Identity, Governance, Privacy and compliance

Erick Torres

Erick Torres

- **SRE** L3
- FLOSS member
- Fullstack Developer
- Mechatronics engineer (IoT specialist)

Important Notes

Identify yourself in Zoom, using your name and last name

Mute your microphone along the course

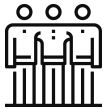
Use the chat for questions during the Q&A sections

Focus your questions on the presented topic

Turn off your camera in case of connection issues

Academy Code of Conduct

Be respectful, there are no bad questions or ideas.



Be welcoming and patient

Be careful in the words that you choose

Session objectives

At the end of the session you will be able to understand:

- Azure identity services(Azure AD, MFA, SSO, etc.)
- Governance(RBAC, Policy)

Table of Contents

Pre requirements

PC with internet connection

SSH Client

Azure identity services

Authentication vs Authorization

Authentication

- Identifies the person or service trying to access a resource.
- Request legitimate login credentials
- Basis for creating secure principles of identity and access control

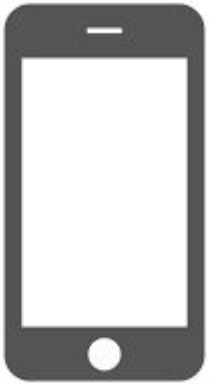
Authorization

- Determines the level of access of an authenticated person or services
- Define what data can be accessed and what can be done with it

Azure Multi-Factor Authentication

Provides additional security for your identities by requiring two or more elements for full authentication

something that is known (Credentials) <-> **something to own (Device)** <-> **Something that is part of you (Biometric data, FaceID)**



Azure Active Directory

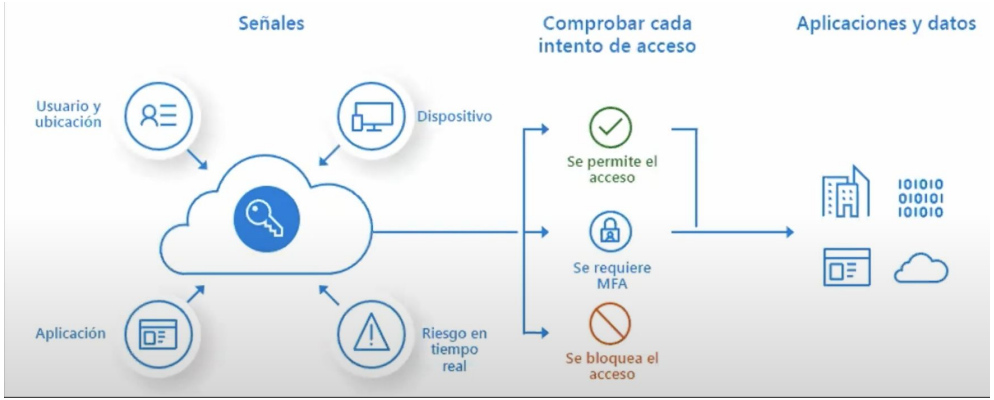
Microsoft cloud-based identity and access management service

- Authentication (Employees log in to access resources)
- Single sign-on (SSO)
- Application Management
- Business to Business (B2B)
- Business-to-customer (B2C) identity services
- Device management
- Azure AD connect(Hybrid)

Conditional access

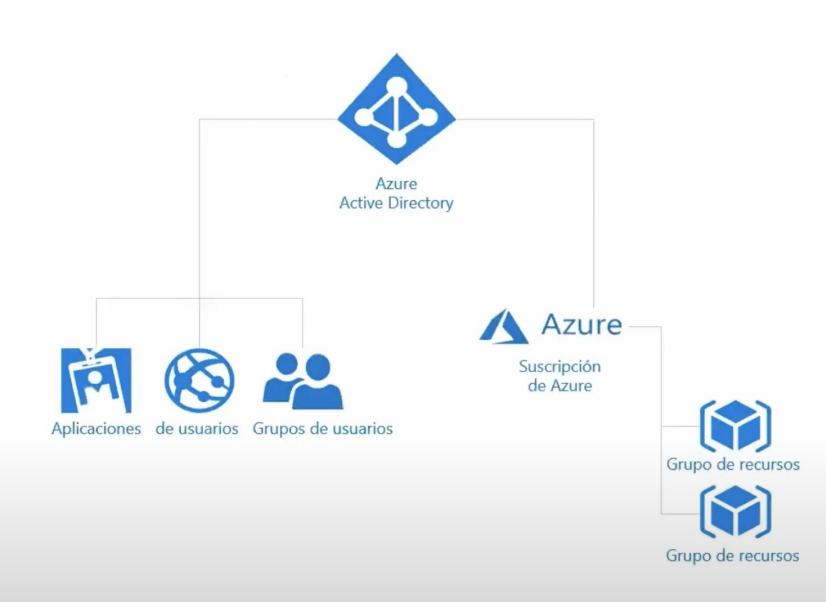
It is what AAD uses to gather signals, make decisions, and apply organizational policies

