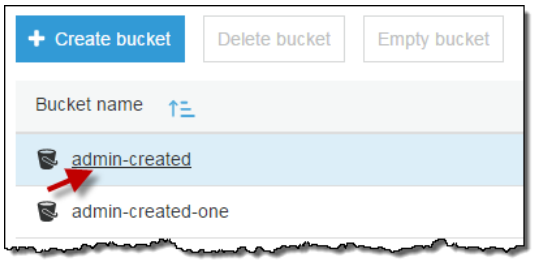
*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*



Amazon Simple Storage Service (Amazon S3) transfer acceleration enables fast, easy, and secure transfers of files between your client and an S3 bucket over long distances. This topic describes how to enable Amazon S3 transfer acceleration for a bucket. For more information, see Amazon S3 Transfer Acceleration in the *Amazon Simple Storage Service Developer Guide*.

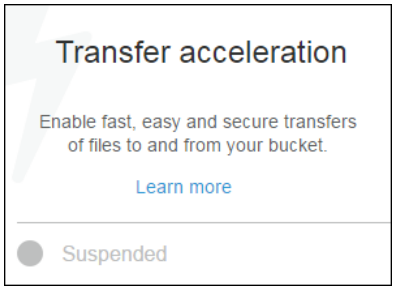
To enable transfer acceleration for an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that you want to enable transfer acceleration for.



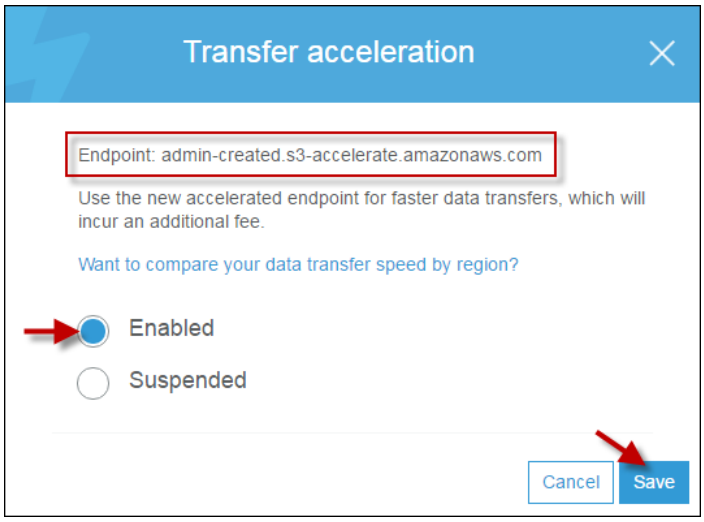
3. Choose **Properties**.

4. Choose **Transfer acceleration**.



5. Choose **Enabled**, and then choose **Save**.

   Endpoint displays the endpoint domain name that you use to access accelerated data transfers to and from the bucket that is enabled for transfer acceleration. If you suspend transfer acceleration, the accelerate endpoint no longer works.



6. (Optional) If you want to run the Amazon S3 Transfer Acceleration Speed Comparison tool, which compares accelerated and non-accelerated upload speeds starting with the Region in which the transfer acceleration bucket is enabled, choose **Want to compare your data transfer speed by region?**. The Speed Comparison tool uses multipart uploads to transfer a file from your browser to various AWS Regions with and without using Amazon S3 transfer acceleration.

More Info

- How Do I View the Properties for an S3 Bucket? (p. 9)

Uploading, Downloading, and Managing Objects

*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

Amazon S3 is cloud storage for the Internet. To upload your data (photos, videos, documents etc.), you first create a bucket in one of the AWS Regions. You can then upload an unlimited number of data objects to the bucket.

The data that you store in Amazon S3 consists of objects. Every object resides within a bucket that you create in a specific AWS Region. Every object that you store in Amazon S3 resides in a bucket.

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 AWS region physically remain in that region. Amazon S3 does not keep copies of objects or move them to any other region. However, you can access the objects from anywhere, as long as you have necessary permissions to do so.

Before you can upload an object into Amazon S3, you must have write permissions to a bucket.

Objects can be any file type: images, backups, data, movies, etc. The maximum size of file you can upload by using the Amazon S3 console is 78GB. You can have an unlimited number of objects in a bucket.

The following topics explain how to use the Amazon S3 console to upload, delete, and manage objects.

Topics

How Do I Upload an Object to an S3 Bucket?

*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

This section explains how to use the AWS Management Console to upload one or more files or entire folders to an Amazon S3 bucket.

Before you can upload an object to an Amazon S3 bucket, you must have write permissions for the bucket. For more information about access permissions, see Setting Bucket and Object Access Permissions (p. 84).

Objects can be any file type: images, backups, data, movies, etc. The maximum size of a file that you can upload by using the Amazon S3 console is 78 GB. You can have an unlimited number of objects in a bucket.

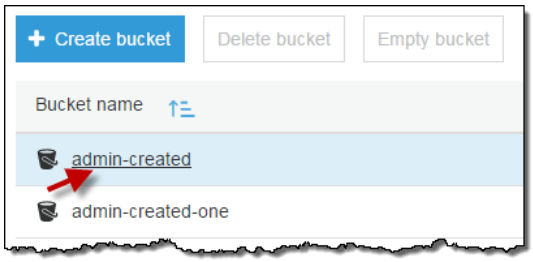
When you upload a folder, Amazon S3 uploads all of the files and subfolders from the specified folder to your bucket. It then assigns a key name that is a combination of the uploaded file name and the folder name. For example, if you upload a folder called `/images` that contains two files, `sample1.jpg`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

If you upload files that are not in a folder, when Amazon S3 uploads the files, it assigns only the file names as the key name for the objects created . For more information on key names, see Object Key and Metadata in the *Amazon Simple Storage Service Developer Guide*.

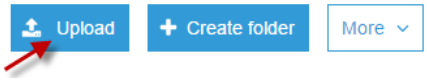
If you upload an object with a key name that already exists in a versioning-enabled bucket, Amazon S3 creates another version of the object instead of replacing the existing object.

To upload an object to an S3 bucket

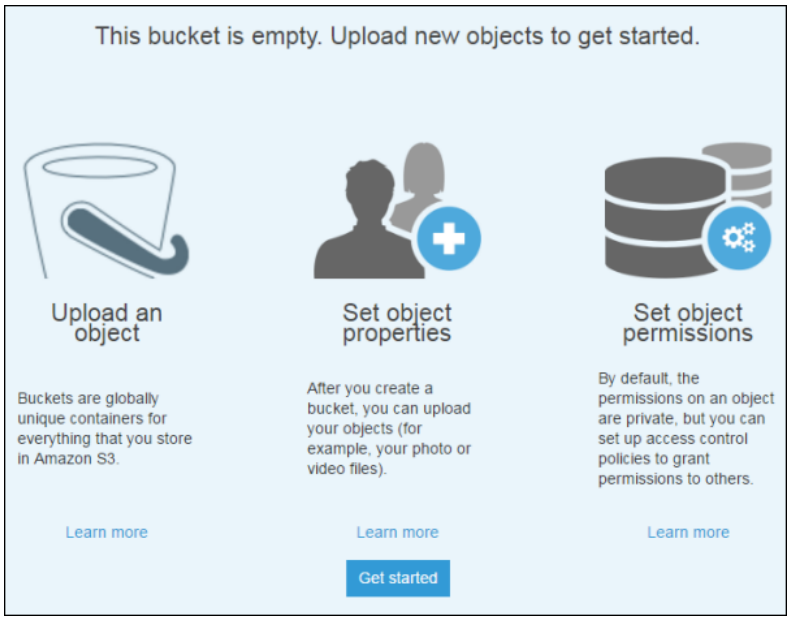
1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that you want to upload your objects to.



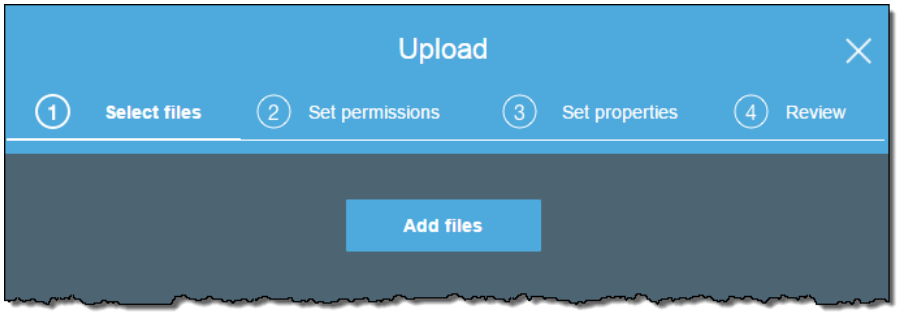
3. Choose **Upload**.



- If the bucket is empty, choose **Get started** or **Upload an object**.

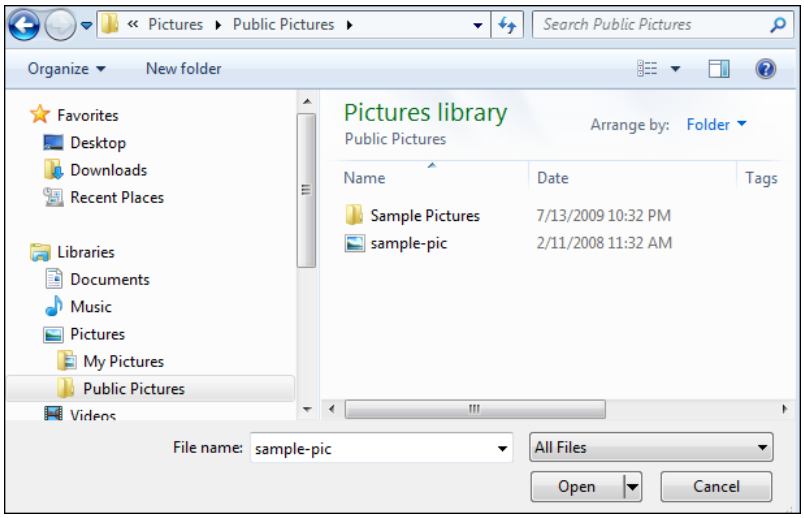


4. In the **Upload** dialog box, choose **Add files** to select the files to upload.

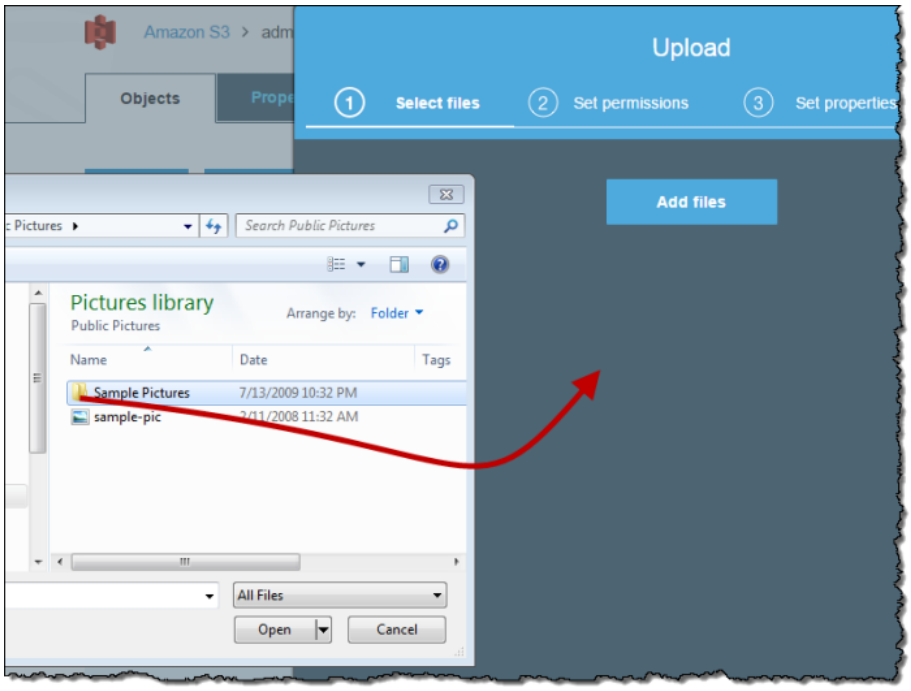


5. In the dialog box, use one of the following methods to add the files that you want to upload:

   a. Choose one or more files and folders to upload, and then choose **Open.**



b. If you are using the Google Chrome browser, you can choose one or more files to upload, and then drag and drop your selection into the **Upload** dialog box.

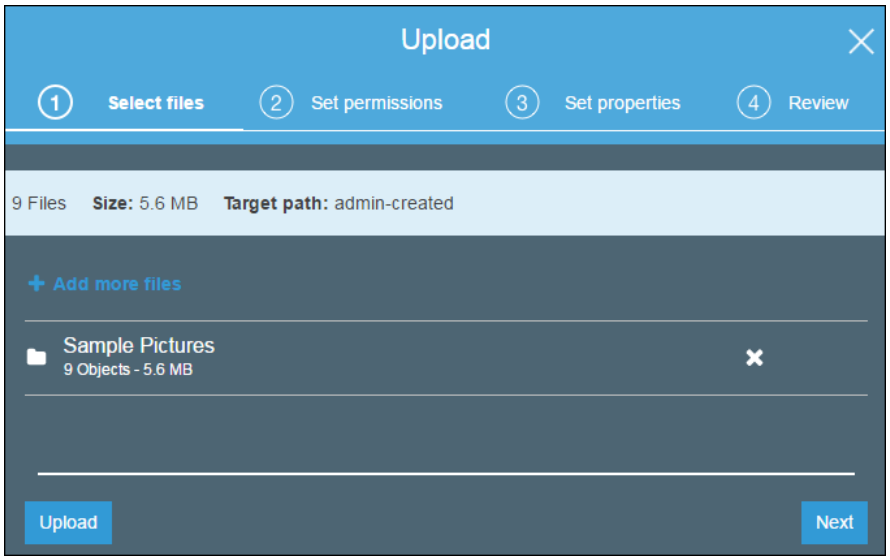


6. The files you chose are listed in the **Upload** dialog box.

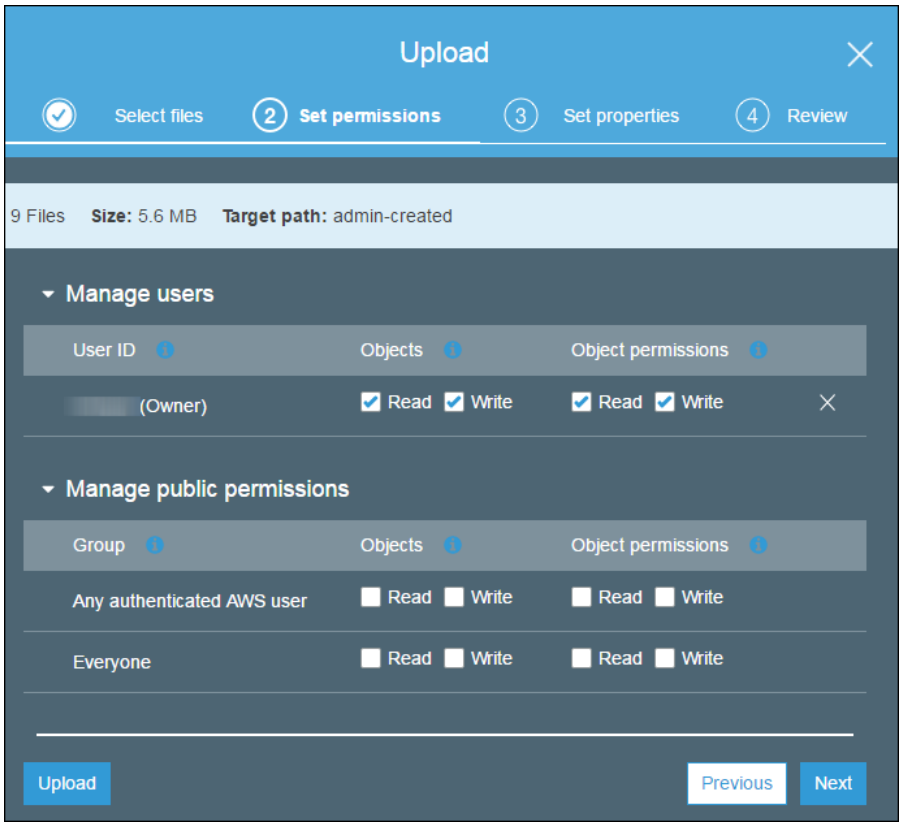
   a. To add more files, choose **Add more files**.

   b. To immediately upload the files, choose **Upload**.

   c. To continue on to setting permissions or properties for the files that you are uploading, choose **Next**.



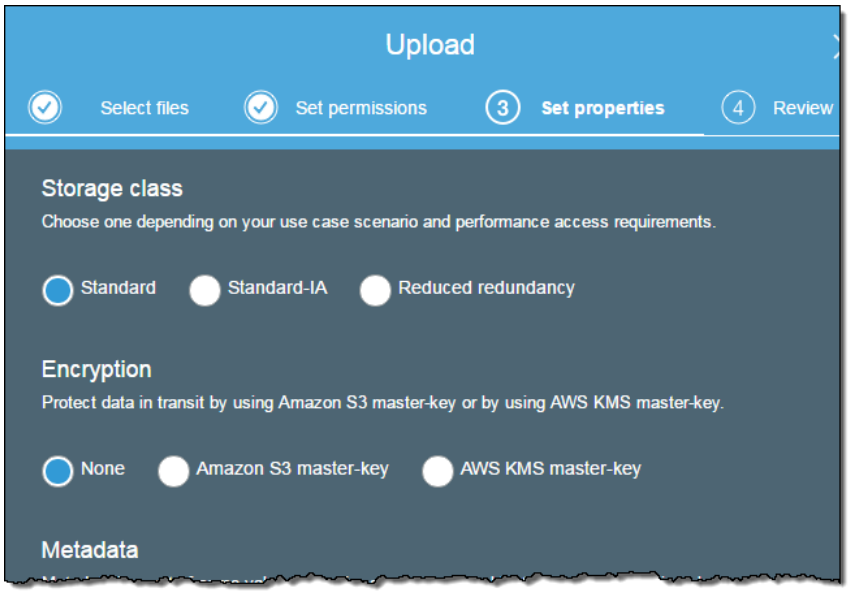
7. On the **Set Permissions** page, you can grant or remove permissions for specific users and set public permissions for the files you are uploading. Make the changes, and then choose **Next**. For more information about object access permissions, see How Do I Set Permissions on an Object? (p. 85).



8. On the **Set Properties** page, choose the storage class and encryption method to use for the objects you are uploading. You can also add or modify metadata.

a. Choose a storage class for the objects you are uploading. For more information about storage classes, see Storage Classes in the *Amazon Simple Storage Service Developer Guide*.

b. Choose the type of encryption for the objects you're uploading, or, if you don't want to encrypt the objects you're uploading, choose **None**.



i. To encrypt your uploaded objects using keys that are managed by Amazon S3, choose **Amazon S3 master-key**. For more information, see Protecting Data with Amazon S3-Managed Encryption Keys Classes in the *Amazon Simple Storage Service Developer Guide*.

ii. To encrypt your uploaded objects using the AWS Key Management Service (AWS KMS), choose **AWS KMS master-key** and then choose a master key from the list of the AWS KMS master keys that you have previously created.

> **Note**
> You can use only keys in the same AWS Region as this bucket to encrypt objects in this bucket.

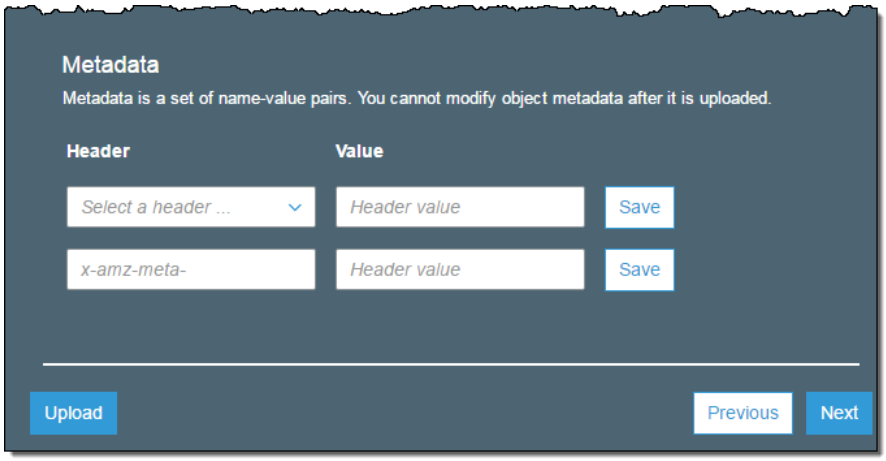
You can give an external account the ability to use an object that is protected by an AWS KMS key. To do this, select **Custom KMS ARN** from the list and enter the Amazon Resource Name (ARN) for the external account. Administrators of an external account that have usage permissions to an object protected by your AWS KMS key can further restrict access by creating a resource-level IAM policy.

