LAB BY THATO KGOLE

DATE : 23 NOVEMBER 2025

DURATION : 35 MINUTES

CLOUD PLATFORM : MICROSOFT AZURE

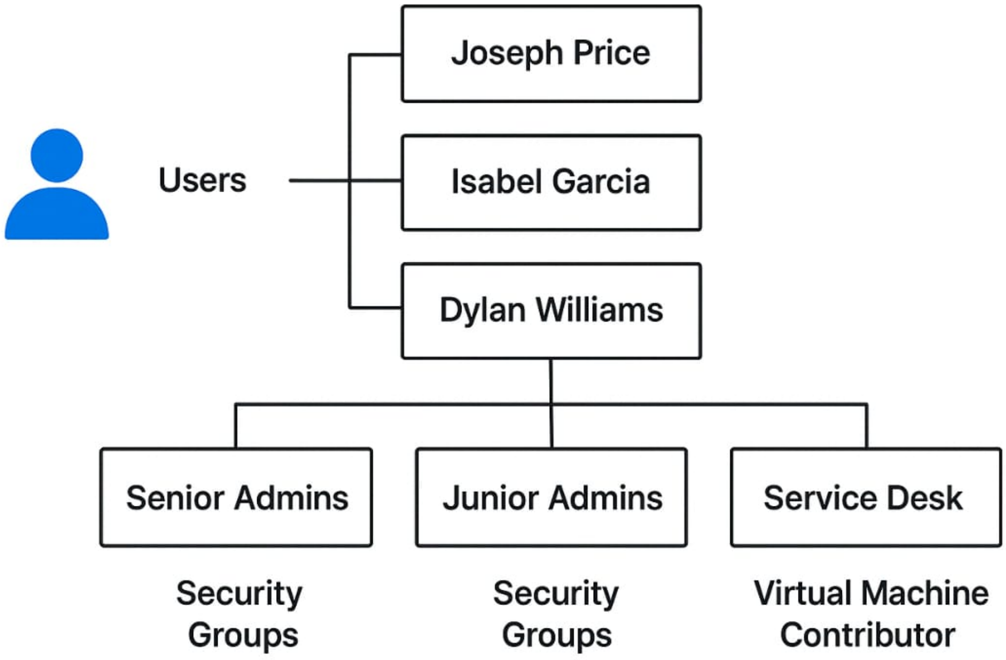
Role-Based Access Control

PROBLEM STATEMENT

An organization needs a secure and scalable method to manage access permissions for different administrative levels within Azure. Currently, access is assigned directly to individual users, increasing risk, maintenance effort, and the chance of privilege misuse.

The business wants to:
. Create a structured identity model using users and groups
. Demonstrate how Azure Role-Based Access Control can be used to assign permissions
. Ensure users receive only the access they need to perform their job(least privilege)

DIAGRAM



GOALS

Business Goals

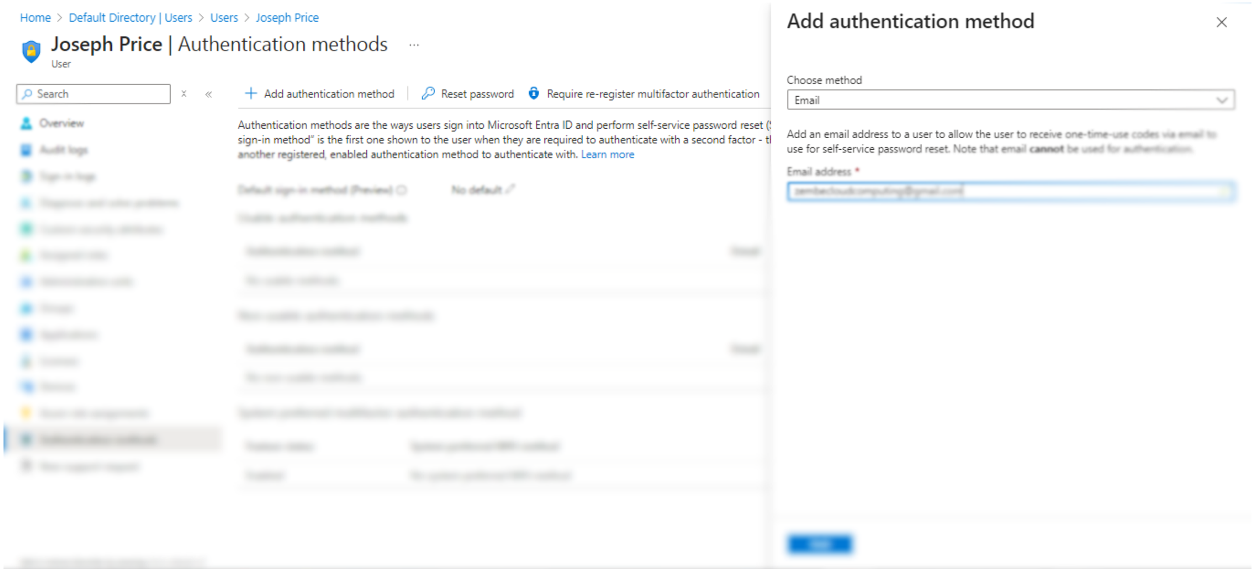
. Demonstrate proper identity hierarchy and access assignment using Azure.
. Reduce admin overhead and improve governance by using group-based access.
. Show how Service Desk, Junior Admins, and Senior Admins are separated by responsibilities.

Security Requirements

. Enforce least privilege by ensuring each group receives only the permissions required.
. Prevent individual users from receiving high-level roles directly.
. Demonstrate role inheritance and correct permission scoping.

Steps Applied

Step 1: Create Users In Entra ID
Created and Added Authentication Methods


Home > Default Directory | Users > Users > Joseph Price
Joseph Price | Authentication methods ···
User
Search
Overview
Audit logs
+ Add authentication method
Reset password
Require re-register multifactor authentication
Add authentication method
Choose method
Email

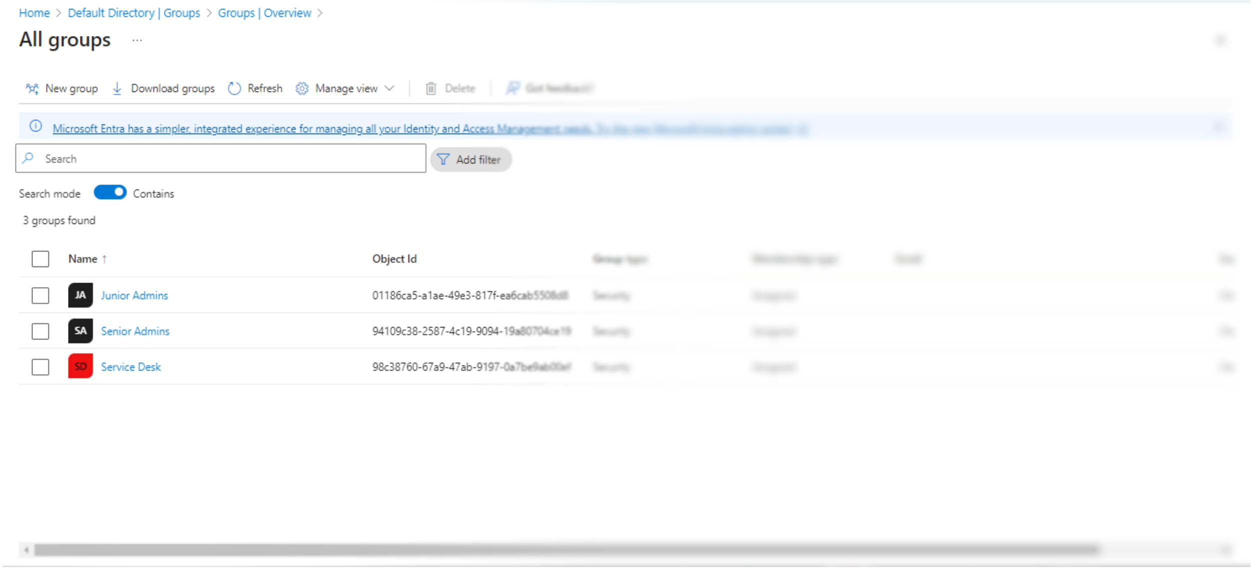
Authentication methods are the ways users sign into Microsoft Entra ID and perform self-service password reset (sign-in method" is the first one shown to the user when they are required to authenticate with a second factor - t another registered, enabled authentication method to authenticate with. Learn more

Default sign-in method (Preview) No default

Add an email address to a user to allow the user to receive one-time-use codes via email to use for self-service password reset. Note that email **cannot** be used for authentication.

