Lab 02a - Manage Subscriptions and RBAC Student lab manual

Lab requirements

This lab requires permissions to create Azure Active Directory (Azure AD) users, create custom Azure Role Based Access Control (RBAC) roles, and assign these roles to Azure AD users. Not all lab hosters may provide this capability. Ask your instructor for the availability of this lab.

Lab scenario

In order to improve management of Azure resources in Contoso, you have been tasked with implementing the following functionality:

- creating a management group that would include all of Contoso's Azure subscriptions
- granting permissions to submit support requests for all subscriptions in the management group to a designated Azure Active Directory user. That user's permissions should be limited only to:
    - creating support request tickets
    - viewing resource groups

Note: An **interactive lab simulation** is available that allows you to click through this lab at your own pace. You may find slight differences between the interactive simulation and the hosted lab, but the core concepts and ideas being demonstrated are the same.

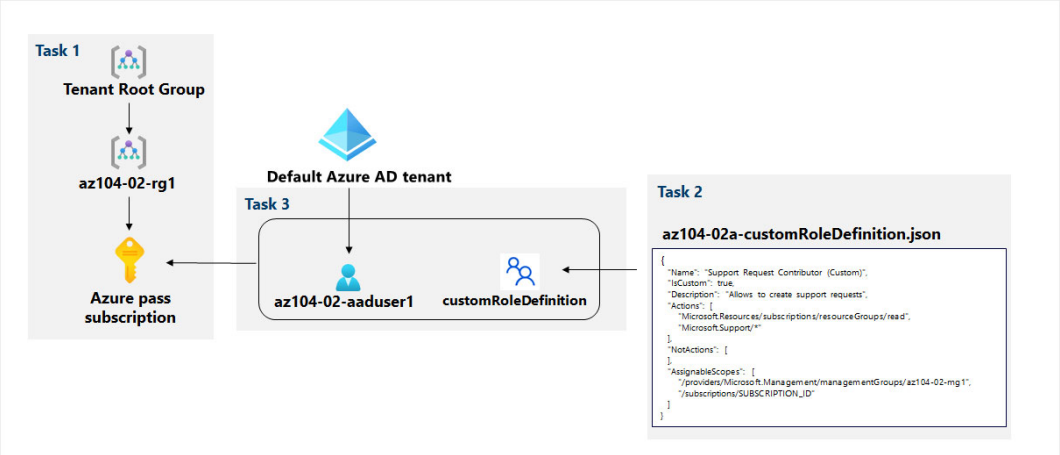
Objectives

In this lab, you will:

- Task 1: Implement Management Groups
- Task 2: Create custom RBAC roles
- Task 3: Assign RBAC roles

Estimated timing: 30 minutes

Architecture diagram



Instructions

Exercise 1

Task 1: Implement Management Groups

In this task, you will create and configure management groups.

1. Sign in to the **Azure portal**.
2. Search for and select **Management groups** to navigate to the **Management groups** blade.
3. Review the messages at the top of the **Management groups** blade. If you are seeing the message stating **You are registered as a directory admin but do not have the necessary permissions to access the root management group**, perfom the following sequence of steps:
   a. In the Azure portal, search for and select **Azure Active Directory**.
   b. On the blade displaying properties of your Azure Active Directory tenant, in the vertical menu on the left side, in the **Manage** section, select **Properties**.
   c. On the **Properties** blade of your your Azure Active Directory tenant, in the **Access management for Azure resources** section, select **Yes** and then select **Save**.
   d. Navigate back to the **Management groups** blade, and select **Refresh**.
4. On the **Management groups** blade, click **+ Create**.

   > **Note**: If you have not previously created Management Groups, select **Start using management groups**

5. Create a management group with the following settings:

Setting	Value
Management group ID	**az104-02-mg1**
Management group display name	**az104-02-mg1**

6. In the list of management groups, click the entry representing the newly created management group.
7. On the **az104-02-mg1** blade, click **Subscriptions**.
8. On the **az104-02-mg1 | Subscriptions** blade, click **+ Add**, on the **Add subscription** blade, in the **Subscription** drop-down list, select the subscription you are using in this lab and click **Save**.

   > **Note**: On the **az104-02-mg1 | Subscriptions** blade, copy the ID of your Azure subscription into Clipboard. You will need it in the next task.

Task 2: Create custom RBAC roles

In this task, you will create a definition of a custom RBAC role.

1. From the lab computer, open the file **\Allfiles\Labs\02\az104-02a-customRoleDefinition.json** in Notepad and review its content:

   Code | Copy

```
{
   "Name": "Support Request Contributor (Custom)",
   "IsCustom": true,
   "Description": "Allows to create support requests",
   "Actions": [
       "Microsoft.Resources/subscriptions/resourceGroups/read",
       "Microsoft.Support/*"
   ],
   "NotActions": [
   ],
   "AssignableScopes": [
       "/providers/Microsoft.Management/managementGroups/az104-02-mg1",
       "/subscriptions/SUBSCRIPTION_ID"
   ]
}
```

> **Note**: If you are not sure where the files are stored locally in your lab environment, please ask your instructor.

2. Replace the `SUBSCRIPTION_ID` placeholder in the JSON file with the subscription ID you copied into Clipboard and save the change.

3. In the Azure portal, open **Cloud Shell** pane by clicking on the toolbar icon directly to the right of the search textbox.

4. If prompted to select either **Bash** or **PowerShell**, select **PowerShell**.

> **Note**: If this is the first time you are starting **Cloud Shell** and you are presented with the **You have no storage mounted** message, select the subscription you are using in this lab, and click **Create storage**.

