

# 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: [ezikaifunanya98@gmail].onmicrosoft.com

The screenshot shows the Microsoft Entra ID Overview page. At the top, there's a navigation bar with 'Microsoft Azure', 'Upgrade', a search bar, and various icons. Below the navigation bar, the page title is 'FuturinCLOUD LTD | Overview'. On the left, there's a sidebar with sections like 'Overview', 'Preview features', 'Diagnose and solve problems', 'Manage', 'Monitoring', and 'Troubleshooting + Support'. The main content area has tabs for 'Overview', 'Monitoring', 'Properties', 'Recommendations', and 'Setup guides'. A prominent message says 'Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra ID!'. Below this, there's a 'Search your tenant' bar and a 'Basic information' section with tables for Name, Tenant ID, Primary domain, License, Users, Groups, Applications, and Devices. The 'Name' row shows 'FuturinCLOUD LTD' with 3 users. The 'Tenant ID' row shows '4ccf689a-eea9-402f-8e41-ab6effdbbb20' with 3 groups. The 'Primary domain' row shows 'ezikaifunanya98@gmail.onmicrosoft.com' with 0 applications. The 'License' row shows 'Microsoft Entra ID Free' with 0 devices.

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

	Display name ↑	User principal name ↑	User type	Is Agent
<input type="checkbox"/>	AI Aisha(Cloud Infrastructure Special)	AishaAdebayo@e...	Member	No
<input type="checkbox"/>	TS Tobi(Technical Support & Respons)	TobiOkeke@ezikai...	Member	No
<input type="checkbox"/>	VC vera(Senior Cloud Security Engine)	VeraEzika@ezikaif...	Member	No

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

	Name ↑	Object Id	Group type
<input type="checkbox"/>	PO platform operations	4026e17e-bbab-414f-98dd-86e71222dd63	Security
<input type="checkbox"/>	SC security core	ac3fcc2d-5481-4c38-a51c-db74342257f2	Security
<input type="checkbox"/>	TS Technical support	ef42f70e-88cc-4760-ac3a-65d67057b021	Security

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

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the Microsoft Azure logo, an 'Upgrade' button, a search bar containing 'Search resources, services, and docs (G+/-)', and a 'Copilot' button. Below the header, the breadcrumb navigation shows 'Home > Groups | All groups > platform operations'. The main content area has a title 'platform operations | Members' with a 'Group' icon. On the left, a sidebar menu includes 'Overview', 'Diagnose and solve problems', 'Manage' (with 'Properties' and 'Members' selected), 'Owners', 'Roles and administrators', 'Administrative units', and 'Group memberships'. The main panel shows two tabs: 'Direct members' (selected) and 'All members'. A search bar and a 'Add filter' button are at the top of the list. The table below shows one member: 'Aisha(Cloud Infrastructure Specialist)' (User type) with an AI icon.

	Name ↑	Type	Email
<input type="checkbox"/>	Aisha(Cloud Infrastructure Specialist)	User	

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

The screenshot shows the Microsoft Azure portal interface for a resource group named 'FuturinCLOUD-Labs-RG'. The top bar is identical to Figure 3. The main content area shows the 'Overview' tab selected in the sidebar. The main panel displays various management actions like 'Create', 'Manage view', 'Delete resource group', 'Refresh', 'Export to CSV', 'Open query', and more. Below these are sections for 'Essentials' (Activity log, Access control (IAM), Tags, Resource visualizer, Events) and 'Resources' (Recommendations). A filtering toolbar at the bottom allows users to filter by Type, Location, and Add filter.

Figure 5: Resource group overview

Home > FuturinCLOUD-Labs-RG | Access control (IAM)

## Add role assignment

Role	Members	Conditions	Review + assign
<b>Role</b>	Virtual Machine Contributor		
<b>Scope</b>	/subscriptions/f770262c-084c-4030-9948-55d6e3c5f8c3/resourceGroups/FuturinCLOUD-Labs-RG		
<b>Members</b>	Name	Object ID	Type
	Technical support	ef42f70e-88cc-4760-ac3a-65d67057b021	Group
<b>Description</b>	Lets you manage virtual machines, but not access to them, and not the virtual network or storage account to which they are connected.		

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.

Tobi(Technical Support & Response Analyst) | Azure role assignments

If this identity has role assignments that you don't have permission to read, they won't be shown in the list. [Learn more](#)

Subscription *	Role	Resource Name	Resource Type	Assigned To	Condition
Azure subscription 1	Virtual Machine Contributor	FuturinCLOUD-Labs-RG	Resource Group	Technical support	None

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.