For more information about creating an AWS KMS key, see Creating Keys in the *AWS Key Management Service Developer Guide*. For more information, see Protecting Data with AWS KMS–Managed Key in the *Amazon Simple Storage Service Developer Guide*.

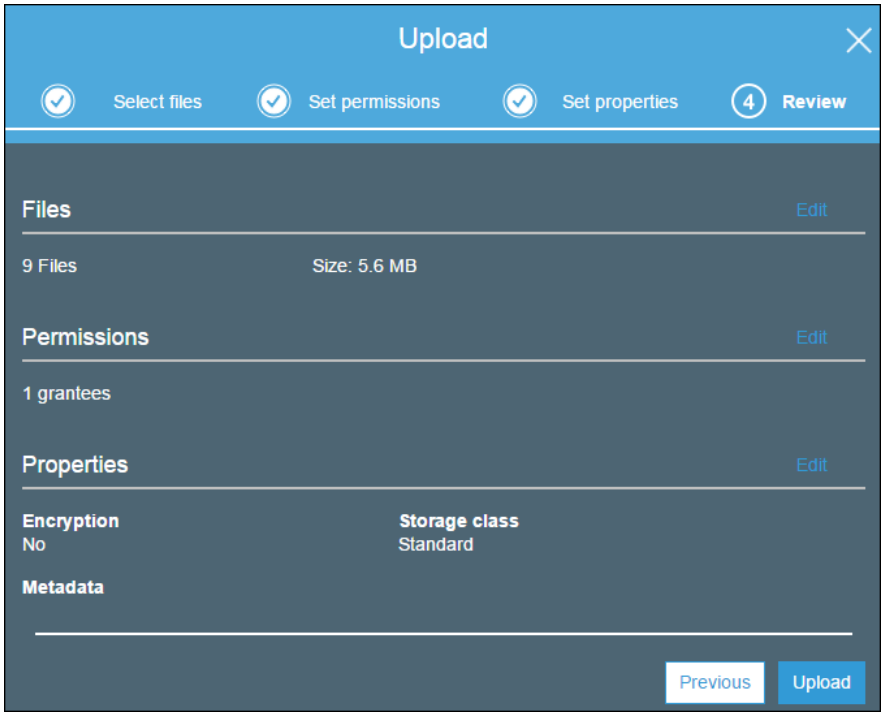
c. If you want to add Amazon S3 system-defined metadata to all of the objects you are uploading, for **Header**, select a header. You can select common HTTP headers, such as **Content-Type** and **Content-Disposition**. Type a value for the header, and then choose **Save**. For a list of system-defined metadata and whether you can add the value or not, see System-Defined Metadata in the *Amazon Simple Storage Service Developer Guide*.

d. To add user-defined metadata to all of the objects that you are uploading, type `x-amz-meta-` plus a custom metadata name in the **Header** field. Type a value for the header, and then choose **Save**. For more information about user-defined metadata, see User-Defined Metadata in the *Amazon Simple Storage Service Developer Guide*.

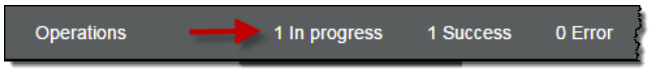
Amazon S3 object metadata is represented by a name-value (key-value) pair. User-defined metadata is stored with the object and returned when you download the object. Amazon S3 does not process user-defined metadata. User-defined metadata can be as large as 2 KB, and both the keys and their values must conform to US-ASCII standards. Any metadata starting with prefix `x-amz-meta-` is treated as user-defined metadata.

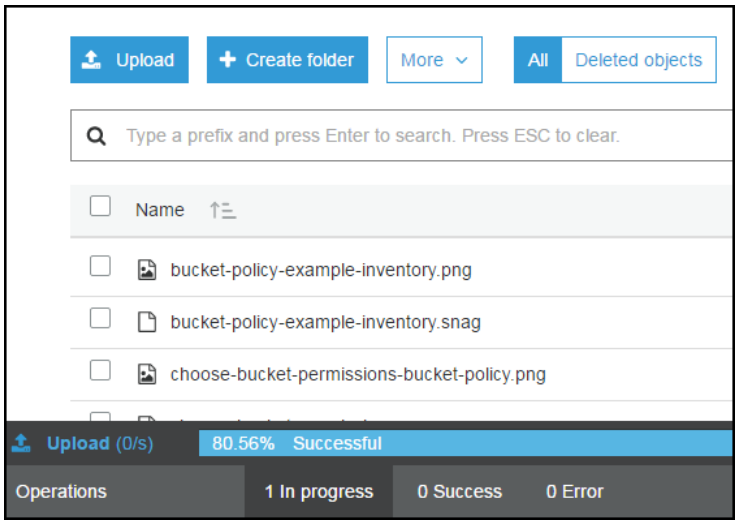


9. Choose **Next**.
10. On the **Upload** review page, verify that your settings are correct, and then choose **Upload**. To make changes, choose **Previous**.

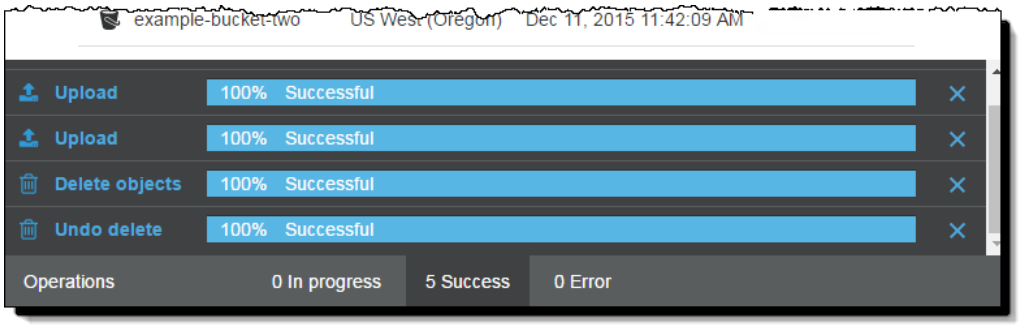


11. To see the progress of your upload, choose **In progress** at the bottom of the browser window.





To see a history of your uploads and other operations, choose **Success**.



More Info

- How Do I Download an Object from an S3 Bucket? (p. 38)

How Do I Download an Object from an S3 Bucket?

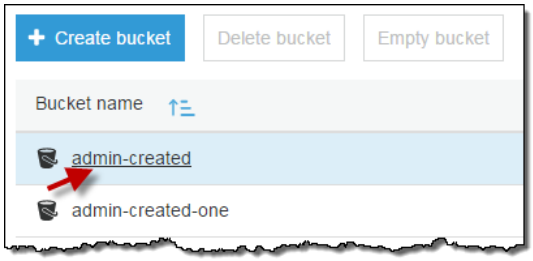
*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

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

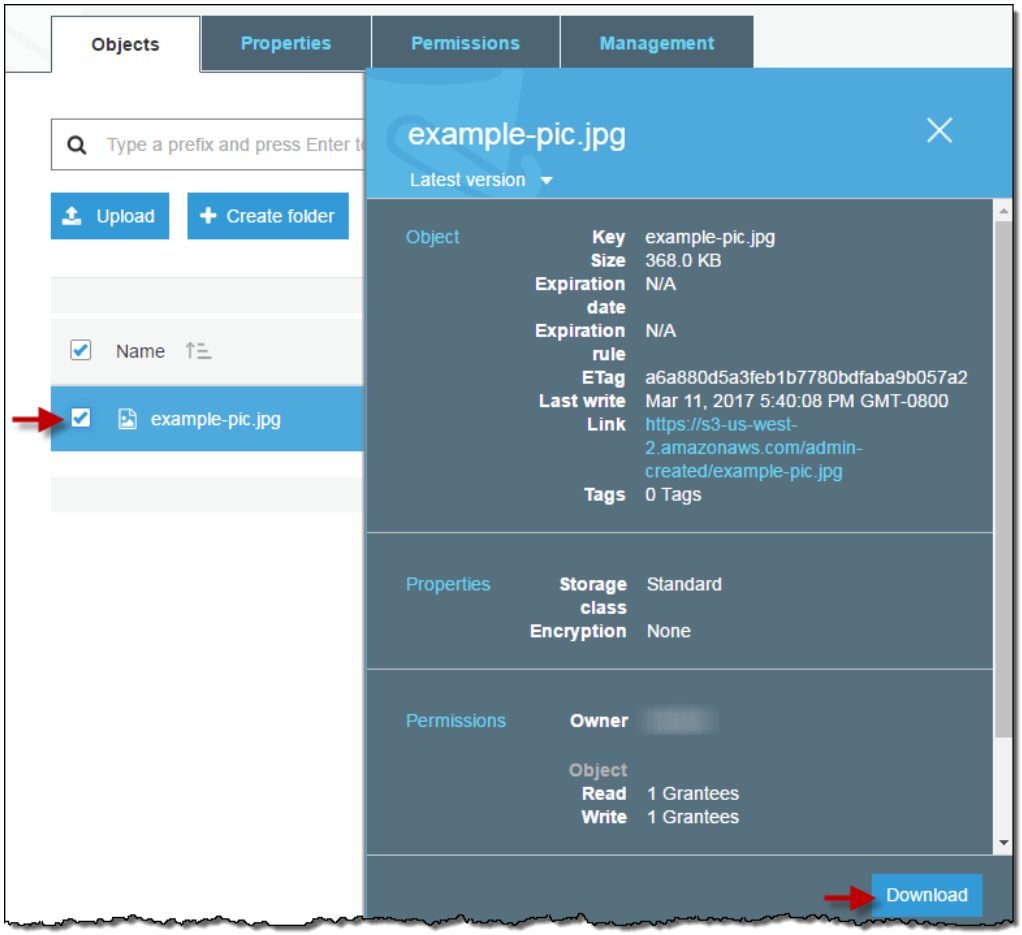
Data transfer fees apply when you download objects. For information about Amazon S3 features, and pricing, see Amazon S3.

To download an object from an S3 bucket

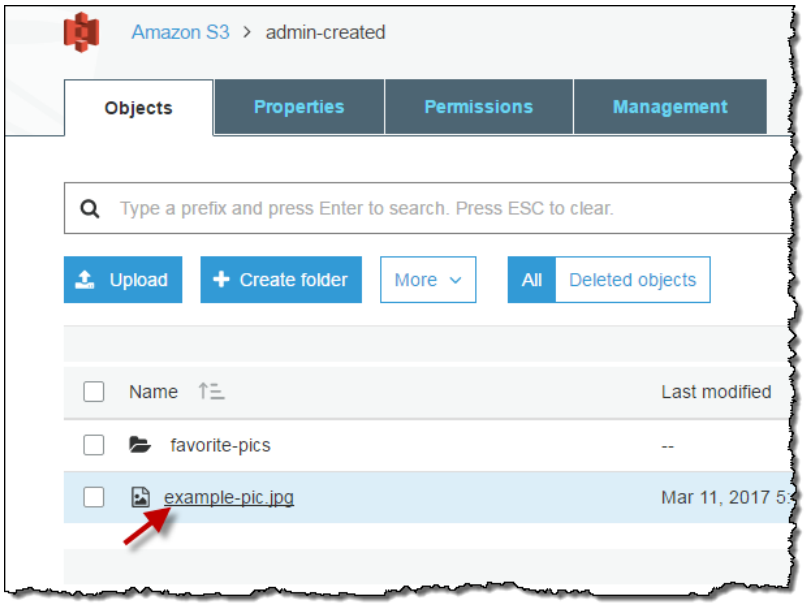
1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that you want to download an object from.



3. You can download an object from an S3 bucket in any of the following ways:
   - In the **Name** list, select the check box next to the object you want to download, and then choose **Download** on the object description page that appears.

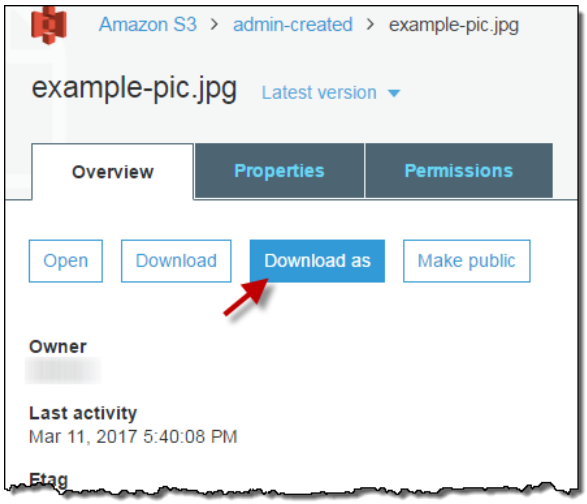


   - Choose the name of the object that you want to download.

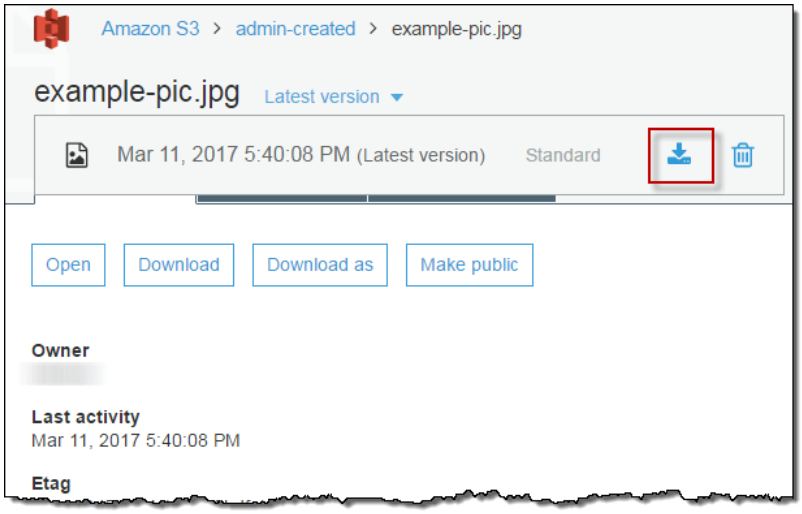


On the **Overview** page, choose **Download**.

- Choose the name of the object that you want to download and then choose **Download as** on the **Overview** page.



- Choose the name of the object that you want to download. Choose **Latest version** and then choose the download icon.



Related Topics

- How Do I Upload an Object to an S3 Bucket? (p. 32)

How Do I Delete Objects from an S3 Bucket?

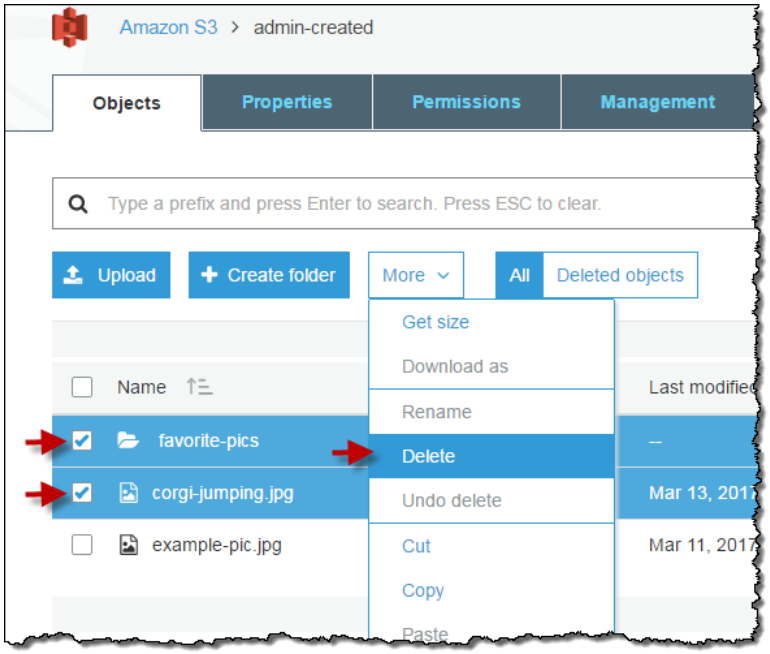
*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

This section explains how to use the Amazon S3 console to delete objects. Because all objects in your 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 needed. You can set up a lifecycle rule to automatically delete objects such as log files.

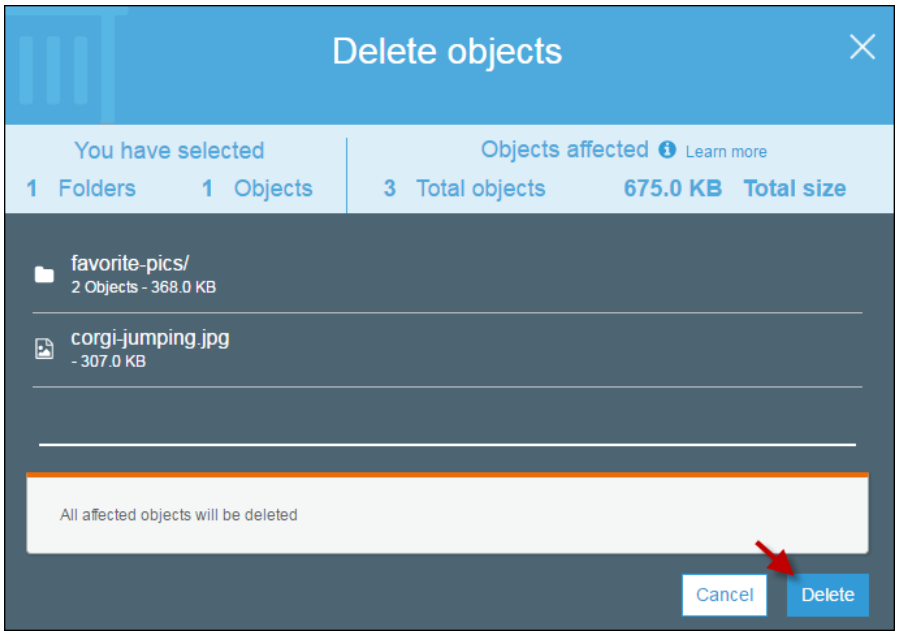
For information about Amazon S3 features and pricing, see Amazon S3.

To delete objects from an S3 bucket

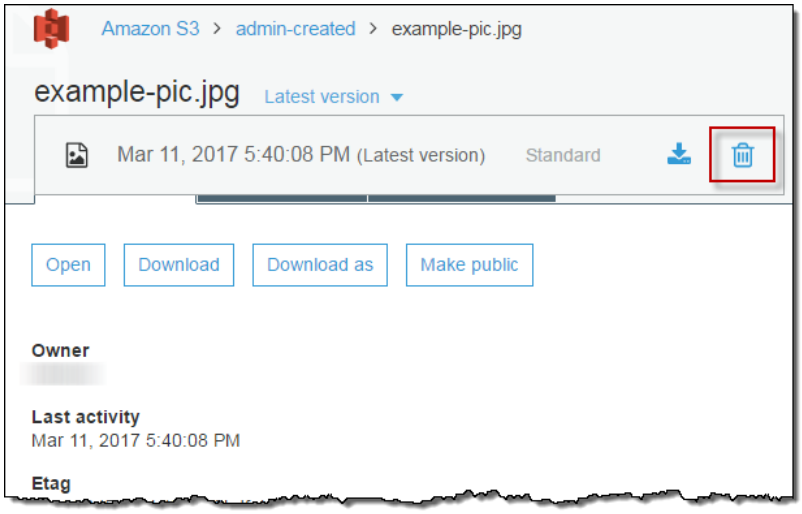
1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that you want to delete an object from.
3. You can delete objects from an S3 bucket in any of the following ways:
   - In the **Name** list, select the check box next to the objects and folders that you want to delete, choose **More**, and then choose **Delete**.



In the **Delete objects** dialog box, verify that the names of the objects and folders you selected for deletion are listed and then choose **Delete**.



- Choose the name of the object that you want to delete, choose **Latest version**, and then choose the trash can icon.



More Info

- How Do I Undelete a Deleted S3 Object? (p. 44)
- How Do I Create a Lifecycle Policy for an S3 Bucket? (p. 66)

How Do I Undelete a Deleted S3 Object?

