Azure Identity and Access Management (IAM) Project

This document showcases key concepts and practical implementations of Azure IAM that demonstrate expertise in managing identities, access, and security in the cloud.

1. Role-Based Access Control (RBAC)

RBAC is a critical Azure IAM feature that enables precise management of access to resources. In this project, the following steps were performed to implement RBAC:

- a. Identified roles for various teams (e.g., Admin, Developer, Read-only).
- b. Assigned built-in roles like 'Owner', 'Contributor', and 'Reader' to users and groups.
- c. Created custom roles with JSON templates for specific permissions.

Outcome: This ensured the principle of least privilege, reducing security risks.

2. Conditional Access Policies

Implemented Conditional Access policies to enforce access controls based on conditions like location, device, and risk level.

- a. Configured policies to block access from untrusted locations.
- b. Required multi-factor authentication (MFA) for sensitive resources.
- c. Enabled session controls to monitor and limit actions.

Outcome: Enhanced security by ensuring access only from trusted environments.

3. Identity Protection

Azure AD Identity Protection was utilized to detect and respond to identity-based threats.

- a. Configured risk-based policies to automatically block risky sign-ins.
- b. Monitored user risk and sign-in risk levels in Azure AD reports.
- c. Automated password resets for compromised accounts.

Outcome: Reduced the risk of unauthorized access through proactive threat management.

4. Privileged Identity Management (PIM)

Privileged Identity Management was implemented to manage, monitor, and control access to sensitive roles.

- a. Enabled just-in-time (JIT) access for privileged roles.
- b. Configured approval workflows for role activation.
- c. Reviewed access logs to ensure compliance.

Outcome: Minimized the attack surface by reducing standing permissions.

5. Integration with Azure Active Directory

Azure AD integration was utilized for seamless identity management across applications.

- a. Integrated on-premises Active Directory with Azure AD using Azure AD Connect.
- b. Enabled single sign-on (SSO) for cloud applications.
- c. Configured application proxy for secure remote access to on-premises apps.

Outcome: Streamlined identity management and improved user productivity.

Conclusion

This project demonstrates a comprehensive understanding of Azure IAM concepts and their application in real-world scenarios. The implementation of RBAC, conditional access, identity protection, PIM, and Azure AD integration highlights the ability to design and manage secure, efficient cloud environments.