Chapitre 3
Administration de Microsoft Entra ID

1. Introduction

Réussir à administrer un environnement cloud repose sur plusieurs facteurs : le bon dimensionnement de l'infrastructure, le bon choix des licences, l'utilisation d'applications adaptées aux besoins, ainsi que la mise en place d'une gouvernance et d'une sécurité des données. Cependant, ces éléments ne suffisent pas sans une gestion des identités. Cette gestion des identités est conduite par Microsoft Entra ID, considéré comme le cœur de Microsoft 365. En effet, Microsoft Entra ID est un service qui permet aux utilisateurs de s'authentifier et d'accéder aux ressources cloud. Sans lui, toute tentative de connexion dans l'environnement Microsoft 365 est impossible.

Pour comprendre comment Microsoft Entra ID a vu le jour, il faut remonter quelques années en arrière. En 2010, Microsoft lance sa première plateforme cloud appelée Windows Azure.

Cette plateforme, composée de plusieurs outils, avait pour but l'hébergement d'applications dans un environnement 100 % Internet. Son atout majeur était sa compatibilité avec la plupart des systèmes d'exploitation.

En 2012, à travers une préversion destinée aux développeurs, Microsoft réalise Windows Azure Active Directory, outil officiel pour la gestion des identités et l'authentification des utilisateurs. Bien que présenté en 2012, Windows Azure Active Directory était déjà implémenté chez Microsoft comme solution de gestion des identités, notamment pour des services comme Dynamics CRM Online, Windows Intune ou encore Office 365.

En 2014, Microsoft change le nom de sa plateforme cloud de Windows Azure en Microsoft Azure. Pour des soucis de cohérence, Microsoft procède également au renommage de Windows Azure Active Directory en Azure Active Directory.

Après plusieurs années de mises à jour régulières et de nouvelles fonctionnalités, en 2023, Azure Active Directory devient Microsoft Entra ID.

2. Vue d'ensemble de Microsoft Entra ID

2.1 Microsoft Entra

Comme Microsoft Defender XDR, Microsoft Entra est la combinaison de plusieurs outils : Microsoft Entra ID, Microsoft Entra ID Governance, Microsoft Entra External ID, Microsoft Entra Permissions Management, Microsoft Entra Verified ID, Microsoft Entra Workload ID, Microsoft Entra Global Secure. Voici une vue d'ensemble des produits de la famille Entra.

Microsoft Entra ID est le plus connu de la famille Entra. C'est un service cloud qui permet de gérer des utilisateurs, des groupes d'authentification et l'accès à des ressources. Lorsqu'un utilisateur se connecte à Microsoft 365, Microsoft Entra ID vérifie son identité et applique les différentes politiques de sécurité définies par les administrateurs.

Microsoft Entra ID Governance est un service qui permet la bonne attribution des accès à travers des règles, des validations et des révocations automatiques.

Microsoft Entra External ID est un service qui permet de gérer l'identité des utilisateurs externes. Cela permet de donner des accès à des ressources de l'organisation tout en gardant le contrôle sur les droits ainsi que sur la durée d'accès.

Microsoft Entra Permissions Management est un service qui permet d'analyser et de supprimer automatiquement les permissions non utilisées dans n'importe quel environnement (Microsoft, Google, Amazon, etc.).

Microsoft Entra Verified ID est un service qui permet de créer et d'échanger des preuves d'identité numériques sécurisées. Ce type de service permet à un utilisateur de ne pas exposer ses documents personnels.

Microsoft Entra Workload ID est un service qui gère les identités liées aux applications et aux services. Cela permet d'ajouter une couche de sécurité aux applications figurant dans le cloud.

Microsoft Entra Global Secure Access est un service qui sécurise l'accès à des périphériques ou applications internes depuis l'appareil d'un utilisateur sans la nécessité d'utiliser un VPN.

