Module 1: Introduction to Azure Identity and Access Management

by Mayowa Bodunwa

Module Objectives:

- **Module1-1:** Overview of Identity and Access Management
- **Module 1-2:** Understanding Azure IAM and its importance
- **Module 1-3:** Azure AD as the foundation of Azure IAM

Overview of Identity and Access Management

Identity and access management ensures that the identity which could be people, machines, and software components get access to the right resources at the right time. First, the person, machine, or software component proves they're who or what they claim to be. Then, the person, machine, or software component is allowed or denied access to or use of certain resources.

Module 1-1

Components of Identity and Access Management

A **digital identity** is a collection of unique identifiers or attributes which represent the following categories.
- Human Identities: A person e.g. an employee.
- Workload Identities: Software workloads or components e.g. an application
- Device Identities: Devices e.g. mobile phone or computer

Authentication proves the identity of a user, machine, or software component.

Authorization grants or denies the user, machine, or software component access to certain resources.

Module 1-1

Components of Identity and Access Management

Authentication	Authorization
Confirms users are who they say they are	Validates users have permission to complete the attempted action

Module 1-1

Importance of Identity and Access Management

- Identity management
- Identity federation
- Provisioning and de-provisioning of users
- Authentication of users
- Authorization of users
- Access control
- Reports and monitoring

Further reading: https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/introduction-identity-access-management

Module 1-2

Azure AD as the foundation of Azure's IAM service

Azure Active Directory (Azure AD) is a cloud-based identity and access management service. Azure AD enables your employees access external resources, such as Microsoft 365, the Azure portal, and thousands of other SaaS applications. Azure Active Directory also helps them access internal resources like apps on your corporate intranet, and any cloud apps developed for your own organization.

Further reading: https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

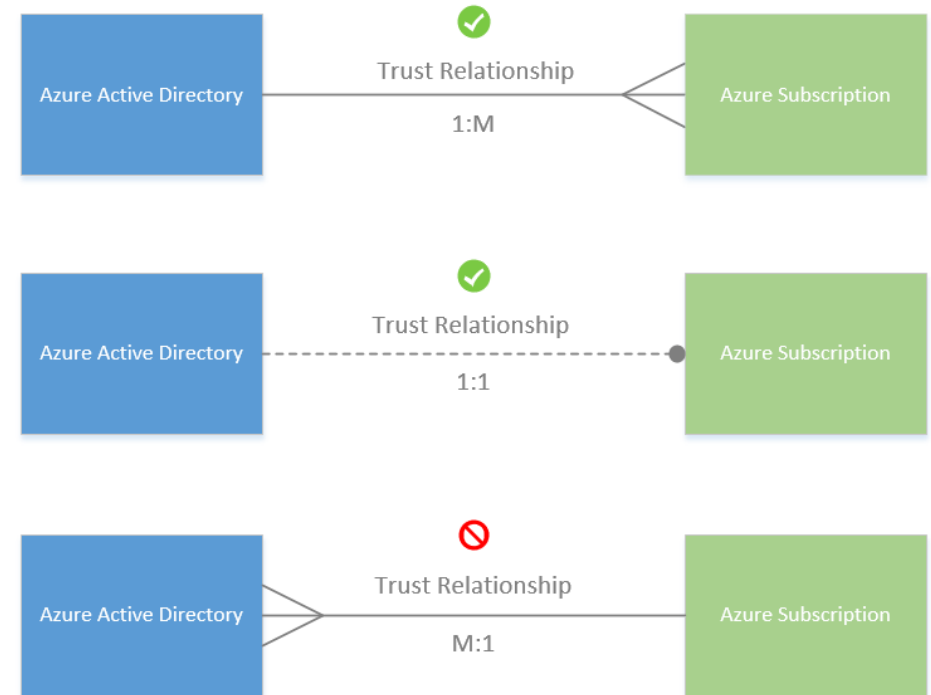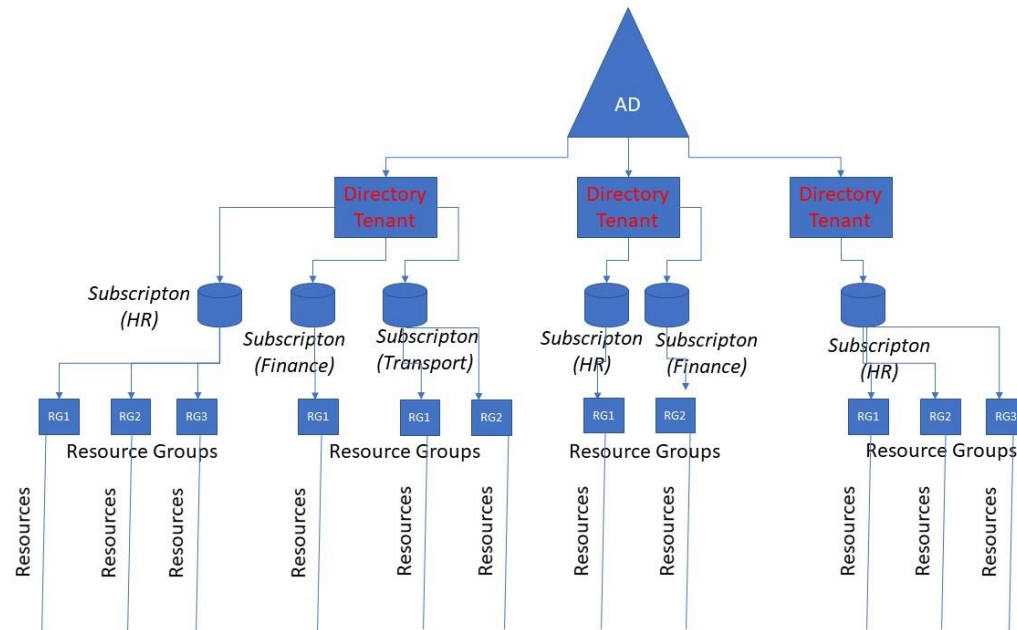**Module 1-3**

Azure AD Architecture Overview

Module 1-3
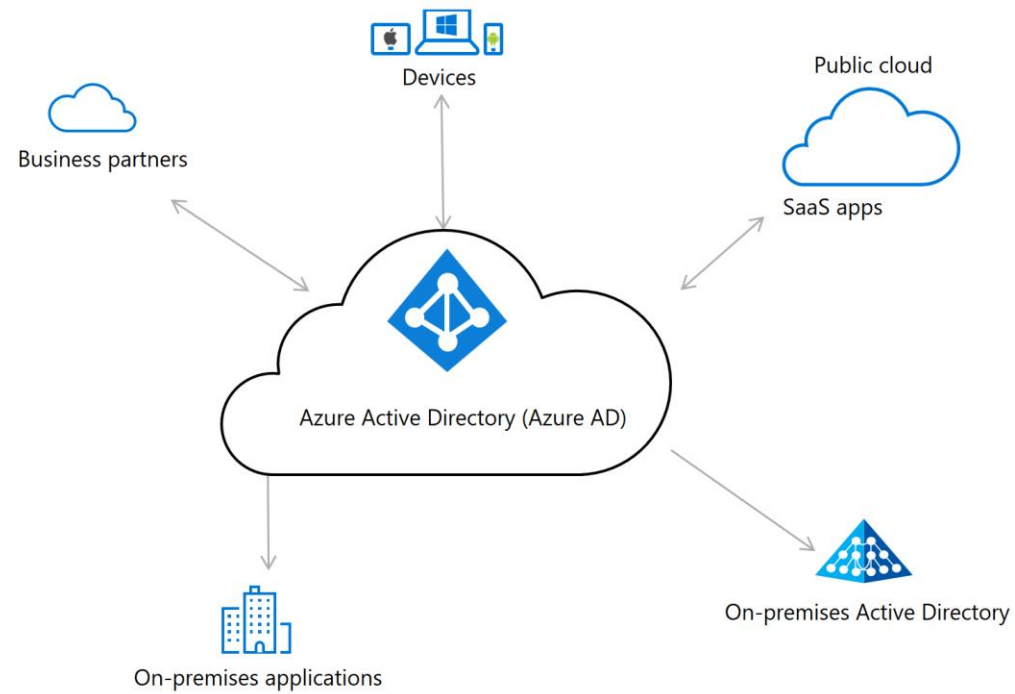
Azure AD Labs

Azure Resource Management Scope Levels:

Azure AD Labs

Tasks:
- Create an Azure AD Directory Tenant
- Create a user in the Azure AD Tenant
- Create a group in the Azure AD Tenant
- Assign a user to the group
- Delete all created resources