IAM access

All services that are organized in a resource group in your account are managed by using IBM Cloud Identity and Access Management (IAM). Account owners are automatically assigned the account administrator role. As the account administrator, you can assign and manage access for users, create resource groups, create access groups, view billing details and track usage, and create service instances. You provide access for users, service IDs, and access groups by creating policies that set a target for the subject of the policy to access and a role that defines what type of access that is allowed.

**What are IAM policies and who can assign them?**

A policy grants a subject one or multiple roles to a set of resources so that specific actions can be taken within the context of the specified target resources.

The following graphic helps to explain how the IAM policy is created. Policies are always created by specifying the subject first. The subject is a specific user, service ID, or an access group. Next, the target of the policy is selected which is what you are allowing the user to access, for example: all services in a resource group, all IAM-enabled services in the account, account management services, or a particular service instance. Finally, you complete your access policy by selecting from the available roles. These roles define exactly what actions a user can complete. More configuration options might be available, depending on the service you select.

Figure 1. How IAM access policies are created by using a subject, target, and role

You can assign and manage policies if you have the proper role. The following table shows policy management tasks and the role that is required for each.

| **Action** | **Required role** |
| --- | --- |
| Create a policy in an account for all services and instances | Account owner or administrator on all account management services and all Identity and Access enabled services |
| Create a policy on a service in an account | Account owner, administrator on all Identity and Access enabled services, or administrator on the service in the account |
| Create a policy on a service instance | Account owner, administrator on all Identity and Access enabled services, administrator on the service in the account, administrator on all services in the relevant resource group, or administrator on the service instance |
| Table 1. Users allowed to create access policies | |

**Common access policy types**

You can provide fine-grained access for users, service IDs, or access groups by assigning the following types of access policies:

* All account management services
* Specific account management service
* All resources within the account
* All resources within all services that belong to an individual resource group with the ability to manage the resource group
* All resources within a single service in a resource group with the ability to manage the resource group
* All resources within a single service across the account, regardless of the resource group they're assigned to
* Resources in an individual instance
* A single resource type within an instance, for example, a bucket in an Object Storage instance

If you want to enable a user full administrator access to complete [account management tasks](https://cloud.ibm.com/docs/account?topic=account-account-services#account-services), such as inviting and removing users, viewing billing and usage, managing service IDs, managing access groups, managing user access, and access to all account resources, you must assign a user the following access:

* A policy for all identity and access enabled services within the account with the administrator and manager roles assigned.
* A policy with the administrator role assigned on all account management services.

**IAM roles**

You can manage and define access based on specific roles for users and resources in your account.

* Platform management roles cover a range of actions, including the ability to create and delete instances, manage aliases, bindings, and credentials, and manage access. The platform roles are administrator, editor, operator, viewer. Platform management roles also apply to [account management services](https://cloud.ibm.com/docs/account?topic=account-account-services#account-management-actions-roles) that enable users to invite users, manage service IDs, access policies, catalog entries, and track billing and usage depending on their assigned role on an account management service.
* Service access roles define a user or service’s ability to perform actions on a service instance, such as accessing the console or performing API calls. The most common service access roles are manager, writer, and reader. Each service maps particular actions for working with the service to each of these roles.

You might not see all of the roles that are listed here as options when you assign policies in the UI because only the roles available for the service that you chose are displayed. For more information on what roles are enabled and what actions each access role allows for each service, see the documentation for that service.

* Custom roles for a service can be created on the IAM Roles page by the account owner or a user assigned the administrator role on the role management service.

You can review the available roles and associated actions for a particular service by going to the [Roles](https://cloud.ibm.com/iam/roles) page, and selecting the service that you want to learn more about. This is the same page where you can create a custom role in the console.

Platform management roles

With platform management roles, users can be assigned varying levels of permission for performing platform actions within the account and on a service. For example, platform management roles that are assigned for catalog resources enable users to complete actions such as creating, deleting, editing, and viewing service instances. And, the platform management roles that are assigned for account management services enable users to complete actions such as inviting and removing users, working with resource groups, and viewing billing information. For more information about the account management services, see [Assigning access to account management services](https://cloud.ibm.com/docs/account?topic=account-account-services).

Select all roles that apply when you create a policy. Each role allows separate actions to be completed and doesn't inherit the actions of the lesser roles.

The following table provides examples for some of the platform management actions that users can take within the context of catalog resources and resource groups. See the documentation for each catalog offering to understand how the roles apply to users within the context of the service that is being used.

|  | **One or all IAM-enabled services** | **Selected service in a resource group** | **Resource group access** |
| --- | --- | --- | --- |
| **Viewer role** | View instances, aliases, bindings, and credentials | View only specified instances in the resource group | View resource group |
| **Operator role** | View instances and manage aliases, bindings, and credentials | Not applicable | Not applicable |
| **Editor role** | Create, delete, edit, and view instances. Manage aliases, bindings, and credentials | Create, delete, edit, suspend, resume, view, and bind only specified instances in the resource group | View and edit name of resource group |
| **Administrator role** | All management actions for services | All management actions for the specified instances in the resource group | View, edit, and manage access for the resource group |
| Table 2. Example platform management roles and actions for services in an account | | | |

For information about the specific actions users can take based on their assigned role on account management services, see [Assigning access to account management services](https://cloud.ibm.com/docs/account?topic=account-account-services).

Some services might map specific actions to the platform management roles that are related to the management of the service rather than to the access of the service. As an example, see the following table that details the Kubernetes Service service actions that are mapped to these roles.

| **Platform management role** | **Actions** | **Example actions for Kubernetes Service** |
| --- | --- | --- |
| Viewer | Can view service instances, but can't modify them | * List clusters * View details for a cluster |
| Editor | Perform all platform actions except for managing the account and assigning access policies | * Bind a service to a cluster * Create a webhook |
| Operator | Perform platform actions required to configure and operate service instances, such as viewing a service's dashboard | * Add or remove worker nodes * Restart or reload worker nodes * Bind a service to a cluster |
| Administrator | Perform all platform actions based on the resource this role is being assigned, including assigning access policies to other users | * Remove a cluster * Create a cluster * Update user access policies * All actions a viewer, editor, and operator can perform |
| Table 3. Example platform management roles and actions for Kubernetes Service service | | |

Service access roles

Service access roles enable users to be assigned different levels of permission for calling the service's API and accessing the UI for the service. The following table provides example actions that can be taken depending on the assigned roles based on using the Object Storage service.

The actions that can be taken based on each assigned role vary based on the service that you selected for the policy. Not all services use these types of roles. See the documentation for the service for more details.

| **Service access role** | **Actions** | **Example actions for Object Storage service** |
| --- | --- | --- |
| Reader | Perform read-only actions within a service, such as viewing service-specific resources | List and download objects |
| Writer | Permissions beyond the reader role, including creating and editing service-specific resources | Create and destroy buckets and objects |
| Manager | Permissions beyond the writer role to complete privileged actions as defined by the service, plus create and edit service-specific resources | Manage all aspects of data storage, create, and destroy buckets and objects |
| Table 4. Example service access user roles and actions | | |

Custom access roles

An account owner or a user assigned the Administrator role on the Role management service can create custom roles for a service on the IAM Roles page. Any number of actions that are available for a service for any platform or service role can be combined and added to a custom named role.

After the role is created, any user who can assign access for that service sees the new custom role as an option. For more information, see [Creating custom roles](https://cloud.ibm.com/docs/account?topic=account-custom-roles).