Email address * [illegible]

Step 2: Create Groups and Add Users
To give permissions to them instead of individuals



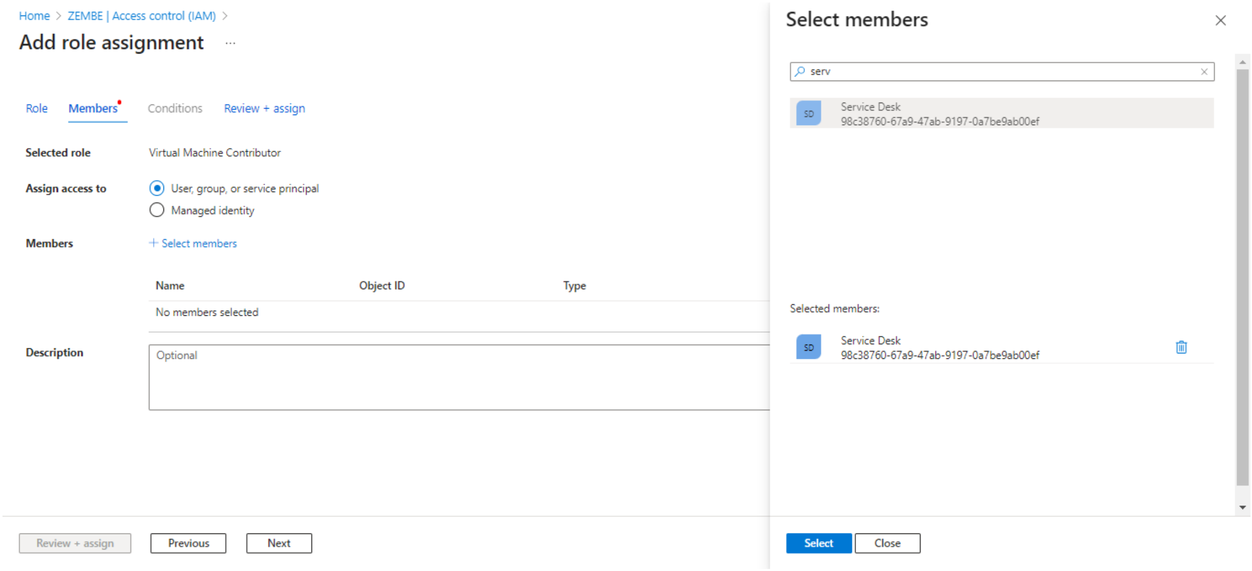
Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center.

Search mode Contains

3 groups found

□	Name ↑	Object Id	Group type	Membership type
□	JA Junior Admins	01186ca5-a1ae-49e3-817f-ea6cab5508d8	Security	Assigned
□	SA Senior Admins	94109c38-2587-4c19-9094-19a80704ce19	Security	Assigned
□	SD Service Desk	98c38760-67a9-47ab-9197-0a7be9ab00ef	Security	Assigned

Step 3: ‘Service Desk’ group
This is the group we assign VM Contributor permission to.



Home > ZEMBE | Access control (IAM) >

Add role assignment ...

Selected role: Virtual Machine Contributor

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

Members: + Select members

Name	Object ID	Type
No members selected		

Description: Optional

Select members

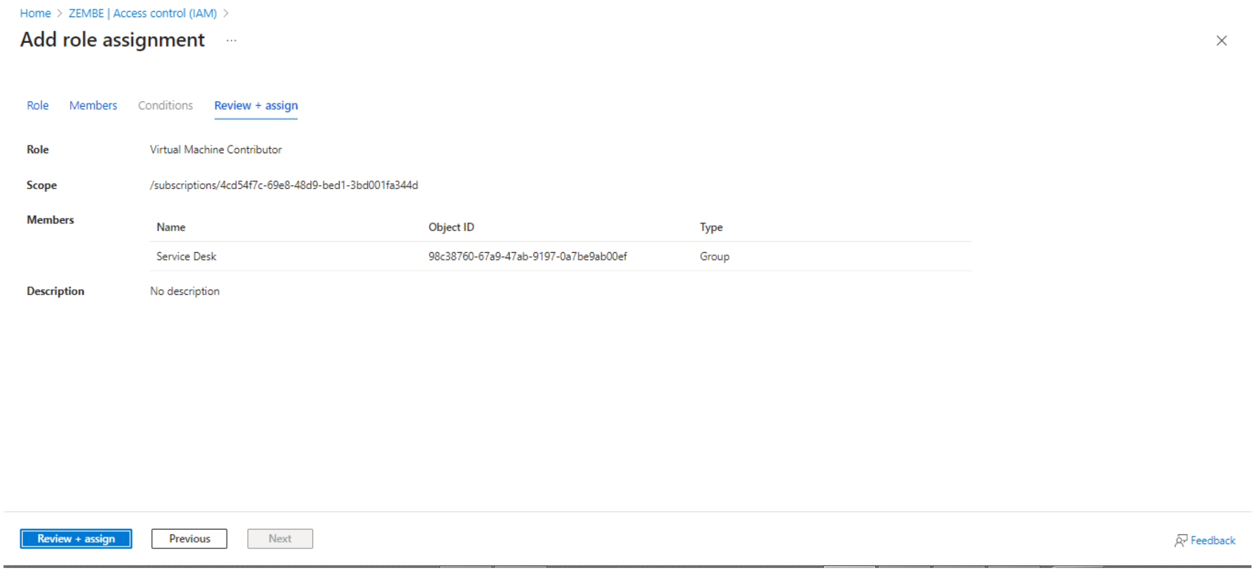
serv

Service Desk 98c38760-67a9-47ab-9197-0a7be9ab00ef

Selected members:

Service Desk 98c38760-67a9-47ab-9197-0a7be9ab00ef

Step 4: Assign “Virtual Machine Contributor” RBAC Role to service Desk Group



Home > ZEMBE | Access control (IAM) >

Add role assignment ...

Role: Virtual Machine Contributor

Scope: /subscriptions/4cd54f7c-69e8-48d9-bed1-3bd001fa344d

Members:

Name	Object ID	Type
Service Desk	98c38760-67a9-47ab-9197-0a7be9ab00ef	Group

Description: No description

Step 5: Testing (Documented)

This part demonstrates that the Service Desk group, containing Dylan Williams, only has the permissions granted by the Virtual Machine Contributor role and no additional privileges.

. Go to your Subscription account

. Open IAM

. Check Access >> In the search bar, type Dylan Williams.

> Expected Results <

> Virtual Machine Contributor (assigned via Service Desk group)

> Scope: Subscription level

{This confirms the role assignment is working and inherited through the group, not assigned directly to the user-demonstrating proper RBAC usage}

Step 5.1 Validate what the Service Desk Group Can Do

. Start, stop and reset virtual machines

. View VM configurations and metrics

. Modify VM size
. Access virtual machine settings
. Manage VM extensions
. Manage attached disks

Step 5.1: Validate what the Service Desk Group Cannot Do
. Cannot delete a resource group
. Cannot delete virtual machines
. Cannot assign RBAC roles
. Cannot access or modify VNETs or subnets
. Cannot modify NSGs or firewalls
. Cannot manage storage account
. Cannot manage subscription-level settings

Conclusion (Lessons Learned)

This project showed how RBAC helps a business control who can do what in Azure. By creating users, placing them into groups, and assigning roles to those groups, we learned that access becomes easier to manage and much safer.

We also learned that even if a group has only one member today, using groups is still the best practice because it keeps permissions organized and prepares the environment for future growth.