Produit Entra	Licence utilisée
Microsoft Entra ID	Entra P1
Microsoft Entra External ID	Entra P1
Microsoft Entra ID Governance	Entra Suite
Microsoft Entra ID Protection	Entra P2
Microsoft Entra Permissions Management	Entra Suite
Microsoft Entra Global Secure Access	Entra Suite
Microsoft Entra Verified ID	Entra P1 / Entra P2 (facturation à l'usage)
Microsoft Entra Workload ID	Entra P1 / Entra P2

2.2 Active Directory vs Microsoft Entra ID

Chez Microsoft, lorsque la gestion des identités est évoquée, deux noms reviennent souvent : Active Directory et Microsoft Entra ID. Bien qu'ils aient certaines choses en commun, comme le fait d'être tous les deux des annuaires qui gèrent des utilisateurs, des groupes et des accès, ils sont différents tant dans leur conception que dans leur usage.

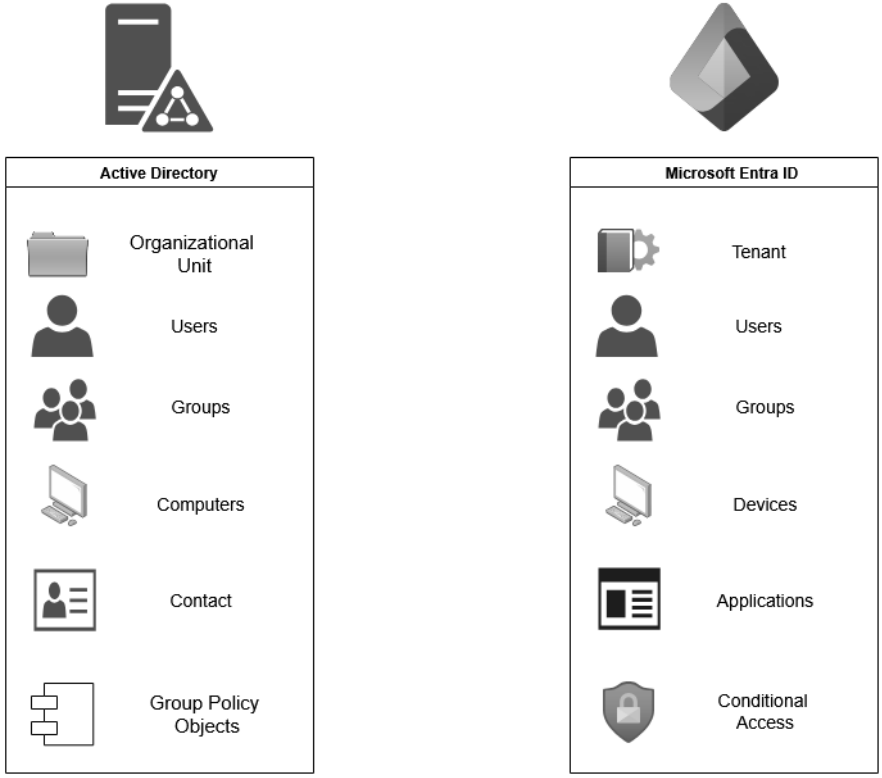
L'Active Directory a vu le jour en 1999 lorsque la plupart des infrastructures reposaient sur des serveurs physiques. Hébergé exclusivement dans un réseau local, son rôle est de centraliser toutes les ressources telles que les comptes utilisateurs, les groupes, les machines et les contacts. Toutes ces ressources sont classées à travers des unités organisationnelles (OU) et sa gestion des politiques se fait à travers des stratégies de groupe (GPO).

Microsoft Entra ID a vu le jour quelques années plus tard en 2010 lorsque le cloud commençait à se démocratiser. Hébergé uniquement dans le cloud, son rôle est de permettre aux utilisateurs de se connecter à Microsoft 365, mais aussi à des applications comme Exchange Online SharePoint, OneDrive et Microsoft Teams. Sa gestion des politiques se fait à travers des accès conditionnels.

Confondre Active Directory et Microsoft Entra ID est une erreur courante. D'autant plus que l'ancien nom de Microsoft Entra ID, Azure Active Directory, pouvait amplifier cette confusion entre les deux produits. Voici les différences majeures :

Fonction	Active Directory	Microsoft Entra ID
Type de produit	Service d'annuaire local	Service d'identité cloud
Environnement	Réseau local	Cloud
Architecture	Domaine et unités organisationnelles	Tenant
Protocole	Kerberos	OAuth 2.0, SAML
Gestion des politiques	Stratégie de groupe	Accès conditionnels
Appareils gérés	Postes de travail et serveurs	Appareils et mobiles

Voici un schéma illustrant les différents objets gérés respectivement par Active Directory et Microsoft Entra ID :



Malgré leurs différences, il est tout à fait possible de les faire cohabiter. C'est ce qu'on appelle une architecture hybride. Active Directory continue de gérer les ressources internes, tandis que Microsoft Entra ID gère l'accès aux services en ligne.

