Azure directory services

UNDERSTANDING MICROSOFT AZURE ARCHITECTURE AND SERVICES

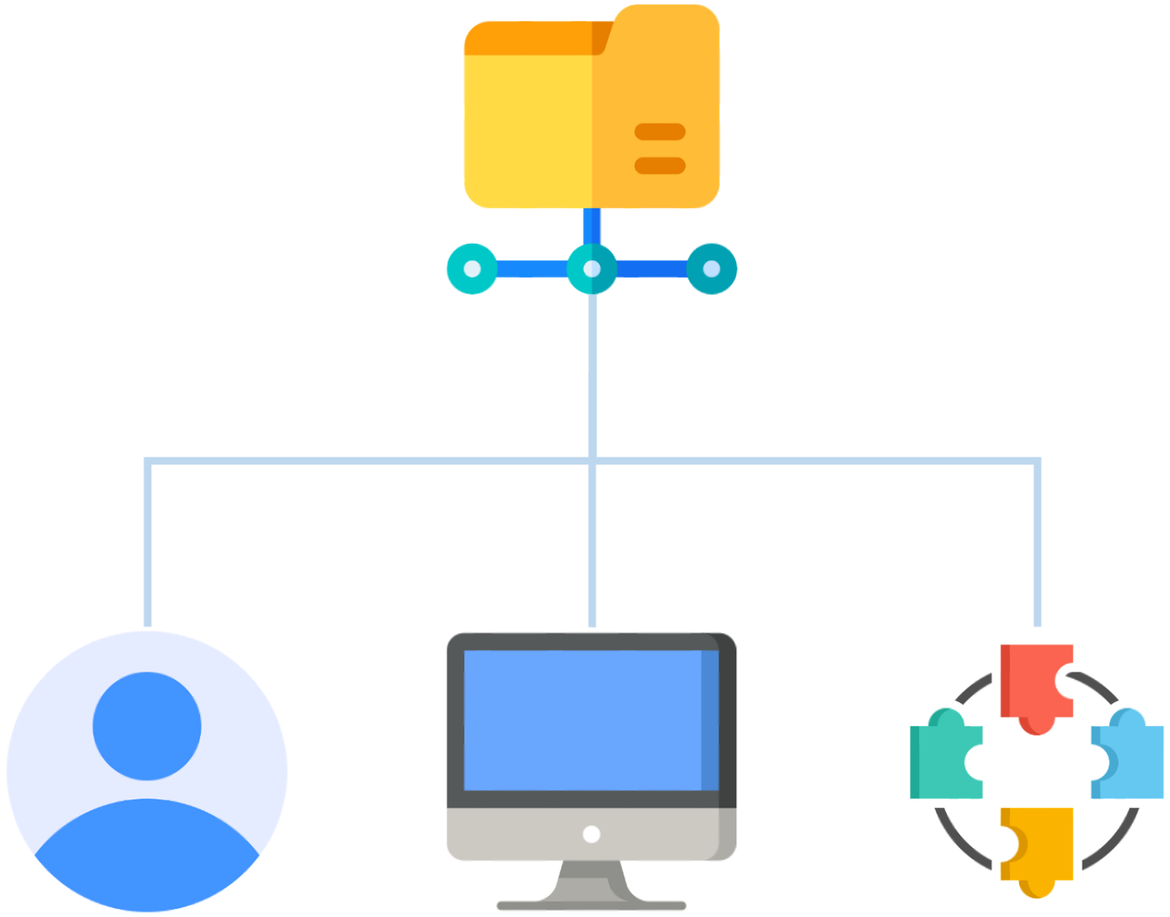
Florin Angelescu
Azure Architect

Directory services

- Active Directory
  - Conventional tool
  - On-premises Windows environments

- Microsoft Entra ID
  - Cloud tool
  - User-friendly online version

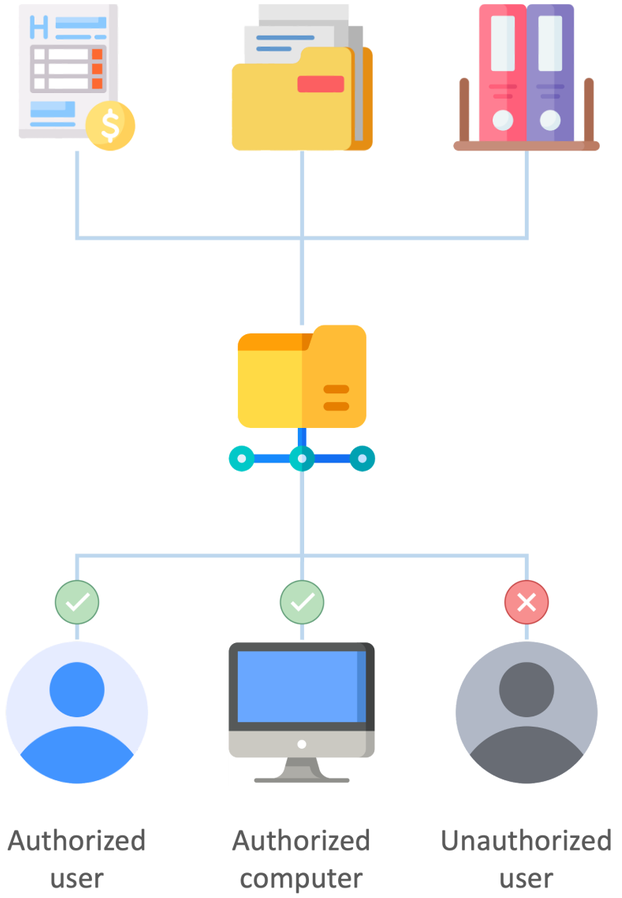
Active Directory (AD)



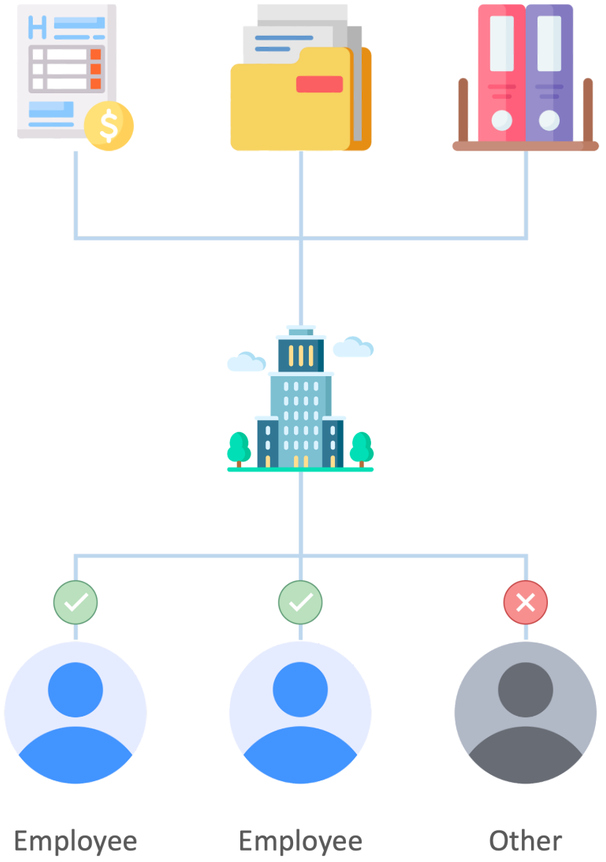
- Address book for an organization's assets
- Organize and store information about:
  - Users
  - Computers
  - Resources
- Centralized identification service

Active Directory (AD)

