CSCI 5902 - Fall 23 - Azure Tutorial

Designed under guidance of Dr. Lu Yang

Harmit Narula

Recap

- Azure DNS
- Bastion
- NAT Gateway
- Azure Private Link
- Service Endpoints
- VNET Peeering
- Hub And Spoke Architecture
- DDoS
- Network Isolation for Azure Resources
- Application Security Groups
- Load Balancer

T8: Azure IAM, RBAC, Security

Identity Fundamentals

- A digital identity is a collection of unique identifiers or attributes that represent a human, software component, machine, asset, or resource in a computer system. An identifier can be:
    - An email address
    - Sign-in credentials (username/password)
    - Bank account number
    - Government issued ID
    - MAC address or IP address
- Identities are used to authenticate and authorize access to resources, communicate with other humans, conduct transactions, and other purposes.

Authentication & Authorization

- 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.

Source: [2]

Identity Provider

- An identity provider creates, maintains, and manages identity information while offering authentication, authorization, and auditing services.
- Microsoft Entra ID is an identity provider, other examples are: Google, Amazon, LinkedIn, Github

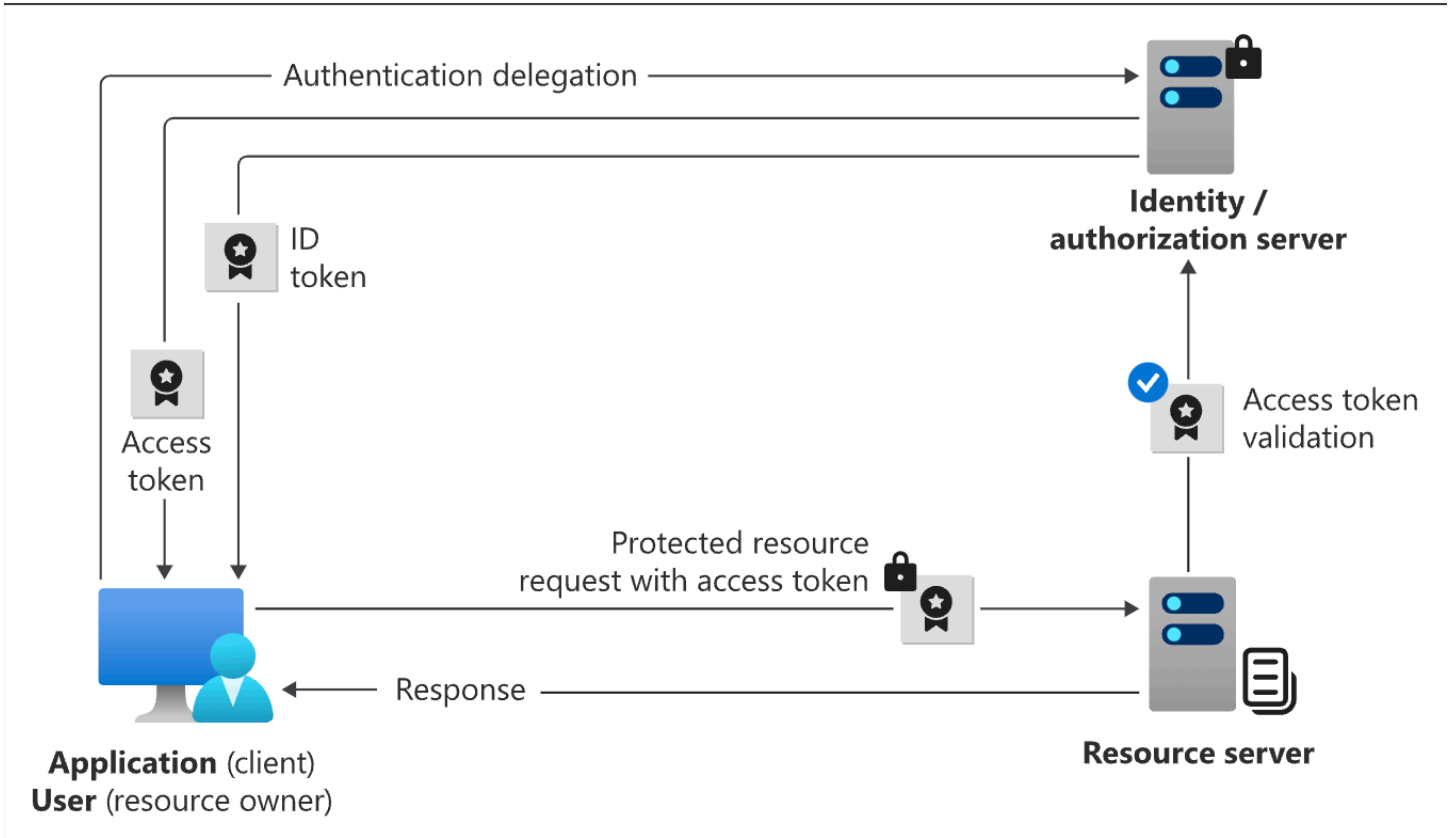
Source: [2]

Identity and Access Management

IAM

- Identity and access management ensures that the right people, machines, and software components get access to the right resources at the right time.
- Core functionalities of IAM:
    - Identity Management
    - Identity Federation
    - Provisioning and deprovisioning users
    - Authentication
    - Authorization
    - Access Control
    - Reports and Monitoring

Working of IAM



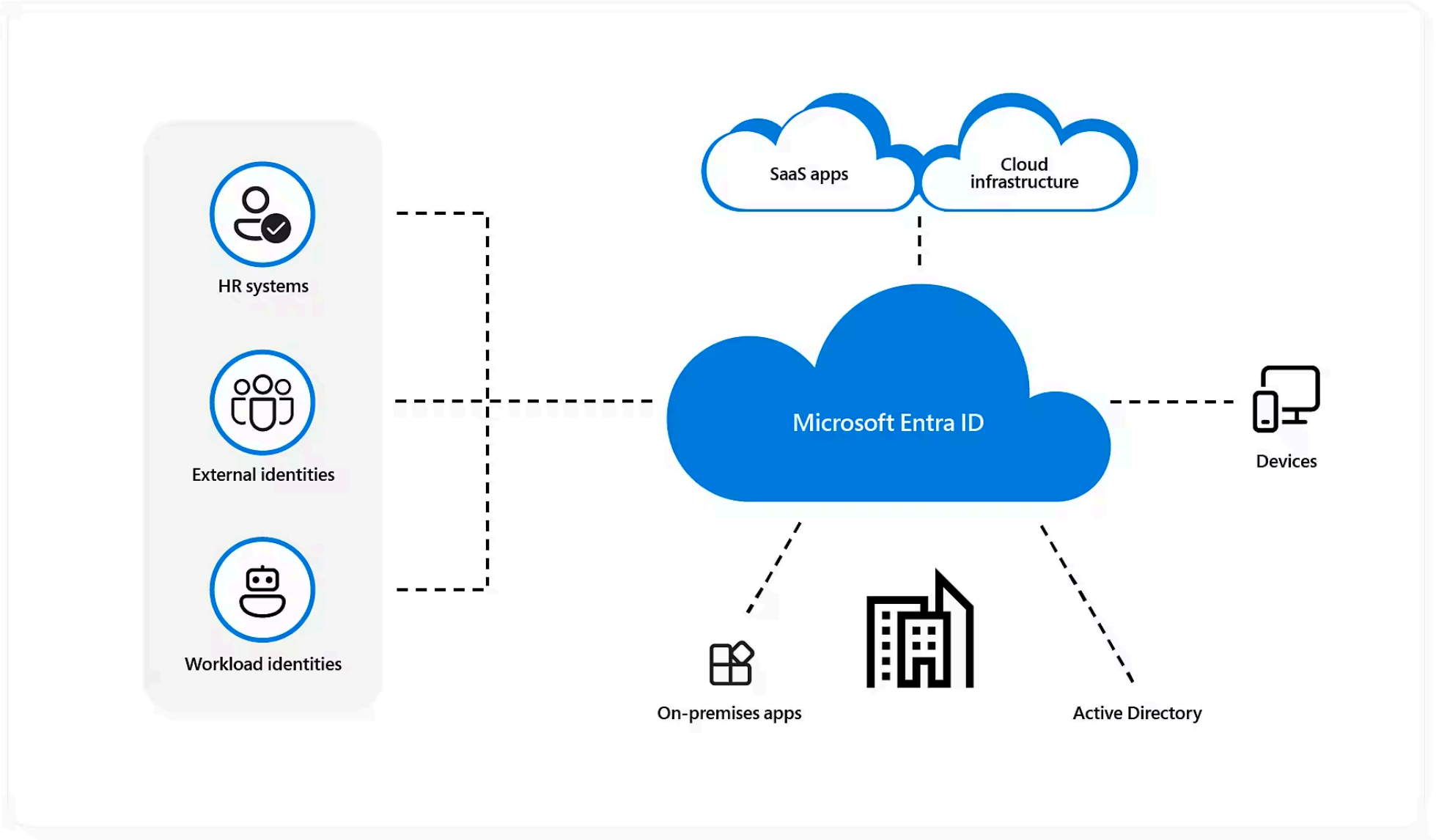
Source: [3]

Azure Active Directory

Now called as Microsoft Entra ID

Microsoft Entra ID

- Microsoft Entra ID is a cloud-based identity and access management service.
- Can be used to access M365, Azure portal, SaaS applications, internal apps(on-premise), cloud hosted apps.
- Features:
    - Secure Adaptive Access: Protect access to resources and data using strong authentication and risk-based adaptive access policies without compromising user experience.
    - Seamless User Experience: Provide a fast, easy sign-in experience across your multicloud environment to keep your users productive, reduce time managing passwords, and increase productivity.
    - Unified Identity Management: Manage all your identities and access to all your applications in a central location, whether they’re in the cloud or on-premises, to improve visibility and control.


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

Source: [1]

Types of Identities in Microsoft Entra

Identity Types

- User Identity: User identities represent people such as employees and external users.
- Workload Identities: A workload identity is an identity you assign to a software workload. In Microsoft Entra, workload identities are applications, service principals, and managed identities.
    - Managed Identities: System Assigned, User Assigned
- Device Identities: A device is a piece of hardware, such as mobile devices, laptops, servers, or printers.
    - Registered, Joined, Hybrid Joined Devices

Identity Types(Contd.)

- Groups: In Microsoft Entra ID, if you have several identities with the same access needs, you can create a group.
    - Security Groups, Microsoft 365(distribution group)
- Hybrid Identities: A common identity for authentication and authorization to all resources, regardless of location.
    - Microsoft Entra ID Connect Cloud Sync
- External Identities: It refers to all the ways you can securely interact with users outside of your organization.
    - B2B Collaboration, B2B direct connect, Multi-tenant organization

Is Microsoft Entra ID same as Active Directory?

Active Directory vs Microsoft Entra Id

- Microsoft Introduced Active Directory in Windows 2000 to give organizations ability to maange multiple on-premise infrastructure components and systems using a single identity per user.
- Microsoft Entra ID is next level of advancement over AD and can be referred as Identity as a Service(IDaaS) solution which helps organizations manage apps across cloud and on-premises.
- The organizations who were using AD for on-premise systems do they need to recreate identities in Cloud?
  - Microsoft Entra Connect can help them sync identities to the cloud.
- Further reading : https://learn.microsoft.com/en-us/entra/fundamentals/compare

Do we have any benefit of using unified identity management service?

