Configuring a Bucket ACL

Service Status

The Object Storage Unit (OSU) service is now END OF SALE. For more information, see End-of-Life Policy.

- EN
- FR

You can use an Access Control List (ACL) to set permissions for other users to access and manage your bucket. For more information, see Access Control List (ACL) Reference.

This feature is not available from Cockpit. This documentation only describes the procedure using AWS CLI.

Related Pages

- Getting Information About a Bucket ACL
- Configuring an Object ACL
- Listing Your Buckets

Tutorial: Setting Up a Bucket with Objects

Previous Step:

(optional) Enabling or Disabling Bucket Versioning

Next Step:

- Objects between 1 byte and 5 GiB: Uploading an Object to a Bucket
- Objects of 100 MiB or more: Creating a Multipart Upload

- To configure the ACL of a bucket, use the **put-bucket-acl** command following this syntax:

Request Sample

```
$ aws s3api put-bucket-acl \
    --profile YOUR_PROFILE \
    --bucket BUCKET \
    --acl private \
    --grant-full-control "id=USER_ID, id=USER_ID" \
    --grant-read "id=USER_ID, id=USER_ID" \
    --grant-read-acp "id=USER_ID, id=USER_ID" \
    --grant-write "id=USER_ID, id=USER_ID" \
    --grant-write-acp "id=USER_ID, id=USER_ID" \
    --endpoint ENDPOINT
```

This command contains the following attributes that you need to specify:

- (optional) `profile`: The named profile you want to use, created when configuring AWS CLI. For more information, see Installing and Configuring AWS CLI.
- `bucket`: The name of the bucket for which you want to set the ACL.

  - When specifying new permissions, all the previous permissions are replaced. Therefore, you need to specify both the existing permissions that you want to keep (including for yourself) and the new permissions that you want to give in a single command.
  - If you are the owner of the bucket, you can lose your own permissions but not the ability to manage the ACL itself.

  For more information about existing permissions, see Getting Information About a Bucket ACL and Getting Information About an Object ACL.

- (optional) `acl`: The permissions you grant for your bucket (`private` | `public-read` | `public-read-write` | `authenticated-read`).
- (optional) `grant-full-control`: One or more IDs of users to whom you grant the `full-control` permission.
- (optional) `grant-read`: One or more IDs of users to whom you grant the`read` permission.
- (optional) `grant-read-acp`: One or more IDs of users to whom you grant the `read-acp` permission.
- (optional) `grant-write`: One or more IDs of users to whom you grant the `write` permission.
- (optional) `grant-write-acp`: One or more IDs of users to whom you grant the `write-acp` permission.

- When using OOS, you need to specify S3 user IDs. You can retrieve S3 user IDs via the Listing Your Buckets and Listing the Objects of a Bucket methods using the `oos` endpoint.
- When using OSU, you need to specify OUTSCALE account IDs.
- In both cases, you can also specify user email addresses using the `emailaddress=name@domain.com` format.

`endpoint`: The endpoint corresponding to the service (`oos` or `osu`) and Region you want to send the request to, in the following format: https://<SERVICE>.<REGION>.outscale.com

The ACL is configured for your bucket.