What is IBM Cloud Identity and Access Management?

Last updated: 2020-09-23

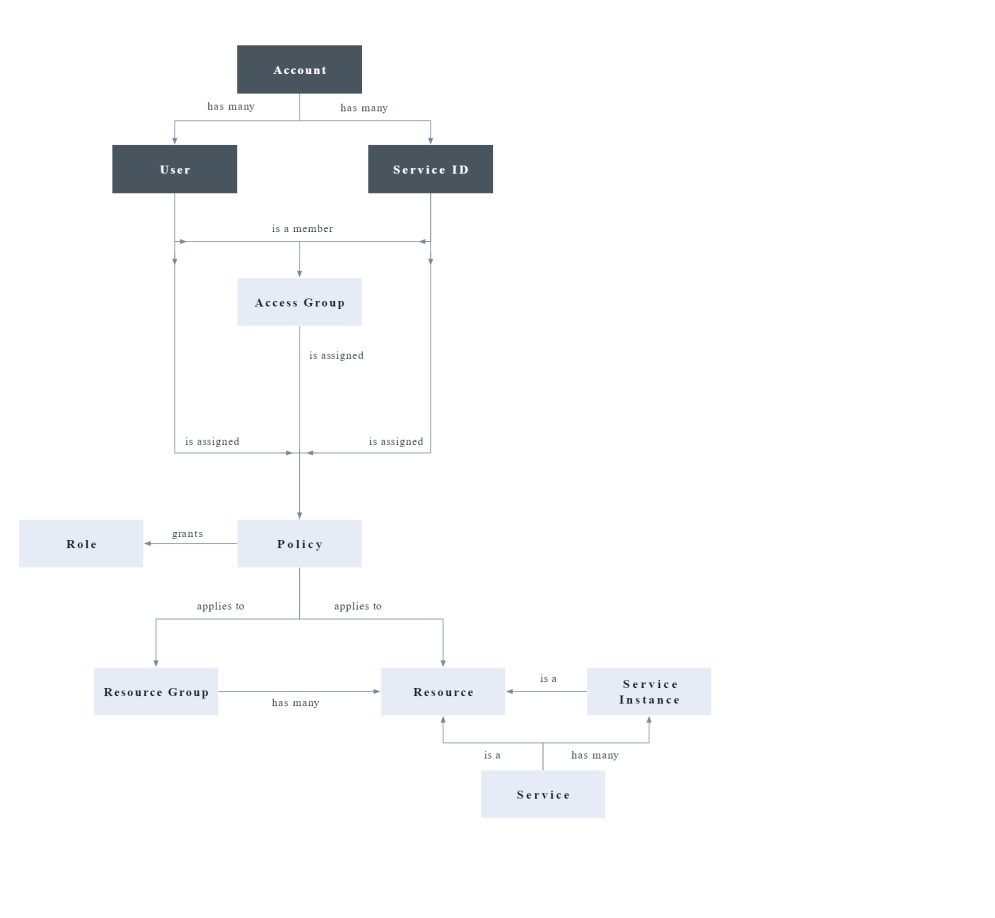
Contribute in GitHub:

[Open doc issue](https://github.com/ibm-cloud-docs/account/issues/new)|[Edit topic](https://github.com/ibm-cloud-docs/account/blob/master/iam-whatis.md)

Learn about what IBM Cloud® Identity and Access Management (IAM) is, how it IAM works, what features are available, and how to access the console, CLI, and APIs to work with IAM in your account.

IAM enables you to securely authenticate users for platform services and control access to resources consistently across IBM Cloud. A set of IBM Cloud services is enabled to use IBM Cloud IAM for access control, and are organized into [resource groups](https://cloud.ibm.com/docs/account?topic=account-rgs) within your account so you can give users access quickly to more than one resource at a time. Each of these services is labeled as "IAM-enabled" in the catalog. You can use IAM access policies to assign users and service IDs access to resources within your account. And, you can group users and service IDs into an [access group](https://cloud.ibm.com/docs/account?topic=account-groups) to easily give all members of the group the same level of access.

Figure 1. How access management works in an account by using IAM



For services that don't support the use of IBM Cloud IAM policies for managing access, you can use [Cloud Foundry access](https://cloud.ibm.com/docs/account?topic=account-cfaccess) or [classic infrastructure permissions](https://cloud.ibm.com/docs/account?topic=account-infrapermission).

The two major concepts of IBM Cloud IAM are identity and access management. For more information, review the following sections.

**Identity**

The identity concept consists of user identities, service and app identities, API keys, and resources. Users are identified by their IBMid, SoftLayer, or AppID user ID. Service IDs are a second type of identity that is used in an account. Service IDs are used to provide a separate identity for services and applications. You can create a service ID to be used by an application that needs access to your IBM Cloud services so that individual user credentials don't need to be used.

IBM Cloud API keys are used to authenticate with an API or CLI as a user or service ID. These API keys are provided through IBM Cloud IAM and can't be used generally to authenticate with IBMid outside of IBM Cloud. You can also use a single classic infrastructure API key to access classic infrastructure APIs; however, this is not required as you can use IBM Cloud API keys to access the same APIs.

The final piece of the identity concept in IAM is IBM Cloud resources, which are identified by their cloud resource names (CRN). For more information, see [Cloud Resource Names](https://cloud.ibm.com/docs/account?topic=account-crn).

**Access management**

The concept of access management consists of a few interrelated components, including users, service IDs, access groups, resources, policies, roles, actions, and the IBM Cloud IAM control system, which allows users to take actions on resources within an account.

IBM Cloud IAM follows an [eventually consistent](https://en.wikipedia.org/wiki/Eventual_consistency) pattern that is common to many cloud-native services. As a result, IAM remains highly available and performant across multiple global regions. Changes that are made to IAM access policies, authorizations, service IDs, API keys, access groups, resource groups, users, or any other access controls are recorded and propagated across all IAM components and IAM-enabled services worldwide. Access changes might not take effect until the propagation process is complete.

Access groups

A group of users and service IDs can be organized so that the same access can be assigned to all members within the group by using one or more policies. With access groups, you can streamline the access assignment process so that you can manage a smaller number of policies and reduce the number of policies in an account, which in turn increases performance. After your groups are set up, you can start assigning policies by selecting an access group as the subject of the policy. For more information, see [Setting up access groups](https://cloud.ibm.com/docs/account?topic=account-groups).

Resources

Account resources are the provisioned service offerings that are selected from the catalog or finer-grained resources within a service instance, such as an IBM® Cloud Object Storage bucket. IAM-enabled resources are added to a resource group when they are created from the catalog.

IAM access management enables fine-grained access, which means that a policy can be set on a wide scale to all resources in a resource group, for example, or to a specific service instance in the account and even a resource type like a IBM Cloud Object Storage bucket within a specific instance.

Access policies

Access policies are how users, [service IDs](https://cloud.ibm.com/docs/account?topic=account-serviceids), and access groups in the account are given permission to access and take actions on account resources. Policies include a subject, target, and role. The subject is the user, service ID, or access group that you are providing access. The target of the policy is the resource to which you want to provide access. And, the IAM roles define the level of access or allowed actions on the target of the policy.

A policy assigns the subject one or more roles that define the level of access and one or more attributes that define the target that the policy allows access to. The policy can provide access to a single service at the instance level, to a set of resources organized together in a resource group or to any set of resources that can be defined by a set of attributes such as region or resource type. A policy can also provide access to account management services. Depending on the IAM roles that you assign, the subject is allowed varying levels of access for completing account management tasks, working with service instances, or accessing a service by using the console or completing API calls.

There are different types of policies that allow access to account resources for users and service IDs: a resource group policy, a resource instance policy, an account-wide policy for access to all IAM-enabled services or all instances of a specified service, and a policy on all or one account management services. Depending on your selections, custom configuration options, such as defining access to resources in a specific region or defining access to the granular level of a service-specific resource within an instance, might be available.