- User or group membership
- IP Location
- Device
- Application
- Risk Detection



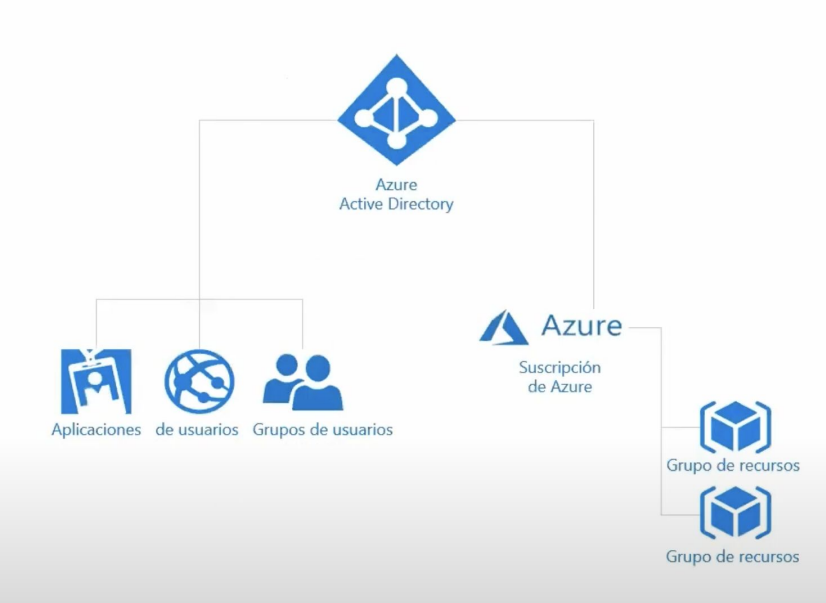
Governance methodologies in Azure

Role Based Access Control (RBAC)



- Specific access management
- Separate tasks within the team
- Grant only the access someone needs to do their job
- Allows access to the portal UI
- Allow access to Azure resources

Tutorial: Manage access with RBAC



Assign roles and view activity logs

1. View and assign roles
2. View the activity log and remove a role assignment

Resource locking

- Prevent update or deletion of azure resources
- Subscription, resource group and individual resource level

Lock Types	Read	Update	Delete
CanNoDelete	Yes	Yes	No
ReadOnly	Yes	No	No

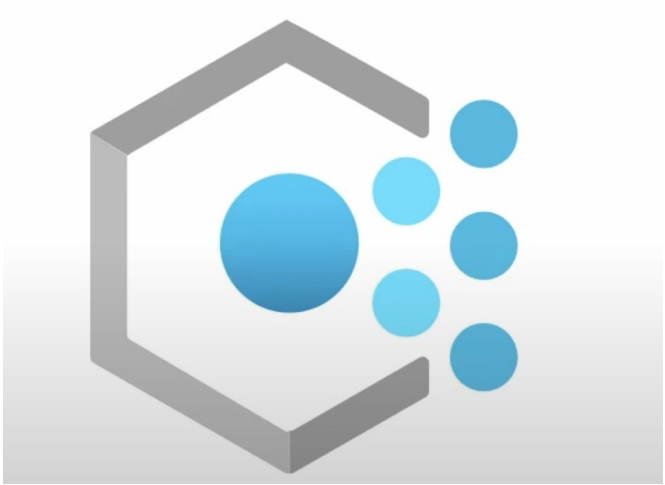
Tags

- Metadata for azure resources
- Organize resources logically
- Key-Value
- Useful to billing info

Azure Policy

Azure policy helps enforce organization standards and assess compliance at scale. Provides resource governance and consistency with regulatory compliance, security, cost, and administration.

- Assess and identify azure resources that are out of compliance
- Provides policy definitions and built-in initiatives, in categories such as storage, networking, compute, security center, and monitoring



Quizizz time!

Thank you

Please answer the survey form of this session:

https://docs.google.com/forms/d/e/1FAIpQLSf8tahLh_1_DA7B4rv10X0RGHLCrvOUEpnh04f9Trnk0LeWKg/viewform