

[New Staging Africa](#)[Journeys ▾](#)[Courses ▾](#)[Job Advisor](#)[Badges](#)[About ▾](#)[Help](#)[My Dashboard](#)[English ▾](#)

## Cloud Computing V2

# Managing your IBM Cloud users and resources

## IBM Cloud: Identity and Access Management

IBM Cloud uses Identity and Access Management (Cloud IAM) to manage user identity. Some of the key IBM Cloud Identity and Access Management (Cloud IAM) features are:

- Unified user management across IBM Cloud PaaS and IaaS

A unified user management console is used to manage your users across the IBM Cloud platform and infrastructure services.

- Enterprise federation

A federated ID can be used to sign up for IBM Cloud only if your company worked with IBM to register. Registering a company's domain with IBM enables users to log in to IBM products and services by using their company user credentials. Authentication is then handled by your company's identity provider. When you log in to IBM Cloud with a

federated ID, you are prompted to log in through your company's login page.

New Staging Africa

Journeys ▾

Courses ▾

Job Advisor

Badges

About ▾

Help

My Dashboard

with fine-grained access control, users can be assigned access to only the resources that they need.

**Reference:**

English ▾

<https://cloud.ibm.com/docs/iam?topic=iam-userroles>

## IBM Cloud: Resources, users, and access control

- A *resource* is an entity in your account that you create from the IBM Cloud catalog, such as a provisioned instance of an IBM Cloud service. For example, Cloudant, a Cloud Foundry application, a VM, or a container are resources. Each account can have multiple resources.
- You can invite multiple users to an account and grant them access to resources.
- Users can be granted access to resources in an account in the following ways:
- Organize resources that are enabled to use Cloud IAM into resource groups that you define in your account and assign users access to the resource groups.
- Rely on a user's role in a Cloud Foundry region, organization, and space to determine whether a user has permission to access the Cloud Foundry apps and services that have not yet enabled the use of Cloud IAM. These resources cannot be added to a resource group

## IBM Cloud: Resource groups

A resource group is a way for you to organize your account resources into customizable groups so that you can quickly

assign users access to more than one resource concurrently.

**New Staging Africa**

Journeys ▾

Courses ▾

Job Advisor

Badges

About ▾

Help

| My Dashboard

- Users are granted access to resources in a resource group .
- Any account resource that is managed by using Cloud IAM access control belongs to a resource group within your account.
- Access to resources is not restricted to Cloud Foundry regions, organizations, and spaces.

Complete the following steps to create a resource group:

1. Select Manage > Account from the top navigation bar.
2. Click Resource Groups.
3. Click Create.
4. Specify the name of the resource group.
5. Click Add.

By default, there is a default resource group that is available, so by default any new resource is added to this group unless the user select a different one.

Resource groups and IBM Cloud accounts:

- If you have a Pay-As-You-Go or Subscription account, you can create multiple resource groups to make managing quotas and viewing billing usage for a set of resources easier. You can also group resources to make it easier for you to assign users access to more than one instance concurrently.
- If you have a Lite account, you cannot create multiple resource groups , but you can rename your default resource group.

New Staging Africa   Journeys ▾   Courses ▾   Job Advisor   Badges   About ▾   Help   |   My Dashboard

Account resources ▾  
Best practices  
Resource groups  
Cloud Foundry orgs  
Tags  
Audit log  
Account settings  
Notifications  
Company contacts  
Company profile

Group resources to organize and assign access to the group. Available for all resources managed by IBM Cloud Identity and Access Management. [Learn more about resource groups.](#)

English ▾  
Filter  Create +

Name	Date Created	Actions
Default	12/6/2018, 5:47:29 PM	...

## IBM Cloud: Resource controller

The *resource controller* is the next-generation provisioning layer that manages the lifecycle of cloud resources. Previously, all services that were integrated into IBM Cloud used Cloud Foundry and an IBM Cloud version of the Cloud Foundry service broker. Although many similarities to the Cloud Foundry model still exist, the resource controller introduces several new concepts and changes to the Cloud Foundry model.

In general, resources that are tracked by the resource controller are intended to have associated usage metrics and billing, but that is not always the case. In some instances, the resource might be associated with the resource controller to ensure that the resource lifecycle can be managed along with the account lifecycle.

The resource controller is responsible for managing the lifecycle of resources in an account. It offers fine-grained access control to resources through IAM. Consider the following points:

- Resources are organized by using RGs.
- Users are granted access to resources in a resource group.

- Access to resources is not restricted to Cloud Foundry regions, organizations, and spaces.