Microsoft Entra ID increases worker productivity and reduces IT friction

Increased end user productivity

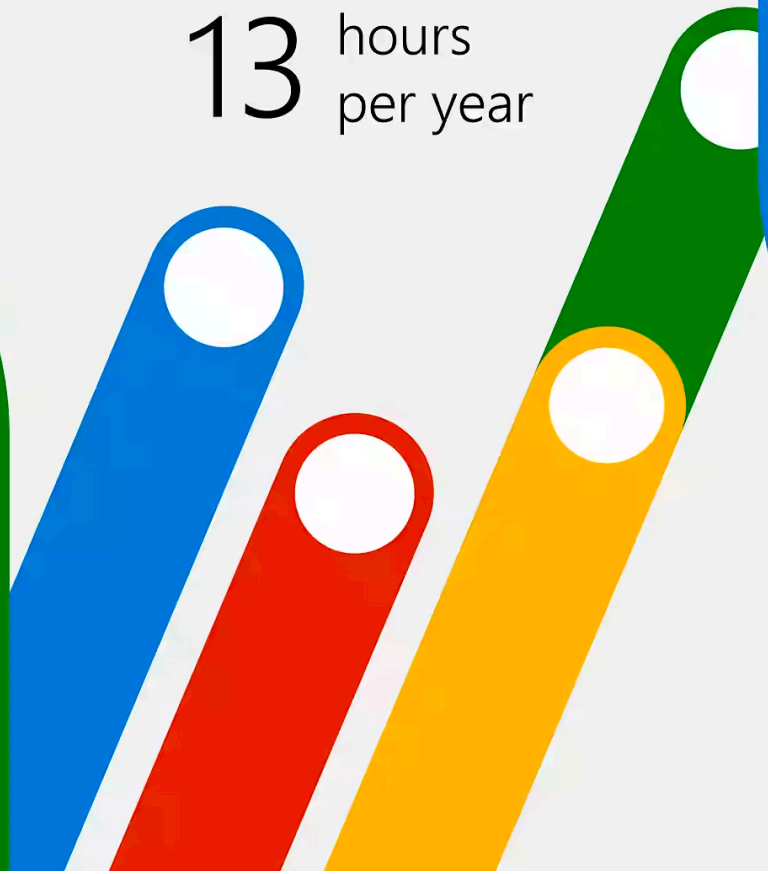
13 hours per year

75%

Reduced password reset requests

50%

Increased IAM team efficiency



FORRESTER®

"The Total Economic Impact™ Of Microsoft Entra" is a commissioned study conducted by Forrester Consulting on behalf of Microsoft published in March 2023.

Azure AD External Identities

Azure AD External Identities

- It is part of Microsoft Entra, provides highly secure digital experience for external users.
- Benefits:
  - SSO simplifies external access.
  - Conditional access and multifactor authentication help protect and govern access.
  - Single identity management platform for internal and external users.
  - Developer tools makes it easier to integrate identity workflow into the apps and services.

IAM Best Practices

Further Reading:
https://learn.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices

Azure AD Domain Services

Azure AD DS

- Azure Active Directory Domain Services is part of Microsoft Entra and helps you use managed domain services - windows Domain Join, group policy, LDAP, Kerbros Authentication - without having to deploy, manage or patch domain controllers.

