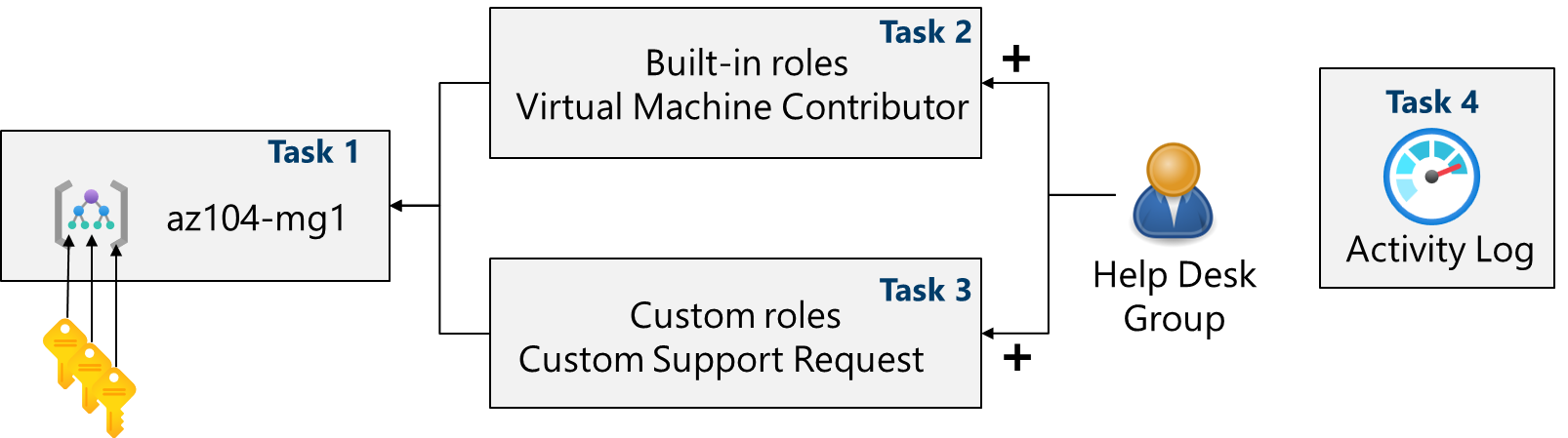
***Manage Subscriptions and RBAC***

**Architecture diagram**



🧠 Lab Summary

This lab focuses on implementing role-based access control (RBAC) and subscription management in Azure. It includes creating management groups, assigning built-in and custom roles, and monitoring role assignments using the Activity Log.

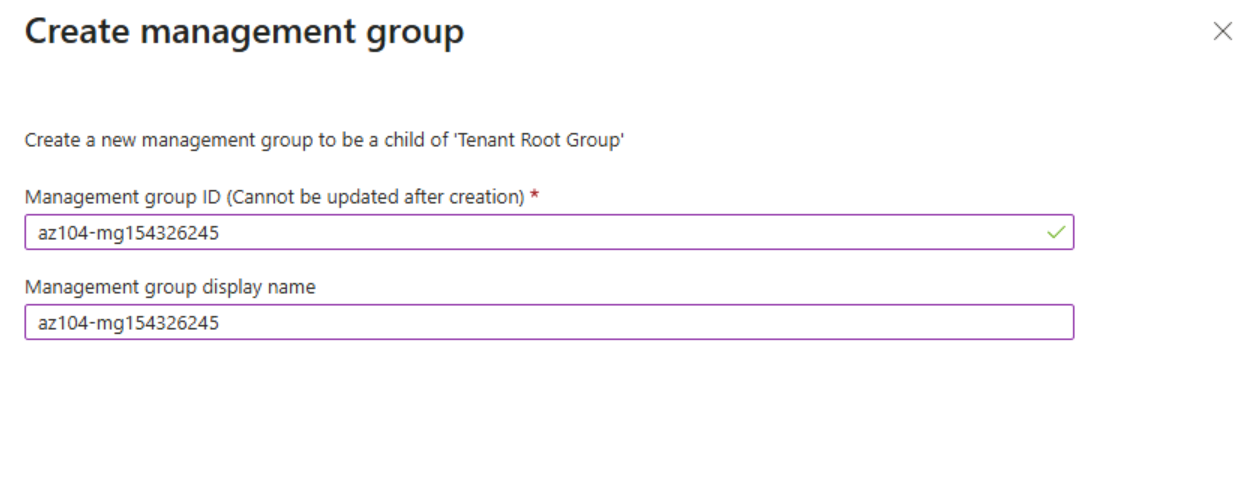
🧩 Task 1: Implement Management Groups

**Objective**  
Create and configure a management group to organize Azure subscriptions and enable centralized RBAC.

**Steps Taken**

* Signed into Azure Portal
* Verified access permissions via Microsoft Entra ID
* Created management group az104-mg1
* Confirmed visibility of root management group

**Screenshot(s)**  
*Figure 1: Management group creation*  
1.Created a management group



**Notes**  
The root management group allows global policy and role assignments across the directory.

🧩 Task 2: Review and Assign a Built-in Azure Role

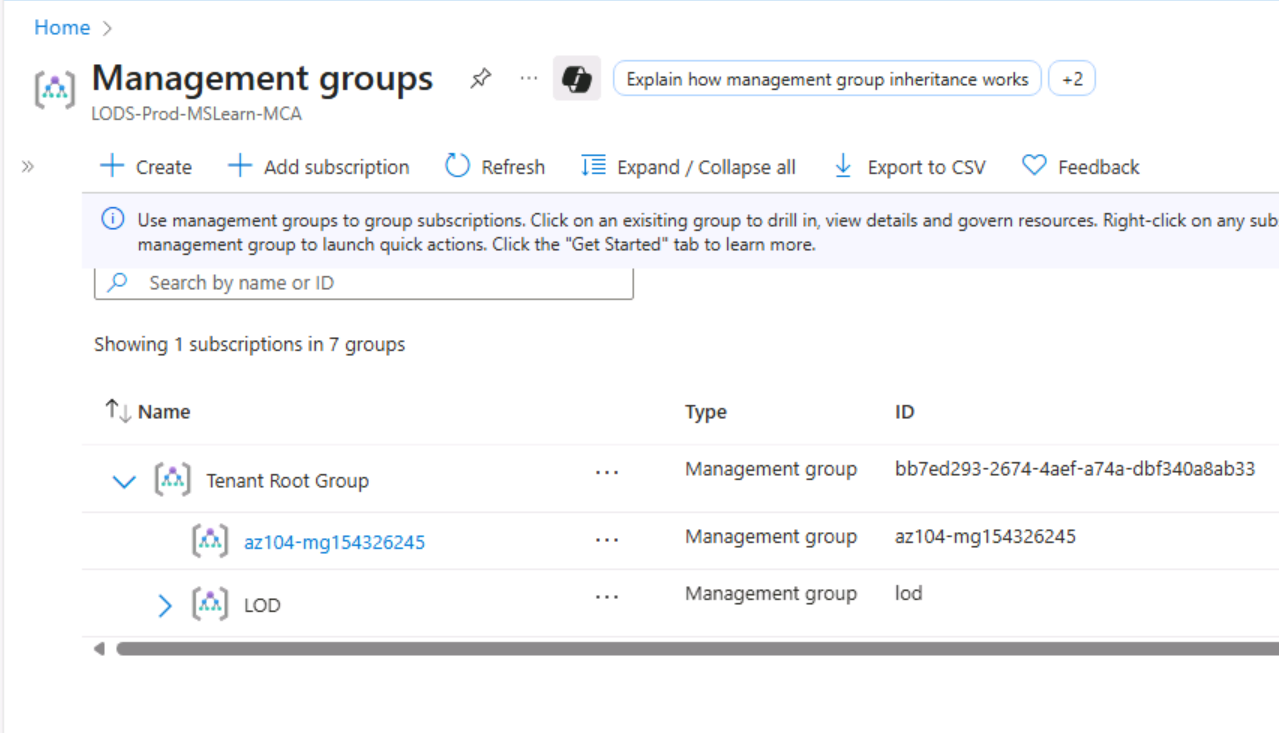
**Objective**  
Assign the Virtual Machine Contributor role to the Help Desk group at the management group level.

**Steps Taken**

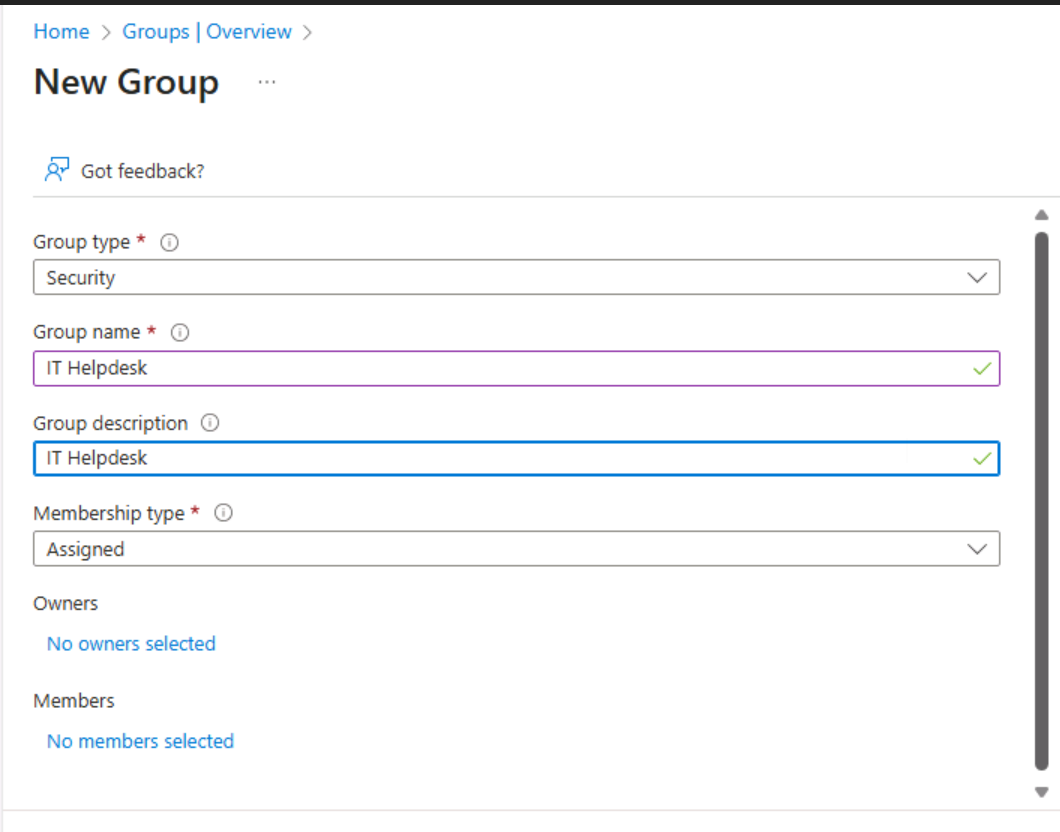
* Navigated to az104-mg1 > Access control (IAM)
* Selected and reviewed built-in roles
* Assigned VM Contributor role to Help Desk group
* Verified role assignment

**Screenshot(s)**  
*Role assignment confirmation*

1.  The root management group is built into the hierarchy to have all management groups and subscriptions fold up to it. This root management group allows for global policies and Azure role assignments to be applied at the directory level.

