ORACLE

Best Practices for Identity and Access Management (IAM) in Oracle Cloud Infrastructure

August 2021, version 1.1

Public

Disclaimer

This document in any form, software, or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

Revision History

The following revisions have been made to this document since its initial publication.

DATE	REVISION
August 2021	Updated to new template and edited
March 2018	Initial publication

Table of Contents

Overview

This technical brief provides best practices for using the Oracle Cloud Infrastructure (OCI) Identity and Access Management (IAM) service when you're planning, designing, and deploying solutions on OCI.

The IAM service lets you control who has access to your cloud resources. You can control what type of access a group of users has and to which specific resources. The service enables you to enforce the security principle of least privilege by default. New users aren't allowed to perform actions on any resources until they're granted with appropriate permissions.

With the IAM service, you can use a single model for authentication and authorization across all OCI services. IAM makes it easy to manage access for organizations of all sizes, from one person working on a single project to large companies with many groups working on many projects at the same time, all within a single account.

This brief describes the different IAM components and provides best practice recommendations.

IAM Service Components

The IAM service consists of several key components that help you control access to your resources. This section provides basic definitions of these components.

- **Resource**: A cloud object that your company's employees create and use when interacting with OCI. Resources include compute instances, block storage volumes, virtual cloud networks (VCNs), subnets, and route tables.
- **User**: An individual employee or system that needs to manage or use your company's OCI resources. Users might need to deploy instances, manage remote disks, work with your virtual cloud network, and so on. End users of your application aren't typically IAM users. Users have one or more IAM credentials.
- **Group**: A collection of users who all need the same type of access to a particular set of resources or compartment.
- **Compartment**: A collection of related resources. Compartments are a fundamental component of OCI for organizing and isolating your cloud resources. You use them to clearly separate resources for the purposes of measuring usage and billing, access (by using policies), and isolation (by separating the resources for one project or business unit from another). A common approach is to create a compartment for each major part of your organization.
- **Tenancy**: The root compartment that contains all your organization's OCI resources. Oracle automatically creates your company's tenancy for you. Directly within the tenancy are your IAM entities: users, groups, compartments, and some policies. You can also put policies into compartments inside the tenancy. You place the other types of cloud resources, such as instances, virtual networks, and block storage volumes, inside the compartments that you create.
- **Policy**: A document that specifies who can access which resources and how. Access is granted at the group level and compartment level. So, you can write a policy that gives a group a specific type of access within a specific compartment or to the tenancy itself. If you give a group access to the tenancy, the group automatically gets the same type of access to all the compartments inside the tenancy. People use the word policy in different ways: an individual statement written in the policy language; a collection of statements in a single, named "policy" document (which has an Oracle Cloud ID (OCID) assigned to it); and the overall body of policies that your organization uses to control access to resources.

- **Home region**: The region where your IAM resources reside. All IAM resources are global and available across all regions, but the master set of definitions resides in a single region, the home region. You make changes to your IAM resources in your home region, and the changes are automatically propagated to all regions.

The following diagram illustrates these key components of the IAM service:

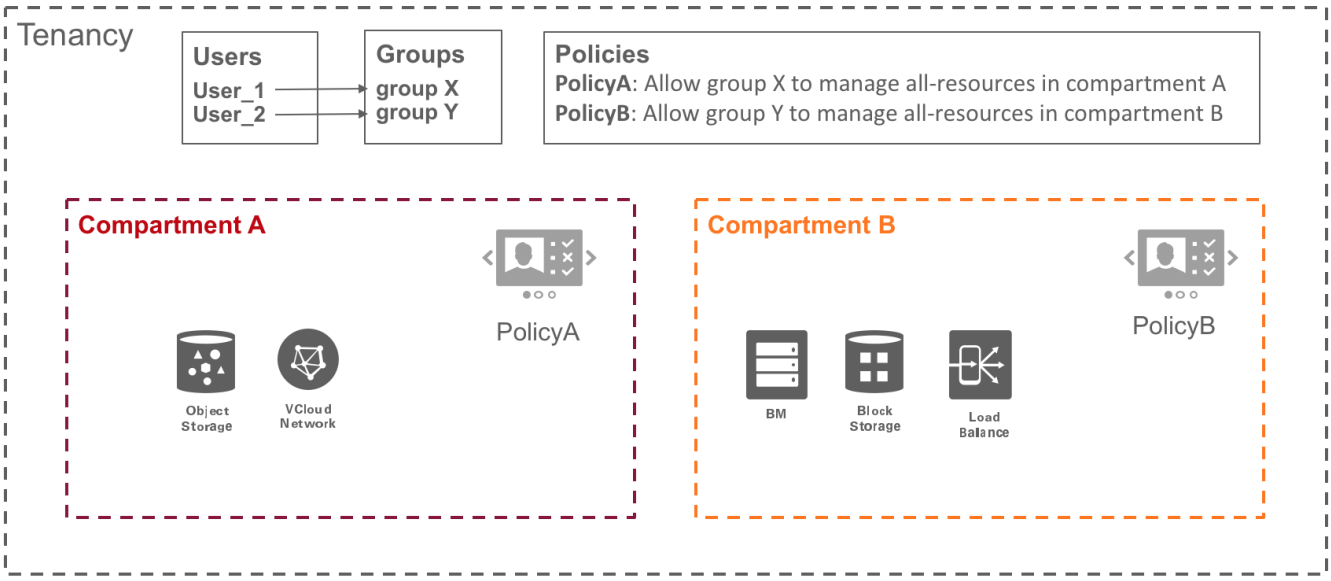

Figure 1: Oracle Cloud Infrastructure IAM Service Components

Tenancy and Compartment Design

Compartments are the primary building blocks that you use to organize your cloud resources. You use compartments to organize and isolate your resources, which makes it easier to manage and secure access to them.

When you start working with Oracle Cloud Infrastructure, carefully consider how you want to use compartments to organize and isolate your cloud resources. After you create a compartment, you can't delete it, so it's important to consider your compartment design for your organization before you implement anything.

Consider the following aspects when you start working with compartments:

- When you create a resource, such as a compute instance, block storage volume, VCN, or subnet, you must place it in a compartment.
- Compartments are logical, not physical, so you can place related resource components in different compartments. For example, you can secure your cloud network subnets with access to an internet gateway in a separate compartment from other subnets in the same cloud network.
- After a resource is created, you can't move it to another compartment.
- When you write a policy rule to grant a group of users access to a resource, specify the compartment to apply the access rule to. If you distribute resources across compartments, you must provide the appropriate permissions for each compartment for users who need access to those resources.
- Compartments can't be deleted, so don't create multiple test compartments with the intent of deleting them later.
- When planning for compartments, consider how you want aggregate usage and auditing data, which might be a consideration for your company in the future.

Your compartment design depends on your use cases and how you want to organize and isolate your resources. The following scenarios are examples.

Proof of Concept, Sandbox Compartment

If your organization is small or if you're still in the proof-of-concept stage of evaluating OCI, consider placing all of your resources in the root compartment (tenancy). This approach makes it easy for you to quickly view and manage all your resources. You can still write policies and create groups to restrict permissions on specific resources to only the users who need access.

If you plan to maintain all your resources in the root compartment, we recommend setting up a separate sandbox compartment to give users a dedicated space to try out features. In the sandbox compartment, you can grant users permissions to create and manage resources, while maintaining stricter permissions on the resources in your tenancy (root) compartment.

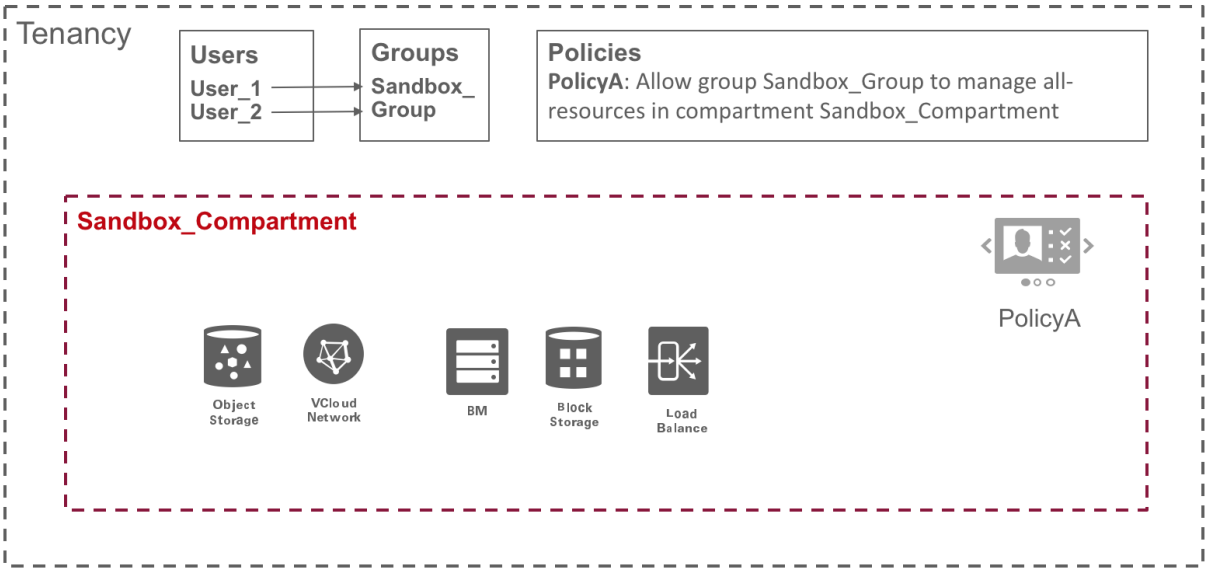

Figure 2: Sandbox Compartment

Production Use

For production, restrict access to your resources and consider how to organize your resources into compartments. Create a plan for your tenancy and compartments before you add users and resources. In your plan, include the compartment hierarchy for organizing your resources and the definitions of the user groups that need access to the resources. These two things impact how you write policies to manage access, so consider them together.