**New Staging Africa**

Journeys ▾

Courses ▾

Job Advisor

Badges

About ▾

Help

| My Dashboard

limiting. For example, the Cloud Foundry service broker specification is a powerful concept that provides an extensible model for service providers to plug their services into the IBM Cloud platform.

However, coarse-grained access control and space-scoped service instances that are tied to a Cloud Foundry region are some of the inherited limitations. As IBM Cloud moves forward into the next generation of cloud, it will retain the service broker extensibility model while breaking away from Cloud Foundry organizations and space constructs.

## IBM Cloud: Access group

Below is an example of the steps by which you can create access group and set up your group's users and service IDs.

You can create an access group by following the steps below:

1. From the menu bar, click **Manage > Access (IAM)**, and select **Access Groups**.
2. Click **Create**.
3. Enter a name and optional description for your group, and click **Create**.

Next, you can set up your group by adding users or service IDs:

1. Select the name of the group to which you want to add.
2. Click **Add** users on the **Users** tab.
3. Select the users that you want to add from the list, and click **Add to group**.
4. To add service IDs to the group, click the **Service IDs** tab, and click **Add service ID**.
5. Select the IDs that you want to add from the list and click **Add to group**.

3. Select the IDs that you want to add from the list, and click **Add to group**.

New Staging Africa

Journeys ▾

Courses ▾

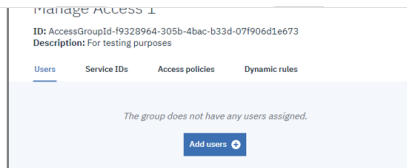
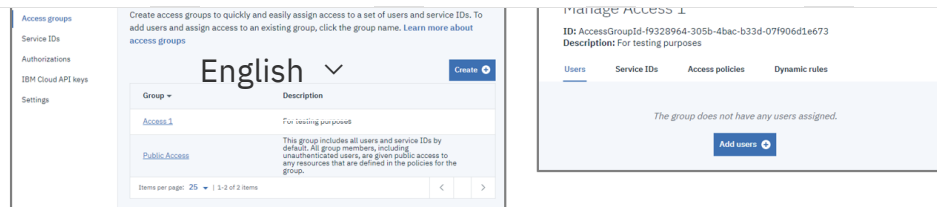
Job Advisor

Badges

About ▾

Help

My Dashboard



## IBM Cloud: IAM policies

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

The figure below explains 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.

I want to give	Subject	access to	Target	with specific permissions	Platform roles	Service roles
	<div>Access Group</div> <div>User</div> <div>Service ID</div>		<div>Account Management Service</div> <div>Resource Group</div> <div>Service</div> <div>Service Instance</div> <div>Service Resource Type</div>		<input checked="" type="checkbox"/> Administrator <input checked="" type="checkbox"/> Editor <input checked="" type="checkbox"/> Operator <input checked="" type="checkbox"/> Viewer	<input checked="" type="checkbox"/> Manager <input checked="" type="checkbox"/> Reader <input checked="" type="checkbox"/> Writer

You can set up your group with users and service IDs, you can assign a common access policy to the group. Remember, any policy that you set for the group applies to all entities within the group.

1. From the menu bar, click Manage > Access (IAM), and select Access Groups.
2. Select the name of the group to which you want to assign access.
3. Click Access policies.
4. Click Assign access.
5. Choose to assign access by resources within a resource group, individual resources available within the account, or account management services.

Groups / Manage Group / Choose Access Type /

Account: ⓘ bmx's Account

### Assign resource group and resource access to Access 1 ⓘ

When you assign a group access to a resource within a resource group, you can also assign access for viewing, editing, or managing access to the group. Select a role for the Assign access to a resource group option to provide access to the group. Select "No access" if you want to only provide access to the specified resource.

**Resource group**

All resource groups + ▾

**Assign access to a resource group ⓘ**

Viewer ▾

As a viewer, you can view service instances, but you can't modify them.

**Services**

No access + ▾

Cancel Assign

## IBM Cloud: Cloud IAM roles

## Platform management roles

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 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

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 service access roles are manager, writer, and reader.



New Staging Africa

Journeys ▾

Courses ▾

Job Advisor

Badges

About ▾

Help

My Dashboard

separate actions to be completed and doesn't inherit the actions of the lesser roles. These roles enable actions to be performed on platform resources, such as creating instance, connecting instance to apps, and assigning user access.

☐ **Administrator**

As an administrator, you can perform all platform actions based on the resource this role is being assigned, including assigning access policies to other users.

☐ **Editor**

As an editor, you can perform all platform actions except for managing the account and assigning access policies.

