Host a Static Website in Azure Storage

Resources

- https://learn.microsoft.com/en-us/azure/storage/blobs/storage-blob-static-website-how-to?tabs=azure-portal
- Sample website - https://drive.google.com/drive/folders/1f8h2RH1HXihM581EsQV3vsAdi37zXGhf?usp=sharing

Authorization and Authentication - Resource Lock , RBAC, Entra ID, Zero Trust Concept

Contents

- Authorization and Authentication
- Resource Lock
- Role-Based Access Control (RBAC)
- Entra ID (Formerly Active Directory)
- Multi-Factor Authentication (MFA)
- Zero Trust Concept

Intro

In almost all cases, attackers are after data:

- Stored in a database
- Stored on disk inside virtual machines
- Stored on a SaaS application such as Office 365
- Stored in cloud storage

It's the responsibility of those storing and controlling access to data to ensure that it's properly secured. Often, there are regulatory requirements that dictate the controls and processes that must be in place to ensure the confidentiality, integrity, and availability of the data.

Authentication and Authorization

Two fundamental concepts that need to be understood when talking about identity and access control are authentication and authorization. They underpin everything else that happens and occur sequentially in any identity and access process:

- Authentication is the process of establishing the identity of a person or service looking to access a resource. It involves the act of challenging a party for legitimate credentials, and provides the basis for creating a security principal for identity and access control use. It establishes if they are who they say they are.

Authentication and Authorization

- Authorization is the process of establishing what level of access an authenticated person or service has. It specifies what data they're allowed to access and what they can do with it. Authentication is sometimes shortened to AuthN, and authorization is sometimes shortened to AuthZ. Azure provides services to manage both authentication and authorization through Azure Active Directory (now Microsoft Entra).

Authentication

The process of verifying the identity of a user or system. It answers the question, "Who are you?"

Types of authentication:

- Single-Factor Authentication (SFA)
- Multi-Factor Authentication (MFA)
- Biometrics
- Certificates

Examples: Username/Password, OTP, Biometrics

Authorization

The process of determining what resources a user or system can access. It answers the question, "What are you allowed to do?"

Methods of authorization:

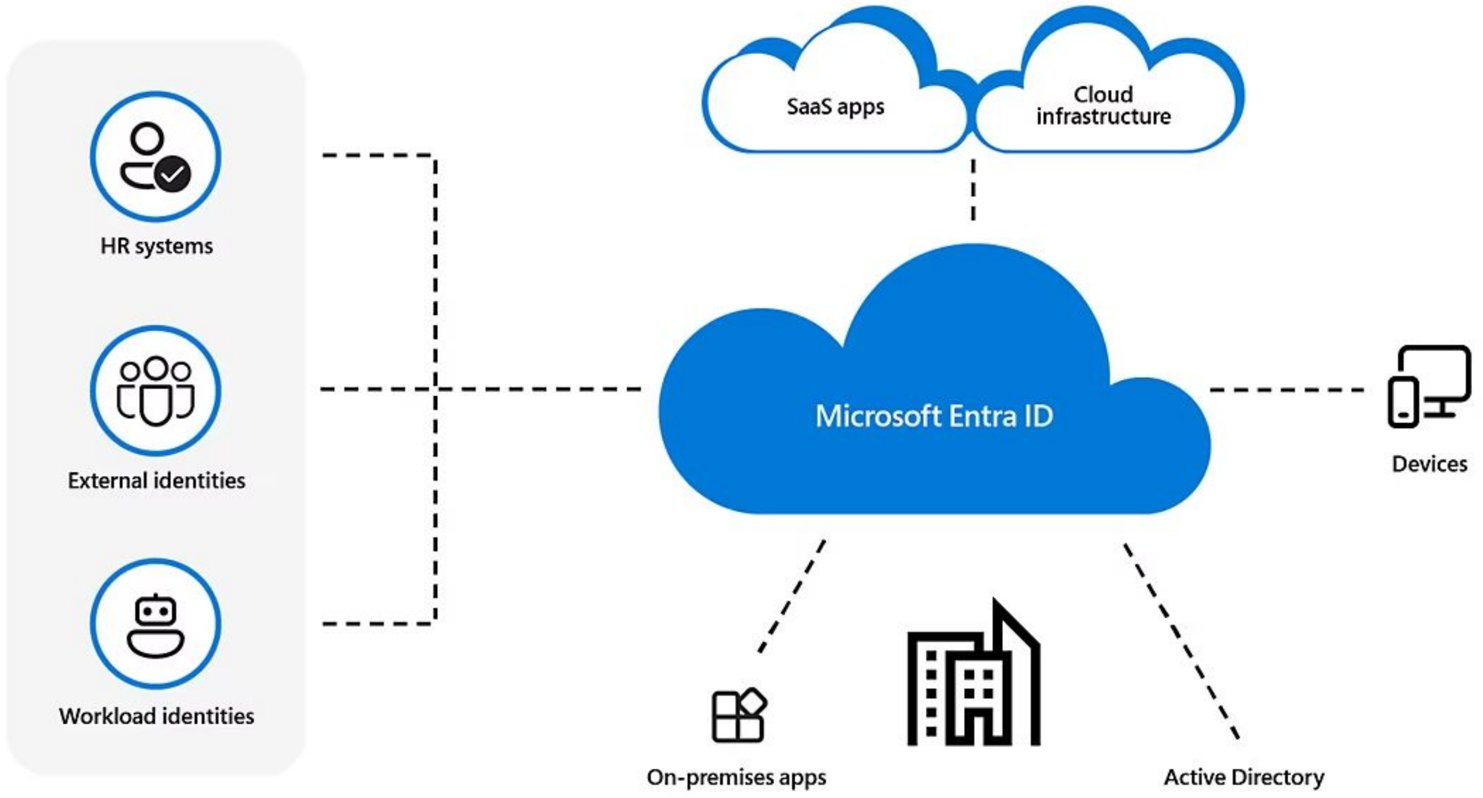
- Access Control Lists (ACLs)
- Role-Based Access Control (RBAC)
- Policies and Rules

Types of Authentication

- **Single-Factor Authentication (SFA)**: Uses one method of verification (e.g., password).
- **Two-Factor Authentication (2FA)**: Combines two methods (e.g., password and SMS code).
- **Multi-Factor Authentication (MFA)**: Uses multiple methods (e.g., password, biometrics, and a security token).
- **Biometric Authentication**: Uses physical characteristics (e.g., fingerprints, facial recognition).

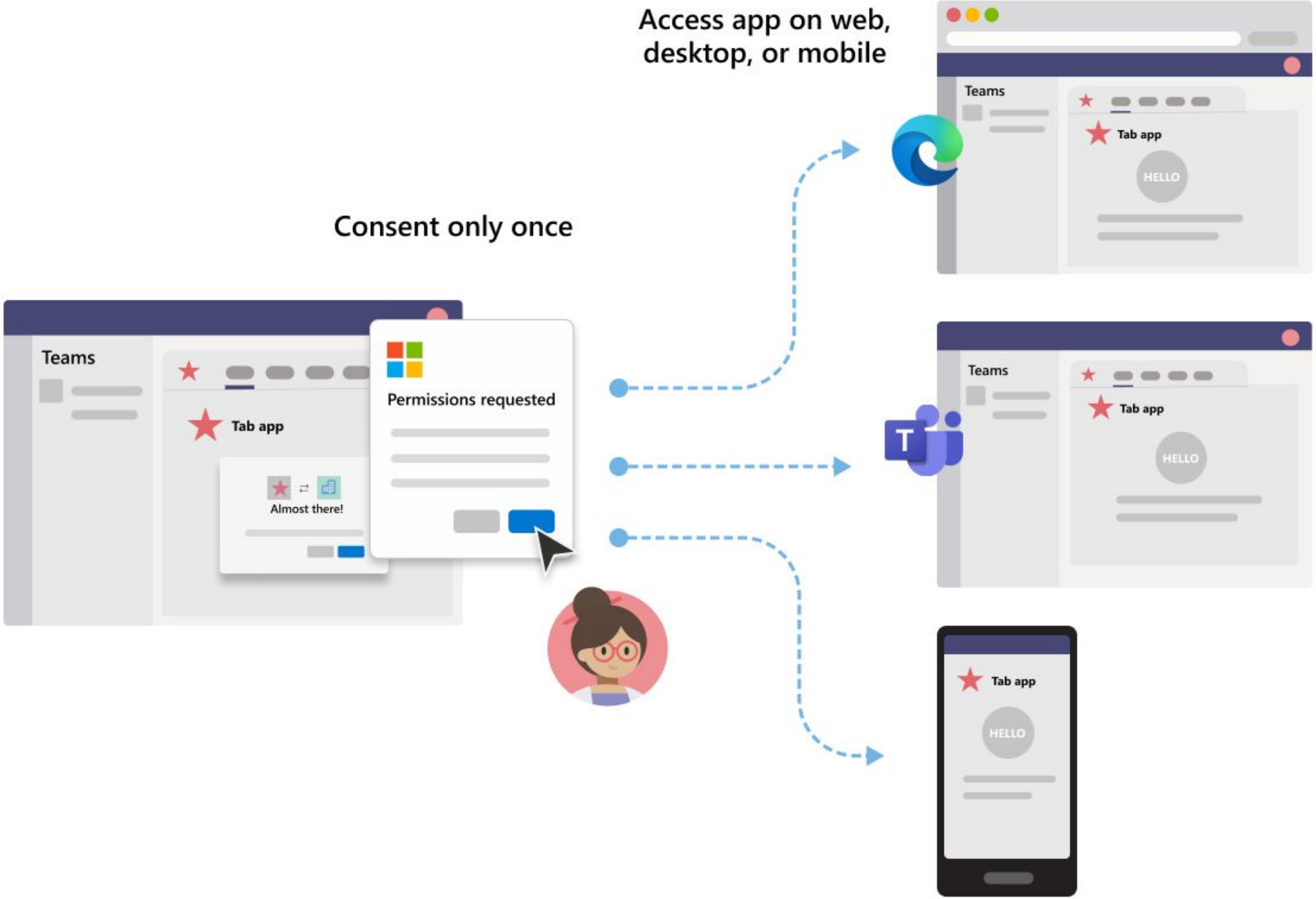
What is Microsoft Entra ID?

Microsoft Entra ID: Formerly known as Azure Active Directory (Azure AD), Microsoft Entra ID is a comprehensive identity and access management service provided by Microsoft.


SaaS apps
Cloud infrastructure
HR systems
External identities
Workload identities
Microsoft Entra ID
Devices
On-premises apps
Active Directory

Key Features of Microsoft Entra ID

- **Single Sign-On (SSO)**:
  - Allows users to sign in once and gain access to multiple applications and services without re-authenticating.
- **Multi-Factor Authentication (MFA)**:
  - Enhances security by requiring two or more verification methods for user sign-ins.
- **Conditional Access**:
  - Policies to enforce who can access what resources under what conditions.



Consent only once

Access app on web, desktop, or mobile

- **Identity Protection**:
  - Uses machine learning to detect and respond to suspicious activities related to identities.
- **Self-Service Password Reset (SSPR)**:
  - Enables users to reset their passwords without administrator intervention.
- **B2B Collaboration**:
  - Allows secure collaboration with external partners and contractors.
- **Application Management**:
  - Centralized management for SaaS apps, including pre-integrated apps from the Azure AD app gallery.
- **Monitoring and Reporting**:
  - Provides logs and alerts to monitor and report suspicious activities or policy violations.

Benefits of Microsoft Entra ID

- **Improved Security**:
  - Comprehensive security controls protect against identity-based attacks.
- **Enhanced Productivity**:
  - Simplifies access to resources, reducing login-related interruptions.
- **Streamlined IT Operations**:
  - Centralized identity management reduces administrative overhead.
- **Compliance Support**:
  - Helps meet regulatory requirements with built-in security and compliance tools.

Use Cases of Microsoft Entra ID

Enterprise Identity Management:

- Managing employee access to internal and external applications.

Customer Identity and Access Management (CIAM):

- Providing secure access for customers to applications and services.

Hybrid Identity Management:

- Integrating on-premises and cloud identities for seamless access.

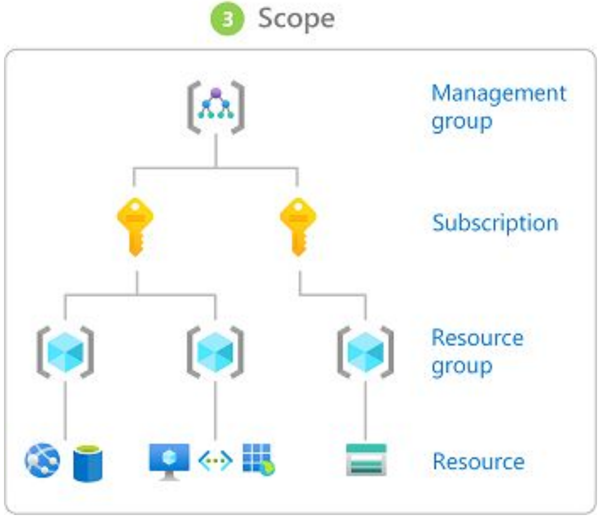
Role Based Access Control

Azure role-based access control (Azure RBAC) helps you manage who has access to Azure resources, what they can do with those resources, and what areas they have access to.

Key components:

- Roles
- Permissions
- Users

Examples: Admin, User, Manager roles



Resource Locks

Resource locks is a mechanism to prevent simultaneous access to resources that can lead to conflicts.

Purpose: Ensures data integrity and consistency by controlling access.

Examples: File locks, database locks, network resource locks

Zero Trust Concept

Security model assuming no implicit trust, verify everything

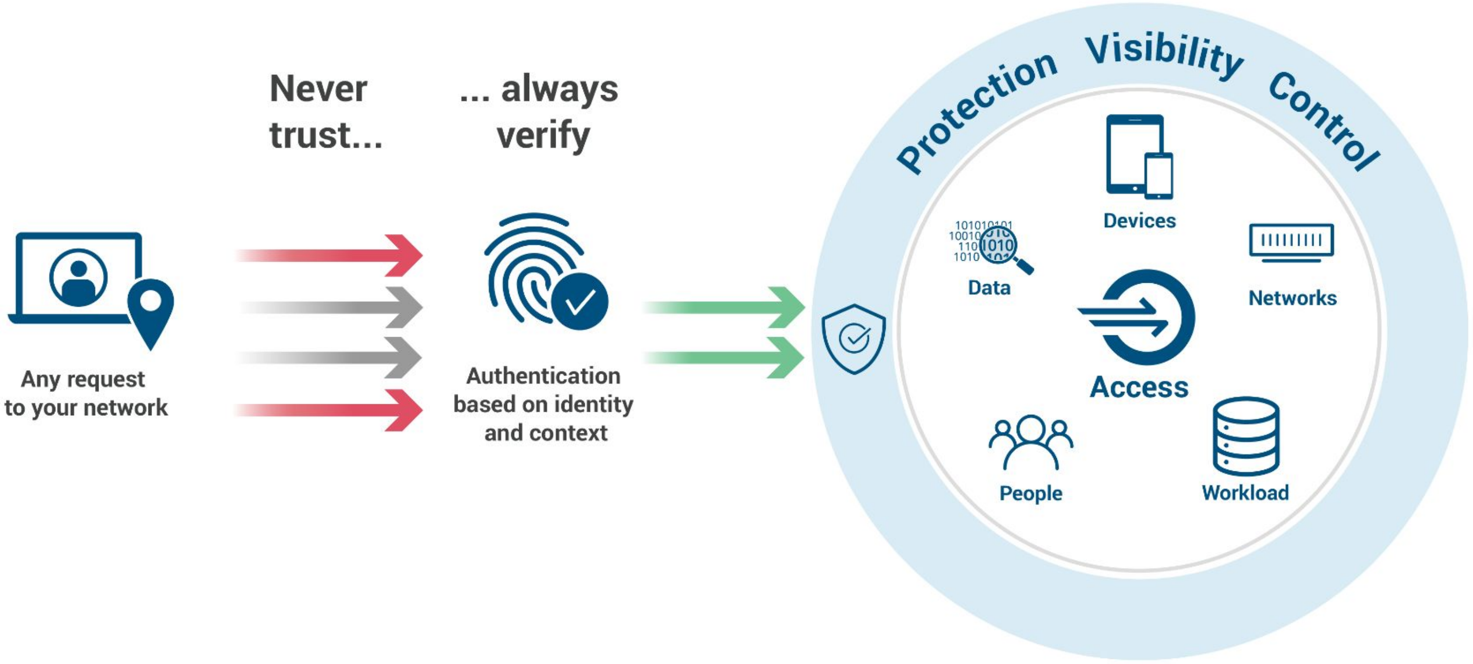
Principles:

