Giving access to resources in resource groups

With IBM Cloud IAM, you have the flexibility to provide fine-grained user access to the resources and resource groups in your account.

You can assign the following types of access policies for users to work with resources in resource groups:

* Access to resources within a resource group. You can grant access to all resources in a group, or only selected services within a group.
* Access to a resource group itself, which enables users to view and edit the resource group, assign access for others to manage the resource group, and most importantly create and add new service instances to a resource group.

Assigning a user access to manage a resource group, meaning a role on the resource group itself, then that user can view billing and usage information for resources that are contained in that resource group.

Review the following table for more information what each assigned platform IAM role provides a user the ability to do:

|  | **Actions for Access to Manage Resource Groups** | **Actions on Resources in Resource Groups** |
| --- | --- | --- |
| **Viewer role** | View the group and its characteristics, but can't view resources in the group without a policy on the resource itself | View resources in the group if a viewer role or higher is assigned on the resource group itself |
| **Operator role** | Not applicable | Not applicable |
| **Editor role** | View or edit the name or other characteristics of the group, but not the resources in the group | Create, delete, edit, suspend, resume, view, bind, and manage access of resources in the resource group |
| **Administrator role** | View, edit, or manage access for the group, but not the resources in the group | Create, delete, edit, suspend, resume, view, bind, and manage access of resources in the resource group |
| Table 1. Access for resource groups | | |

If you want a user to create a new service instance and add it to a resource group, you must assign a viewer role or higher on the resource group and an editor role or higher on the service.