In addition to access policies for users and service IDs, there is a policy type that is called an authorization that allows specific services or instances of services access to other services. You can learn more about assigning access between services in the [Using authorizations to grant access between services](https://cloud.ibm.com/docs/account?topic=account-serviceauth) documentation.

Roles

IBM Cloud IAM access roles allow users and service IDs to complete specific tasks within the context of the target resources that are defined in the policy. There are two types of predefined access roles: platform management and service access. The third type of access role is a custom role that you can create for a service to combine any set of available actions to meet your organizational needs.

Platform management roles define allowable actions, such as assigning user access and creation of service instances, for managing resources at the platform level. Platform roles also apply to actions that can be taken within the context of account management services, such as inviting and removing users, managing access groups, managing service IDs, and private catalog offerings.

Service access roles define allowable actions, such as calling service APIs or accessing a service's dashboard. These roles are customized based on the service that is selected within the policy.

When you assign access within the console, next to the role you can see the number of actions that are mapped to each role and drill down into that list to see exactly what each role allows.

For more information, see [IAM roles](https://cloud.ibm.com/docs/account?topic=account-userroles).

Actions

Actions are mapped to IBM Cloud IAM roles so that users can perform only specific tasks when they are assigned the different roles. Sometimes actions are also referred to as permissions or operations. Allowable actions for each role change based on the service that is being accessed because each service defines how that role maps to the use of the service.

Access management system

The IBM Cloud IAM control system allows or denies actions by users or service IDs within the context of a service based on their assigned access policies. By default, every user and service ID has no access. Each access policy that is added enables the user or service ID to perform an action within the account based on the specified target and role that is selected in the access policy. When a user tries to complete a specific action, the control system uses the attributes that are defined in the policy to determine whether the user has permission to perform that task. For more information about this process, check out the next section on How IBM Cloud IAM works.

**How does IBM Cloud IAM work?**

There are two common types of IAM systems in cloud providers and understanding each of these models can help you gain a better understanding of how IAM works in IBM Cloud.

* Attribute-based access control (ABAC) uses attributes from identities, such as users and service IDs, environments, and resources. These attributes are used by an access decision engine to determine if an access request should be permitted or denied. ABAC provides more flexibility, control, and features than role-based access control systems. ABAC is typically used when fine-grained access control is needed, or if a wide variety of access control use cases needs to be solved by the same decision engine. ABAC helps reduce security risks by providing fine-grained access control and is typically more complex, especially during initial setup.
* Role-based access control (RBAC) uses a mapping from an identity, such as a user or service ID, to a role. The RBAC role defines the type of access that an identity with the RBAC role can take against a resource. Typically access can be granted for a resource type or a grouping of resources. RBAC roles are usually defined based on job responsibilities within an organization. The RBAC role grants the access that is needed for an identity to do its job. This is a simple model because IAM administrators manage the mapping of RBAC roles to an identity. RBAC roles setup can be simpler than ABAC initial setup.

IBM Cloud IAM uses an ABAC model using identity and resource attributes. IBM Cloud IAM uses access policies to store the attribute information that is needed by the IAM access decision engine. And, the access policies tell the IAM decision engine which attributes the author of the policy requires to grant access to a resource.

Supported attributes for identities are:

* iam\_id
* access group ID

Supported attributes for resources belong to one of the following categories:

* Fields defined in the resource [CRN](https://cloud.ibm.com/docs/account?topic=account-crn), for example the service name.
* System-wide defined resource attributes, such as resource groups.
* Service-specific resource attributes such as namespaces or buckets.

Each service defines the supported attributes for resources it manages. Refer to the documentation for the service you're using for more information.

A best practice in IBM Cloud IAM is to use access groups to manage access for identities. After the access group access policies are defined, granting and revoking access is simply a matter of adding and removing identities to or from access groups. A user or service ID can belong to as many access groups as the administrator wants, and the members of the group inherit all access that is assigned to the access group. This approach provides the fine-grained access benefits of ABAC with the simplicity of RBAC.

