ONE PAGE SUMMARY

IT & Software › Microsoft Azure › Azure Active Directory

Introduction to Azure Active Directory

Unlocking the Power of Azure Active Directory

DEFINITION

> Azure Active Directory (Azure AD) is a cloud-based identity and access management service. It helps organizations manage user identities and secure access to resources.

KEY CONCEPTS

Identity Management

Azure AD allows organizations to create and manage user accounts and their access to applications.

Single Sign-On (SSO)

SSO enables users to log in once and access multiple applications without re-entering credentials.

Multi-Factor Authentication (MFA)

MFA adds an extra layer of security by requiring two or more verification methods for user access.

Role-Based Access Control (RBAC)

RBAC assigns permissions to users based on their roles, ensuring they only access necessary resources.

Conditional Access

Conditional Access policies control access to applications based on user conditions, such as location or device.

EXAMPLES

→ A company uses Azure AD for employee login to Office 365.

→ Users access Salesforce with SSO through Azure AD.

→ An organization implements MFA for sensitive data access.

MEMORY TIPS

★ Remember 'AAD' as 'All Access Done' for Azure AD's role in managing access.

★ Think of SSO as 'Single Sign-On' - one key opens many doors.

★ Use 'MFA' as 'More Factors Always' for enhanced security.

COMMON MISTAKES

✗ Confusing Azure AD with traditional Active Directory.

✗ Overlooking the importance of MFA for security.

✗ Not utilizing Conditional Access for risk management.

QUICK RECAP

Azure Active Directory is essential for managing identities and securing access in the cloud. Key features include SSO, MFA, and RBAC, which enhance security and user experience. Understanding these concepts is crucial for effective identity management.