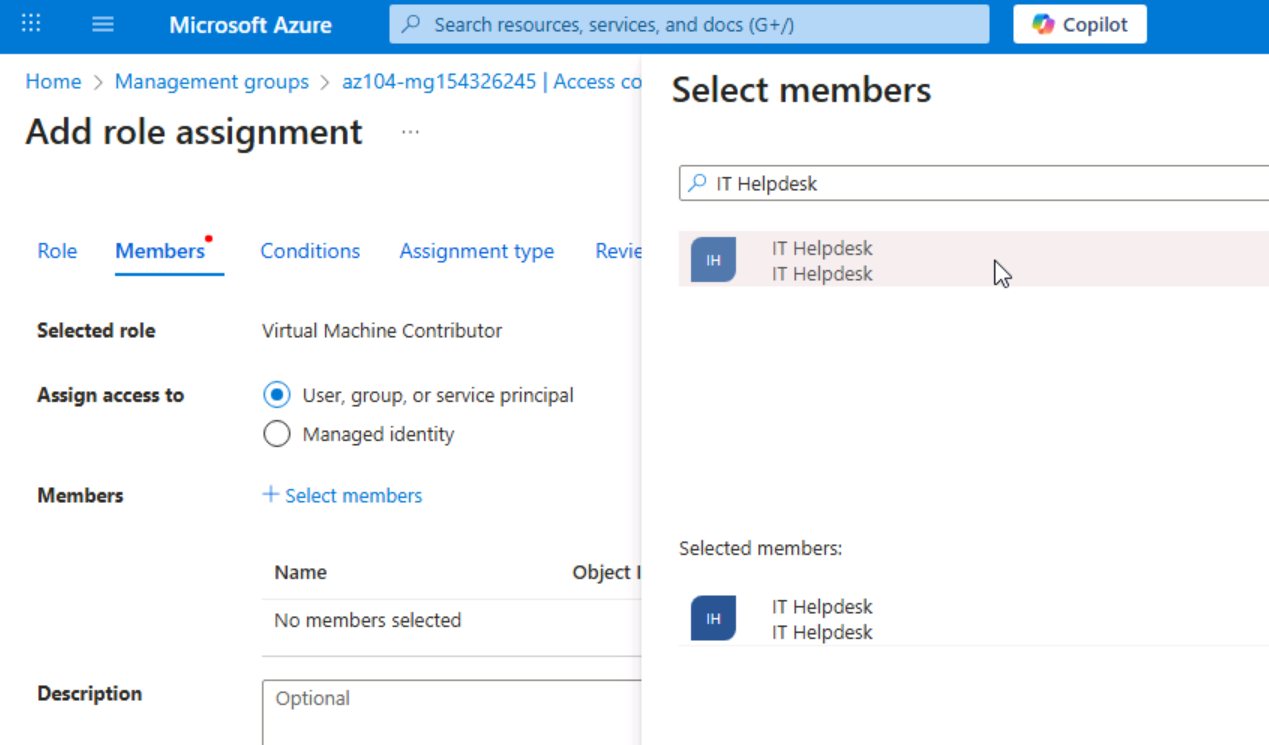


2. Created the ip helpdesk group

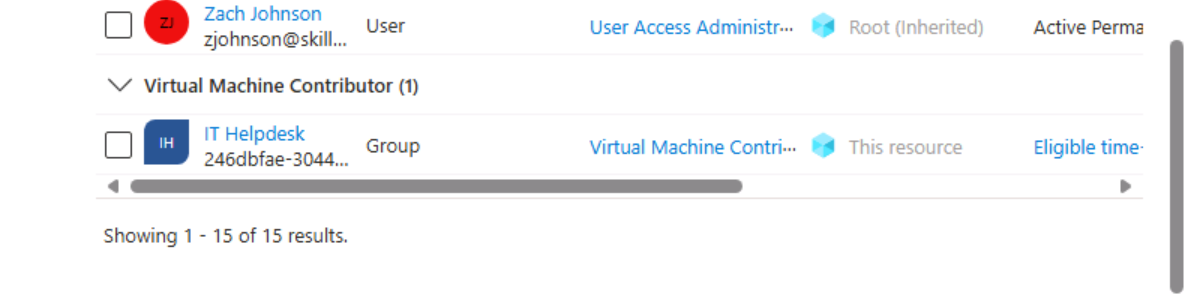
****

**Notes**  
Roles should be assigned to groups, not individuals, for better scalability and governance.

3. Adding the role assignment to the group



4. Confirmation that IT helpdesk has the virtual machine contributor role



🧩 Task 3: Create a Custom RBAC Role

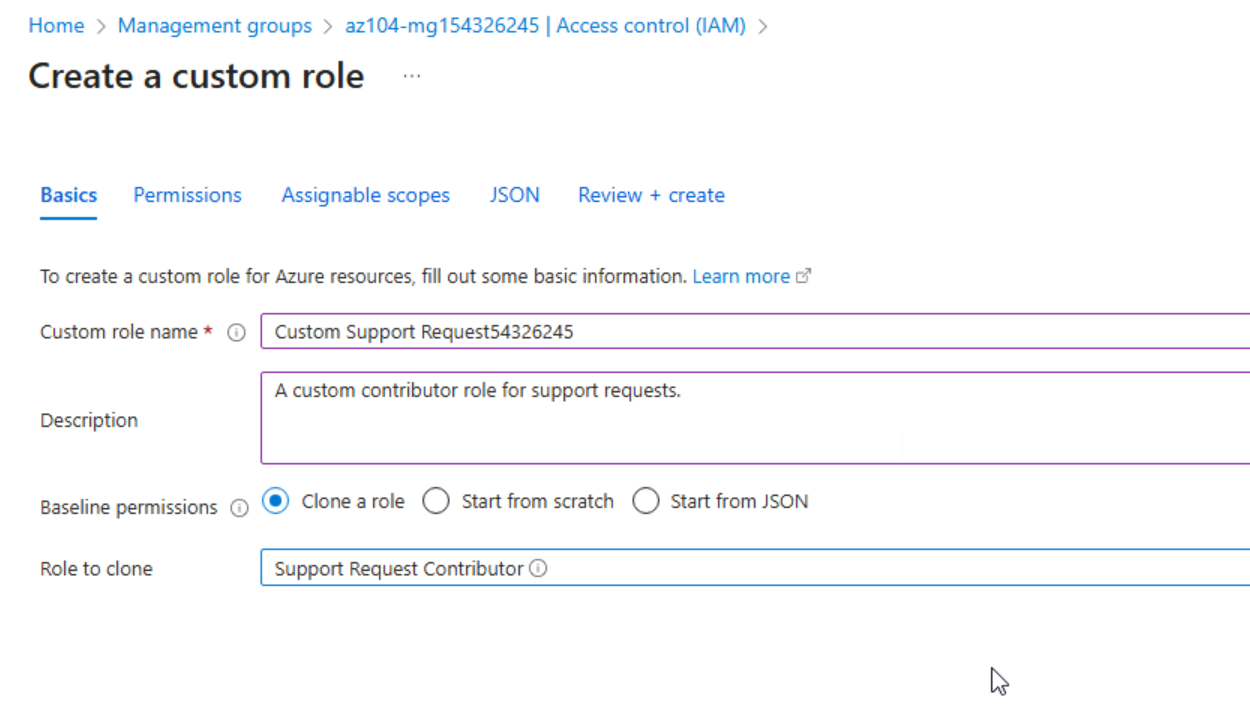
**Objective**  
Design a custom role that allows support ticket creation but excludes provider registration.

**Steps Taken**

* Cloned Support Request Contributor role
* Excluded Microsoft.Support/register/action permission
* Scoped role to az104-mg1
* Reviewed and created custom role