*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

This section explains how to use the Amazon S3 console to recover (undelete) deleted objects.

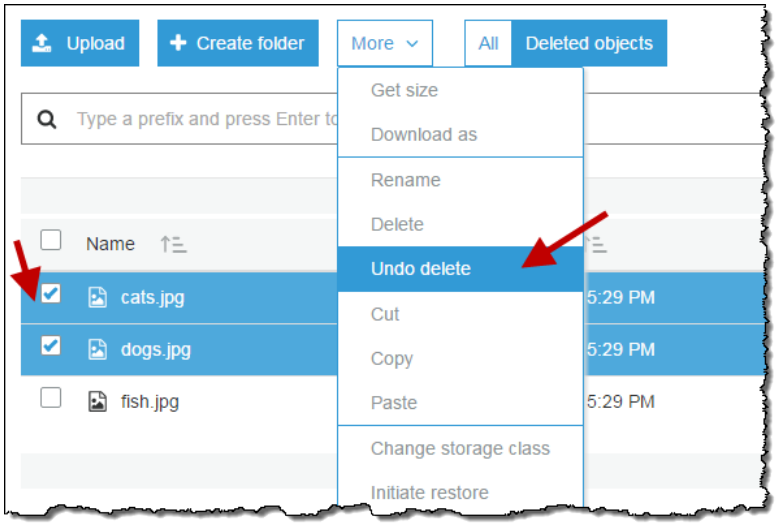
To be able to undelete a deleted object, you must have had versioning enabled on the bucket that contains the object before the object was deleted. For information about enabling versioning, see How Do I Enable or Suspend Versioning for an S3 Bucket? (p. 10).

You can undelete only an object that was deleted as the latest (current) version. You can't undelete a previous version of an object that has been deleted. For more information, see Object Versioning and Using Versioning in the *Amazon Simple Storage Service Developer Guide*.

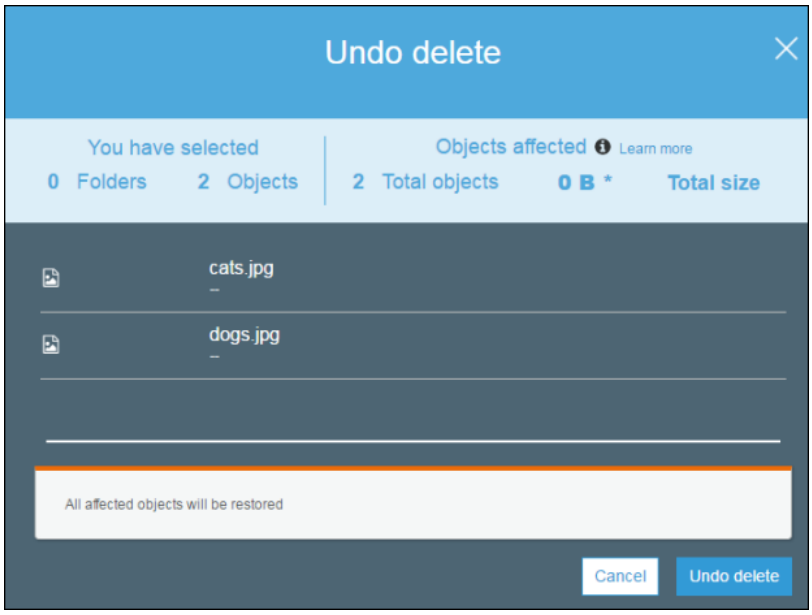
To recover deleted objects from an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that you want to recover a deleted object from.
3. Choose **Deleted objects** to see the objects that have been deleted from the bucket.
4. Select the check box next to the object or objects that you want to recover, and then choose **Undo delete** from the **More** menu.

   If the object you want to recover is in a folder. Choose the name of the folder, select the object or objects that you want to recover, and then choose **Undo delete** from the **More** menu.



5. On the **Undo delete** review page, verify that the objects that are listed are correct, and then choose **Undo delete**. Otherwise, choose **Cancel** and return to step 3.



More Info

- How Do I Enable or Suspend Versioning for an S3 Bucket? (p. 10)
- How Do I Delete Objects from an S3 Bucket? (p. 41)

How Do I Delete Folders from an S3 Bucket?

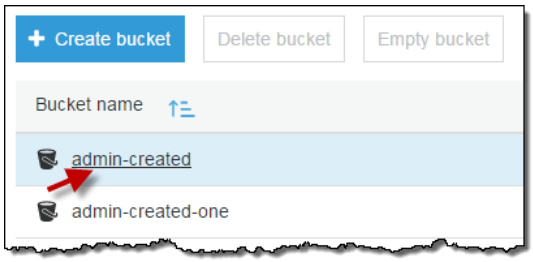
*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

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

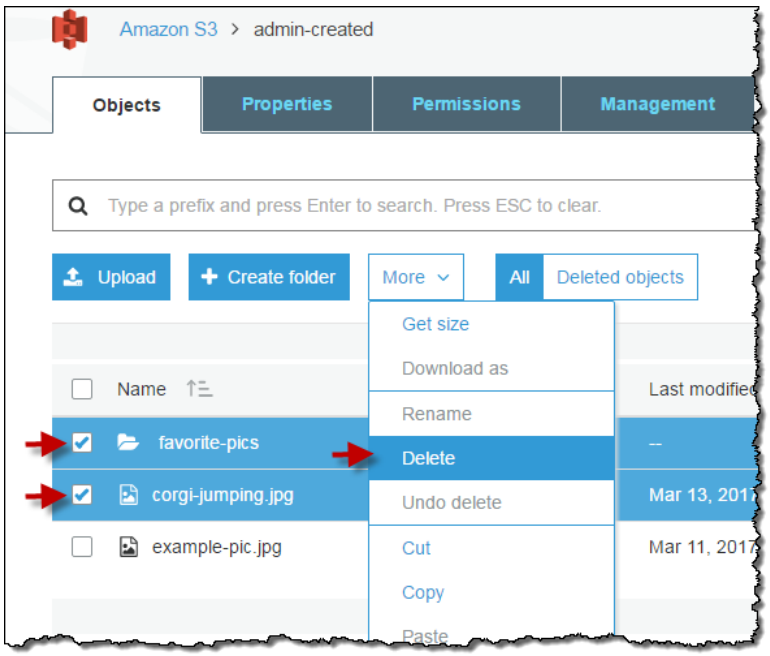
For information about Amazon S3 features and pricing, see Amazon S3.

To delete folders from an S3 bucket

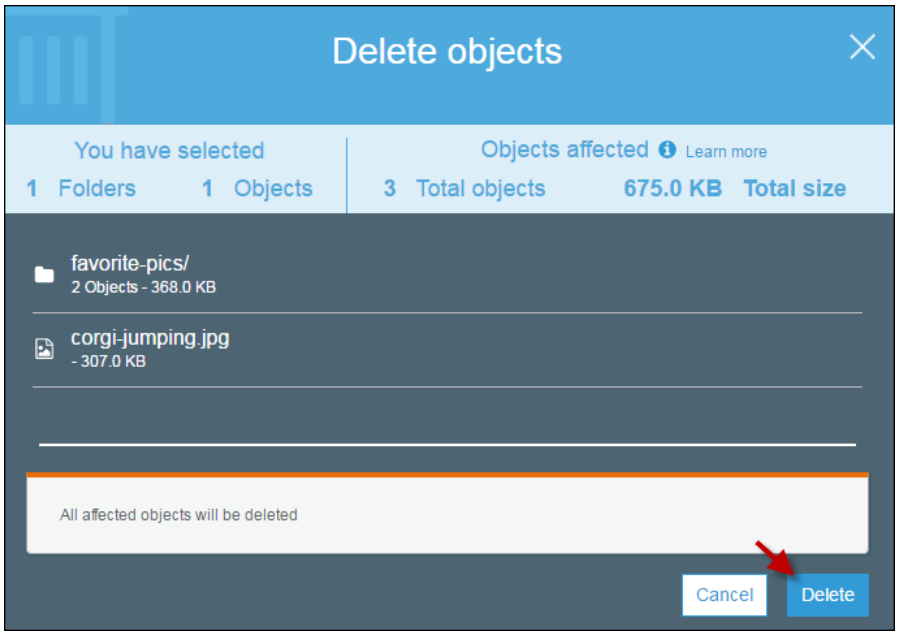
1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that you want to delete folders from.



3. In the **Name** list, select the check box next to the folders and objects that you want to delete, choose **More**, and then choose **Delete**.



In the **Delete objects** dialog box, verify that the names of the folders you selected for deletion are listed and then choose **Delete**.



Related Topics

- How Do I Delete Objects from an S3 Bucket? (p. 41)

How Do I See an Overview of an Object?

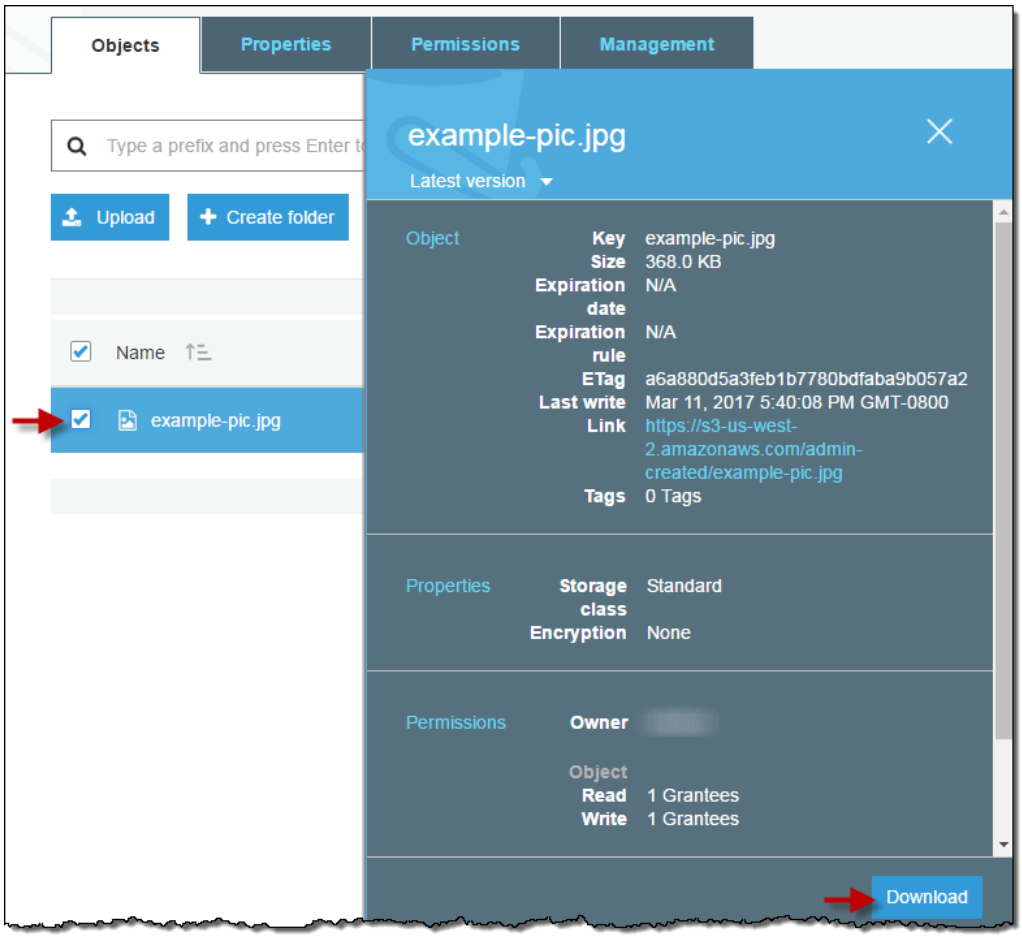
*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

This section explains how to use the console to view the object overview panel.

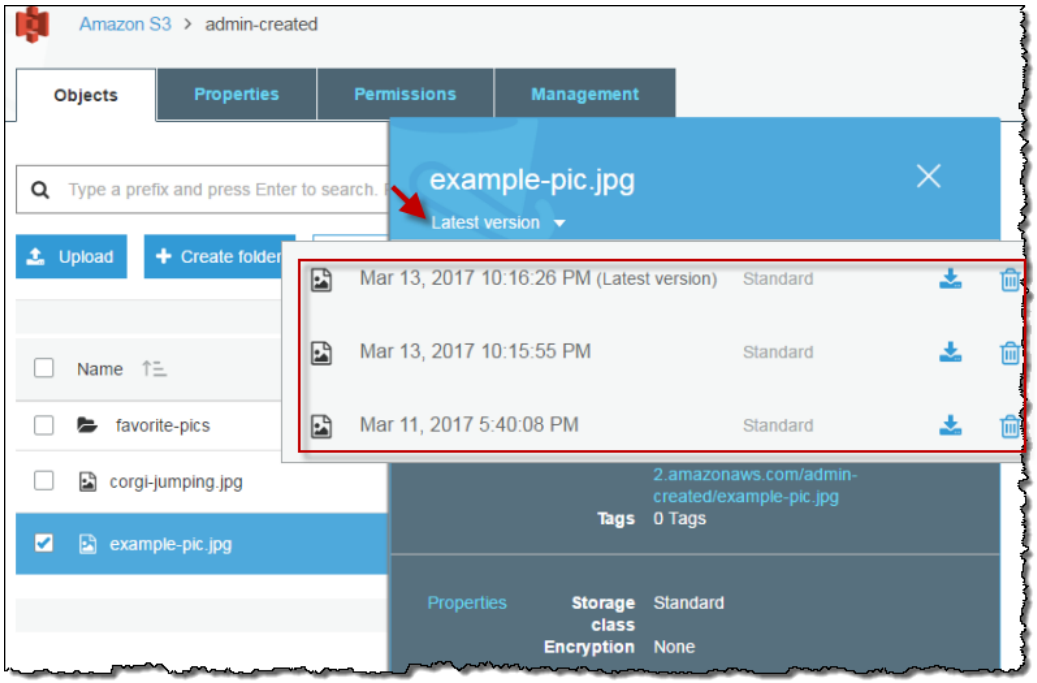
The overview panel provides an overview of the essential information about an object in one place.

To see the overview panel for an object

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that contains the object.
3. In the **Name** list, select the check box next to the name of the object for which you want an overview.



4. If the bucket is versioning-enabled, you can choose **Latest versions** to see all of the versions of the object.



5. You can then choose the download icon to download an object version, or choose the trash can icon to delete an object version.

   Important
   You can undelete only an object that was deleted as the latest (current) version. You can't undelete a previous version of an object that has been deleted. For more information, see Object Versioning and Using Versioning in the *Amazon Simple Storage Service Developer Guide*.

More Info

- How Do I See the Versions of an S3 Object? (p. 49)

How Do I See the Versions of an S3 Object?

*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

This section explains how to use the console to see the multiple versions of an object.

A versioning-enabled bucket can have many versions of the same object, one current (latest) version and zero or more noncurrent (previous) versions. For information about enabling versioning, see How Do I Enable or Suspend Versioning for an S3 Bucket? (p. 10).

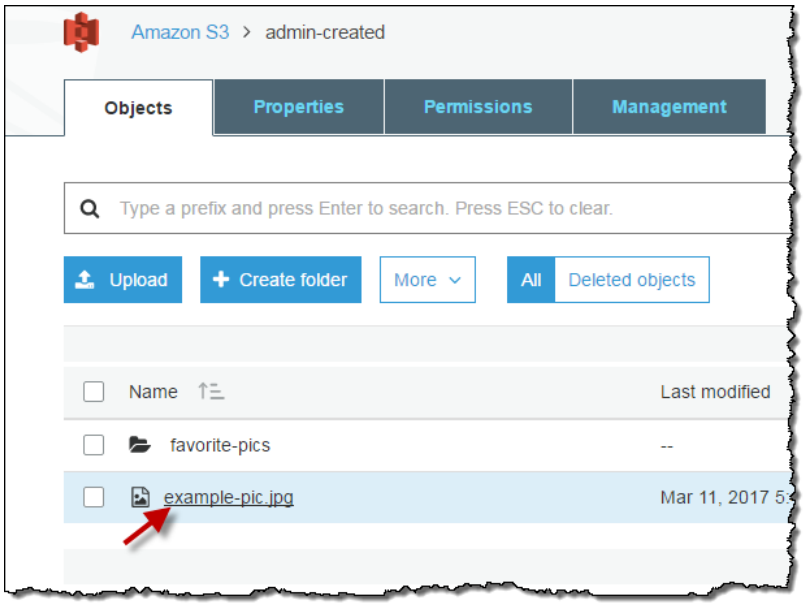
If a bucket is versioning-enabled, Amazon Simple Storage Service creates another version of an object under the following conditions:

- When you upload an object with a name that already exists in the bucket, Amazon S3 creates another version of the object instead of replacing the existing object.
- If you update any object properties after the object is first uploaded, such as changing the storage details or any other metadata changes, then Amazon S3 creates a new object version in the bucket.

For more information about versioning support in Amazon S3, see Object Versioning and Using Versioning in the *Amazon Simple Storage Service Developer Guide*.

To see multiple versions of an object

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that contains the object.
3. In the **Name** list, choose the name of the object for which you want to see the versions.



4. Choose **Latest versions** to see a list of the versions of the object.

5. You can then choose the download icon to download an object version, or choose the trash can icon to delete an object version.

   Important
   You can undelete only an object that was deleted as the latest (current) version. You cannot undelete a previous version of an object that has been deleted. For more information, see Object Versioning and Using Versioning in the *Amazon Simple Storage Service Developer Guide*.

You also can view object versions in the object overview panel, see How Do I See an Overview of an Object? (p. 47).

More Info

- How Do I Enable or Suspend Versioning for an S3 Bucket? (p. 10)
- How Do I Create a Lifecycle Policy for an S3 Bucket? (p. 66)

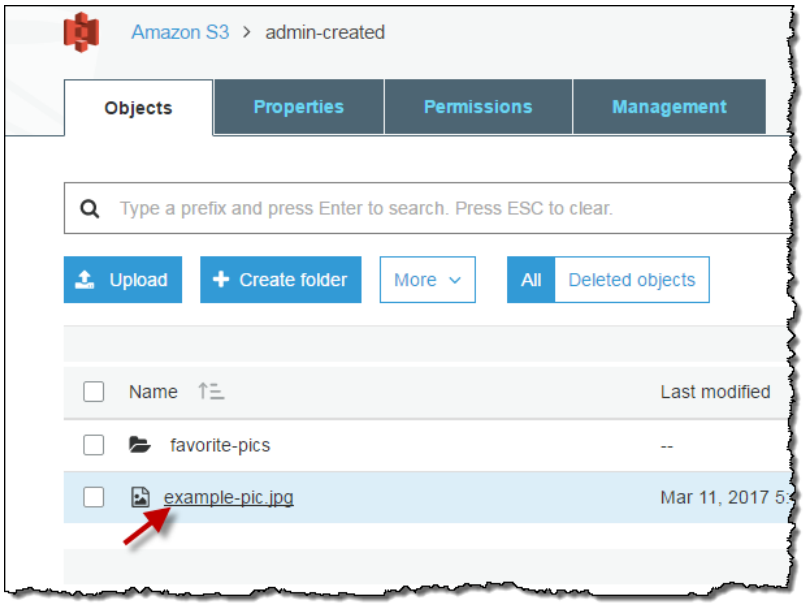
How Do I View the Properties of an Object?

