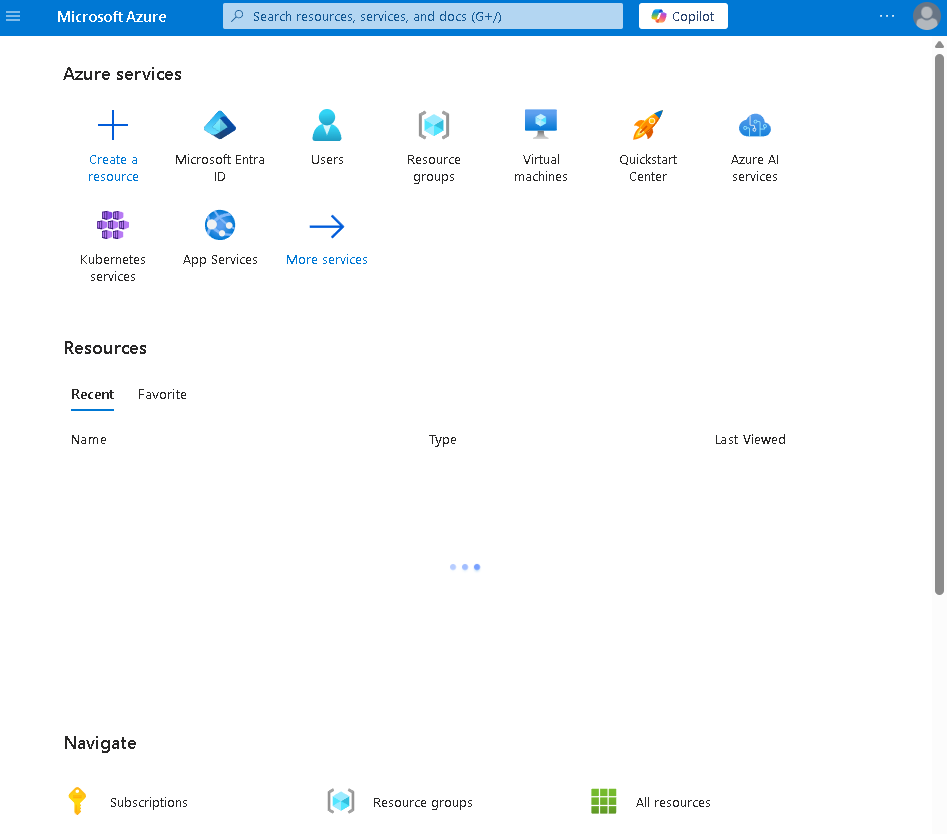
# Lab 02a - Manage Subscriptions and RBAC