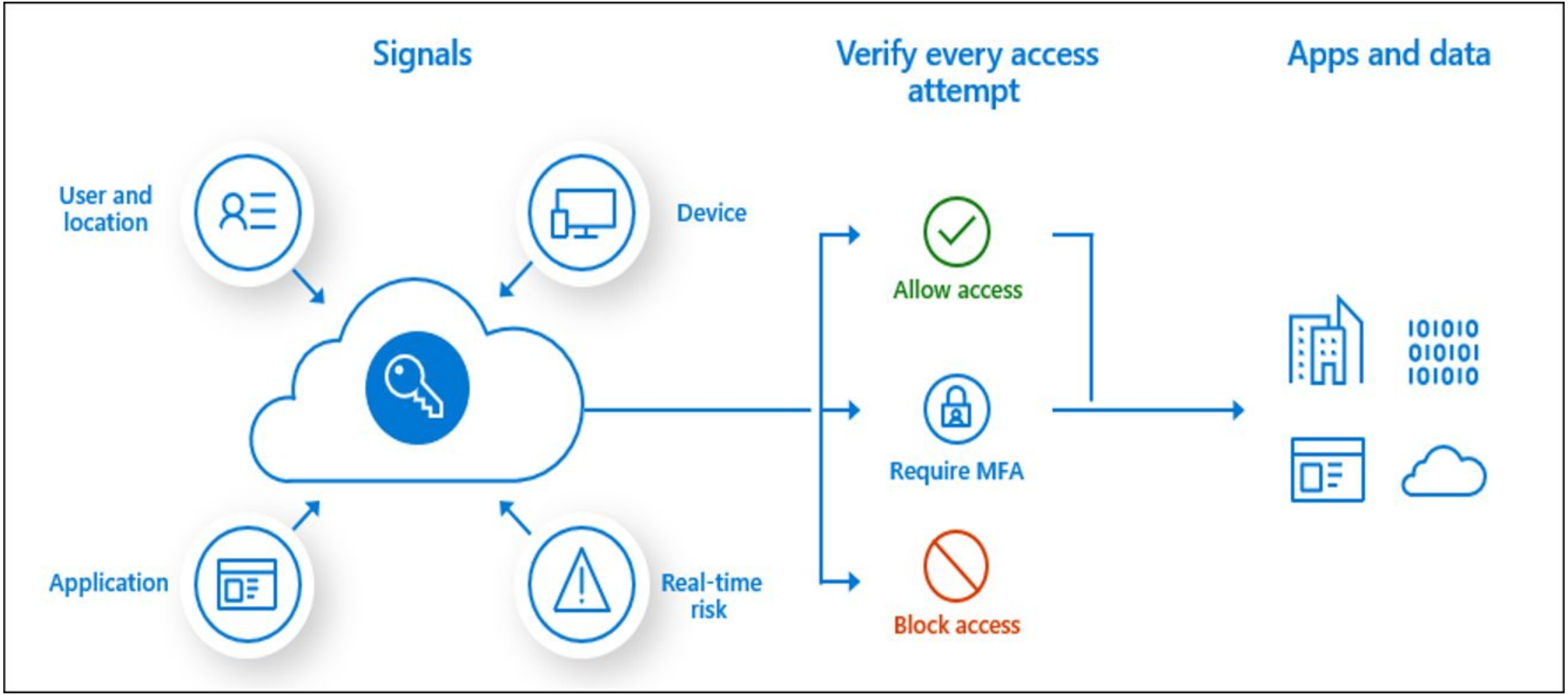
- Verify explicitly
- Use least privilege access
- Assume breach

Implementation:

- Continuous verification
- Micro-segmentation
- Strong authentication

Zero Trust Security





Signals

Verify every access attempt

Apps and data

User and location

Device

Application

Real-time risk

Allow access

Require MFA

Block access

Resources

- https://learn.microsoft.com/en-us/azure/role-based-access-control/overview
- https://learn.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles
- https://learn.microsoft.com/en-us/azure/security/fundamentals/zero-trust
- https://learn.microsoft.com/en-us/entra/fundamentals/whatis

Assignment

1. Write a blog on how to host static website on Azure Blob Storage

★ Attempt Storage Applied Skill Assessment - https://learn.microsoft.com/en-us/credentials/applied-skills/secure-storage-azure-files-azure-blob-storage/

Submission Deadline: Friday

Submission Link:

★ https://forms.gle/xykwGPnziuEMZbRL6