*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

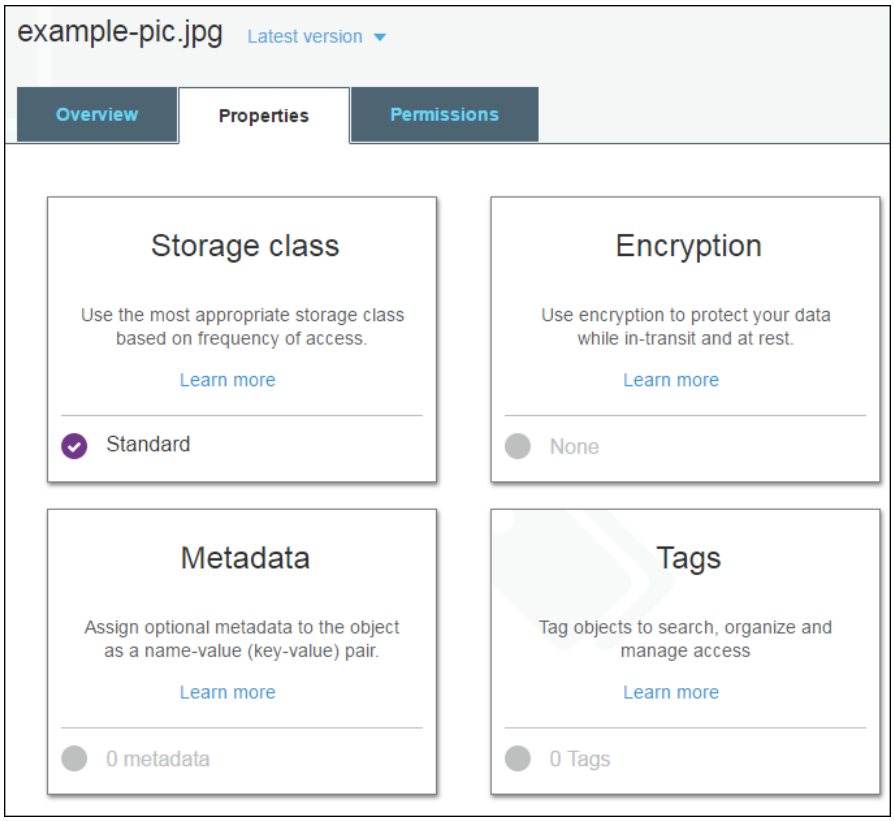
This section explains how to use the console to view the properties of an object.

To view the properties of an object

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that contains the object.
3. In the **Name** list, choose the name of the object you want to view the properties for.



4. Choose **Properties**.



5. On the **Properties** page, you can configure the following properties for the object.

   a. **Storage class** – Each object in Amazon S3 has a storage class associated with it. The storage class that you choose to use depends on how frequently you access the object. The default storage class for S3 objects is STANDARD. You choose which storage class to use when you

upload an object. For more information about storage classes, see Storage Classes in the *Amazon Simple Storage Service Developer Guide*.

To change the storage class after you upload an object, choose **Storage class**. Choose the storage class that you want, and then choose **Save**.

b. **Encryption** – You can encrypt your S3 objects. For more information, see How Do I Add Encryption to an S3 Object? (p. 53).

c. **Metadata** – Each object in Amazon S3 has a set of name-value pairs that represents its metadata. For information on adding metadata to an S3 object, see How Do I Add Metadata to an S3 Object? (p. 56).

d. **Tags** – You can add tags to an S3 object. For more information, see How Do I Add Tags to an S3 Object? (p. 62).

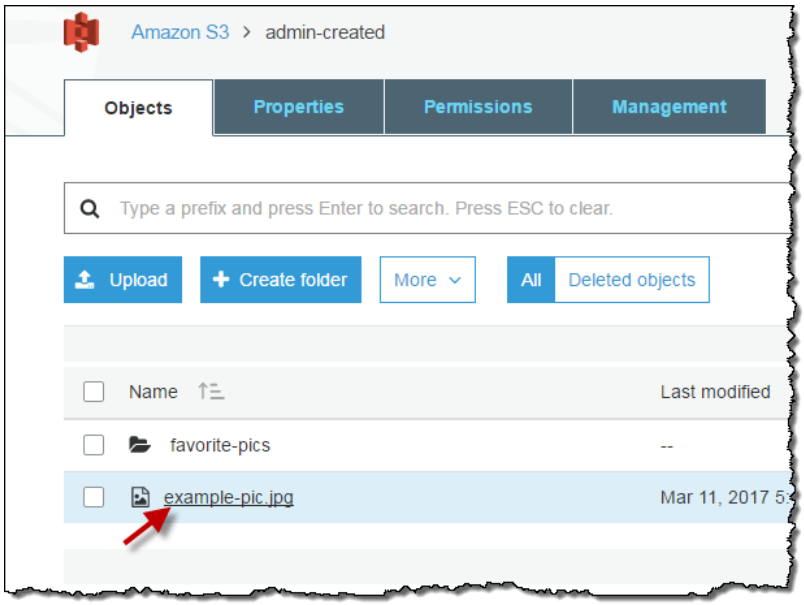
How Do I Add Encryption to an S3 Object?

*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

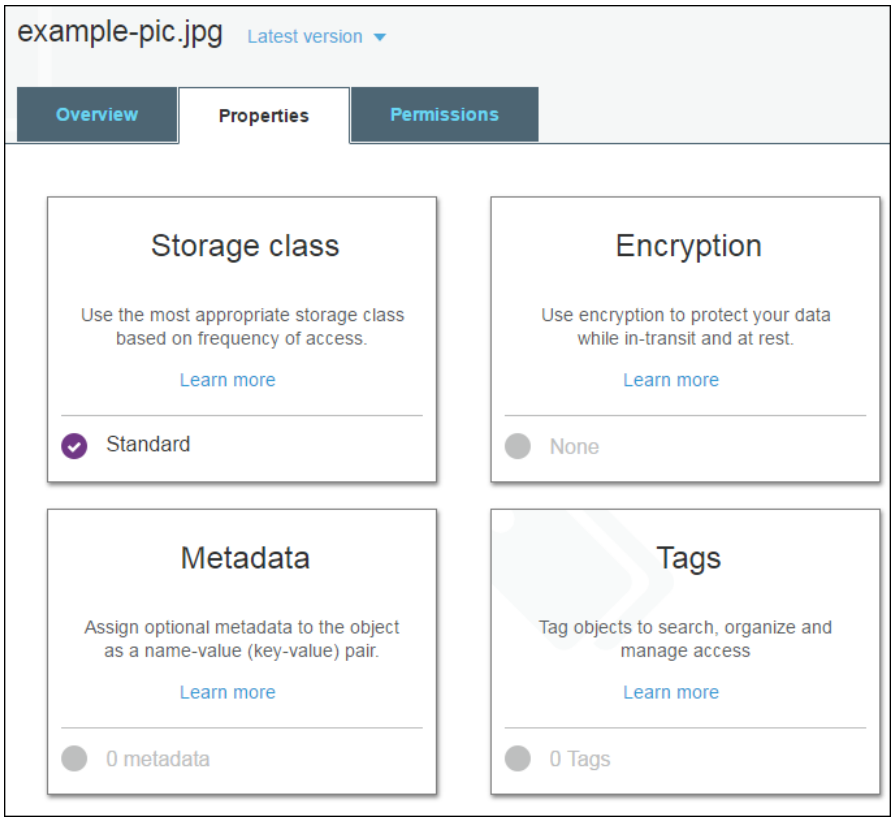
This topic describes how to set or change the type of encryption an object is using.

To add encryption to an object

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that contains the object.
3. In the **Name** list, choose the name of the object that you want to add encryption to.



4. Choose **Properties**, and then choose **Encryption**.



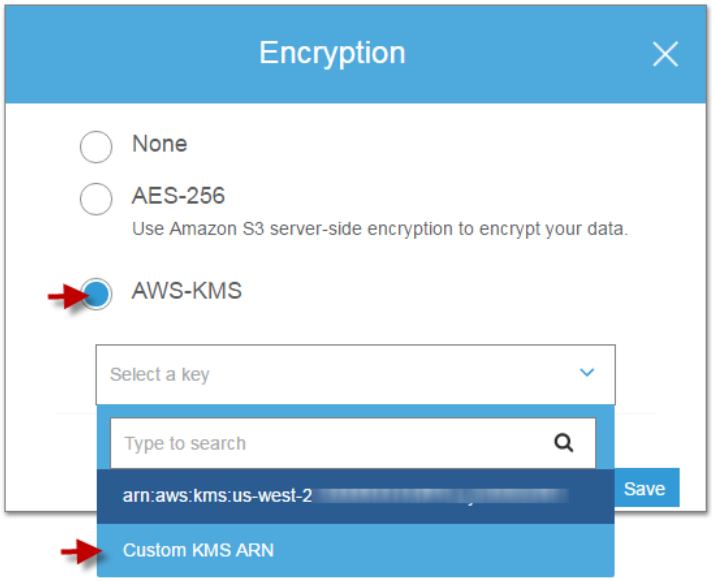
5. Select **AES-256** or **AWS-KMS**.

   a. To encrypt your object using keys that are managed by Amazon S3, select **AES-256**. For more information about using Amazon S3 server-side encryption to encrypt your data, see Protecting Data with Amazon S3-Managed Encryption Keys Classes in the *Amazon Simple Storage Service Developer Guide*.

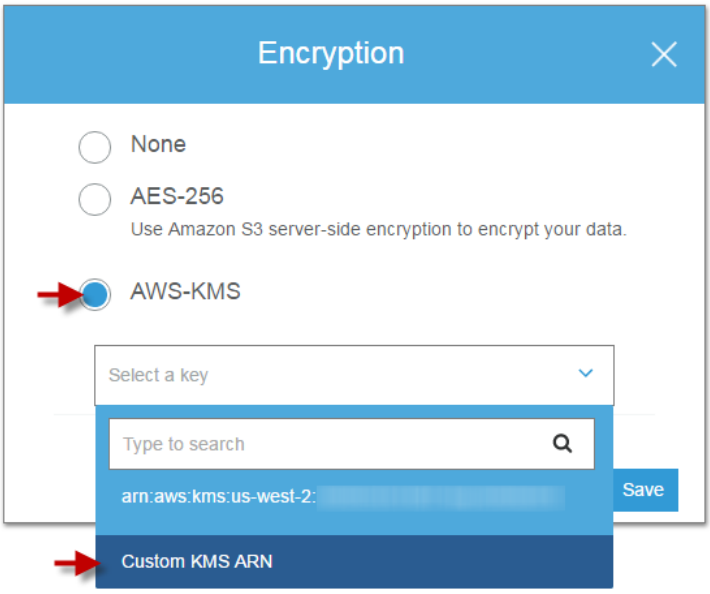
   b. To encrypt your object using AWS Key Management Service (AWS KMS), choose **AWS-KMS**, choose a master key from the list of the AWS KMS master keys that you have created, and then choose **Save**.

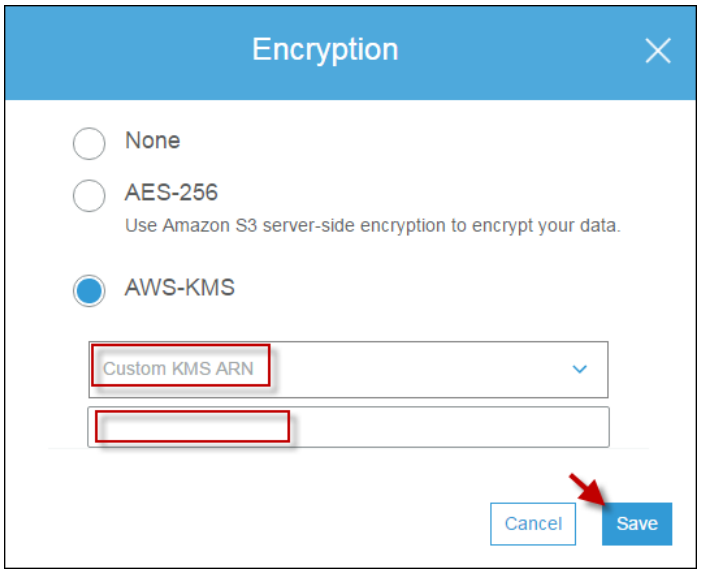
Note
To encrypt objects in the bucket, you can use only keys that are enabled in the same AWS Region as the bucket.

For more information about creating an AWS KMS key, see Creating Keys in the *AWS Key Management Service Developer Guide*. For more information, see Protecting Data with AWS KMS–Managed Key in the *Amazon Simple Storage Service Developer Guide*.



You can give an external account the ability to use an object that is protected by an AWS KMS key. To do this, select **Custom KMS ARN** from the list, type the Amazon Resource Name (ARN) for the external account, and then choose **Save**. Administrators of an external account that have usage permissions to an object protected by your AWS KMS key can further restrict access by creating a resource-level AWS Identity and Access Management (IAM) policy.





More Info

- How Do I View the Properties of an Object? (p. 51)
- Uploading, Downloading, and Managing Objects (p. 31)

How Do I Add Metadata to an S3 Object?

*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

Each object in Amazon Simple Storage Service (Amazon S3) has a set of name-value pairs that provides metadata about the object. *Metadata* is additional information about the object. Some metadata is set by Amazon S3 when you upload the object, for example,`Date` and `Content-Length`. You can also set some metadata when you upload the object, or you can add it later. This section explains how to use the Amazon S3 console to add metadata to an S3 object.

Object metadata is a set of name-value (key-value) pairs. For example, the metadata for content length, `Content-Length`, is the name (key) and the size of the object in bytes (value). For more information about object metadata, see Object Metadata in the *Amazon Simple Storage Service Developer Guide*.

There are two kinds of metadata for an S3 object, system metadata and user-defined metadata:

- **System metadata**–There are two categories of system metadata. Metadata such as the `Last-Modified` date is controlled by the system. Only Amazon S3 can modify the value. There is also system metadata that you control, for example, the storage class configured for the object.
- **User-defined metadata**–You can define your own custom metadata, called user-defined metadata. You can assign user-defined metadata to an object when you upload the object or after the object has been

uploaded. User-defined metadata is stored with the object and is returned when you download the object. Amazon S3 does not process user-defined metadata.

The following topics describe how to add metadata to an object.

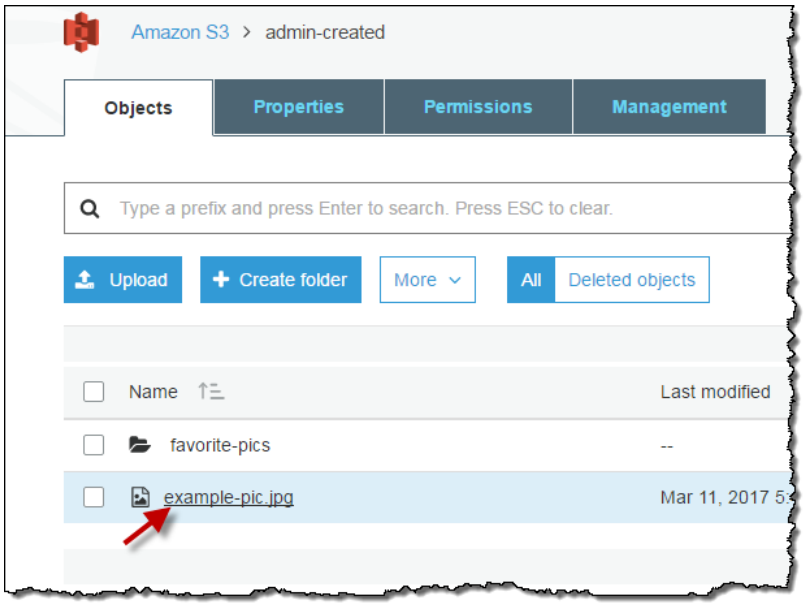
Topics

Adding System-Defined Metadata to an Object

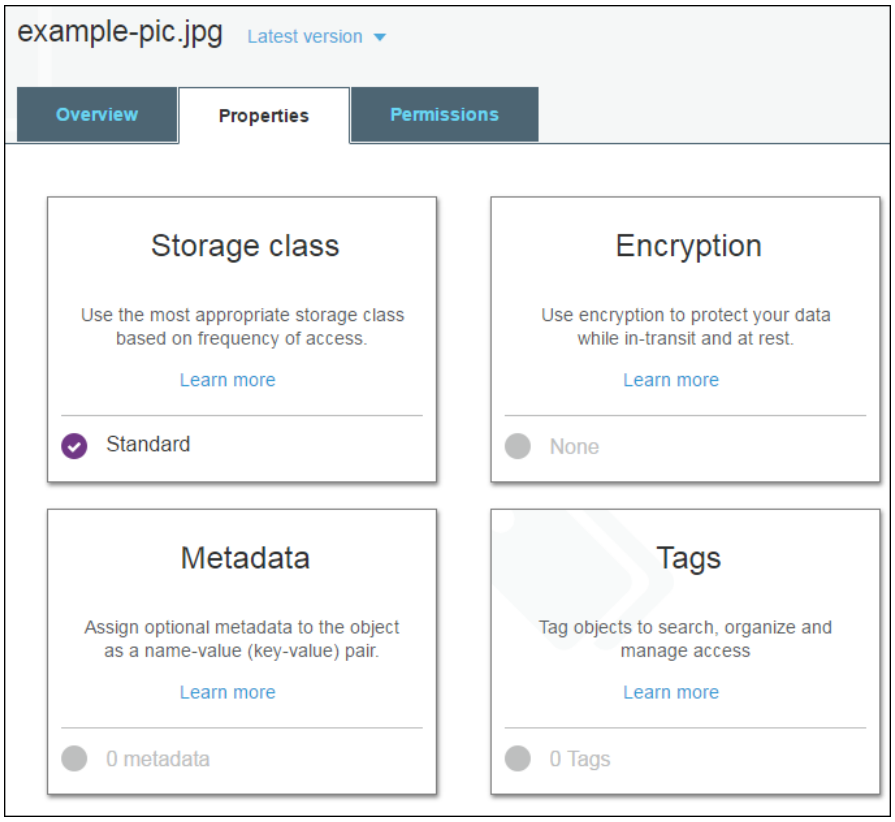
You can configure some system metadata for an S3 object. For a list of system-defined metadata and whether you can modify their values, see System-Defined Metadata in the *Amazon Simple Storage Service Developer Guide*.

To add system metadata to an object

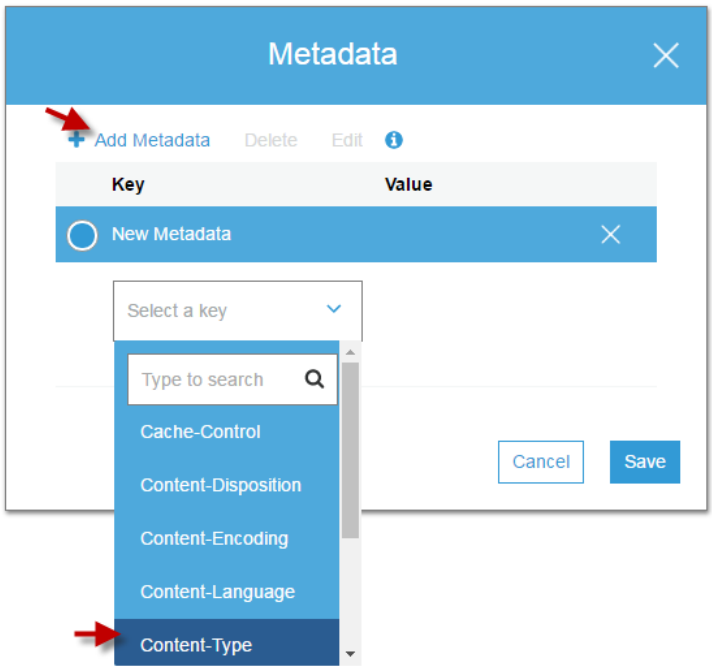
1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that contains the object.
3. In the **Name** list, choose the name of the object that you want to add metadata to.



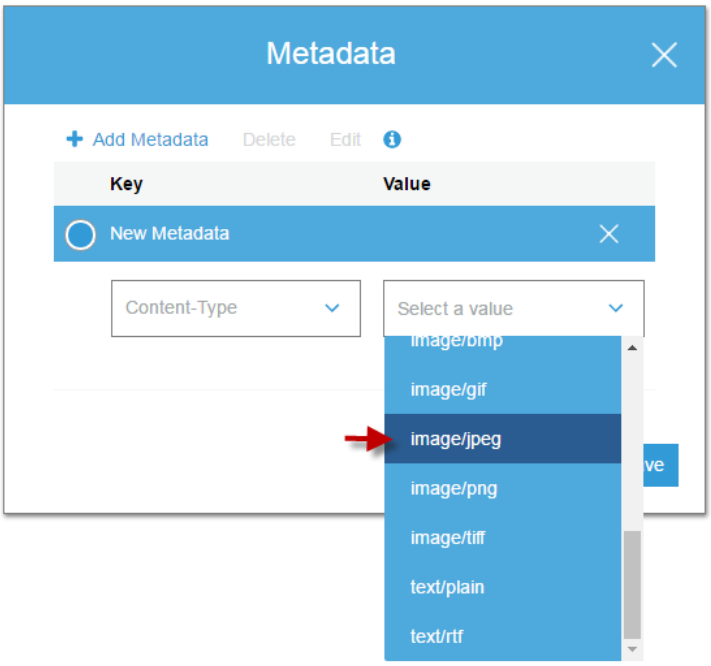
4. Choose **Properties**, and then choose **Metadata**.



