Identity and Access Management (IAM): Create IAM Components

Lab 2-1 Practices

Get Started

Overview

Oracle Cloud Infrastructure (OCI) Identity and Access Management (IAM) lets you control who has access to your cloud resources.

In this lab, we will help you create a compartment, group, user, and policy. We will also provide the steps to create a dynamic group.

Note: We have instructions for accounts with and without Identity Domains enabled.

In this lab, you'll:

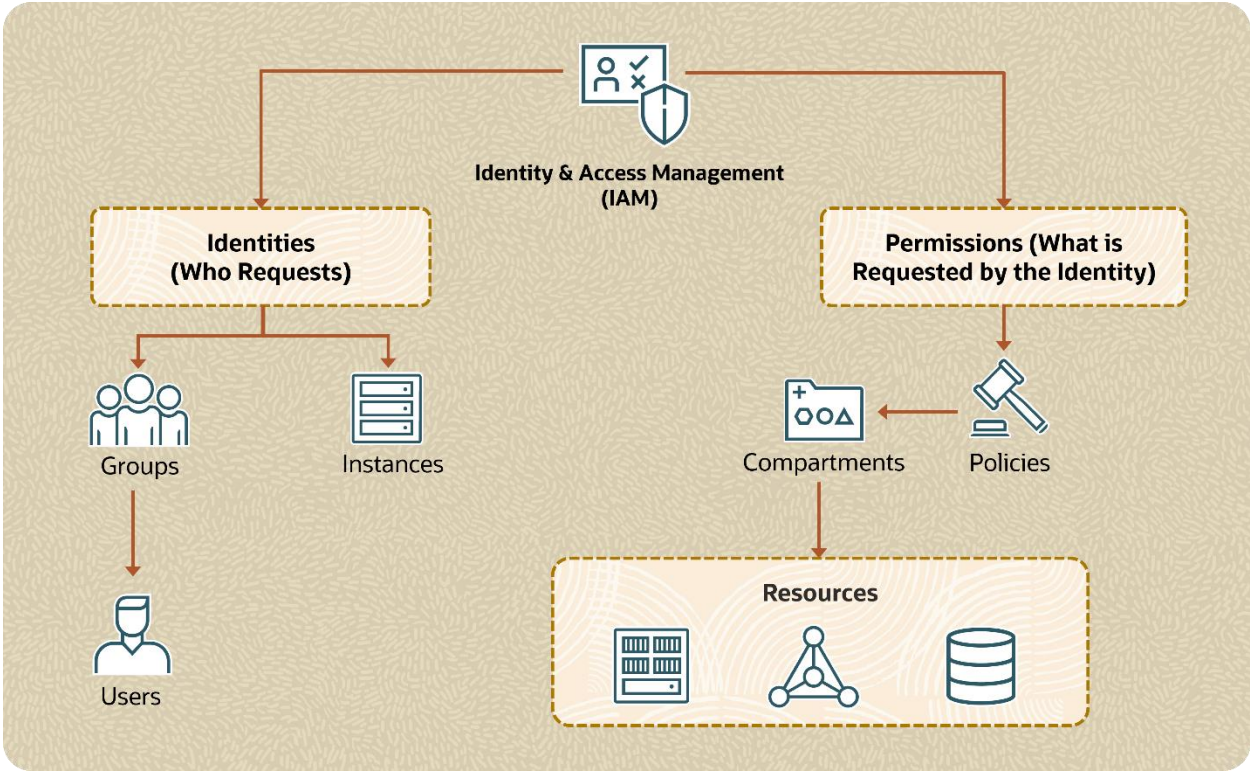
a. Create a compartment

b. Create a user

c. Create a group, and add a user to the group

d. Create a policy

e. Create a dynamic group



Create a Compartment (With Identity Domains Enabled)

A compartment is a collection of related resources. Compartments are fundamental components of OCI and are used for organizing and isolating your cloud resources.

In this practice, you will learn how to create a compartment.

Tasks

1. Sign in to the OCI Console.
2. Open the **Main Menu** and select **Identity & Security**. Under **Identity**, click **Compartments**. A list of the compartments to which you have access appears.
3. Click **Create Compartment.**
4. Do the following:
    a. **Name:** Enter a unique name for the compartment. The name must be unique across all the compartments in your tenancy.
    b. **Description:** Enter a compartment-related description.
    c. **Parent Compartment:** The compartment you are in appears by default.
5. Click **Create Compartment**. The Child Compartment now appears in the list of compartments.