5. In the toolbar of the Cloud Shell pane, click the **Upload/Download files** icon, in the drop-down menu click **Upload**, and upload the file **\Allfiles\Labs\02\az104-02a-customRoleDefinition.json** into the Cloud Shell home directory.

6. From the Cloud Shell pane, run the following to create the custom role definition:

Code Copy

```
New-AzRoleDefinition -InputFile $HOME/az104-02a-customRoleDefinition.json
```

7. Close the Cloud Shell pane.

Task 3: Assign RBAC roles

In this task, you will create an Azure Active Directory user, assign the RBAC role you created in the previous task to that user, and verify that the user can perform the task specified in the RBAC role definition.

1. In the Azure portal, search for and select **Azure Active Directory**, on the Azure Active Directory blade, click **Users**, and then click **+ New user**.

2. Create a new user with the following settings (leave others with their defaults):

Setting	Value
User name	**az104-02-aaduser1**
Name	**az104-02-aaduser1**
Let me create the password	enabled

Setting	Value
Initial password	**Provide a secure password**

> **Note**: **Copy to clipboard** the full **User name**. You will need it later in this lab.

3. In the Azure portal, navigate back to the **az104-02-mg1** management group and display its **details**.
4. Click **Access Control (IAM)**, click **+ Add** and then **Add role assignment**. On the **Role** tab, search for **Support Request Contributor (Custom)**.

> **Note**: if your custom role is not visible, it can take up to 10 minutes for the custom role to appear after creation.

5. Select the **Role** and click **Next**. On the **Members** tab, click **+ Select members** and **select** your user account az104-**********.***.onmicrosoft.com. Click **Next** and then **Review and assign**.
6. Open an **InPrivate** browser window and sign in to the Azure portal using the newly created user account. When prompted to update the password, change the password for the user.

> **Note**: Rather than typing the user name, you can paste the content of Clipboard.

7. In the **InPrivate** browser window, in the Azure portal, search and select **Resource groups** to verify that the az104-02-aaduser1 user can see all resource groups.
8. In the **InPrivate** browser window, in the Azure portal, search and select **All resources** to verify that the az104-02-aaduser1 user cannot see any resources.
9. In the **InPrivate** browser window, in the Azure portal, search and select **Help + support** and then click **+ Create a support request**.
10. In the **InPrivate** browser window, on the **Problem Desription/Summary** tab of the **Help + support - New support request** blade, type **Service and subscription limits** in the Summary field and select the **Service and subscription limits (quotas)** issue type. Note that the subscription you are using in this lab is listed in the **Subscription** drop-down list.

> **Note**: The presence of the subscription you are using in this lab in the **Subscription** drop-down list indicates that the account you are using has the permissions required to create the subscription-specific support request.

> **Note**: If you do not see the **Service and subscription limits (quotas)** option, sign out from the Azure portal and sign in back.

11. Do not continue with creating the support request. Instead, sign out as the az104-02-aaduser1 user from the Azure portal and close the InPrivate browser window.

Task 4: Clean up resources

> **Note**: Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not see unexpected charges, although, resources created in this lab do not incur extra cost.

> **Note**: Don't worry if the lab resources cannot be immediately removed. Sometimes resources have dependencies and take a longer time to delete. It is a common Administrator task to monitor resource usage, so just periodically review your resources in the Portal to see how the cleanup is going.

1. In the Azure portal, search for and select **Azure Active Directory**, on the Azure Active Directory blade, click **Users**.
2. On the **Users - All users** blade, click **az104-02-aaduser1**.
3. On the **az104-02-aaduser1 - Profile** blade, copy the value of **Object ID** attribute.
4. In the Azure portal, start a **PowerShell** session within the **Cloud Shell**.
5. From the Cloud Shell pane, run the following to remove the assignment of the custom role definition (replace the `[object_ID]` placeholder with the value of the **object ID** attribute of the **az104-02-aaduser1** Azure Active Directory user account you copied earlier in this task):

   Code Copy

   ```
   $scope = (Get-AzRoleDefinition -Name 'Support Request Contributor
   (Custom)').AssignableScopes[0]

   Remove-AzRoleAssignment -ObjectId '[object_ID]' -RoleDefinitionName 'Support Request
   Contributor (Custom)' -Scope $scope
   ```

6. From the Cloud Shell pane, run the following to remove the custom role definition:

   Code Copy

   ```
   Remove-AzRoleDefinition -Name 'Support Request Contributor (Custom)' -Force
   ```

7. In the Azure portal, navigate back to the **Users - All users** blade of the **Azure Active Directory**, and delete the **az104-02-aaduser1** user account.
8. In the Azure portal, navigate back to the **Management groups** blade.
9. On the **Management groups** blade, select the **ellipsis** icon next to your subscription under the **az104-02-mg1** management group and select **Move** to move the subscription to the **Tenant Root management group**.

   > **Note**: It is likely that the target management group is the **Tenant Root management group**, unless you created a custom management group hierarchy before running this lab.

10. Select **Refresh** to verify that the subscription has successfully moved to the **Tenant Root management group**.
11. Navigate back to the **Management groups** blade, click the **ellipsis** icon to the right of the **az104-02-mg1** management group and click **Delete**.

    > **Note**: If you are unable to delete the **Tenant Root management group**, chances are that the **Azure Subscription** is under the management group. You need to move **Azure Subscription** out of the **Tenant Root management group** and then delete the group.

Review

In this lab, you have:

- Implemented Management Groups
- Created custom RBAC roles
- Assigned RBAC roles