



# Chapitre 4

## Gestion des appareils

### 1. Introduction

Comme les utilisateurs, les appareils et applications doivent être gérés. Cette gestion doit être bien entendue sécurisée, mobile pour offrir plus de productivité aux utilisateurs de son entreprise, et industrielle afin d'offrir aux équipes informatiques de bons outils de travail pour l'administration ou encore le dépannage.

Le but est d'offrir un monde mobile et sécurisé, comme le dit si bien le PDG de Microsoft "Cloud First - Mobile first" ; bien entendu, qui dit cloud et monde mobile, dit forcément problématiques de sécurité à traiter. Azure Active Directory comme évoqué précédemment, fait partie de la suite EMS Enterprise Mobility + Security et de Microsoft Entra qui va permettre aux entreprises de gérer leurs utilisateurs, leurs appareils (stations de travail, téléphones mobiles) de manière centralisée et sécurisée tout en offrant de la mobilité.

Bien évidemment, pour avoir de la gestion globale au niveau des appareils, il faudra aussi aborder la partie Microsoft Intune. Dans cet ouvrage, nous allons couvrir uniquement la partie Azure Active Directory/Microsoft Entra.

Comme vous le savez sans doute, dans Active Directory, il est possible de joindre des machines Windows, ce qui veut dire que si la machine est jointe au domaine, celle-ci aura accès aux ressources du domaine et va bénéficier de toutes les politiques de sécurité liées à ce domaine Active Directory. Nous allons voir la même approche côté cloud avec Azure Active Directory.

## 1.1 Le Modern Management

Il faut savoir que dans Azure Active Directory, il est également possible d'inscrire et de joindre des appareils. Avec l'arrivée de Windows 10 et Windows 11, cette étape prend encore plus de sens, car l'Azure Active Directory sera la pièce maîtresse en tant que fournisseur d'identité afin d'offrir aux entreprises un nouveau mode qui se nomme le Modern Management.

Le Modern Management va permettre aux entreprises de gérer leurs postes de travail et leur flotte mobile de manière totalement différente de ce que nous avons connu jusqu'à aujourd'hui avec l'Active Directory classique, car au lieu de créer des GPO, nous allons créer des politiques avec Microsoft Intune, par exemple. Nous allons également pouvoir gérer les machines de manière totalement mobile et sécurisée depuis le cloud de Microsoft.

Le Modern Management de Windows 10/Windows 11 se présente comme une solution sécurisée qui va simplifier la gestion tout en conservant l'aspect sécurité du système d'information. Microsoft permet aux entreprises de s'offrir le Modern Management avec leur suite nommée **Microsoft 365** permettant de répondre à toutes les problématiques des entreprises (sécurité, mobilité, gestion des postes de travail Windows 10, collaboration et productivité).

D'ailleurs durant le COVID-19 et le confinement, la suite Microsoft 365 a permis à beaucoup d'entreprises de rester compétitives dans leur domaine en ayant de bons outils de collaboration.

Microsoft 365 offre les suites listées ci-après :

- Office 365
- EMS
- Windows 10

Microsoft propose deux plans pour les entreprises, à savoir E3 et E5 :

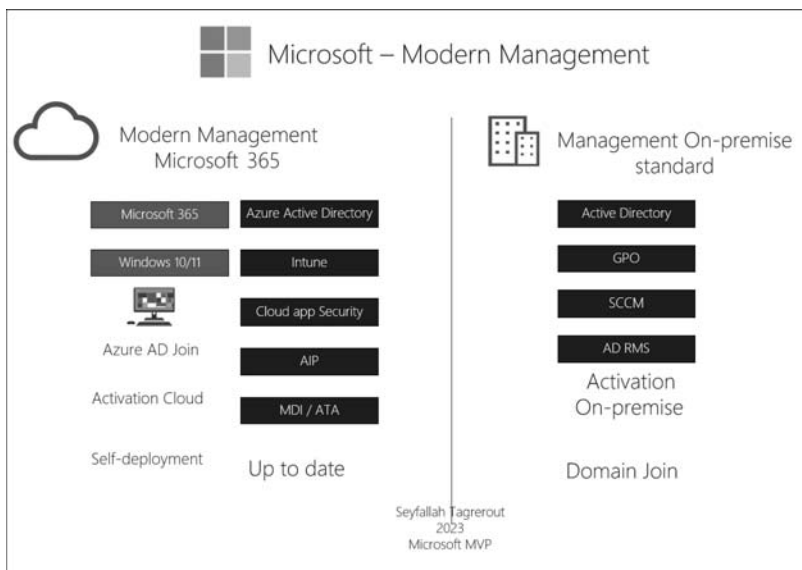
**E3** : dans ce plan, il sera possible de bénéficier des suites ci-dessous :

- Office 365 E3
- EMS E3
- Windows 10 Entreprise E3

**E5** : dans ce plan, il sera possible de bénéficier des suites ci-dessous :

- Office 365 E5
- EMS E5
- Windows 10 Entreprise E5

Des différences notables existent entre le Modern Management et la gestion locale d'un annuaire Active Directory :



Côté Modern Management, nous disposons de nouveaux outils plus puissants, plus simples et surtout centralisés qui vont permettre de gérer des postes de travail de façon moderne, au lieu de manipuler un serveur SCCM avec toutes les difficultés que cela engendre. Nous utilisons Microsoft Intune pour la gestion des postes de travail Windows 10/11 afin de gérer les mises à jour et pousser des applications. De plus, avec cette même plateforme, il sera possible de gérer vos appareils mobiles et de faire du MDM (*Mobile Device Management*) ou encore du MAM (*Mobile Application Management*).

Les postes de travail ne seront ainsi plus joints à un domaine Active Directory classique, mais à Azure Active Directory. Au lieu de pousser des GPO qui sont difficiles à maintenir au quotidien, ce sont des politiques via Intune qui gèrent les paramètres. Ce sont toutes ces notions et différences qui nous permettent de constater que le modern management et la gestion dite traditionnelle n'appartiennent pas au même monde.

Bien entendu, toutes les entreprises ne peuvent pas, du jour au lendemain, migrer toute leur infrastructure dans le cloud. Microsoft propose ainsi aux entreprises désirant se diriger vers le cloud petit à petit, le **modèle hybridation de service**, comme évoqué précédemment dans le livre. L'hybridation des services on-premise avec des services cloud va permettre aux entreprises de conserver leurs applications locales et de les connecter aux mêmes services, mais dans le cloud.

# 250 \_\_\_\_\_ Azure Active Directory

Gestion des identités hybrides (concepts et mise en œuvre)

L'exemple le plus concret est l'Azure Active Directory : nous pourrions conserver notre annuaire Active Directory interne et en étendre une partie afin de faire de l'hybridation de service Active Directory. C'est également valable, par exemple, pour AD RMS ou Microsoft Purview Information Protection, ainsi qu'un grand nombre d'autres services.

Azure Active Directory permet de joindre les postes de travail on-premise, offrant ainsi plusieurs avantages aux entreprises. De plus, Azure Active Directory offre trois possibilités :

- L'inscription d'appareils
- La jonction d'appareils
- La jonction des appareils hybrides

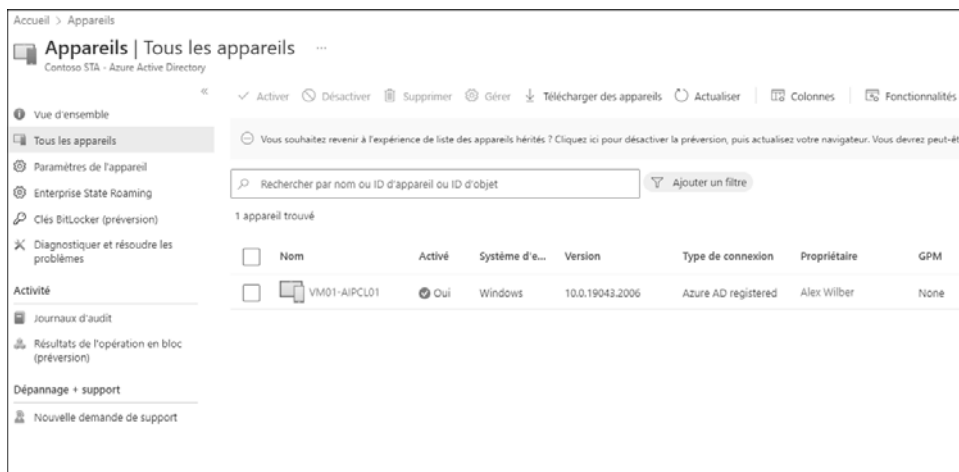
Nous allons étudier ci-après la différence existant entre chacun de ces modes et leurs apports.

## 1.2 L'identité d'appareil dans Azure Active Directory

Avant de commencer, il est important de comprendre en quoi consiste l'identité dans un appareil dans Azure Active Directory. Ceci donnera toutes les connaissances nécessaires au lecteur pour la suite de l'ouvrage.

Lorsqu'on manipule des appareils dans Azure Active Directory, on est confronté à des objets de type appareil dans ce dernier. Ces objets représentent en réalité les identités d'appareil dont Azure Active Directory a besoin pour gérer ses appareils.

On peut voir ici un appareil dans Azure AD représentant l'identité d'un appareil :



Il contient les informations suivantes :

Nom	VM01-AIPCL01
ID de l'appareil	a0232013-a586-4ff0-82af-29aa3b26a568
ID de l'objet	0e204b57-71f2-479e-a148-2dc215d8bfc3
Activé	Oui
Système d'exploitation	Windows
Version	10.0.19043.2006
Type de connexion	Azure AD registered
Propriétaire	Alex Wilber
Nom d'utilisateur principal	AlexW@M365x03481655.OnMicrosoft.com
GPM	Aucun
Conforme	N/A
Inscrit	20/09/2022 01:12:16
Activité	21/02/2023 22:00:04
Groupes	Aucun
Attributs d'extension	Aucun attribut d'extension

La gestion des appareils dans Azure AD dispose de plusieurs rubriques que vous allez retrouver dans **Tous les appareils** dans Azure AD ou Microsoft Entra :

- **Tous les appareils** : liste tous les appareils.
- **Paramètres de l'appareil** : permet de configurer les appareils, ce que nous allons voir plus bas.
- **Enterprise State Roaming** : permet de synchroniser les paramètres et données d'application sur plusieurs appareils.
- **Clés BitLocker (préversion)** : permet de lister les clés BitLocker des appareils.
- **Journaux d'audit** : permet d'afficher toutes les activités liées aux appareils dans Azure Active Directory.

### 1.3 Paramètres dans Azure Active Directory

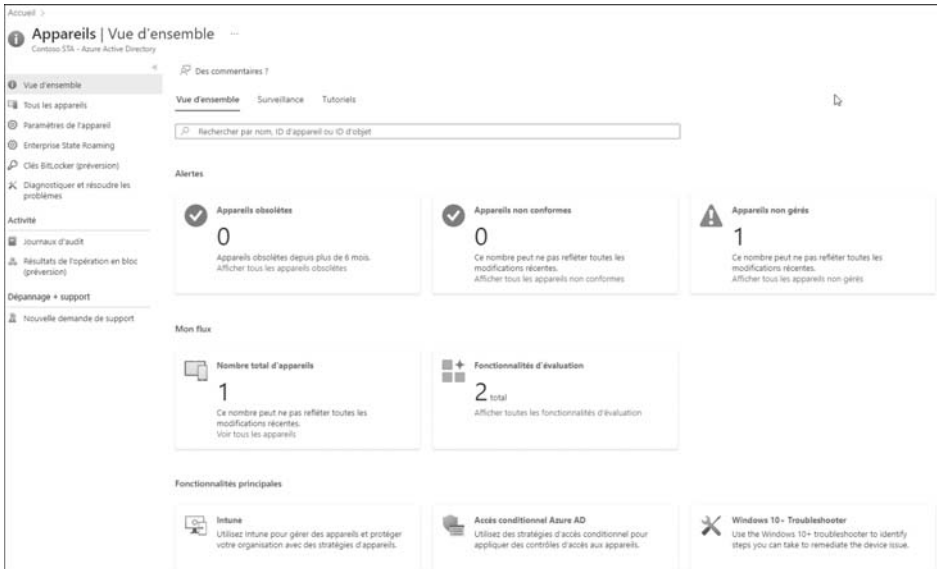
Dans la rubrique **Appareils**, plusieurs paramètres sont proposés par Microsoft afin de prendre en compte ces inscriptions et ajouter des appareils dans Azure Active Directory.

- On peut y accéder en se rendant dans l'interface Azure Active Directory Admin Center via la rubrique **Appareils** puis **Paramètres de l'appareil**, ou depuis le portail Azure Active Directory ou Microsoft Entra (<https://entra-microsoft.com>).

# 252 — Azure Active Directory

Gestion des identités hybrides (concepts et mise en œuvre)

Plusieurs paramètres y apparaissent permettant de configurer au mieux les appareils présents dans notre annuaire Azure Active Directory en cliquant sur **Paramètres de l'appareil** :



Dans les paramètres de l'appareil, nous retrouvons les options suivantes :

- **Les utilisateurs peuvent joindre des appareils à Azure AD** : ce paramètre donne le droit aux utilisateurs de joindre leur appareil (exemple Windows 10/11) à Azure Active Directory. Il est bien entendu possible d'être granulaire et de choisir quelques utilisateurs spécifiques (groupes ou utilisateurs) si la politique de l'entreprise l'exige. Il aussi est possible d'empêcher les utilisateurs de joindre leurs appareils à Azure Active Directory en sélectionnant la valeur **Aucun**.
- **Les utilisateurs peuvent inscrire leurs appareils sur Azure AD** : ce paramètre permet de donner l'autorisation ou non aux utilisateurs d'inscrire leurs appareils dans Azure Active Directory.

- **Exiger l'authentification multifactor pour inscrire ou joindre des appareils dans Azure AD** : ce paramètre permet d'activer ou non le MFA lorsqu'un utilisateur tentera d'inscrire ou d'ajouter sa machine dans Azure Active Directory. Il est recommandé d'utiliser les stratégies d'accès conditionnel pour gérer cette option. Cette partie sera abordée au chapitre lié à la sécurité.
- **Nombre maximal d'appareils par utilisateur** : ce paramètre permet de fixer le nombre maximal d'appareils qu'un utilisateur pourra avoir sur Azure Active Directory.
- **Gérer Administrateurs locaux supplémentaires sur tous les appareils joints à Azure AD** : il est possible ici de spécifier des administrateurs locaux sur les appareils qui sont joints à Azure Active Directory. Par défaut, seuls les administrateurs globaux de l'annuaire Azure Active Directory le sont. Bien entendu, il sera uniquement possible de choisir des utilisateurs spécifiques, la notion de groupe n'est pas possible.
- **Restrict non-admin users from recovering the BitLocker key(s) for their owned devices** : ce paramètre permet de donner la possibilité aux utilisateurs de récupérer leur clé de récupération BitLocker en mode self- service :

Accueil > Appareils

## Appareils | Paramètres de l'appareil

Contoso S1A - Azure Active Directory

Enregistrer ✕ Ignorer | Des commentaires ?

Les utilisateurs peuvent joindre des appareils à Azure AD

Tout Sélectionné Aucun

Sélectionné

Aucun membre sélectionné

Les utilisateurs peuvent inscrire leurs appareils sur Azure AD

Tout Aucun

En savoir plus sur le fonctionnement de ce paramètre

Exiger l'authentification multifactor pour inscrire ou joindre des appareils avec Azure AD

Oui Non

⚠ Nous vous recommandons d'exiger l'authentification multifactor pour inscrire ou joindre des appareils avec Azure AD à l'aide de l'accès conditionnel. Définissez ce paramètre d'appareil sur Non si vous avez besoin d'utiliser l'authentification multifactor avec l'accès conditionnel.

Nombre maximal d'appareils par utilisateur

5

Gérer Administrateurs locaux supplémentaires sur tous les appareils joints à Azure AD

Restrict non-admin users from recovering the BitLocker key(s) for their owned devices (preview)

Oui Non