0- Terminologies

`#Entra_ID`: Identities are stored in Microsoft Entra ID.

`#Tenant`: Dedicated and trusted instance of Microsoft Entra ID.

- automatically created when your organization signs up for Microsoft cloud service subscription.
- In azure, tenant represent a single organization.

`#Single_tenant`: Azure tenants that access other services in a dedicated environment are considered as Single tenant.

`#multi-tenant`: source.

- B2B Collaboration.
- B2B Direct Connect.
- Cross Tenant Sync.

`#Entra_Directory`: Every tenant has a dedicated and trusted Microsoft Entra directory.

- Container which includes all the users, groups and apps.
- Used to perform identity and access management functions for tenant resources.
- source

`#Custom_domain`: Every Microsoft Entra directory comes with an initial domain name, for example `domainname.onmicrosoft.com`.

- In additional to that initial domain name, you can also add your org's domain names.

Azure Entra ID and Entra_Directory

- So an `#Entra_Id` is a service which provides a single platform for identity and access management.

A `#tenant` is a trusted instance of an Entra ID.

`#tenant_and_directory`

- ! There can be exist only one directory in a tenant at a time.
- A `#Entra_Directory` is a container containing users, groups and apps. And there exists only one directory for a single tenant.
- Philosophy of having only 1 `#Entra_Directory`:
  - Single source of truth

- #Entra_ID is designed to be a single source of truth for all identity information within a tenant.
- Having multiple directories could create confusion and inconsistency
- Adding support for multiple directories would require significate changes and could impact the scalability.

"Pasted image 20231208162235.png" is not created yet. Click to create.

Both Entra ID and Entra directory play crucial roles in identity and access management (IAM), but they serve different purposes:

Entra ID:

- #Entra_ID provides the overall **IAM platform** with a comprehensive set of features, including:
  - User provisioning and management
  - Single sign-on (SSO)
  - Multi-factor authentication (MFA)
  - Conditional access
  - Identity governance
  - Application access management
  - Identity protection

Entra Directory:

- #Entra_Directory acts as the **storage container** within Entra ID for a specific tenant. It stores all identity information relevant to that tenant, including:
  - Users
  - Groups
  - Applications
  - Devices

Think of it like this:

- #Entra_ID is like a **large library** with various books and resources representing IAM functionalities.
- #Entra_Directory is like a **specific section within the library** holding the curated collection of books (users, groups, apps) relevant to a particular tenant.

While #Entra_Directory stores the actual #identity information, it relies on #Entra_ID's broader IAM capabilities for managing and securing those identities.

Here's a table summarizing the key differences:

Feature	Entra ID	Entra Directory
Function	Provides IAM platform features	Stores tenant-specific identity informat
Scope	Global service	Specific instance within a tenant
Functionality	User provisioning, SSO, MFA, conditional access, etc.	Adding, editing, deleting identities, assigning permissions

Therefore, Entra ID provides the services for identity and access management, while the Entra directory serves as the storage for tenant-specific identity data. Both work together to enable comprehensive and secure IAM solutions.

"Pasted image 20231208162235.png" is not created yet. Click to create.

Terminology

To better understand Microsoft Entra ID and its documentation, we recommend reviewing the following terms.

Expand table

Term or concept	Description
#Identity	A thing that can get authenticated. An identity can be a user with a username and password. Identities also include applications or other servers that might require authenticati through secret keys or certificates.
#Account	An identity that has data associated with it. You can't have account without an identity.
#Microsoft_Entra_account	An identity created through Microsoft Entra ID or another Microsoft cloud service, such as Microsoft 365. Identities ar stored in Microsoft Entra ID and accessible to your organization's cloud service subscriptions. This account is a sometimes called a Work or school account.
#Account_Administrator	This classic subscription administrator role is conceptually billing owner of a subscription. This role enables you to mar all subscriptions in an account. For more information, see Az roles, Microsoft Entra roles, and classic subscription administrator roles.
#Service_Administrator	This classic subscription administrator role enables you to manage all Azure resources, including access. This role has t equivalent access of a user who is assigned the Owner role at the subscription scope. For more information, see Azure roles Microsoft Entra roles, and classic subscription administrator roles.
#Owner	This role helps you manage all Azure resources, including access. This role is built on a newer authorization system called Azure role-based access control (Azure RBAC) that provides fine-grained access management to Azure resources. F more information, see Azure roles, Microsoft Entra roles, and classic subscription administrator roles.

Term or concept	Description
#Microsoft_Entra_Global_Administrator	This administrator role is automatically assigned to whomever created the Microsoft Entra tenant. You can have multiple Glo Administrators, but only Global Administrators can assign administrator roles (including assigning other Global Administrators) to users. For more information about the vari administrator roles, see Administrator role permissions in Microsoft Entra ID.
#Azure_subscription	Used to pay for Azure cloud services. You can have many subscriptions and they're linked to a credit card.
#Azure_tenant	A dedicated and trusted instance of Microsoft Entra ID. The tenant is automatically created when your organization signs for a Microsoft cloud service subscription. These subscriptio include Microsoft Azure, Microsoft Intune, or Microsoft 365. Azure tenant represents a single organization.
#Single_tenant	Azure tenants that access other services in a dedicated environment are considered single tenant.
#Multi-tenant	Azure tenants that access other services in a shared environment, across multiple organizations, are considered multi-tenant.
#Microsoft_Entra_directory	Each Azure tenant has a dedicated and trusted Microsoft Entra directory. The Microsoft Entra directory includes the tenant' users, groups, and apps and is used to perform identity and access management functions for tenant resources.
#Custom_domain	Every new Microsoft Entra directory comes with an initial dom name, for example `domainname.onmicrosoft.com`. In addition to th initial name, you can also add your organization's domain nam Your organization's domain names include the names you use to business and your users use to access your organization's resources, to the list. Adding custom domain names helps you create user names that are familiar to your users, such as alain@contoso.com.
#Microsoft_account (also called, MSA)	Personal accounts that provide access to your consumer-orient Microsoft products and cloud services. These products and services include Outlook, OneDrive, Xbox LIVE, or Microsoft 3 Your Microsoft account is created and stored in the Microsoft consumer identity account system that's run by Microsoft.