Chapitre 4
Concepts de base

1. Introduction

Dans les chapitres précédents, nous avons vu comment créer une machine virtuelle et l'insérer dans un groupe de ressources. Néanmoins, celle-ci s'appuie sur un compte de stockage, un réseau virtuel et bien d'autres services nécessaires à son fonctionnement. Tout propriétaire d'un abonnement doit pouvoir appréhender facilement les concepts de base utilisés dans Azure, ceux-ci lui seront utiles lors de l'administration quotidienne de la plateforme. Ce chapitre aborde ces concepts.

2. Convention de nommage

Choisir un nom cohérent pour désigner une ressource Azure est important, car il est difficile de le modifier par la suite, et au vu du nombre de services proposés par le Cloud de Microsoft (plus d'une centaine), une convention de nommage s'avère bien souvent indispensable. La recherche d'une ressource est dans ce cas facilitée. Il est recommandé d'utiliser des préfixes (début) ou des suffixes courants (fin) pour identifier la ressource.

Par exemple, pour identifier une machine virtuelle supportant une base de données SQL dans un environnement dev et dans une région Azure France, saisissez comme nom dev-vm-sql-name01-fr en ajoutant en affixe l'environnement. Si plusieurs machines virtuelles supportaient la même application, il suffirait de rajouter 01, 02, etc.

Voici quelques abréviations utilisées couramment :

– Groupe de ressources = rg (resource group)
– Groupe à haute disponibilité = as (availability set)
– Compte de stockage = data
– Réseau virtuel = vnet
– Interface réseau = nic
– Groupe de sécurité réseau = nsg (network security group)
– Equilibreur de charge = lb (load balancer)
– Azure Application Gateway = agw

Il est aussi conseillé d'utiliser les étiquettes (décrites dans le chapitre précédent) pour identifier précisément une ressource ainsi que son propriétaire.

Microsoft propose d'utiliser une convention de nommage propre à Azure et adaptable aux conventions propres à chaque client, via le site ci-dessous : https://learn.microsoft.com/fr-fr/azure/cloud-adoption-framework/ready/azure-best-practices/naming-and-tagging

3. Groupe de ressources

Nous l'avons vu dans le chapitre Interfaces d'exploitation, le modèle Resource Manager inclut des fonctionnalités telles que la balise, le modèle RBAC et… le groupe de ressources. Grâce à ce dernier, les ressources d'un même projet (ou client) sont déployées dans un ordre précis, puis regroupées dans le même groupe. Celui-ci peut se voir attribuer une délégation des droits particuliers et des balises à des fins de facturation. Un groupe de ressources appartient à un abonnement. Chaque ressource ne peut être membre que d'un seul groupe de ressources, quelle que soit sa région, et elle peut être déplacée à tout moment vers un autre groupe, puis supprimée au besoin. En résumé, un groupe de ressources est la limite logique théorique des actions permises à un propriétaire désigné.

Dans pratiquement tous les cas de création d'une ressource (machine virtuelle, compte de stockage, réseau virtuel, Web App, etc.), un groupe de ressources est nécessaire à son fonctionnement. Enfin, sachez qu'un groupe de ressources a une structure plate, il ne peut pas être imbriqué dans un autre groupe de ressources.

Nous allons créer un groupe de ressources :

- Dans le panneau d'actions situé à gauche de l'interface, cliquez sur **Groupes de ressources**, puis sur **Créer**. Saisissez son nom (dans notre exemple **RG-livreazure**), l'abonnement à utiliser pour l'héberger, ainsi que sa région (dans notre cas **West Europe**).
- Cliquez sur le bouton **Vérifier + créer** puis sur le bouton **Créer**.

Il est possible d'épingler le groupe de ressources au tableau de bord en sélectionnant ce dernier puis en cliquant sur la punaise située à droite (**Épingler au tableau de bord**).

Remarque

Rappel : lorsqu'un groupe de ressources est supprimé, toutes les ressources qu'il contient le sont aussi.