Create a User (With Identity Domains Enabled)

A user is an individual employee or system that needs to manage or use your company's OCI resources.

In this practice, you'll learn how to create a user.

Tasks

1. Open the **Main Menu** and select **Identity & Security**. Under **Identity**, click **Domains**. A list of domains in your tenancy appears.
2. Select the Domain that is allotted to you. Otherwise, you can click on the **Default** domain.
3. Under **Identity domain**, click **Users**. A list of the users in your domain appears.
4. Click **Create User**.
5. Enter the following:
    a. **First Name:** Enter first name of user.
    b. **Last Name:** Enter last name of user.
    c. **Username/Email:** Enter an email address for the user.
    d. Check the **Use the same email address as the username.** Do not select the **Assign cloud account administrator role** check box.
6. Click **Create**. The user now appears in the list of users.

Create a Group, and Add a User to the Group (With Identity Domains Enabled)

A group is a collection of users who need the same type of access to a particular compartment or set of resources.

In this practice, you'll learn how to create a group, and add a user to a group.

Tasks

1. Open the **Main Menu** and select **Identity & Security**. Under **Identity**, click **Domains**. A list of domains in your tenancy appears.
2. Click on the **Default** domain.
3. Under **Identity domain**, click **Groups**. A list of the groups in your domain appears.
4. Select the **Administrators** group.
5. Click **Assign User to Groups**.
6. Select the user created earlier from the **Users** drop-down list, and then click **Add**. The user now appears in the group.
7. Use the breadcrumb trail to go back to the **Groups** page and click **Create Group**.
8. Enter the following:
    a. **Name:** Enter a unique name for the group**.**
    b. **Description:** Enter a group-related description.
9. Click **Create.** The group now appears in the list of groups.

Create a Policy (With Identity Domains Enabled)

A policy is a document that specifies who can access which resources, and how.

In this practice, you'll learn how to create a policy.

Tasks

1. Open the **Main Menu** and select **Identity & Security**. Under **Identity**, click **Policies**.
2. Click **Create Policy**.
3. Enter the following:
    a. **Name:** Enter a unique name for the policy.
    b. **Description:** Enter a policy-related description.
    c. **Compartment:** If you want to attach the policy to a compartment other than the one you're viewing, select it from the drop-down list. Remember, where the policy is attached controls who can later modify or delete it.
4. In the **Policy Builder** section, click **Show manual editor** and enter the policy statement.

    Note: A sample statement would look like the following:

    ```
    allow group <group_name> to manage virtual-network-family in
    compartment <compartment_name>
    ```

5. Click **Create.** The policy now appears in the list of policies.

Create a Dynamic Group (With Identity Domains Enabled)

A dynamic group is a special type of group that contains resources, such as compute instances, which match rules that you define. This means that group membership can change dynamically as matching resources are created or deleted. These instances serve as "principal" actors and can make API calls to services according to policies that you write for the dynamic group.

In this practice, you'll learn how to create a dynamic group.

Tasks

1. Open the **Main Menu** and select **Identity & Security**. Under **Identity**, click **Domains.** A list of domains in your tenancy appears.
2. Click on the **Default** domain.
3. Under **Identity domain**, click **Dynamic Groups**.
4. Click **Create Dynamic Group**.
5. Enter the following:
   a. **Name:** Enter a unique name for the group. The name must be unique across all groups in your tenancy, including dynamic groups and user groups.
   b. **Description:** Enter a friendly description.
6. Enter the **Matching Rules**. Resources that meet the rule criteria are members of the dynamic group.
   a. **Rule 1:** Enter a rule by following the guidelines in https://docs.oracle.com/en-us/iaas/Content/Identity/Tasks/managingdynamicgroups.htm#Writing https://docs.oracle.com/en-us/iaas/Content/Identity/Tasks/managingdynamicgroups.htm.
      Note: You can manually enter the rule in the text box or launch the rule builder.
      - For example, to include all instances that are in a specific compartment, add a rule with the following syntax:
        `instance.compartment.id = '<compartment_ocid>'`
   b. Enter additional rules as needed. To add a rule, click **+Additional Rule.**
7. Click **Create.** The dynamic group now appears in the list of dynamic groups.

Create a Compartment (Without Identity Domains Enabled)

A compartment is a collection of related resources. Compartments are fundamental components of OCI and are used for organizing and isolating your cloud resources.

In this practice, you will learn how to create a compartment.