If your company has multiple departments that you want to manage separately or several distinct projects that would be easier to manage separately, we recommend aligning your compartment structure with different departments or projects. With this approach, you can add a dedicated administrator group for each compartment (project) who can set the access policies for just that project. (Users and groups still must be added at the tenancy level.) You can give one group control over all their resources, while not allowing them administrator rights to the root compartment or any other projects. This way, you can enable different groups at your company to set up their own "subclouds" for their own resources and administer them independently.

The following scenario illustrates how to design your compartments and define related policies.

Company ACME has three major departments: A, B, and C. ACME has multiple types of administrators: department database administrators (DBAs), network administrators, storage administrators, and security administrators. Each DBA manages their own department's database. Network, storage, and security administrators need to access and manage corresponding network, storage, and security-related resources for all three departments.

To accommodate these needs, create three compartments to align with ACME's department structure. Then, define groups that map to each type of administrator. Finally, define policies to control who can access which resources.

The following diagram illustrates a possible compartment and policy design for this scenario:

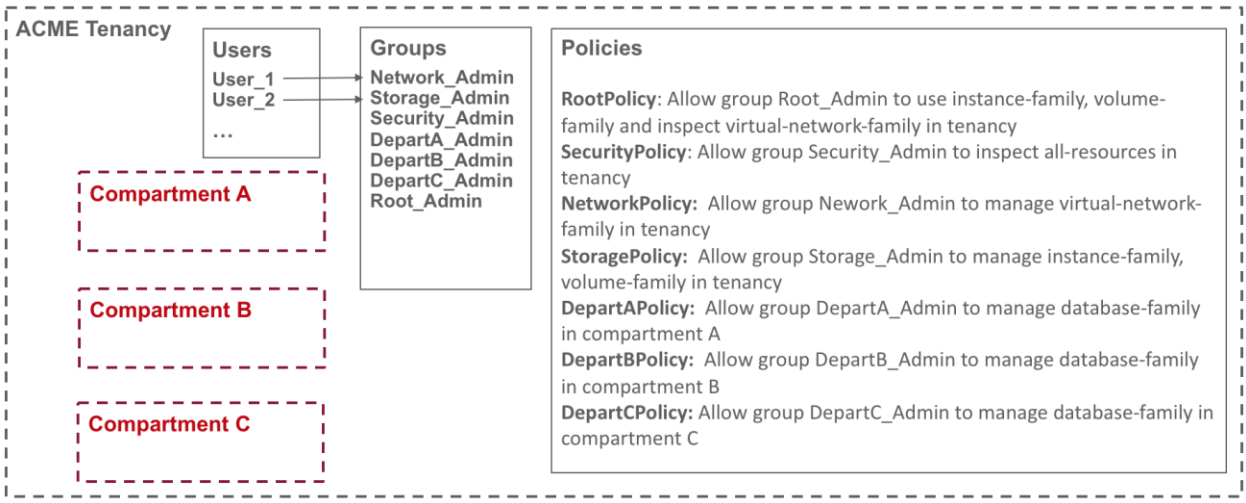

Figure 3: Scenario for Compartment and Policy Design

Basic User and Permission Management

To manage users, you must be in the Administrators group in the IAM service. Depending on your use cases, you can delegate user management tasks to other users. For example, you can create a policy that gives someone power to create users and credentials but no permission to control which groups those users are in. You can also create a policy that gives someone permission to determine what groups users are in but no permission to create or delete users.

When creating a user, provide an unchangeable name for the user that's unique across all users within your tenancy. A new user has no permissions until you place the user in a group that has at least one policy that gives that group permission to either the tenancy or a compartment.

We recommend clearly categorizing the roles of your new users first and then placing them in groups with the appropriate governing policies. For example, if a user is a DBA, you can place them in a database administrator group that has policies that grant permissions to manage the "database-family" resource-type for the corresponding compartments.

We also recommend starting users with least privilege and then gradually grant the more permissions as necessary.

Permission management in Oracle Cloud Infrastructure is done through policies. A policy allows a group to work in certain ways with specific types of resources in a particular compartment or tenancy. Policies give access to groups of users, not to individual users. Users gain access by being in groups.

Policies only allow access; they can't explicitly deny it. If you need to restrict a particular user's access, you can remove the user from a particular group of interest or delete the user from the IAM service entirely.

