Scenario

You are an Azure Solutions Architect at Contoso Ltd., a company with multiple departments (Development, Operations, and Finance). Each team requires specific access to Azure resources. Your task is to design and implement Role-Based Access Control (RBAC) policies to enforce least privilege access while ensuring seamless collaboration.

Objectives

Understand RBAC principles and apply them in a real-world scenario.

Assign appropriate roles to different teams using the Azure Portal.

Validate that permissions are correctly enforced.

Instructions

Create Azure AD Groups: Navigate to Azure Active Directory (Azure AD) in the Azure Portal. Create three groups: Dev-Team, Ops-Team, and Finance-Team. Add sample users to each group to simulate team members. Ensure each group has at least two users for testing purposes.

Assign RBAC Roles: Go to the "Access Control (IAM)" section of a Resource Group. Assign the Contributor role to the Dev-Team, Reader role to the Finance-Team, and Network Contributor role to the Ops-Team. Justify your role assignments based on job responsibilities.

Test Permissions: Log in as a user from each group and verify their permissions. For example, a Dev-Team member should be able to create resources, while a Finance-Team member should only view them. Document any discrepancies.

Refine Access: If any team lacks necessary permissions or has excessive access, adjust the roles accordingly. Ensure least privilege is maintained.