3.1 Verrou

Il est possible de verrouiller un groupe de ressources afin que d'autres utilisateurs ne puissent pas modifier (verrou en lecture seule) ou supprimer (verrou supprimer) ce qu'il contient, même s'ils ont les droits RBAC pour le faire :

- Cliquez sur **Groupes de ressources** depuis le menu d'actions situé à gauche de l'interface, puis sur le groupe de ressources précédemment créé (**RG-livreazure**). Dans le panneau des paramètres, cliquez sur **Verrous**.

Remarque

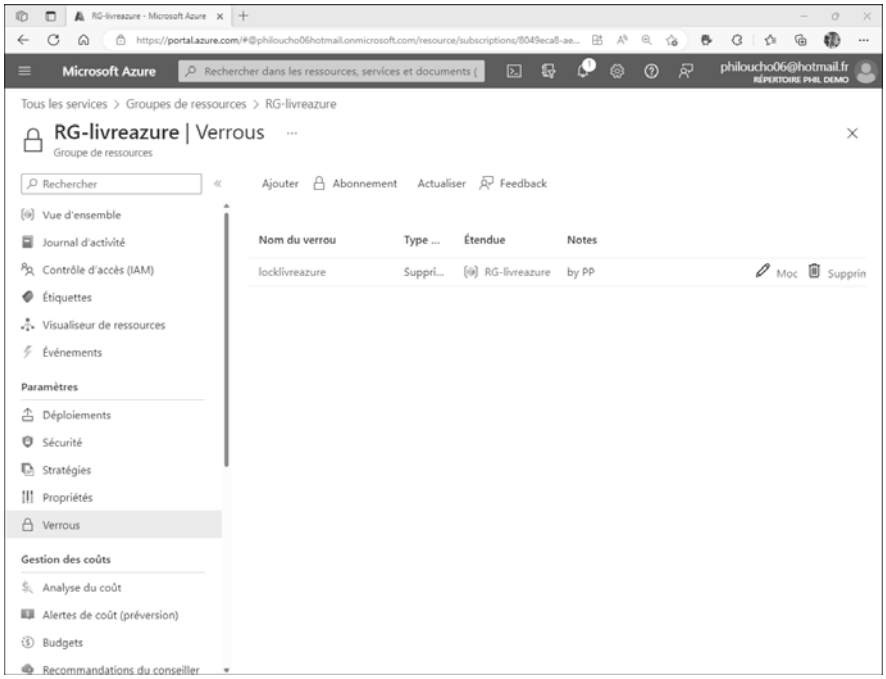
Le verrouillage peut aussi s'effectuer sur d'autres ressources, et même sur un abonnement.

- Cliquez sur **Ajouter**. Saisissez un nom (dans notre exemple **locklivreazure**), choisissez son type (**Supprimer** dans notre cas). Si nécessaire, saisissez une remarque pour documenter sa création.
- Confirmez la création du verrou en cliquant sur le bouton **OK**.

Toutes les ressources contenues dans le groupe de ressources **RG-livreazure** seront impactées par ce verrou en lecture seule, grâce à l'héritage.

- Cliquez sur **Vue d'ensemble** et sur **Delete resource group**. Saisissez le nom **RG-livreazure** dans le champ prévu à cet effet, et cliquez sur le bouton **Supprimer**. L'opération échoue, ce qui est normal, à cause du verrou apposé précédemment.

- Pour supprimer le verrou précédemment appliqué, dans le paramètre **Verrous**, cliquez sur **Supprimer**.



3.2 Déplacement de ressources

L'administrateur peut déplacer une ressource d'un groupe de ressources vers un autre, la déplacer vers une autre région, et même vers un autre abonnement si celui-ci est attribué au même client (locataire ou tenant).

En effet, dans Azure Active Directory, un client représente l'entreprise dans son ensemble via une instance dédiée. Comme aucune ressource Azure ne peut être renommée (à l'exception du nom d'un abonnement), il peut être utile d'utiliser cette méthode pour pallier cette lacune.

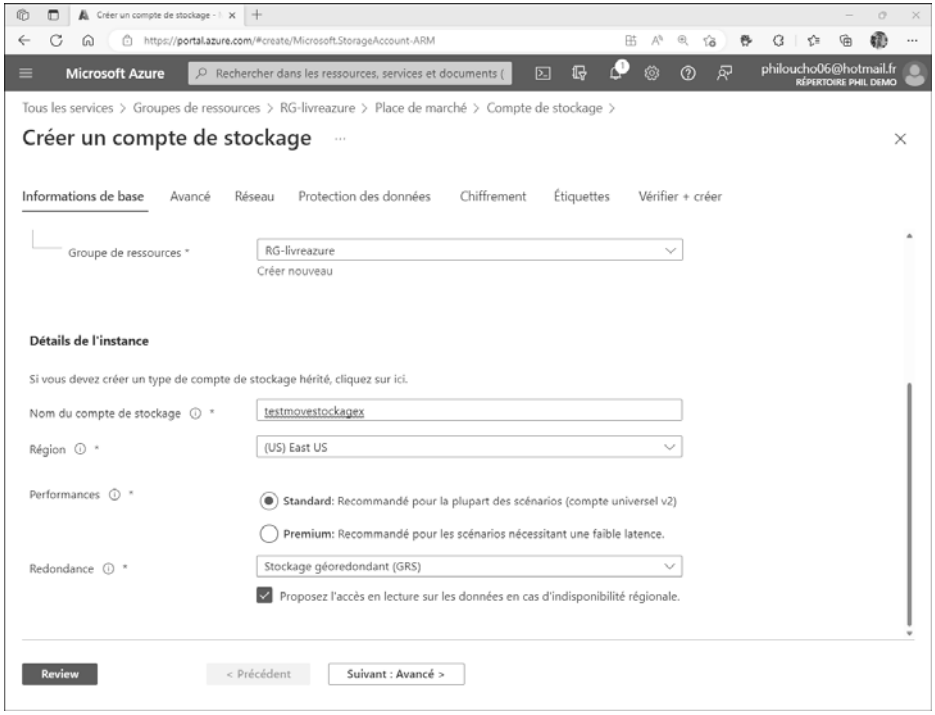
Mais il peut être aussi utile de déplacer une ressource dans un autre groupe de ressources lorsque celle-ci n'a plus le même cycle de vie que son groupe d'appartenance.

Remarque

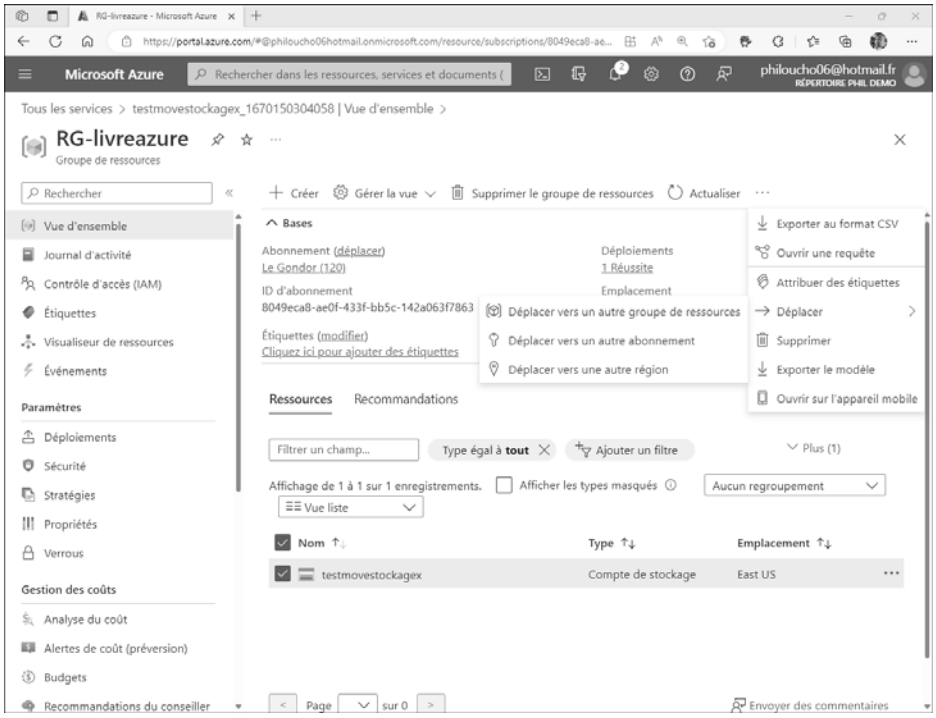
Tous les services Azure ne prennent pas en compte le déplacement des ressources (Application Gateway, ExpressRoute...). Une liste mise à jour des services tolérant les déplacements est disponible via le lien : https://learn.microsoft.com/fr-fr/azure/azure-resource-manager/management/move-support-resources

Vous allez déplacer un compte de stockage créé dans le groupe de ressources **RG-livreazure** vers le groupe de ressources **livreazure** :

- Cliquez sur **Groupes de ressources** depuis le menu d'actions situé à gauche de l'interface, puis sur le groupe de ressources **RG-livreazure**. Cliquez sur **Créer** et saisissez **stockage** puis cliquez sur **Créer**. Dans le champ **Groupe de ressources**, sélectionnez **RG-livreazure**. Dans le champ **Nom du compte de stockage**, saisissez **testmovestockagex** (où x est un chiffre choisi par vos soins). Laissez les autres options par défaut.



- Cliquez sur le bouton **Review** puis sur **Créer**. Patientez quelques instants pendant la création du compte de stockage.
- Cliquez sur le groupe de ressources **RG-livreazure**. Dans le panneau situé en haut de l'interface, sélectionnez le compte de stockage **testmovestockagex** puis cliquez sur **Déplacer** puis sur **Déplacer vers un autre groupe de ressources**.



- Dans le menu déroulant de la section **Groupe de ressources**, sélectionnez **livreazure**. Cliquez sur le bouton **Suivant**. Cochez la case **Je comprends que les outils et les scripts associés aux ressources déplacées ne fonctionnent pas tant que je ne les mets pas à jour pour utiliser de nouveaux ID de ressource**, puis cliquez sur le bouton **Déplacer**.

Le compte de stockage dans le groupe de ressources RG-livreazure va être déplacé dans le groupe de ressources livreazure.

En utilisant Azure PowerShell, l'applet à exécuter est `Move-AzResource`.

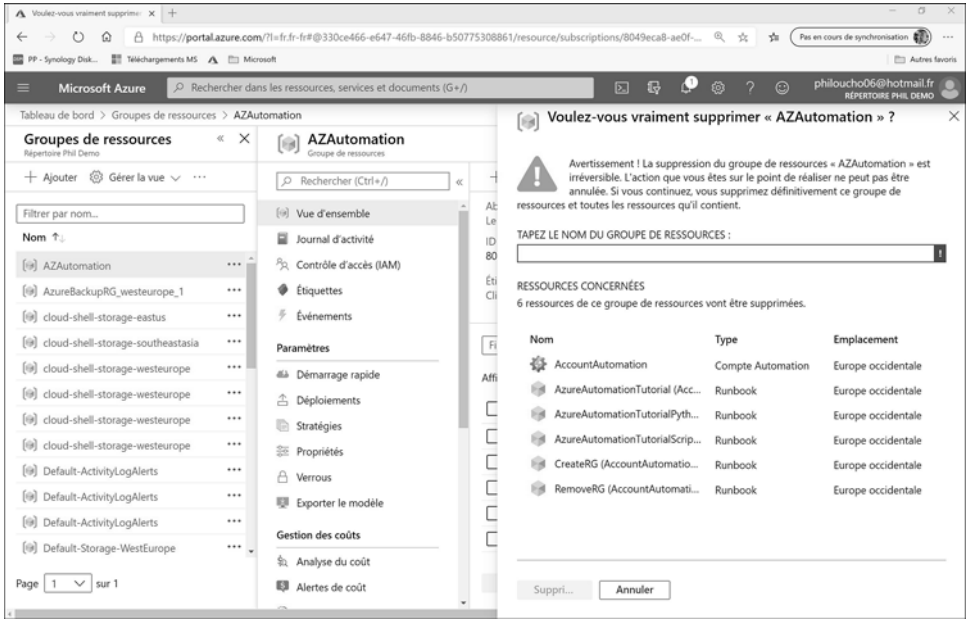
3.3 Suppression d'une ressource ou d'un groupe de ressources

Pour supprimer une ressource spécifique :

- Cliquez dessus dans le groupe de ressources d'appartenance, puis sur **Supprimer**.
- Confirmez la suppression en cliquant sur le bouton **Oui**.

Pour supprimer un groupe de ressources, et par extension, toutes les ressources qu'il contient :

- Cliquez sur **Groupes de ressources** depuis le menu d'actions situé à gauche de l'interface, puis sur le groupe de ressources cible. Dans le panneau de droite, cliquez sur **Supprimer le groupe de ressources**. Saisissez le nom du groupe de ressources et confirmez en cliquant sur le bouton **Supprimer**.



Chapitre 4
Gestion des appareils

1. Introduction

Comme les utilisateurs, les appareils et applications doivent être gérés. Cette gestion doit être bien entendu 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 policies 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 :

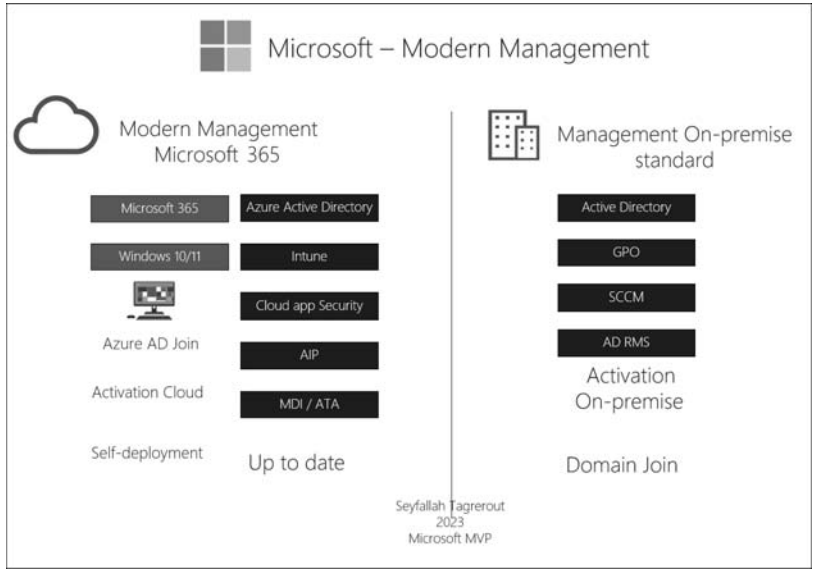
E3 : dans ce plan, il sera possible de bénéficier des suites ci-dessous :

- 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 Modem 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 policies 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.

L'exemple le plus concret est l'Azure Active Directory : nous pourrons 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

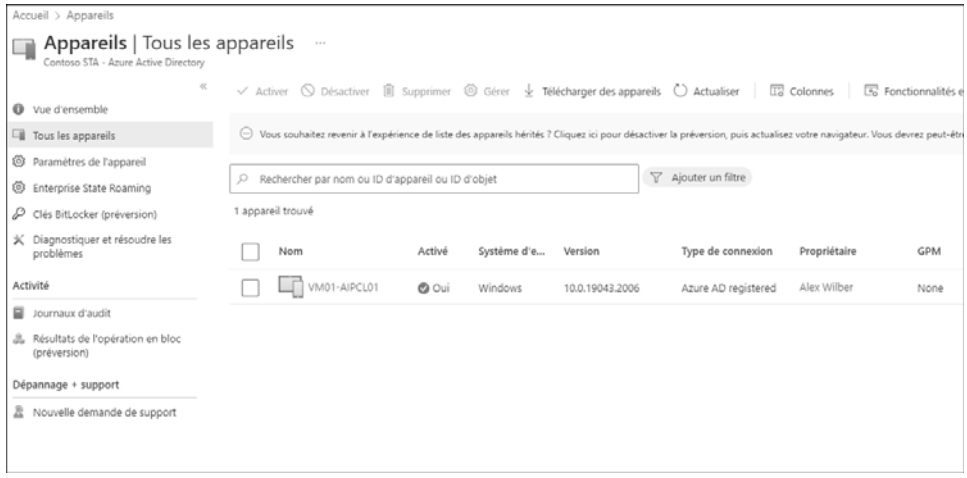
Nous allons étudier ci-après la différence existant entre chacun de ces modes et leurs apports.

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 :

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).

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 multifacteur 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 :