Using authorizations to grant access between services

Use IBM Cloud® Identity and Access Management (IAM) to create or remove an authorization that grants one service access to another service. Use authorization delegation to automatically create access policies that grant access to dependent services.

Many of the capabilities of the IAM system are focused on managing and enforcing user and application access to IBM Cloud resources. However, there might be other scenarios in which you need to provide one service with access to a user's resource in another service. This type of access is called an authorization.

In some cases, you can authorize dependent services in addition to the source service. The source service that is enabled to access the target service depends on another service. The dependent service must be assigned access to complete the workflow. Review the following example to understand how the relationship between the source, target, and dependent services works.

As an example, you might have an IBM Watson™ service that relies on an instance of IBM Cloud Object Storage to store data. When you enable an authorization between your IBM Watson service and IBM® Key Protect service, there might be a need for the Object Storage instance to access a key in the user's Key Protect instance. So, while the authorization is between your IBM Watson service and Key Protect service, the Object Storage service is also given access as a dependent service of the IBM Watson service. By selecting the option to enable authorizations for dependent services, you don't need to take any additional action because the policies are automatically created for the dependent services.

The source service's dependent services might be in the source service's account, which means that they are not visible to you in your account. However, any access policies that are created by the source service for its dependent services are always visible to you. You can tell which authorizations a user created or a source service that is created by checking the Type column for the specific authorization on the Authorizations page.

**Creating an authorization in the console**

You must have access to the target service to create an authorization between services. You can grant only the level of access that you have as a user of the target service. For example, if you have viewer access on the target service, you can assign only the viewer role for the authorization.

1. In the IBM Cloud console, click **Manage** > **Access (IAM)**, and select **Authorizations**.
2. Click **Create**.
3. Select a source service and specify whether you want the authorization to be for all instances or only a specific instance in the account or instances only in a certain resource group.
4. Select a target service and specify whether you want the authorization to be for all instances or only a specific instance in the account or instances only in a certain resource group.
5. Optional: Select **Enable authorization to be delegated** to allow the source service to delegate its access to any dependent services. This option is displayed only if the source service has dependent services. By selecting this option, policies are automatically created by the source service for the dependent services.
6. Select a role to assign access to the source service that accesses the target service.
7. Click **Authorize**.

Creating an authorization by using the CLI

To authorize a source service access a target service, run the ibmcloud iam authorization-policy-create command.

The following sample uses mock data to create a policy where a specific source service instance of IBM Cloud Object Storage is authorized to access a specific target service instance of IBM Key Protect:

ibmcloud iam authorization-policy-create cloud-object-storage kms Reader --source-service-instance-id 123123 --target-service-instance-id 456456

For more information about all of the parameters that are available for this command, see [ibmcloud iam authorization-policy-create](https://cloud.ibm.com/docs/cli?topic=cli-ibmcloud_commands_iam" \l "ibmcloud_iam_authorization_policy_create).

Creating an authorization by using the API

To authorize a source service access to a target service, use the [IAM Policy Management API](https://cloud.ibm.com/apidocs/iam-policy-management#create-a-policy). See the following API example for Create a policy method with the type=authorization specified. All of the possible attributes are listed.

The supported attributes for creating an authorization policy depend on what each service supports. For more information about the supported attributes for each service, refer to the documentation for the services that you're using.

curl --request POST \

--url https://iam.test.cloud.ibm.com/v1/policies \

--header 'Authorization: Bearer <token>' \

--header 'Content-Type: application/json' \

--data '{

"type": "authorization",

"subjects": [

{

"attributes": [

{

"name": "accountId",

"value": "<account-id>"

},

{

"name": "serviceName",

"value": "<service-name>"

},

{

"name": "serviceInstance",

"value": "<instance-id>"

}

]

}

],

"roles": [

{

"role\_id": "crn:v1:bluemix:public:iam::::serviceRole:Reader"

}

],

"resources": [

{

"attributes": [

{

"name": "accountId",

"value": "<account-id>"

},

{

"name": "serviceName",

"value": "<service-name>"

},

{

"name": "serviceInstance",

"value": "<instance-id>"

},

{

"name": "resourceType",

"value": "<resource-type>"

},

{

"name": "resource",

"value": "<id>"

}

]

}

]

}'

Not all services support policies at the resourceType and individual resource level. Examples of services that do support these attributes are IBM Cloud Object Storage and IBM Key Protect, where buckets and keys are the resource type and the ID is listed to specify the specific resource.

**Removing an authorization**

You can remove any authorization between services in the account if you are assigned the Administrator role on the target service. If you remove any access policies created by the source service for its dependent services, the source service is unable to complete the workflow or access the target service.

1. In the console, click **Manage** > **Access (IAM)**, and select **Authorizations**.
2. Identify the row for the authorization that you want to remove from the account.
3. From the **Actions**  menu, select **Remove**.
4. Select **Remove**.

If the source service is removed from the account, any policies that are created by that service for its dependent services are deleted automatically. Similarly, if the dependent service is removed from the account, any access policies that are delegated to that service are also deleted.