Bucket permissions

Assign access roles for users and Service IDs against buckets, by using either the UI or the CLI to create policies.

| **Access role** | **Example actions** |
| --- | --- |
| Manager | Make objects public, create, and destroy buckets and objects |
| Writer | Create and destroy buckets and objects |
| Reader | List buckets, list objects, and download objects. |
| Content Reader | List and download objects |
| Object Reader | Download objects |
| Object Writer | Upload objects |

**Granting access to a user**

If the user needs to be able to use the console, it is necessary to **also** grant them a minimum platform access role of Viewer on the instance itself in addition to the service access role (such as Reader). This allows them to view all buckets and list the objects within them. Then, select **Bucket permissions** from the left navigation menu, select the user, and select the level of access (Manager or Writer) that they require.

If the user interacts with data by using the API and doesn't require console access, *and* they are a member of your account, you can grant access to a single bucket without any access to the parent instance.

**Policy enforcement**

IAM policies are enforced hierarchically from greatest level of access to most restricted. Conflicts are resolved to the more permissive policy. For example, if a user has both the Writer and Reader service access role on a bucket, the policy granting the Reader role is ignored.

This is also applicable to service instance and bucket level policies.

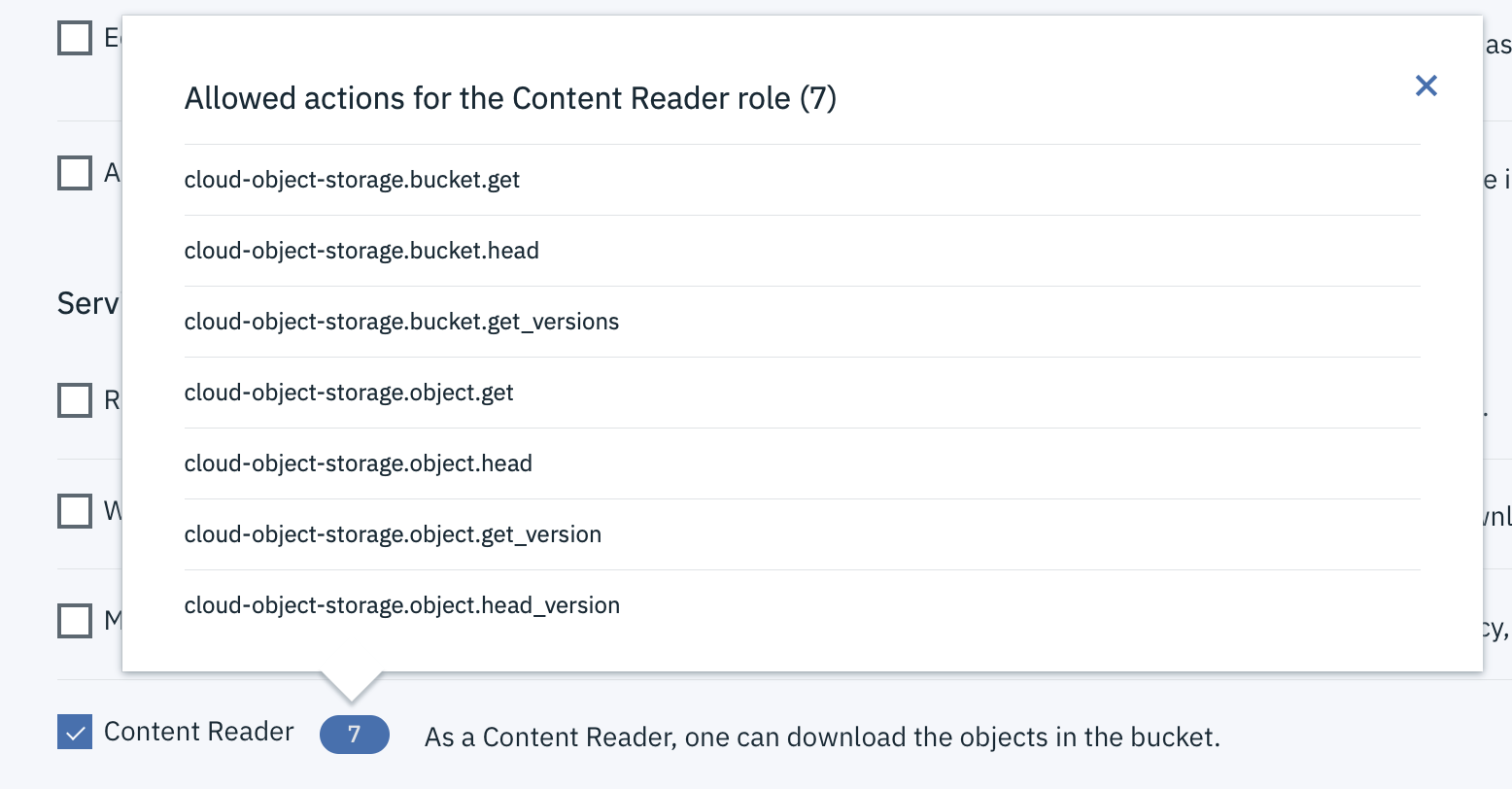
* If a user has a policy granting the Writer role on a service instance and the Reader role on a single bucket, the bucket-level policy is ignored.
* If a user has a policy granting the Reader role on a service instance and the Writer role on a single bucket, both policies are enforced and the more permissive Writer role will take precedence for the individual bucket.

If it is necessary to restrict, access to a single bucket (or set of buckets) ensure that the user or Service ID doesn't have any instance level policies by using either the console or CLI.

Using the UI

To create a new bucket-level policy:

1. Navigate to the **Access IAM** console from the **Manage** menu.
2. Select **Users** from the left navigation menu.
3. Select a user.
4. Select the **Access Policies** tab to view the user's existing policies, assign a new policy, or edit an existing policy.
5. Click **Assign access** to create a new policy.
6. Choose **Assign access to resources**.
7. First, select **Cloud Object Storage** from the services menu.
8. Then, select the appropriate service instance. Enter bucket in the **Resource type** field and the bucket name in the **Resource ID** field.
9. Select the wanted service access role. Selecting the lozenge with the number of actions show the actions available to the role, as exemplified for "Content Reader" in Figure 1.
10. Click **Assign**

Figure 1. Example actions per Content Reader role

Note that leaving the **Resource Type** or **Resource** fields blank will create an instance-level policy.

Using the CLI

From a terminal run the following command:

ibmcloud iam user-policy-create <user-name> --roles <role> --service-name cloud-object-storage --service-instance <resource-instance-id> --resource-type bucket --resource <bucket-name>

To list existing policies:

ibmcloud iam user-policies <user-name>

To edit an existing policy:

ibmcloud iam user-policy-update <user-name> <policy-id> --roles <role> --service-name cloud-object-storage --service-instance <resource-instance-id> --resource-type bucket --resource <bucket-name>

**Granting access to a service ID**

If you need to grant, access to a bucket for an application or other non-human entity, use a Service ID. The Service ID can be created specifically for this purpose, or can be an existing Service ID already in use.

Using the UI

1. Navigate to the **Access (IAM)** console from the **Manage** menu.
2. Select **Service IDs** from the left navigation menu.
3. Select a Service ID to view any existing policies, and assign a new policy or edit an existing policy.
4. Select the service instance, service ID, and desired role.
5. Enter bucket in the **Resource Type** field and the bucket name in the **Resource** field.
6. Click **Submit**

Note that leaving the **Resource Type** or **Resource** fields blank will create an instance-level policy.

Using the CLI

From a terminal run the following command:

ibmcloud iam service-policy-create <service-id-name> --roles <role> --service-name cloud-object-storage --service-instance <resource-instance-id> --resource-type bucket --resource <bucket-name>

To list existing policies:

ibmcloud iam service-policies <service-id-name>

To edit an existing policy:

ibmcloud iam service-policy-update <service-id-name> <policy-id> --roles <role> --service-name cloud-object-storage --service-instance <resource-instance-id>

--resource-type bucket --resource <bucket-name>