Each policy consists of one or more policy statements that follow this basic syntax:

```
Allow group <group_name> to <verb> <resource-type> in compartment <compartment_name>
```

The `<verb>` denotes the type of access: `inspect`, `read`, `use`, or `manage`. Each successive type of access includes the access in the preceding types. For example, `inspect` gives users in the group the ability to list resources without access to confidential information or user-specified metadata in the resource. The type `read` includes `inspect` plus the ability to get user-specified metadata and the actual resource itself.

The `<resource-type>` can be an aggregate (family) resource or an individual resource. For example, `database-family` is an aggregate resource-type, and `db-systems` and `db-nodes` are individual resource-types in that family.

We recommend starting with more granular policy definitions and then updating them for different use cases. For more information, see How Policies Work in the IAM service documentation.

Credential Management

You manage the following types of credentials with Oracle Cloud Infrastructure IAM:

- **Console password**: For signing in to the Console, which is the user interface for interacting with OCI
- **API signing key** (in PEM format): For sending API requests, which require authentication
- **Swift password**: For using a Swift client with Recovery Manager (RMAN) to back up an Oracle Database system (DB system) database to Object Storage

OCI already enforces a strong password policy for Console and Swift passwords. For example, the password requires twelve or more characters, at least one lowercase letter, at least one uppercase letter, at least one number, and at least one special character, and it can't be the same as the username.

However, these credentials currently have no expiration, so we recommend setting up a policy to change these credentials periodically. Because you can create multiple API signing keys and Swift passwords for a single user, we recommend deleting credentials that are no longer used.

Instance Principals and Dynamic Groups

The instance principals feature of IAM allows users to call IAM-protected APIs from an OCI Compute instance (virtual machine or bare metal) without the need to create IAM users or manage credentials for each instance.

For example, you have an application running on a Compute instance that needs to access the Object Storage service. Without instance principals, you need to create a specific user and then create a policy to grant permission to read and write to a bucket in the Object Storage service and then assign this policy to that user. The application uses the credential for the user to access the object bucket. The problem with this approach is that the private key for the user must be accessible to the application, probably by storing it in a configuration file. The process for obtaining the private key and storing it in the configuration file can be complicated and create security risks.

When you use instance principals, you create dynamic groups. Dynamic groups allow you to group compute instances as principal actors, like user groups. You can then create policies to permit instances to make API calls against OCI services. When creating a dynamic group, provide an unchangeable name for the dynamic group that's unique across all groups within your tenancy.

Note: Any user who has access to the instance automatically inherits the privileges granted to the instance. Before you use this feature to grant permissions to an instance, find out who can access the instance and determine whether they need authorization with the permissions that you're granting to the instance.

Federation

IAM supports federation with Oracle Identity Cloud Service and Microsoft Active Directory Federation Services (AD FS), using the Security Assertion Markup Language (SAML) 2.0 protocol.

To federate, an administrator sets up a relationship, commonly referred to as a federation trust, between the company's identity provider (IdP) and OCI. After that relationship is established, any person in the company who goes to the Oracle Cloud Console is prompted with a "single sign-on" experience provided by the IdP. The user signs in with the login ID and password that they've already set up with the IdP and use elsewhere. The IdP authenticates the user, and then that user can access OCI.

When working with your IdP, your administrator defines groups and assigns each user to one or more groups according to the type of access the user needs. OCI also uses groups with IAM policies to define the type of access that a user has. As part of setting up the relationship with the IdP, your administrator can map each IdP group to a similarly defined IAM group, so that your company can reuse the IdP group definitions when authorizing user access to OCI resources.

To make applying a filter rule easy, we recommend naming IdP groups that you intend to map to OCI groups with a common prefix. For example, you can use OCI_Administrators, OCI_NetworkAdmins, OCI_InstanceLaunchers, and so on.

Note: When you sign up for OCI, your tenant administrator account is automatically federated with Oracle Identity Cloud Service. Federating OCI with Oracle Identity Cloud Service automatically allows you to have a seamless connection between services without having to create a separate username and password for each one.

Conclusion

This brief recommends best practices for using the Oracle Cloud Infrastructure IAM service to securely manage and control access to your cloud resources. The following highlights summarize these best practices:

- Plan your tenancy and compartments before you add users and resources.
- Align your compartment design with your departments' or projects' structures.
- Categorize the roles of your users first and then place them into groups with the appropriate governing policies.
- Grant least privilege to users and gradually grant more permissions as needed.
- Enforce strong password policies and update passwords regularly.
- Use instance principals and dynamic groups when calling OCI services from Compute instances.
- Name federated identity provider (IdP) groups with the same prefix as OCI groups when mapping these groups.

Oracle Cloud Infrastructure is continuously evolving with new features. Stay updated through online documents and training at https://www.oracle.com/cloud/.

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle