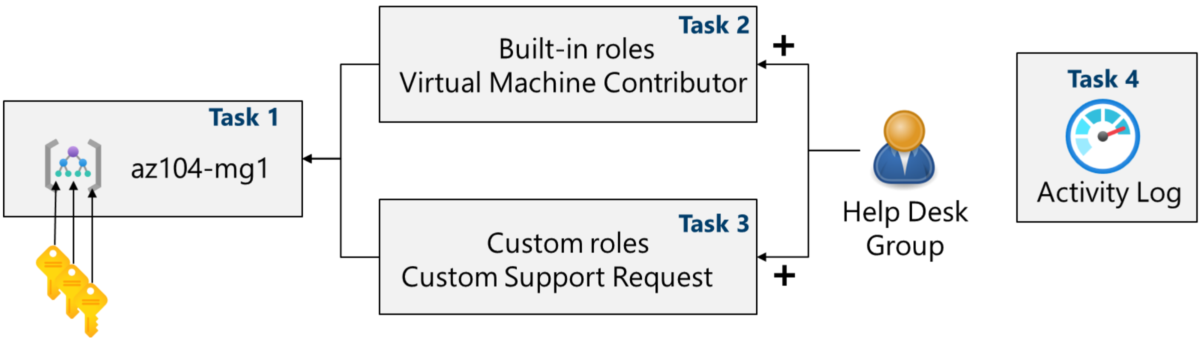
Manage Subscriptions and RBAC

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.

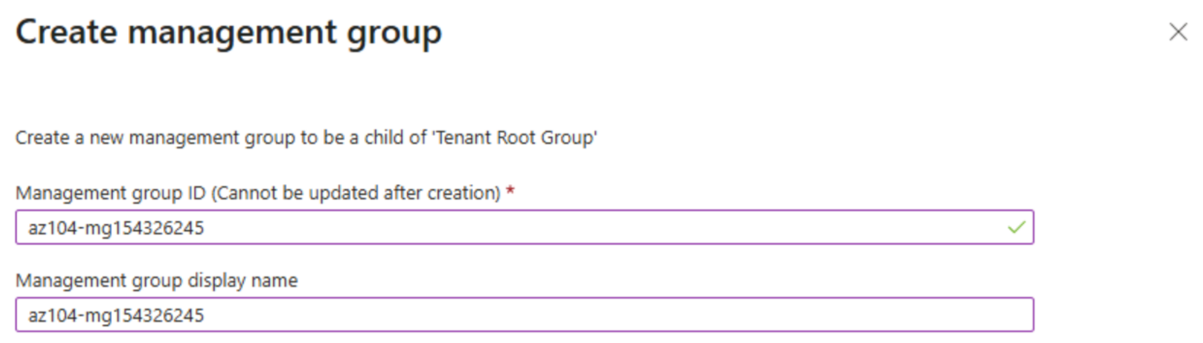
Task 1: Implement Management Groups

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



Create management group

Create a new management group to be a child of 'Tenant Root Group'

Management group ID (Cannot be updated after creation) *

az104-mg154326245

Management group display name

az104-mg154326245

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

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

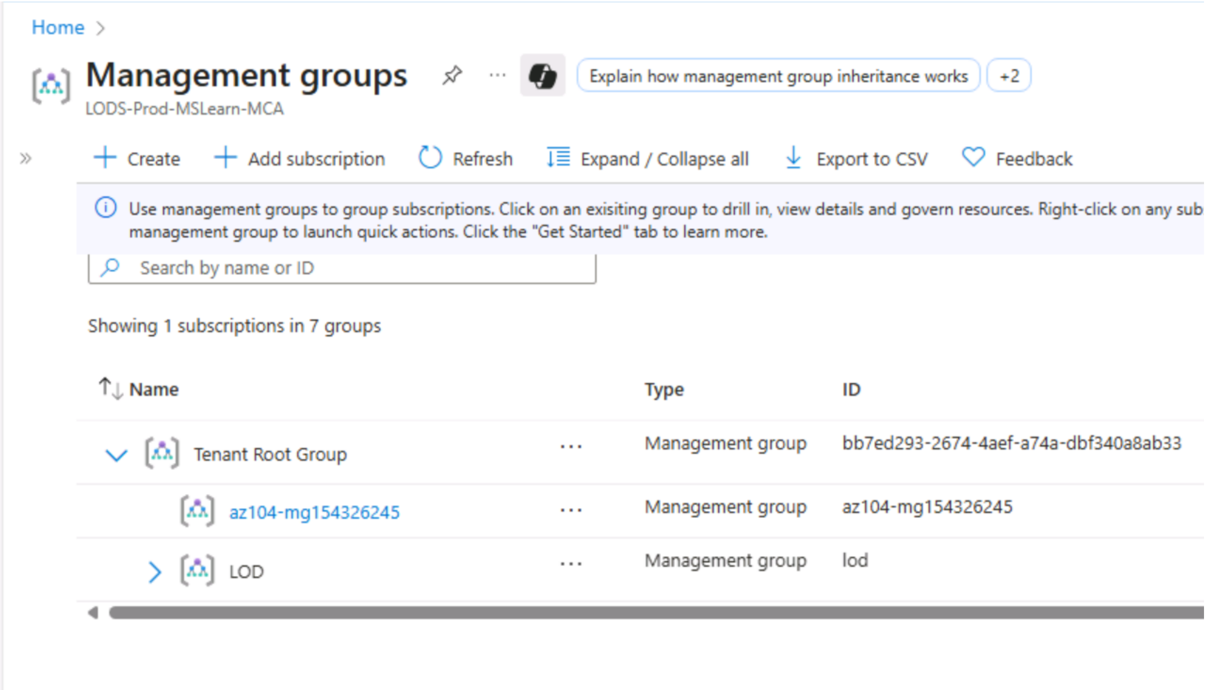
Objective
Assign the Virtual Machine Contributor role to the Help Desk group at the management group level.