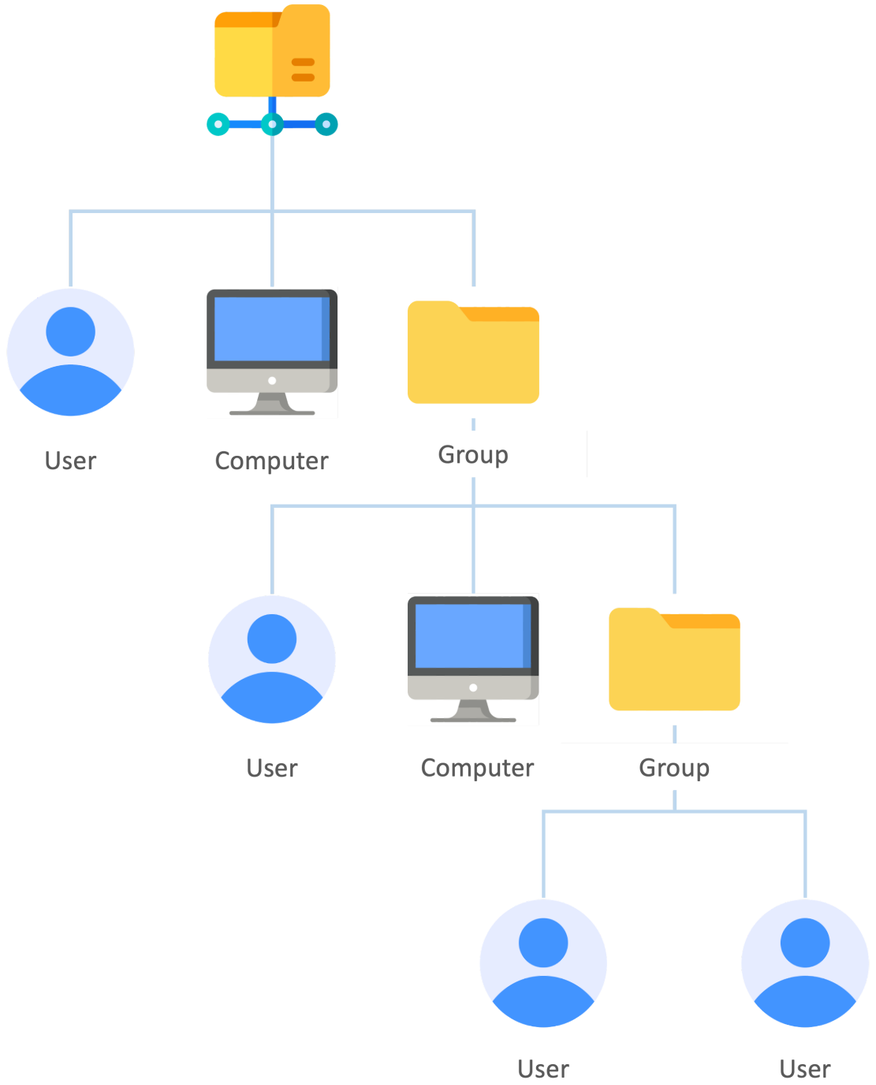
- Only authorized users can access



- Similar to how employees have building access



AD structure



Azure directory services

- Managing user identities and access
- Secure access to applications and resources
- Microsoft Entra ID

Microsoft Entra ID

- Simplifyies online experience
- Single set of login credentials for services
- Eliminates the need to remember multiple usernames and passwords

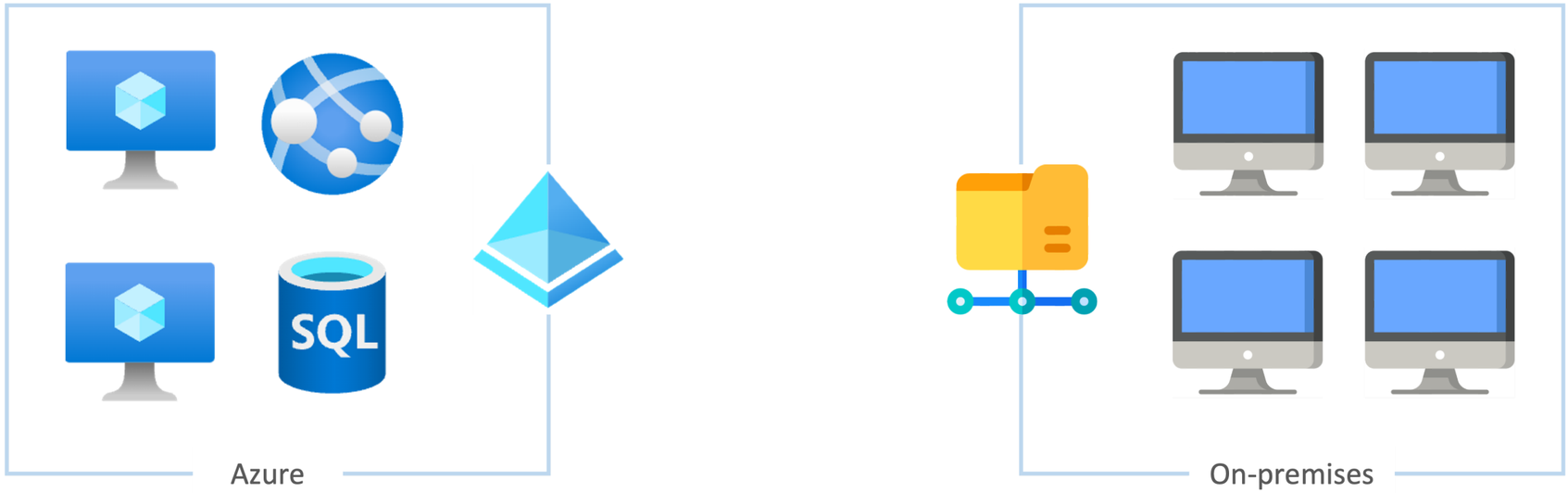
Microsoft Entra ID use cases

- Authentication
- Single Sign-On (SSO)
- Application management
- Device management and access policies

External identities

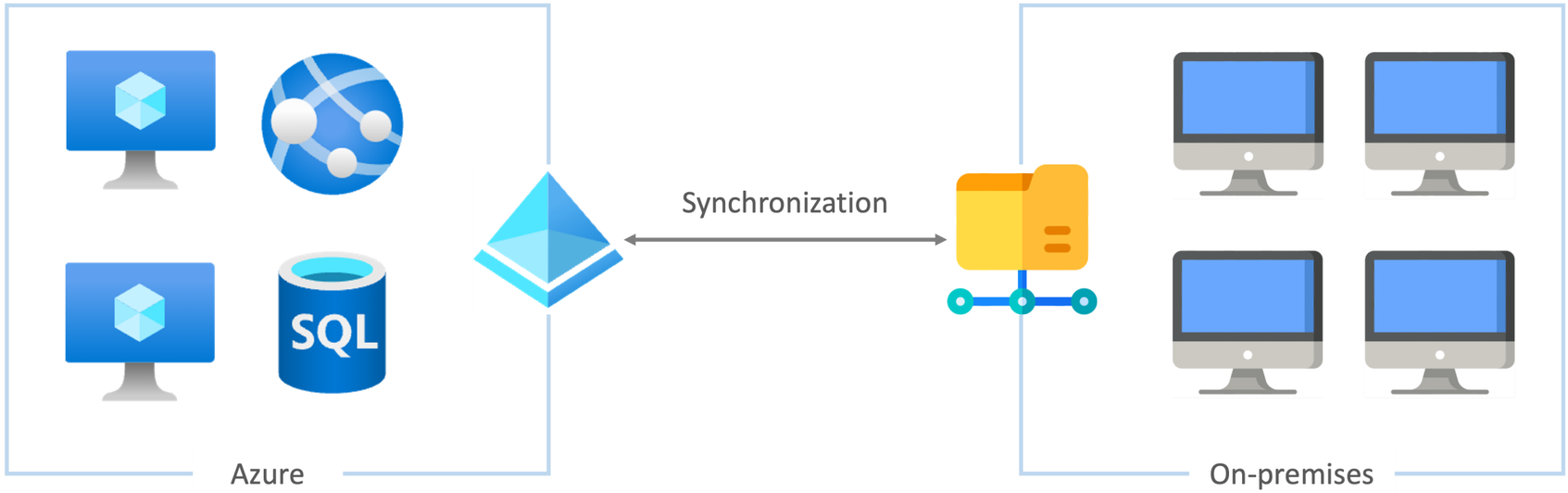
- Improves collaboration using external identities
- Beneficial when working with external partners
- Simplifies resource access without the need for new user accounts

Hybrid environments



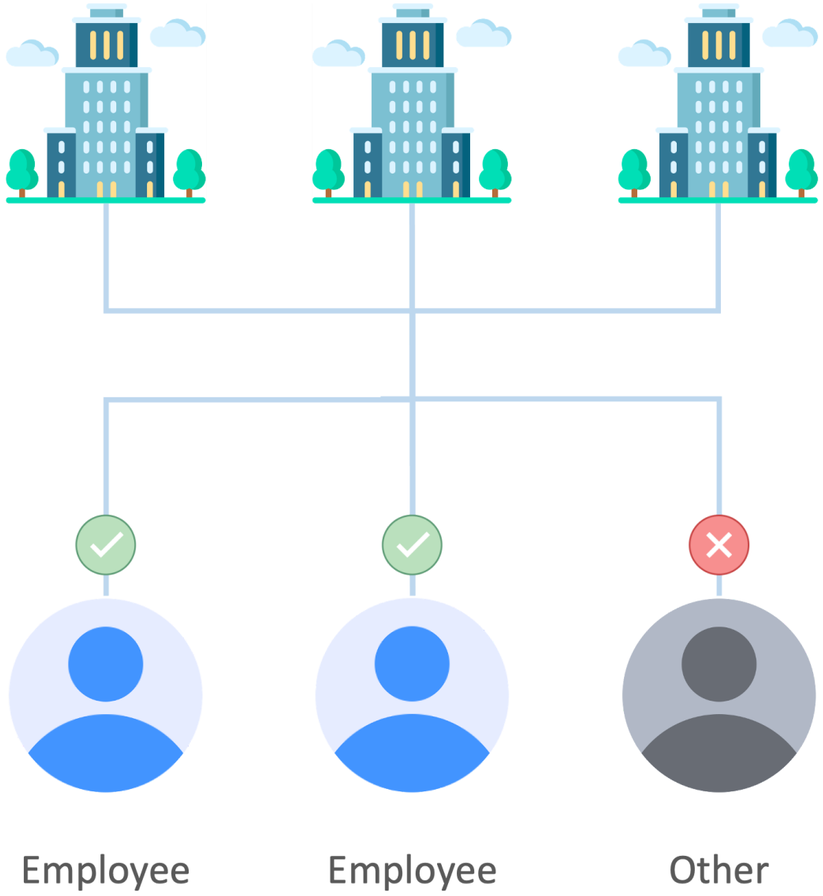
- Infrastructure that combines elements of both on-premises and cloud-based services
- Leverage the benefits of both on-premises and cloud solutions
- Allows businesses to transition gradually to the cloud

Hybrid environments



- Active Directory and Microsoft Entra ID can work together
- Share information about users, computers, groups, and their properties
- Synchronization enables access to resources in both cloud and local networks

Hybrid environments



Conclusion

Microsoft Entra ID

- Essential for efficient and secure identity and access management in the cloud
- Provides a unified set of credentials for accessing various resources

Let's practice!

UNDERSTANDING MICROSOFT AZURE ARCHITECTURE AND SERVICES

Azure identity services and access control

UNDERSTANDING MICROSOFT AZURE ARCHITECTURE AND SERVICES

Florin Angelescu
Azure Architect

datacamp

Azure authentication methods

- Authentication = Verifying the identity of an individual, service, or device
- Presenting credentials to prove who they are

Multi-factor authentication (MFA)

- Requires an additional form of identification during sign-in
- Safeguards against unauthorized access, even when password has been compromised
- Provides additional security by requiring two or more elements to fully authenticate

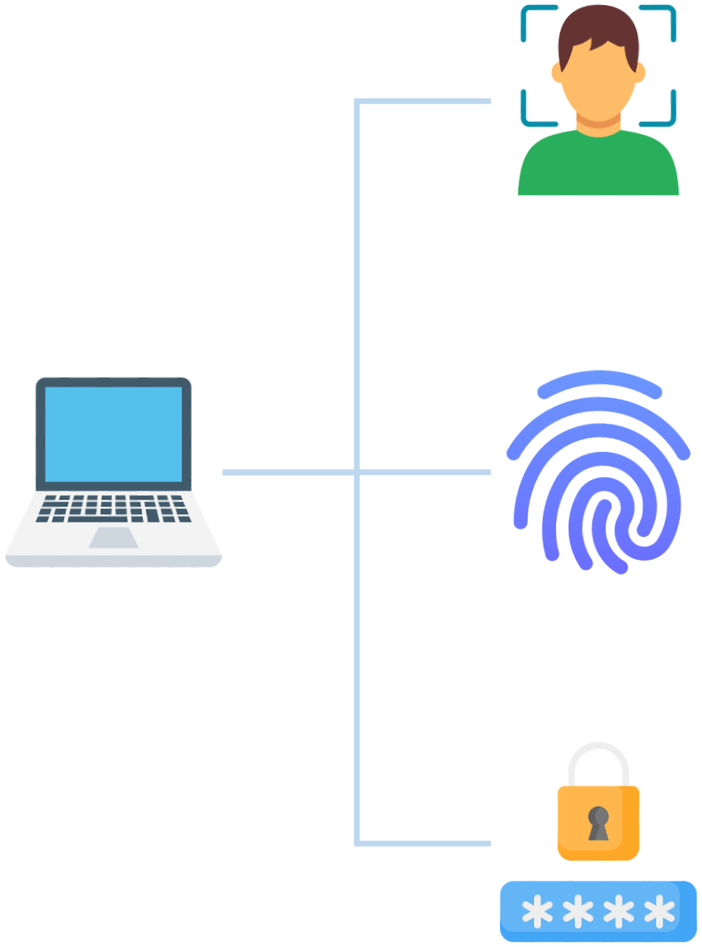
Multi-factor authentication

- Code sent to a user's phone
- Biometric property
- Respond to a challenge question

Passwordless authentication

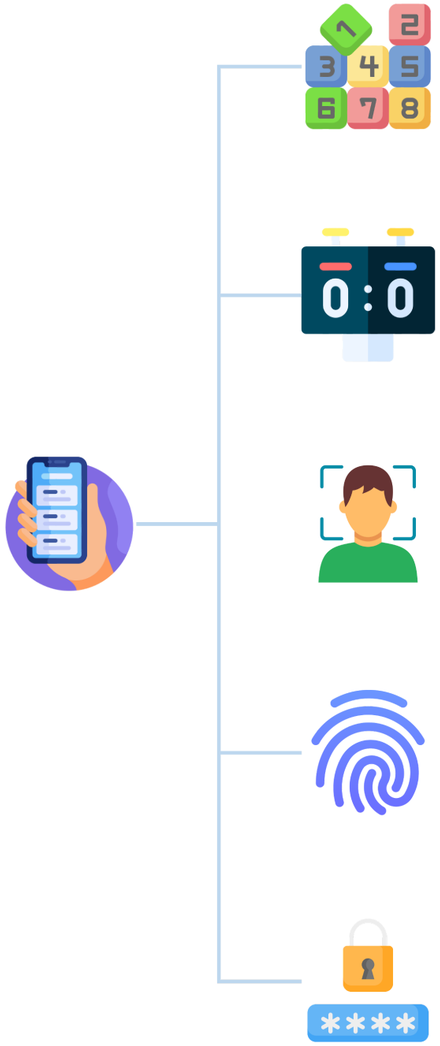
- Eliminate the need for passwords
- Devices need to be registered and associated with a user
- Authentication can occur using something the user has, knows, or is

Windows Hello for Business



- Ideal for individuals with Windows computer
- Users can access their computer using:
  - Fingerprint
  - Face recognition
  - PIN code
- Prevents unauthorized access by others

Microsoft Authenticator App



- Mobile app that offers a MFA options
- Can transform any phone into a secure passwordless tool
- Sign in by:
  - Receiving a notification
  - Matching displayed numbers
  - Confirming with biometric
  - PIN code

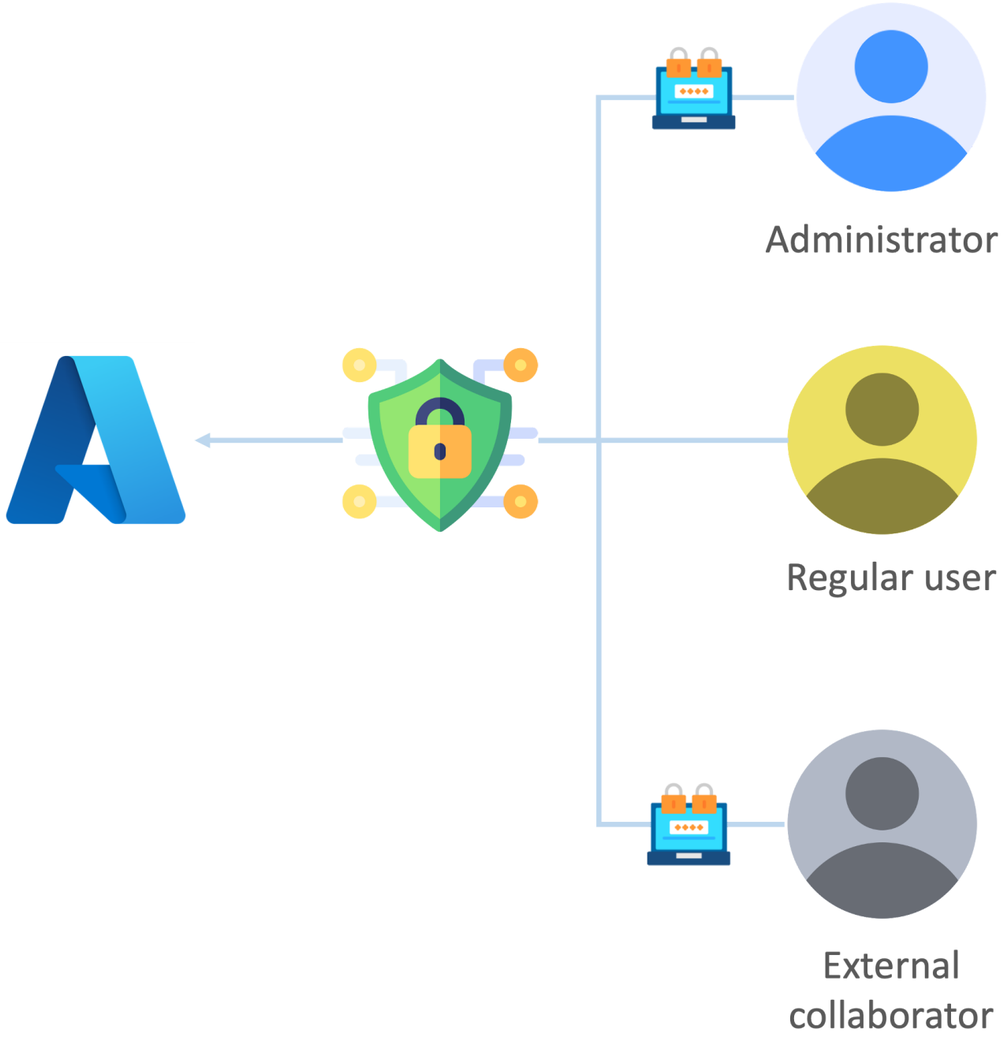
FIDO2 security keys

- Secure and passwordless authentication method
- Open standard by the FIDO Alliance
- Key is available in different forms, including USB devices

Conditional access

- Resource access based on:
  - User identity
  - Location
  - Device
- Collects and analyzes such details at login
- Decides to:
  - Allow access
  - Deny access
  - Enforce MFA

Conditional access use cases

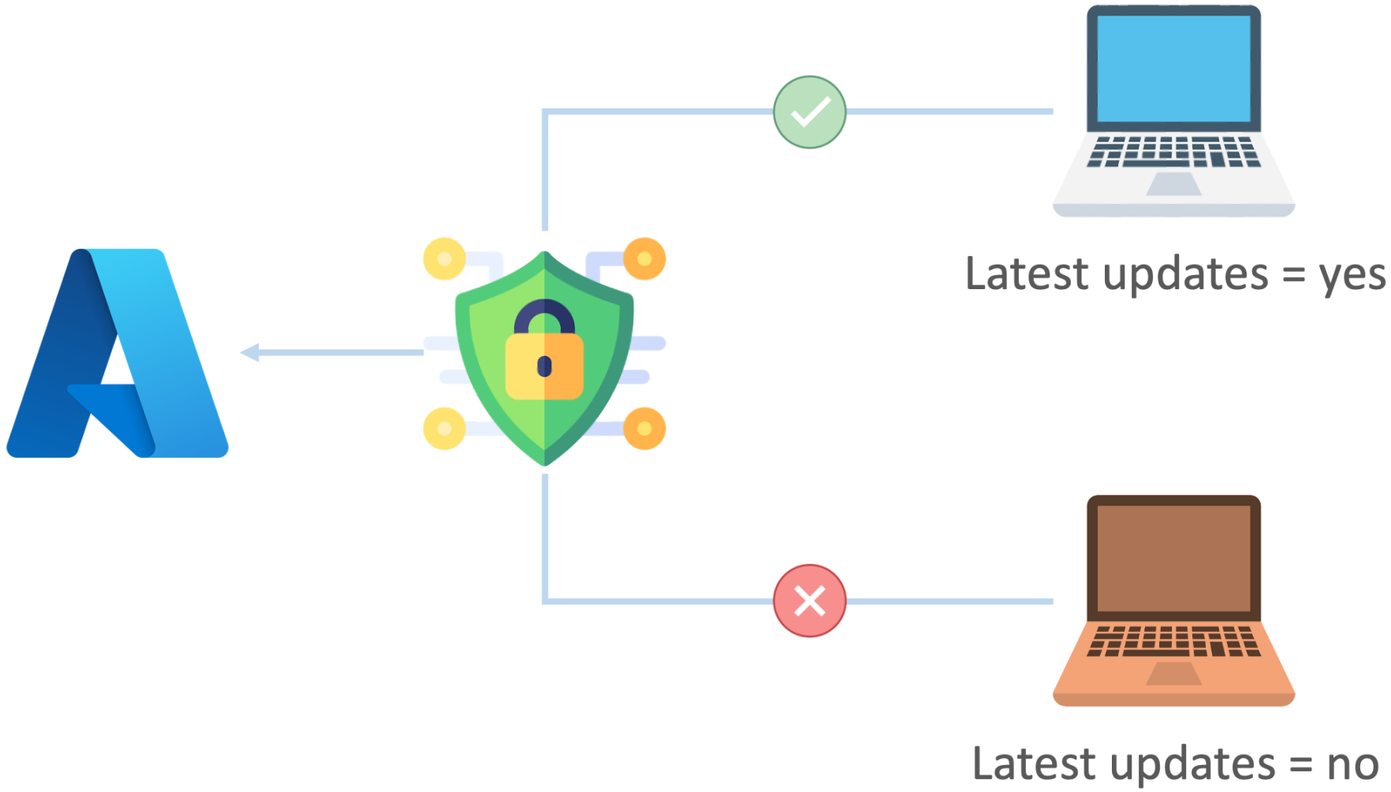


- Enforce MFA based on:
  - Roles
  - Location
  - Network

Conditional access use cases

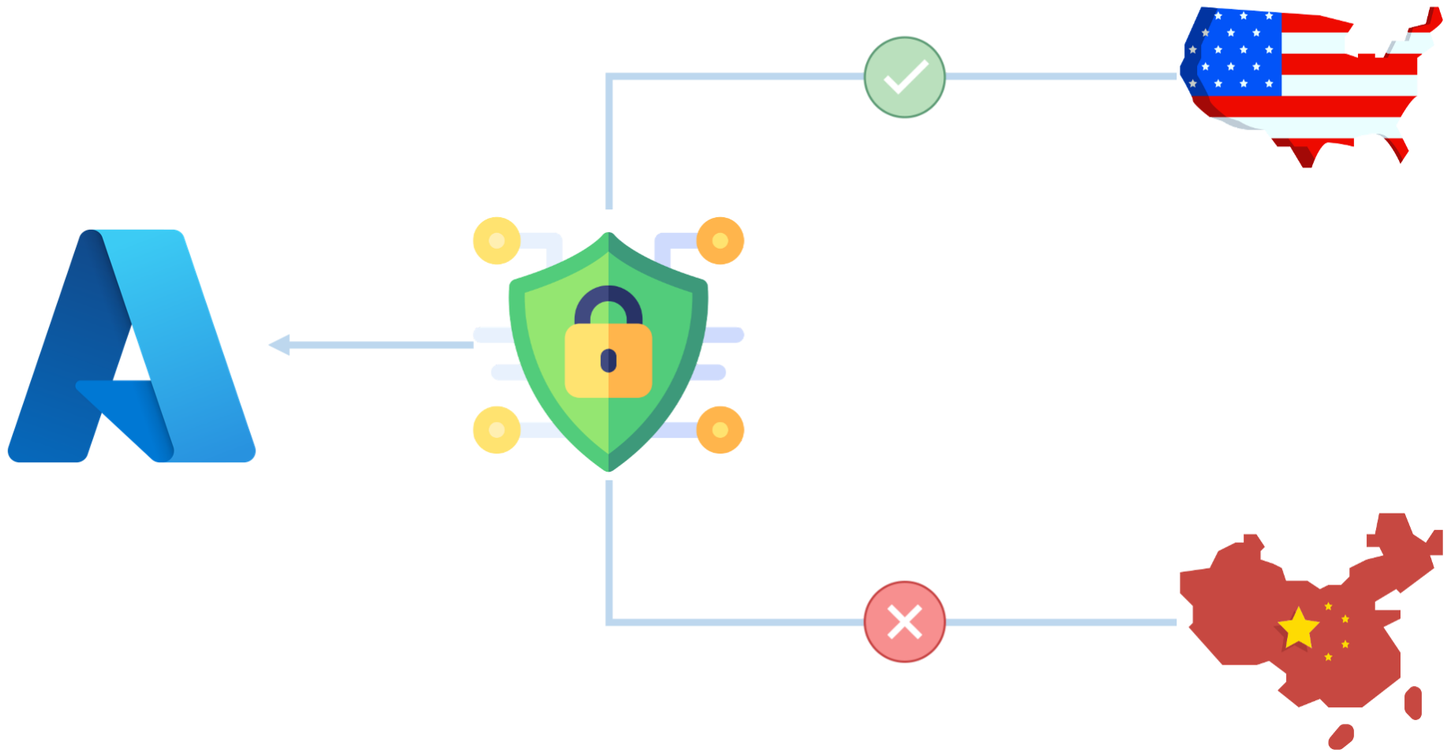
- Allow access to services exclusively through approved client applications
- Control which applications can connect to specific services

Conditional access use cases



- Restrict application access to users on managed devices that meet security and compliance standards

Conditional access use cases



- Prevent access from untrusted sources, including unknown or unexpected locations

Let's practice!

UNDERSTANDING MICROSOFT AZURE ARCHITECTURE AND SERVICES

Create users and groups in Entra ID

UNDERSTANDING MICROSOFT AZURE ARCHITECTURE AND SERVICES

Florin Angelescu
Azure Architect

Let's practice!

UNDERSTANDING MICROSOFT AZURE ARCHITECTURE AND SERVICES

Azure permission model

UNDERSTANDING MICROSOFT AZURE ARCHITECTURE AND SERVICES

Florin Angelescu
Azure Architect

Azure permission model

- Structure and system in place for managing and controlling access to Azure resources
- Two primary models for managing access:
  - Directory roles
  - Role-Based Access Control (RBAC)

What is a role?

- Collection of permissions
- Define the actions an entity can perform on Azure resources
- Azure offers:
  - Predefined roles
  - Creation of custom roles

Directory roles

- Identity and access management within the organization
- Not related to managing access to Azure resources

Directory roles

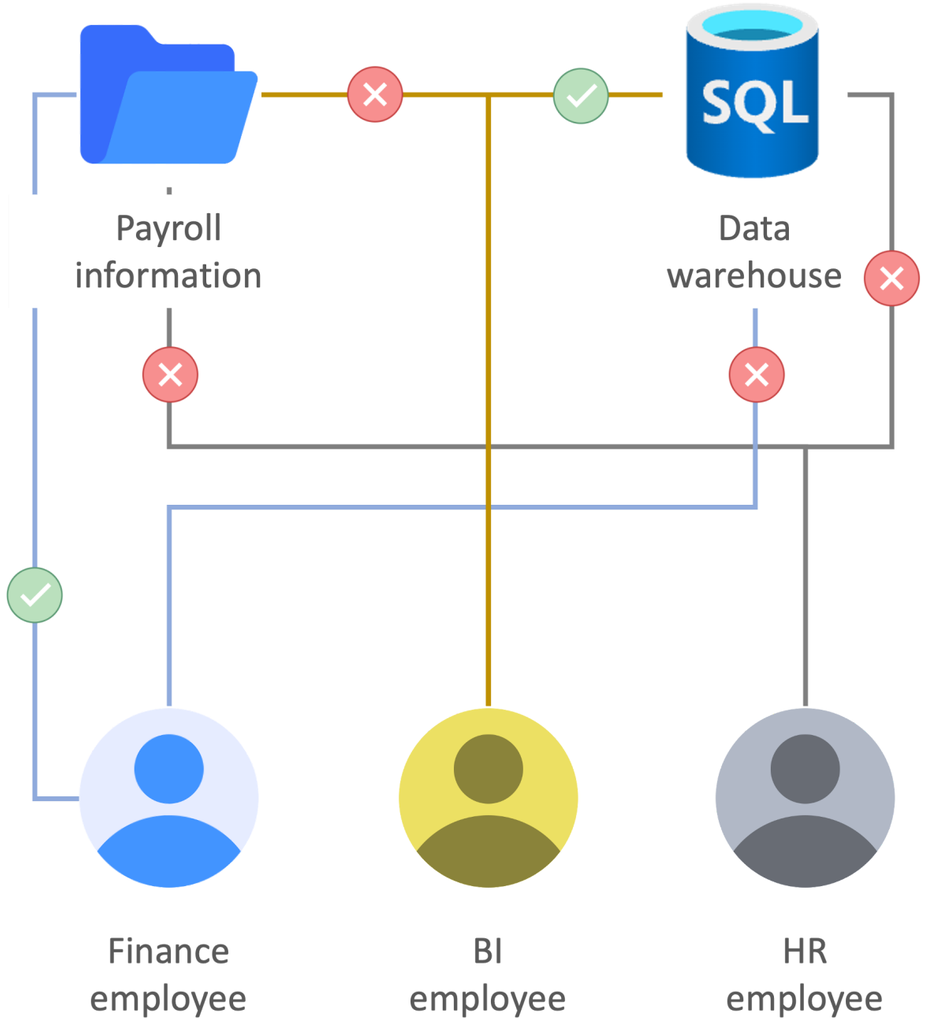
Directory roles use cases

- Administrative tasks related to:
  - User accounts
  - Groups
  - Directory settings
- Example: IT administrator

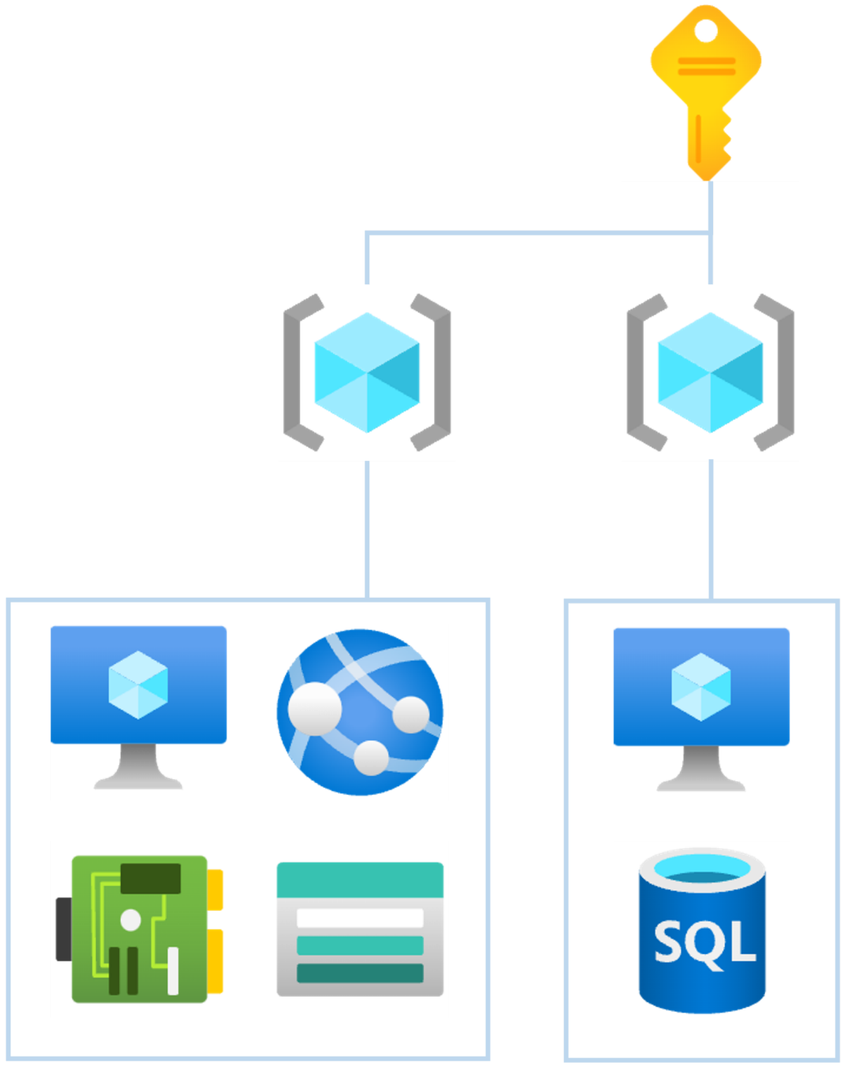
Role-based access control (RBAC)

- Manage access to Azure resources
- Control who can do what within:
  - Subscription
  - Resource group
  - Individual resource
- Assign specific roles
- Assign only the necessary permissions