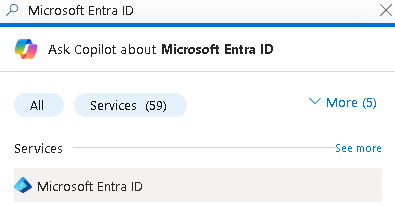
Made by Valeriy Manuilyk <3

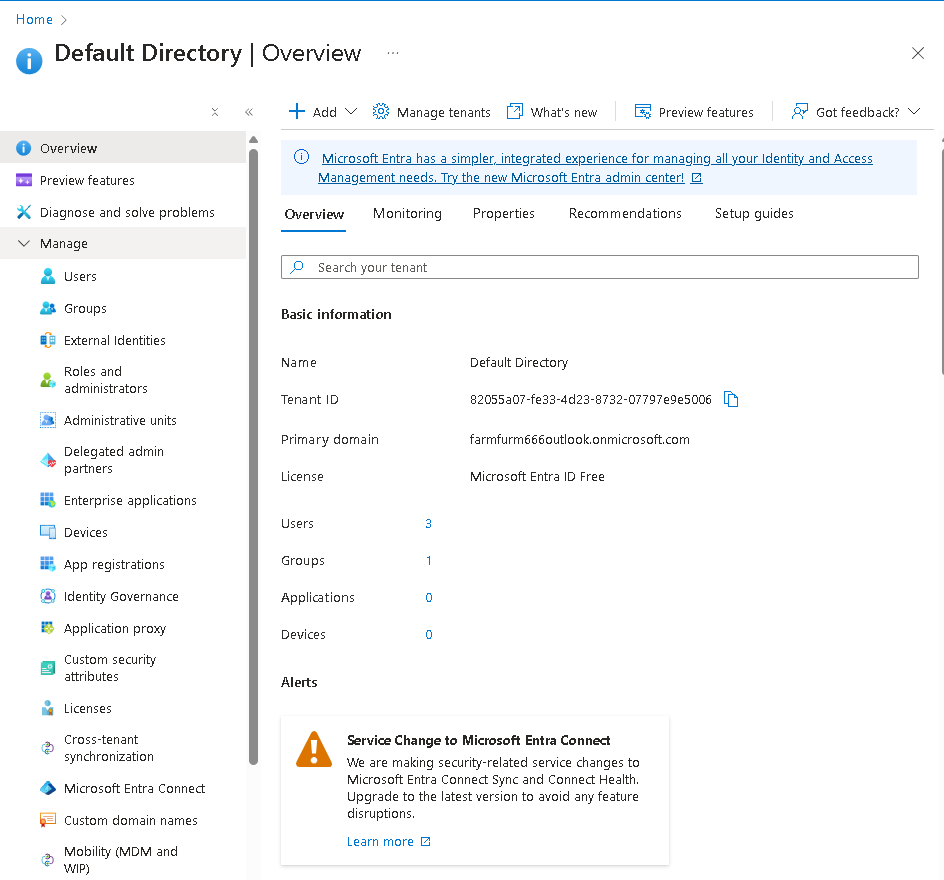
## Task 1: Implement Management Groups

1. Sign in to the ****Azure portal**** - <https://portal.azure.com.>



1. Search for and select Microsoft Entra ID.



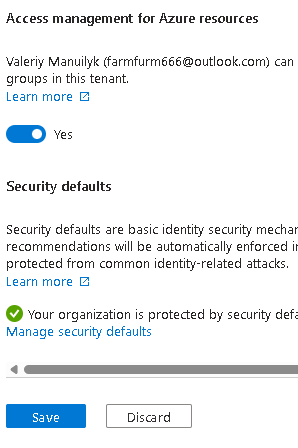


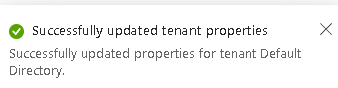
3.In the ****Manage**** blade, select ****Properties****.



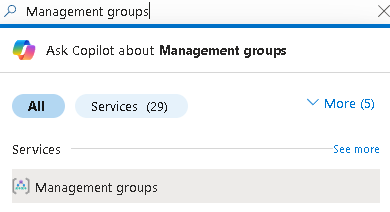


4.Review the ****Access management for Azure resources**** area. Ensure you can manage access to all Azure subscriptions and management groups in the tenant.

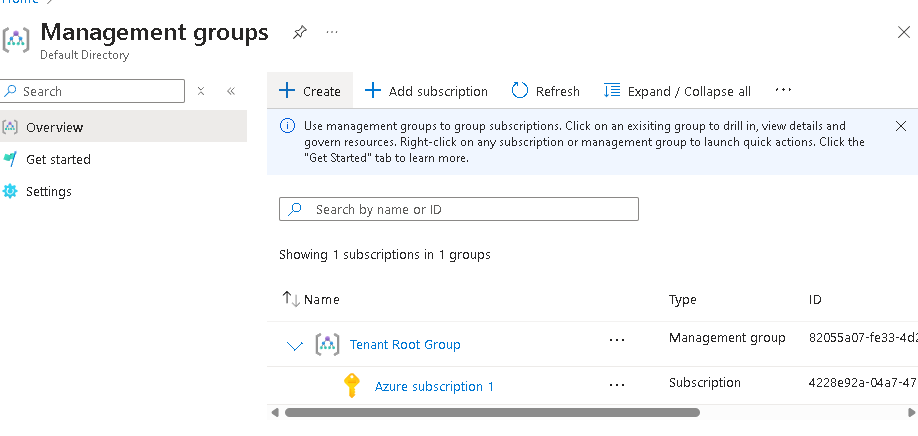




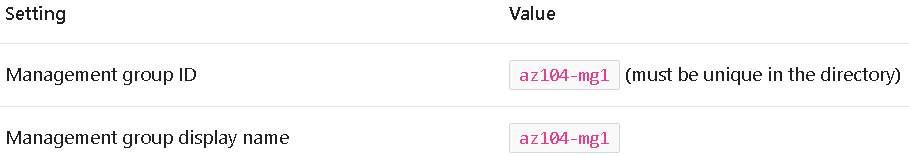
5.Search for and select Management groups.