IAM administrators familiar with RBAC might use access groups to mimic an RBAC model. Conceptually an access group is similar to an RBAC role. If you're more familiar with using traditional RBAC roles like system administrator, network administrator, or storage administrator, these can be defined in IBM Cloud IAM by using access groups with specific access policies assigned to each. For more information about using access groups and the best practices for assigning access, see [Best practices for organizing resources and assigning access](https://cloud.ibm.com/docs/account?topic=account-account_setup).

For example, you can create an access group called Storage Administrators. When it is first created, no access is granted to any members of the access group. The access group can then be assigned policies granting the Administrator role to all storage resources in the account that are currently provisioned as well as any that will be created in the future. If a new user joins the team and their job in the organization is a storage administrator for the account, then they can simply be added to the access group and have all of the access that they need to do their job.

This is a simple example, but the approach can be applied to any job, role, or responsibility in an organization. The access policies assigned to the access group can be fine-grained allowing for use cases like storage administrator of all storage in a specific resource group, and even for only a specific storage type.

For more information about getting up and running quickly with IBM Cloud IAM by setting up access groups for quick access assignments, inviting users to your account, and managing their access, see [Inviting users](https://cloud.ibm.com/docs/account?topic=account-access-getstarted).

**What features are provided?**

IBM Cloud IAM provides a wide range of features for your identity and access management needs.

User management

With unified user management, you can add and delete users in an account for both platform and classic infrastructure services. You can organize a group of users in an access group to make assigning access for more than one user or service ID at a time a quick and easy task.

Fine-grained access control

Access for users, service IDs, and access groups is defined by a policy. Within the policy, the scope of access can be assigned to a set of resources in a resource group, a single resource, or account management services. After the target is set, you can define what actions are allowed by the subject of the policy by selecting access roles. Roles provide a way to tailor the level of access that is granted for the subject of the policy to perform actions on the target of policy, whether it is platform management tasks within the account or accessing a service's UI or completing API calls.

Access groups for streamlined access management

Quickly and easily assign access for a group or users or service IDs organized in an access group by assigning access to the group, and then add or remove users or service IDs as needed to grant or deny access to account resources. Access groups enable you to manage a minimal number of policies in the account. For more information, see [Setting up access groups](https://cloud.ibm.com/docs/account?topic=account-groups).

API keys for user authentication

You can create multiple API keys for a user to support key rotation scenarios, and the same key can be used for accessing multiple services. IBM Cloud API keys enable users who use two-factor authentication or a federated ID to automate authentication to the console from the command line. A user can also have a single classic infrastructure API key that can be used to access classic infrastructure APIs; however, this is not required as you can use IBM Cloud API keys to access the same APIs. For more information, see [Understanding API keys](https://cloud.ibm.com/docs/account?topic=account-manapikey).

Service IDs

A service ID identifies a service or application similar to how a user ID identifies a user. These are IDs that can be used by applications to authenticate with an IBM Cloud service. Policies can be assigned to each service ID to control the level of access that is allowed by an application that uses the service ID, and an API key can be created to enable the authentication. For more information, see [Creating and working with service IDs](https://cloud.ibm.com/docs/account?topic=account-serviceids).

Multifactor authentication

You can require multifactor authentication (MFA) for every user in the account or just users with non-federated IDs who do not use SSO. All users with an IBMid use a time-based one-time passcode (TOTP) MFA method, and any users with a different type of ID must be enabled to use the TOTP, security questions, or external authentication method separately. For more information, see [Types of multifactor authentication](https://cloud.ibm.com/docs/account?topic=account-types).

Service to service authorizations

In a scenario that you need to provide one service access to another, you can create a policy by using a service to service authorization. For more information, see [Using authorizations to grant access between services](https://cloud.ibm.com/docs/account?topic=account-serviceauth).

**How do I use IBM Cloud IAM?**

You can access and use IBM Cloud IAM through the Access (IAM) UI, CLI, or API.

* To access IBM Cloud IAM by using the console, go to **Manage** > **Access (IAM)**.
* Go to [Managing IAM access, API keys, service IDs, and access groups](https://cloud.ibm.com/docs/cli?topic=cli-ibmcloud_commands_iam) to review the available CLI commands.
* Go to the following API docs to review the available APIs:
  + [IAM Identity Services API](https://cloud.ibm.com/apidocs/iam-identity-token-api)
  + [IAM Access Groups API](https://cloud.ibm.com/apidocs/iam-access-groups)
  + [IAM Policy Management API](https://cloud.ibm.com/apidocs/iam-policy-management)

**Mapping IBM Cloud IAM concepts to other cloud providers**

Identity and access management is used to securely authenticate users and provide access to cloud resources. While IAM across cloud providers is a consistent way of securing authentication and access, the concepts within each cloud provider and how they apply might differ. Review the following information in the table to learn more about how concepts in IBM Cloud IAM relate or compare to those of other cloud providers to help you onboard smoothly with IBM Cloud.

The following mappings of IBM Cloud IAM concepts to those of other cloud providers, such as Amazon Web Services (AWS), Google Cloud Platform, and Microsoft Azure, might not be an exact one-to-one match. However, if you are familiar with a particular concept within another provider, this mapping is intended to help you find the closest related concept in IBM Cloud.

| **IBM Cloud concept** | **IBM Cloud description** | **AWS** | **Azure** | **Google Cloud Platform** |
| --- | --- | --- | --- | --- |
| **Identities** | Users and service IDs | Users, groups, and roles | User, group, service principal, managed identity | User accounts and service accounts. Supported identity types: Google Account, Service account, Google group, G Suite domain, Cloud Identity domain |
| **Users** | Managed outside IAM. Users are uniquely identified in IBM Cloud with the iam\_id value, but can come from IBMid, App ID, or SoftLayer | Managed in IAM. Identity federated to external identity management system. | Managed in Active Directory | Managed outside IAM. Identity federated to external identity management system. |
| **Service IDs** | An ID for an app or service. | Roles assigned to an app | User-assigned identity | Service accounts |
| **API key** | A credential used for a user or service ID | Access Key | api-key | API key |
| **Access groups** | A way to organize users and service IDs where all members of the group are assigned the same access. | Groups, roles | Active Directory groups | Google Groups |
| **Policy** | Access assignment made up of a subject, target, and role. | Policy | Role assignment | Policy |
| **Policy subject** | A user, service ID, or access group | An IAM user, group, or a role | Security principal | A resource |
| **Roles** | A role is a collection of actions for a specific resource that are used as a building block to make an access policy. | AWS-managed policy | Role definition | Predefined roles |
| **Custom roles** | Customer-defined and named role, including only the actions chosen by the user. | Customer-managed policies | Custom roles | Custom roles |
| **Actions** | What is allowed to be completed within the context of the platform or service | Actions | Permissions | Permissions |
| **Resources** | Target of an access policy | Resources | Resources | Resources |
| **Resource groups** | Logical organization container for IAM-enabled services | Tags | Resource groups | Projects |
| **Public access** | Public access to specific resources is enabled through a default access group called Public Access. This feature can be disabled on each account. | Feature of Amazon S3 that can be enabled for specific resources, and can be disabled at the account or bucket level. | Public read access can be enabled for specific account types or resources. It can be disabled at the storage account or container level. | Google has an identifier for allAuthenticatedUsers that represents all service accounts and all users who are authenticated with a Google Account, which can also be granted access. |
| **Auditing** | Audit with Activity Tracker | Audit with AWS CloudTrail | Azure Logging and Auditing Activity logs | Audit with Audit logging |
| Table 1. IBM Cloud IAM concept comparison | | | | |

IBM Cloud access policies

To help you further understand how access is assigned by using access policies in IBM Cloud in relation to other cloud providers that you might be familiar with, check out the following details and example of an access policy.

IBM Cloud IAM policies consist of the identity who (subject) is being given access, such as the user or service ID, the specific resources or services (target) to which they are being given access, and roles that define what actions are allowed within the context of the selected resource or service.

In IBM Cloud, a user, service ID, or the members of an access group don't have any access by default. The IBM Cloud access model is simple when it comes to understanding how you get permitted or denied to complete specific actions. It isn't until an administrator assigns an access policy with a particular access role that access is granted. The IAM system doesn't have to evaluate permit and deny policies to determine what actions are allowed, instead the system just evaluates what resources you have policies for and what level of access is allowed by your assigned roles.

When you specify a resource in a policy because IBM Cloud is [attribute-based](https://cloud.ibm.com/docs/account?topic=account-iamoverview#how-iam-works), you can specify a broad set of resources for a user to have access to, for example all resources in a resource group. Or, you can narrow the user's access to a specific instance of a single service or even a subresource type, such as a Object Storage bucket. IBM Cloud IAM provides a high level of flexibility and granularity to help you assign only the type of access that is required. A few examples of the different levels of access that you can assign by using attributes in an access policy are the following:

* All account management services
* A specific account management service
* All IAM resources within the account
* All resources that belong to a resource group
* All resource types of a single service across the entire account, regardless of resource group assignment
* A specific instance of a service in the account
* A single subresource type within an instance, for example, a bucket in an Object Storage instance

If a specific predefined platform or service role doesn't fit what you're looking for when assigning the level of access, you can create a [custom role](https://cloud.ibm.com/docs/account?topic=account-custom-roles) for a specific service and then choose from the available actions to create a role that fits your organization's needs.

**Policy example**

This policy example gives access to all service resources that belong to a resource group named default with an ID of abcd2e6fg1h74i44j5kl467m701n5289 with the Viewer platform role assigned. This policy can be assigned to a user, service ID, or access group. In this case, it is assigned to a user with an iam\_id of IBMid-3IAMISBEST1.

Access groups are not identities like a user or service ID; however, they are a grouping mechanism for identities. An access group can be defined as a subject of an access policy, and the assigned access on the group applies to all members added to it.

{

"type": "access",

"subjects": [

{

"attributes": [

{

"name": "iam\_id",

"value": "IBMid-3IAMISBEST1"

}

]

}

],

"roles": [

{

"role\_id": "crn:v1:bluemix:public:iam::::role:Viewer"

}

],

"resources": [

{

"attributes": [

{

"name": "accountId",

"value": "7e522a19eb77477e88e96a600c44fb22"

},

{

"name": "resourceGroupId",

"value": "abcd2e6fg1h74i44j5kl467m701n5289"

}

]

}

]

}

In addition to an access policy for a user, service ID, or access group that can provide access to a service, specific resource, or resource group in the account, IBM Cloud also provides the capability to assign an access policy called a service to service authorization, which provides access between services. For an example of this policy type, see [Creating an authorization by using the API](https://cloud.ibm.com/docs/account?topic=account-serviceauth#auth-api).

Federating users to IBM Cloud

IBM Cloud offers two ways for you to federate your corporate identity provider (IdP), which simplifies login by giving your employees access to IBM Cloud with their company username and password. The first option is to [federate with IBMid](https://ibm.box.com/v/IBMid-Federation-Guide), and the other option is to create an IBM Cloud App ID service instance and use that as a way to federate users into an IBM Cloud account. For more information, see [Enabling authentication from an external identity provider](https://cloud.ibm.com/docs/account?topic=account-idp-integration).

In both cases, the federated user must be member of the account to be able to complete operations. In the case of IBMid, the account owner or administrator must invite individual IBMids into the IBM Cloud account. Only if the invited IBMid accepts the invitation is the user added the account as an active user. In the case of App ID, the user is automatically onboarded to IBM Cloud without a need to invite each user to the account. In both types of federation, the users are active IBM Cloud account users that can access the platform, including IAM-enabled resources, Cloud Foundry, and class infrastructure all depending on their assigned access.

IBM Cloud deals with federated users differently than other cloud providers, such as AWS. In AWS, if the customer federates their corporate IdP, users from that IdP aren't added as what we might consider normal account users. Instead, they get an IAM Role assigned, which enables them to complete their work. If that user logs out from their IAM Role, then there is no further information or other elements that are stored for that IAM Role. AWS isn't onboarding those users into their IAM system.