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.



Management groups

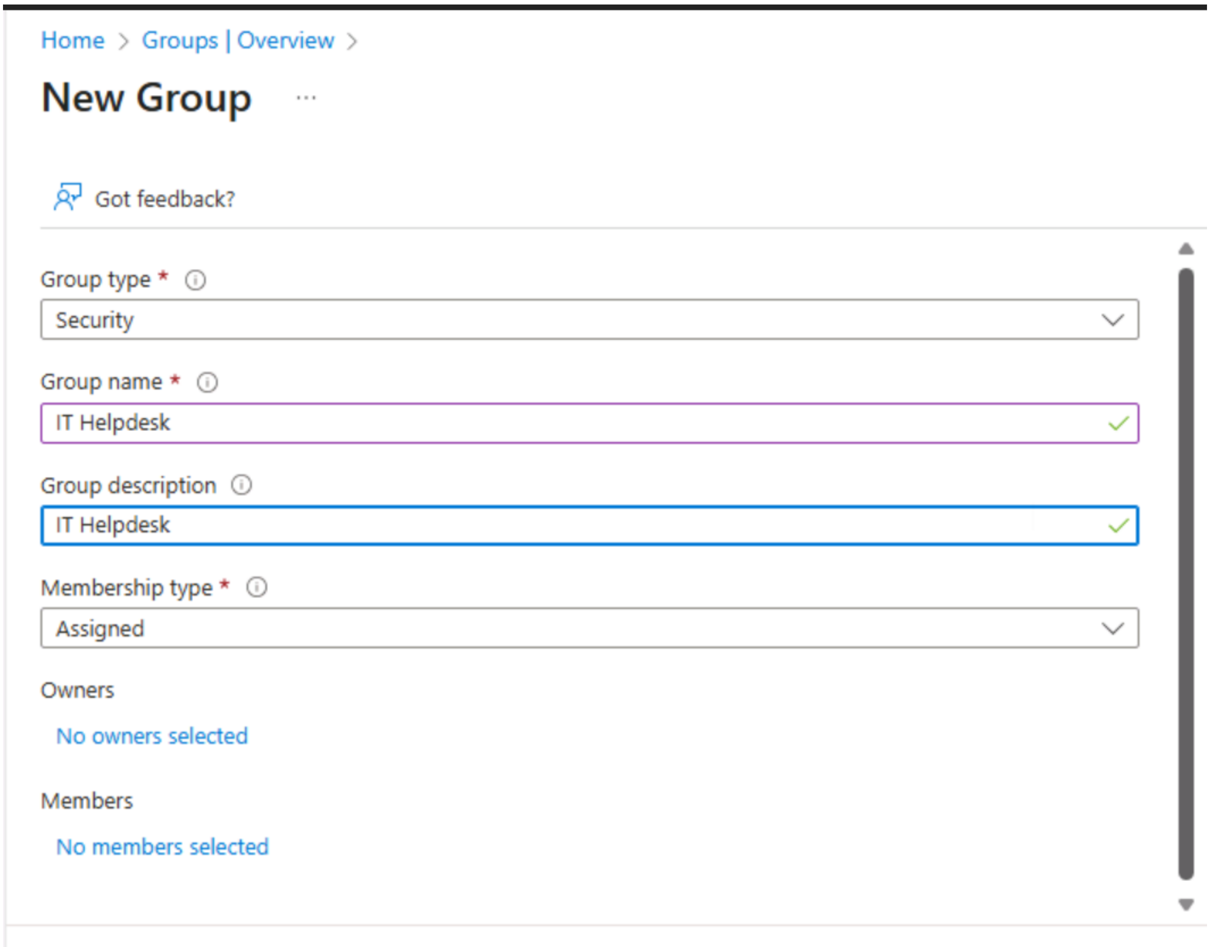
LODS-Prod-MSLearn-MCA

Use management groups to group subscriptions. Click on an exisiting group to drill in, view details and govern resources. Right-click on any sub management group to launch quick actions. Click the "Get Started" tab to learn more.

Showing 1 subscriptions in 7 groups

Name		Type	ID
Tenant Root Group	···	Management group	bb7ed293-2674-4aef-a74a-dbf340a8ab33
az104-mg154326245	···	Management group	az104-mg154326245
LOD	···	Management group	lod

2. Created the ip helpdesk group



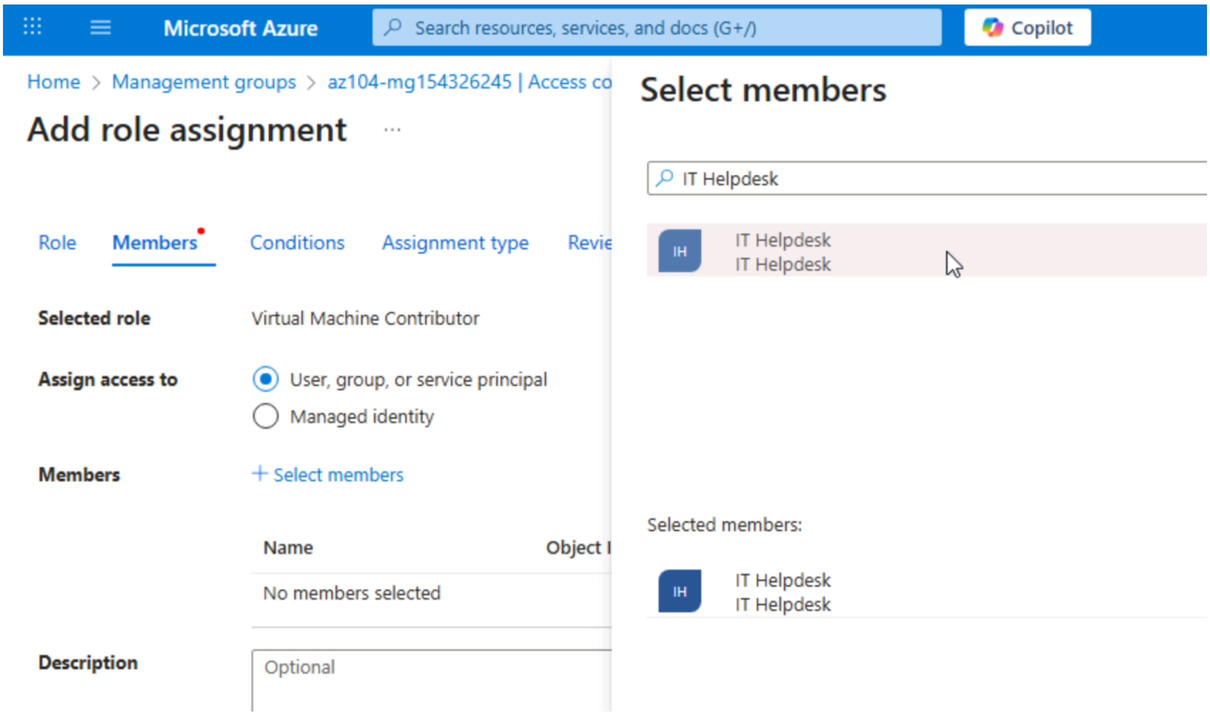
New Group

Group type *	Security
Group name *	IT Helpdesk
Group description	IT Helpdesk
Membership type *	Assigned
Owners	No owners selected
Members	No members selected

Notes

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

3. Adding the role assignment to the group


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Management groups > az104-mg154326245 | Access co
Role
Members
Conditions
Assignment type
Revie
+ Select members
Select members
IH