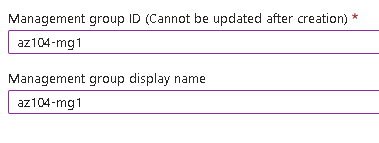


1. On the ****Management groups**** blade, click ****+ Create****.



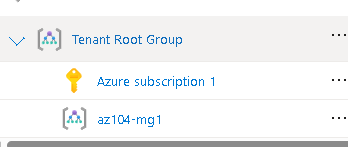
7.Create a management group with the following settings. Select ****Submit**** when you are done.





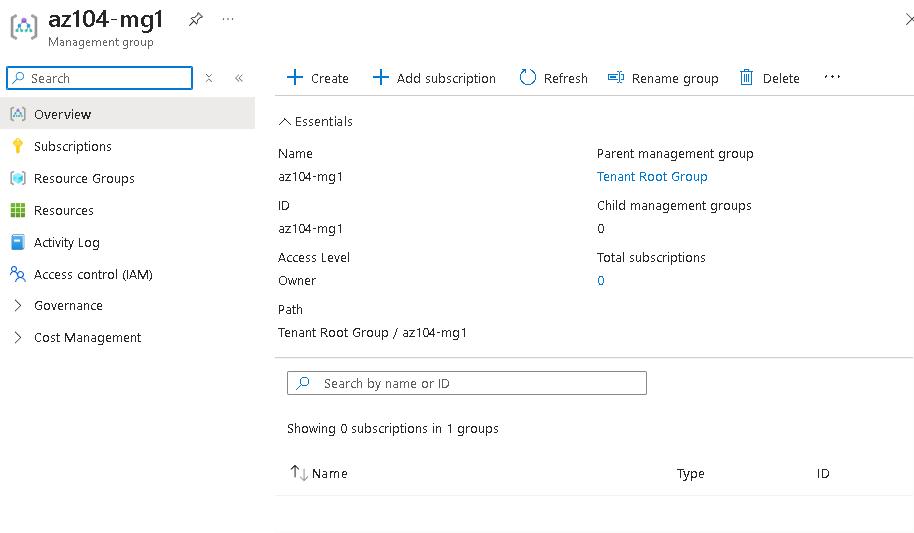


1. ****Refresh**** the management group page to ensure your new management group displays. This may take a minute.

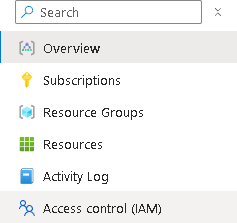


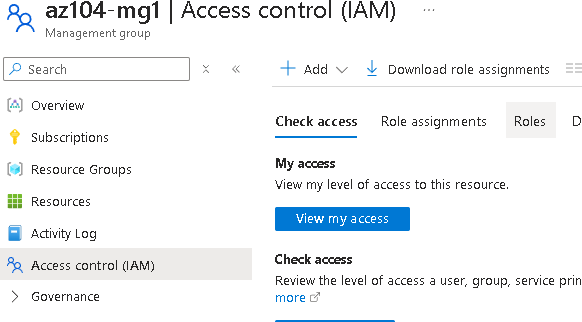
## Task 2: Review and assign a built-in Azure role