**Screenshot(s)**

1. creating a custom RBAC role by cloning the support request contributor role



**2.**

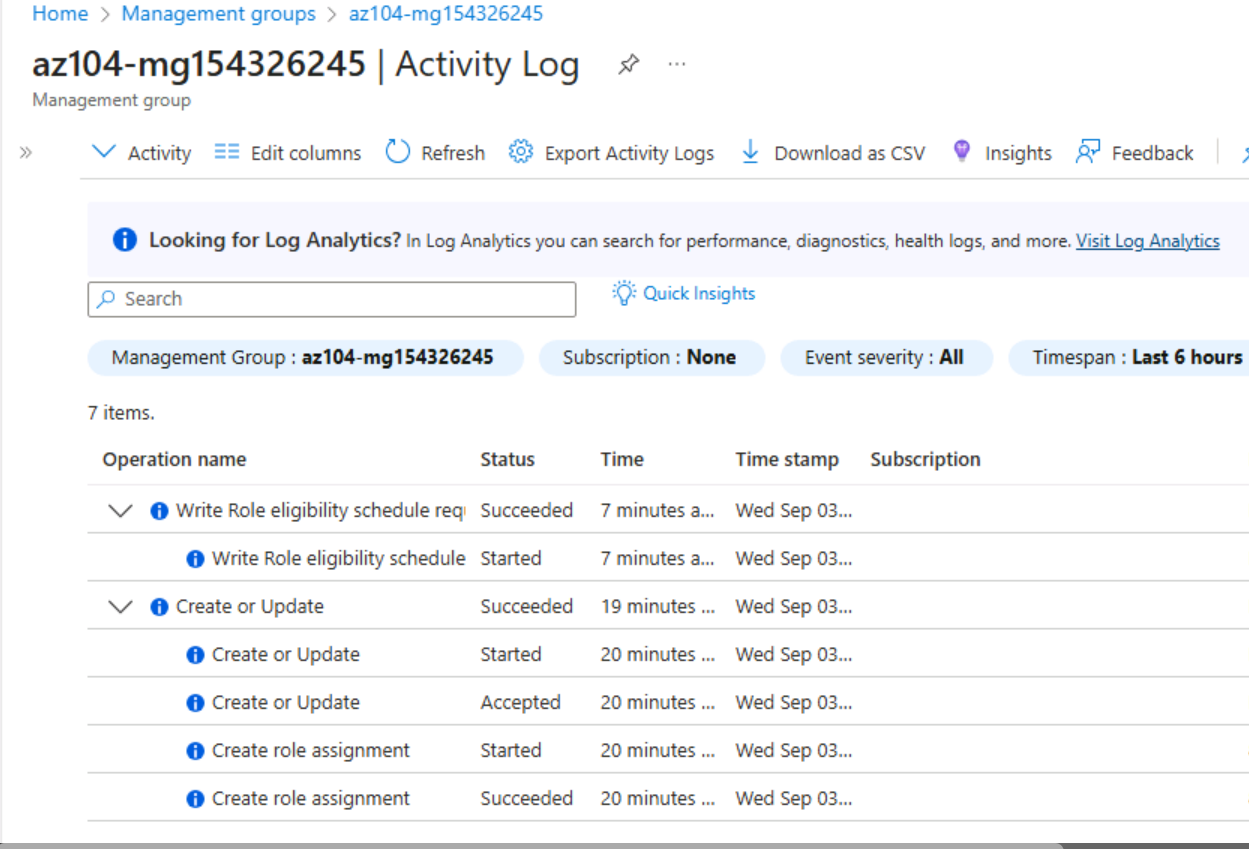
**Notes**  
This enforces least privilege by removing unnecessary permissions from the Help Desk role.

🧩 Task 4: Monitor Role Assignments with the Activity Log

**Objective**  
Use the Activity Log to track role assignment events.

**Steps Taken**

* Opened Activity Log for az104-mg1
* Filtered for role assignment operations
* Reviewed recent changes

**Screenshot(s)**  
*1. Activity log filtered view*  


**Notes**  
The Activity Log provides visibility into permission changes and governance actions.

✅ Final Reflection

This lab reinforced the importance of structured access control in Azure. Creating a custom RBAC role helped me apply the principle of least privilege, while management groups simplified subscription-level governance. Monitoring via the Activity Log added an extra layer of accountability. In future implementations, I’d explore automating role assignments using Azure CLI or Bicep templates.