Add role assignment

Selected role: Virtual Machine Contributor

Assign access to: ● User, group, or service principal ○ Managed identity

Members

Name	Object I
No members selected	

Description: Optional

Select members

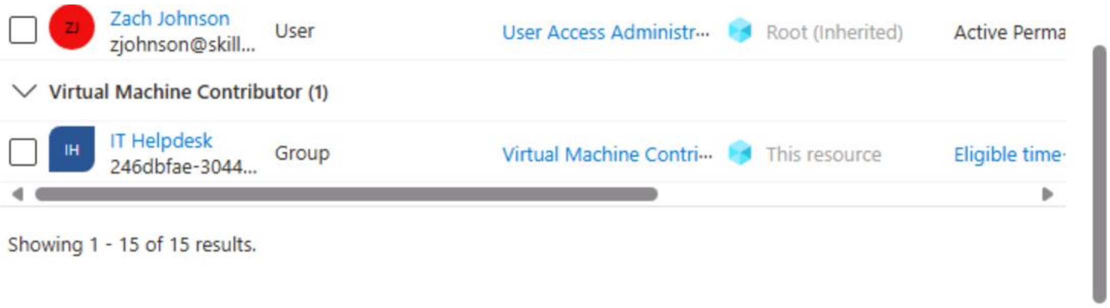
IT Helpdesk

IT Helpdesk
IT Helpdesk

Selected members:

IT Helpdesk
IT Helpdesk

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



□	Zach Johnson zjohnson@skill...	User	User Access Administr...	Root (Inherited)	Active Perma
Virtual Machine Contributor (1)					
□	IT Helpdesk 246dbfae-3044...	Group	Virtual Machine Contri...	This resource	Eligible time

Showing 1 - 15 of 15 results.

Task 3: Create a Custom RBAC Role

Objective

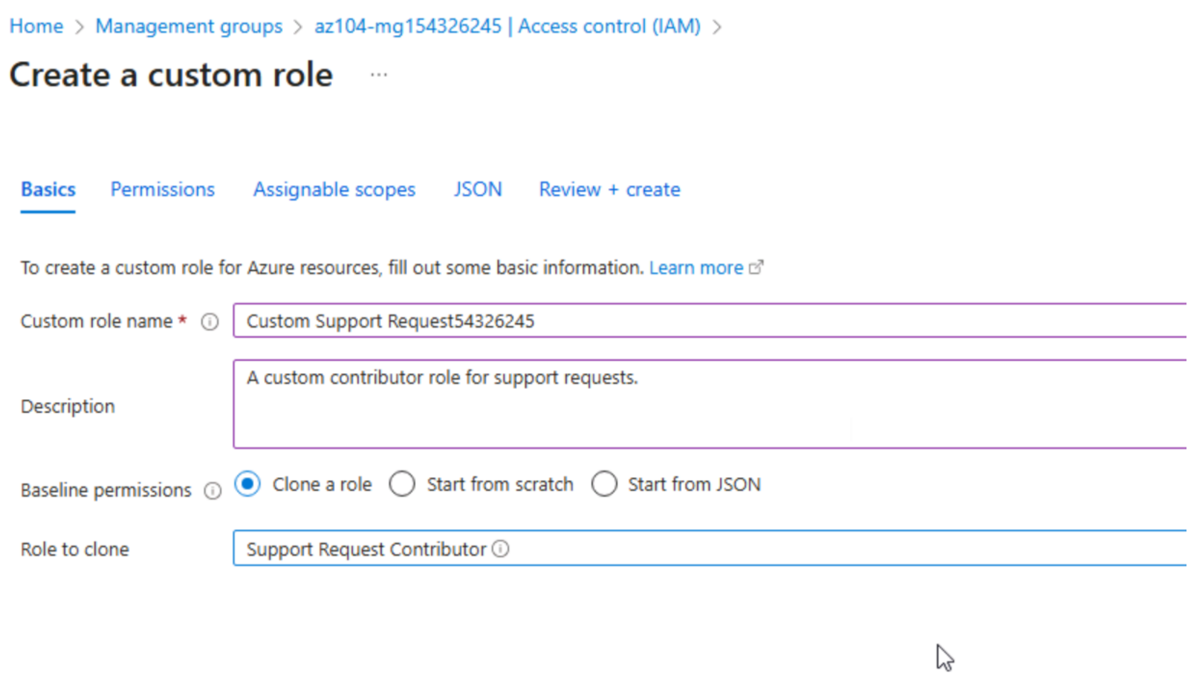
Design a custom role that allows support ticket creation but excludes provider registration.

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



Home > Management groups > az104-mg154326245 | Access control (IAM) >

Create a custom role ...

Basics
Permissions
Assignable scopes
JSON
Review + create

To create a custom role for Azure resources, fill out some basic information. Learn more

Custom role name * : Custom Support Request54326245

Description: A custom contributor role for support requests.

Baseline permissions: ● Clone a role ○ Start from scratch ○ Start from JSON

Role to clone: Support Request Contributor

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

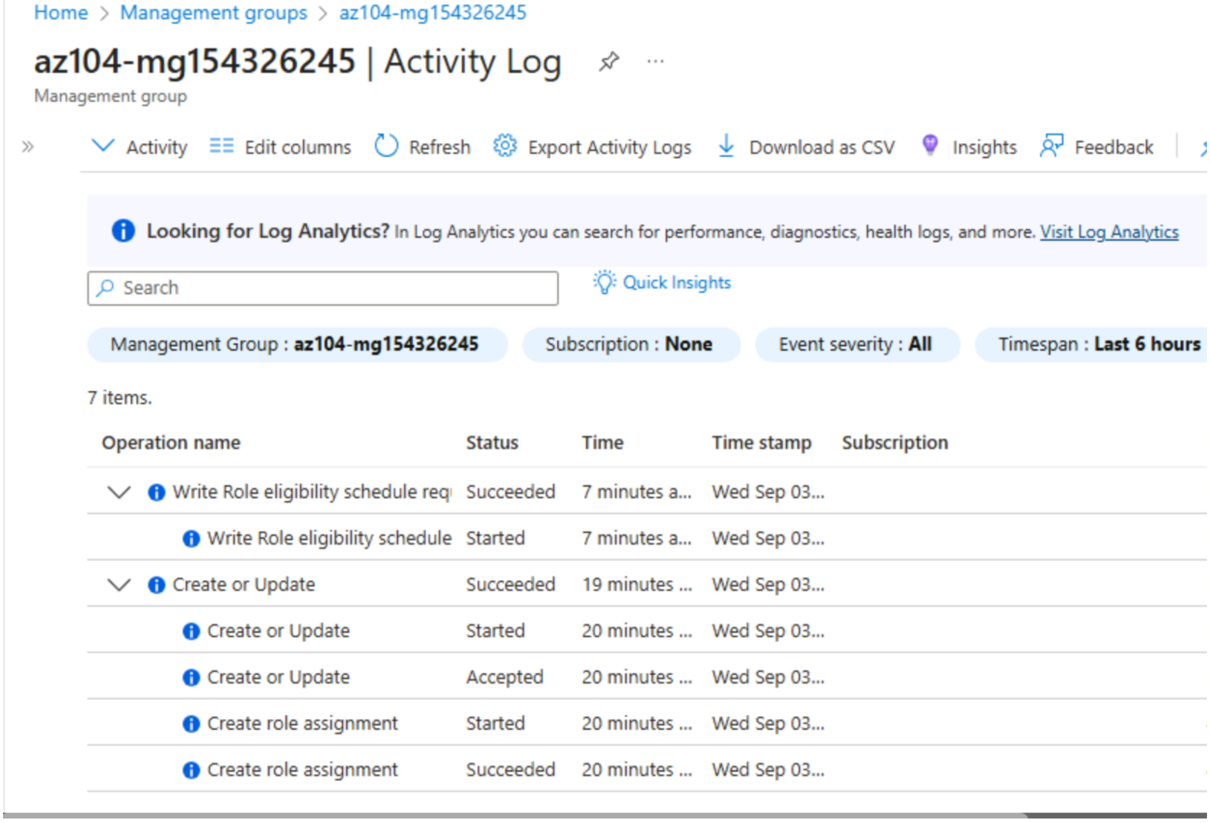
Use the Activity Log to track role assignment events.

Steps Taken

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

Screenshot(s)

1. *Activity log filtered view*



az104-mg154326245 | Activity Log

Management group

Looking for Log Analytics? In Log Analytics you can search for performance, diagnostics, health logs, and more. Visit Log Analytics

Management Group : **az104-mg154326245** Subscription : **None** Event severity : **All** Timespan : **Last 6 hours**

7 items.

Operation name	Status	Time	Time stamp	Subscription
Write Role eligibility schedule req	Succeeded	7 minutes a...	Wed Sep 03...	
Write Role eligibility schedule	Started	7 minutes a...	Wed Sep 03...	
Create or Update	Succeeded	19 minutes ...	Wed Sep 03...	
Create or Update	Started	20 minutes ...	Wed Sep 03...	
Create or Update	Accepted	20 minutes ...	Wed Sep 03...	
Create role assignment	Started	20 minutes ...	Wed Sep 03...	
Create role assignment	Succeeded	20 minutes ...	Wed Sep 03...	

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.