1. Select the ****az104-mg1**** management group.

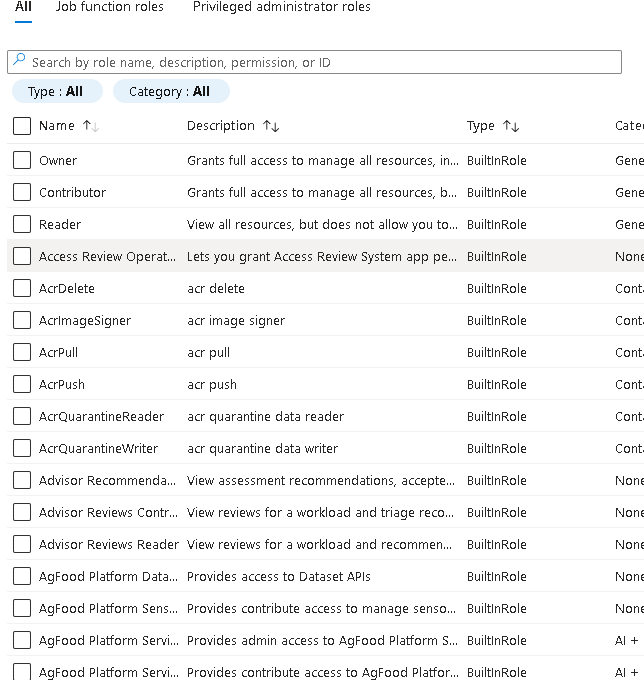


2.Select the ****Access control (IAM)**** blade, and then the ****Roles**** tab.

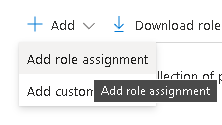




3.Scroll through the built-in role definitions that are available. ****View**** a role to get detailed information about the ****Permissions****, ****JSON****, and ****Assignments****. You will often use owner, contributor, and reader.



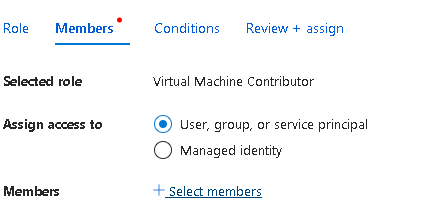
4.Select ****+ Add****, from the drop-down menu, select ****Add role assignment****.



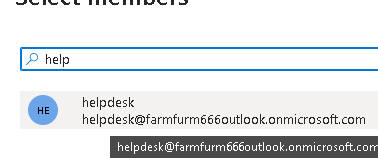
5.On the ****Add role assignment**** blade, search for and select the ****Virtual Machine Contributor****. The Virtual machine contributor role lets you manage virtual machines, but not access their operating system or manage the virtual network and storage account they are connected to. This is a good role for the Help Desk. Select ****Next****.



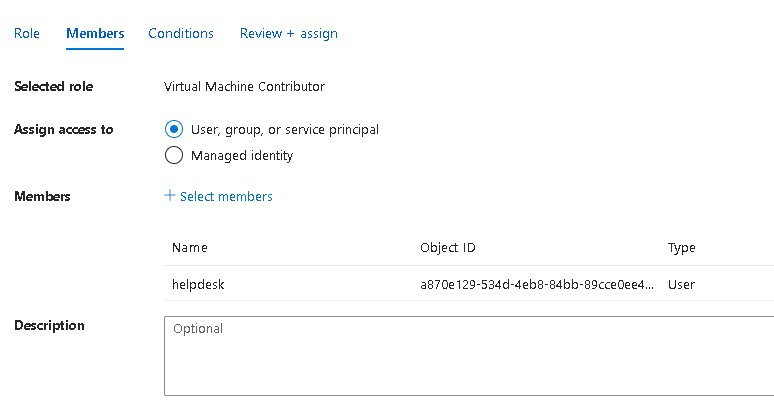
6.On the ****Members**** tab, ****Select Members****.



7.Search for and select the helpdesk group. Click ****Select****.



1. Click ****Review + assign**** twice to create the role assignment.



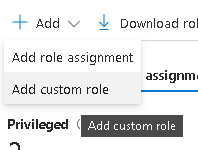
9.Continue on the ****Access control (IAM)**** blade. On the ****Role assignments**** tab, confirm the ****helpdesk**** group has the ****Virtual Machine Contributor**** role.



## Task 3: Create a custom RBAC role

1.Continue working on your management group. Navigate to the ****Access control (IAM)**** blade.

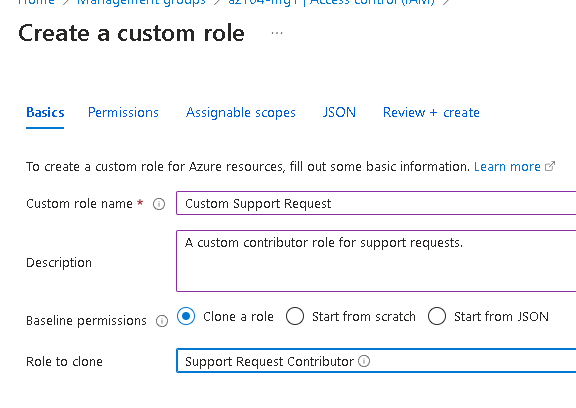
2.Select ****+ Add****, from the drop-down menu, select ****Add custom role****.



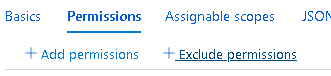
3.On the Basics tab complete the configuration.



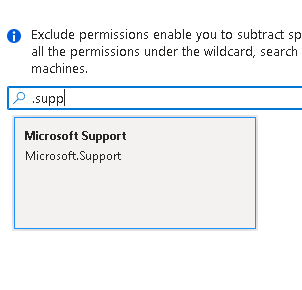
4.For ****Baseline permissions****, select ****Clone a role****. In the ****Role to clone**** drop-down menu, select ****Support Request Contributor****.



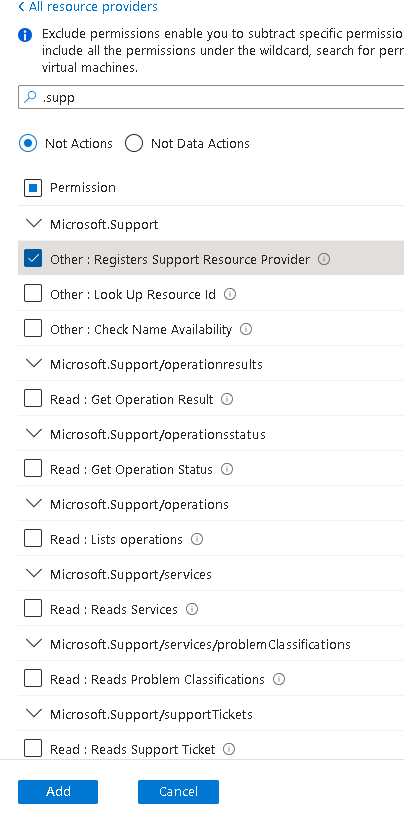
5.Select ****Next**** to move to the ****Permissions**** tab, and then select ****+ Exclude permissions****.



6.In the resource provider search field, enter .Support and select ****Microsoft.Support****.

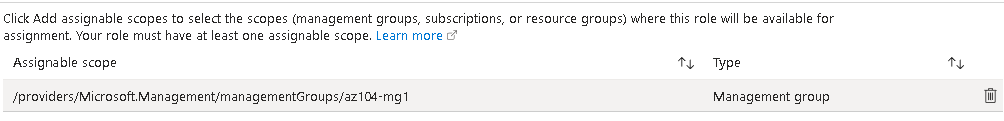


7.In the list of permissions, place a checkbox next to ****Other: Registers Support Resource Provider**** and then select ****Add****. The role should be updated to include this permission as a NotAction.



8.On the ****Assignable scopes**** tab, ensure your management group is listed, then click ****Next****.

