Chapitre 6
Gestion des identités hybrides

1. Introduction

Jusqu'à présent, nous nous sommes majoritairement focalisés sur une infrastructure *full cloud* Azure Active Directory pour la gestion, entre autres, des comptes utilisateurs. Bien entendu, ce genre de configuration ne convient pas si l'entreprise dispose d'un annuaire Active Directory local et souhaite accéder à des applications ou services cloud tels qu'Office 365 (SharePoint Online, Exchange Online, OneDrive Online, Microsoft Teams, etc.) avec ses utilisateurs locaux.

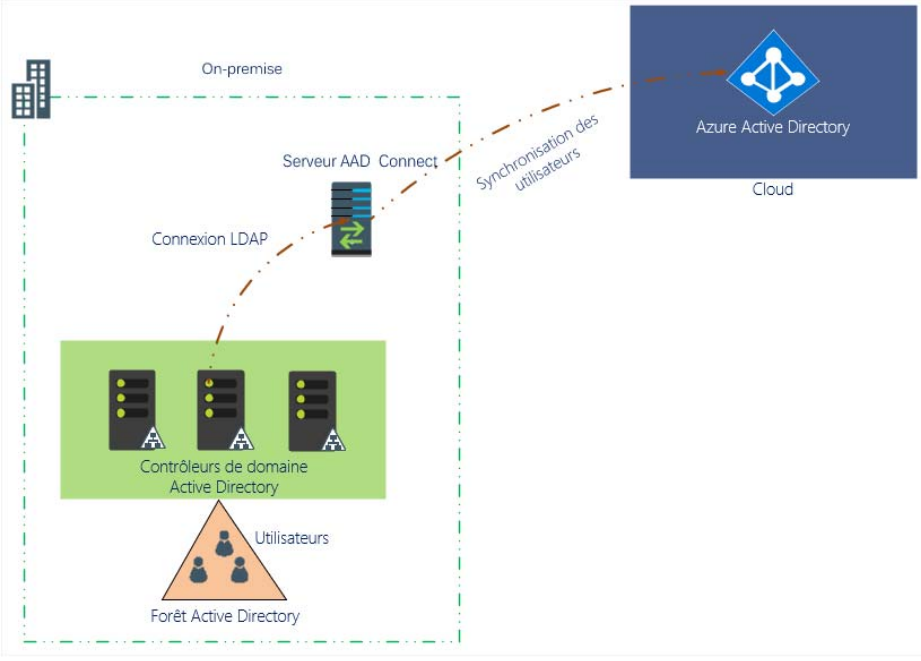
Dans ce cas, il faut étudier la mise en œuvre d'une solution hybride permettant à un utilisateur, dont l'identité est contenue dans l'annuaire Active Directory local, d'accéder aux ressources internes de l'entreprise et de disposer d'une identité dans le cloud (et plus précisément dans Azure Active Directory) pour consommer et s'authentifier auprès des services cloud et applications Office 365.

Cette configuration revient à synchroniser les utilisateurs d'un Active Directory local avec l'annuaire Azure Active Directory dans le cloud. C'est ce qui revient à dire qu'avec Azure Active Directory, nous accédons à plusieurs applications avec une **seule et unique identité**.

Avec Azure Active Directory, notre façon de gérer l'identité change et devient hybride. La gestion des identités ne s'effectue plus seulement en local, mais également, pour les comptes synchronisés, dans le cloud. De nouvelles méthodes d'authentification à administrer apparaissent permettant d'accéder, à l'aide d'une seule identité, aux services cloud et applications SaaS. Nous verrons plus loin dans ce chapitre la gestion de ces authentifications ainsi que les différentes méthodes permettant l'extension d'un Active Directory local vers Azure Active Directory.

2. Extension d'un Active Directory local vers Azure Active Directory

Comme expliqué à plusieurs reprises, l'extension d'un Active Directory local consiste à synchroniser des utilisateurs de l'Active Directory local vers Azure Active Directory. Voici une illustration qui montre ce concept d'hybridation d'identité :



Dans une infrastructure à identité hybride, nous possédons au moins les composants suivants :

– un annuaire Active Directory
– un serveur AAD Connect
– des utilisateurs/groupes d'utilisateurs - OU
– un annuaire Azure Active Directory

Remarque

Volontairement, nous n'avons pas indiqué ici de ferme AD FS, car il s'agit de lister les éléments minimums afin de synchroniser des utilisateurs locaux vers Azure Active Directory.

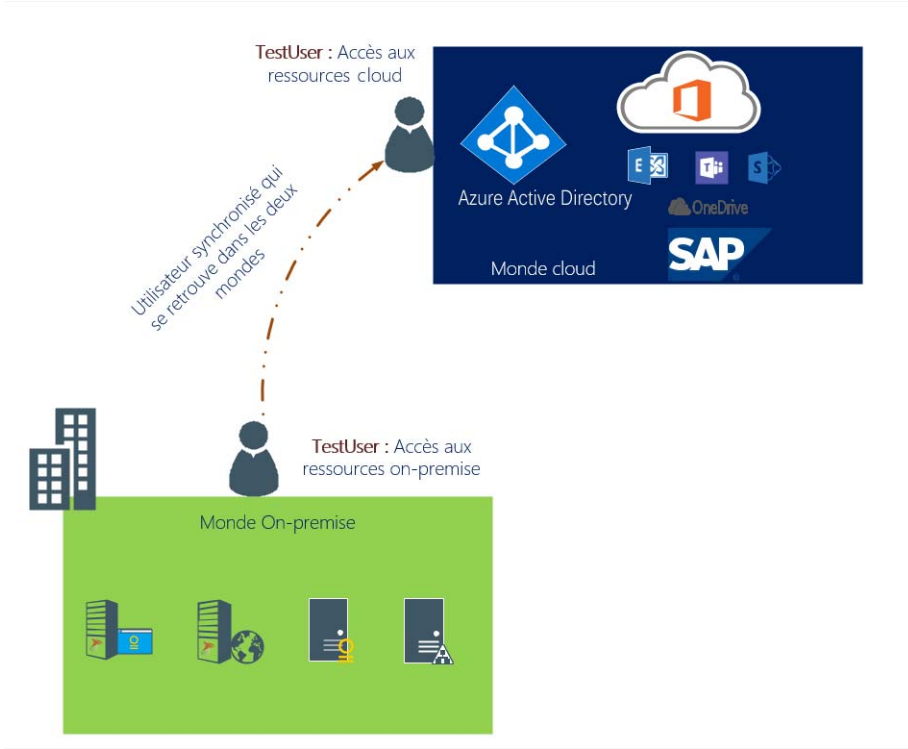
Sur l'illustration précédente, nous remarquons que le serveur Azure Active Directory Connect se connecte à la forêt Active Directory via l'un des contrôleurs de domaine et effectue une synchronisation avec Azure Active Directory en fonction des règles et filtrage d'OU imposés. Avec cette configuration précise, certains utilisateurs posséderont à la fois un compte au sein de l'annuaire Active Directory local et dans l'annuaire Azure Active Directory, d'où le nom « identité hybride ».

2.1 Pourquoi étendre ses utilisateurs vers Azure Active Directory ?

Même si nous avons déjà répondu à cette question, il est très important de comprendre ce que cela représente, et dans quel but on choisit d'étendre un Active Directory vers Azure Active Directory.

Comme évoqué à plusieurs reprises, le cloud est un monde complètement à part. Microsoft offre plusieurs services : les services Office 365, Azure ou encore des applications SaaS. Ces services nécessitent, comme tout service, une authentification sécurisée qui s'appuie pour cela sur l'annuaire Azure Active Directory. Une entreprise qui souhaite bénéficier de ces services et les proposer à ses utilisateurs ne va pas leur proposer un compte et un mot de passe pour chaque application et service, en plus de leur compte local Active Directory. Cela deviendrait lourd à gérer pour les utilisateurs et pour les administrateurs.

La nécessité d'étendre un annuaire Active Directory local est alors démontrée. En faisant cela, l'utilisateur peut accéder aux services cloud et non cloud avec la même identité. Il s'agit d'un enjeu crucial pour les grandes entreprises.



2.2 Les attributs Active Directory stockés dans Azure Active Directory

Bien sûr, vous l'avez compris, en synchronisant un utilisateur, ses attributs vont se dupliquer dans le cloud, et plus principalement dans l'annuaire Azure Active Directory. À la nuance près qu'une partie seulement des attributs seront synchronisés : ceux nécessaires a minima pour l'authentification auprès des services et applications cloud.

Beaucoup d'entreprises européennes s'interrogent sur l'emplacement du stockage de leurs données pour des questions de législation, refusant par exemple de les entreposer dans des datacenters aux États-Unis.

Il faut savoir que l'emplacement de stockage des données, en ce qui concerne les offres cloud Microsoft, dépend de l'adresse fournie lors de l'inscription au service Office 365 ou Azure Active Directory pour mieux répondre aux problématiques légales de certains pays européens concernant la localisation de leurs données.

Un site de Microsoft très bien fait explique tout cela : https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located

Remarque

La plupart des attributs des utilisateurs des entreprises européennes sont stockés dans les datacenters en Europe, à l'exception des attributs utilisateurs listés ci-dessous qui demeurent entreposés dans les datacenters aux USA :

- givenName
- Name
- UserPrincipalName
- Domain
- PasswordHash
- SourceAnchor
- AccountEnabled
- PasswordPolicies
- StrongAuthenticationRequierment
- ApplicationPassword
- PUID

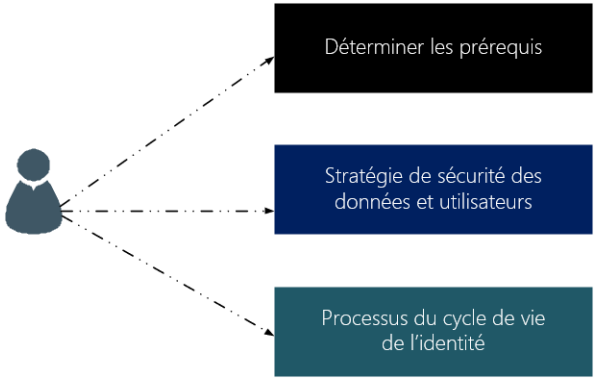
Ces attributs permettent l'authentification et le fonctionnement des utilisateurs. Aucune donnée personnelle des utilisateurs n’est stockée.

2.3 Avant d'étendre son Active Directory

Tout d'abord, il est important de définir les besoins, d'analyser l'existant et de choisir la bonne stratégie. Cette étape d'étude est très importante, et il est préférable de la mettre en œuvre dans chaque projet.

Cette étape regroupe :

– la détermination des prérequis
– la stratégie de sécurité des données et utilisateurs
– le processus du cycle de vie de l'identité



Détermination des prérequis

Cette phase est importante car il s'agit de déterminer les besoins métiers de l'entreprise et de connaître sa stratégie sur le court et le long terme vis à vis du cloud.

Plusieurs points sont à prendre en compte dans cette partie :

– Pourquoi une architecture hybride et pour quels besoins ?
– Pourquoi se diriger vers le cloud ? Connaître et définir la stratégie de l'entreprise.
– Lister les moyens d'authentification utilisés actuellement dans l'entreprise, ce qui permet de définir les besoins techniques pour intégrer une architecture hybride avec Azure Active Directory.