Aujourd'hui, la grande majorité des entreprises adoptent un modèle hybride. Selon les dernières tendances près de 70 à 80 % des organisations utilisent une infrastructure mêlant les deux technologies, reliées par l'outil de synchronisation Microsoft Entra Connect. Avec ce type d'environnement, les différences entre Active Directory et Microsoft Entra deviennent des atouts complémentaires.

Remarque

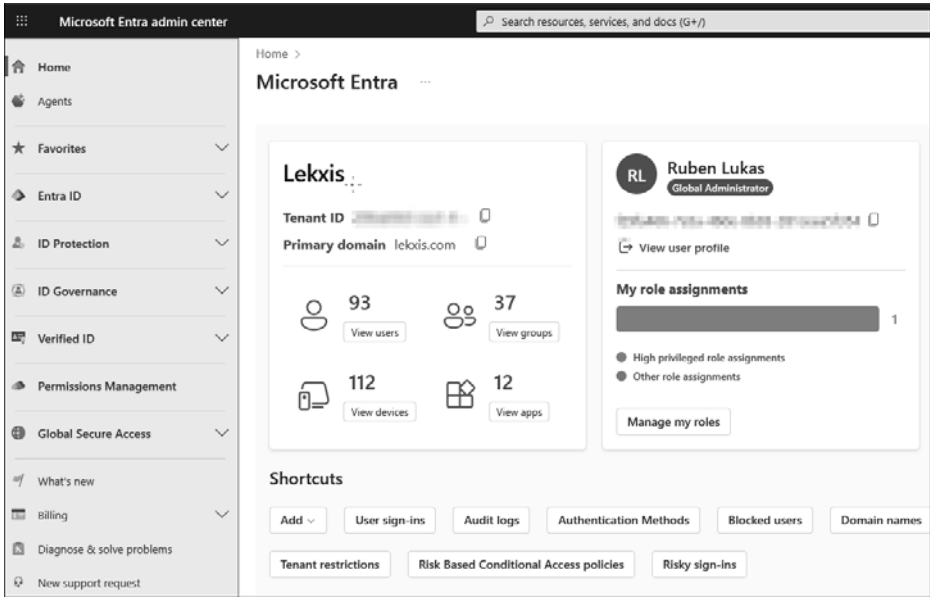
Un descriptif plus complet sur les différences entre Active Directory et Microsoft Entra ID est disponible sur le site de Microsoft : https://learn.microsoft.com/en-us/entra/fundamentals/compare

2.3 Centre d'administration de Microsoft Entra ID

Le centre d'administration de Microsoft Entra ID regroupe tous les paramètres liés à la gestion des identités et des accès. Comme pour le centre d'administration de Microsoft 365, il dispose de son propre rôle, le Global Administrator. Étant donné que Microsoft Entra ID est le noyau central de Microsoft 365, sa gestion nécessite des autorisations permettant de gérer l'ensemble des services du tenant. Toutefois, d'autres rôles peuvent également y accéder, mais avec des droits limités et une visibilité restreinte.

Le centre d'administration est accessible depuis l'adresse https://entra.microsoft.com ou depuis le centre d'administration de Microsoft 365 disponible à l'adresse https://admin.microsoft.com.

Il se compose de deux sections principales : la partie centrale affichant plusieurs informations liées au tenant, et la partie de gauche qui regroupe les différents menus présents dans le portail d'administration.



Présentation des menus du centre d'administration de Microsoft Entra ID :

- **Home** : vue d'ensemble du centre d'administration ;
- **Agents** : gestion des agents IA de Microsoft ;
- **Favorites** : création de raccourcis ;
- **Entra ID** : gestion des fonctionnalités liées à l'identité ;
- **ID Protection** : gestion des fonctionnalités liées à la protection ;
- **ID Governance** : administration des accès ;
- **Verified ID** : vérification des identités ;
- **Permissions Management** : gestion des permissions ;
- **Global Secure Access** : sécurisation des accès ;
- **What's new** : affichage des nouvelles fonctionnalités ;
- **Biling** : management des licences ;
- **Diagnose & solve problems** : identification et résolution des problèmes ;
- **New support request** : accès à la documentation et au support de Microsoft.

3. Gestion des identités

La gestion des identités est la fonction première de Microsoft Entra ID.

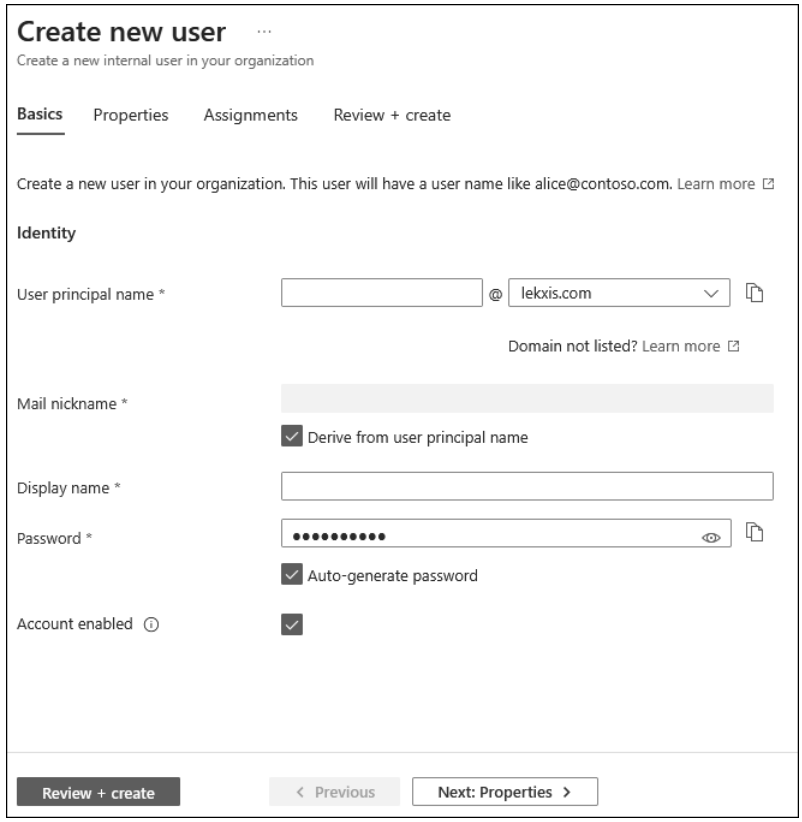
Une identité est un objet unique qu'on autorise à accéder à des ressources. Elle peut être de différents types : utilisateur, groupe ou application. Chaque identité possède un ensemble d'attributs.

3.1 Création des utilisateurs

Dans Microsoft Entra ID, les utilisateurs peuvent être ajoutés de plusieurs manières : manuellement depuis le portail Microsoft Entra ID, par importation depuis l'Active Directory (synchronisation avec Microsoft Entra Connect) ou avec PowerShell.

Création d'un compte avec le Microsoft Entra ID

- Pour créer un compte, rendez-vous dans le sous-menu **All users** du menu **Users**, cliquez sur l'onglet **Add a user** puis sur **Create new user**.
- Dans la fenêtre de configuration, renseignez les champs suivants :
  - **User principal name** : l'identifiant de connexion de l'utilisateur dans Microsoft 365 ;
  - **Mail nickname** : l'alias ;
  - **Display name** : le nom complet de l'utilisateur ;
  - **Password** : le mot de passe ;
  - **Account enabled** : le paramètre pour activer le compte après la création.



- Après avoir rempli les champs, cliquez sur **Next: Properties** pour continuer le processus de création ou sur **Review + create** pour passer à la dernière étape.
- Une fois à la dernière étape, cliquez sur **Create** pour valider la création du compte.

Voici un aperçu du message reçu après la création du compte :