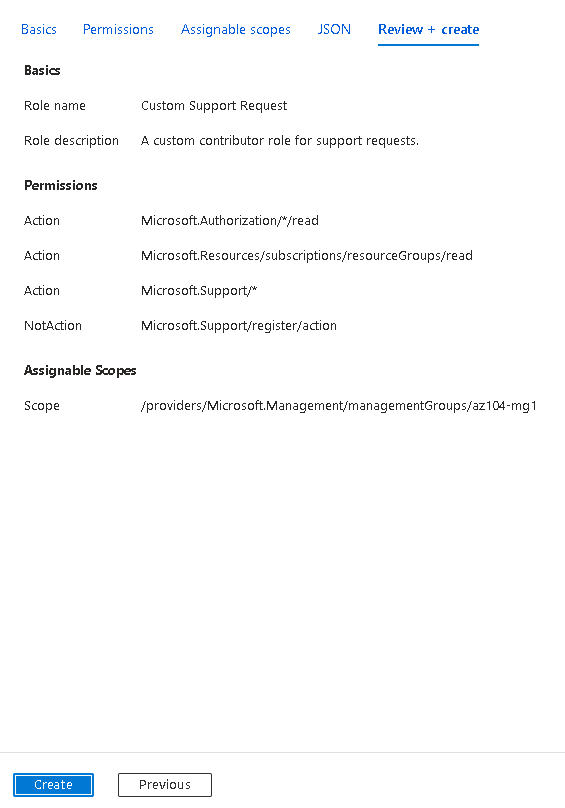


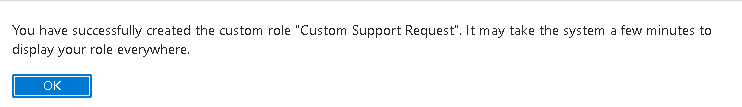


9.Review the JSON for the Actions, NotActions, and AssignableScopes that are customized in the role.



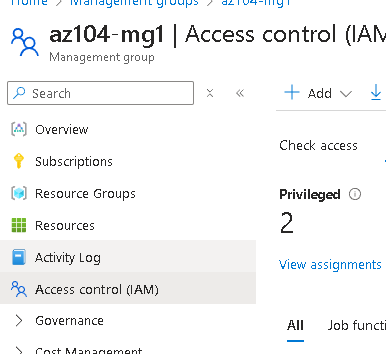
1. Select ****Review + Create****, and then select ****Create****.



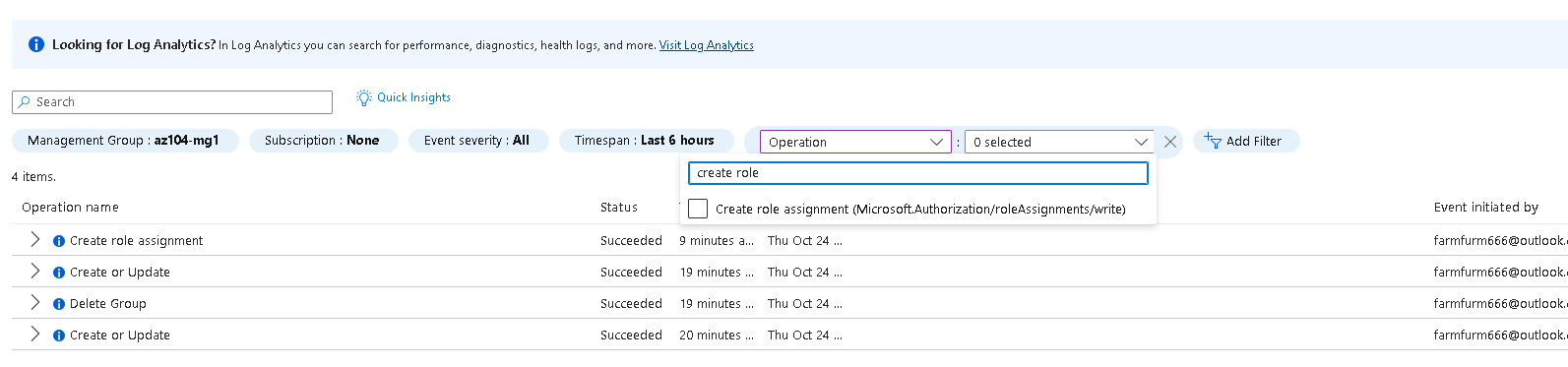


## Task 4: Monitor role assignments with the Activity Log

1. In the portal locate the ****az104-mg1**** resource and select ****Activity log****. The activity log provides insight into subscription-level events.



2.Review the activites for role assignments. The activity log can be filtered for specific operations.



**Conclusions:**

Management groups are used to logically organize subscriptions.

The built-in root management group includes all the management groups and subscriptions.

Azure has many built-in roles. You can assign these roles to control access to resources.

You can create new roles or customize existing roles.

Roles are defined in a JSON formatted file and include Actions, NotActions, and AssignableScopes.

You can use the Activity Log to monitor role assignments.