Zero-Trust Identity & Access Hub

Portfolio Lab By THATO KGOLE
Date: November 2025
Cloud Platform: Microsoft Azure

Overview

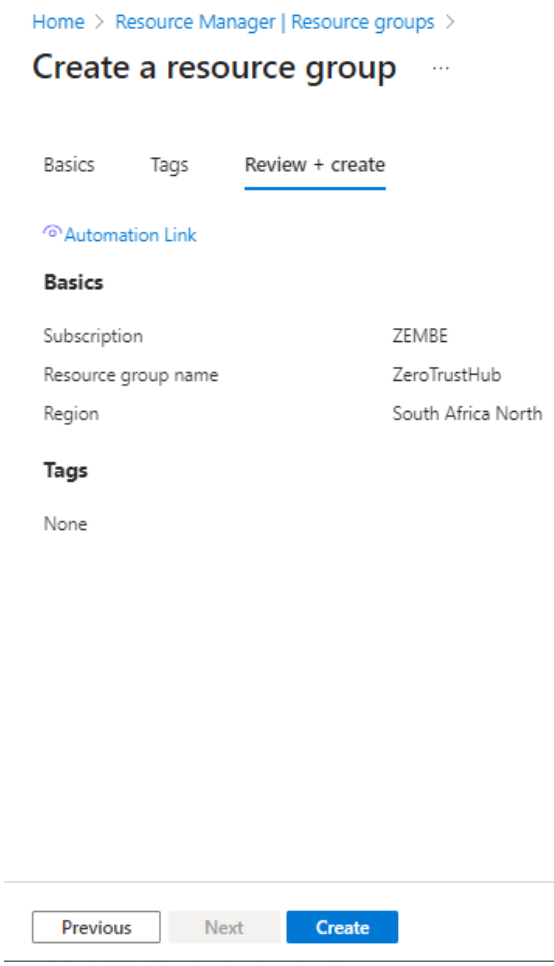
This Project demonstrates the implementation of a Zero-Trust security model in Azure by focusing on identity and access management. The goal is to secure resources by controlling who can access them, under what conditions, and with what privileges.

Problem Statement

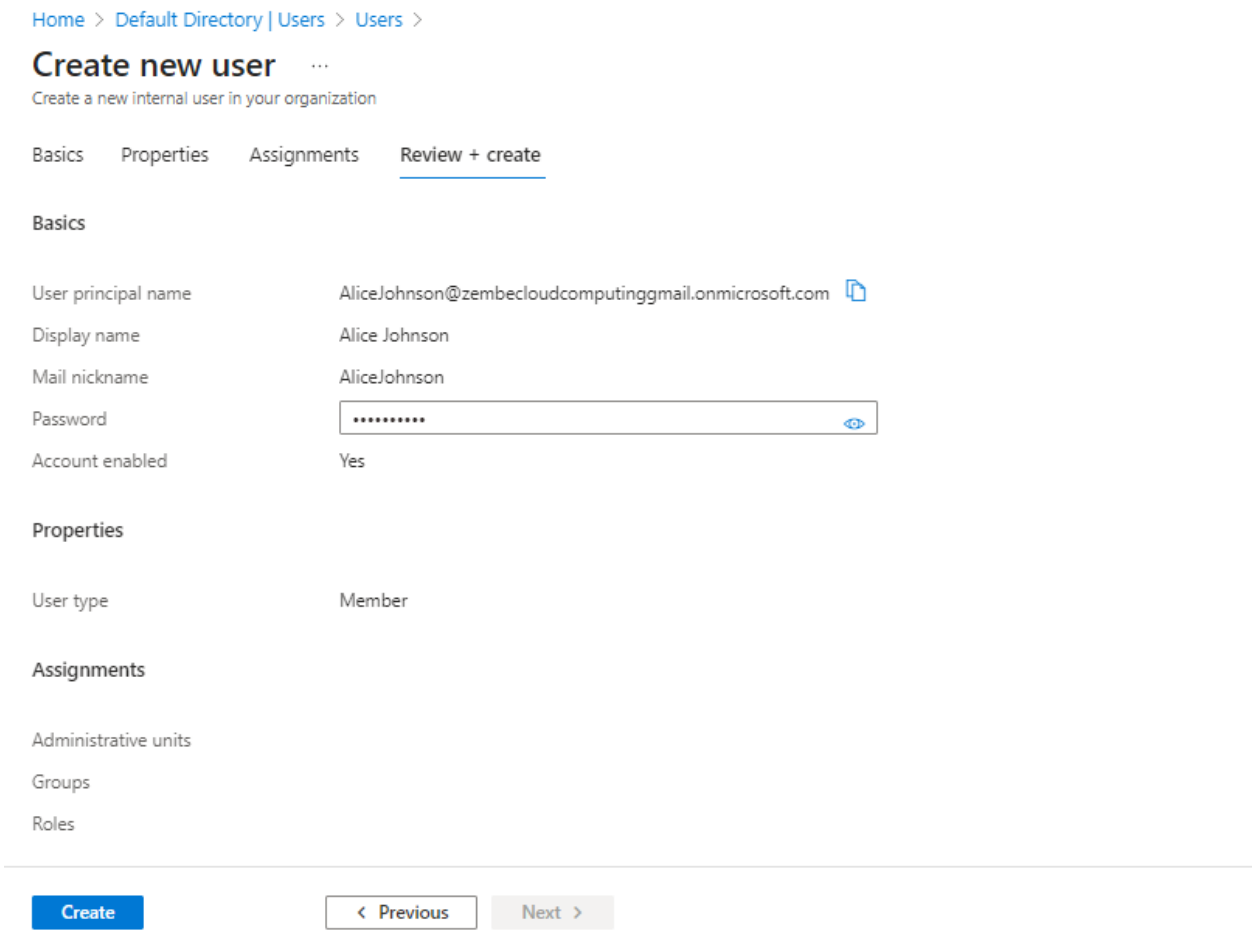
Many organizations face risks of unauthorized access and data breaches. Traditional perimeter-based security is insufficient, as users may access from multiple locations or devices.

SOLUTION

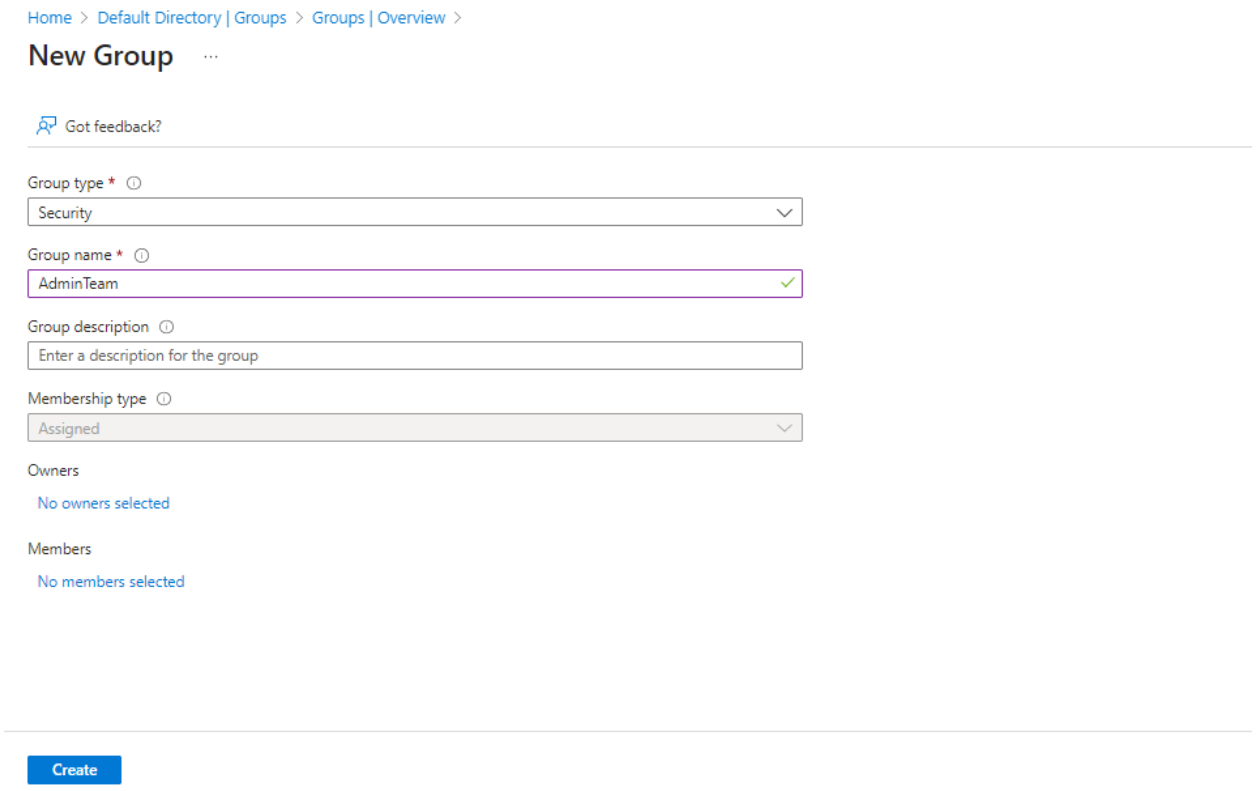
Step 1: Create a Resource Group
To group all related content