Tasks

1. Sign in to the OCI Console.
2. Open the **Main Menu** and select **Identity & Security**. Under **Identity**, click **Compartments**. A list of the compartments to which you have access appears.
3. Under **Child Compartment**, click **Create Compartment.**
4. Do the following:
    a. **Name:** Enter a unique name for the compartment. The name must be unique across all the compartments in your tenancy.
    b. **Description:** Enter a compartment-related description.
    c. **Parent Compartment:** The compartment you are in appears by default. To choose another compartment in which to create this compartment, select from the drop-down list.
5. Click **Create Compartment**. The Child Compartment now appears in the list of compartments.

Create a User (Without Identity Domains Enabled)

A user is an individual employee or system that needs to manage or use your company's OCI resources.

In this practice, you'll learn how to create a user.

Tasks

1. Open the **Main Menu** and select **Identity & Security**. Under **Identity**, click **Users**. A list of users in your tenancy appears.
2. Click **Create User**.
3. Enter the following:
    e. **Name:** Enter a unique name or email address for the user.
    f. **Description:** This value could be the user's full name, a nickname, or any other descriptive information.
    g. **Email:** Enter an email address for the user. This email address is used for password recovery.
4. Click **Create**. The user now appears in the list of users.

Create a Group, and Add a User to the Group (Without Identity Domains Enabled)

A group is a collection of users who need the same type of access to a particular compartment or set of resources.

In this practice, you'll learn how to create a group, and add a user to a group.

Tasks

1. Open the **Main Menu** and select **Identity & Security**. Under **Identity**, click **Groups**. A list of the groups in your tenancy appears.
2. Click on the **Administrators** group.
3. Click **Add User to Group**.
4. Select the user created earlier from the **Users** drop-down list, and then click **Add**. The user now appears in the group.
5. Use the breadcrumb trail to go back to the **Groups** page and click **Create Group**.
6. Enter the following:
    c. **Name:** Enter a unique name for the group**.**
    d. **Description:** Enter a group-related description.
7. Click **Create.** The group now appears in the list of groups.

Create a Policy (Without Identity Domains Enabled)

A policy is a document that specifies who can access which resources, and how.

In this practice, you'll learn how to create a policy.

Tasks

1. Open the **Main Menu** and select **Identity & Security**. Under **Identity**, click **Policies**.
2. Choose a compartment.
3. A list of the policies in the compartment you're currently viewing appears.
4. Click **Create Policy**.
5. Enter the following:

    d. **Name:** Enter a unique name for the policy.

    e. **Description:** Enter a policy-related description.

    f. **Compartment:** If you want to attach the policy to a compartment other than the one you're viewing, select it from the drop-down list. Remember, where the policy is attached controls who can later modify or delete it.

6. In the **Policy Builder** section, click **Show manual editor** and enter the policy statement.

   Note: A sample statement would look like the following:

   ```
   allow group <group_name> to manage virtual-network-family in
   compartment <compartment_name>
   ```

7. Click **Create.** The policy now appears in the list of policies.

Create a Dynamic Group (Without Identity Domains Enabled)

A dynamic group is a special type of group that contains resources, such as compute instances, which match rules that you define. This means that group membership can change dynamically as matching resources are created or deleted. These instances serve as “principal” actors and can make API calls to services according to policies that you write for the dynamic group.

In this practice, you’ll learn how to create a dynamic group.

Tasks

1. Open the **Main Menu** and select **Identity & Security**. Under **Identity**, click **Dynamic Groups**.
2. Click **Create Dynamic Group**.
3. Enter the following:
   c. **Name:** Enter a unique name for the group. The name must be unique across all groups in your tenancy, including dynamic groups and user groups.
   d. **Description:** Enter a friendly description.
4. Enter the **Matching Rules**. Resources that meet the rule criteria are members of the dynamic group.
   c. **Rule 1:** Enter a rule by following the guidelines in https://docs.oracle.com/en-us/iaas/Content/Identity/Tasks/managingdynamicgroups.htm#Writing https://docs.oracle.com/en-us/iaas/Content/Identity/Tasks/managingdynamicgroups.htm.
   Note: You can manually enter the rule in the text box or launch the rule builder.
      – For example, to include all instances that are in a specific compartment, add a rule with the following syntax:
      `instance.compartment.id = '<compartment_ocid>'`
   d. Enter additional rules as needed. To add a rule, click **+Additional Rule.**
5. Click **Create.** The dynamic group now appears in the list of dynamic groups.