RBAC use cases



RBAC inheritance



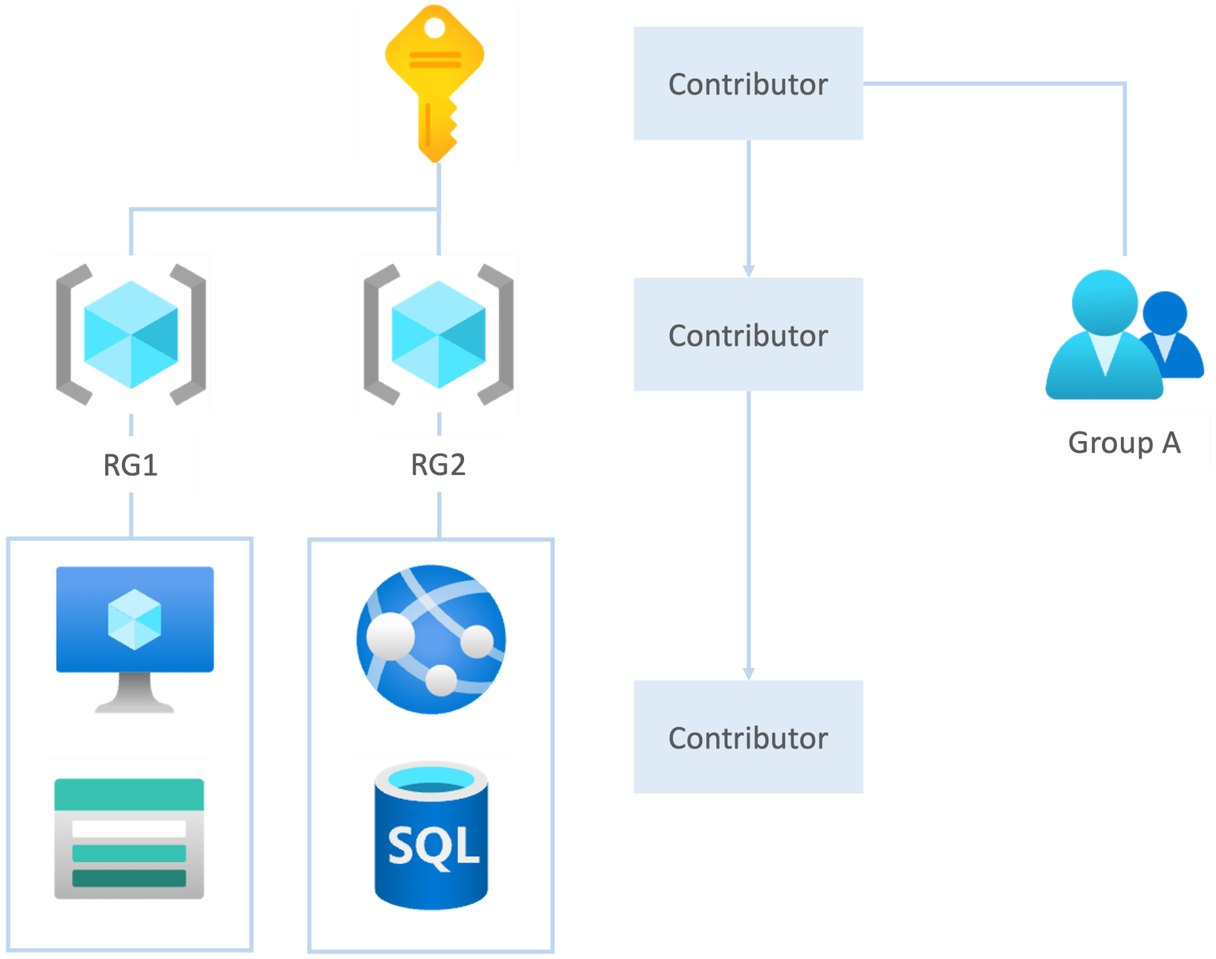
Subscriptions

Resource groups

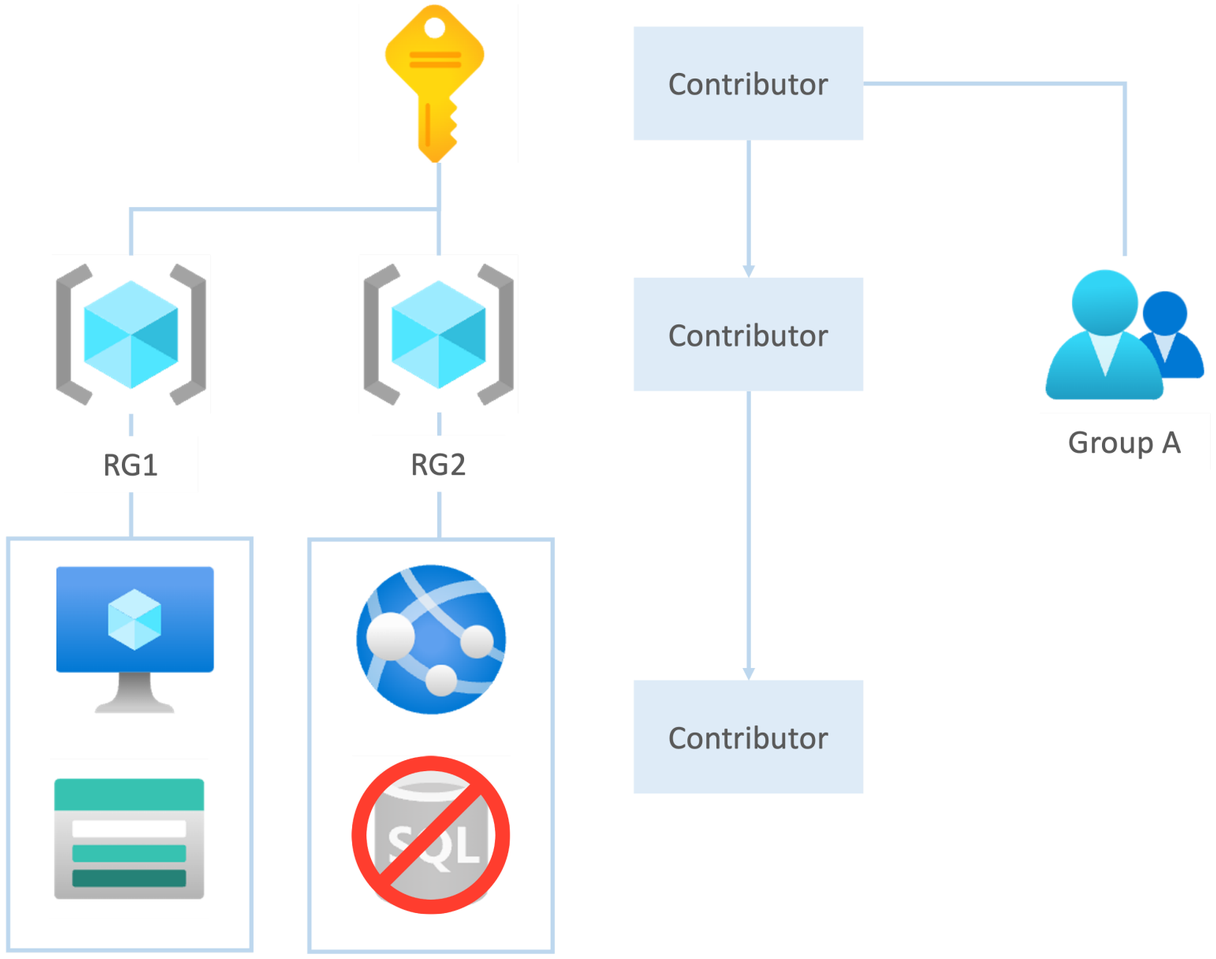
Resources

- Permissions are propagated through different levels of the resource hierarchy
- Permissions assigned at a higher level are automatically inherited by lower levels

RBAC inheritance



RBAC inheritance



Let's practice!

UNDERSTANDING MICROSOFT AZURE ARCHITECTURE AND SERVICES

Configure Azure permissions

UNDERSTANDING MICROSOFT AZURE ARCHITECTURE AND SERVICES

Florin Angelescu
Azure Architect

datacamp

Let's practice!

UNDERSTANDING MICROSOFT AZURE ARCHITECTURE AND SERVICES

Cloud security in Azure

UNDERSTANDING MICROSOFT AZURE ARCHITECTURE AND SERVICES

Florin Angelescu
Azure Architect

datacamp

Cloud security

- Protection of data, applications, and infrastructure
- Involves practices like:
  - Data encryption
  - Identity management
  - Network security
  - Compliance adherence
  - Measures to detect and respond to security incidents

Cloud security

- Responsibility is shared between the cloud service provider and the users
- Aims to ensure the confidentiality, integrity, and availability of information

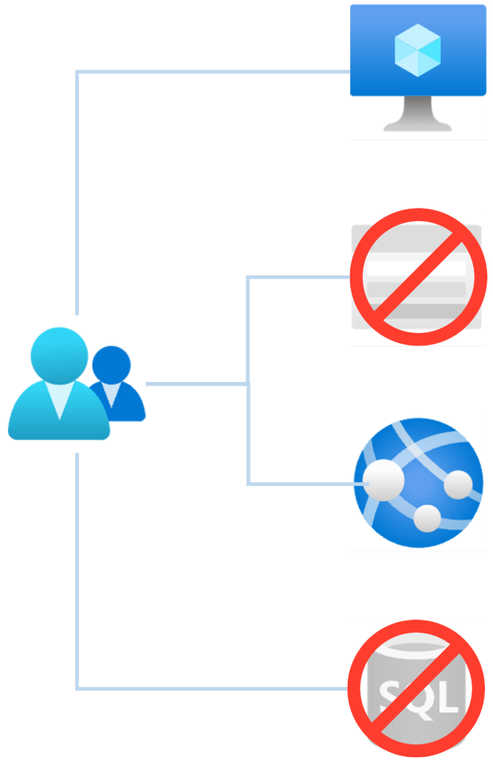
Zero trust model

- Assumption of a potential breach
- Safeguards resources accordingly
- Verifies each request as if it originated from an unsecured network

Zero trust - explicit verification

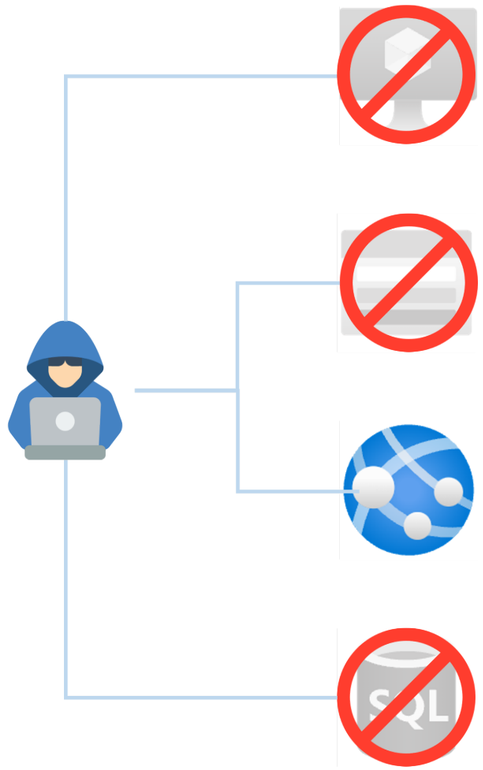
- Always authenticate and authorize based on all available channels

Zero trust - least privilege access



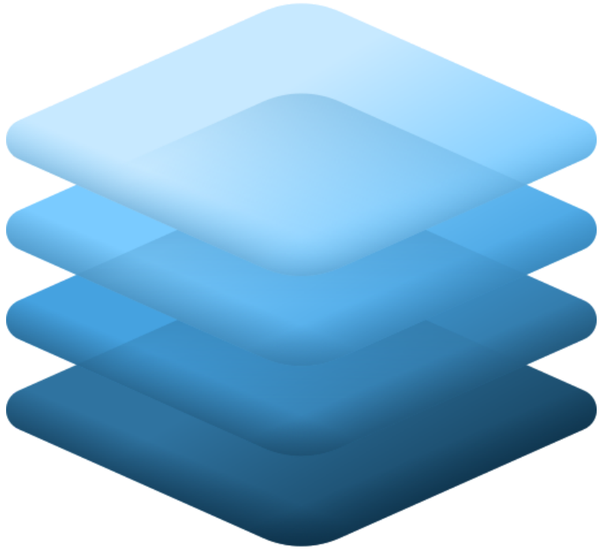
- Users should only be granted access to the resources and permissions essential for their specific job roles

Zero trust - assume breach



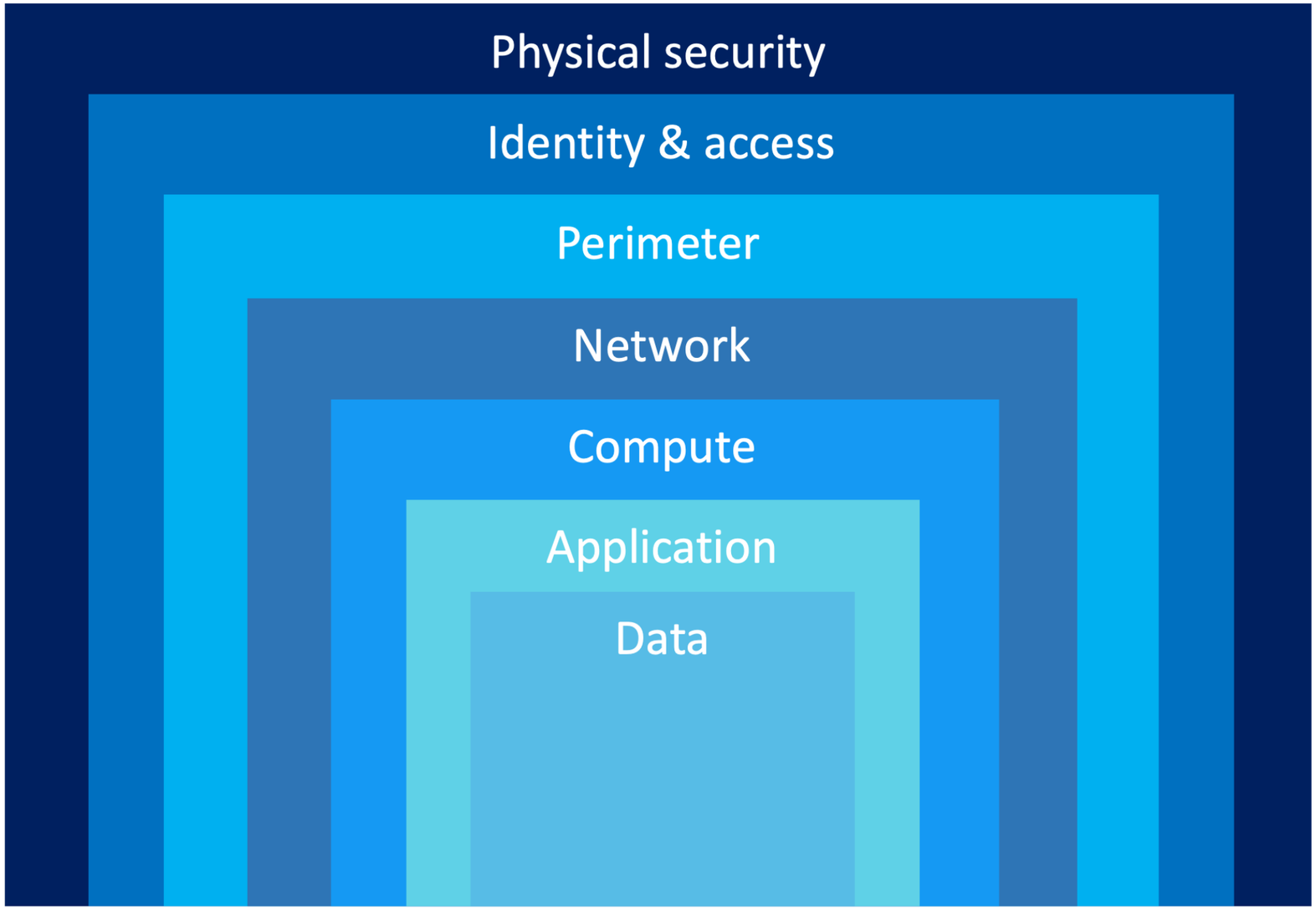
- Determined attackers may find a way in
- Minimize the impact of a breach

Defense-in-depth



- Safeguard resources and prevent unauthorized access and information theft
- Employs multiple layers of mechanisms to block the progress of an attack
- Central data is surrounded by protective layers to ensure its security

Defense-in-depth layers



Microsoft Defender for Cloud

- Monitoring tool for security posture management and threat protection
- Provides guidance and notifications to enhance security
- Integrates into Azure natively

Assess, secure and defend

Asses

- Identify and track vulnerabilities

Secure

- Strengthen resources and services

Defend

- Detect and resolve threats

Importance of cloud security

- Foundation of trust in our digital landscape
- Protects data, applications, and systems
- Ensures confidentiality, integrity, and availability

Let's practice!

UNDERSTANDING MICROSOFT AZURE ARCHITECTURE AND SERVICES

Azure Architecture and Services

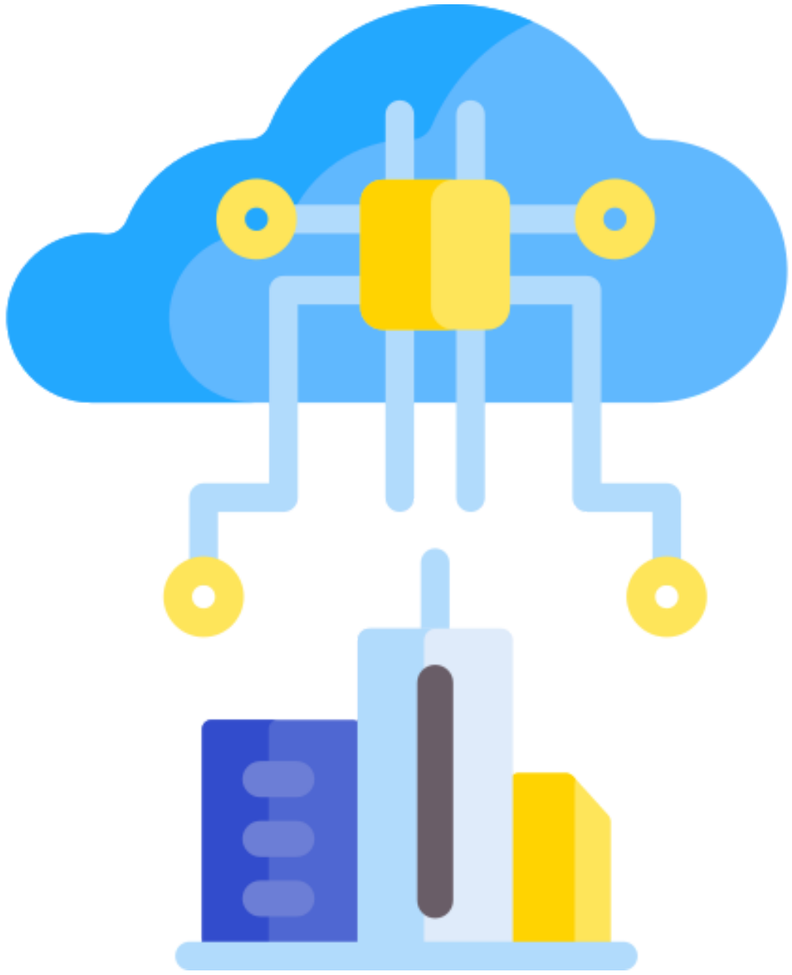
UNDERSTANDING MICROSOFT AZURE ARCHITECTURE AND SERVICES

Florin Angelescu
Azure Architect

datacamp

Wrap-up

Keep exploring



Let's practice!

UNDERSTANDING MICROSOFT AZURE ARCHITECTURE AND SERVICES