Azure Cloud Security Project

Project Title: Identity & Access Management with Azure RBAC

Project Author: Ezika Ifunanya

Company: FuturinCLOUD Limited

Date: February 2026

Executive Summary

This lab demonstrates secure identity and access management using Microsoft Entra ID and Azure Role-Based Access Control (RBAC) in a simulated enterprise environment for *FuturinCLOUD Limited*, a Lagos-based cloud security and infrastructure provider.

Key Outcomes:

- Created 3 enterprise users with strong password policies and forced a reset
- Established 3 departmental security groups with clear descriptions
- Assigned least-privilege RBAC role (Virtual Machine Contributor) to the support team at the resource group scope
- Used three management tools: Azure Portal, PowerShell, and Azure CLI

Business Value:

Enables scalable, governed access while adhering to zero-trust and least-privilege principles.

1. Lab Environment

Tenant / Organization Name: FuturinCLOUD Limited

Primary Domain: [ezikaifunanya98gmail].onmicrosoft.com

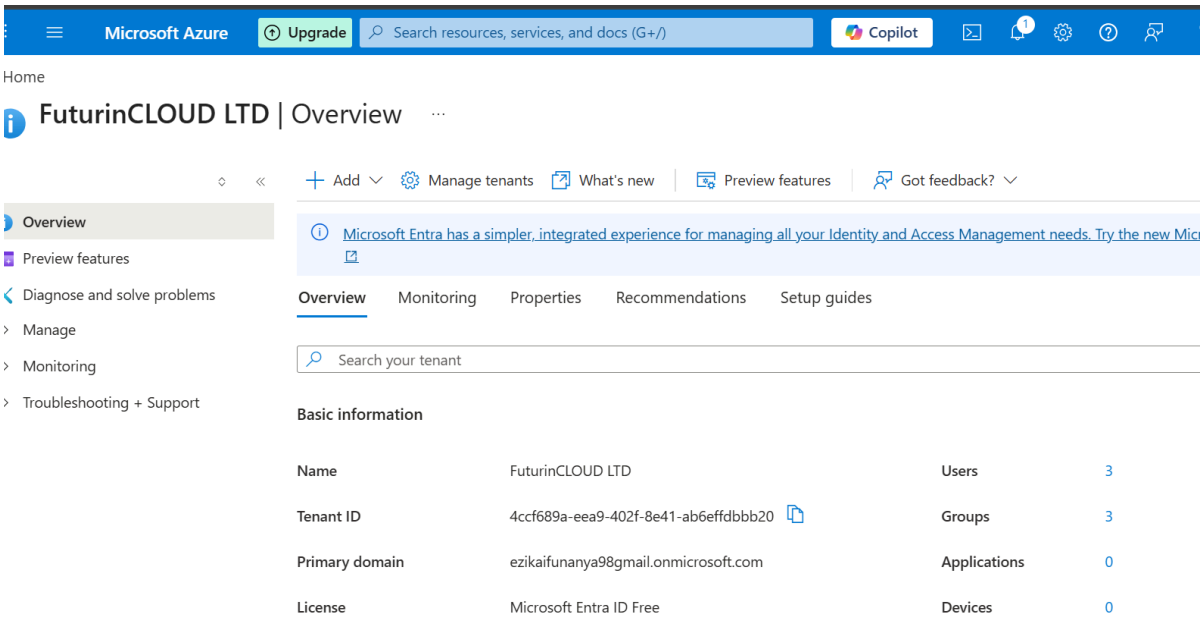

Figure 1: Microsoft Entra ID Overview – showing branded organization name and primary domain

2. User Creation

- Vera Ezika (Employee ID: FCL-SEC-001) – Senior Cloud Security Engineer
- Aisha Adebayo (Employee ID: FCL-OPS-042) – Cloud Infrastructure Specialist
- Tobi Okeke (Employee ID: FCL-SUP-119) – Technical Support & Response Analyst

All users were created with Strong password complexity and force password change on their next sign in

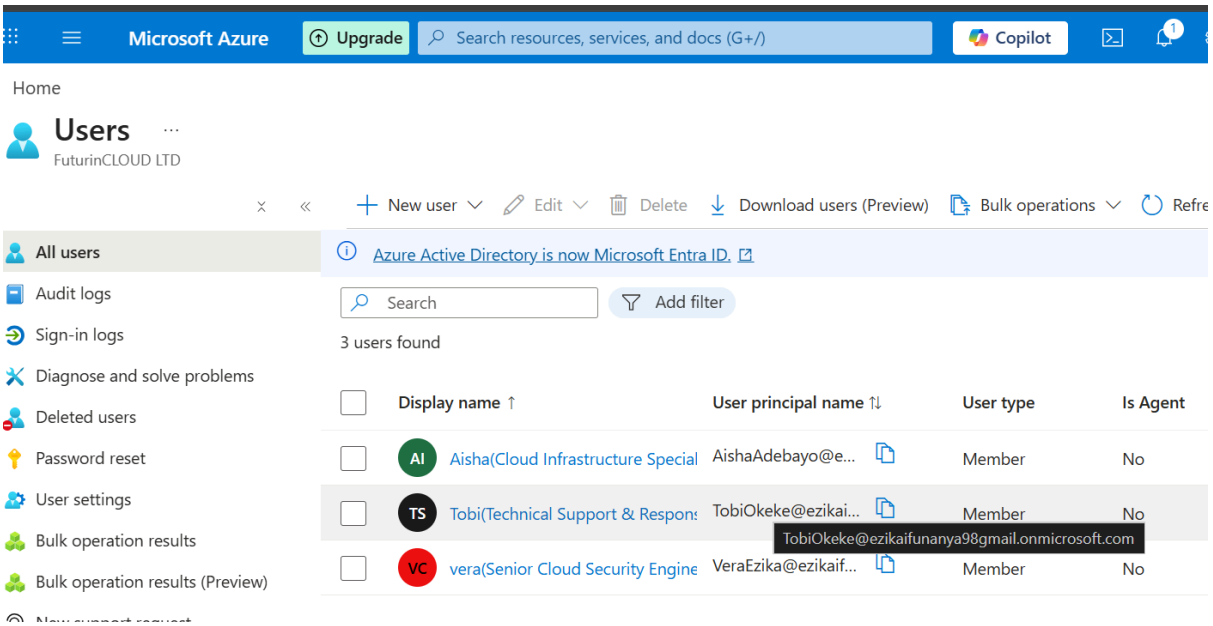

Figure 2: All users created – showing names, UPNs, and account status

3. Group Creation & Membership

Groups Created:

- FuturinCLOUD Security Core
- FuturinCLOUD Platform Operations
- FuturinCLOUD Technical Support

Each group includes: Security group type, Assigned membership and Professional description

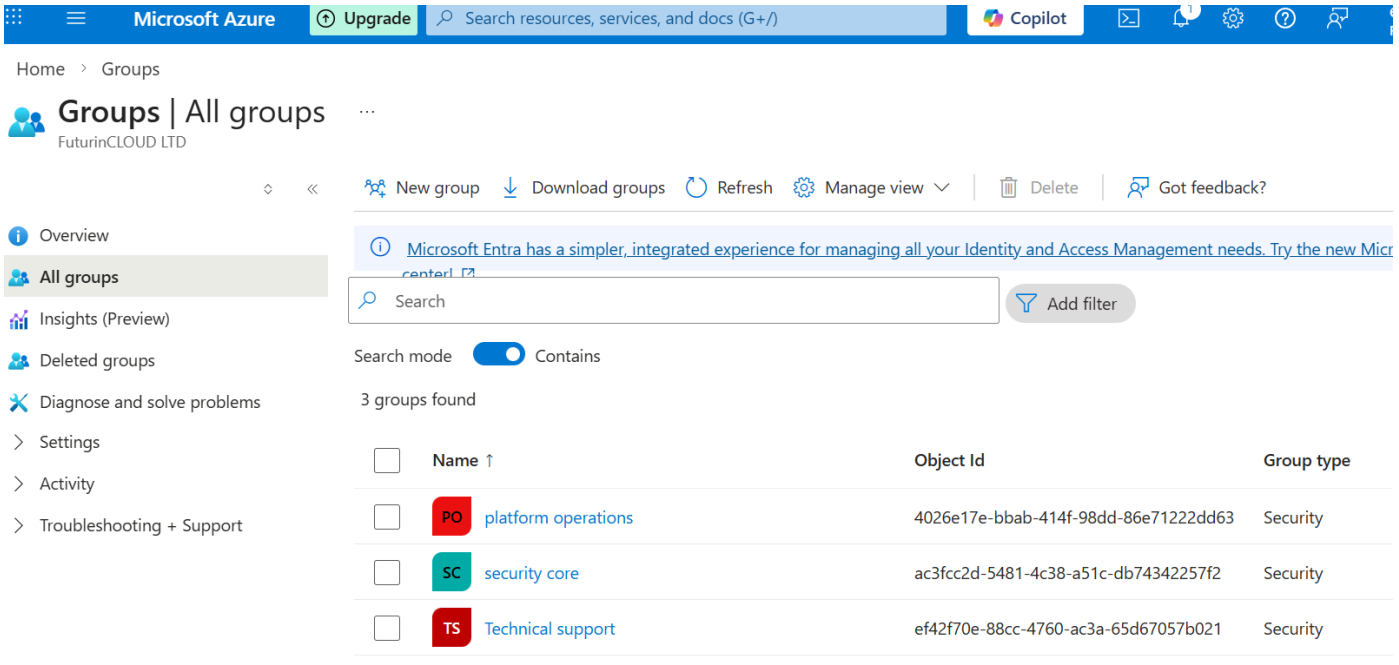

Figure 3: All groups created – listing the three departmental groups

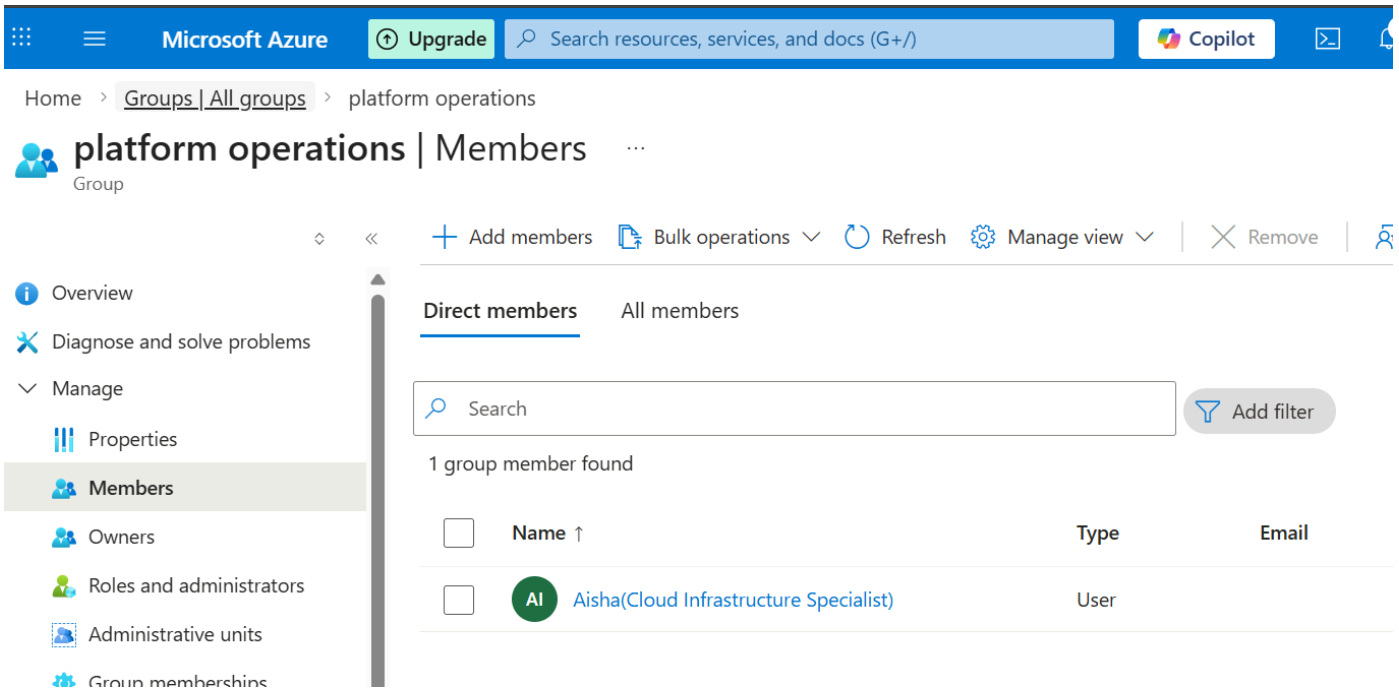

Figure 4: Platform Operations Unit – Members tab showing Aisha

4. RBAC Role Assignment

- Role Assigned: Virtual Machine Contributor
- Principal: Technical Support (group)
- Scope: Resource group (FuturinCLOUD-Labs-RG) – least privilege applied

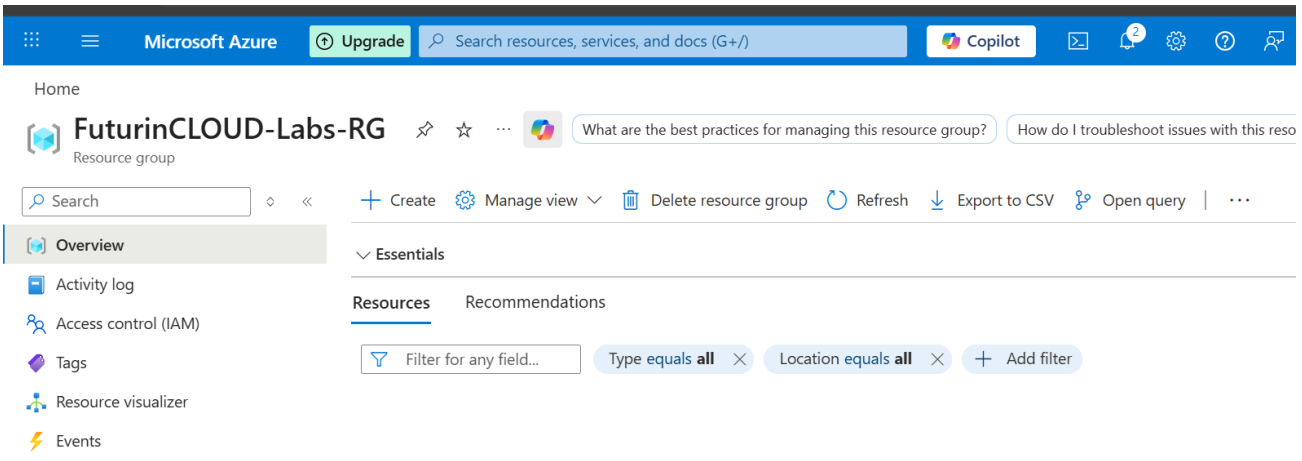

Figure 5: Resource group overview

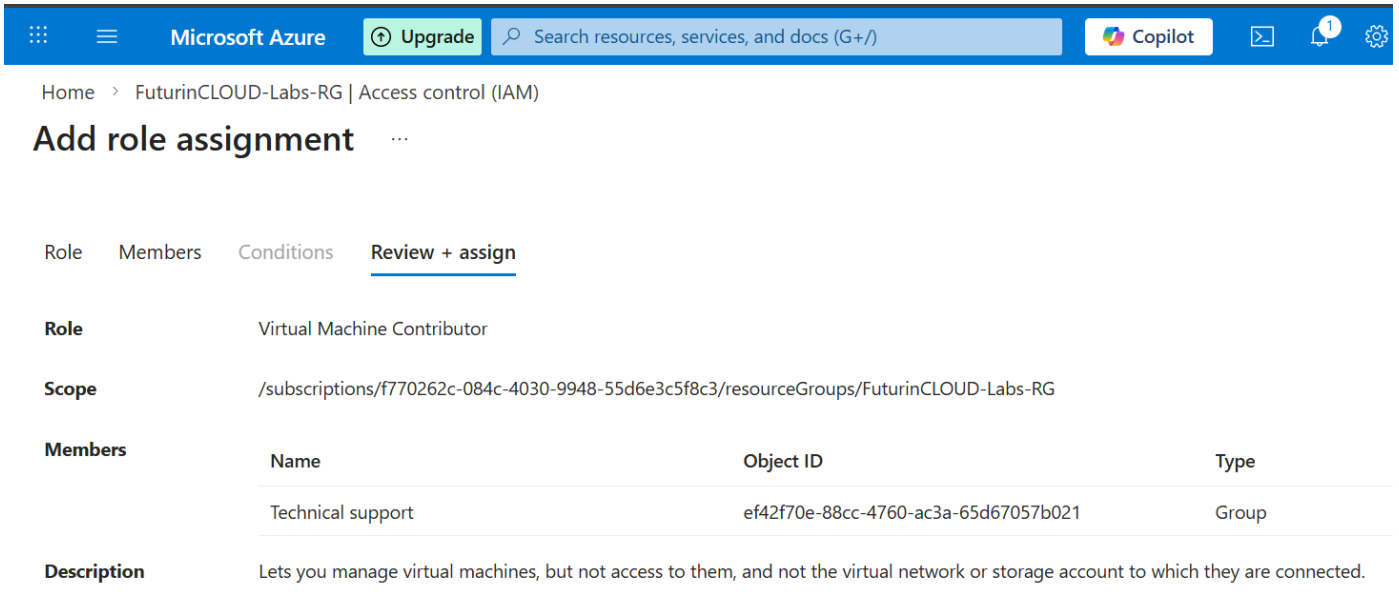

Figure 6: RBAC role assignment – Virtual Machine Contributor assigned to Technical Support

Rationale: Enables support team to troubleshoot client VMs securely without granting broad subscription level access.

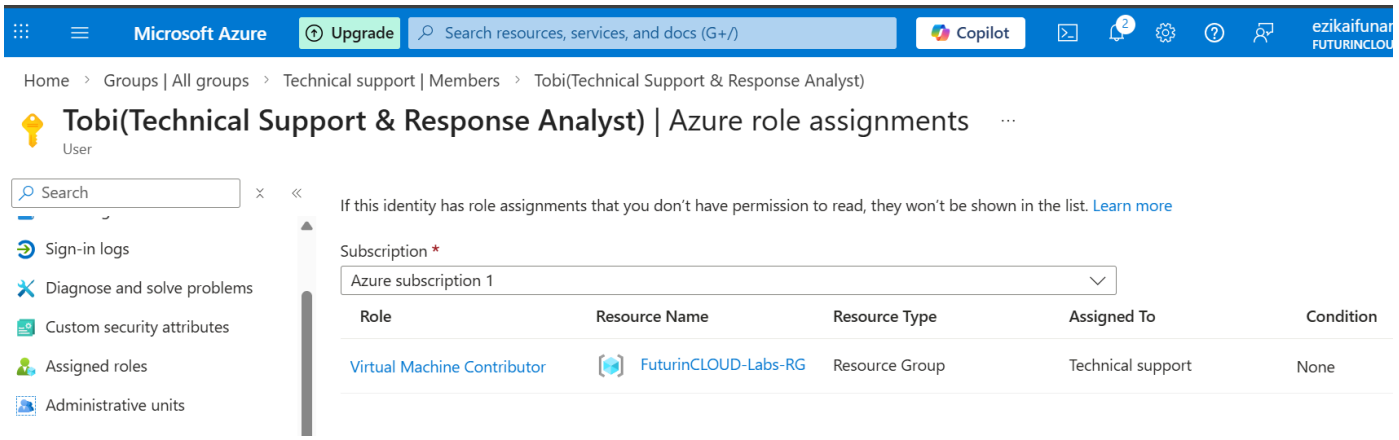

Figure 7: Effective permissions check –Tobi Okeke inherits VM Contributor role via group membership

Key Takeaways & Best Practices Demonstrated

- Group-based access instead of individual assignments for easier management & auditing
- Least-privilege RBAC scoping (resource group level) reduces blast radius
- Strong password policies and forced reset improves security posture

Technologies & Skills Showcased

- Microsoft Entra ID (users, groups, properties, descriptions)
- Azure Role-Based Access Control (RBAC) – built-in roles & scoping
- Resource group management
- Azure Portal, PowerShell (AzureAD), Azure CLI
- Least-privilege & zero-trust principles

Recommendation

Based on the successful implementation of Lab 1, the following recommendations are proposed to strengthen identity and access management in a production-like FuturinCLOUD environment:

- Enable multi-factor authentication (MFA) for all users (especially admins) to protect against credential compromise.
- Implement Privileged Identity Management (PIM) to provide just-in-time and time-bound access to elevated roles instead of permanent assignments.
- Use Conditional Access policies to restrict sign-ins based on location, device compliance, or risk level.
- Regularly review role assignments using Access Reviews in Microsoft Entra ID to ensure only necessary permissions remain active.
- Adopt least-privilege at scale by creating more granular custom roles (e.g., “VM Reader” instead of Contributor) for future labs and projects.
- Centralize identity governance by integrating Microsoft Entra ID with Azure Policy to enforce RBAC standards across all resource groups and subscriptions.

Conclusion

This Project successfully established a secure identity and access foundation for FuturinCLOUD Limited by:

- Creating three user accounts and three security groups
- Assigning the Virtual Machine Contributor role to a group at the resource group scope
- Demonstrating least-privilege access control using Azure RBAC

The lab proved that group-based role assignments reduce administrative overhead and improve security posture compared to individual user permissions. By limiting VM management rights to a single resource group, unauthorized access to other environments is prevented.This foundational RBAC configuration serves as a scalable model for future labs and real-world deployments, aligning with zero-trust principles and compliance requirements.