☐ **Operator**

As an operator, you can perform platform actions required to configure and operate service instances, such as viewing a service's dashboard.

☐ **Viewer**

As a viewer, you can view service instances, but you can't modify them.

performing service API calls. Each role is customized by the selected service. Refer to the service's documentation for more details.

☐ **Manager**

As a manager, you have permissions beyond the writer role to complete privileged actions as defined by the service. In addition, you can create and edit service-specific resources.

☐ **Writer**

As a writer, you have permissions beyond the reader role, including creating and editing service-specific resources.

☐ **Reader**


As a reader, you can perform read-only actions within a service such as viewing service-specific resources.

FEEDBACK

## IBM Cloud: Organizing resources

When creating a resource, you select the resource group, as shown in the figure to organize your resources within groups. Most of the services in the IBM Cloud catalog use Cloud IAM for access control.

← View all

 **Cloudant**  
Lite • IBM

IBM Cloudant is a fully managed JSON document database that offers independent serverless scaling of provisioned throughput capacity and storage. Cloudant is compatible with Apache CouchDB and accessible through a simple to use HTTPS API for web, mobile, serverless, and IoT applications. Cloudant is SOC2 and ISO 27001 compliant with HIPAA

Service name:

Choose a region/location to deploy in:

Select a resource group: ⓘ

# Cloud Foundry: Organizing resources

**New Staging Africa**

Journeys ▾

Courses ▾

Job Advisor

Badges

About ▾

Help

My Dashboard

When you create a Cloud Foundry resource (application or service), you must specify the region, organization, and space to which the resource is assigned, as shown in the figure below.

You can create a resource only in a space for which you have *developer access*.

← View all

**Create a Cloud Foundry App**

Liberty for Java™

Develop, deploy, and scale Java web apps with ease. IBM WebSphere Liberty Profile is a highly composable, ultra-fast, ultra-light profile of IBM WebSphere Application Server designed for the cloud.

[View Docs](#) [Terms](#)

VERSION: 3.x  
TYPE: Application  
LOCATION: Sydney, Frankfurt, London, Washington DC, Dallas

App name: test-java-app

Host name: test-java-app

Domain: eu-gb.cf.appdomain.cloud

Choose a region/location to deploy in: London

Choose an organization: bmx\_student\_bmx66@y...

Choose a space: dev

Tags: 1

Examples: env:dev, version:1

[Need Help?](#)  
[Contact IBM Cloud Support](#)

[Add to estimate](#) [Create](#)

Free

Services that use Cloud IAM have the following advantages over services that are based on Cloud Foundry:

- They can connect to apps and services in any Cloud Foundry space, which allows you to connect apps and services from different regions.
- Each resource that is managed by Cloud IAM belongs to a resource group, and resource groups are not scoped by region. Therefore, you can provision apps and services from different regions into the same resource group.
- You can use fine-grained access control down to an individual resource.

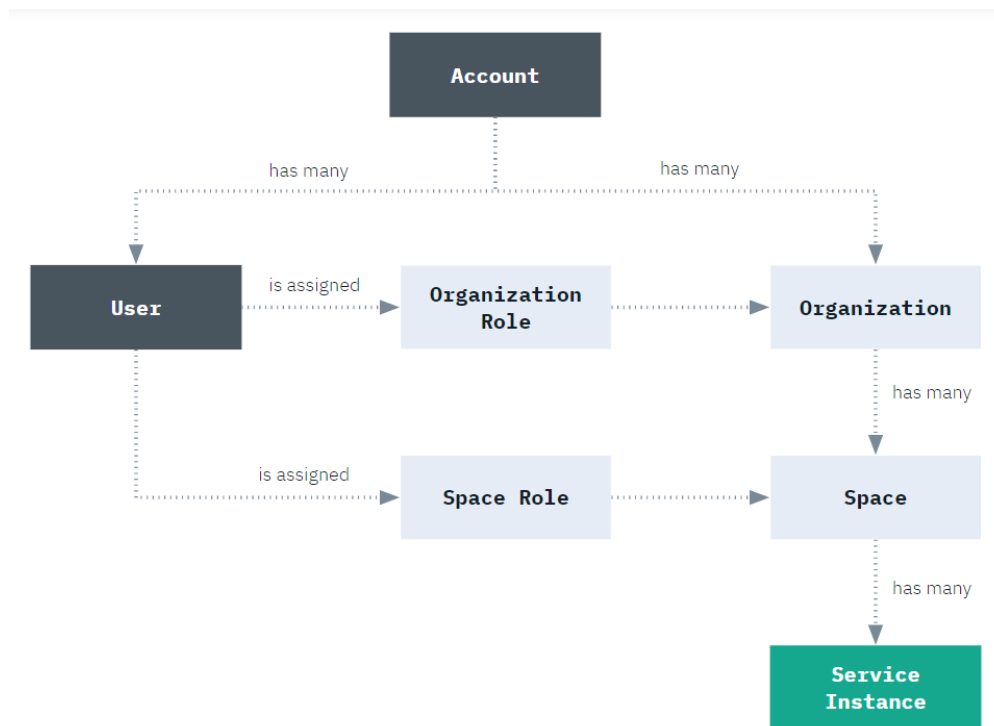
# Cloud Foundry: Access

[New Staging Africa](#)[Journeys ▾](#)[Courses ▾](#)[Job Advisor](#)[Badges](#)[About ▾](#)[Help](#)[My Dashboard](#)

which the instance belongs with a Cloud Foundry role assigned.

[English ▾](#)

The figure below outlines how Cloud Foundry orgs, spaces, and roles relate within an account. An account can have many users, orgs, and spaces. Each user can be assigned to as many orgs and spaces as necessary, and when they are assigned to an org and space, you can set the level of access to work within each by assigning a Cloud Foundry role.



## Cloud Foundry: Organizations

- Organizations are defined by:

- Users (team members)

New Staging Africa

Journeys ▾

Courses ▾

Job Advisor

Badges

About ▾

Help

| My Dashboard

- Quota

English ▾

- A user (team member) has a role with basic permissions in organizations and spaces:
- Users must be assigned to an organization before they can be granted permissions to the spaces within an organization.
- Users can belong to more than one organization (which is how you share access to control and monitor your applications and services).

## Cloud Foundry: Domains and quota

Domains provide the route on the internet that is allocated to the organization. Consider the following points:

- A route has a subdomain and a domain.
- A subdomain is the host name, which is typically the application name.
- A domain might be a system domain, or a custom domain that you registered for your application.
- The domain and the route determine how users interact with your IBM Cloud applications over the network.

Quota represents the resource limits for the organization, including the number of services and the amount of memory that can be allocated for use by the organization. Consider the following points:

- Quotas are assigned when organizations are created.
- Any application or service in a space of the organization contributes to the usage of the quota.
- With the subscription plans, you can adjust your quota for Cloud Foundry applications and containers as the needs of your organization change.

your organization change.

**New Staging Africa**

Journeys ▾

Courses ▾

Job Advisor

Badges

About ▾

Help

| My Dashboard

- A space is a mechanism to group a set of applications, services, and team members within an organization:
- An organization can contain multiple spaces.
- Two organizations cannot share a space.
- Spaces can have the same name in different organizations.
- All applications and services are associated with a space.
- Users must be a member of an organization to have access to a space within that organization.
- A member of a space can view the applications within the space.
- Only users in the developer role can create applications and services in the space.
- You can use spaces to represent different types of deployment environments, for example, a development, testing, staging, or production environment.

## Cloud Foundry: User roles

The figure below defines the Users' roles in both spaces and organizations:

New Staging Africa

Journeys ▾

Courses ▾

Job Advisor

Badges

About ▾

Help

My Dashboard

managers	<ul style="list-style-type: none"> <li>• Invite users to the organization and manage users.</li> <li>• Manage domains of the organization.</li> </ul>
Billing managers	English ▾ View (read-only) runtime and service usage information for the organization.
Organization auditors	View application and service content in the organization.
Space managers	<ul style="list-style-type: none"> <li>• Add users to the space and manage users.</li> <li>• Enable features for the space.</li> </ul>
Space developers	<ul style="list-style-type: none"> <li>• Create, delete, and manage applications and services within the space.</li> <li>• Have access to logs within the space.</li> </ul>
Space auditors	Have read-only access to settings, logs, applications, and services.

## Managing Cloud Foundry organizations

Organization managers control who has which type of access to the organization (Manager, Billing Manager, or Auditor).

The organization's managers can invite users to the organization and assign them the various roles.

## Inviting users to IBM Cloud

You can invite users, cancel invitations, and resend a pending invitation to an invited user. In addition, you can invite a single user or multiple users at once.

[New Staging Africa](#)[Journeys](#) ▾[Courses](#) ▾[Job Advisor](#)[Badges](#)[About](#) ▾[Help](#)[My Dashboard](#)[English](#) ▾[Contact](#)[Privacy](#)[Terms of use](#)[Accessibility](#)[Report Abuse](#)[Feedback](#)[Cookie preferences](#)