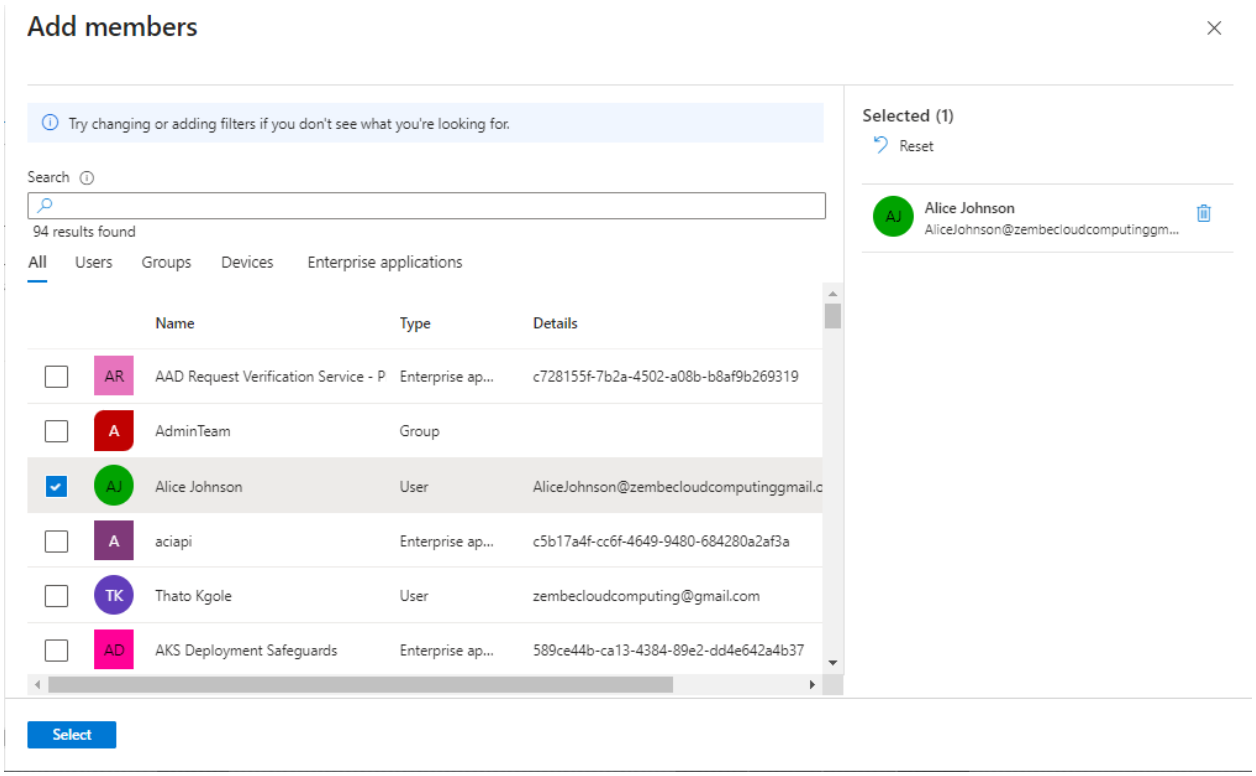
Step 2: Add user
To give permission and access later



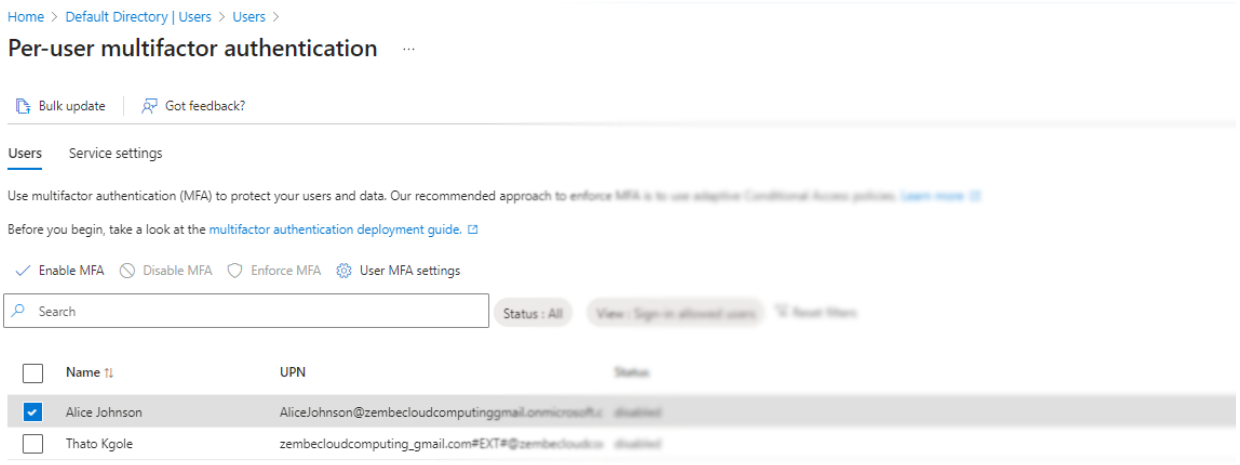
Step 3: Create Groups
To assign access all at once



Step 4: Add User Groups



Step 5: Enable MFA
For extra Security Measures



Step 6: Create Conditional Access Policy

Goal > To restrict access to admins based on location, device and require MFA

Action Taken > Conceptually created AdminAccessPolicy

Limitation > Could not enforce conditions because Conditional access requires Azure AD Premium P1 features

Step 7: Privileged Identity Management (PIM)

Goal > Allow temporary admin privileges for safe operations

Action Taken > Conceptually assigned Alice as eligible for Global Admin.

Limitation > Require P2 for activation