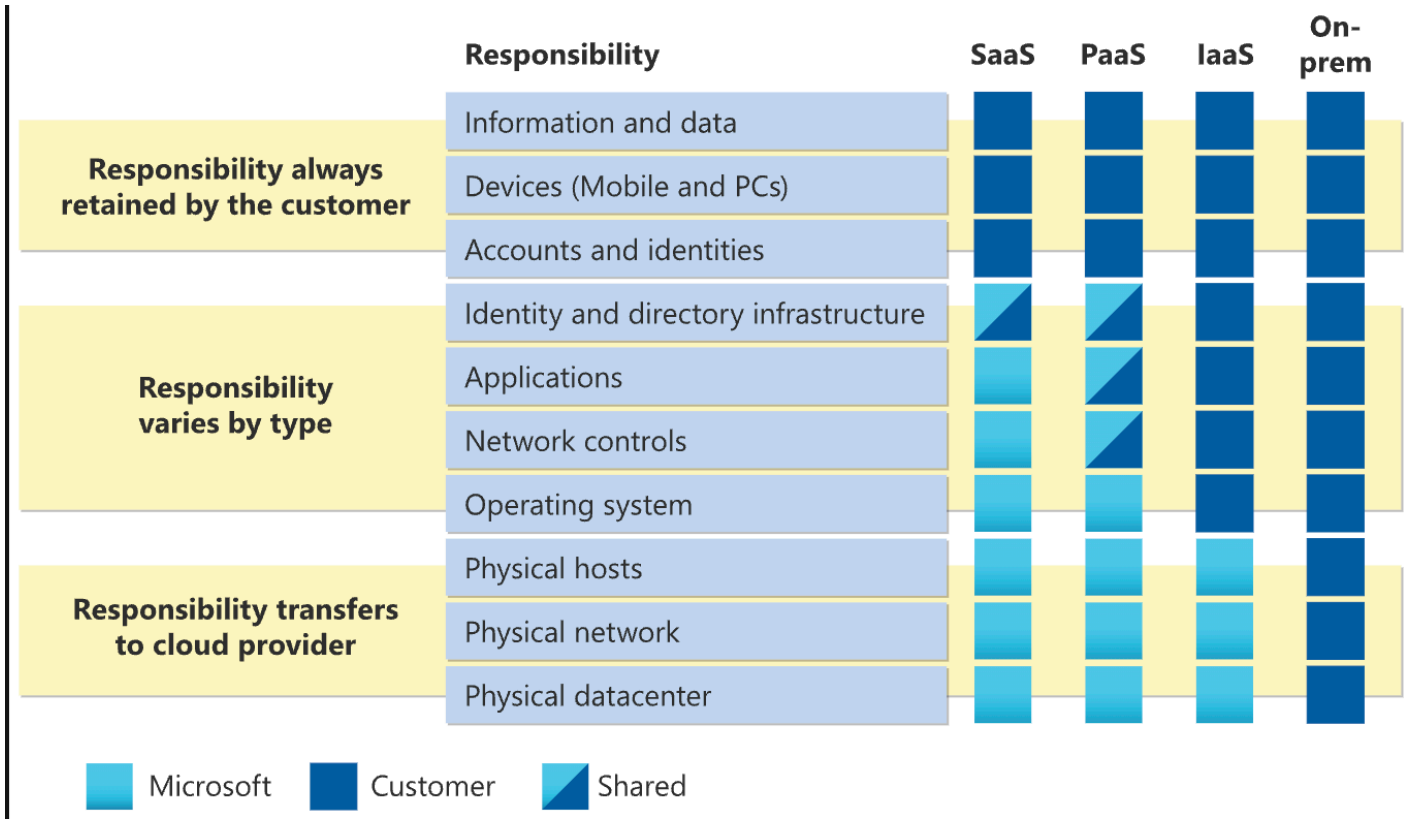
Role Based Access Control(RBAC)

Azure RBAC

- 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.
- By using RBAC we can avoid human errors and automation errors that create security risks.
- Access is restricted based on “Need to Know” and “Least Priviledge” security principles.
- Example built in roles: Reader, Contributor, Owner, Security Reader

Azure Security

Shared Responsibility Model



Azure Security Capabilities

- **Microsoft Sentinel**
  - Microsoft Sentinel is a scalable, cloud-native, security information and event management (SIEM) and security orchestration, automation, and response (SOAR) solution.
  - Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for attack detection, threat visibility, proactive hunting, and threat response.
- **Microsoft Defender for Cloud**
  - It helps you prevent, detect, and respond to threats with increased visibility into and control over the security of your Azure resources.
  - Defender for Cloud helps with security operations by providing you a single dashboard that surfaces alerts and recommendations that can be acted upon immediately.
  - Responsible for Collect and Detect roles whereas Sentinel is responsible for Collect, Detect, Investigate and Respond roles.

Azure Security Capabilities(Contd.)

- **Azure Resource Manager**
  - Azure resource manager enables you to work with the resources in your solution as a group. You can deploy, update, or delete all the resources for your solution in a single, coordinated operation.
- **Application Insights**
  - It is Application Performance Management service.
  - Application Insights creates charts and tables that show you, for example, what times of day you get most users, how responsive the app is, and how well it is served by any external services that it depends on.

Azure Security Capabilities(Contd.)

- **Azure Monitor**
  - It offers visualization, query, routing, alerting, auto scale, and automation on data both from the Azure subscription and each individual Azure resource.
- Azure Monitor Logs
- Azure Advisor
- Key Vault
- Web Application Firewall(WAF) - Available under Application Gateway, helps protect web applications from common web-based attacks like SQL injection, cross-site scripting attacks, and session hijacking. It is preconfigured with OWASP 10 rules.

It’s a wrap

References

[1] https://www.microsoft.com/en-ca/security/business/identity-access/microsoft-entra-id#overview

[2] https://learn.microsoft.com/en-us/entra/fundamentals/identity-fundamental-concepts

[3] https://learn.microsoft.com/en-us/entra/fundamentals/introduction-identity-access-management

[4] https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility