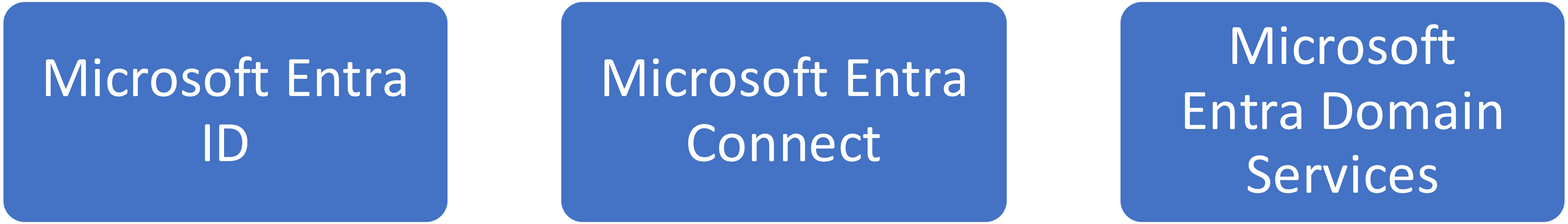
Azure Directory Services

Praveenkumar Bouna, CodeWithPraveen.com

Types of AD Services in Azure



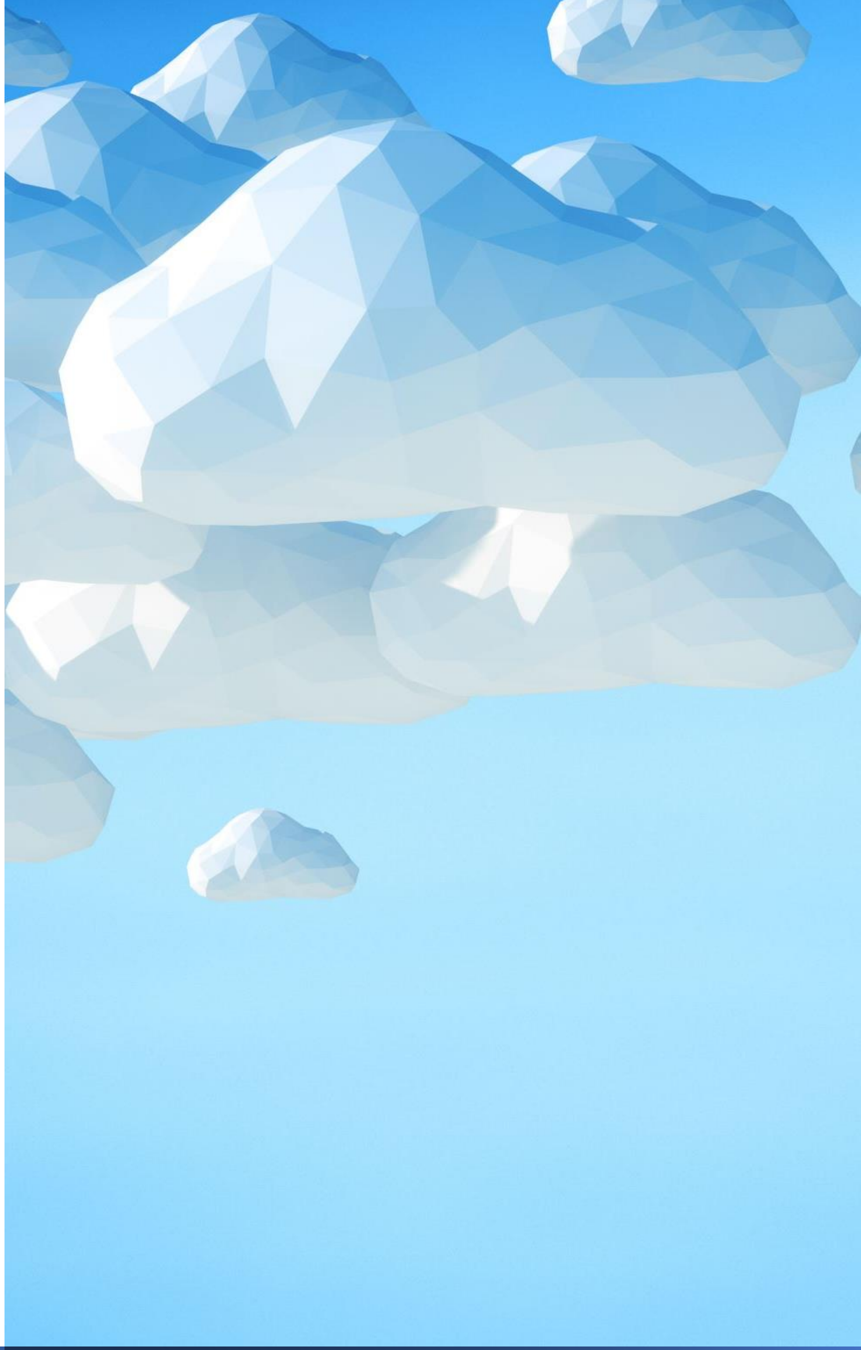
Microsoft Entra ID

Microsoft Entra Connect

Microsoft Entra Domain Services

Microsoft Entra ID: Overview

- Access Microsoft apps
- Access custom apps
- AD on cloud



Microsoft Entra ID: Features

- Authentication
- Single Sign-on (SSO)
- Application management

Microsoft Entra ID: Users

- Administrators
- Developers
- End-users

Microsoft Entra Connect

- Connect on-prem AD with Microsoft Entra ID.
- Syncs identities

Microsoft Entra Directory Services: Overview

- Managed domain services
- Supports legacy apps
- Integrates with Microsoft Entra ID

Microsoft Entra Domain Services: Features

- Domain join
- Group policy

Azure Authentication Methods

Praveenkumar Bouna, CodeWithPraveen.com

Authentication Methods

- Standard passwords
- Single sign-on (SSO)
- Multifactor authentication (MFA)
- Passwordless

Standard Passwords

Low security but high convenience

Common with apps

Simple to implement and use

Single Sign-On (SSO)

Sign in once and use multiple apps

Ease of account management

Multifactor Authentication (MFA)

Additional identification during sign-in

At least two methods of authentication

More secured form of authentication

Microsoft Entra Multi-Factor Authentication

Azure offering of MFA

Passwordless Authentication

Authenticate without manual passwords

Increased convenience.

Azure offerings:

Windows Hello for Business

Microsoft Authenticator app

FIDO2 security keys

Azure External Identity

Praveenkumar Bouna, CodeWithPraveen.com

Overview of Azure External Identity

- Secure authentication with external users
- Grant or revoke access to guests
- Support for B2B and B2C use cases

Types of Azure External Identities

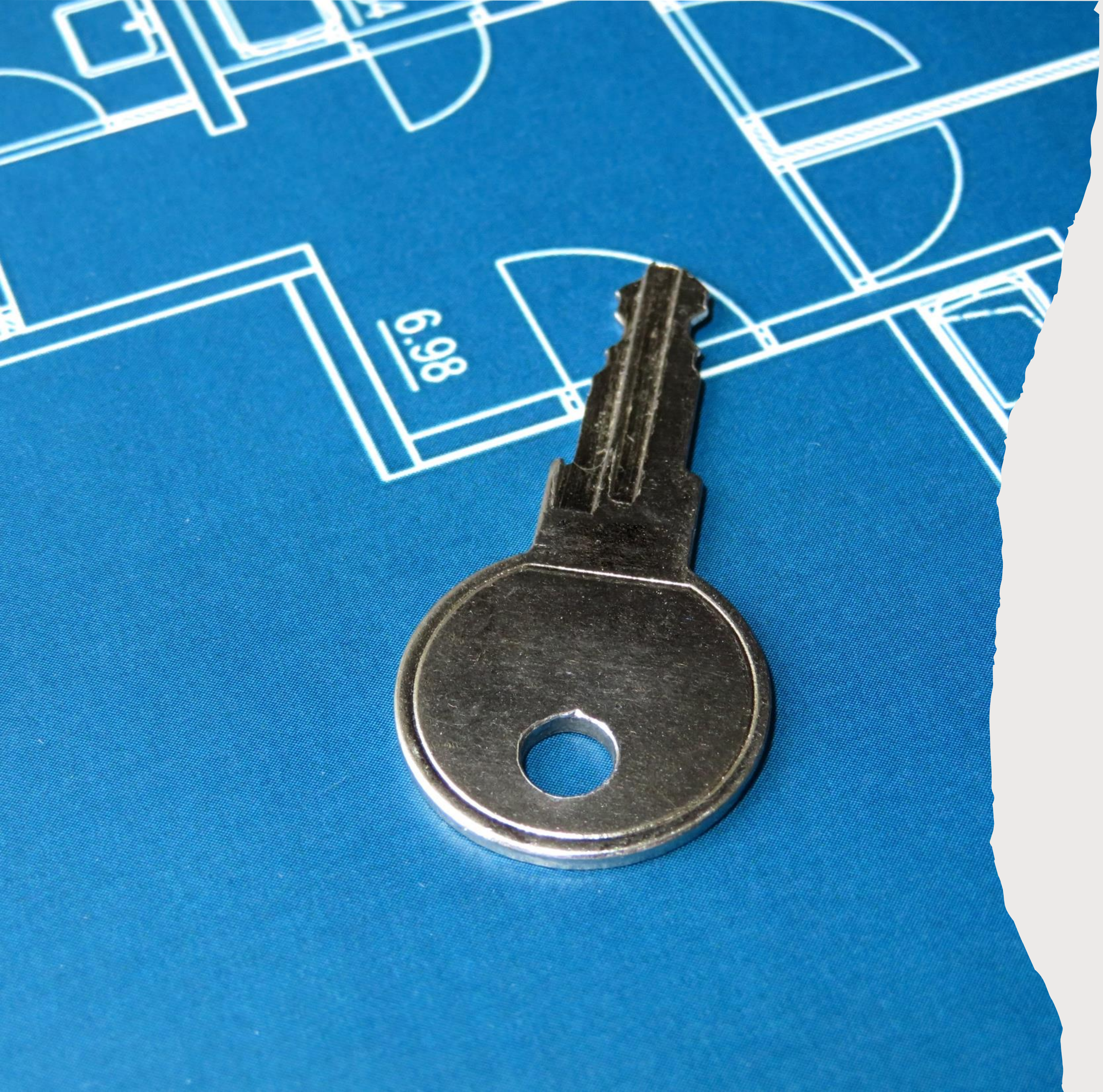
Business to Business:
B2B Collaboration

Business to Business:
B2B Direct Connect

Business to Consumer:
Azure AD B2C

Azure Conditional Access

Praveenkumar Bouna, CodeWithPraveen.com



Conditional Access allows or blocks access to resources based on certain conditions (signals)

Uses of Conditional Access

Access resources from anywhere

Secure resources

More refined MFA

Conditional Access

Parameters

- User location
- User device
- App used

Action

- Allow full access
- Require second authentication
- Block access

Azure Role-Based Access Control

Praveenkumar Bouna, CodeWithPraveen.com

Azure RBAC: Overview

Detailed access management

Based on roles

Roles applied to scope

Azure RBAC: Benefits

Improved security

Easier administration

Azure RBAC: Use Cases

- Control access to Azure resources
- Temporary access to guests
- Enforce least privilege model

Defense-in-depth and Zero Trust Models

Praveenkumar Bouna, CodeWithPraveen.com

Zero Trust Model: Overview

- Requires authentication & authorization for all access
- Uses least privilege model
- Threat detection

Zero Trust Model: Benefits

IMPROVED SECURITY

REDUCED RISK

INCREASED FLEXIBILITY

Zero Trust Model: Limitations

Complexity

Cost

Implementation challenges

Defense-in-depth

Protect information and prevent it from being stolen by those who aren't authorized to access it

Defense-in-depth: Layers

- Physical security
- Identity and access
- Perimeter
- Network
- Compute
- Application
- Data

Defense-in-depth: Benefits

Limit attacks

Layered approach for security

Slows down an attack & its impact

Defender for Cloud

Praveenkumar Bouna, CodeWithPraveen.com

Microsoft Defender for Cloud offers high-level security monitoring and advanced threat protection for cloud environments

Defender for Cloud: Supported Environments

- Azure
  - Azure services
- On-Prem
  - Extends to your non-Azure on-prem server
- Multi-cloud
  - AWS and GCP

Defender for Cloud: Operation

Assess

Secure

Defend