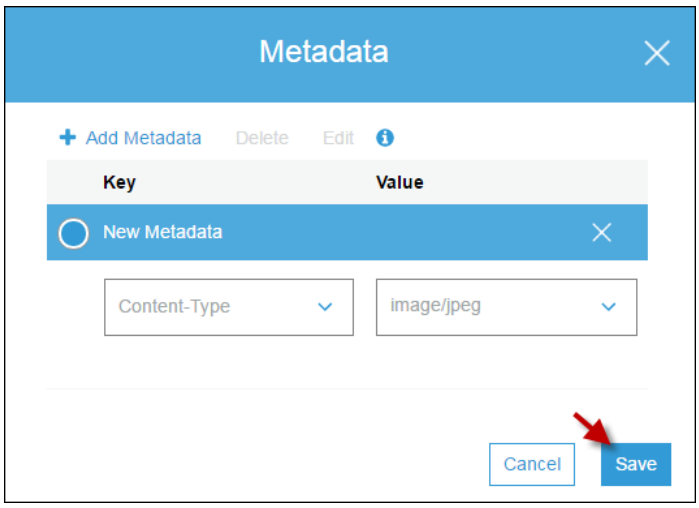
5. Choose **Add Metadata**, and then choose a key from the **Select a key** menu.



6. Depending on which key you chose, choose a value from the **Select a value** menu or type a value.



7. Choose **Save**.



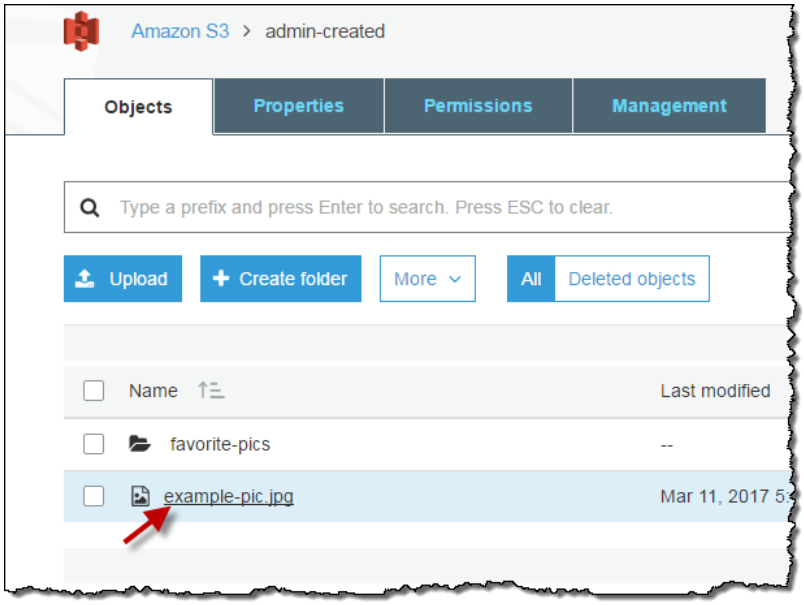
Adding User-Defined Metadata to an Object

You can assign user-defined metadata to an object. User-defined metadata must begin with the prefix "`x-amz-meta-`", oherwise Amazon S3 will not set the key value pair as you define it. You define custom metadata by adding a name that you choose to the `x-amz-meta-` key. This creates a custom key. For example, if you add the custom name `alt-name`, the metadata key would be `x-amz-meta-alt-name`.

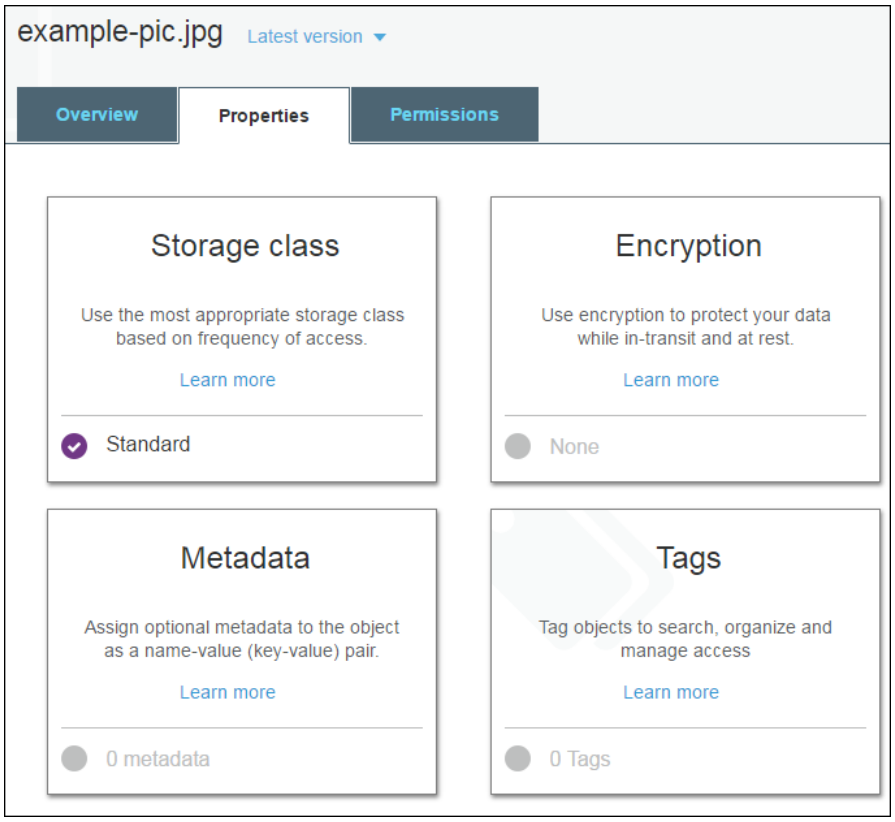
User-defined metadata can be as large as 2 KB. Both keys and their values must conform to US-ASCII standards. For more information, see User-Defined Metadata in the *Amazon Simple Storage Service Developer Guide*.

To add user-defined metadata to an object

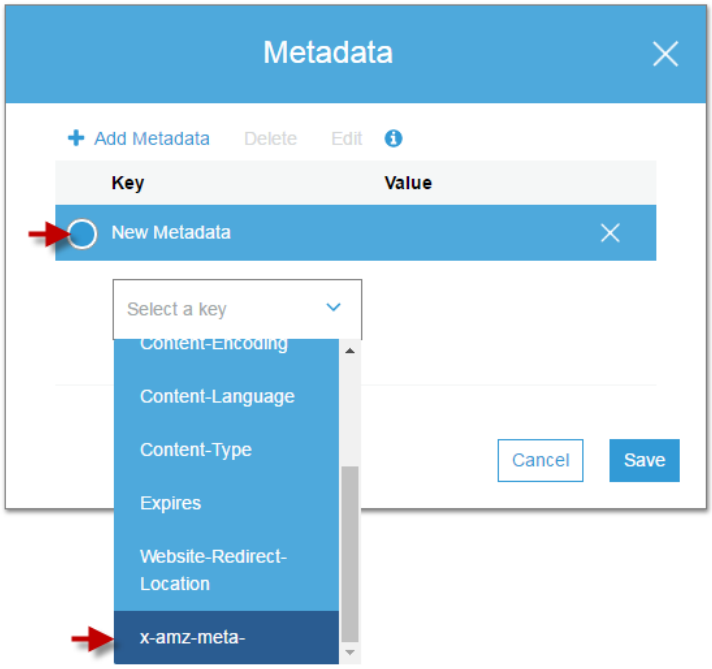
1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that contains the object.
3. In the **Name** list, choose the name of the object that you want to add metadata to.



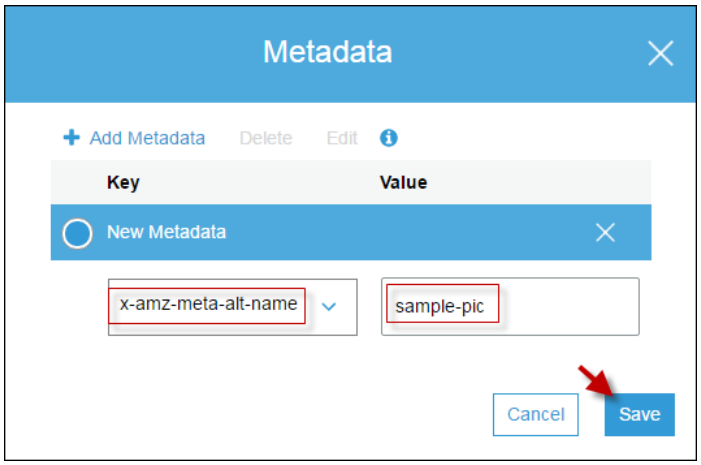
4. Choose **Properties**, and then choose **Metadata**.



5. Choose **Add Metadata**, and then choose the `x-amz-meta-` key from the **Select a key** menu. Any metadata starting with the prefix `x-amz-meta-` is user-defined metadata.



6. Type a custom name following the `x-amz-meta-` key. For example, for the custom name `alt-name`, the metadata key would be `x-amz-meta-alt-name`. Enter a value for the custom key, and then choose **Save**.



More Info

- How Do I View the Properties of an Object? (p. 51)
- Uploading, Downloading, and Managing Objects (p. 31)

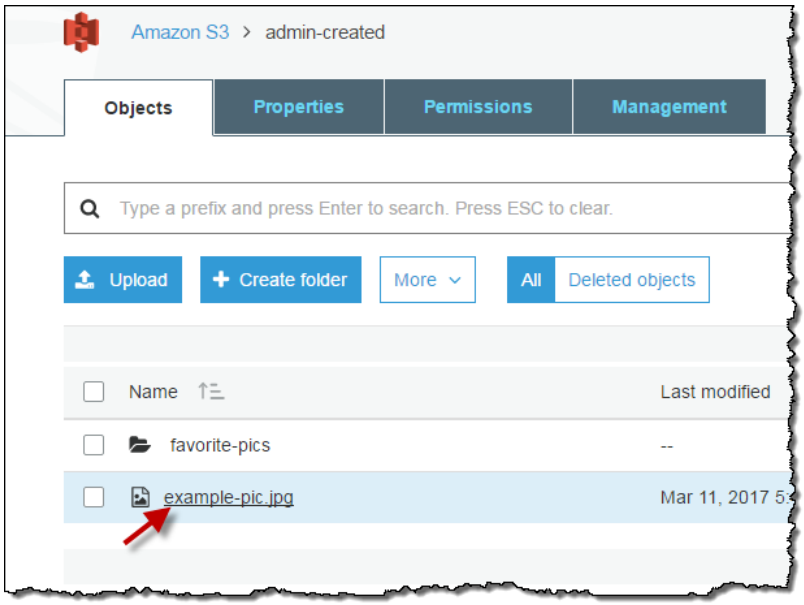
How Do I Add Tags to an S3 Object?

*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

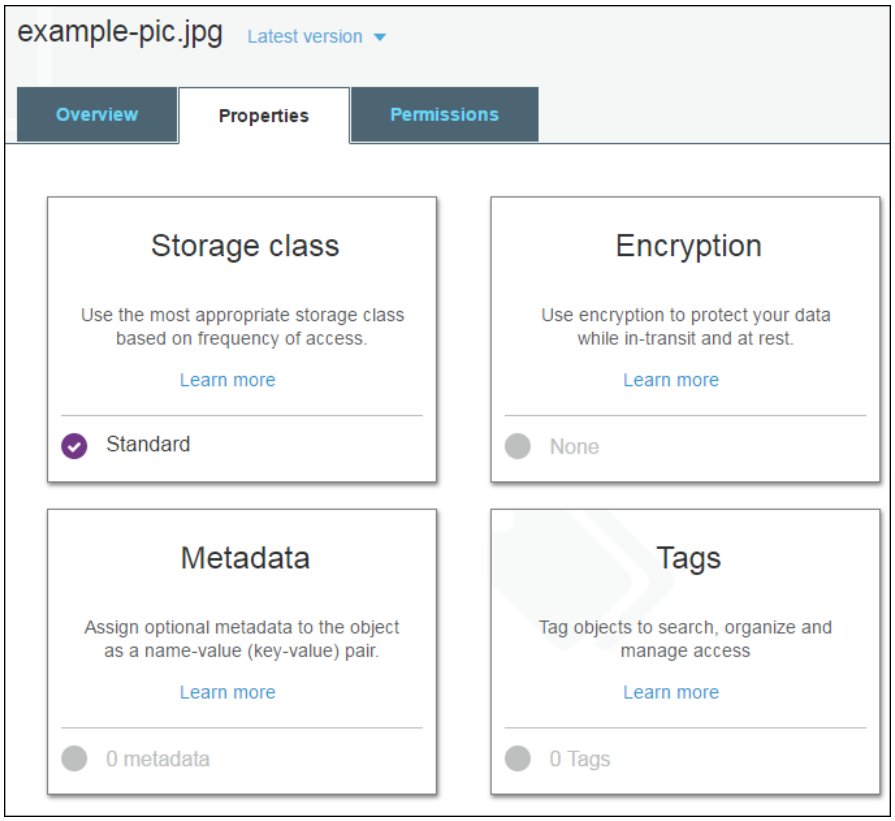
This topic explains how to use the console to add tags to an S3 object. For information about object tags, see Object Tagging in the *Amazon Simple Storage Service Developer Guide*

To add tags to an object

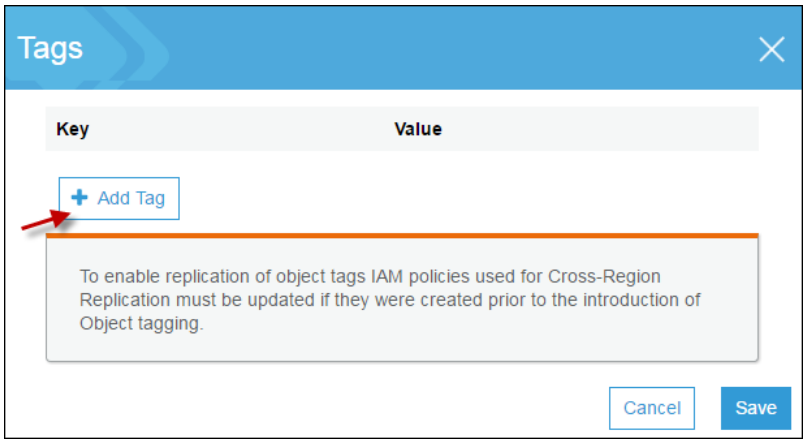
1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that contains the object.
3. In the **Name** list, choose the name of the object you want to add tags to.



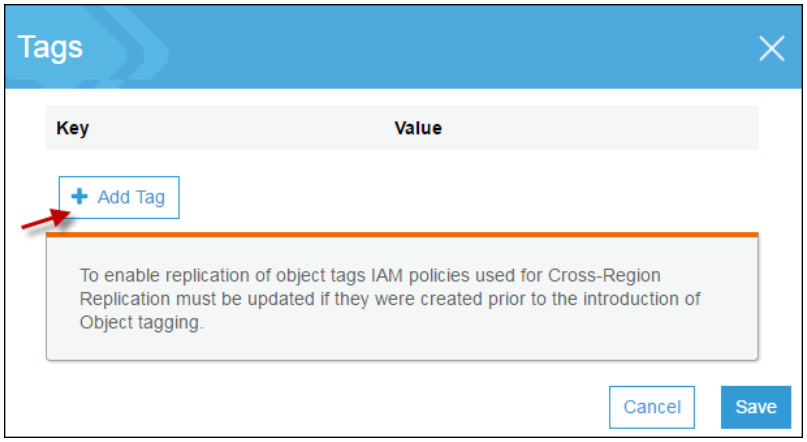
4. Choose **Properties**.



5. Choose **Tags** and then choose **Add Tag**.

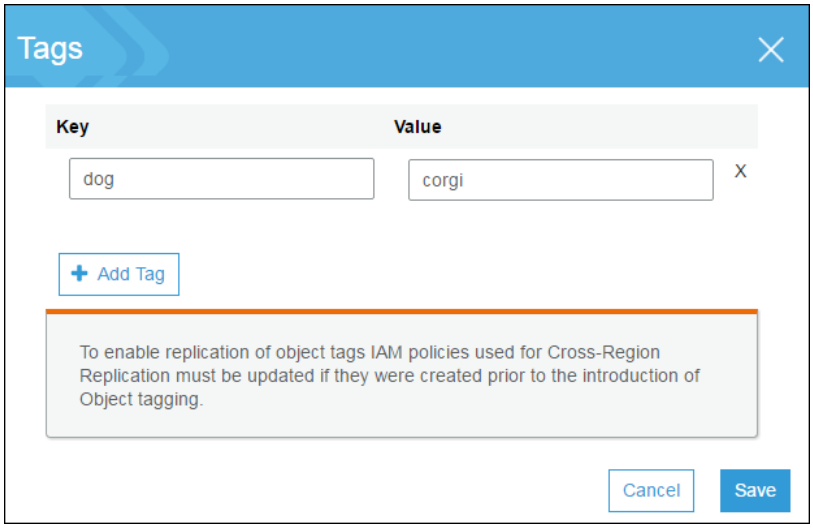


6. Choose **Tags** and then choose **Add Tag**.



7. Each tag is a key-value pair. Type a **Key** and a **Value**. Then choose **Add Tag** to add another tag or choose **Save**.

   You can enter up to 10 tags for an object.



More Info

- How Do I View the Properties of an Object? (p. 51)
- Uploading, Downloading, and Managing Objects (p. 31)

Storage Management

*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

This section explains how to configure Amazon S3 storage management tools.

Topics

How Do I Create a Lifecycle Policy for an S3 Bucket?

*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

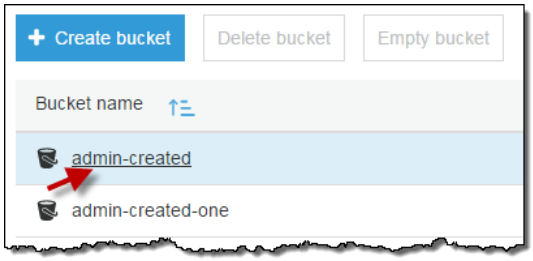
You can use lifecycle policies to define actions you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time).

You can define a lifecycle policy for all objects or a subset of objects in the bucket by using a shared prefix (that is, objects that have names that begin with a common string).

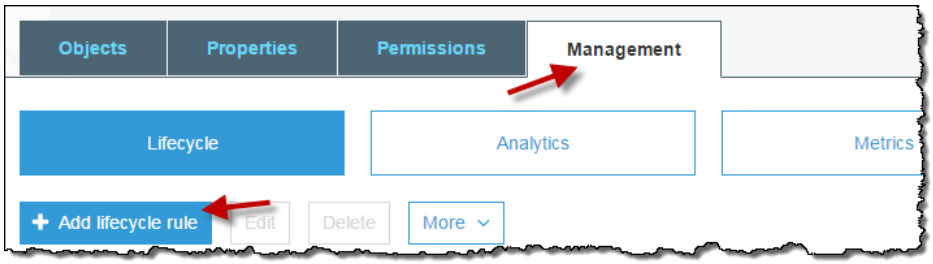
A versioning-enabled bucket can have many versions of the same object, one current version and zero or more noncurrent (previous) versions. Using a lifecycle policy, you can define actions specific to current and noncurrent object versions. For more information, see Object Lifecycle Management and Object Versioning and Using Versioning in the *Amazon Simple Storage Service Developer Guide*.

To create a lifecycle policy

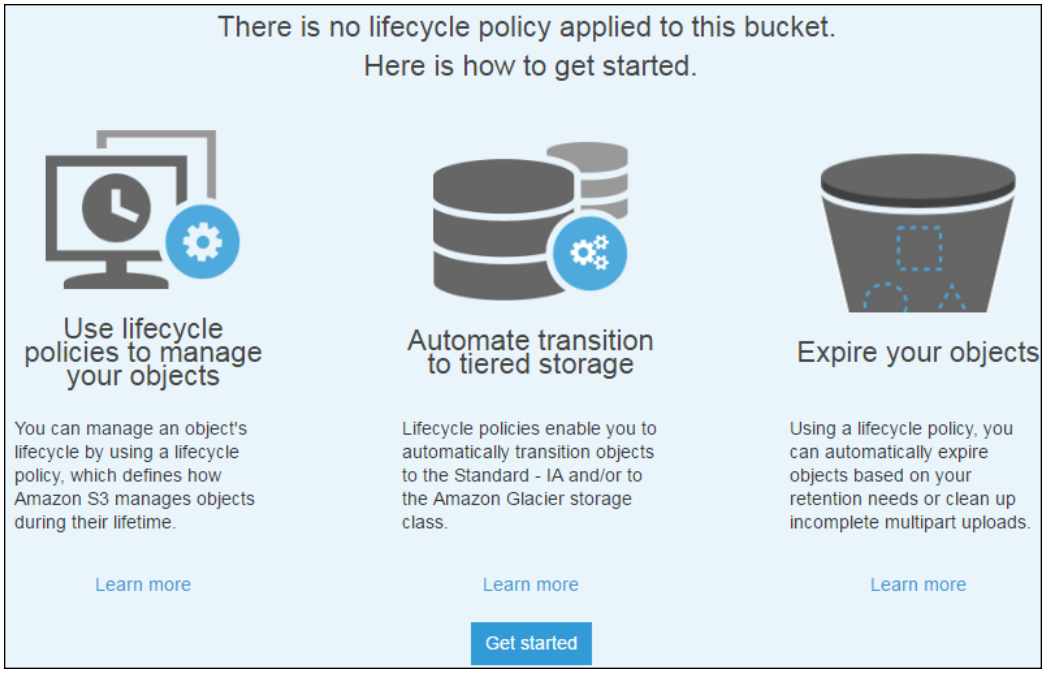
1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that you want to create a lifecycle policy for.



3. Choose the **Management** tab, and then choose **Add lifecycle rule**.

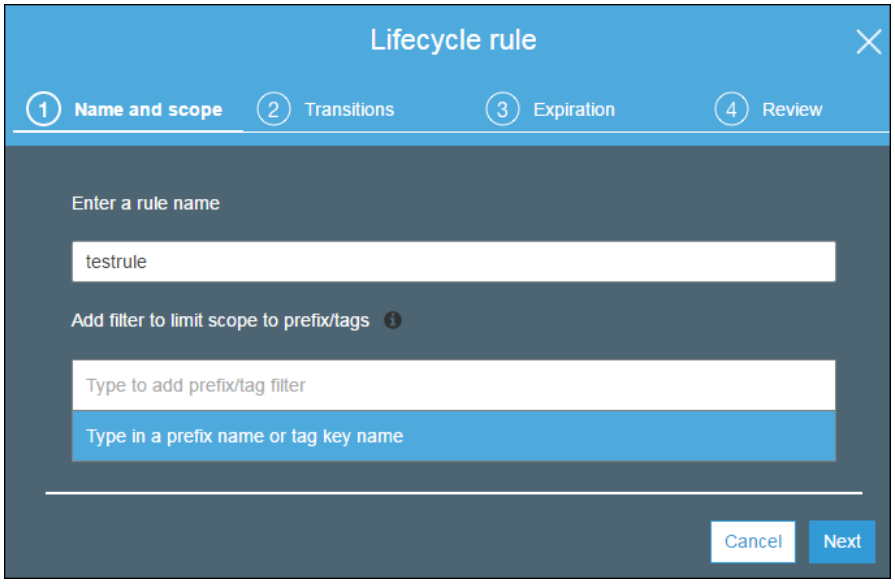


- If the bucket does not have a lifecycle policy, you can choose **Get started**.



4. In the **Lifecycle rule** dialog box, type a name for your rule to help identify the rule later. The name must be unique within the bucket. Configure the rule as follows:

   - To apply this lifecycle rule to all objects with a specified name prefix (i.e., objects whose name begins with a common string), type in a prefix. You can also limit the lifecycle rule scope to one or more object tags. You can combine a prefix and tags. For more information about object name prefixes, see Object Keys in the *Amazon Simple Storage Service Developer Guide*. For more information about object tags, see Object Tagging in the *Amazon Simple Storage Service Developer Guide*
   - To apply this lifecycle rule to all objects in the bucket, choose **Next**.

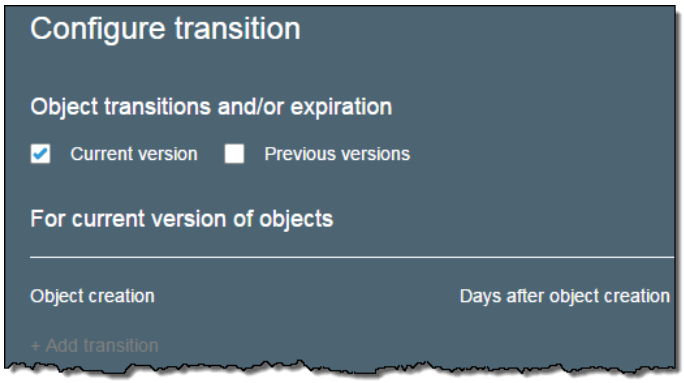


5. You configure lifecycle rules by defining rules to transition objects to the Standard-IA and Amazon Glacier storage classes. For more information, see Storage Classes in the *Amazon Simple Storage Service Developer Guide*.

   You can define transitions for current or previous object versions, or for both current and previous versions.

   a. Select **Current version** to define transitions that are applied when an object is created that is within the scope of the rule.

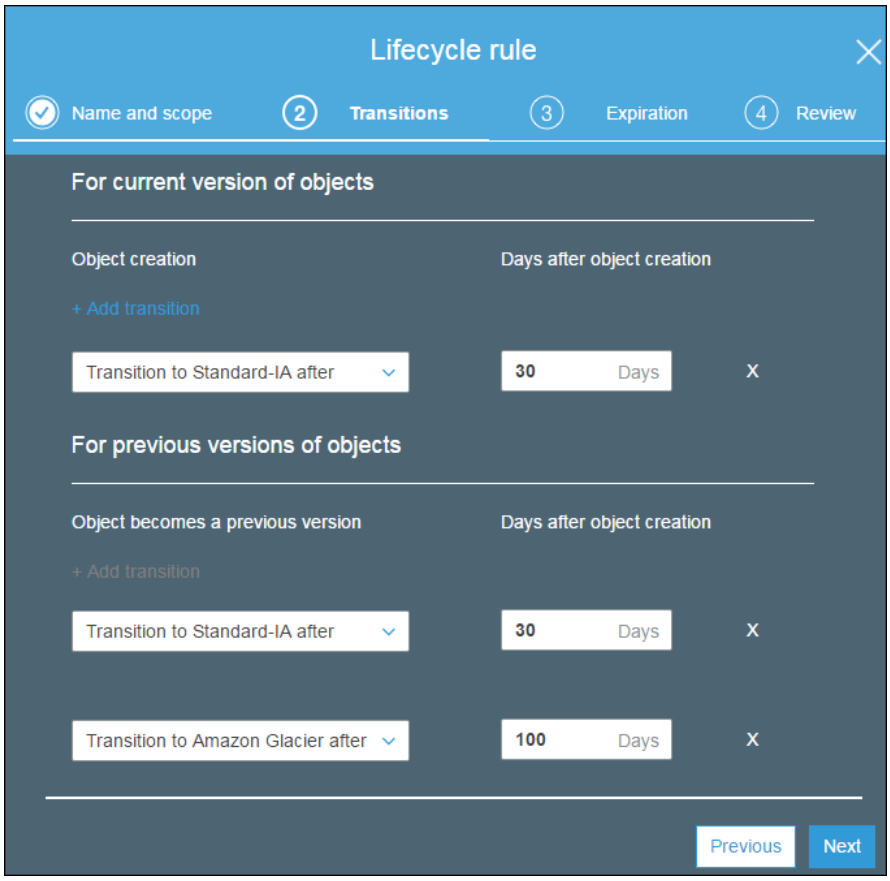
      Select **Previous version** to define transitions that are applied when an object is created that is within the scope of the rule.



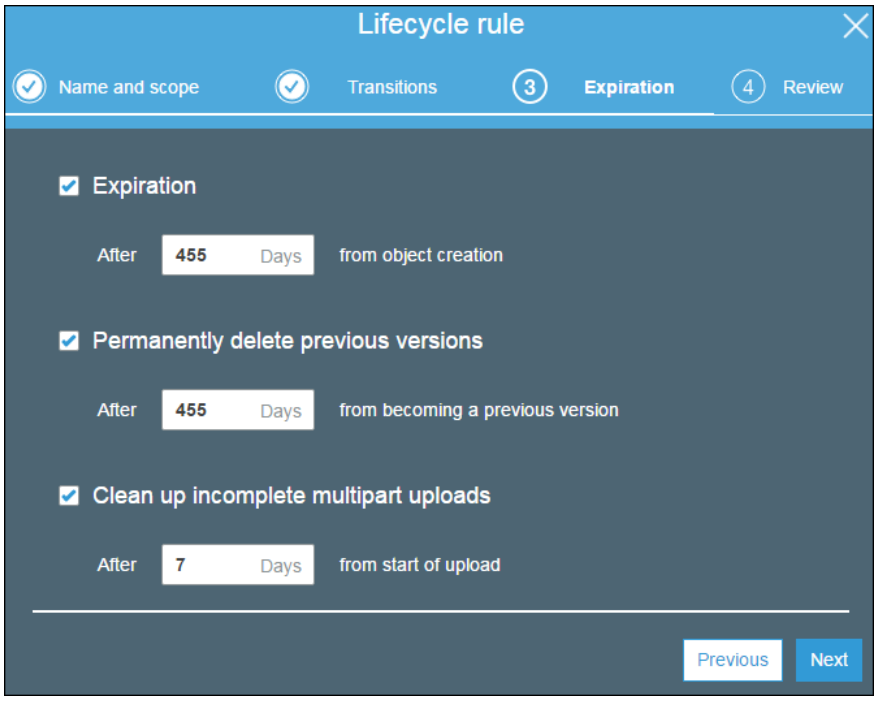
b. Choose **Add transitions** and specify one of the following transitions:

- Choose **Transition to Standard-IA after**, and then type the number of days after the creation of an object that you want the transition to be applied (for example, 30 days).
- Choose **Transition to Amazon Glacier after**, and then type the number of days after the creation of an object that you want the transition to be applied (for example, 100 days).

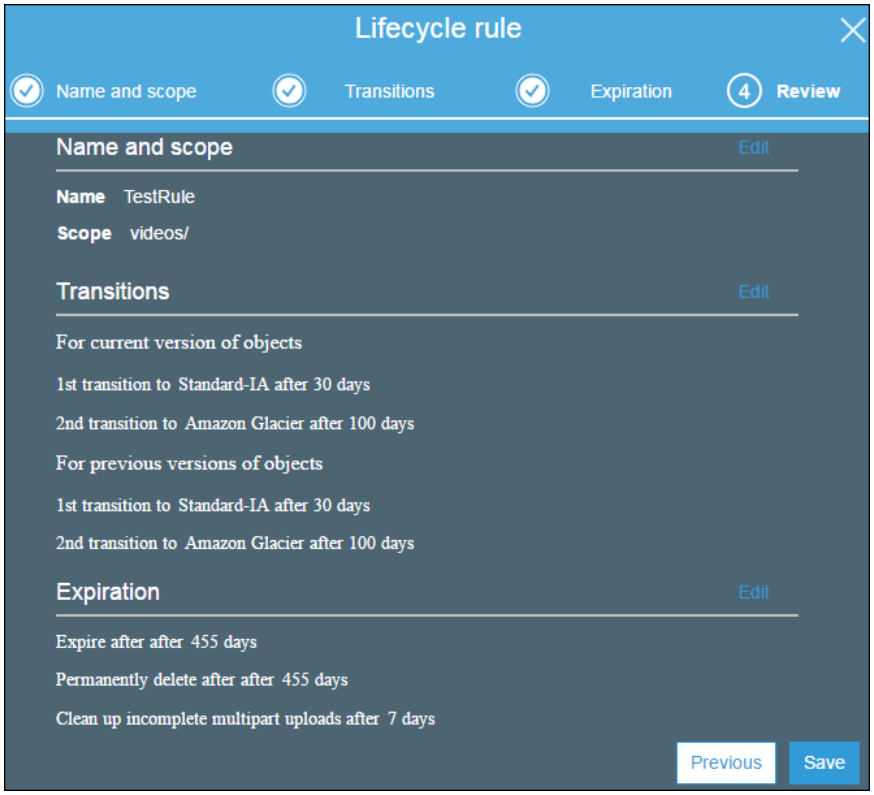
6. When you are done configuring transitions, choose **Next**.



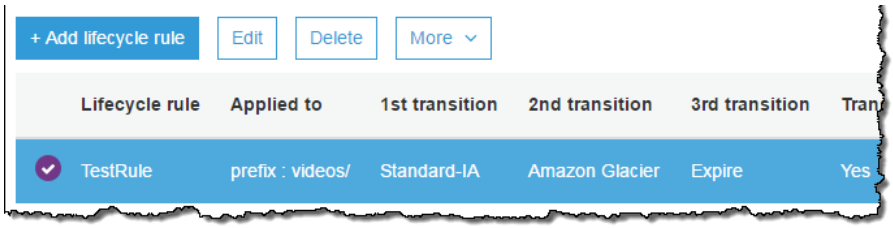
7. Select **Expiration** and then enter the number of days after object creation to delete the object (for example, 455 days).
8. Select **Permanently delete previous versions** and then enter the number of days after an object becomes a previous version to permanently delete the object (for example, 455 days).
9. It is a recommended best practice to always select **Clean up incomplete multipart uploads**. For example, type 7 for the number of days after the multipart upload initiation date that you want to end and clean up any multipart uploads that have not completed. For more information about multipart uploads, see Multipart Upload Overview in the Amazon Simple Storage Service Developer Guide.
10. Choose **Next**.



11. For **Review**, verify the settings for your rule. If you need to make changes, choose **Previous**. Otherwise, choose **Save**.



12. If the rule does not contain any errors, it is listed on the **Lifecycle** page and is enabled.



How Do I Configure Storage Class Analysis?

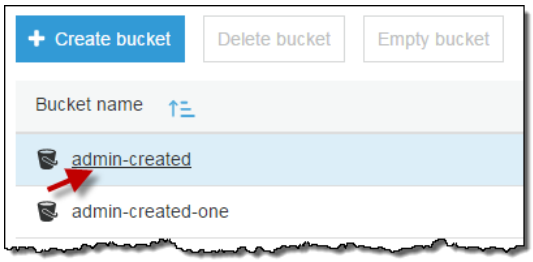
*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

By using the Amazon S3 analytics storage class analysis tool you can analyze storage access patterns to help you decide when to transition the right data to the right storage class. Storage class analysis observes data access patterns to help you determine when to transition less frequently accessed STANDARD storage to the STANDARD_IA (IA, for infrequent access) storage class. For more information about STANDARD_IA, see the Amazon S3 FAQ and Storage Classes in the *Amazon Simple Storage Service Developer Guide*.

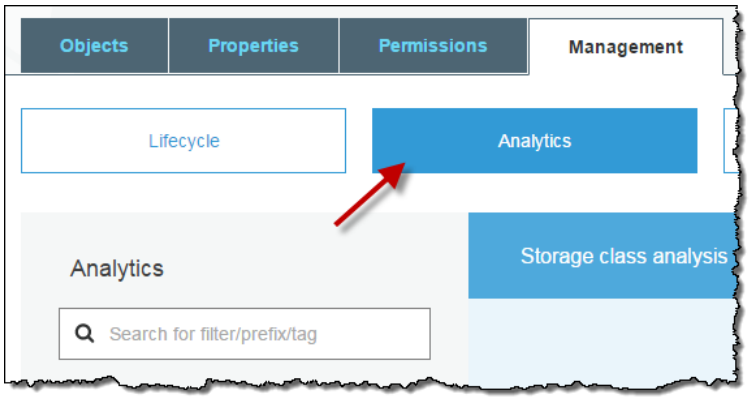
For more information about analytics, see Amazon S3 Analytics – Storage Class Analysis in the *Amazon Simple Storage Service Developer Guide*.

To configure storage class analysis

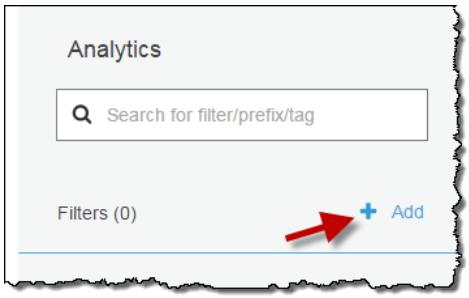
1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket for which you want to configure storage class analysis.



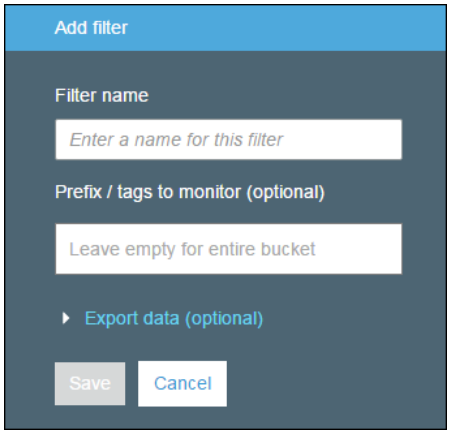
3. Choose the **Management** tab, and then choose **Analytics**.



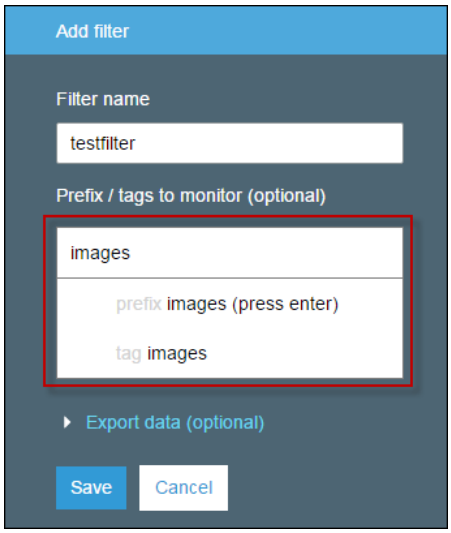
4. Choose **Add**.



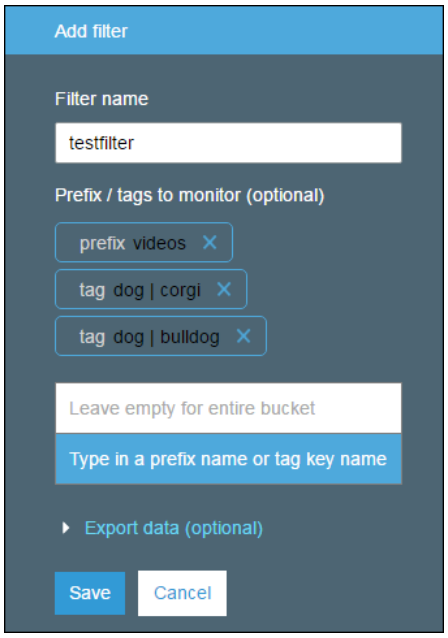
5. Type a name for the filter. If you want to analyze the whole bucket, leave the **Prefix / tags** field empty.



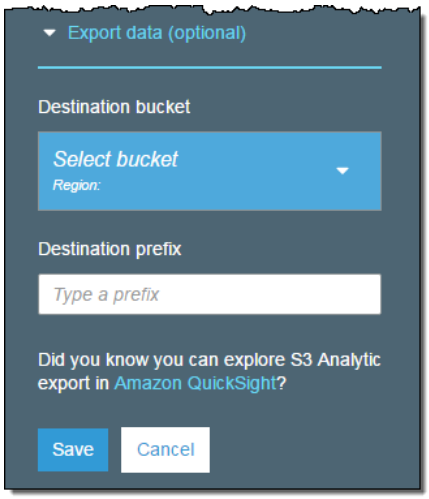
6. In the **Prefix / tags** field, type text for the prefix or tag for the objects that you want to analyze, or choose from the dropdown list that appears when you start typing.



7. If you chose **tag**, enter a value for the tag. You can enter one prefix and multiple tags.



8. Optionally, you can choose **Export data** to export analysis reports to a comma-separated values (.csv) flat file. Choose a destination bucket where the file can be stored. You can type a prefix for the destination bucket. The destination bucket must be in the same AWS Region as the bucket for which you are setting up the analysis. The destination bucket can be in a different AWS account.



9. Choose **Save**.

After you choose **Save**, Amazon S3 creates a bucket policy on the destination bucket to grant Amazon S3 write permission to allow the export data to be written to the bucket.

If there is an error when trying to create the bucket policy you'll will be given instructions on how to fix the error. For example, if you chose a destination bucket in another AWS account and do not have permissions to read and write the bucket policy, you'll see the following message. You must have the destination bucket owner add the displayed bucket policy to the destination bucket. If the policy is not added to the destination bucket you won't get the export data because Amazon S3 doesn't have permission to write to the destination bucket. If the source bucket is owned by a different account than that of the current user, then the correct account ID of the source bucket must be substituted in the policy.

For information about the exported data and how the filter works, see Amazon S3 Analytics – Storage Class Analysis in the *Amazon Simple Storage Service Developer Guide*.

More Info

- Storage Management (p. 66)

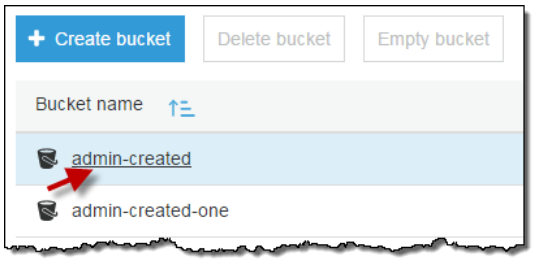
How Do I Configure Storage Inventory?

*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

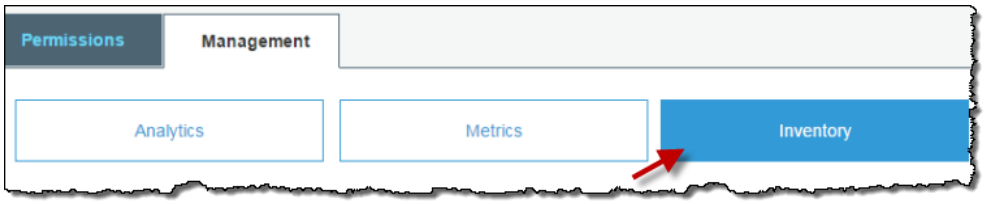
Amazon S3 inventory provides a flat file list of your objects and metadata, which is a scheduled alternative to the Amazon S3 synchronous List API operation. Amazon S3 inventory provides a comma-separated values (.csv) flat-file output of your objects and their corresponding metadata on a daily or weekly basis for an S3 bucket or for objects that share a prefix (objects that have names that begin with the same string). For more information, see Amazon S3 Storage Inventory in the *Amazon Simple Storage Service Developer Guide*.

To configure inventory

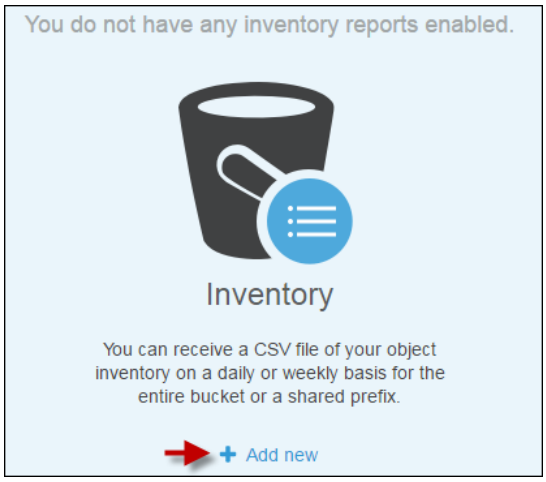
1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket for which you want to configure storage inventory.



3. Choose the **Management** tab, and then choose **Inventory**.

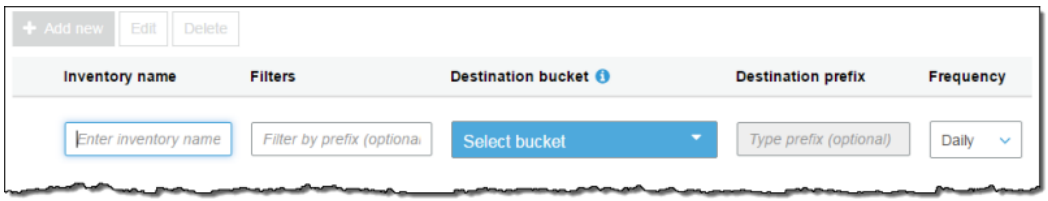


4. Choose **Add new** if you do not have any inventory reports enabled.



5. Type a name for the inventory and set it up as follows:

   - Optionally, add a prefix for your filter to inventory only objects whose names begin with the same string.
   - Choose the destination bucket where you want reports to be saved. The destination bucket must be in the same AWS Region as the bucket for which you are setting up the inventory. The destination bucket can be in a different AWS account.
   - Optionally, choose a prefix for the destination bucket.
   - Choose how frequently to generate the inventory.

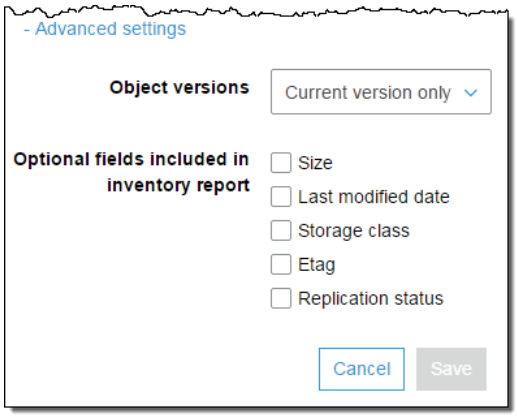


6. Under **Advanced Settings** you can set the following.

   a. To include all versions of the objects in the inventory, choose **Include All Versions** from the **Object Versions** menu. By default the inventory includes only the current version of the objects.

   b. Select one or more of the following optional fields to add to the inventory report:

      - **Size** – Object size in bytes.
      - **Last modified date** – Object creation date or the last modified date, whichever is the latest.
      - **Storage class** – Storage class used for storing the object.
      - **ETag** – The entity tag is a hash of the object. The ETag reflects changes only to the contents of an object, not its metadata. The ETag may or may not be an MD5 digest of the object data. Whether or not it is depends on how the object was created and how it is encrypted.
      - **Replication status** – The Cross Region Replication status of the object. For more information, see How Do I Enable and Configure Cross-Region Replication for an S3 Bucket? (p. 19).



7. Choose **Save**.

After you choose **Save**, Amazon S3 creates a bucket policy on the destination bucket to grant Amazon S3 write permission to allow data for the inventory reports to be written to the bucket.

If there is an error when trying to create the bucket policy you'll will be given instructions on how to fix the error. For example, if you chose a destination bucket in another AWS account and do not have permissions to read and write the bucket policy, you'll see the following message. In this case you must have the destination bucket owner add the displayed bucket policy to the destination bucket. If the policy is not added to the destination bucket you won't get an inventory report because Amazon S3 doesn't have permission to write to the destination bucket. If the source bucket is owned by a different account than that of the current user, then the correct account ID of the source bucket must be substituted in the policy.

For more information about storage inventories, see Amazon S3 Storage Inventory in the *Amazon Simple Storage Service Developer Guide*.

More Info

- Storage Management (p. 66)

How Do I Configure Request Metrics for an S3 Bucket?

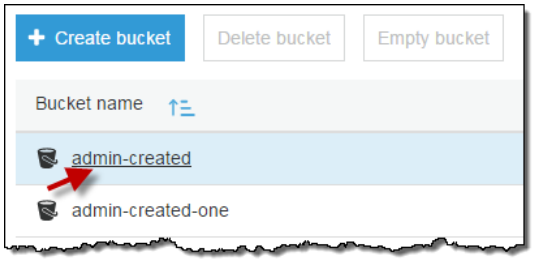
*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

There are two types of CloudWatch metrics for Amazon S3: storage metrics and request metrics. Storage metrics are reported once per day and are provided to all customers at no additional cost. Request metrics are available at 1-minute intervals after some latency to process, and metrics are billed at the standard CloudWatch rate. To get request metrics, you must opt into them by configuring them in the console or with the Amazon S3 API.

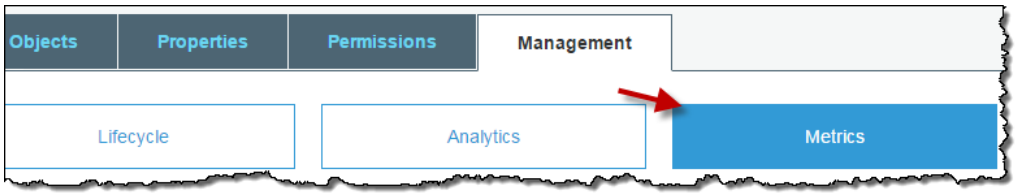
For more conceptual information about CloudWatch metrics for Amazon S3, see Monitoring Metrics with Amazon CloudWatch in the *Amazon Simple Storage Service Developer Guide*.

To configure request metrics on a bucket

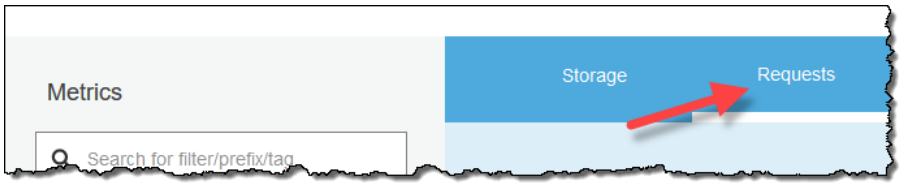
1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that has the objects you want to get request metrics for.



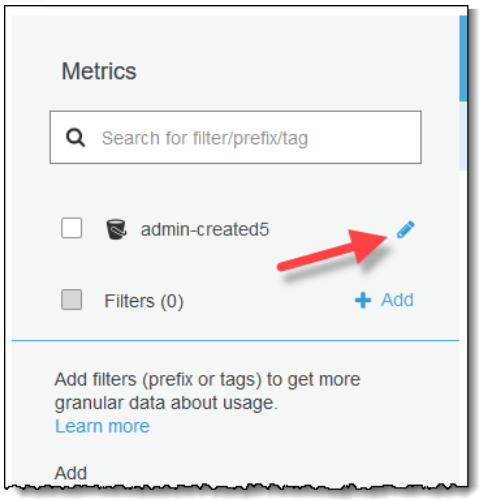
3. Choose the **Management** tab, and then choose **Metrics**.



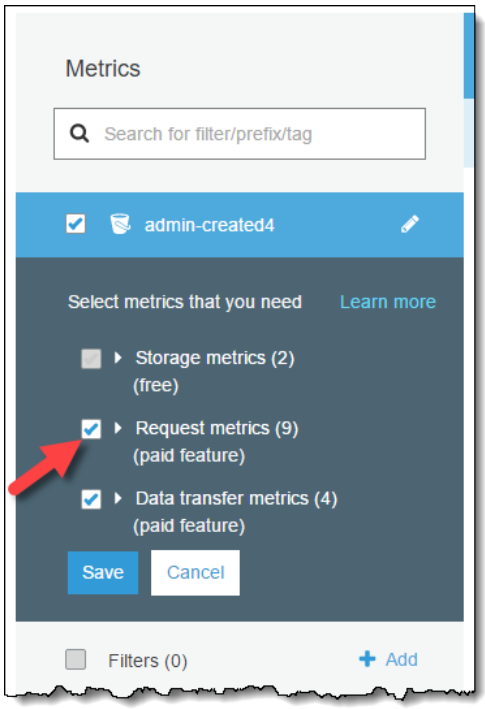
4. Choose **Requests**.



5. From the name of your bucket in the left-side pane, choose the edit icon.



6. Choose the **Request metrics** check box. This also enables Data Transfer metrics.



7. Choose **Save**.

You have now created a metrics configuration for all the objects in an Amazon S3 bucket. About 15 minutes after CloudWatch begins tracking these request metrics, you can see graphs for the metrics in both the Amazon S3 or CloudWatch consoles. You can also define a filter so the metrics are only collected and reported on a subset of objects in the bucket. For more information, see How Do I Configure a Request Metrics Filter? (p. 81).

How Do I Configure a Request Metrics Filter?

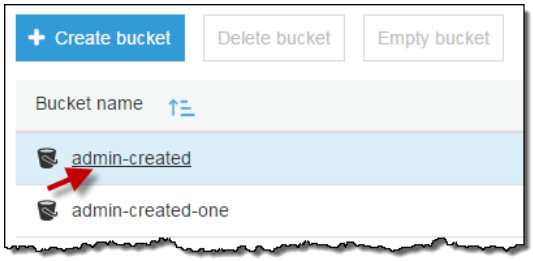
*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

There are two types of CloudWatch metrics for Amazon S3: storage metrics and request metrics. Storage metrics are reported once per day and are provided to all customers at no additional cost. Request metrics are available at 1 minute intervals after some latency to process, and metrics are billed at the standard CloudWatch rate. To get request metrics, you must opt into them by configuring them in the console or with the Amazon S3 API.

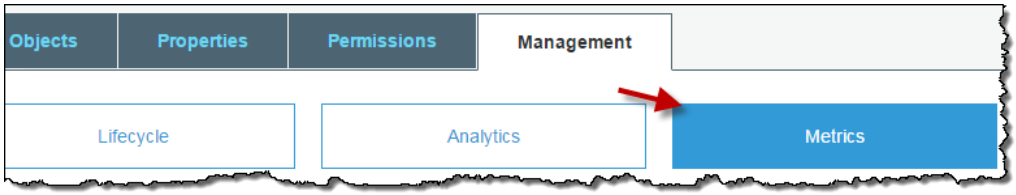
For more conceptual information about CloudWatch metrics for Amazon S3, see Monitoring Metrics with Amazon CloudWatch in the *Amazon Simple Storage Service Developer Guide*.

To filter request metrics on a subset of objects in a bucket

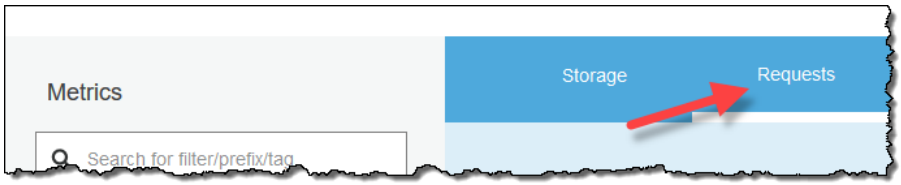
1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that has the objects you want to get request metrics for.



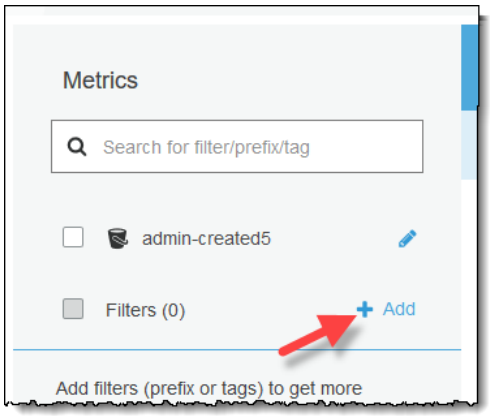
3. Choose the **Management** tab. and then choose **Metrics**.



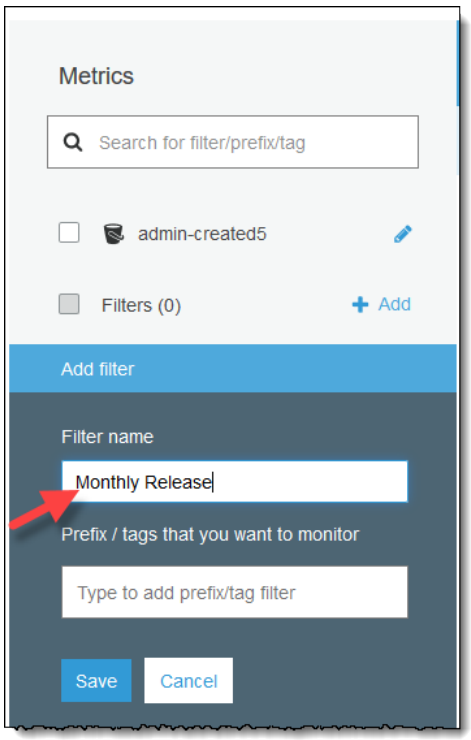
4. Choose **Requests**.



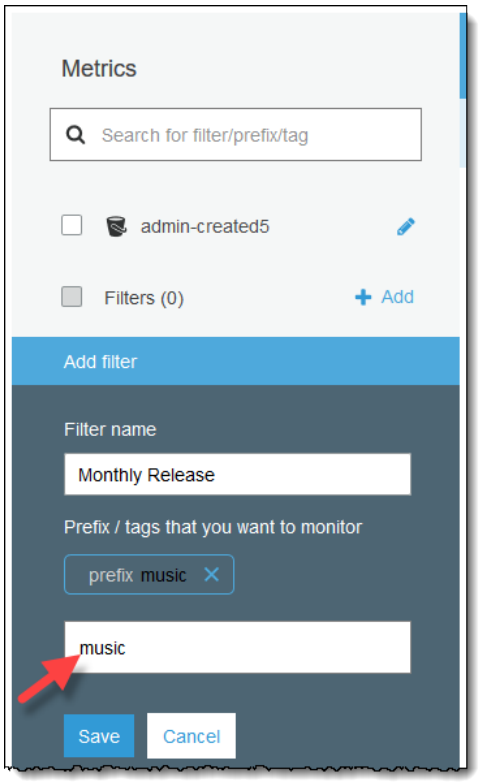
5. From **Filters** in the left-side pane, choose **Add**.



6. Provide a name for this metrics configuration.



7. Provide one or more prefixes or tags, separated by commas, in **Prefix /tags that you want to monitor**. From the drop down, select whether the value you provided is a tag or a prefix.



8. Choose **Save**.

You have now created a metrics configuration for request metrics on a subset of the objects in an Amazon S3 bucket. About 15 minutes after CloudWatch begins tracking these request metrics, you can see graphs for the metrics in both the Amazon S3 or CloudWatch consoles. You can also request metrics at the bucket level. For information, see How Do I Configure Request Metrics for an S3 Bucket? (p. 79)

Setting Bucket and Object Access Permissions

*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

The topics in this section explain how to use the Amazon S3 console to grant access permissions to your buckets and objects by using resource-based access policies. An access policy describes who has access to resources. You can associate an access policy with a resource.

Buckets and objects are Amazon Simple Storage Service (Amazon S3) resources. By default, all Amazon S3 resources are private, which means that only the resource owner can access the resource. The resource owner is the AWS account that creates the resource. For more information about resource ownership and access policies, see Overview of Managing Access in the *Amazon Simple Storage Service Developer Guide*.

Bucket access permissions specify which users are allowed access to the objects in a bucket and which types of access they have. *Object access permissions* specify which users are allowed access to the object and which types of access they have. For example, one user might have only read permission, while another might have read and write permissions.

Bucket and object permissions are independent of each other. An object does not inherit the permissions from its bucket. For example, if you create a bucket and grant write access to a user, you will not be able to access that user's objects unless the user explicitly grants you access.

To grant access to your buckets and objects to other AWS accounts and to the general public, you use resource-based access policies called access control lists (ACLs).

A *bucket policy* is a resource-based AWS Identity and Access Management (IAM) policy that grants other AWS accounts or IAM users access to an S3 bucket. Bucket policies supplement, and in many cases,

replace ACL-based access policies. For more information on using IAM with Amazon S3, see Managing Access Permissions to Your Amazon S3 Resources in the *Amazon Simple Storage Service Developer Guide*.

For more in-depth information about managing access permissions, see Introduction to Managing Access Permissions to Your Amazon S3 Resources in the *Amazon Simple Storage Service Developer Guide*.

This section also explains how to use the Amazon S3 console to add a cross-origin resource sharing (CORS) configuration to an S3 bucket. CORS allows client web applications that are loaded in one domain to interact with resources in another domain.

Topics

How Do I Set Permissions on an Object?

*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

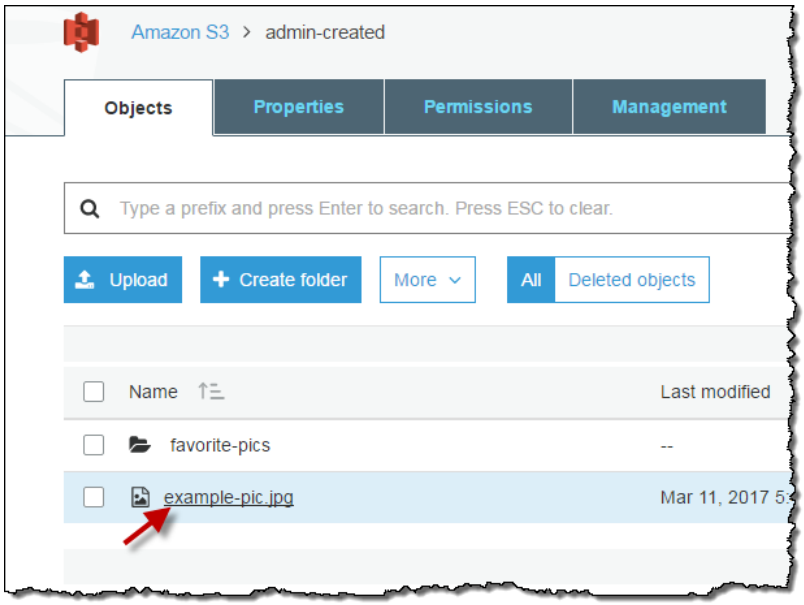
This section explains how to use the Amazon Simple Storage Service (Amazon S3) console to manage access permissions for an S3 object by using access control lists (ACLs). ACLs are resource-based access policies that grant access permissions to buckets and objects. For more information about managing access permissions with resource-based policies, see Overview of Managing Access in the *Amazon Simple Storage Service Developer Guide*.

In addition to granting permissions to your own AWS account, you can grant permissions to other AWS accounts or predefined groups. The user or group that you grant permissions to is called the grantee. By default, the owner, which is the AWS account that created the bucket, has full permissions.

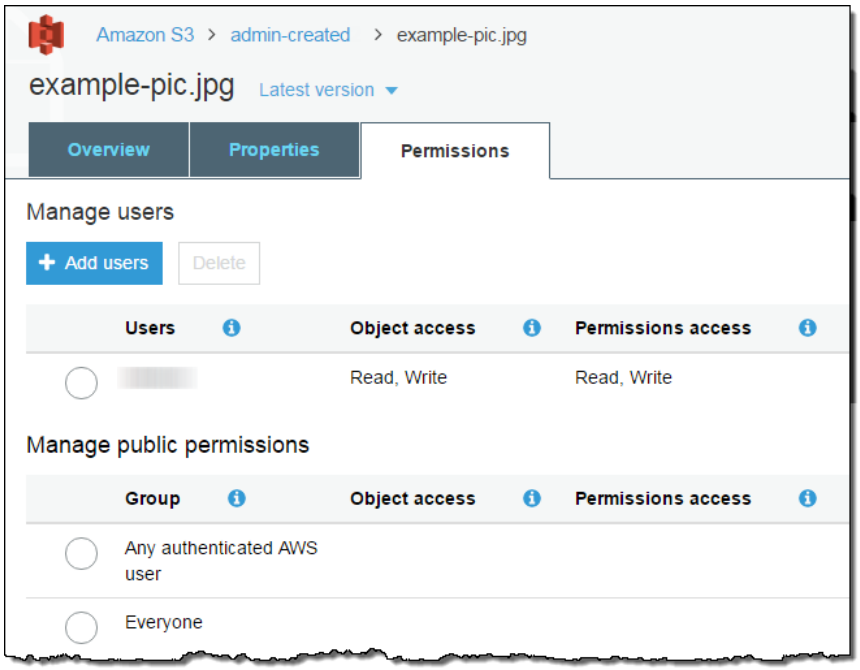
Each permission you grant for a user or a group adds an entry in the ACL associated with the object. The ACL lists grants, which identify the grantee and the permission granted. For more information about ACLs, see Managing Access with ACLs in the *Amazon Simple Storage Service Developer Guide*.

To set permissions for an object

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that contains the object.
3. In the **Name** list, choose the name of the object for which you want to set permissions.

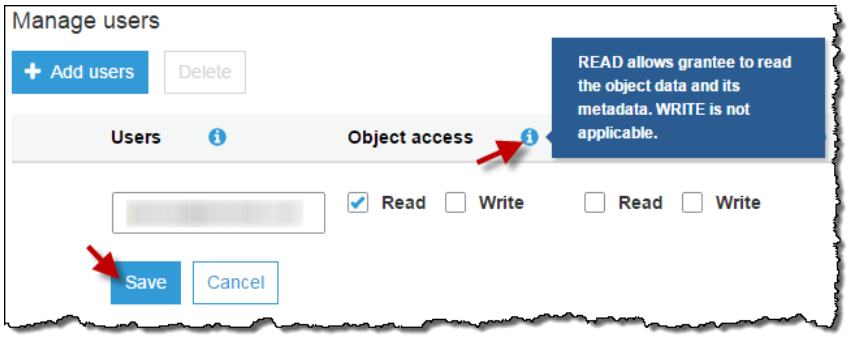


4. Choose **Permissions**.



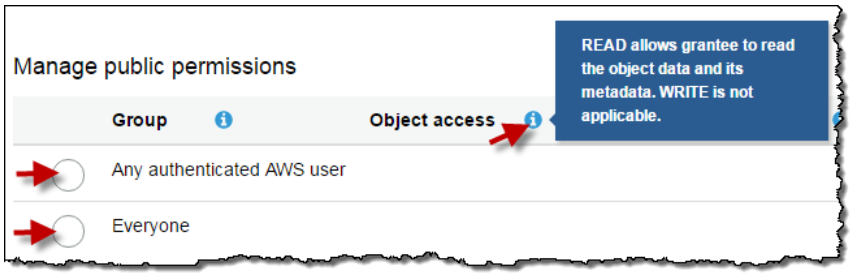
5. You can **Manage Users** or **Manage Public Permissions**.
   - To grant permissions to an AWS user from a different AWS account, under **Manage users**, choose**Add users**. In the **Enter an ID or email** field, type an email address or the canonical ID of the AWS user that you want to grant object permissions to. The email address must be the same one that the user gave when signing up for an AWS account. For information on finding a canonical ID, see AWS Account Identifiers in the *Amazon Web Services General Reference*. You can add as many as 99 users.

Select the check boxes for the permissions that you want to grant to the user, and then choose **Save**. To display information about the permissions, choose the help icons.

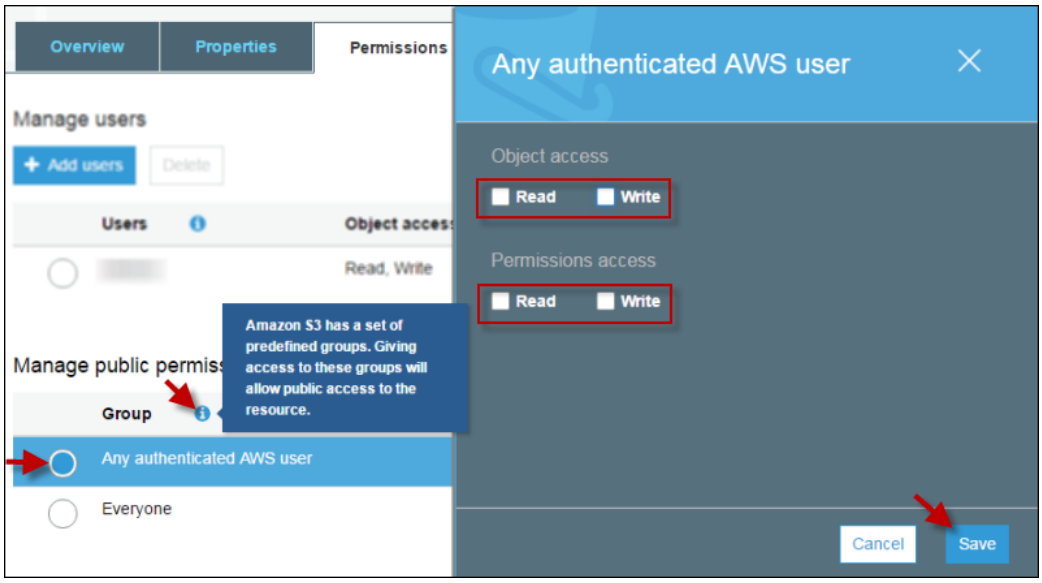


- To give public access to your object, under **Manage public permissions** choose one of the following predefined groups:
  - **Any authenticated AWS user**–This group represents all AWS accounts worldwide. Access permission to this group allows any authenticated AWS account user to access the object.
  - **Everyone**–Access permission to this group allows anonymous access, which means that anyone in the world can access the object.

  Choose the help icons to display information about the permissions.



  Select the check boxes for the permissions that you want to grant to the user, and then choose **Save**.



You can also set object permissions when you upload objects. For more information on setting permissions when uploading objects, see How Do I Upload an Object to an S3 Bucket? (p. 32).

More Info

- Setting Bucket and Object Access Permissions (p. 84)
- How Do I Set ACL Bucket Permissions? (p. 88)

How Do I Set ACL Bucket Permissions?

*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

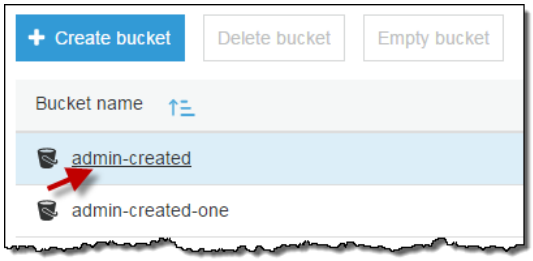
This section explains how to use the Amazon Simple Storage Service (Amazon S3) console to manage access permissions for S3 buckets by using access control lists (ACLs). ACLs are resource-based access policies that grant access permissions to buckets and objects. For more information about managing access permissions with resource-based policies, see Overview of Managing Access in the *Amazon Simple Storage Service Developer Guide*.

In addition to granting permissions to your own AWS account, you can grant permissions to other AWS account users or to predefined groups. The user or group that you are granting permissions to is called the grantee. By default, the owner, which is the AWS account that created the bucket, has full permissions.

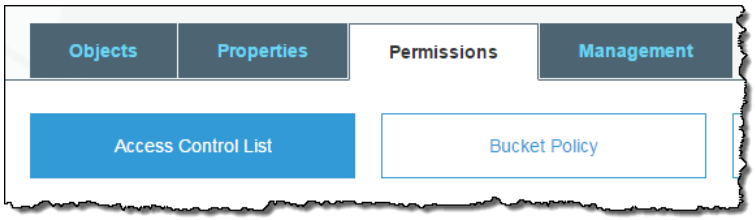
Each permission you grant for a user or group adds an entry in the ACL associated with the bucket. The ACL lists grants, which identify the grantee and the permission granted. For more information about ACLs, see Managing Access with ACLs in the *Amazon Simple Storage Service Developer Guide*.

To set ACL access permissions for an S3 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 **Bucket name** list, choose the name of the bucket that you want to set permissions for.

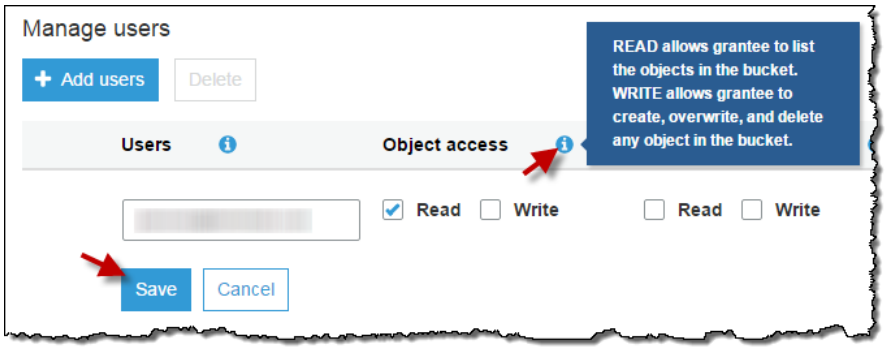


3. Choose **Permissions**.



4. You can **Manage Users** or **Manage Public Permissions**.
   - To grant permissions to an AWS user from a different AWS account, under **Manage users** choose **Add users**. In the **Enter an ID or email** field, type an email address or the canonical ID of the AWS user that you want to grant bucket permissions to. The email address must be the same one that the user gave when signing up for an AWS account. For information on finding a canonical ID, see AWS Account Identifiers in the *Amazon Web Services General Reference*. You can add as many as 99 users.

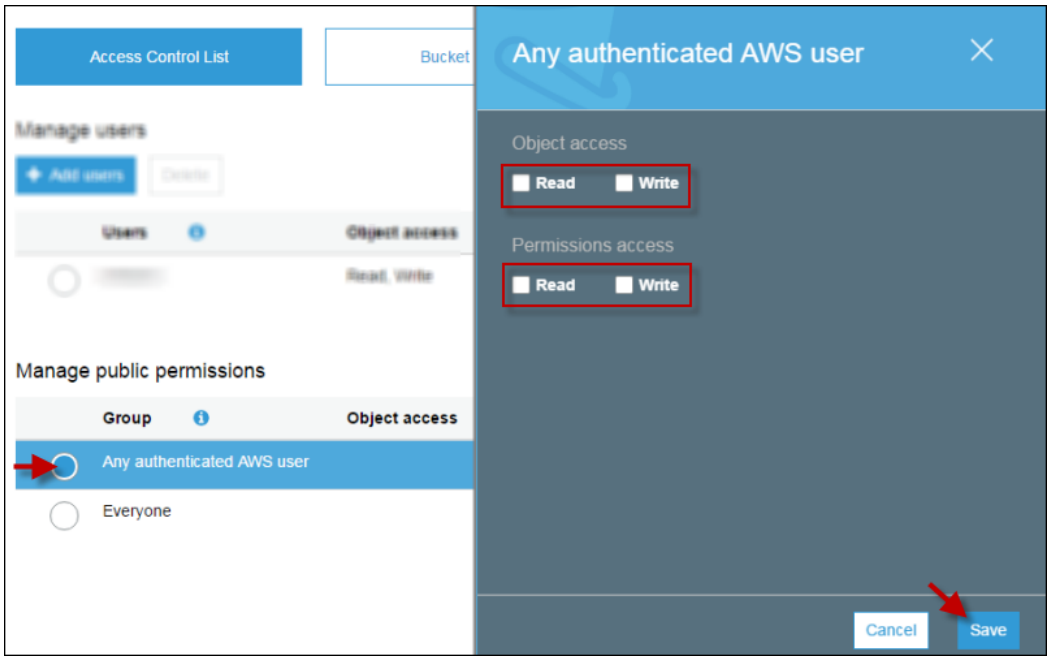
   Select the check boxes next to the permissions that you want to grant to the user, and then choose **Save**. To display information about the permissions, choose the help icons.



- To give public access to your bucket, under **Manage public permissions**, choose one of the following predefined groups:
  - **Any authenticated AWS user**–This group represents all AWS accounts worldwide. Access permission to this group allows any authenticated AWS account user to access the objects in the bucket.
  - **Everyone**–Access permission to this group allows anonymous access, which means that anyone in the world can access the bucket.

  To display information about the permissions, choose the help icons.

  Select the check boxes for the permissions that you want to grant to the user, and then choose **Save**.



Caution

We highly recommend that you *do not* grant the Everyone group object write permissions. 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 might want to keep.

More Info

- Setting Bucket and Object Access Permissions (p. 84)
- How Do I Set Permissions on an Object? (p. 85)
- How Do I Add an S3 Bucket Policy? (p. 91)

How Do I Add an S3 Bucket Policy?

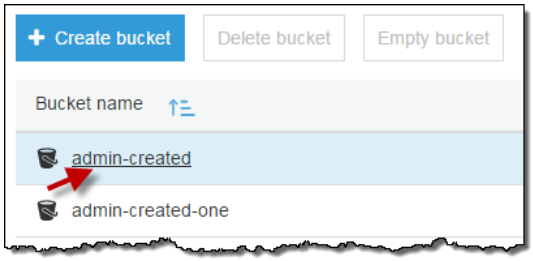
*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

This section explains how to use the Amazon Simple Storage Service (Amazon S3) console to add a new bucket policy or edit an existing bucket policy. A bucket policy is a resource-based AWS Identity and Access Management (IAM) policy. You add a bucket policy to a bucket to grant other AWS accounts or IAM users access permissions for the bucket and the objects in it. Object permissions apply only to the objects that the bucket owner creates. For more information about bucket policies, see Overview of Managing Access in the *Amazon Simple Storage Service Developer Guide*.

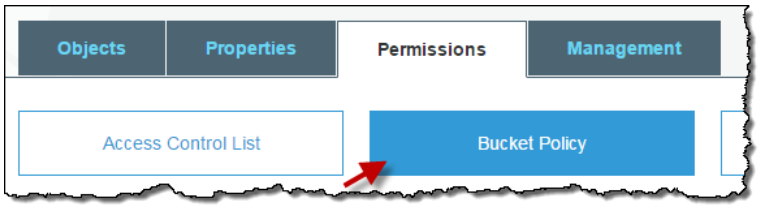
For examples of Amazon S3 bucket policies, see Bucket Policy Examples in the *Amazon Simple Storage Service Developer Guide*.

To create or edit a bucket policy

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that you want to create a bucket policy for or whose bucket policy you want to edit.



3. Choose **Permissions**, and then choose **Bucket Policy**.



4. In the **Bucket policy editor** text box, type or copy and paste a new bucket policy, or edit an existing policy. The bucket policy is a JSON file. The text you type in the editor must be valid JSON.

5. Choose **Save**.

> **Note**
> Amazon S3 displays the Amazon Resource Name (ARN) for the bucket next to the **Bucket policy editor** title. For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *Amazon Web Services General Reference*.

Directly below the bucket policy editor text box is a link to the **Policy Generator**, which you can use to create a bucket policy.

More Info

- Setting Bucket and Object Access Permissions (p. 84)
- How Do I Set ACL Bucket Permissions? (p. 88)

How Do I Allow Cross-Domain Resource Sharing with CORS?

*If you are in the old Amazon S3 console, to use the new console, choose **Opt In** in the following box, which appears on the old Amazon S3 console home page. Note that **Opt In** is not available in all Regions.*

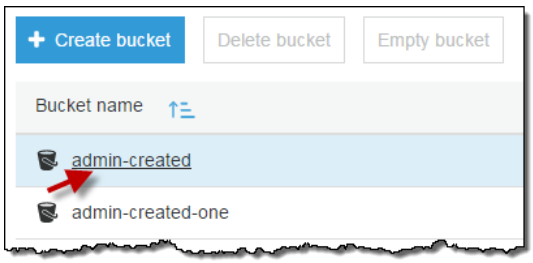
This section explains how to use the Amazon S3 console to add a cross-origin resource sharing (CORS) configuration to an S3 bucket. CORS allows client web applications that are loaded in one domain to interact with resources in another domain.

To configure your bucket to allow cross-origin requests, you add CORS configuration to the bucket. A CORS configuration is an XML document that defines rules that identify the origins that you will allow to access your bucket, the operations (HTTP methods) supported for each origin, and other operation-specific information. For more information about CORS, see Cross-Origin Resource Sharing (CORS) in the *Amazon Simple Storage Service Developer Guide*.

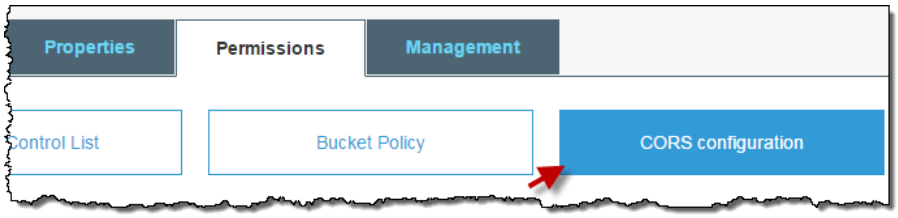
When you enable CORS on the bucket, the access control lists (ACLs) and other access permission policies continue to apply.

To add a CORS configuration to an S3 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 **Bucket name** list, choose the name of the bucket that you want to create a bucket policy for.



3. Choose **Permissions**, and then choose **CORS configuration**.



4. In the **CORS configuration editor** text box, type or copy and paste a new CORS configuration, or edit an existing configuration. The CORS configuration is a XML file. The text that you type in the editor must be valid XML.

5. Choose **Save**.

   Note
   Amazon S3 displays the Amazon Resource Name (ARN) for the bucket next to the **CORS configuration editor** title. For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *Amazon Web Services General Reference*.

More Info

- Setting Bucket and Object Access Permissions (p. 84)
- How Do I Set ACL Bucket Permissions? (p. 88)
- How Do I Add an S3 Bucket Policy? (p. 91)

AWS Glossary

For the latest AWS terminology, see the AWS Glossary in the *AWS General Reference*.